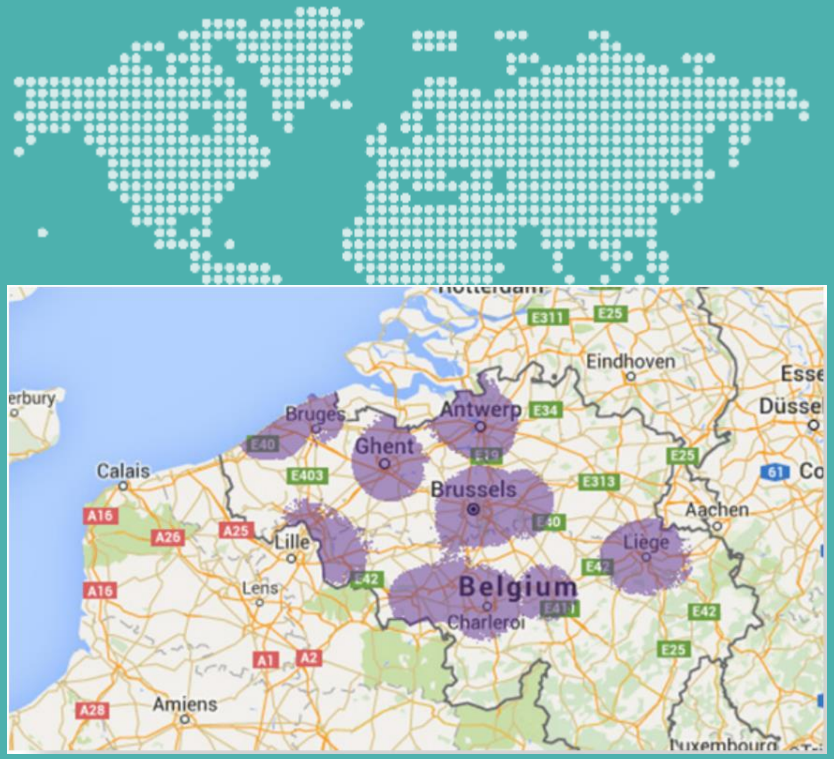
SENSING LABS

LoRaWan basics

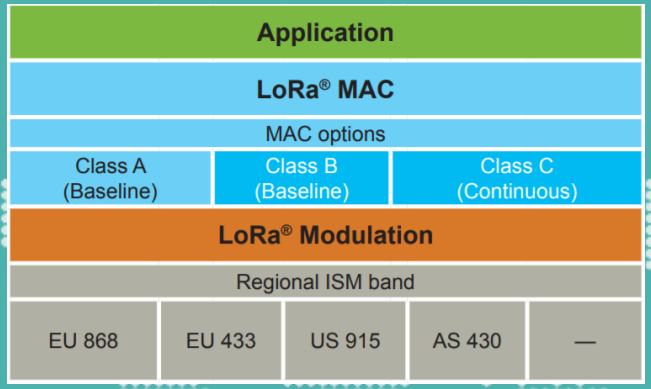
October 2017

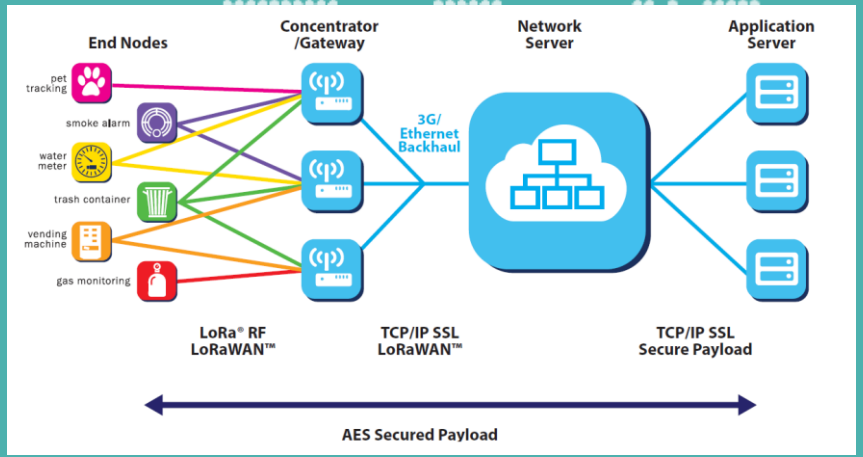
What is LoRa?



- LoRa is the physical layer used for LoRaWan long range communication link
- Chirp spread spectrum modulation
  - Used in military and space since decades
  - LoRa is the first low cost implementation
- Advantages
  - Long range capability
  - Best link budget among all standardized wireless communication technologies
- A single gateway or base station can cover entire cities or hundreds of km2

What is LoRaWan?





- LoRaWan defines the communication protocol and system architecture for the network while the LoRa physical layer enables the long-range communication link.

- The network architecture implies:
  - End nodes
  - Gateways/concentrators/Base stations
  - Network server
  - Application server
  - Authentication server

LoRa Alliance

Office

LoRa Alliance™
3855 SW 153rd Drive

Beaverton, OR 97003
Phone: +1 503-619-2685
Fax: +1 503-644-6708

admin@mail.lora-alliance.org

- LoRa Alliance
  - Open
  - non-profit
  - initiated by industry leaders
- In charge of specifying and promoting the LoRaWan protocol

Public and Private Networks

- Operators are deploying LoRaWan networks
  - These are Public networks
- Some users do not want or cannot (due to coverage lacks) rely on these public networks
  - It is thus possible to deploy private networks
- In theory, public and private networks do not see each other
  - However, in reality, both types of network use the same radio bands

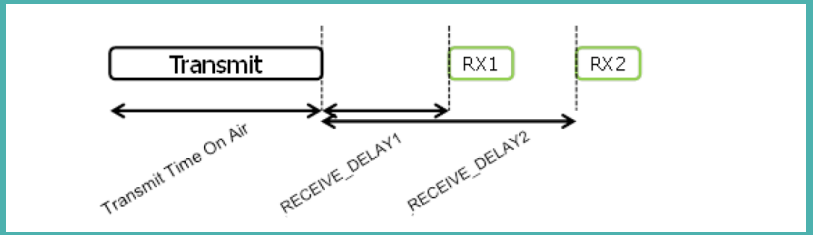
Asymmetric Networks

- An asymmetric network is a communication network where the different elements do not present the same level of complexity
- These networks usually present a star topology, meaning that the end nodes communicate directly with the network receivers, without using any repeater
- LoRaWan networks are highly asymmetric:
  - End nodes can use only a single channel at a time
  - Network receivers usually handle 48 different channels in parallel
    - 8 frequencies
    - 6 datarates per frequency

Frequency plan

- The frequency plan is the list of radio channels used at a given instant:
  - End nodes can use only one at once
  - Base stations listen all at once
- Base stations usually listen 48 channels
  - 8 different frequencies
  - Multiplied by 6 different datarates on each channel
- The minimal frequency plan includes 3 mandatory channels on the minimum datarate

1.5 communication mode (class A)



- Usual communication mode are
  - Monodirectional (transmit only)
  - Bidirectional (end node can receive messages at any moment or almost)
- LoRaWan is based on 1.5 communication mode
  - The end nodes open short reception window(s) after each transmission
  - Communication are always initiated by end nodes
- This mechanism
  - Increases the battery lifetime of end nodes (the energy budget of permanent reception is high)
  - While keeping the possibility of sending downlink frames to end nodes

Adaptative datarate

Spreading factor (at 125 kHz)	Bitrate	Range (indicative value, depending on propagation conditions)	Time on Air (ms) For 10 Bytes app payload
SF7	5470 bps	2 km	56 ms
SF8	3125 bps	4 km	100 ms
SF9	1760 bps	6 km	200 ms
SF10	980 bps	8 km	370 ms
SF11	440 bps	11 km	740 ms
SF12	290 bps	14 km	1400 ms

(with coding rate 4/5 ; bandwidth 125Khz ; Packet Error Rate (PER): 1%)

- One of the fundamental features of LoRaWan
  - The device allows the network to modify its datarate
  - The network can thus optimize the radio medium usage
- Improves the time on air of messages transmitted by nodes with high link budget
- Improves the global capacity of the network, that is the global number of messages it can handle on a given period

Security in LoRaWan

- By design, LoRaWan security is split in two levels:
  - Network Security
  - Application security
- The network security, based on a first AES128 key, allows managing:
  - Data integrity
  - Source authenticity
- The application security, based on a second AES128 key, allows managing end to end confidentiality of application data
  - In particular, the network cannot see the data it transports from the end nodes to the applications

The two connection methods

- Whatever the connection method used, the identity of the device – the DevEUI - must be shared between the device and the system
- ABP connection method – Activation By Personalization
  - Connectivity critical parameters are know a priori and manually configured into the end node AND the network system
    - The 2 security keys:
      - AppSKey (Application Session Key)
      - NwkSKey (Network Session Key)
    - The frequency plan
    - The network address
- OTAA connection method – Over The Air Activation
  - A single information needs to be shared: a security key
    - It is configured into the end node
    - It can be managed by a trusted authority on network side
  - On connection, all the connectivity critical parameters are computed and/or transmitted by the network to the end node

Thank you

SENSING LABS

Delivering Intelligence

Additional features

- At the application level: the confirmed mode
  - End node requires an acknowledge from the network
  - Preferentially not used as downlink medium is the critical resource for the network (radio regulations)
- At the network level: MAC commands
  - linkCheck, linkADR, DutyCycle, RxParam, DevStatus, NewChannel, RXTiming