Source : https://youtu.be/cUhAyyzlv20 (whole playlist)

Slides : https://www.mobilefish.com/developer/lorawan/lorawan_quickguide_tutorial.html

Range vs Power

LPWAN stands for Low Power Wide Area Network and this type of wireless communication is designed for sending small data packages over long distances, operating on a battery

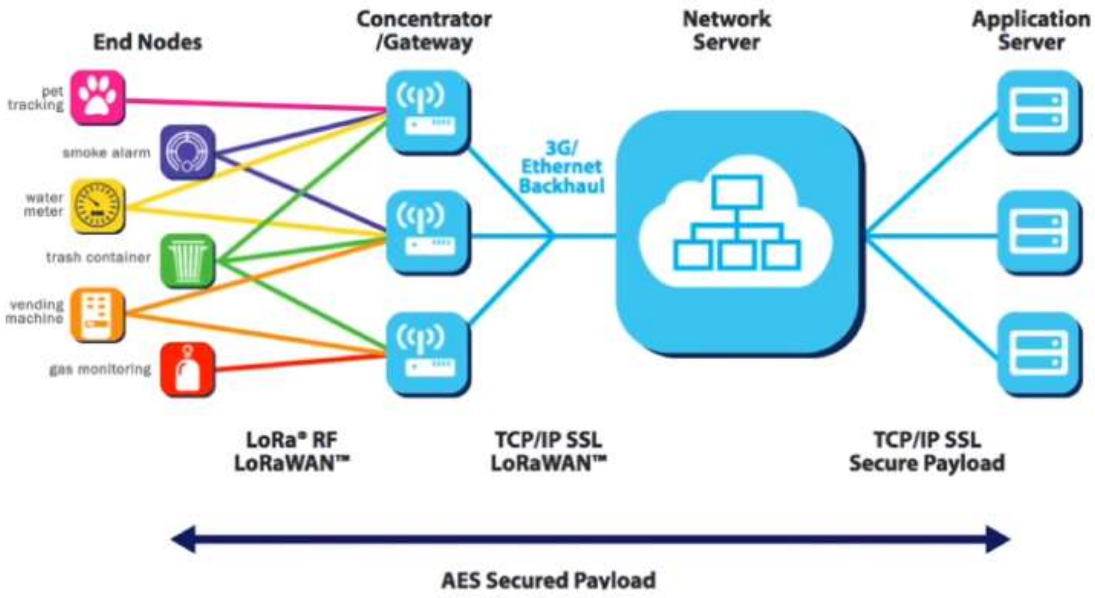
Technology	Wireless Communication	Range	Tx Power
Bluetooth	Short range	10 m	2.5 mW
Wifi	Short range	50 m	80 mW
3G/4G	Cellular	5 km	5000 mW
LoRa	LPWAN	• 2-5 km (urban) • 5-15 km (rural) • > 15 km (LOS)	20 mW

LoRa modulation / radio part -> closed sources

Between 0.3 kbps to 5.5 kbps.

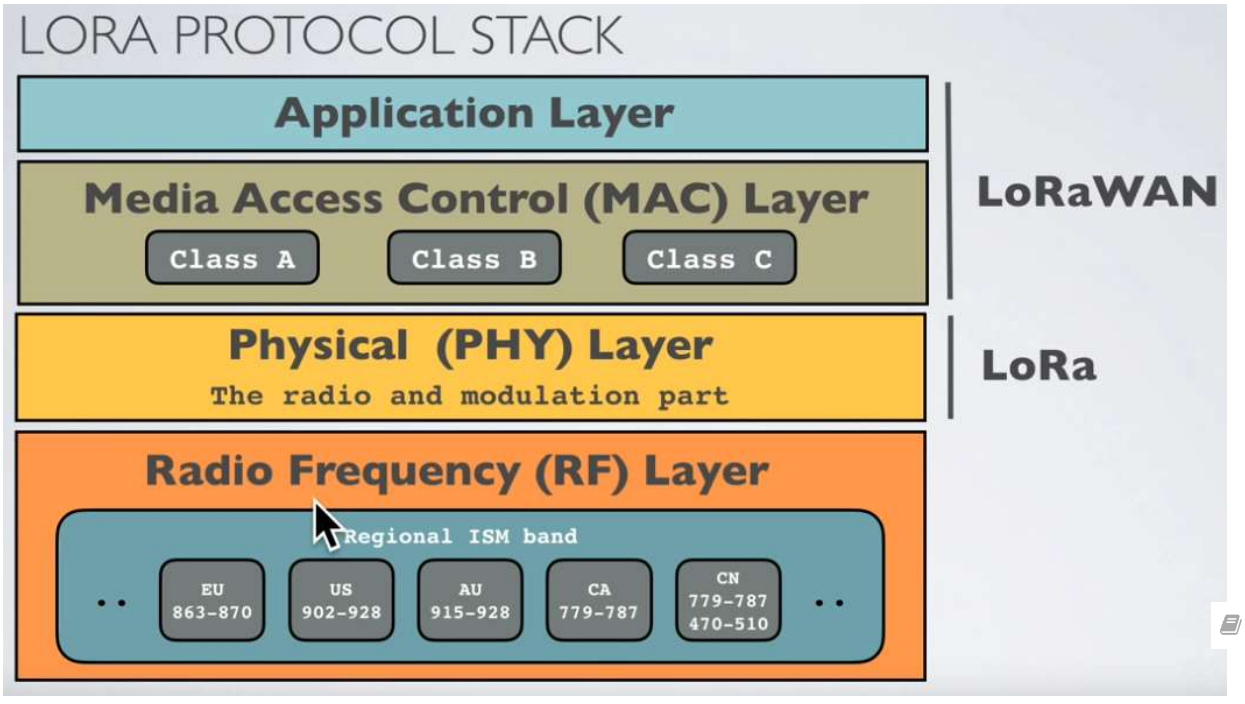
LoRa networks

- Gateways can handle 100s of devices at the same time.
- The gateways can listen to multiple frequencies simultaneously, in every spreading factor at each frequency.
- Communications are bidirectional



- uplink : end node -> gateways
- downlink : gateway -> end node
- The LoRaWAN protocol does not support direct communication between end nodes. If you want direct communication between LoRa devices without the use of gateways, use the RadioHead Packet Radio library for embedded microprocessors. It provides a complete object-oriented library for sending and receiving packet sized messages via a variety of radios such as LoRa on a range of embedded microprocessors: https://www.airspayce.com/mikem/arduino/RadioHead

LoRa protocol stack



General considerations

LoRa operates in the unlicensed ISM (Industrial, Scientific and Medical) radio band that are available worldwide.

Region	Frequency (MHz)
Asia	433
Europe, Russia, India, Africa (parts)	863-870
US	902-928

Region	Frequency (MHz)
Australia	915-928
Canada	779-787
China	779-787, 470-510

A more detailed list of LoRa frequencies used per country can be found at:

https://www.thethingsnetwork.org/docs/lorawan/frequencies-by-country.html

https://www.thethingsnetwork.org/docs/lorawan/frequency-plans.html

https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf

In Europe the European Telecommunications Standards Institute (ETSI) creates standards which are used by local (= country) regulatory authorities.

https://www.etsi.org/

In the US the Federal Communications Commission (FCC) creates these standards.

https://www.fcc.gov/

ISM band advantages:

- Anyone is allowed to use these frequencies.
- No license fee is required.

ISM band disadvantages:

- Low data rate.
- Lots of interference because anyone can use these frequencies.

In Europe

For example in Europe when using the ISM band frequencies (863 MHz - 870 MHz) users must comply to the following rules:

- For uplink, the maximum transmission power is limited to 25mW (14 dBm).
- For downlink (for 869.525MHz), the maximum transmission power is limited to 0.5W (27 dBm)
- There is an 0.1% and 1.0% duty cycle per day depending on the channel.
- Maximum allowed antenna gain +2.15 dBi.

Besides these ISM band rules, the network operator (for example The Things Network) can also add additional restrictions.

The Things Network restrictions

If you use The Things Network (free public community LoRaWAN network), the following fair use policy applies:

- The uplink airtime is limited to 30 seconds per day (24 hours) per node.
- The downlink messages are limited to 10 messages per day (24 hours) per node.

More information about the TTN fair use policy: https://www.thethingsnetwork.org/docs/lorawan/duty-cycle.html

Duty cycle / time on air (ToA)

When a signal is send from a sender it takes a certain amount of time before a receiver receives this signal. This time is called **Time on Air (ToA)**.

Duty cycle is the proportion of time during which a component, device, or system is operated. The duty cycle can be expressed as a ratio or as a percentage. As mentioned previously in Europe there is a 0.1% and 1.0% duty cycle per day depending on the channel.

To respect the 1% duty cycle :

For example : ToA = 530ms => affer sending a message, we have to wait 99x530ms = 52.47s before sending a new message.

LoRaWAN Device Classes

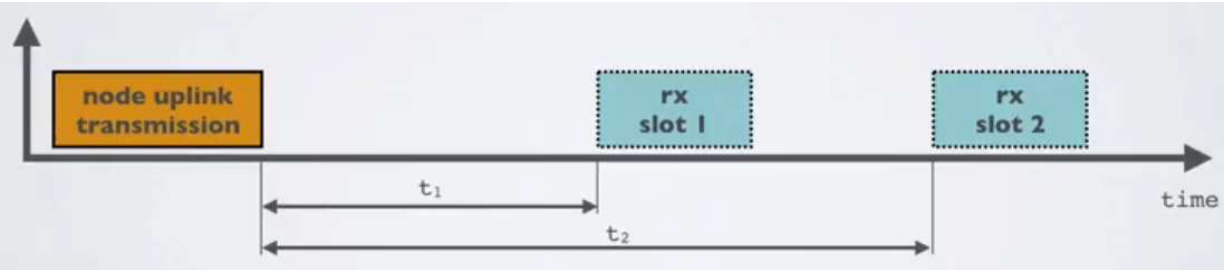
The LoRaWAN specification defines three device classes:

- A(ll) Battery powered devices. Each device uplink to the gateway and is followed by two short down-link receive windows.
- B(eacon) Same as class A but these devices also opens extra receive windows at scheduled times.
- C(ontinuous) Same as A but these devices are continuously listening. Hence these devices uses more power and are often mains powered.

Class A

At any time an end node can broadcast a signal. After this uplink transmission (tx) the end node will listen for a response from the gateway.

The end node opens two receive slots at t1 and t2 seconds after an uplink transmission. The gateway can respond within the first receive slot or the second receive slot, but not both. Class B and C devices must also support class A functionality.

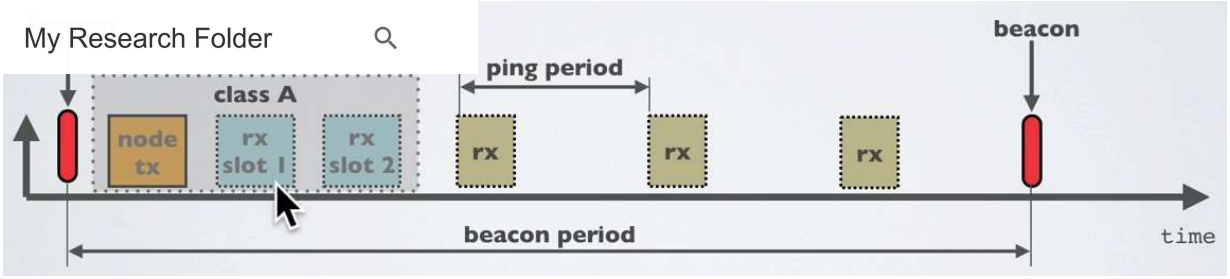


Note : "All" means the class A mode is supported by all classes.

Class B

In addition to Class A receive slots, class B devices opens extra receive slots at scheduled times.

The end node receives a time synchronised beacon from the gateway, allowing the gateway to know when the node is listening. A class B device does not support device C functionality.



Class C

In addition to Class A receive slots a class C device will listen continuously for responses from the gateway. A class C device does not support device B functionality.

dBm, dBi, dBd

- dBm : reference is 1mW
- dBi : refers to the antenna gain with respect to an isotropic antenna
- dBd : dBd refers to the antenna gain with respect to a reference dipole antenna

dBi = dBd + 2.15

Free space losses

L(fs) = 32.45 + 20log(D) + 20log(f)

- Lfs = Free space loss in dB
- D = Distance between end node and gateway in km
- f = frequency in MHz

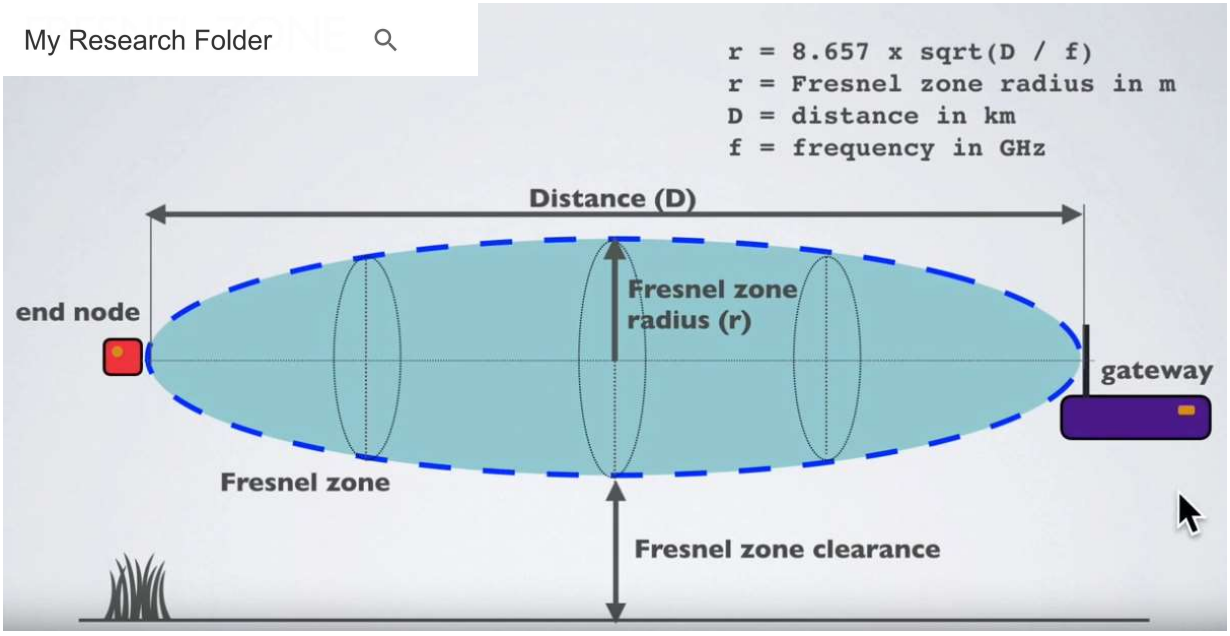
For example: f=868MHz

- D=0.01 km, Lfs = 32.45 + 20log(0.01) + 20log(868) = 51 dB
- D=0.05 km, Lfs = 32.45 + 20log(0.05) + 20log(868) = 65 dB
- D=0.10 km, Lfs = 32.45 + 20log(0.10) + 20log(868) = 71 dB
- D=0.50 km, Lfs = 32.45 + 20log(0.50) + 20log(868) = 85 dB
- D=1.00 km, Lfs = 32.45 + 20log(1.00) + 20log(868) = 91 dB

Fresnel zone

The Fresnel zone is an elliptical shaped body around the direct line of sight path between the end node and the gateway.

Any obstacle within this volume, for example buildings, trees, hilltops or ground can weaken the transmitted signal even if there is a direct line of sight between the end node and the gateway.



=> avoid objects within the Fresnel zone

Earth curvature influence :

- To calculate height H:

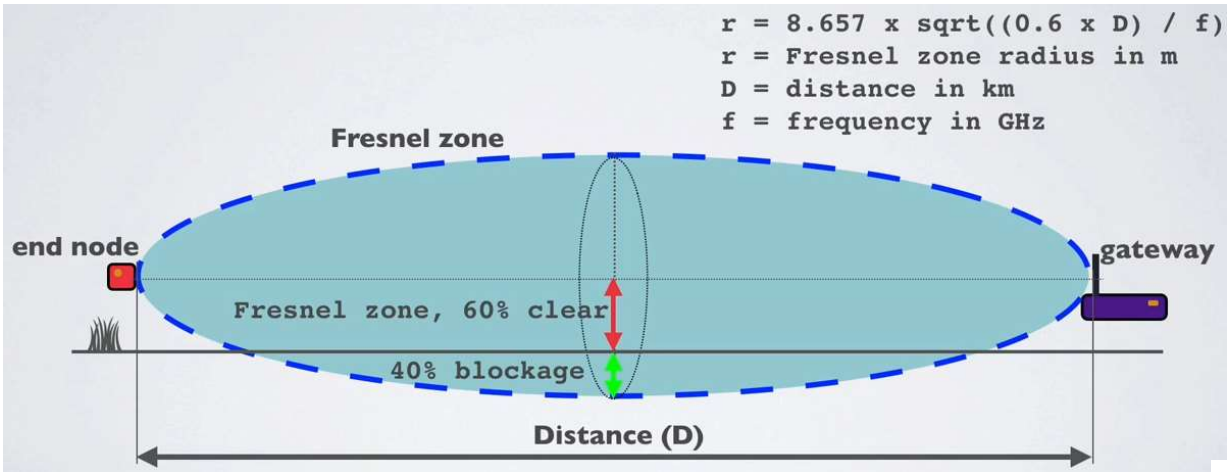
$$H = 1000 \times D^2 / (8 \times R_{earth})$$

H = Height (or earth curvature allowance) in m
D = Distance between end node and gateway in km
R_{earth} = Earth radius in km = 8504 km

Distance (km)	Height (m)
0.1	Negligible
0.5	Negligible
1	Negligible
2	Negligible
5	0.4

Distance (km)	Height (m)
10	1.5
15	3.3
20	5.9
25	9.2
30	13.2

As a rule of thumb Fresnel zone should always be clear of obstruction but this can be impractical so it is said that beyond 40% blockage, signal loss will become significant.



Example :

- r+H : minimum end node and gateway height above ground

Example: f = 868 MHz = 0.868GHz H is the earth curvature allowance.
100% clear: **r = 8.657 x sqrt(D / f)**, 60% clear: **r = 8.657 x sqrt((0.6xD) / f)**

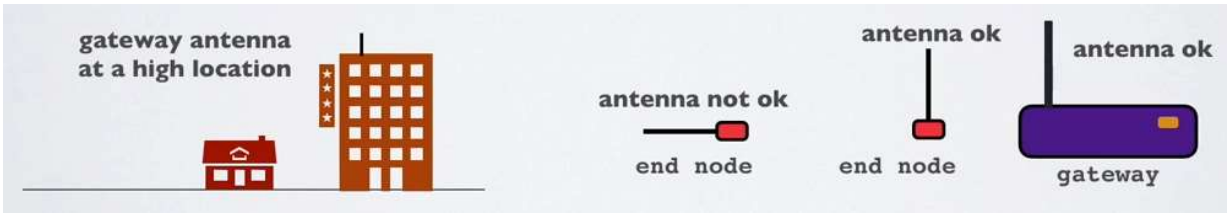
100 % clear

D (m)	D (km)	r (m)	r + H (m)
100	0.1	2.94	2.94
500	0.5	6.57	6.57
1000	1.0	9.29	9.29
2000	2.0	13.14	13.14
5000	5.0	20.78	21.18
10000	10.0	29.38	30.88

60 % clear

D (m)	0.6 x D (km)	r (m)	r + H (m)
100	0.06	2.28	2.28
500	0.3	5.09	5.09
1000	0.6	7.20	7.20
2000	1.2	10.18	10.18
5000	3.0	16.09	16.49
10000	6.0	22.76	24.26

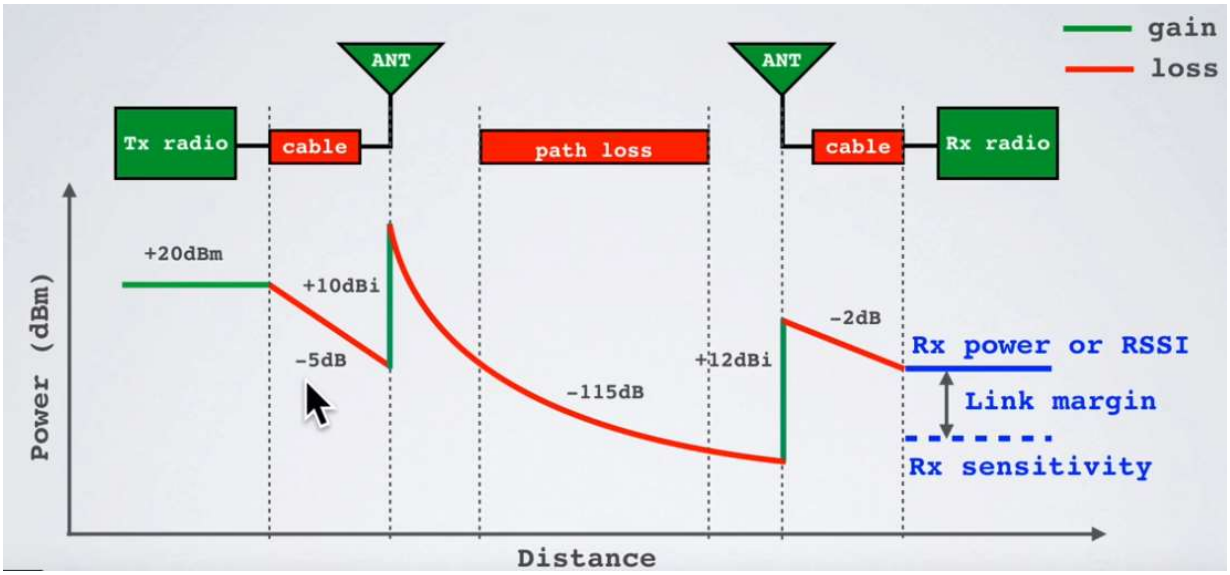
- For the best radio signal performance: The gateway antenna must be placed outdoors at a high location (avoiding obstacles in the Fresnel zone).
- The antenna design for both gateway and end nodes must be optimised for its regional frequency.
- Keep the antenna polarisation vertical for both gateway and end nodes and use omnidirectional antenna to cover a large area.



Link Budget

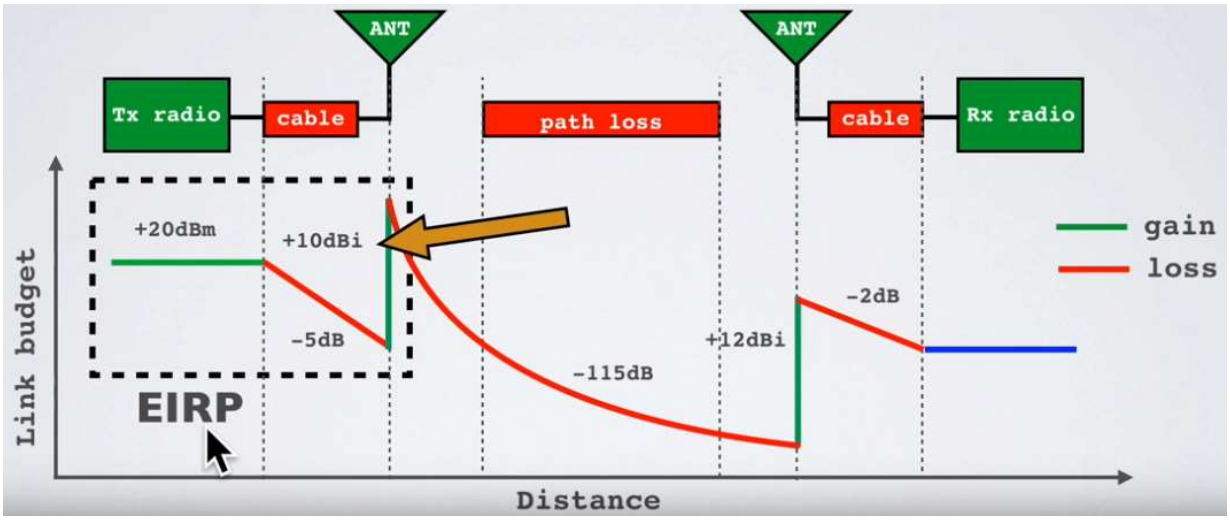
A link budget is the sum of all of the gains and losses from the transmitter, through the medium (aka free space), to the receiver in a telecommunication system. It is a way of quantifying the link performance.

The receiver sensitivity is the lowest power level at which receiver can receive or demodulate the signal.

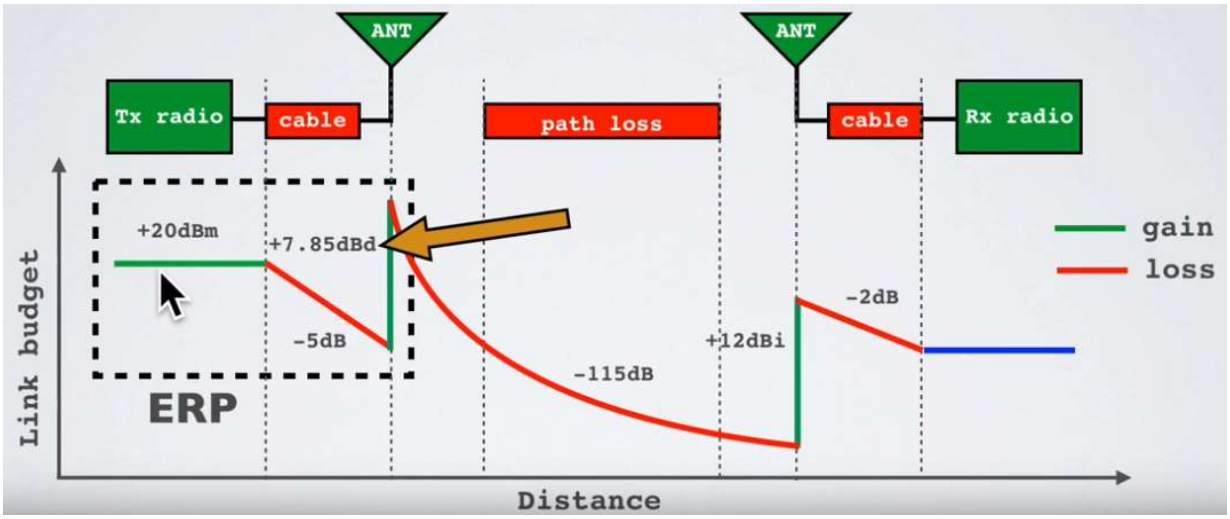


EIRP and ERP

EIRP) is the total power radiated by a hypothetical isotropic an-



The Effective Radiated Power (ERP) is the total power radiated by an actual antenna relative to a half-wave dipole rather than a theoretical isotropic antenna.



EIRP = Tx power (dBm) + antenna gain (dBi) - cable loss (dBm)

For example: EIRP = 20 + 10 - 5 = 25 dBm

ERP = Tx power (dBm) + antenna gain (dBd) - cable loss (dBm)

For example: ERP = 20 + 7.85 - 5 = 22.85 dBm

Relationship EIRP and ERP: EIRP (dBm) = ERP (dBm) + 2.15

What is the purpose of ERP and EIRP?

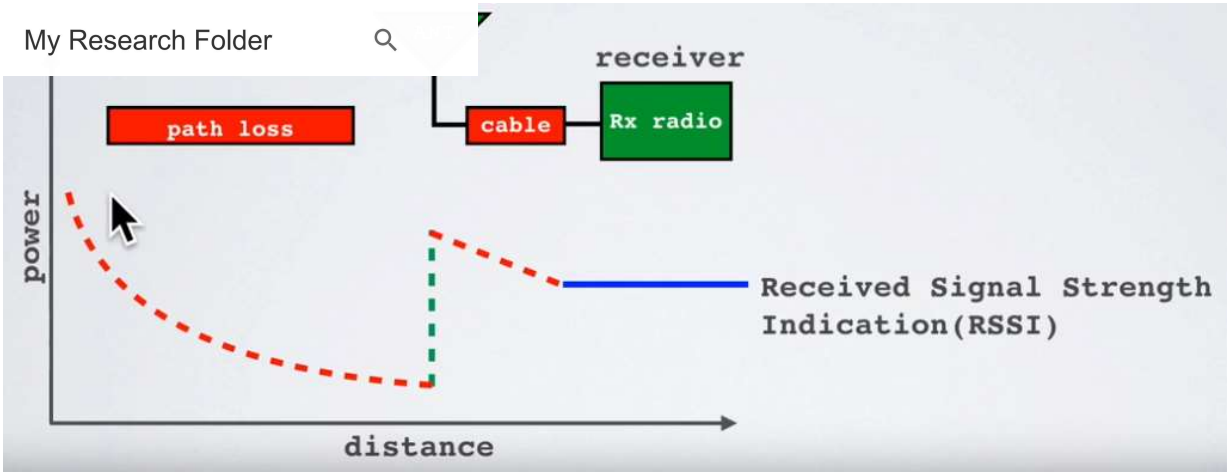
RF transmitting systems must adhere to certain rules set by the regulatory bodies such as FCC or ETSI.

One of these rules: radio devices must not exceed certain ERP or EIRP values set by these regulatory bodies.

RSSI

The Received Signal Strength Indication (RSSI) is the received signal power in milliwatts and is measured in dBm.

This value can be used as a measurement of how well a receiver can “hear” a signal from a sender.



The RSSI is measured in dBm and is a negative value.

The closer to 0 the better the signal is.

Typical LoRa RSSI values are:

RSSI minimum = -120 dBm.

- If RSSI=-30dBm: signal is strong.
- If RSSI=-120dBm: signal is weak.

SNR

Signal-to-Noise Ratio (SNR) is the ratio between the received power signal and the noise floor power level.

The noise floor is an area of all unwanted interfering signal sources which can corrupt the transmitted signal and therefore re-transmissions will occur.

- If SNR is greater than 0, the received signal operates above the noise floor.
- If SNR is smaller than 0, the received signal operates below the noise floor.

Normally the noise floor is the physical limit of sensitivity, however LoRa works below the noise level.

Typical LoRa SNR values are between: -20dB and +10dB

A value closer to +10dB means the received signal is less corrupted.

LoRa can demodulate signals which are -7.5 dB to -20 dB below the noise floor.

Frequencies

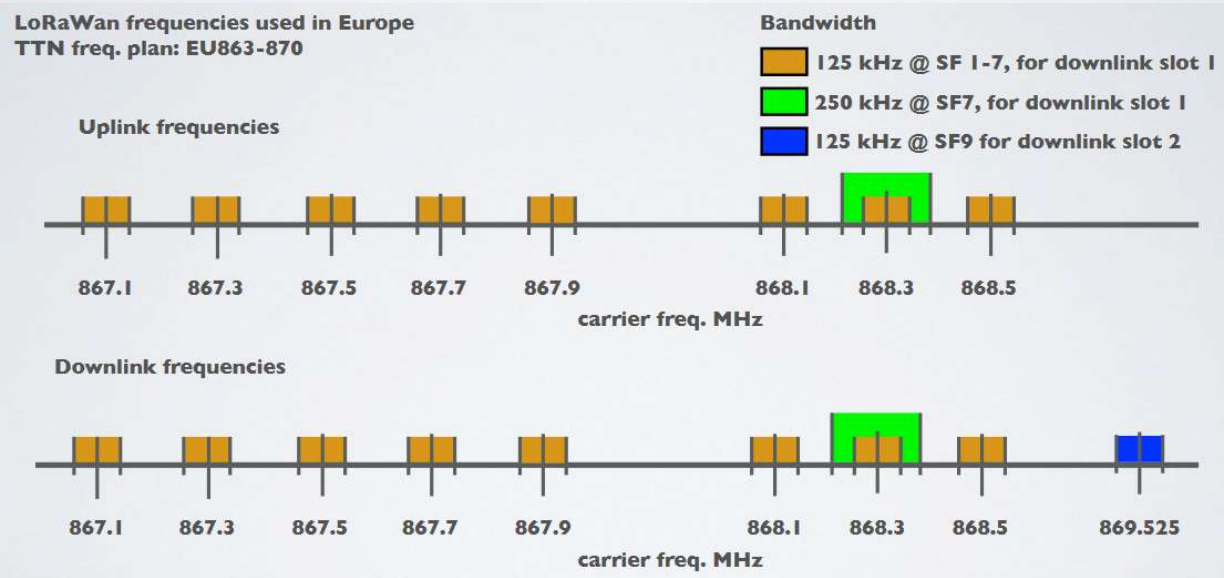
Regional LoRa Alliance parameters :

https://lora-alliance.org/lorawan-for-developers

		SPREADING FACTOR & BANDWIDTH RANGE
0	868.1	SF7BW125 to SF12BW125
1	868.3	SF7BW125 to SF12BW125 and SF7BW250
2	868.5	SF7BW125 to SF12BW125
3	867.1	SF7BW125 to SF12BW125
4	867.3	SF7BW125 to SF12BW125
5	867.5	SF7BW125 to SF12BW125
6	867.7	SF7BW125 to SF12BW125
7	867.9	SF7BW125 to SF12BW125
8	868.8	FSK

Downlink : same as uplink with an additional one :

Download freq (MHz)	SPREADING FACTOR & BANDWIDTH RANGE
	Uplink channels 0-8 (RX1)
869.525	SF9BW125 (RX2 downlink only)



If your country uses the EU863-870 ISM band, than according to the LoRaWAN Regional Parameters document every EU868MHz end device must implement the following default channels:

- 868.10 MHz, bandwidth = 125 kHz
- 868.30 MHz, bandwidth = 125 kHz
- 868.50 MHz, bandwidth = 125 kHz

and additional 5 frequencies.

The other 5 frequencies can be freely attributed by the network operator. For example, The Things Network implemented the following frequencies: 867.1, 867.3, 867.5, 867.7 and 867.9.

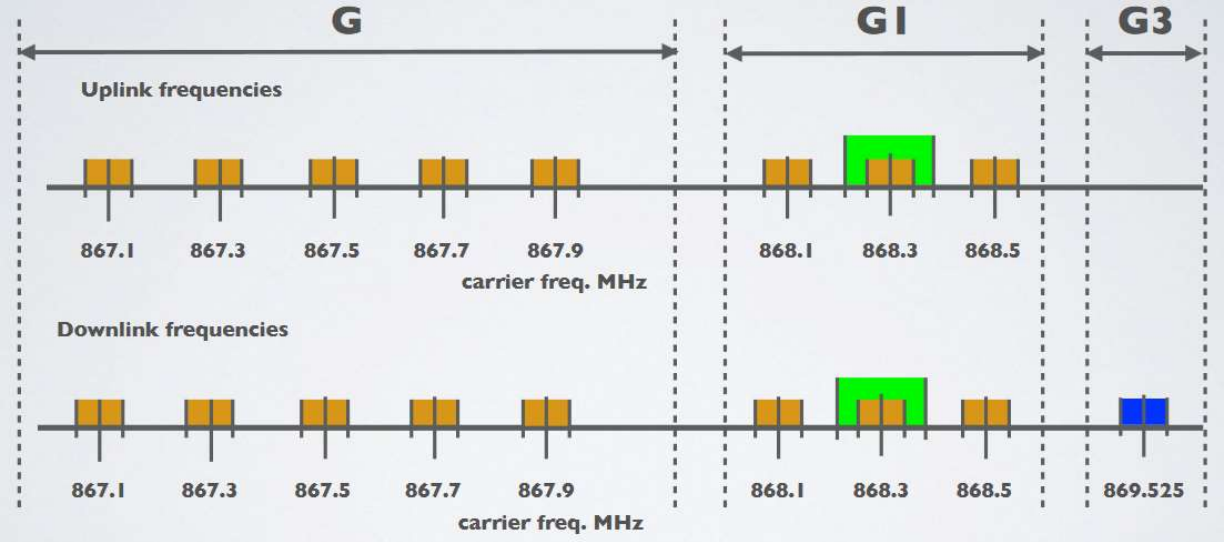
LoRaWAN only uses the following bandwidth ranges: 125 kHz, 250 kHz and 500 kHz.

Which of these 3 ranges are actual used depends on the region or frequency plan.

For example in Europe only the bandwidths 125kHz and 250 kHz are used.

ETSI Sub bands 863-870

		Limitations
G	863.0 - 868.0	EIRP<25 mW - duty cycle < 1%
G1	868.0 - 868.6	EIRP<25 mW - duty cycle < 1%
G2	868.7 - 869.2	EIRP<25 mW - duty cycle < 0.1%
G3	869.4 - 869.65	EIRP<500 mW - duty cycle < 10%
G4	869.7 - 870.0	EIRP<25 mW - duty cycle < 1%

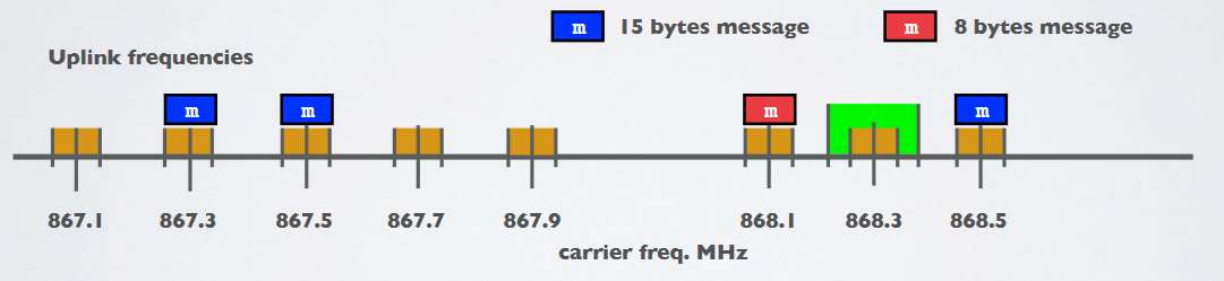


Changing frequencies for every transmission

An end device changes channel in a pseudo-random fashion for every transmission.

Changing frequencies makes the system more robust to interferences.

For example in Europe for uplink transmissions 8 different frequencies are used.



Dwell time & hop time

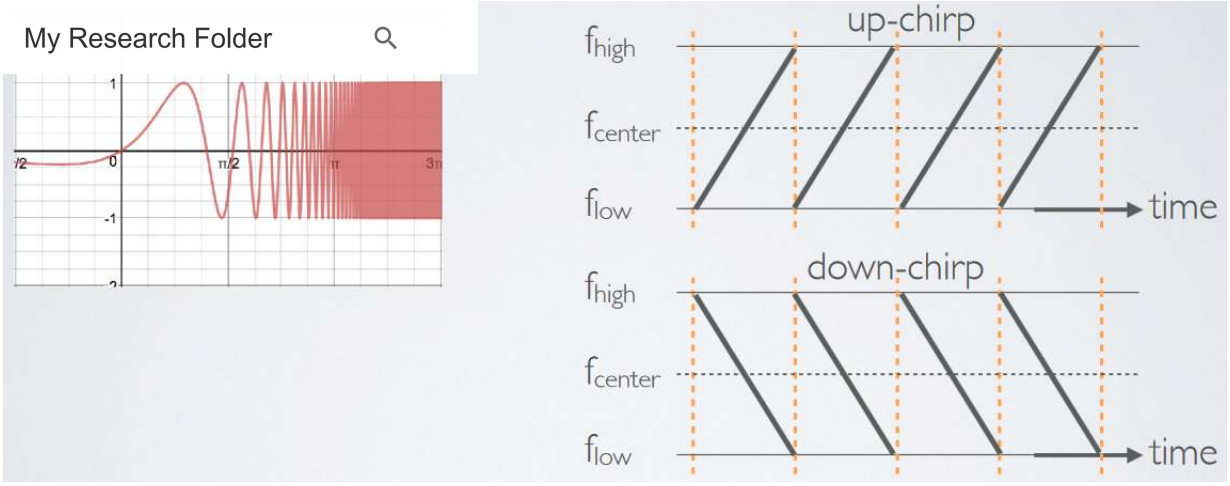
Dwell time (or transmit time) is the amount of time needed to transmit on a frequency.

Hop time is the amount of time needed to change from one frequency to another in which the radio is not transmitting

Modulation Types and Chirp Spread Spectrum

TO CHECK

- LoRa is a proprietary spread spectrum modulation scheme that is based on Chirp Spread Spectrum modulation (CSS).
- **Chirp** Spread Spectrum is a spread spectrum technique that uses wideband linear frequency modulated chirp pulses to encode information. A chirp pulse is a sweep in frequency on the corresponding bandwidth (125kHz, 250kHz...) defined earlier. Here



- **Spread spectrum** techniques are methods by which a signal is deliberately spread in the frequency domain. For example a signal is transmitted in short bursts, "hopping" between frequencies in a pseudo random sequence.

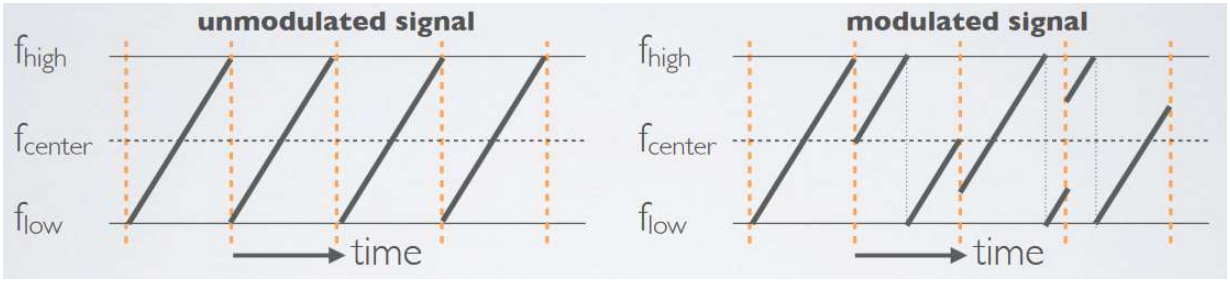
Symbol, Spreading Factor and Chip

TO CHECK

https://electronics.stackexchange.com/questions/278192/understanding-the-relationship-between-lora-chips-chirps-symbols-and-bits

To generate symbols/chirps, the modem modulates the phase of an oscillator. The number of times per second that the modem adjusts the phase is called the **chip rate** and defines the modulation bandwidth. Chip rate is a direct subdivision of the quartz frequency (32 MHz).

Basic chirps are simply a ramp from fmin to fmax (up-chirp) or fmax to fmin (down-chirp). Data-carrying chirps are chirps that are cyclically-shifted, and this cyclical shift carries the information.



Spreading Factor (SF) : defines the number of bits that can be encoded by a symbol.

LoRaWan packets format

```
example : 80C02301260021000266EEA76CCE0C1BBC7A36F69F
80      C0230126   00      2100   02      66EEA76CCE0C1BBC   7A36F69F
MTYPE   devaddr    FCtrl   FCnt   FPort   DATA               MIC
```

Decrypt raw LoRaWan packets

```
from lora.crypto import loramac_decrypt

payload = '80C02301260021000266EEA76CCE0C1BBC7A36F69F'
sequence_counter = int(payload[14:16] + payload[12:14], 16)
app_session_key = '91299DA630B26526967B442361820CAD'
dev_addr = payload[8:10] + payload[6:8] + payload[4:6] + payload[2:4]
decrypted_payload = loramac_decrypt(
                                payload[18:34],
```

```
                                    equence_counter,
                                    op_session_key,
                                   uev_addr)
# Result : 0xbe 0xef 0xde 0xad 0xbe 0xef 0xde 0xad
```