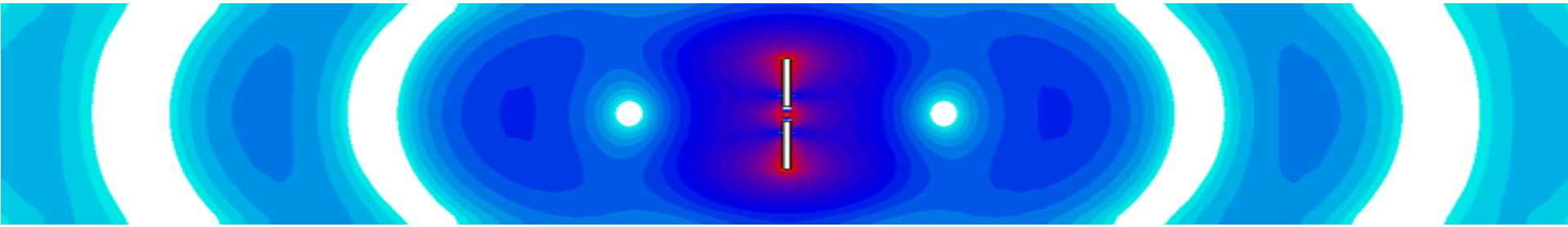
Laboratory of Electronics
Antennas and Telecommunications

LABORATOIRE D'ELECTRONIQUE
ANTENNES ET TELECOMMUNICATIONS



LP-WAN Technology

Ver. 1.35 - 2024

Fabien Ferrero
Université Côte d'Azur

Seminar Objectives

- Key physical parameters for IoT applications
- Provide a complete view of LoRa protocol from the physical layer to the MAC layer
- Practical labs using a miniature terminal to LoRaWAN protocol

Labs report

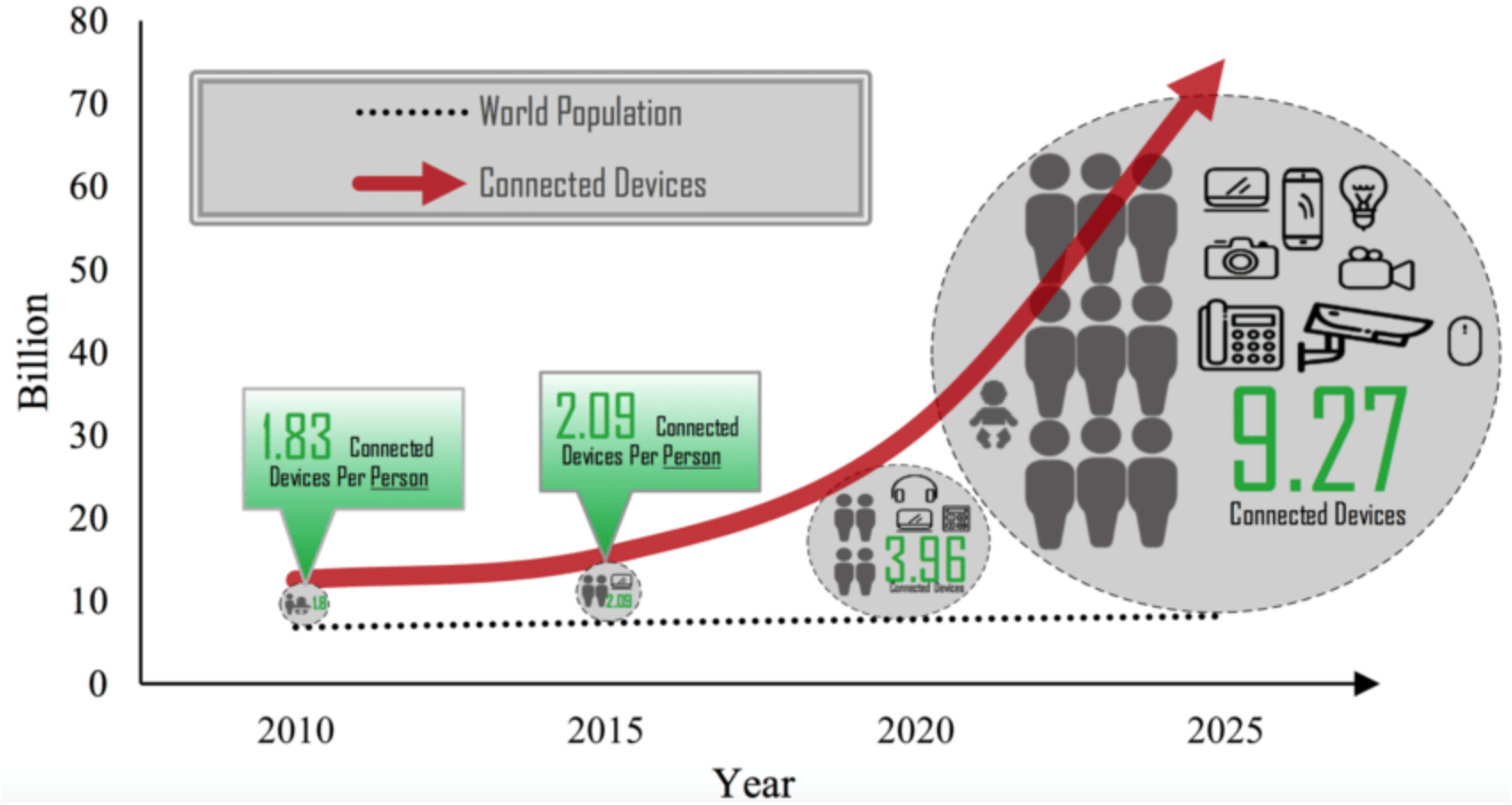
- Small report on the lab :

- « What is the advantages and drawback of a LoRaWan protocol?»

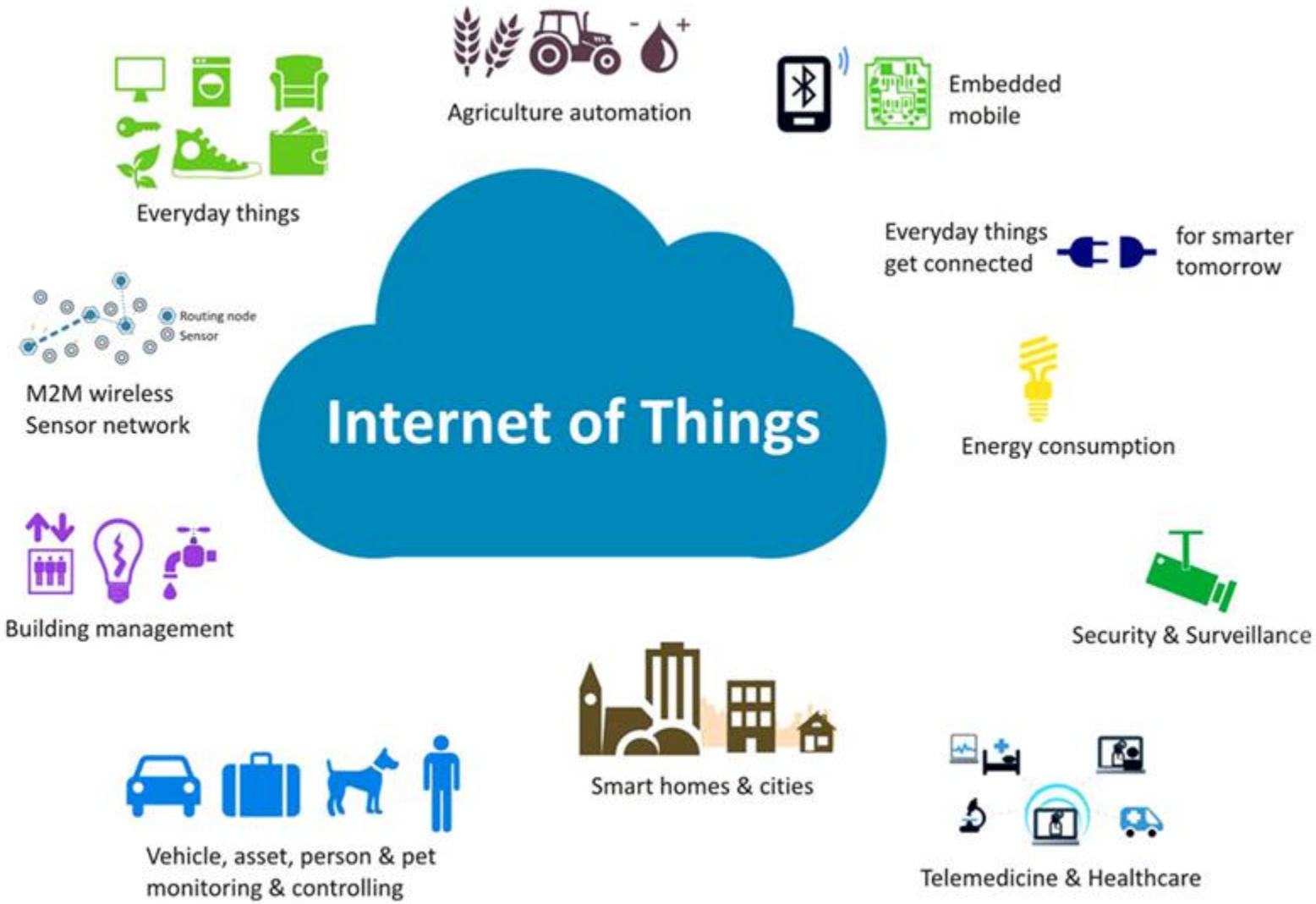
Outline

0. Introduction
I. Wireless Propagation
II. Physical layer : Bands & Modulation
III. MAC layer (LoRaWAN) and security

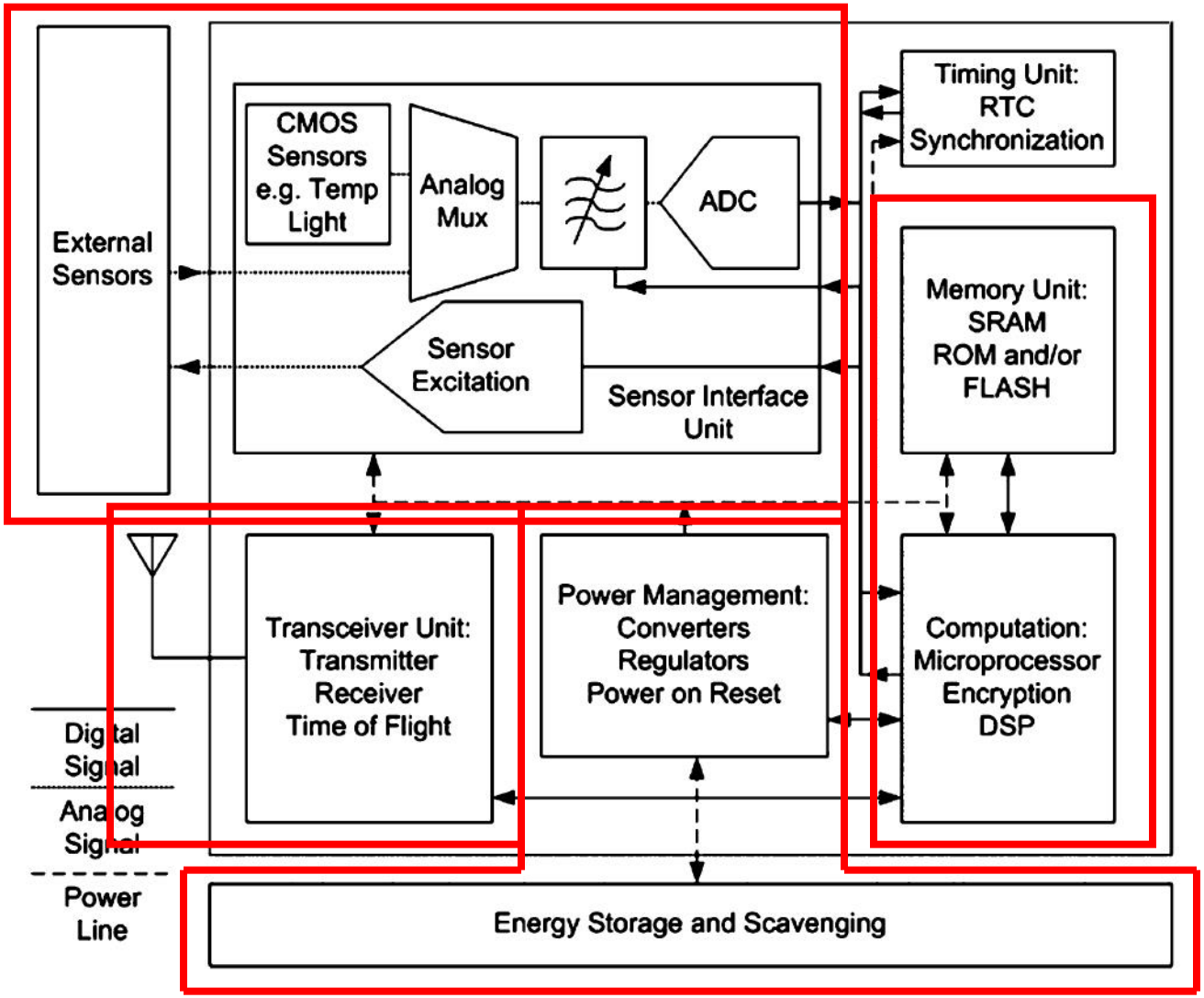
“Thing” connected to the internet



Internet of Things



Anatomy of an IoT device



Outline

0. Introduction
I. Wireless Propagation
II. Physical layer : Bands & Modulation
III. MAC layer (LoRaWAN) and security

Wireless propagation

How does a wireless communication work ?

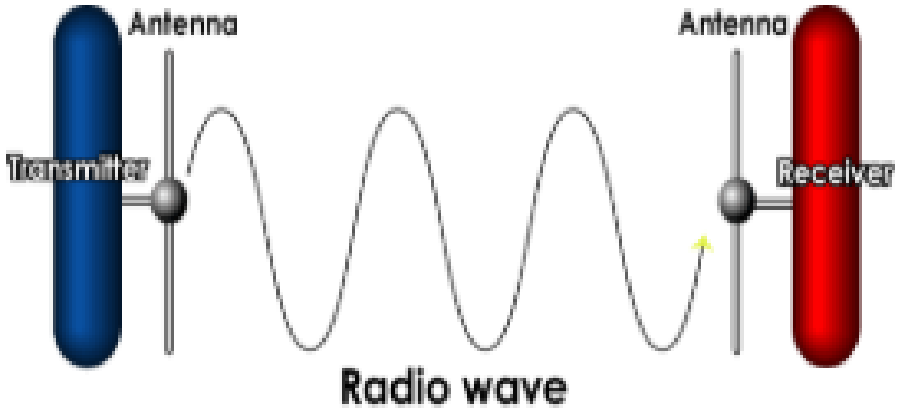
What is the physical phenomenon used to transport information between two separated places ?

What is the influence of distance on the communication link ?

Wireless propagation

Wireless communication use electromagnetic waves to transmit information

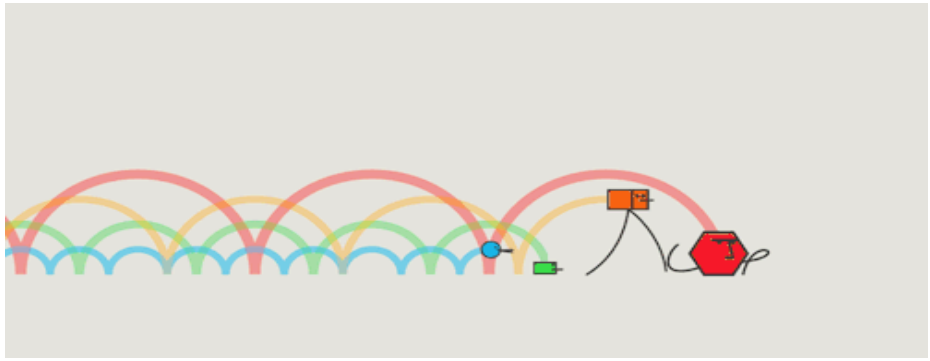
Antenna is a **reciprocal** transducer that convert an electrical signal into an electromagnetic wave (and the reverse operation)

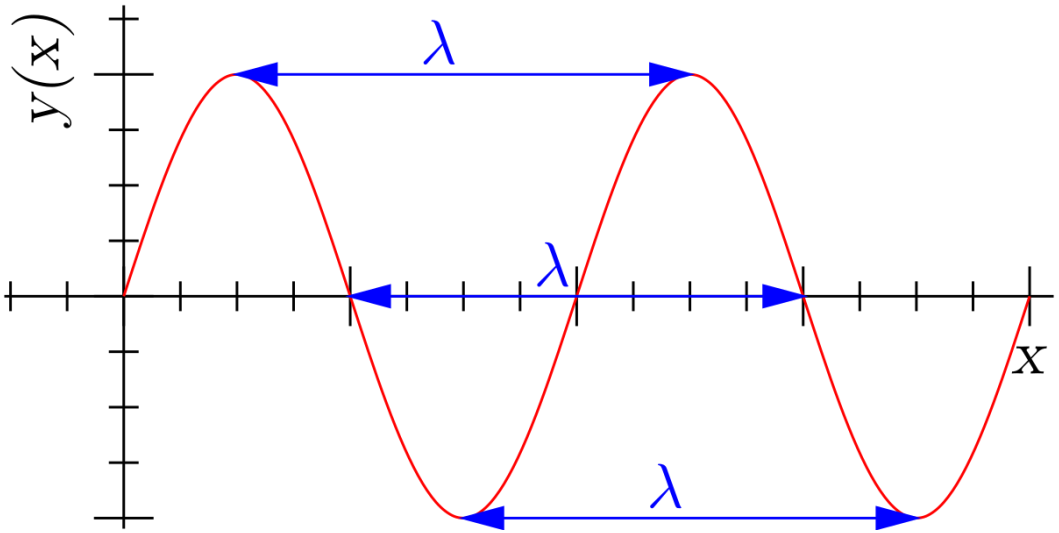


It is important to predict the evolution of the wave between the transmitter and the receiver

Wavelength

In physics, the wavelength is the spatial period of a periodic wave
The distance over which the wave's shape repeats.





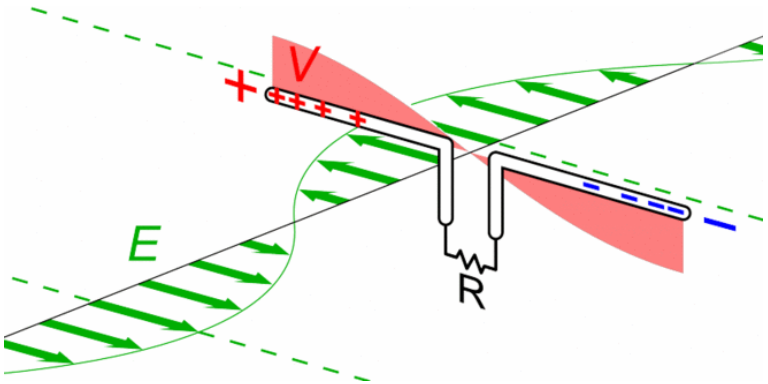
$$\lambda = \frac{c}{f}$$

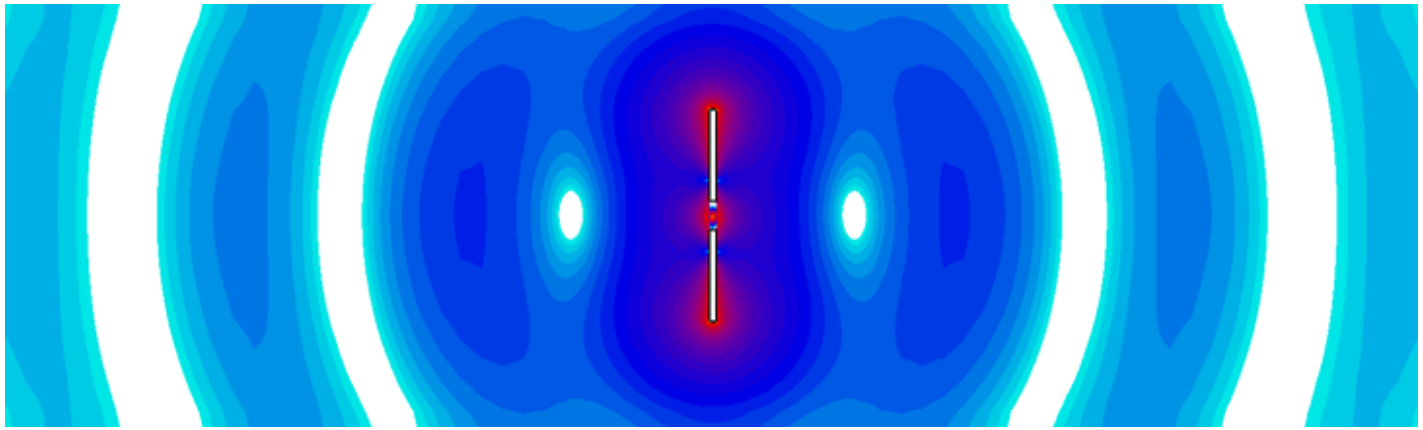
With c being the speed of light $c=3.10^8$

And f the frequency of the electro-magnetic wave

Antenna parameters

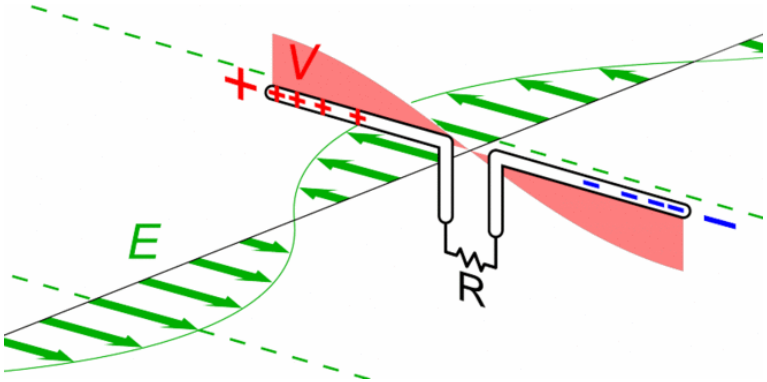
- Antenna is transducer
  - Current and voltage oscillate in the structure
  - Voltage induces electric field
  - Current induces magnetic field
  - Local variation of electric and magnetic field generate an electro-magnetic wave





Antenna parameters

- Antenna is a resonnant structure
  - Limited frequency bandwidth



  - Totat efficiency η_{rad} is the ratio between the radiated power Prad and the power injected into the antenna.

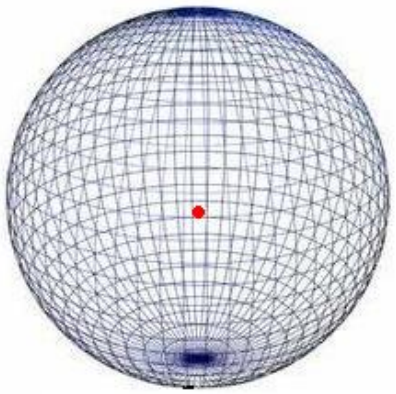
$$\eta_{rad} = {P_{rad}}/{P_{in}}$$

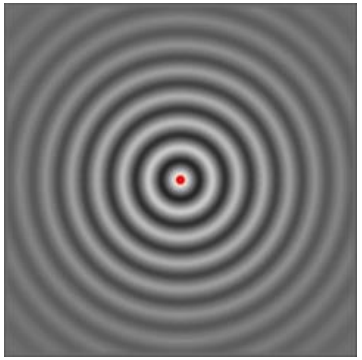
  - Antenna can have a low efficiency due to metallic or dielectric losses
  - The size of an antenna is proportional to the wavelength

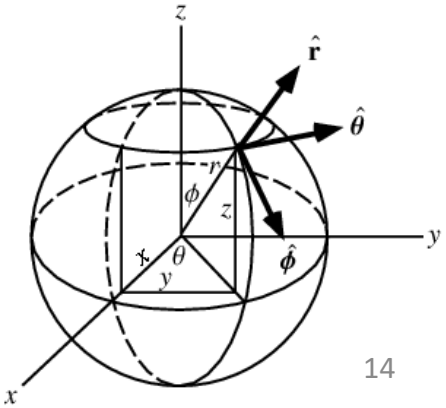
$$l_{ant} \propto \lambda$$

Isotropic Antenna

- An isotropic antenna is a theoretical antenna that radiates equally in all directions
- It is a loss-less antenna $\eta_{rad} = 1$
- It is impossible to build
- It is used as a reference for antenna gain
- Gain referenced to an isotropic radiator is in dBi





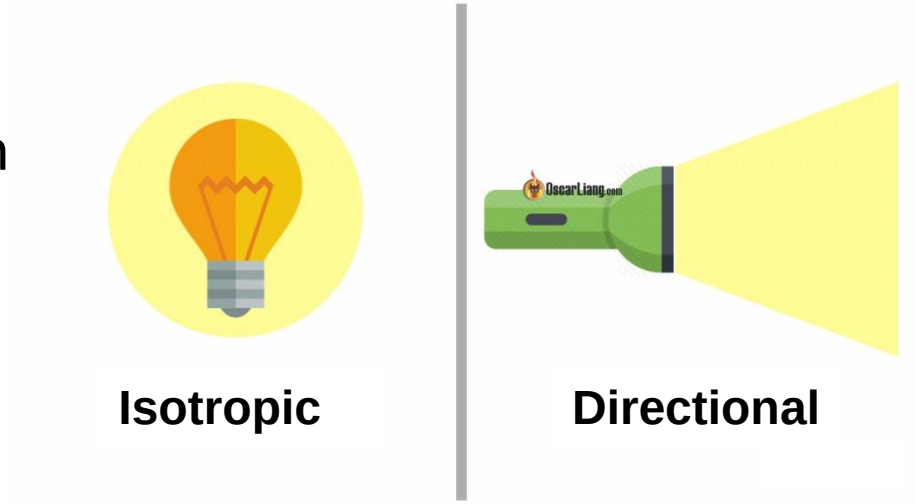


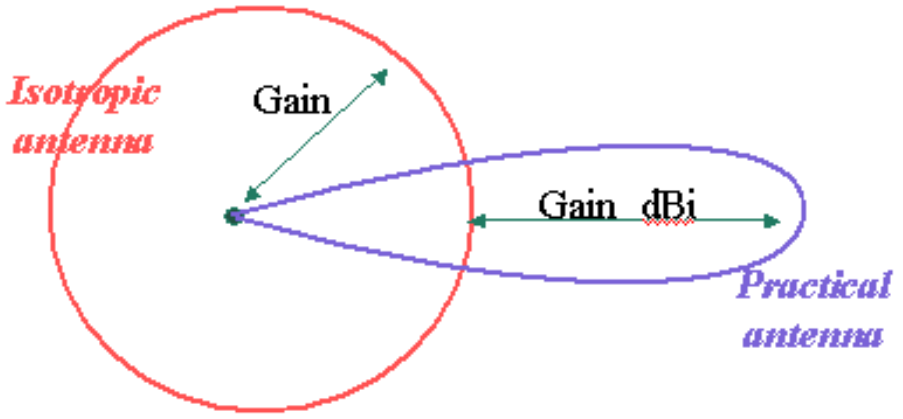
$$G_{AntISO}(\forall\,\theta, \forall\,\varphi) = 0\ dB$$

Antenna Directivity

- Directivity is the measure of the concentration of power density in a particular direction.
- Directivity is expressed in dBi
- Gain include antenna loss

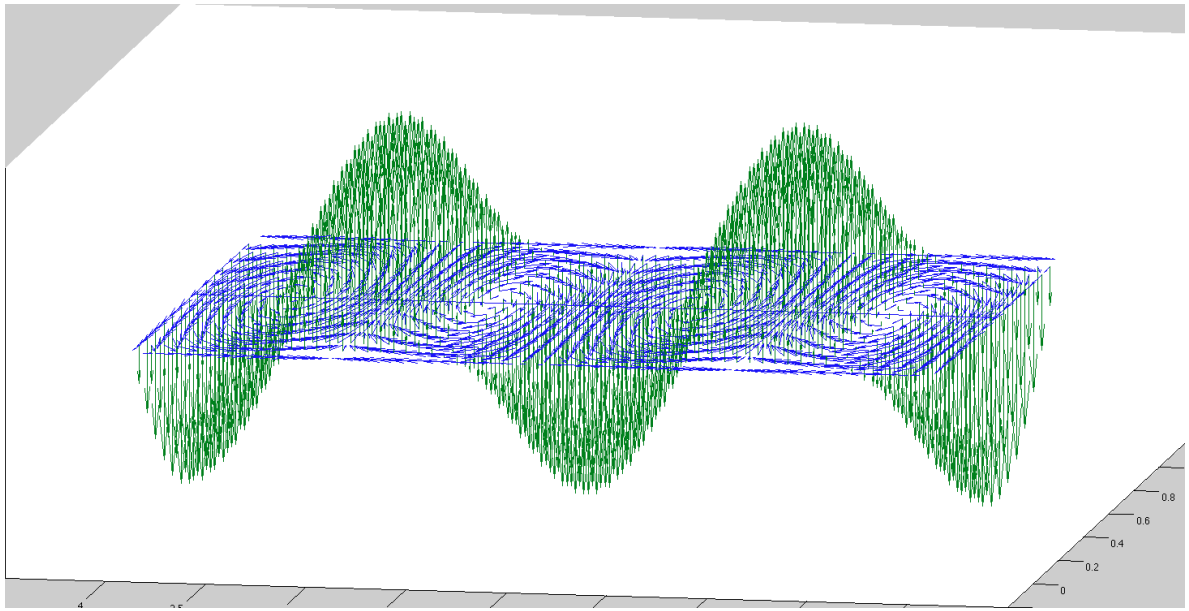
$$Gain = Dir * \eta_{rad}$$





Wireless propagation : Free space loss

- Free space is a region where these is nothing
- In free space, a radio wave launched from a point in any given direction will propagate outwards from that point at the speed of light.
- The energy, carried by photons, will travel in a straight line, as there is nothing to prevent them doing so.
- Do you think it can exist on earth ?



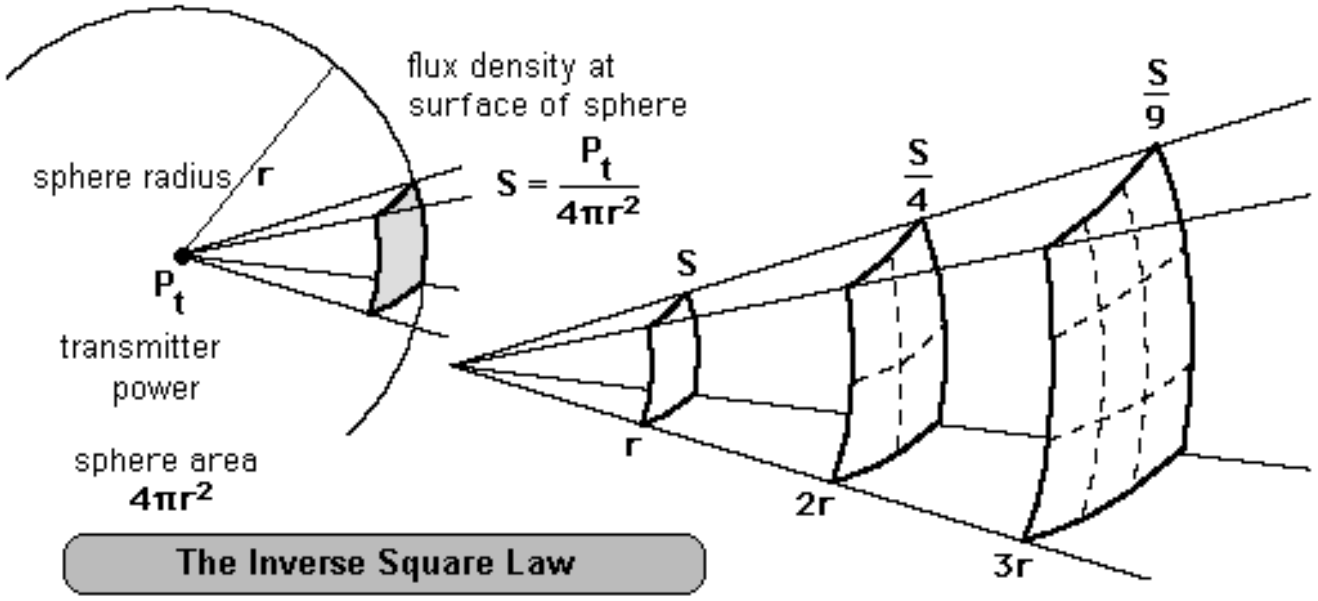
Anechoic chamber for Antenna measurement

- Walls are covered with Electro-magnetic absorbers
- The pyramidal shape improve absorption ratio

Wireless propagation : Transmission

As the energy in a radio wave goes on propagating forever without loss, why do people talk about "free space loss" ?

Free space loss is not really a loss at all. It relates to the intensity of the wave at a distance from the source measured by some standard collector, like an antenna or a telescope. As the wave spreads out, the intensity becomes lower.



Wireless propagation : Transmission

- The area of this sphere is proportional to the radius:

$$A = 4\pi r^2$$

- The power per unit area is simply the total power divided by the total area. If the power is measured in watts this is:

$$Watt/m^2 = \frac{Total\ Power\ (W)}{Total\ Area\ (m^2)}$$

- This power is usually referred to as the power flux density:
  - For an isotropic antenna

$$Power\ flux\ density = \frac{Ptx(W)}{4\pi r^2}$$

  - For a directive antenna

$$Power\ flux\ density = Gtx\frac{Ptx(W)}{4\pi r^2}$$

For example, at a radius of 8.9m, the total area of the sphere is 1000 square m. Over a collecting area of 1 square m, only 1/1000th of the total energy is to be found. This represents "loss" of 1000, equivalent to 30 dB.

Wireless propagation : Receiver

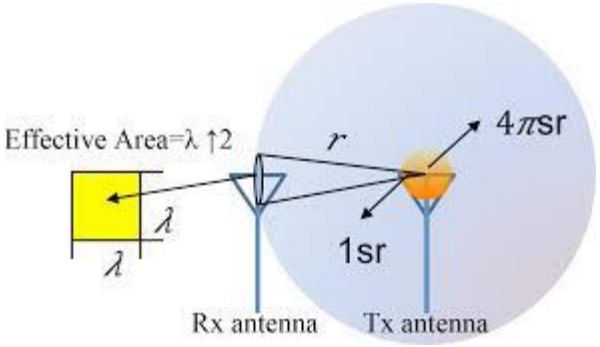
- The amount of power collected by an ideal antenna is simply the power flux density multiplied by the effective capture area of the antenna Ae.

$$P_{rx}(W) = Ae * Power\ flux\ density$$

- The effective capture area of an antenna *Ae* is related to the gain G_{rx} of the antenna and wavelength :

$$Ae = Grx\frac{\lambda^2}{4\pi} \qquad \text{with} \qquad \lambda = \frac{c}{f}$$

- Which give the **friis formula** :



$$P_{rx}/P_{tx} = Gtx\ Grx\left(\frac{\lambda}{4\pi r}\right)^2$$

$$P_{rx}/P_{tx} \propto \frac{1}{r^2}$$

Practical consideration for propagation

Carrier frequency ↑

Channel losses over the same distance ↑

Carrier frequency ↓

Antenna dimensions ↑

Communication distance X 10

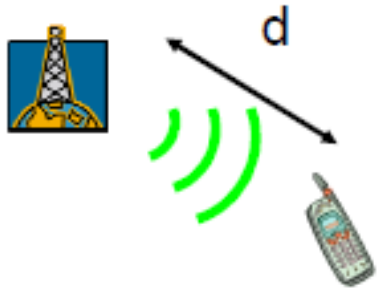
Channel attenuation X 100 Ideally

X 1000 Usually, even more…

Channel Ideal model

Free-space propagation

- No obstacles between transmitter and receiver
- The atmosphere is a uniform and non-absorbing medium
- Attenuation L_p depends on the distance *d* and the wavelength of the signal λ
- $\lambda = c/f$ and $c = 3 \times 10^8$ m/s



$$P_{rx}/P_{tx} = Gtx\ Grx \left(\frac{\lambda}{4\pi r}\right)^2 \longrightarrow P_{rx}/P_{tx} = \frac{1}{L_p} \propto \frac{1}{d^n}$$

Real channel model

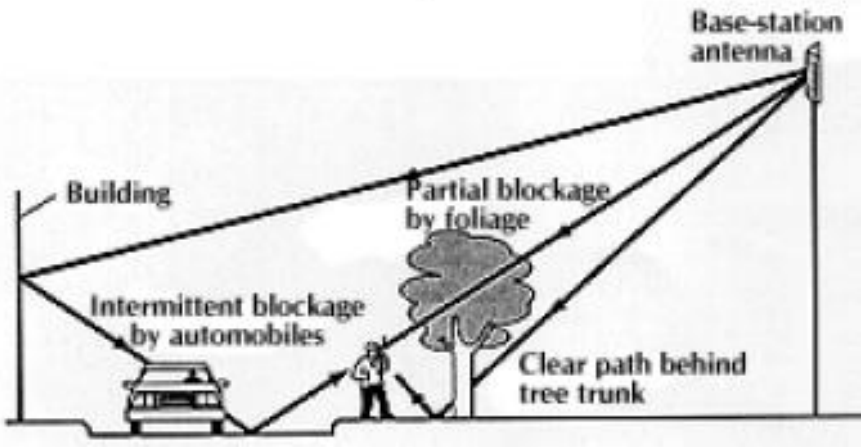
Real propagation :

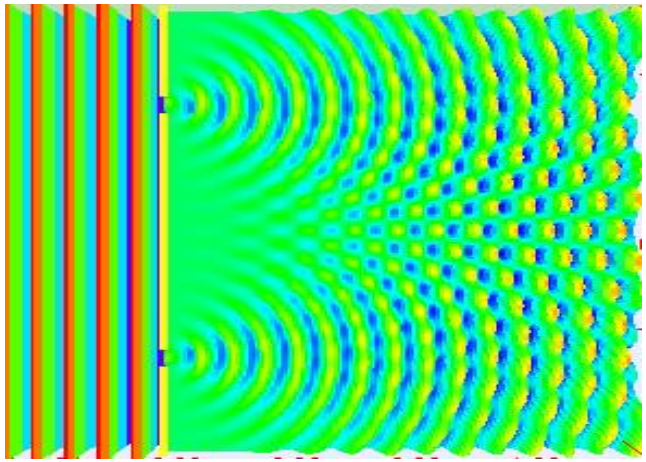
- No Line of Sight
- Multiple paths between the transmitter and the receiver
- Attenuation L_p depends **not only** on the distance d and the wavelength λ of the signal

Real Propagation

Practically, the free-space model is inadequate since:

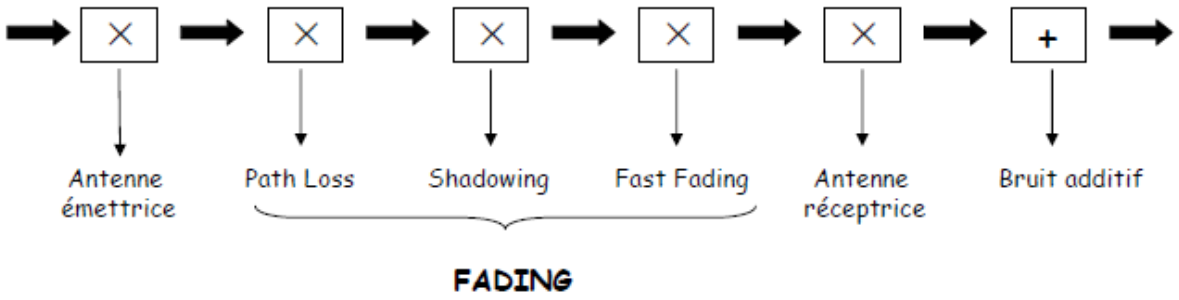
- Multipath phenomenon
  - Multiple paths between the transmitter and the receiver
- Shadowing phenomenon
  - Obstruction of the direct line of sight between transmitter and receiver
- Fast fading phenomenon
  - Destructive composition of different signal path that are close in time (phase opposition)





Attenuation

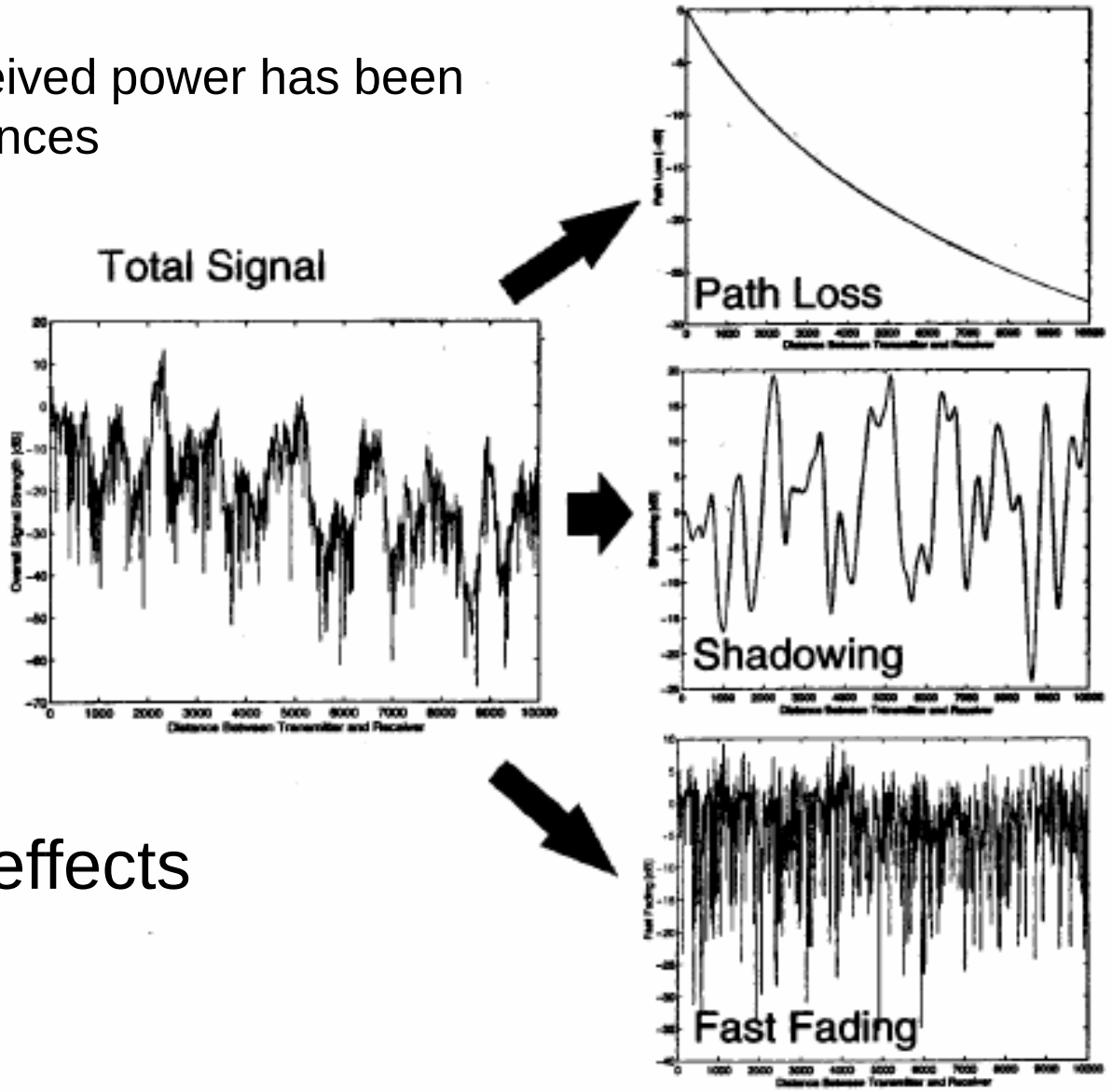
3 types of attenuation



- Path loss (distance attenuation)
  - Decrease of the signal power due to the distance (deterministic)
- Shadowing (or slow fading)
  - Slow variation of the signal amplitude due to successive attenuation
- Fast fading
  - Fast variation of the signal amplitude (constructive or destructive combination of the electromagnetic waves)

Attenuation

In this experiment, the received power has been measured to different distances



We can observe 3 effects

Shadowing Statistical and path loss

- **Average link loss**: Average loss between the emitter and receiver
- Log-normale variation around the average loss

$$L_p(d) = \overline{L_p}(d) * X_\sigma$$

- Loss expressed with formula that mimic Friis free space formula (with d^n , d being the distance between the emitter and receiver)

$$P_{rx}/P_{tx} = \frac{1}{L_p} \propto \frac{1}{d^2} \longrightarrow L_p \propto d^n$$

Average loss: power law model

$$L_p = k \,.\, d^n$$

$$(L_p)_{dB} = 10n.\log(d) + k$$

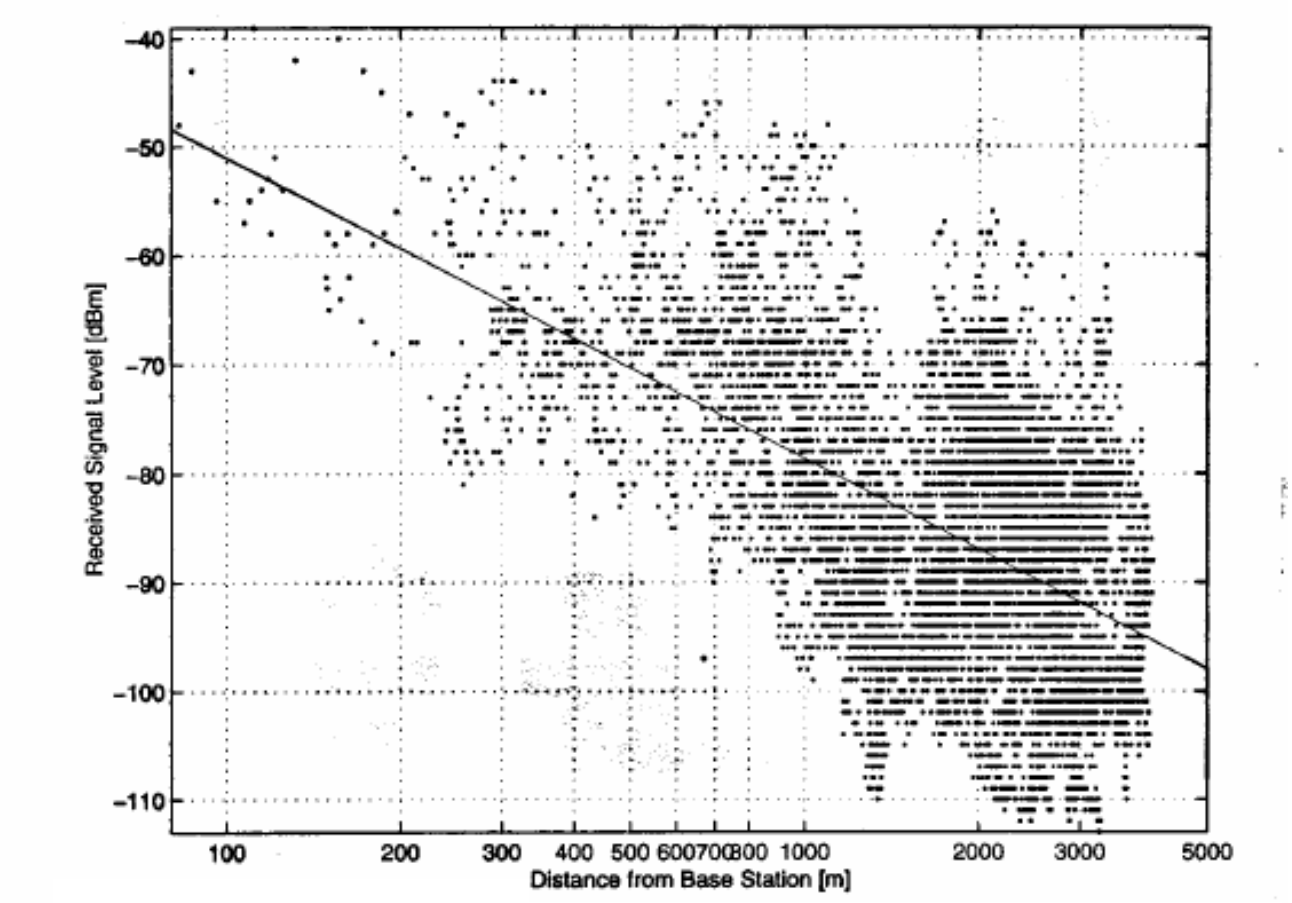
$$(L_p)_{dB} = 10n.\log\left(\frac{d}{d_{ref}}\right) + L_{ref}$$

- n : path loss calculated with measurements
- Can be expressed in relative compared to a reference distance d_{ref}
- Usually, a distance of 1m is choosen.

Power law model

Set of measurements done in a dedicated environment

Curve interpolation fitting with the measured points



Power law model

2. Variability of the signal strength in close spatial proximity to a particular location → fading models → small-scale

Environment	Path Loss Exponent n	Standard Deviation s
Free space	2	0dB
Urban area cellular radio	2.7 to 3.5	10-14dB
Shadowed urban cellular radio	3 to 5	11-17dB
In-building line-of-sight (LOS)	1.6 to 1.8	4-7dB
Obstructed in-building (NLOS)	4 to 6	5-12dB
Obstructed in-factories (NLOS)	2 to 3	6-9dB

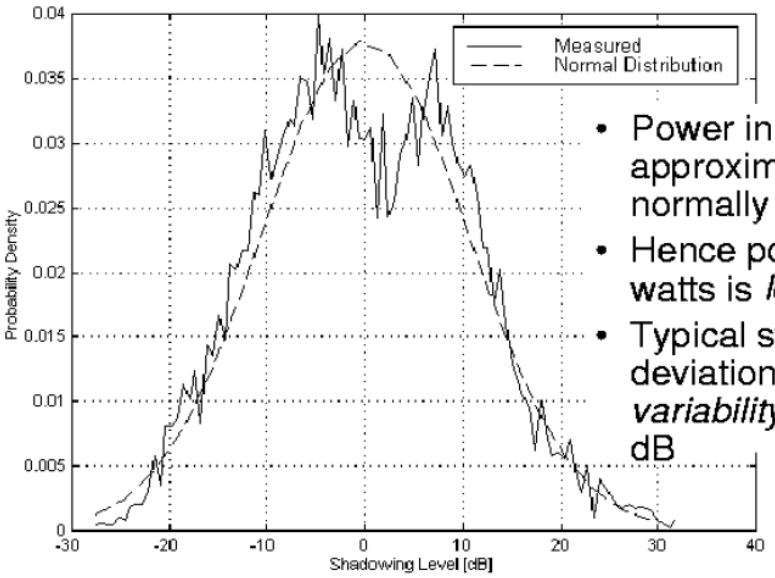
Path loss exponent and log-normal shadowing standard deviation

Log-normal distribution around the link average loss

Losses due to shadowing is a random variable Ls(d) composed with a random fluctuation Xs with a log-normal probability density.

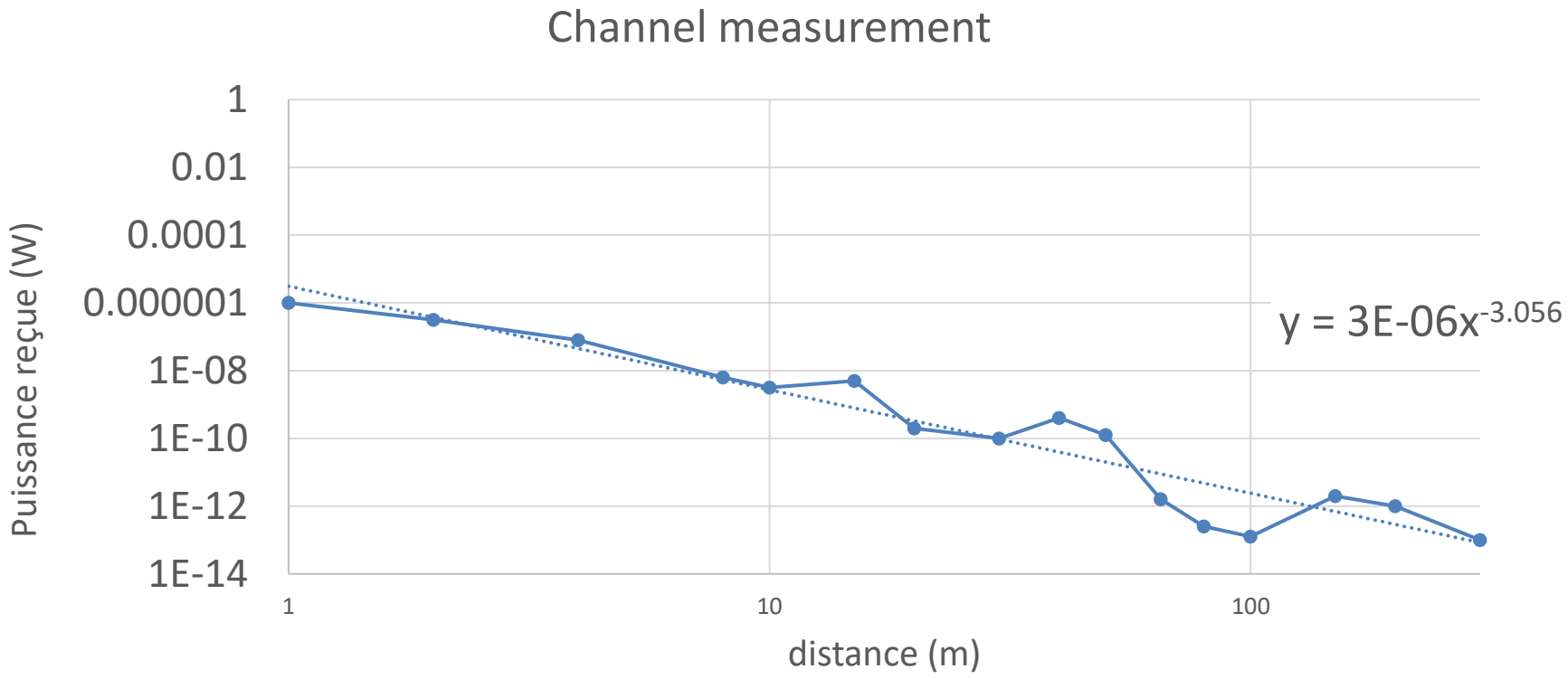
- If the fluctuation Xs fits with a log-normal distribution, then, Xs fits a normal distribution $N(0,s^2)$ in dB
- Dynamic : from 6 to 13 dB, even more

$$L_p(d) = \overline{L_p}(d) * X_\sigma$$



- Power in dB is approximately normally distributed
- Hence power in watts is *lognormal*
- Typical standard deviation (*location variability*) of 5-12 dB

Example


Channel measurement
Puissance reçue (W)
1
0.01
0.0001
0.000001
1E-08
1E-10
1E-12
1E-14
1
10
100
distance (m)
y = 3E-06x-3.056

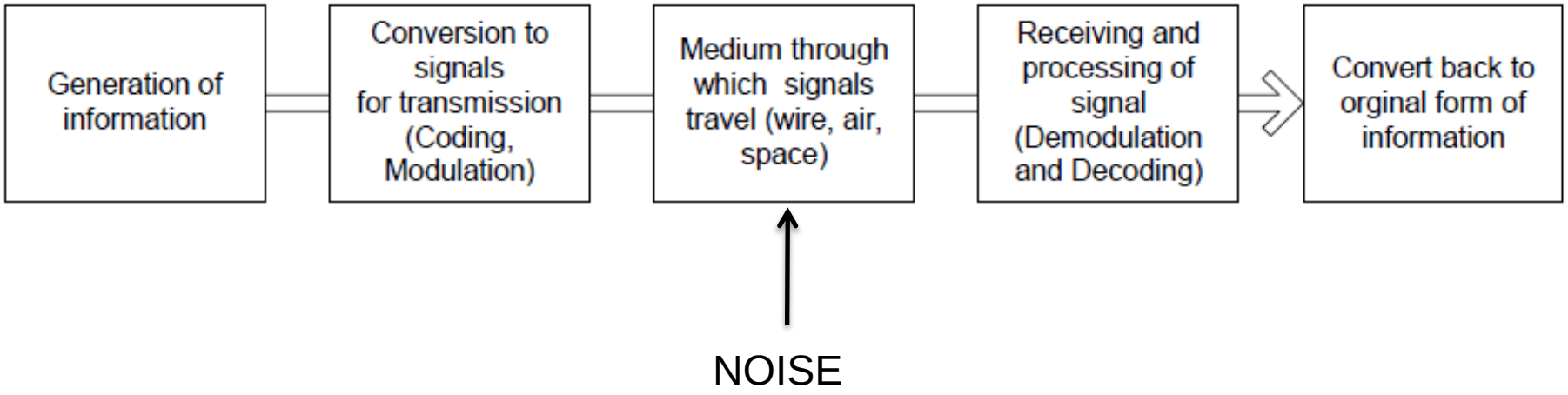

0
100.00 m
200.00 m
303.61 m

Outline

0. Introduction
I. Wireless Propagation
II. Physical layer : Bands & Modulation
III. MAC layer (LoRaWAN) and security

Communication

The objective of a communication chain is to transmit a piece of information between different users.



We have seen in last course that electro-magnetic wave can propagate between two different points without any wire.

Propagation & Antenna

Propagation : Losses versus distance

Carrier frequency 

Channel losses over the same distance 

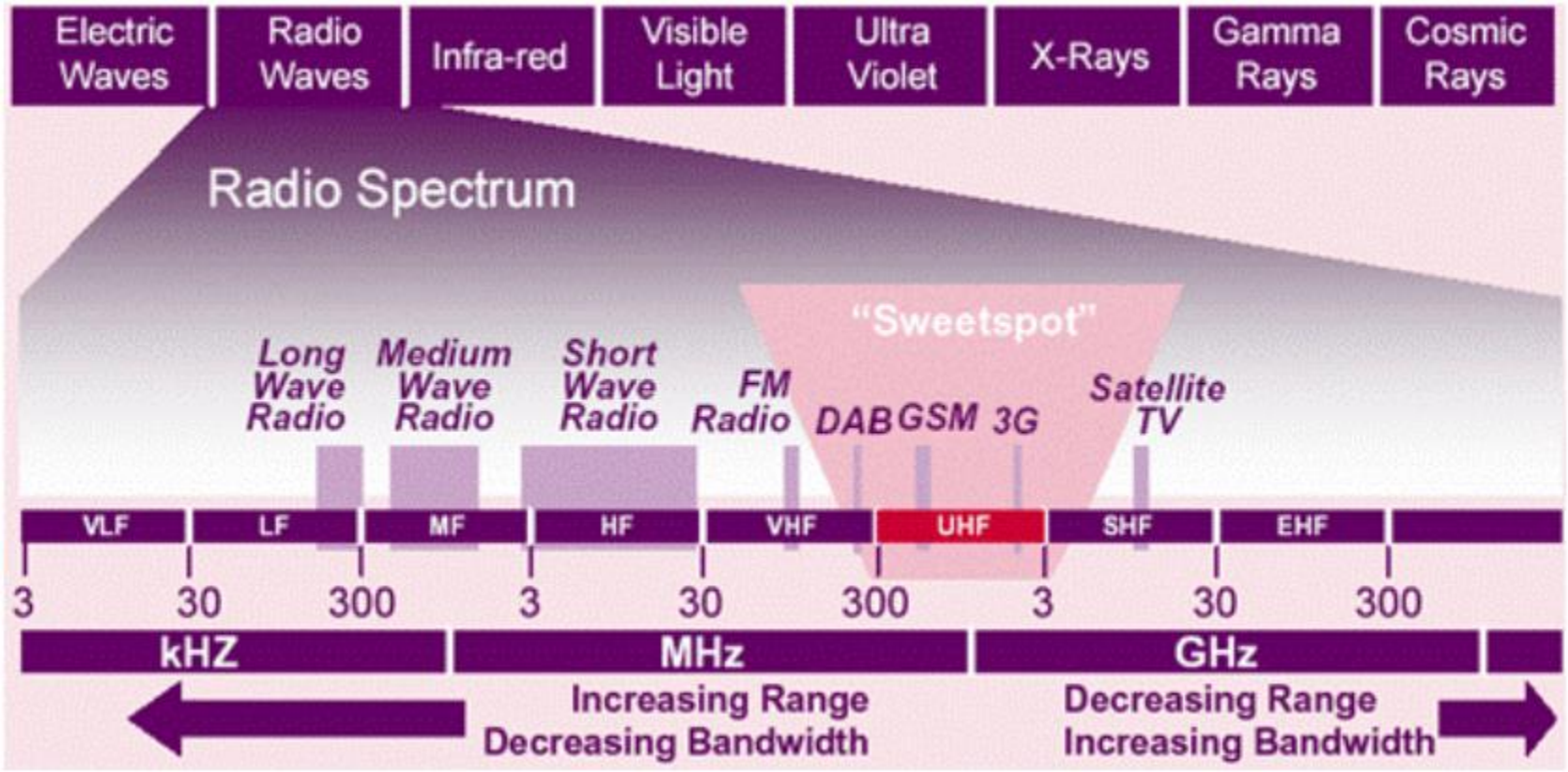
Carrier frequency 

Antenna dimensions 

If we want compact devices and long communication range, only some frequency range are suitable

Frequency band for communication

Radio-Spectrum

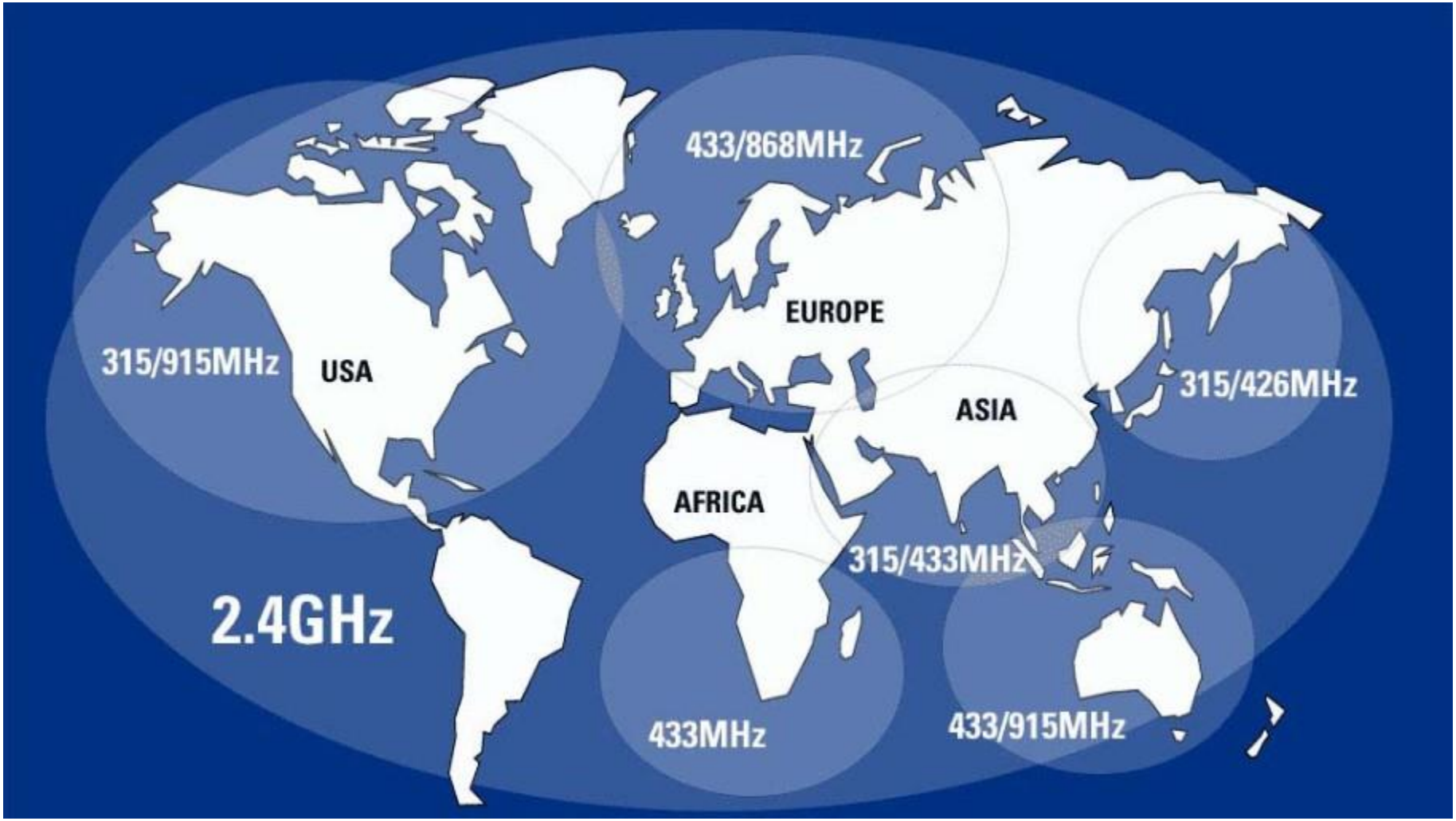


Frequency band for communication

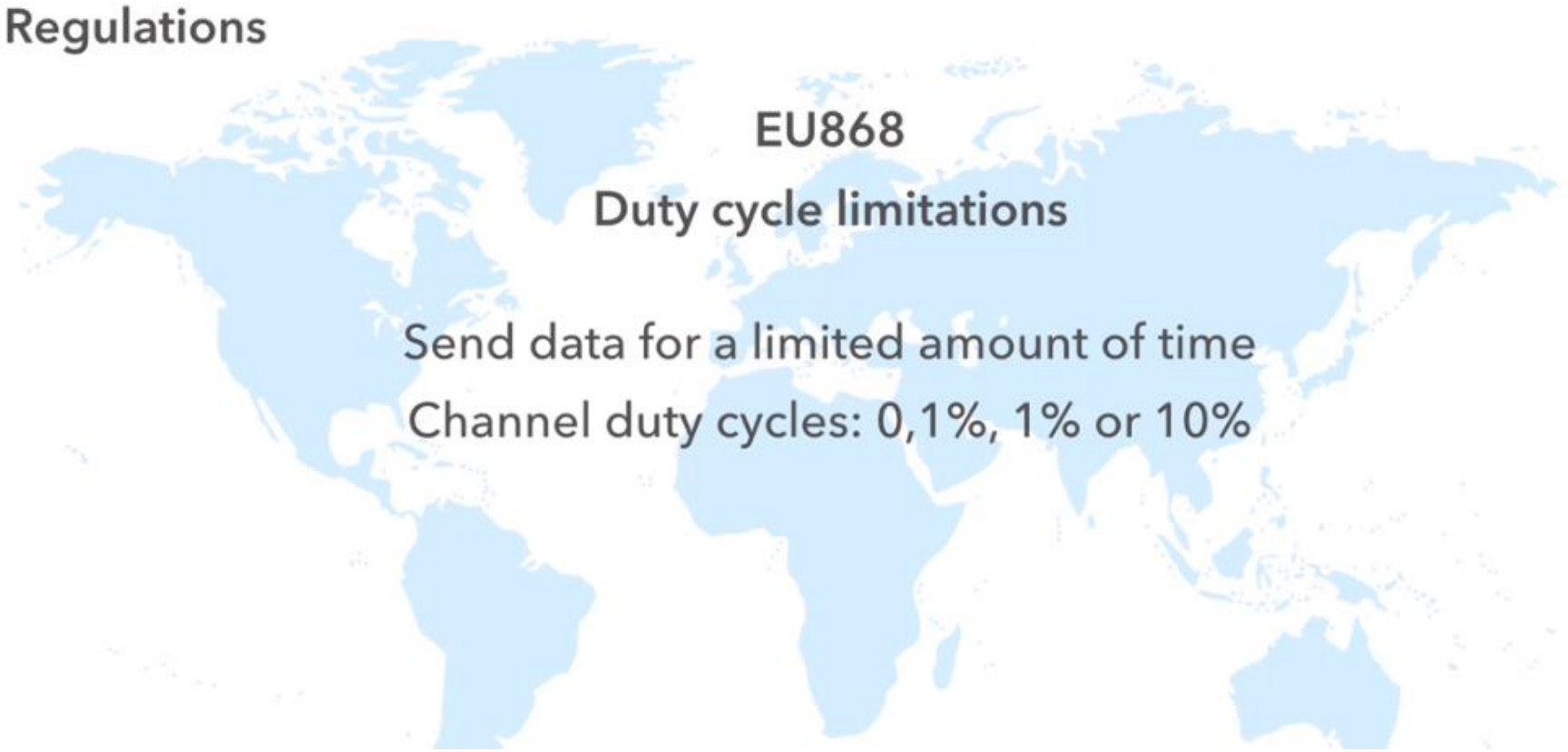
Spectrum : Licensed or unlicensed band

- Parts of the radio spectrum are sold or licensed to operators of private radio transmission services (cellular telephone operators or broadcast television stations).
- Some part of the spectrum can be accessed for free, it is usually named ISM bands
- The industrial, scientific and medical (ISM) radio bands are radio bands (portions of the radio spectrum) reserved for unlicensed operation.
- Rules have to be respected on ISM band to limit interferences between users

Worlwide Unlicensed band



Exemple : LoRaWan bands

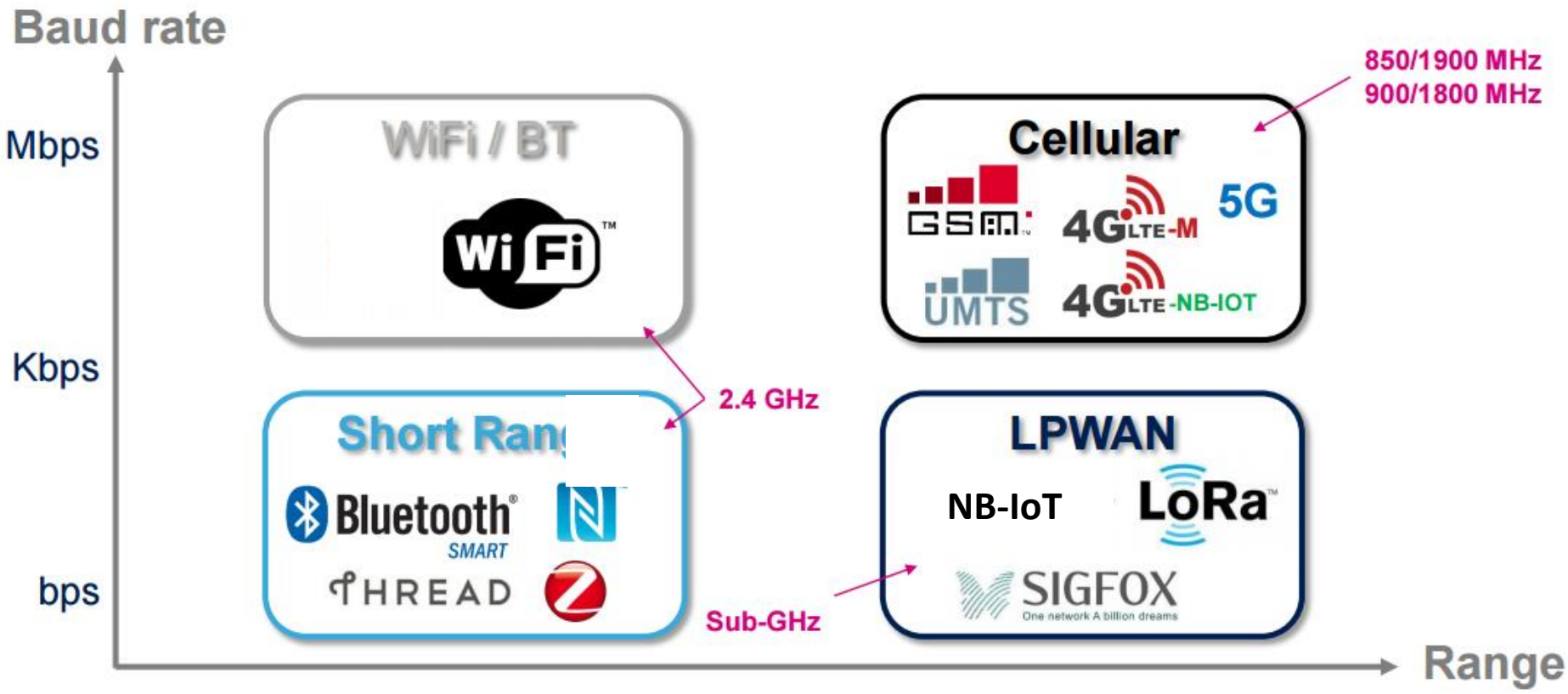


Worldwide Unlicensed band

- Below 1 GHz
  - different bands are used worldwide
  - Duty cycle restriction
  - Limited bandwith
- 2.4-2.48 GHz band
  - available for license-free operation in most countries
  - Large bandwidth allow high datarate
  - Short range
- 5-6GHz band
  - Available worlwide
  - Very large bandwith
  - Shorter range
- 57-64 GHz
  - Worlwide availibiility
  - Huge bandwith for huge datarate
  - Very limited range

Communication Technology

Data rate / Range



LP-WAN connectivity overview

	LoRa™	SIGFOX	NB-IoT 3GPP
Range (km)	10km (suburban) 3-6km (urban)	30km (Rural) 10km (urban)	
Frequency Band (MHz)	Sub GHz (ISM)	868-900MHz (ISM)	Licensed LTE bands
Max. Coupling Loss	155dB		164dB
Modulation type	Chirp Spread Spectrum (CSS)	Ultra narrow band / GFSK / BPSK	LTE - OFDMA / SC-FDMA
Bandwidth	125 – 500 kHz	100 Hz	180 kHz
Datarate	300 bps – 50 kbps	100 bps	Up to 250 kbps (UL) – low latency
Max /message / day (Uplink)	Unlimited*	140 msg/day – 12bytesmax/msg	Unlimited (lice. Spectrum)
Max /message / day (Downlink)	Unlimited*	4 msg/day (8bytes max/msg)	Unlimited (lice. Spectrum)
Network density	+++ (ADR)	+	+++
Battery peak current	< 50 mA (14dBm)	< 50 mA (14dBm)	~300mA (@23dBm)
Average sensor autonomy	+++ (ADR)	++	+
Interference immunity	high	Low	Sensitive to downlink jamming
Native payload encryption	Yes	Proprietary	Yes
Able to create private networks	Yes	No	No
Location (w/o GPS)	Yes	No	M1 only, not deployed(**)
Commercial availability	Now	Now	Starting in 2017

(*) Adaptive Data Rate

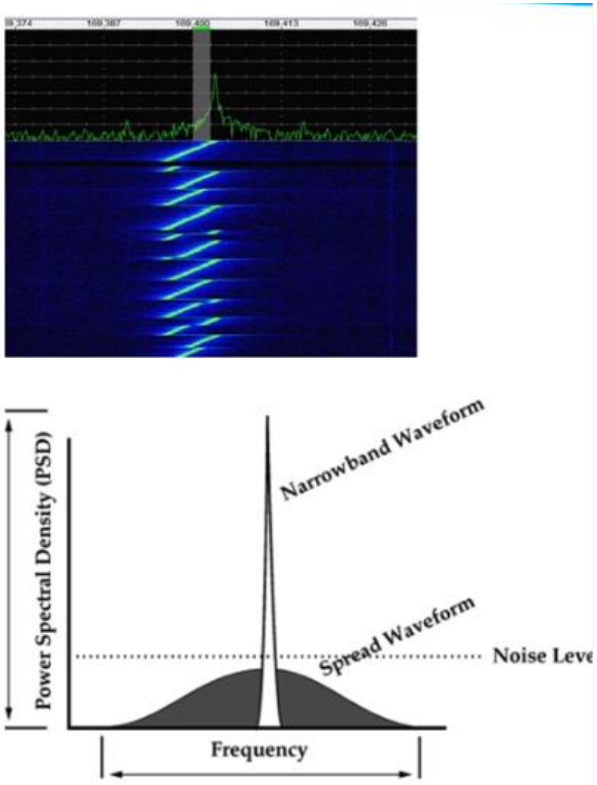
(**) Requires optional Location Measurement Units (LMU) in BTS. Not deployed except E911 phase 2 in US

LoRa modulation

Spread spectrum technique :

Increase communication distance by increasing energy per bit :

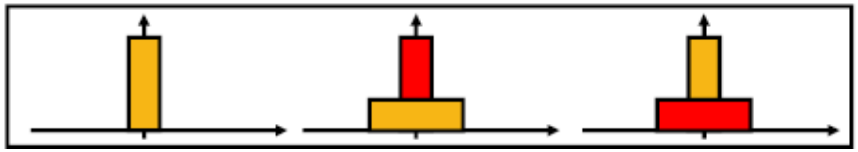
- Increase transmit power
- Lower modulation rate



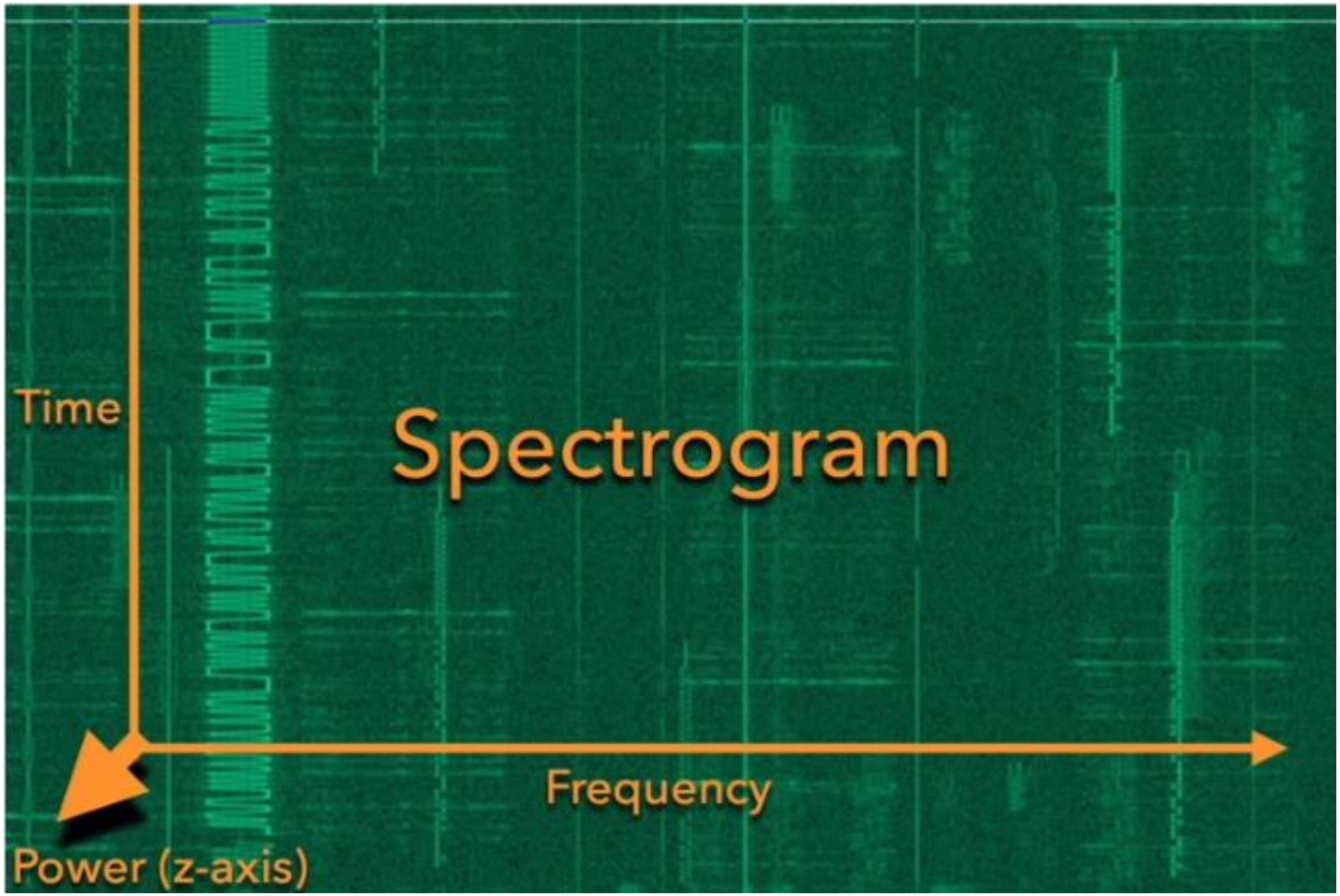
3 types of spread spectrum technique :

- FHSS : Freq Hopping (used in Bluetooth)
- DSSS : Direct Sequence (UMTS and Zigbee)
- CCS : Chirp Spread Spectrum (LoRa)

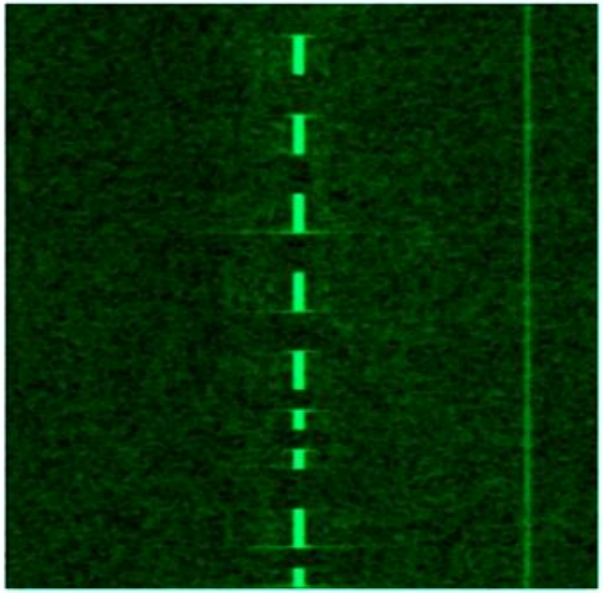
Robust to interference, multipath and fading



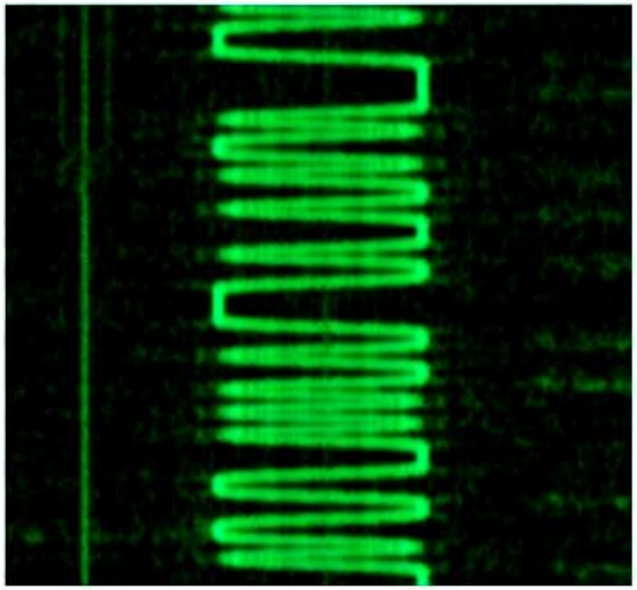
CSS : Chirp Spread Spectrum



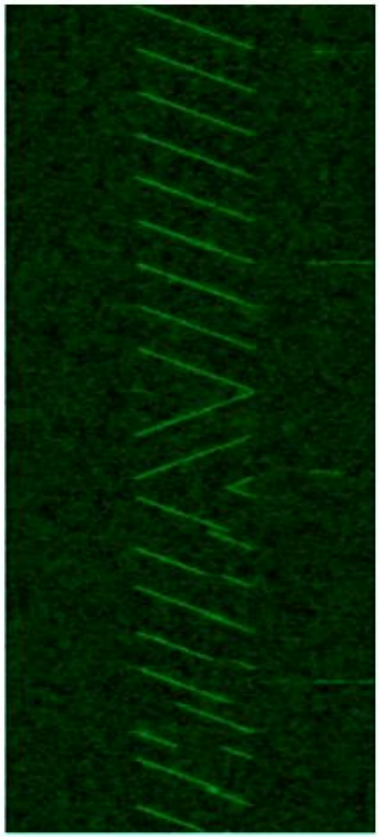
CSS : Chirp Spread Spectrum



On-Off Keying



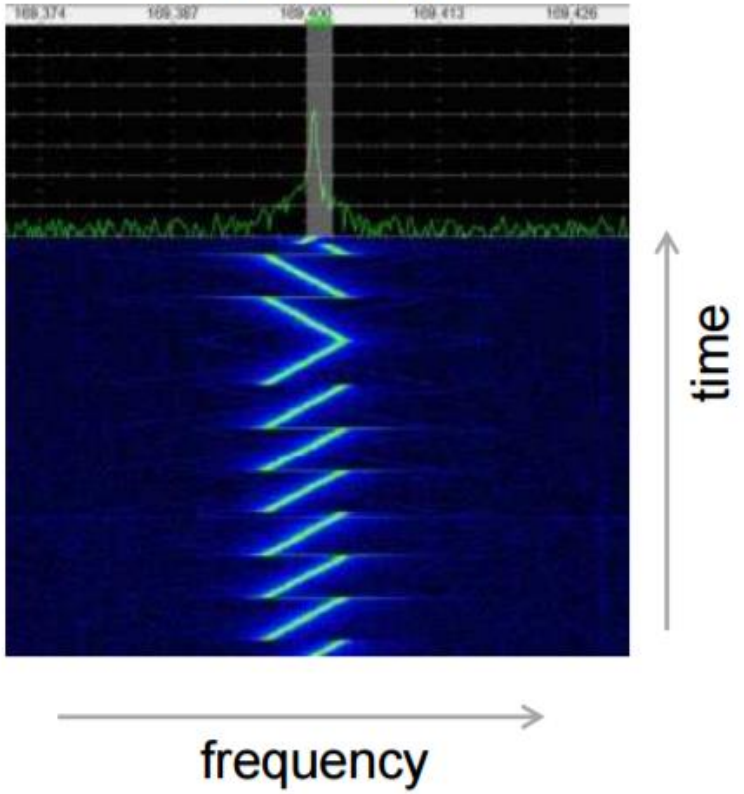
Frequency-shift Keying



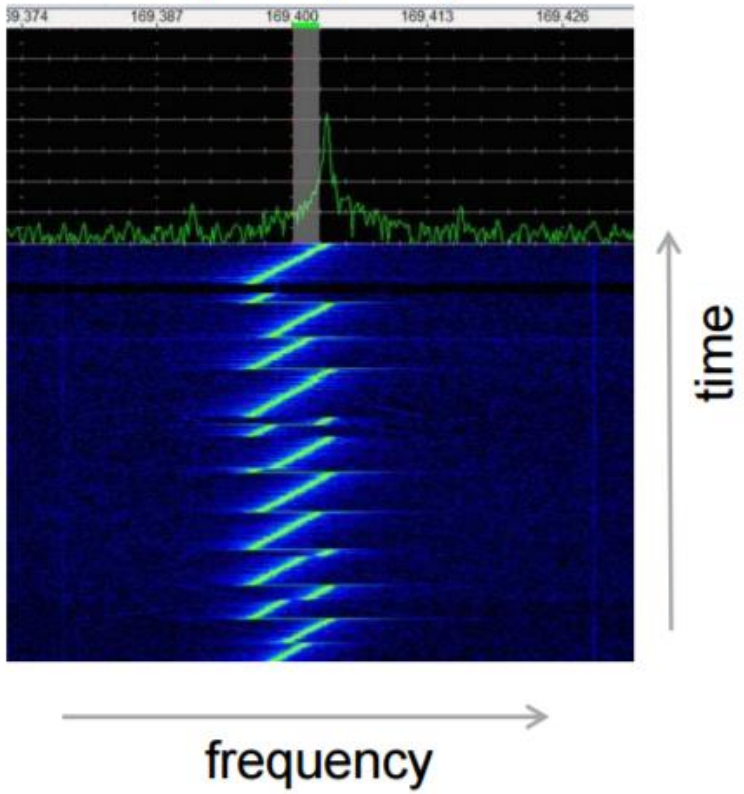
LoRa

LoRa Chirp Spread Spectrum (CSS)

LoRa pre-amble signal:
10 symbols or “chirps”,
2 reverse “chirp”.



LoRa data signal:
A symbol is a “chirp” with a frequency “hop”.



LoRa Bit rate

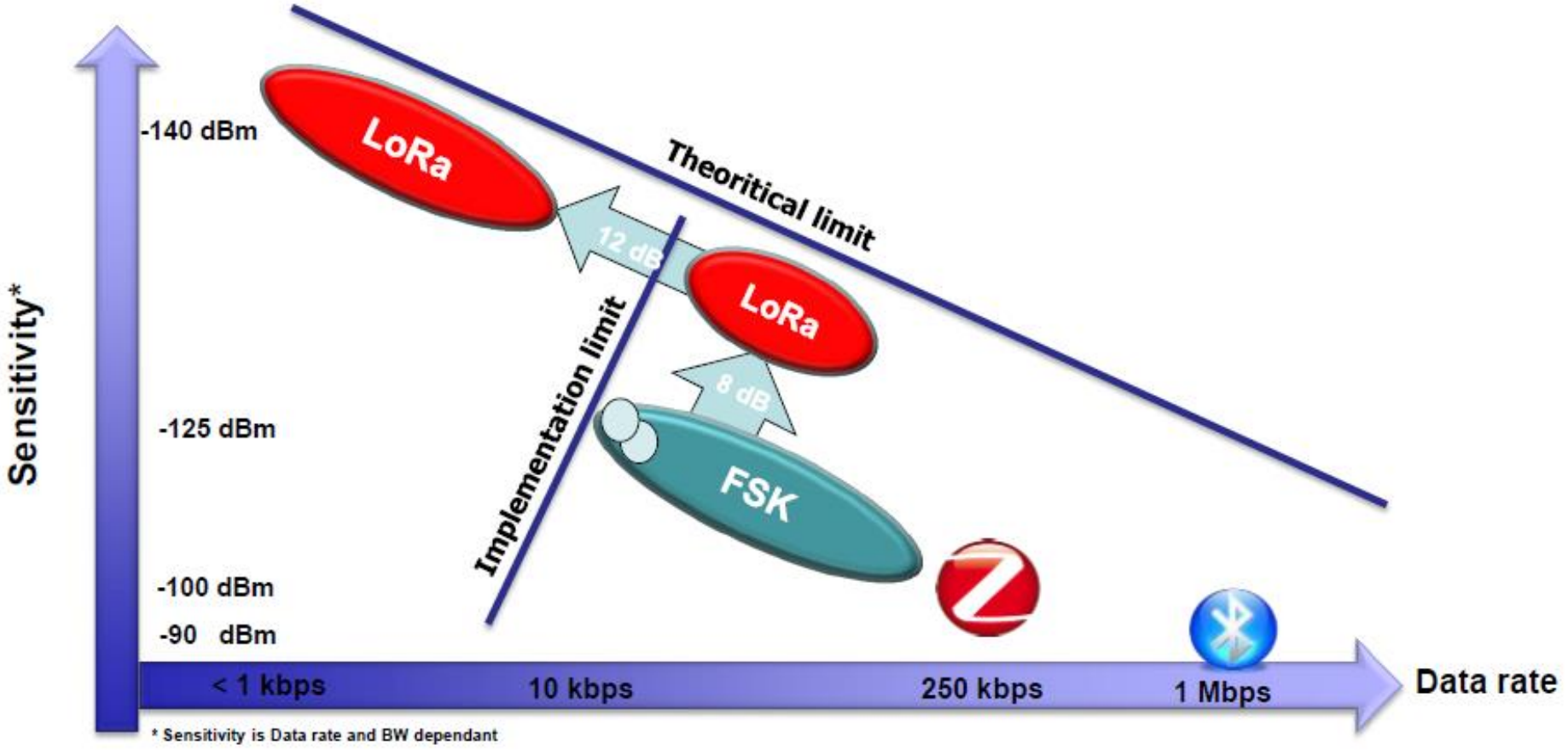
Some LoRaWAN data rates

		$T_{Symbol} = 2^{SF}/BW$		ohne FEC	4/5 FEC (CR=1)	
BW / kHz	SF	T_{symbol} / ms	R_{symbol} / Hz	R_{bit} / bps	R_{bit} / bps	Sensitivity
125	7	1.024	976.56	6835.94	**5468**	S_{ref} = -125 dBm
125	8	2.048	488.28	3906.25	**3125**	- 2.4 dB
125	9	4.096	244.14	2197.27	**1757**	- 4.9 dB
125	10	8.192	122.07	1220.70	**976**	- 7.5 dB
125	11	16.384	61.04	671.39	**537**	- 10 dB
125	12	32.768	30.52	366.21	**292**	- 12.7 dB

using SF = 12 rather than SF = 7

- improves the sensitivity by ~**13 dB**
  or the range by a factor of ~**2.3** (assuming a path loss of 35 dB/decade)
- but increases the symbol time T_{symbol} by a factor of **32**
  (and, thus, the "time on air" and the current consumption)

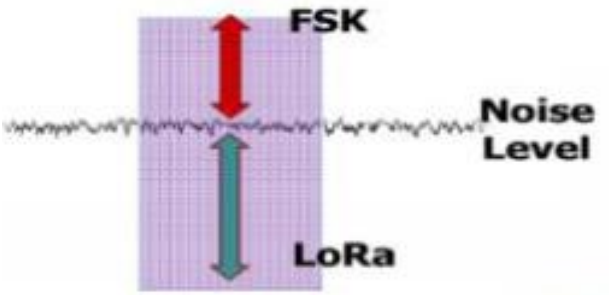
LoRa CSS modulation



LoRa Modulation : Synthesis

Benefits :

- Simple to implement (Constant enveloppe)
- Bandwidth scalable
- Very resistant to in-band and out-of band interferences
- High immunity to multi path and fading



- Doppler shift resitance
- Moving devices
- High clock tolerances

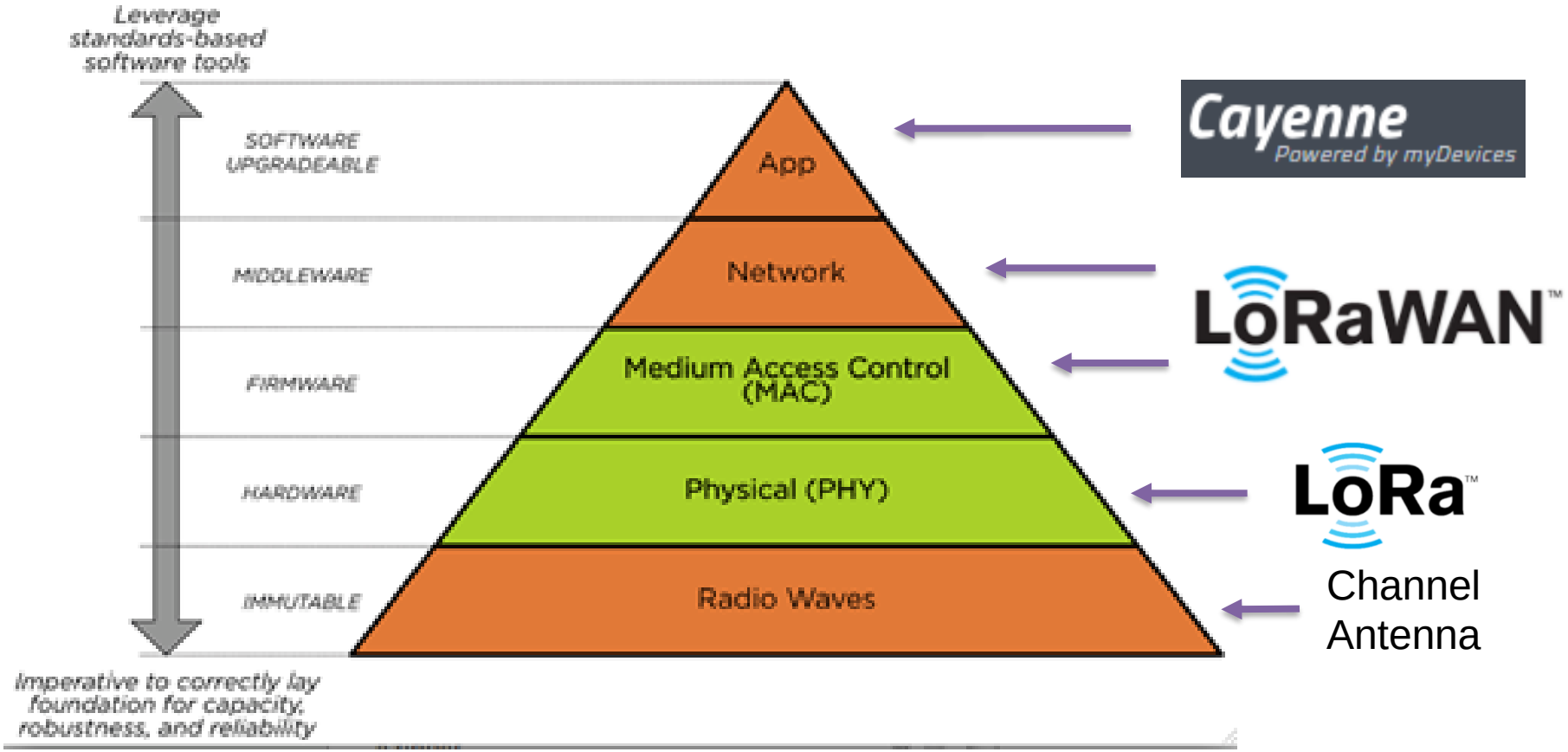
- Orthogonal with other non-LoRa communications (OFDM, narrowband FSK…)
- Orthogonal with LoRa systems using a different Spreading Factor

- Good sensitivity
- Lora reception is simple

Outline

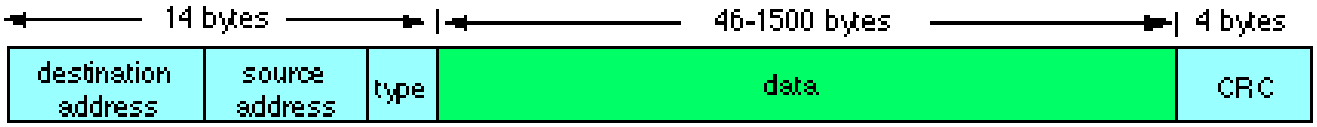
0. Introduction
I. Wireless Propagation
II. Physical layer : Bands & Modulation
III. MAC layer (LoRaWAN) and security

Medium Access Control (MAC)



MAC layer

- Media access control (MAC) is a sublayer of the data link layer (DLL) in the seven-layer OSI network reference model.
- The basic function of MAC is to provide an addressing mechanism and channel access so that each node available on a network can communicate with other nodes available on the same or other networks.
- *Exemple : In Ethernet LAN system, the MAC protocol is*
  - *encapsulating a SDU (payload data)*
  - *adding a 14 byte header (Protocol Control Information (PCI)) before the data*
  - *appending an integrity checksum, The checksum is a 4-byte (32-bit) Cyclic Redundancy Check (CRC) after the data.*
  - *The entire frame is preceded by a small idle period (the minimum inter-frame gap, 9.6 microsecond (µS)) and a 8 byte preamble (including the start of frame delimiter).*



LoRaWan

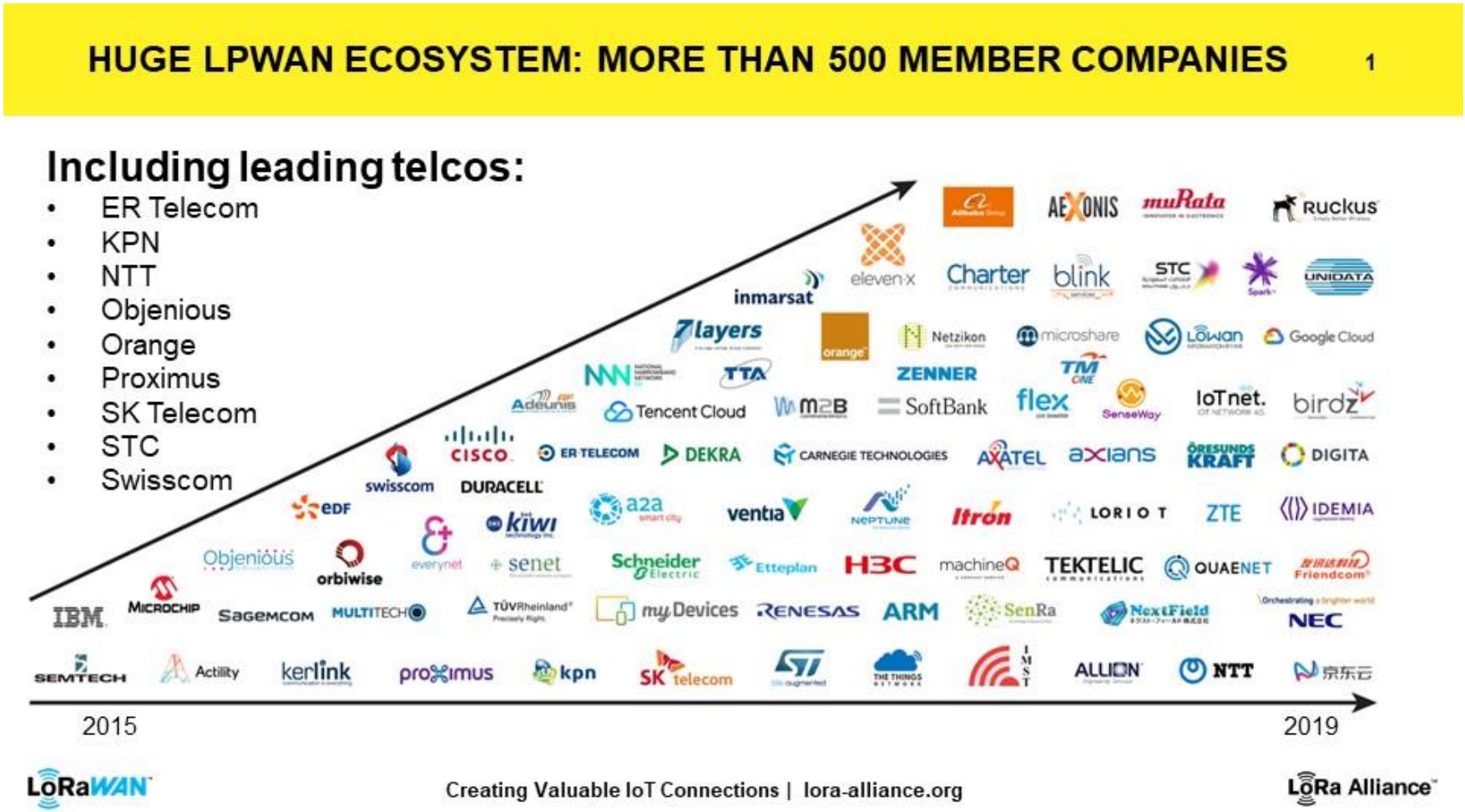
- **LoRaWan** is a software protocol using lora physical layer

- **LoRaWan** include :
  - Session Layer
  - Network Layer
  - Data Link Layer

- It defines the packet format, and the way the packet are processed by the network

LoRaWan

- **LoRaWan is defined by the Lora alliance**



LoRaWan bands

	Europe	North America	China	Korea	Japan	India
Frequency band	867-869MHz	902-928MHz	470-510MHz	920-925MHz	920-925MHz	865-867MHz
Channels	10	64 + 8 +8	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee	In definition by Technical Committee
Channel BW Up	125/250kHz	125/500kHz				
Channel BW Dn	125kHz	500kHz				
TX Power Up	+14dBm	+20dBm typ (+30dBm allowed)				
TX Power Dn	+14dBm	+27dBm				
SF Up	7-12	7-10				
Data rate	250bps- 50kbps	980bps-21.9kpbs				
Link Budget Up	155dB	154dB				
Link Budget Dn	155dB	157dB				

LoRaWan bands

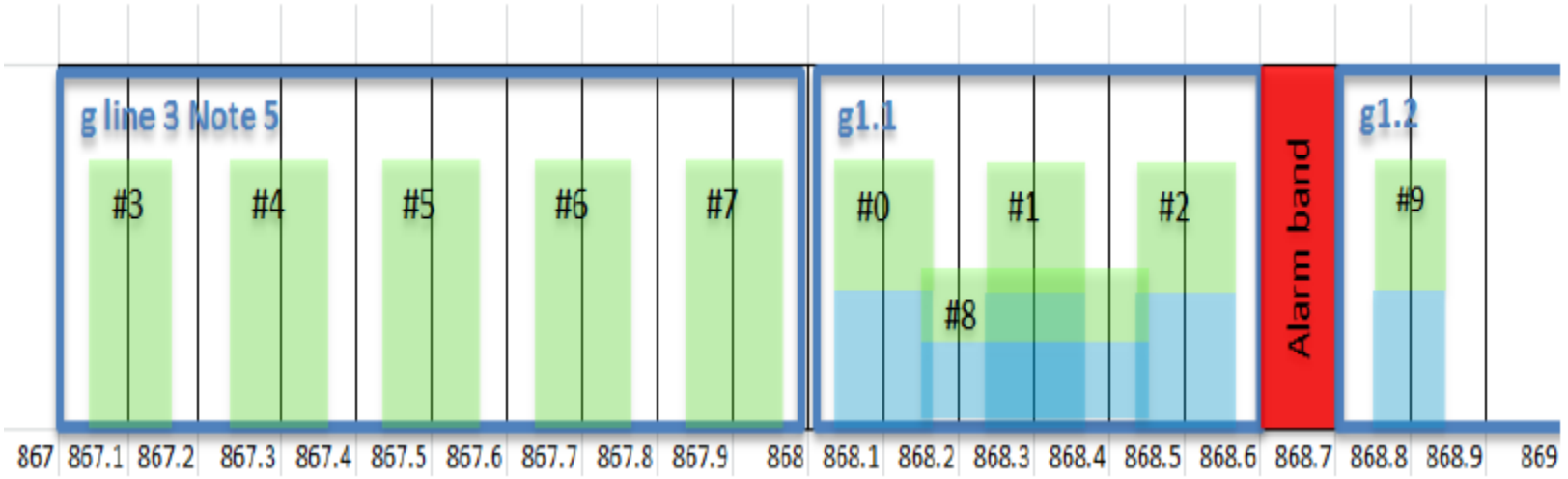
License free Sub-GHz Frequencies :

- Europe 868 MHz Band (863 ~ 870 MHz)
- Network channels can be freely attributed by the network operator
- Three mandatory channels that all gateways should constantly receive, and used by the end-points during the Join procedure :

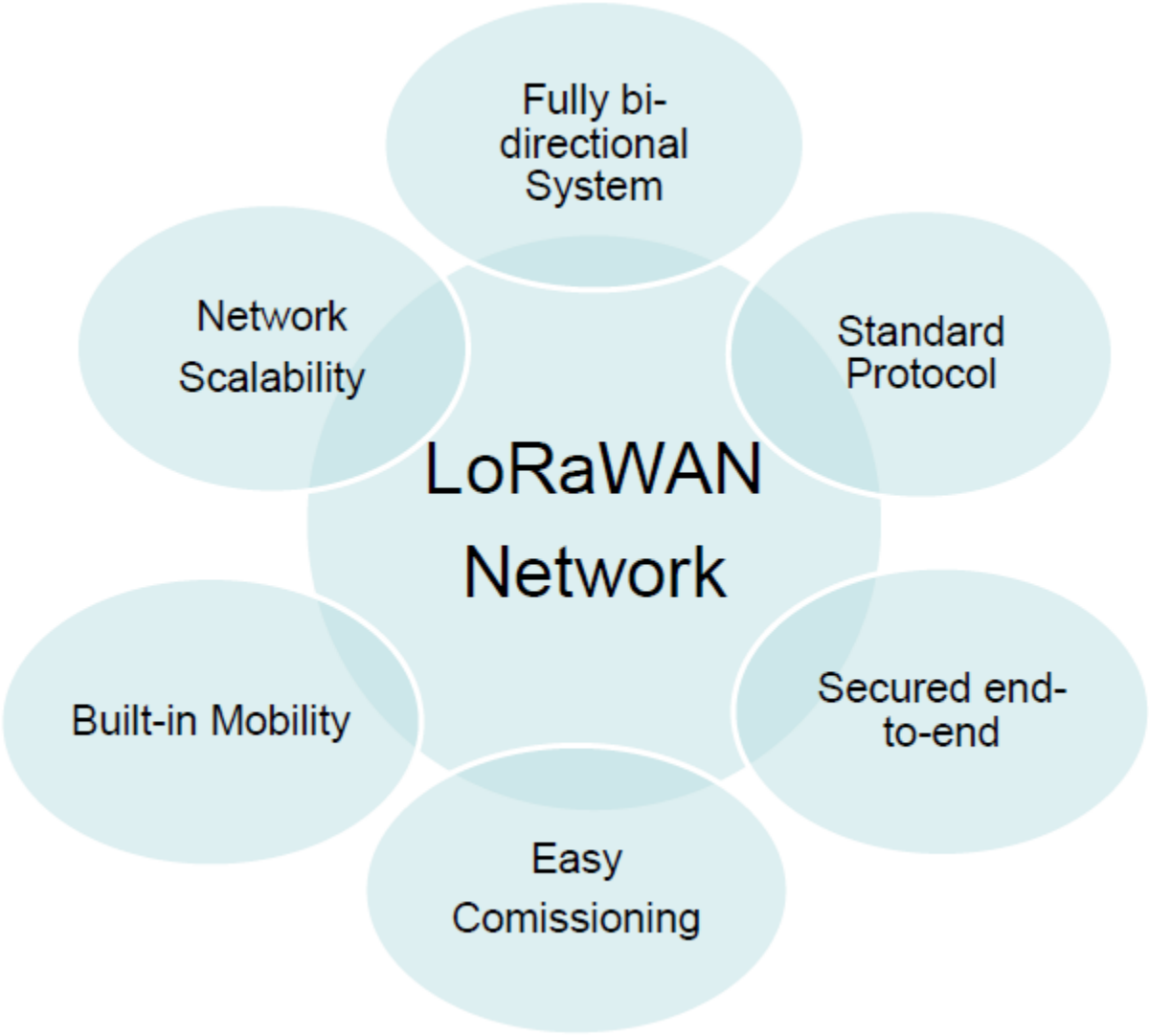
Modulation	Bandwidth [kHz]	Channel Frequency [MHz]	FSK Bitrate or LoRa DR / Bitrate	Nb Channels	Duty cycle
LoRa	125	868.10 868.30 868.50	DR0 to DR5 / 0.3-5 kbps	3	<1%

LoRaWan bands

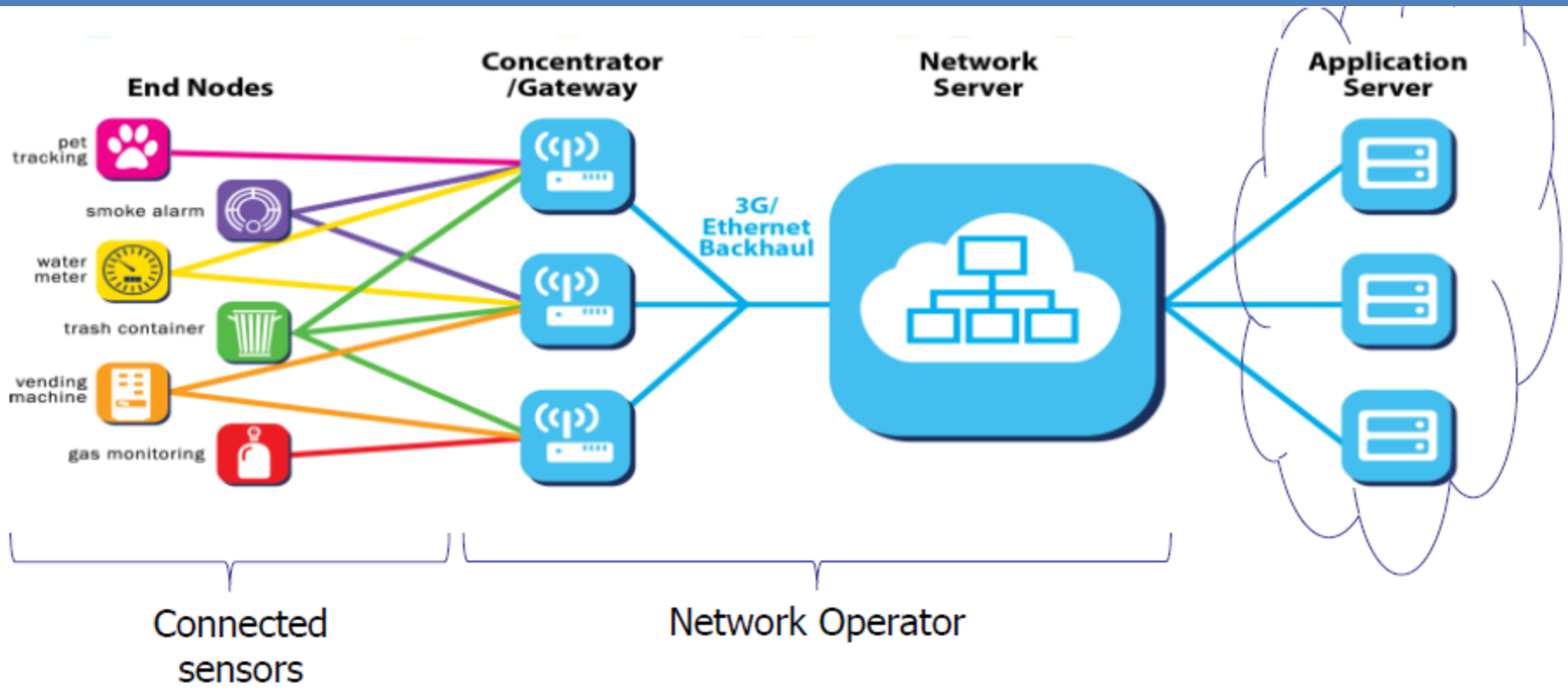
- **8 channels with multi-datarate 240 bps to 5.5 kbps**
- **1 high-speed LoRa channel 11 kbps**
- **1 high speed GFSK channel 50 kbps**



LoRaWan


Fully bi-directional System
Network Scalability
Standard Protocol
LoRaWAN Network
Built-in Mobility
Secured end-to-end
Easy Comissioning

LoRaWan



Centralized intelligence, cloud based

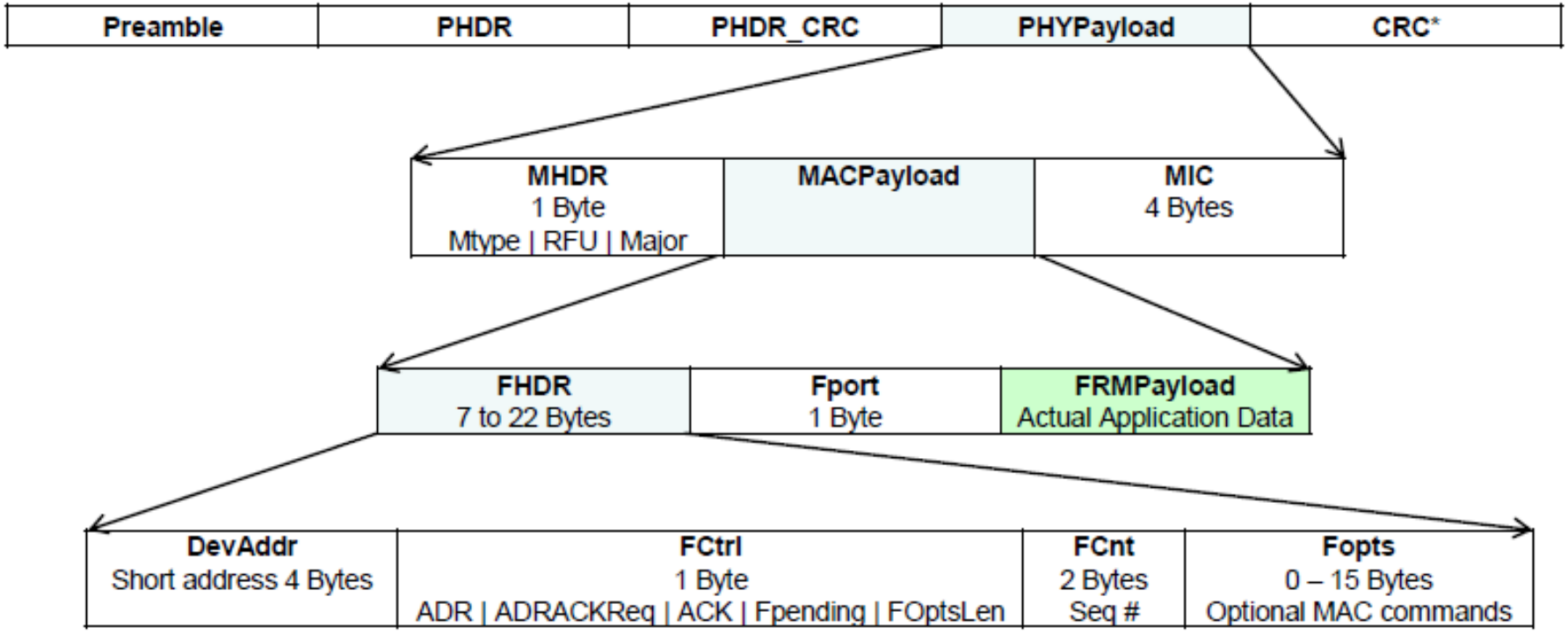
- No notion of connection or pairing from GW to device
- Mostly uplink, Aloha type system

– IOT cannot support connection-based systems, from the energy standpoint

– Scheduling requires negociation and therefore energy

– Scheduling in a license-free band wouldn't be efficient

LoRaWan



Typ. 12 Bytes of Overhead: Lightweight protocol

LoRaWan

Class Name	Intended Usage
A « All »	**Battery powered sensors**, or actuators with no downlink latency constraint. Most energy efficient communication class. Must be supported by all devices
B « Beacon »	**Battery powered actuators** Energy efficient communication class for latency controlled downlink. Based on slotted communication synchronized with a network beacon
C « Continuous »	**Mains powered actuators** Devices which can afford to listen continuously. No latency for downlink communication.

Class A
Report status a few times per day
No planned actuation required
Extremely low energy

Class B
Report moisture, t° a few times per day
Turn valves on or off with a few minutes latency
Very low-energy, which depends on latency

Class C
Maintenance and index info a few times / day
Constantly listens for network «ping»
For low-latency actuation

LoRaWan – Class A

Current consumption for Transciever

Uplink : Node –> GW
Downlink : GW - > Node

Transmit : 40 mA
Receive : 11 mA
Sleep : 10 uA !!! uA = mA/1000

Save the battery –> 100% in sleep mode

Uplink ?
-> easy to do : Aloha protocol

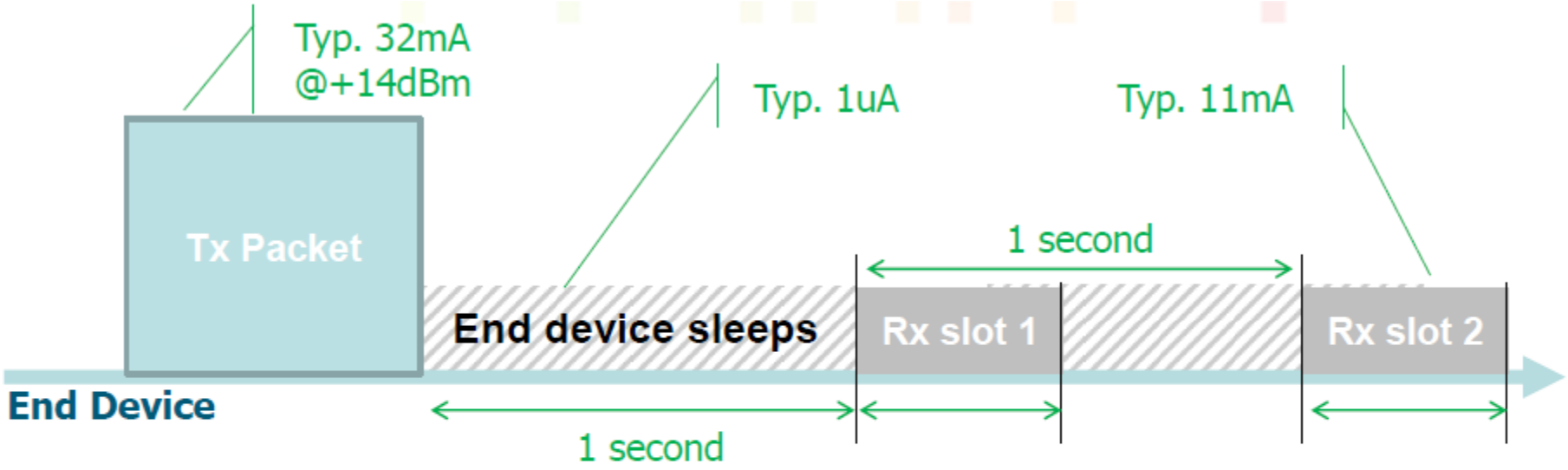
Downlink ?
-> Wait for an uplink !

LoRaWan – Class A

Bidirectional communication

- Unicast messages
- End-devices initiates communication (uplink)
- Server communicates with end-device (downlink) during predetermined response windows
- Pros : Lowest power consumption = longest battery life
- Cons : downlink latency driven by the uplink pace

LoRaWan – Class A



Minimum Rx wake-up time = 5 Symbols :

5.1 ms @ SF7

10.2 ms @ SF8

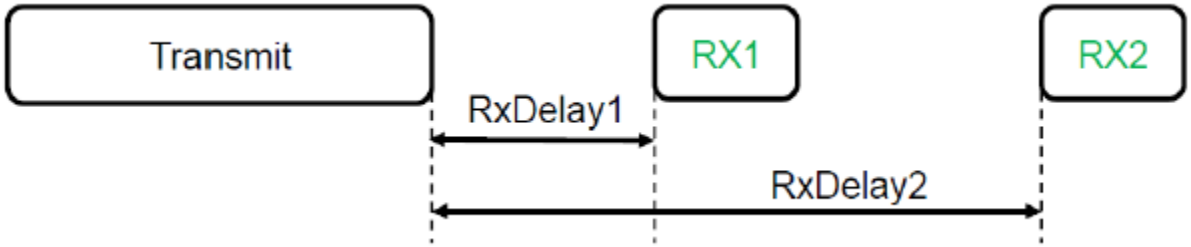
...

164 ms @ SF12

No (wake-up time only) Rx Slot OR Rx Slot 1 OR Rx Slot 2 is used

❑The energy drain when no downlink is << the Tx energy

LoRaWan – Class A



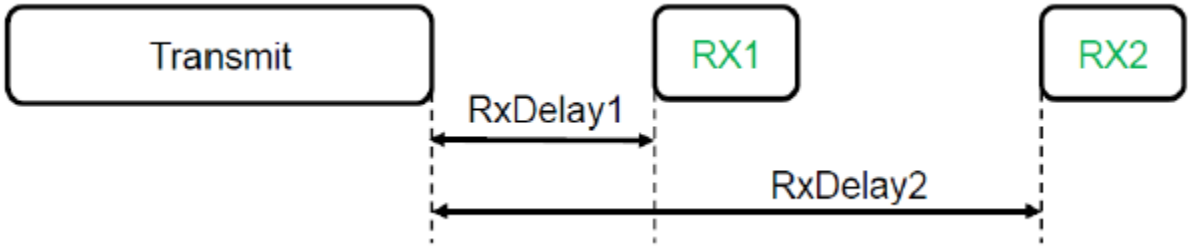
First receive window «RX1» :

✓RxDelay1 is a fixed configurable delay in seconds. Default is 1 second.
✓RX1 frequency uses the same frequency channel as the uplink.
✓RX1 Data Rate is programmable, can equal or lower than the uplink data rate. By default the first receive window data rate is identical to the data rate of the last uplink.

Second receive window «RX2» :

✓RxDelay2 is a fixed configurable delay in seconds. Must be RxDelay1 + 1 second. Default is 2 seconds.
✓RX2 frequency is a fixed configurable frequency.
✓RX2 Data Rate is a fixed configurable data rate.

LoRaWan – Class A



Receive window duration :
The length of a receive wondow must be at least the time required by the end-device's radio transciever to effectively detect a downlink preamble

Receiver activity during the receive windows :
If a preamble is detected during one the receive windows, the radio receiver stays active until the dowlink frame is demodulated.

Is Second receive window «RX2» mandatory ?
If the end-device did not receive the downlink frame during the first receive window "RX1", it must open a second receive window "RX2".
The end-device does not open the second receive window if a frame intended for this end-device has correctly checked the address and MIC (message integrity code) during the first receive window

LoRaWan – Class A

FRMPayload size (Bytes)	240 bps SF12/125k	1 kbps SF10/125k	5.5 kbps SF7/125k
4	~5 uA	~2.2 uA	~1.2 uA
16	~7 uA	~2.5 uA	~1.3 uA
30	~9 uA	~3 uA	~1.4 uA

Assumptions: Pout = +14 dBm, Average Current

- 10 packets / day
- Sleep current ~1uA (includes the MCU)
- MCU is mostly Off during Tx
- No ACK received
- The energy usage of the 2 unused Rx windows is low (<10%)
- Pout = +14 dBm, IDDTX = 32 mA

LoRaWan – Class B

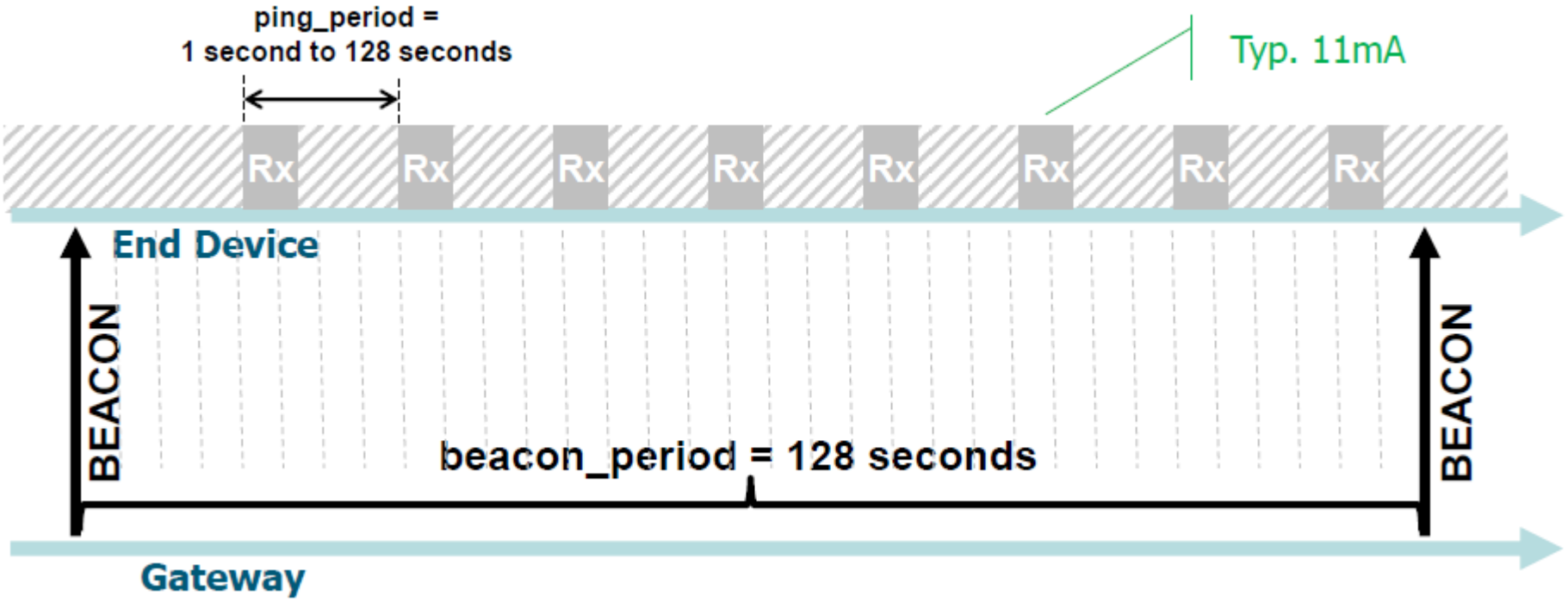
Low downlink latency end-device

Bidirectional communication with scheduled receive slots

- Unicast and Multicast messages
- Periodic beacon from gateway
- Extra receive windows
- Server can initiate transmission at fixed intervals
- Pros : deterministic downlink latency
- Cons : higher power consumption

LoRaWan – Class B

Coordinated Sampled Listening : Network may send downlink packet to node at any Rx slot

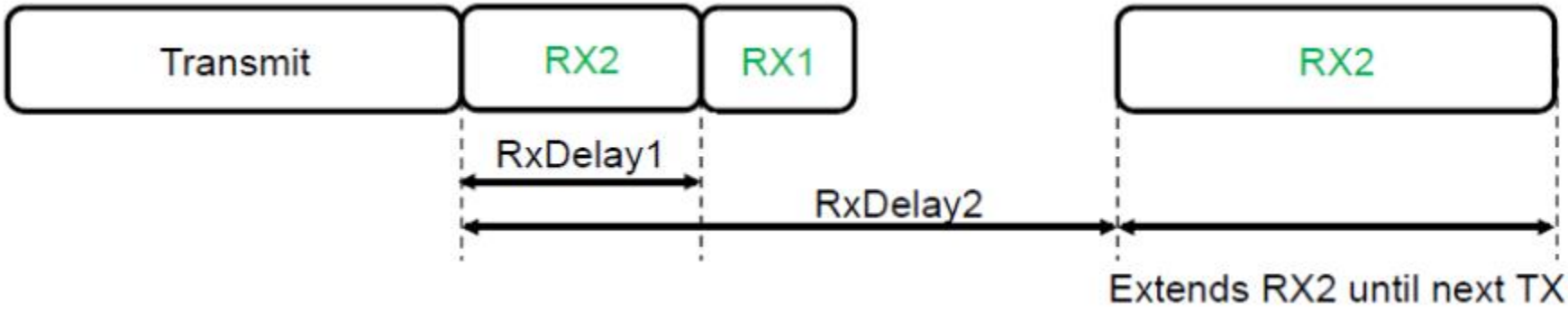


LoRaWan – Class C

No downlink latency end-device

Bidirectional communication

- Unicast and Multicast messages
- Server can initiate transmission at any time
- End-device is constantly receiving
- Pros : Lowest downlink latency
- Cons : highest power consumption (expect end-device to be mains powered)



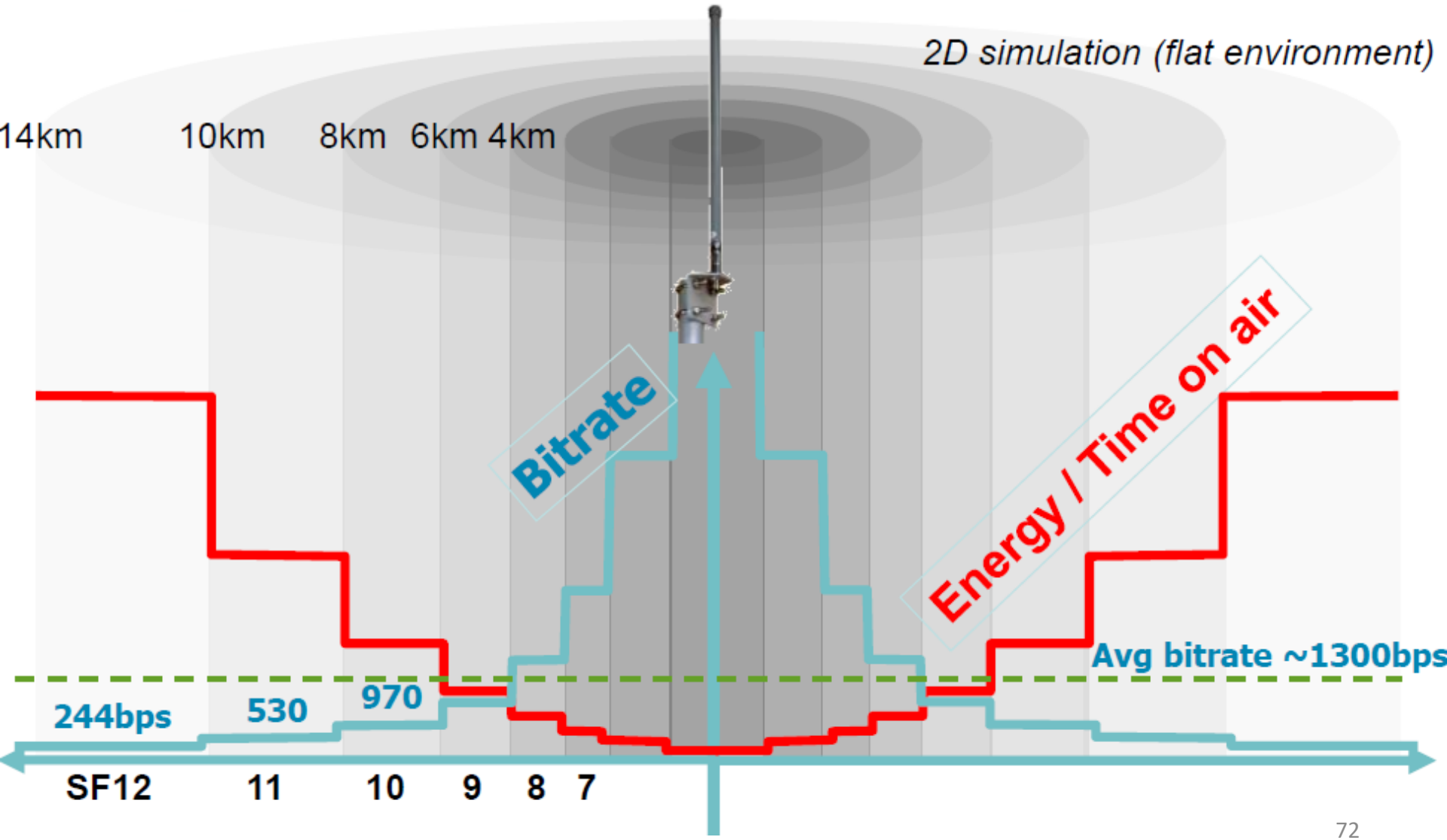
Adaptative datarate

ADR stands for Adaptive Data Rate.
It is the process of adapting the end-device's transmitter output power, data rate and transmit diversity based on the average radio channel attenuation.

- If the average radio link is good the data rate can be increased
- If the demodulation is marginal, the data rate must be lowered

Consequence:
Identical end-devices in different locations might use different data rates / output power

Adaptative datarate



Modulation settings

Longest distance on LoRa modulation :

Data Rate (DR) = 0
- LoRa modulation
- Spreading Factor (SF) = SF12
- Bandwidth (BW) = 125 kHz
- Coding Rate (CR) = 4/5
- Low Datarate Optimize = Enabled

Bit Rate = 244 bps

Receive Sensitivity = -137 dBm

Max Application Payload Size = 51 bytes
- Preambule (programmed) = 8 symbols
- Time On Air = 2466 ms

Modulation settings

Highest Bit Rate on LoRa modulation :

Data Rate (DR) = 6
- LoRa modulation
- Spreading Factor (SF) = SF7
- Bandwidth (BW) = 250 kHz
- Coding Rate (CR) = 4/5
- Low Datarate Optimize = Disabled

Bit Rate = 10938 bps

Receive Sensitivity = -124 dBm

Max Application Payload Size = 222 bytes
- Preambule (programmed) = 8 symbols
- Time On Air = 174 ms

Security

• Encryption : One key field in security is encryption. It protects your data from being read everyone. As IoT may handle sensitive data, it's important for you to understand this concept as you may need to protect the information your device sends.

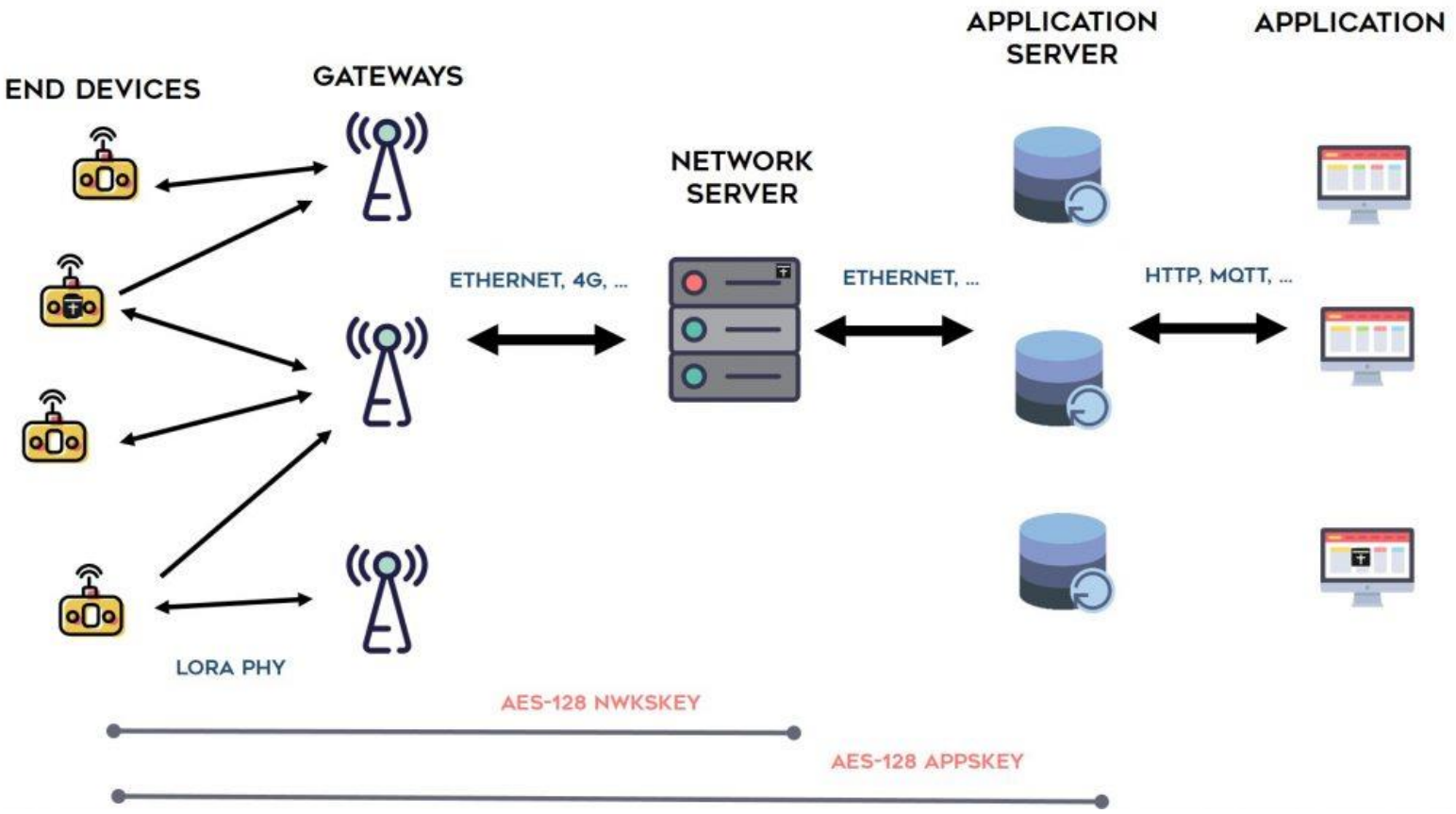
• https://www.makeuseof.com/tag/encryption-care/

•What is Encryption?

Encryption is a modern form of cryptography that allows a user to **hide information** from others. Encryption uses a complex algorithm called a cipher in order to turn normalized data (plaintext) into a series of seemingly random characters (ciphertext) that is unreadable by those without a special key in which to decrypt it. Those that possess the key can decrypt the data in order to view the plaintext again rather than the random character string of ciphertext.

Security

Step1: Encryption: only FRMPayload is encrypted (1 to 1) with the 128-bit AppSKey
Step 2: Authentication: MIC is generated using the 128-bit NwkSKey, and appended to the frame for packet authentication



Security

1. DevAddr: Device Address
   - 32-bit identifier stored in the end-device
   - Uniquely identifies the device on the network
   - Transported in each frame to and from the end-device
   - Obtained during the Activation process

2. NwkSKey: Network Session Key, 128-bit AES encryption key
   - Specific to the end-device
   - Used to encrypt/decrypt payload of MAC-only messages (port 0 between end-device MAC and Network controller)
   - Used to calculate the MIC to ensure message integrity
   - Obtained during the Activation process

3. AppSKey: Application Session Key, 128-bit AES encryption key
   - Specific to the end-device
   - Used to encrypt/decrypt payload of application messages
   - Obtained during the Activation process

Security

DevAddr : Device 32 bits device address on a network. This address is dynamically set by the network operator during the on-boarding process .The same DevAddr can be reused in a network or across different networks. In case of address collision, the cryptographic signature allows to disambiguate

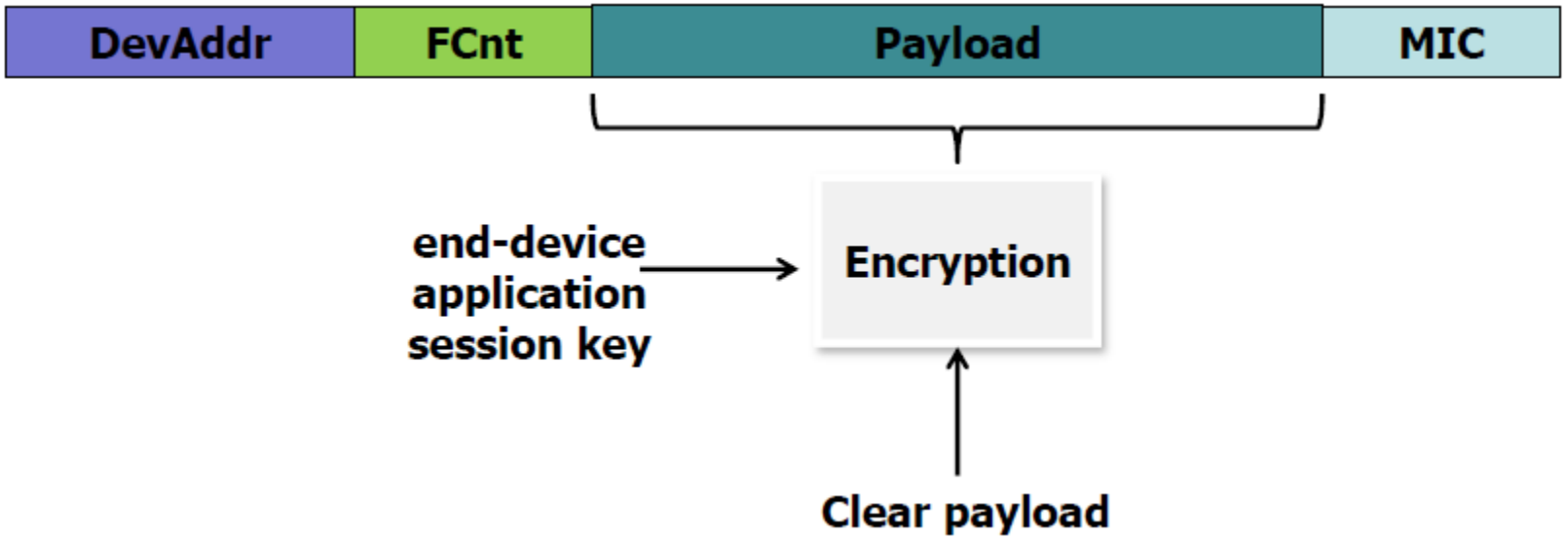
NID : The NID (Network Id) consists of the 7 LSB of the operator network ID (NetID) which is a 3 bytes unique network identifier allocated by the LoRa alliance . Two different networks must have different NetID but may end up with the same NID. The NID field eases the roaming process by reducing the amount of signaling required between Network Servers. Experimental/Private network must use 0000000 or 0000001 for NID.

Security

The **NwkSKey** is a **network session key** specific for the end-devices. It is used by both the network server and the end-device to calculated and verify the **MIC** (message integrity code) of all data messages to ensure data integrity. It is further used to encrypt and decrypt the payload field of a MAC-only data messages.

The **AppSKey** is an application session key specific for the end-devices. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages. It is also used to calculated and verify an application level MIC that may be included in the payload of application – specific data messages.

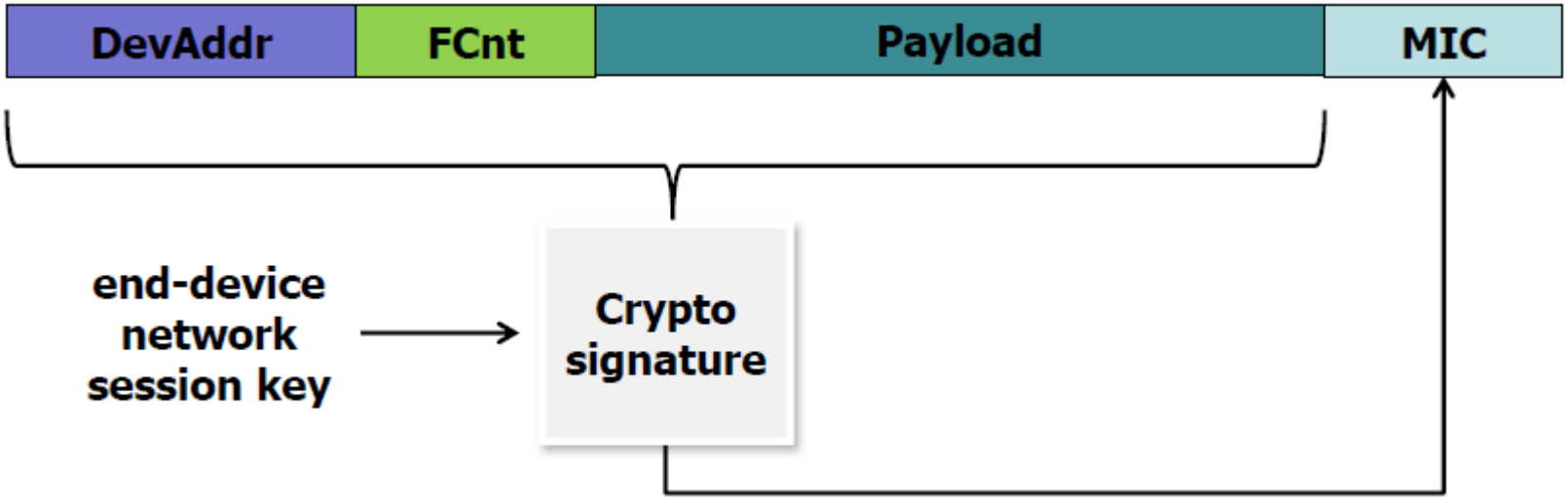
Step 1 : Payload Encryption



All payloads are encrypted using an AES algorithm with a 128bits secret key, the Application Session Key

Each end-device has its own unique Application Session Key only known by the end-device and the application server and only used for encryption

Step 2 : Packet authentification



All frames contain a 32bits cryptographic MIC signature computed using an AES algorithm with a 128bits secret key, the Network Session Key

- **The Network Session Key is different from the Application key Session**
- **Each end-devices has its own Network Session Key only known by the end-device and the network server and only used for signature**

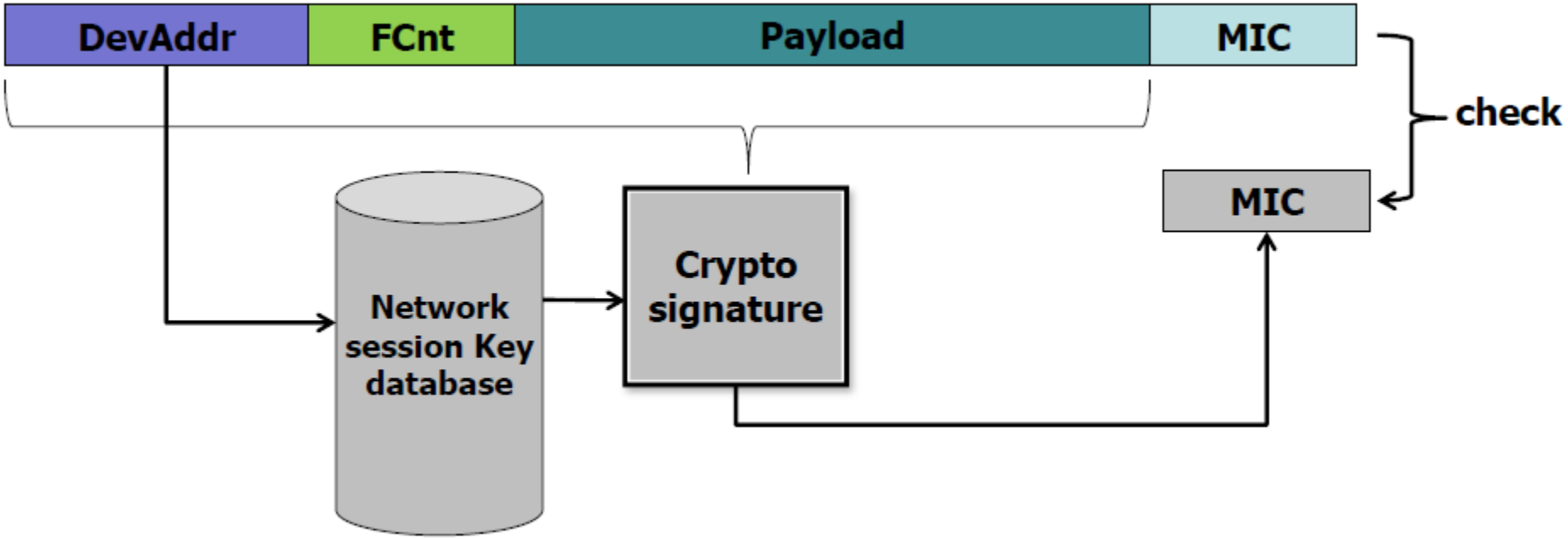
Frame signature

The frame signature (Message Integrity Code “MIC”) is computed over the entire frame

- Therefore the frame cannot be modified in any way between the end-device and the network server without compromising the signature.
- The only components involved are:
- The end-device
- The network server
- The gateway, the gateway backhaul link, etc, … are totally transparent from a security perspective

Authentification of the uplink

Upon reception of a frame, the network server checks that the frame received MIC signature matches the one computed using the end-device's network session key contained in its key database



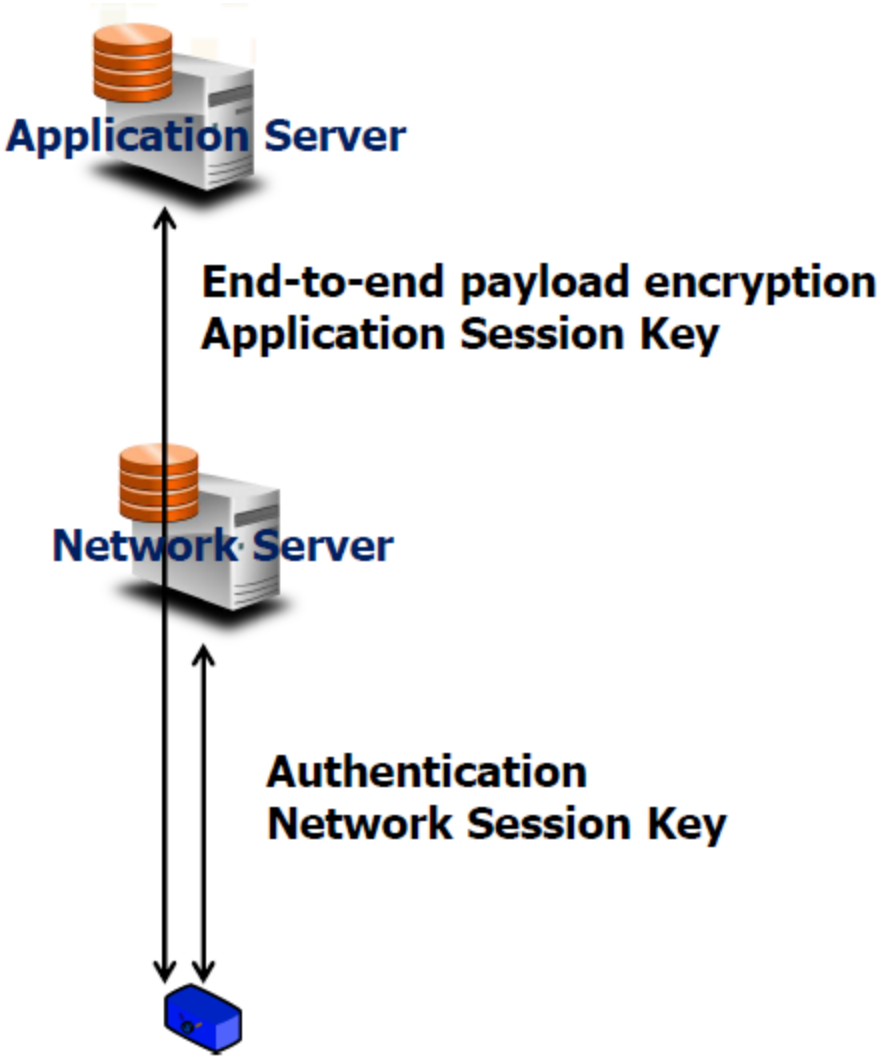
If the 2 MICs match then the frame is really coming from the legitimate end-device and its content hasn't been modified in any way

Authentification of the downlink

- **The same process happens on the down-link.**
- **The network server signs each frame with a MIC computed over the entire transmitted packet using the destination end-device's Network Session Key.**

- This way, the server can differentiate a legitimate end-device from one trying to steal the end-device's DevAddr (cloning attack).
- The end-device can check that the commands coming from the network are legitimate.
- Additionally each frame contains a frame counter forbidding "replay" attacks.

End to End security



End-device personalization and Activation

To participate in a LoRaWAN network, each end-device has to be personalized and activated :

- Personalization : End-device is configured at production time.
- Activation : Before an end-device can communicate on a LoRaWan network, it must be actived.

End-device Activation : 2 methods

By Personalization «ABP»

Over the Air «OTAA»

Activation By Personalization

Network authority and Application provider negociate

- A set of DevAddr (for instance 1000 Addresses, unique to the network)
- A set of AppSKey
- A set of NwkSKey

Advantage: devices are already pre-commissionned[1]
Drawback: roaming from network to network is impossible

Activation By Personalization

This is the simplest scenario , targeting mainly B2B use cases.

The device is registered by the service provider with a given network operator before being personalized.

The operator directly provides the correct DevAddr and network/app session keys The device is directly personalized at fabrication with the correct DevAddr and network+application session keys.

The device is fully functional on the network as soon as powered-up.

The device is therefore tied to a given network and service provider

Over the Air Activation “OTAA”

The join procedure requires the end-device to be personnalized with the following information before it starts the join procedure : a globally unique end-device identifier (DevEUI), the application identifier (AppEUI) and a an AES-128 key (AppKey)

- **DevEUI:** unique source address identifying the node of the application provider
- **AppEUI:** shared secret, destination address, globally unique identifier owned by the application provider. AppEUI routes the Join Req to the right Join Server
- **AppKey:** used forJoinReq and JoinAccept authentication

Warning ! AppKey is different from AppSKey

Over the Air Activation “OTAA”

DevEUI : Device 64 bits unique device identifier. Equivalent to the MAC address of a network adapter card. This address is written in the device by the manufacturer at the same time than the firmware. It consists of a 24bits Organizationally Unique Identifier (*) and a 40 bit serial number. The OUI code is unique for any manufacturer and provided by the IEEE and the serial code is set freely by the manufacturer.

Over the Air Activation “OTAA”

AppEUI : Join Server 64 bits unique server identifier. This number uniquely identifies a Join Server It consists of a 24bits Organizationally Unique Identifier (*) and a 40 bit serial number. The OUI code is the manufacturer’s code of the entity operating the Join Server. The serial number can be used if several Join Server are operated by the same entity. For example Semtech might operate a Join Server with AppEUI : 00 16 C0 00 00 00 00 01 “00 16 C0” is Semtech’s OUI

Over the Air Activation “OTAA”

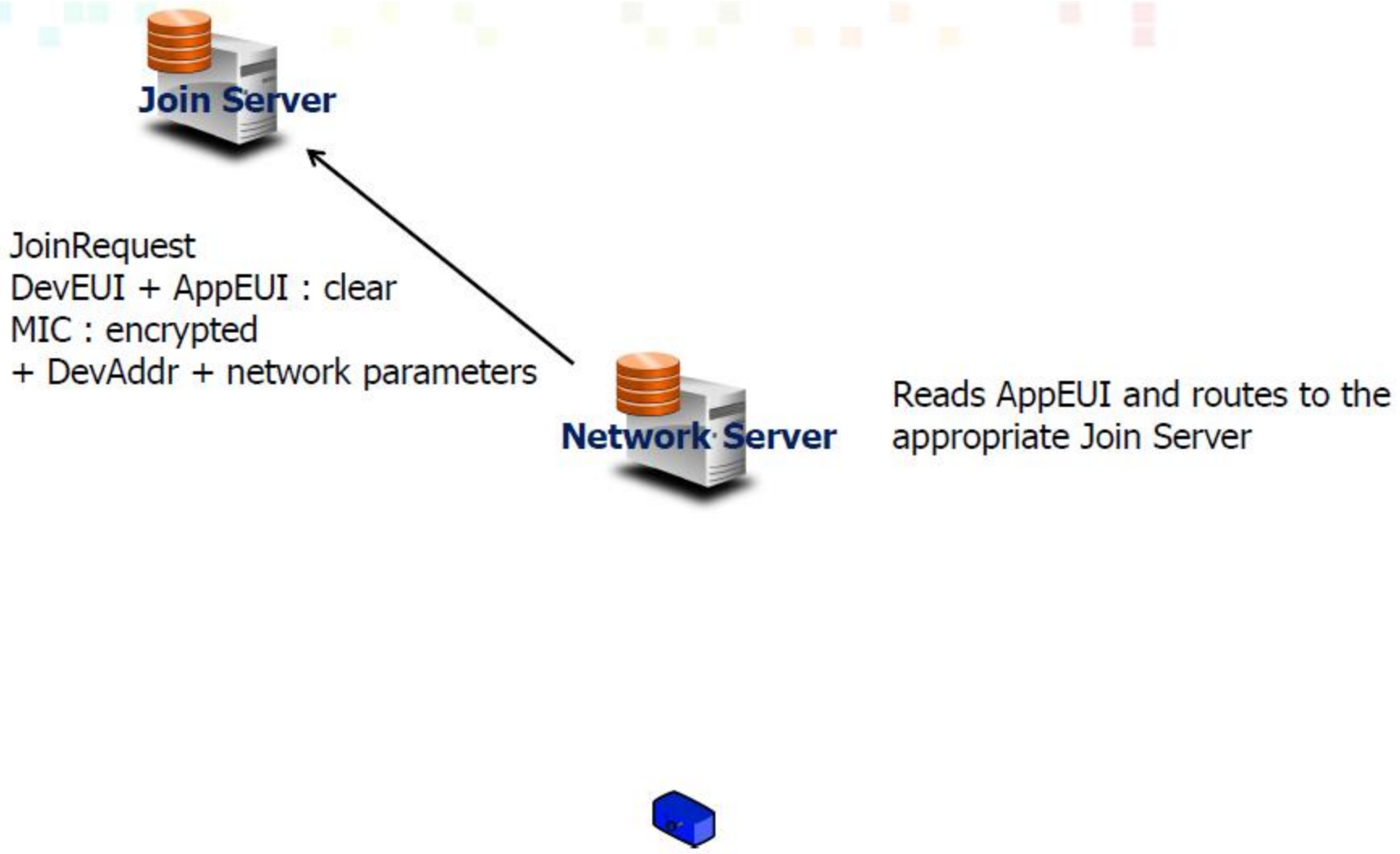
The **AppKey** is an AES-128 application key specific for the end-device that is assigned by the application owner to the end-device and most likely derived from an application specific root key exclusively known to and under control of the application provider.
Whever an end-devices joins a network via OTAA, the AppKey is used to derive the session keys NwkSKey and AppSKey specific for the end-device to encrypt and verify network communication and application data.

Over the Air Activation “OTAA”

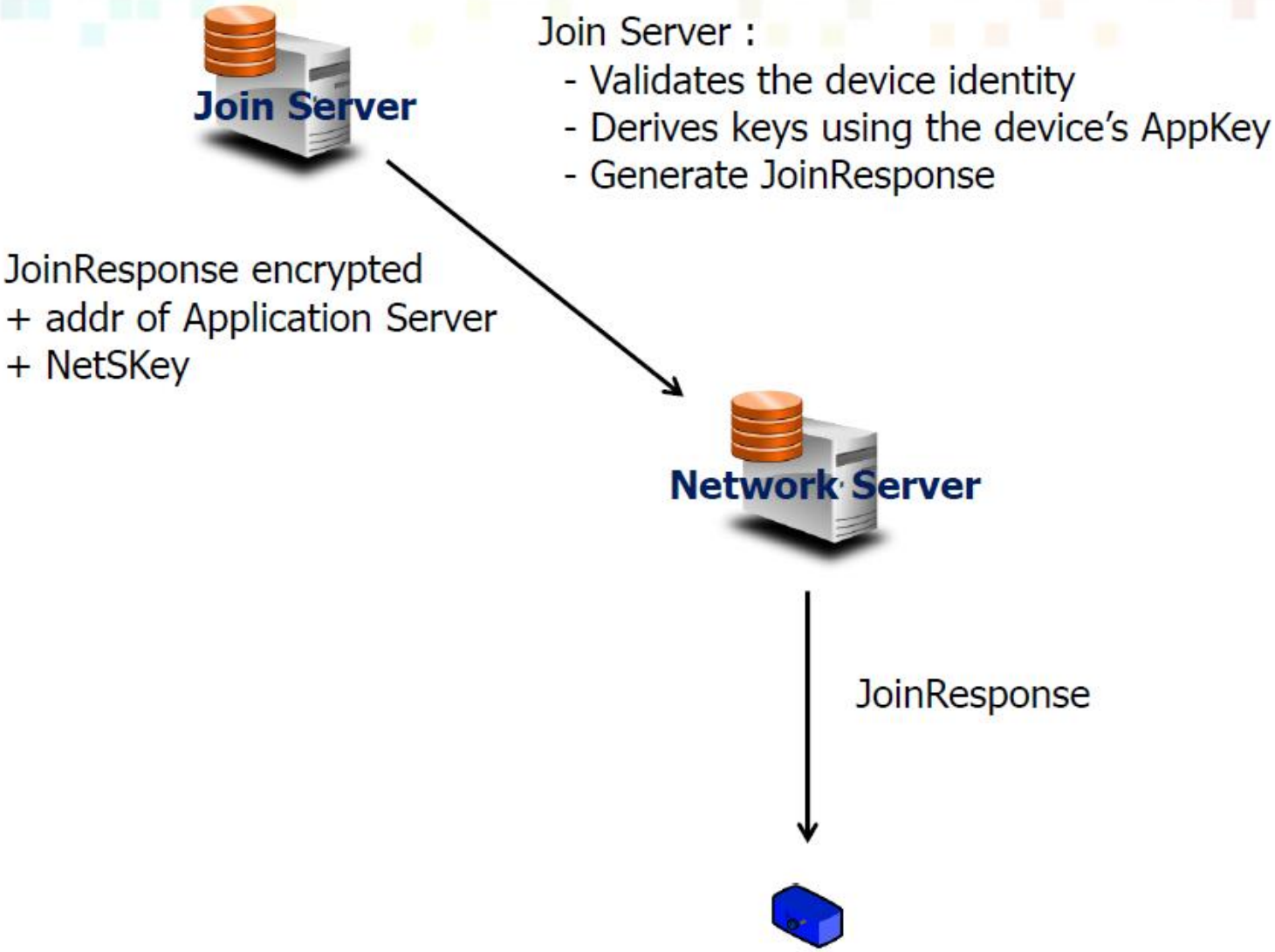
End-device manufacturer transfers DevEUI + AppKey to the Join Server

Over the Air Activation “OTAA”

Over the Air Activation “OTAA”



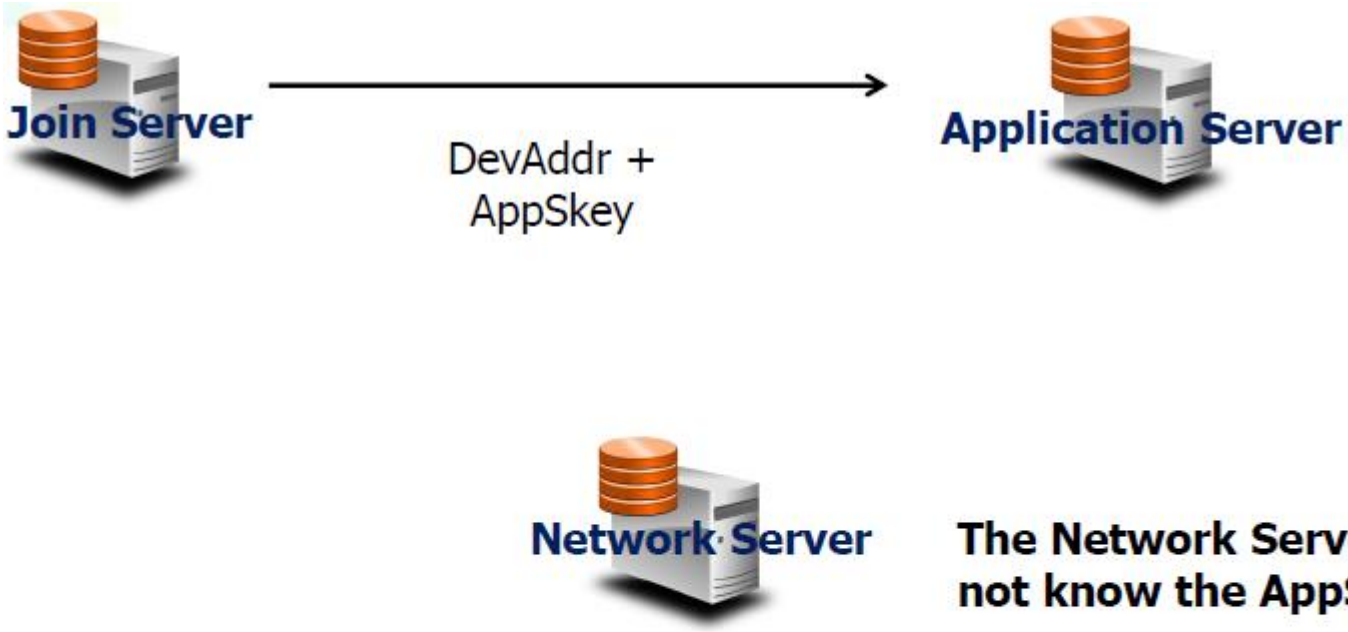
Over the Air Activation “OTAA”



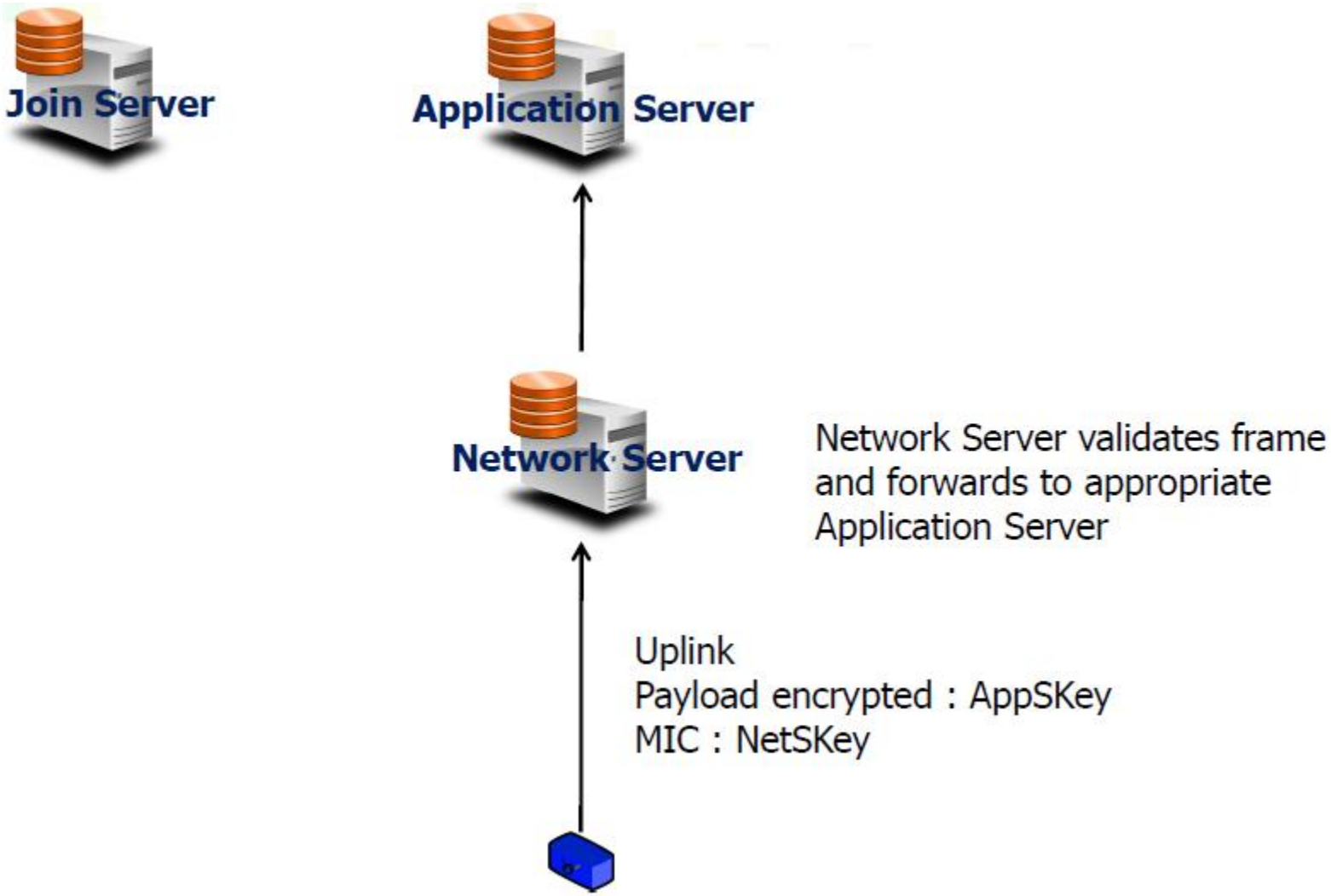
Over the Air Activation “OTAA”

Device derives the same AppSkey and NetSKey from content of JoinResponse + AppKey

Over the Air Activation “OTAA”



Over the Air Activation “OTAA”



Over the Air Activation “OTAA”

In this scenario the device is specific of a given service provider but is activated over-the-air on any network.
The device’s devEUI and AppKey (the device root key) are allocated autonomously by the device manufacturer.
The device’s AppEUI is set to point to the wanted Join Server (selected or operated by the service provider).
The device is service provider specific. The device is purchased by the service provider along with its devEUI and AppKey.
The device is activated over the air with the chosen operator. The same device can operate on any network and in different countries.

The selection of the operator is performed during the JoinReq – JoinResponse message exchange.