LoRa by Experimentalists

KIVI
Engineering Society

October 10, 2016 **KIVI - Prinsessegracht 23, 2514 AP Den Haag**

Presenters : Pieter van Nieuwaal lorasensor@gmail.com
Dirk Gooris loragateway@gmail.com

Introduction

- About us
- How to gain knowledge of new technologies ?
- We hope to inspire you in the way we work

Purpose of this presentation

- Our way of working
- What is LoRa and LoRaWAN
- How does it work
- What can you do with it
- Don’t forget the Demo….

LoRa in the world of IoT

Internet of Things:

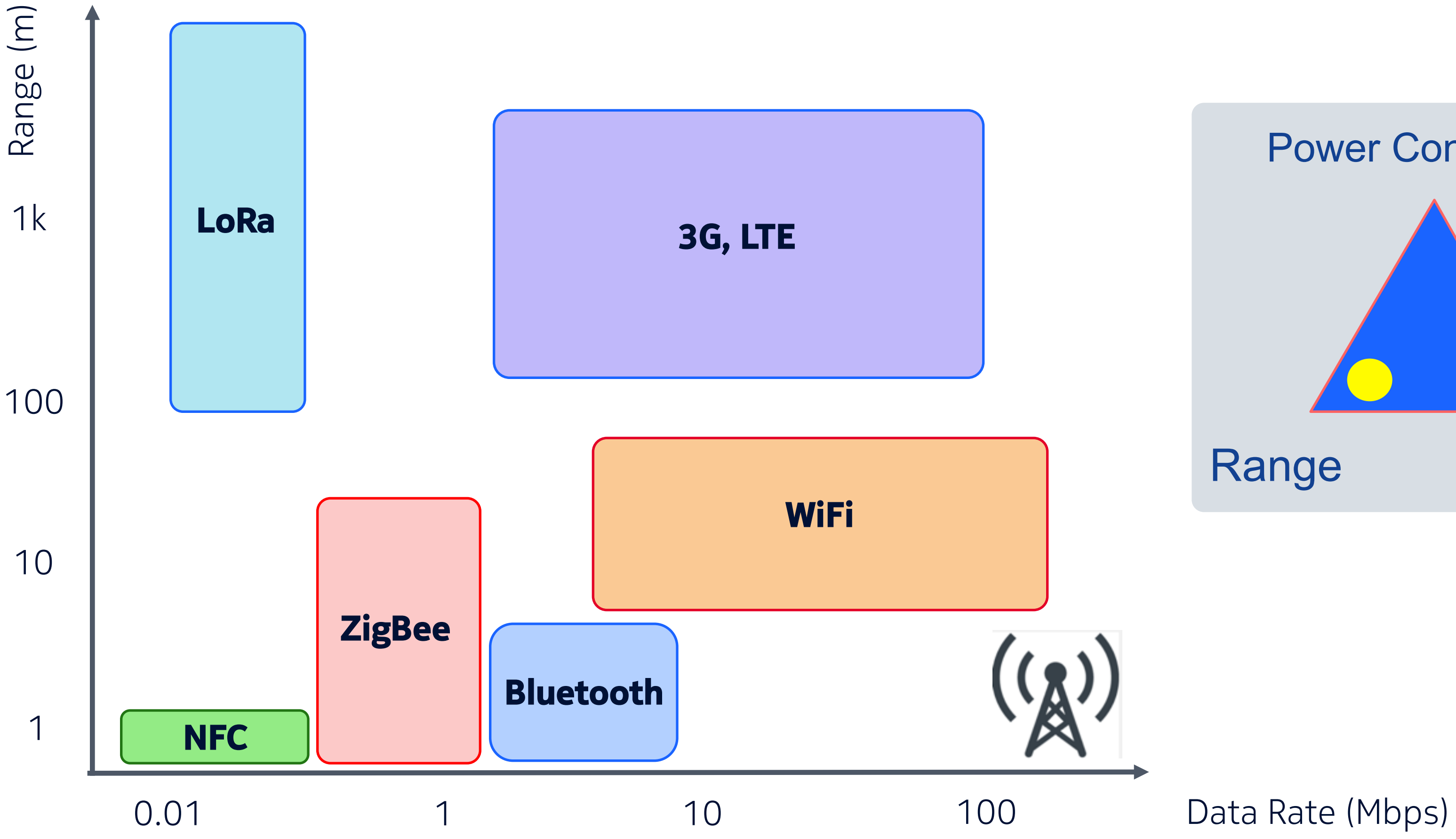
Diversity of devices having specific communication needs
Think about :

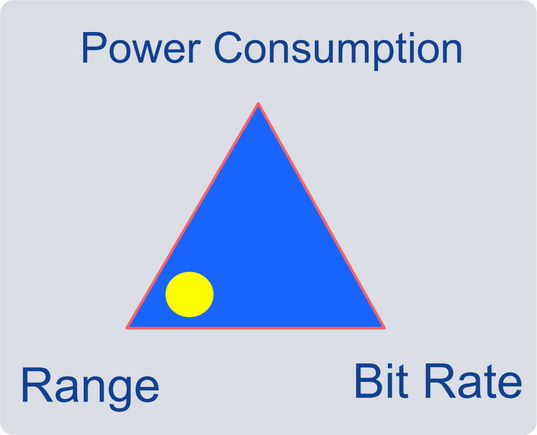
- Power
- Range
- Bitrate
- Complexity

Which technology supports :

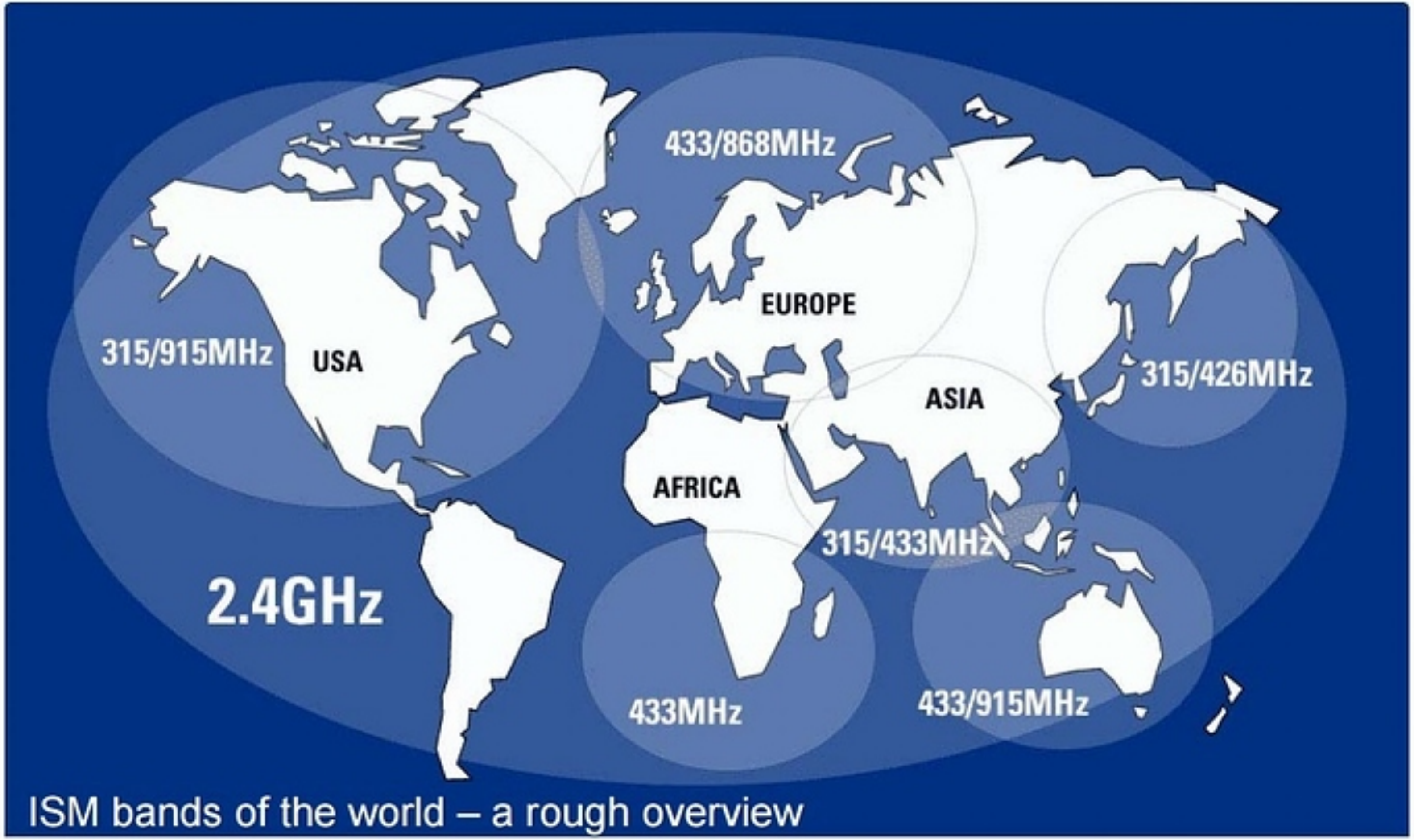
- Very low power consumption – 5 year battery lifetime
- Long Range > 5km
- Bitrate – may be low
- Complexity – must be low: cost reduction

LoRa versus other radio technologies





LoRa frequencies using unlicensed spectrum



What is LoRa

LoRa (Long Range)

LoRa is a **modulation technique** that provides significantly longer range than competing technologies.

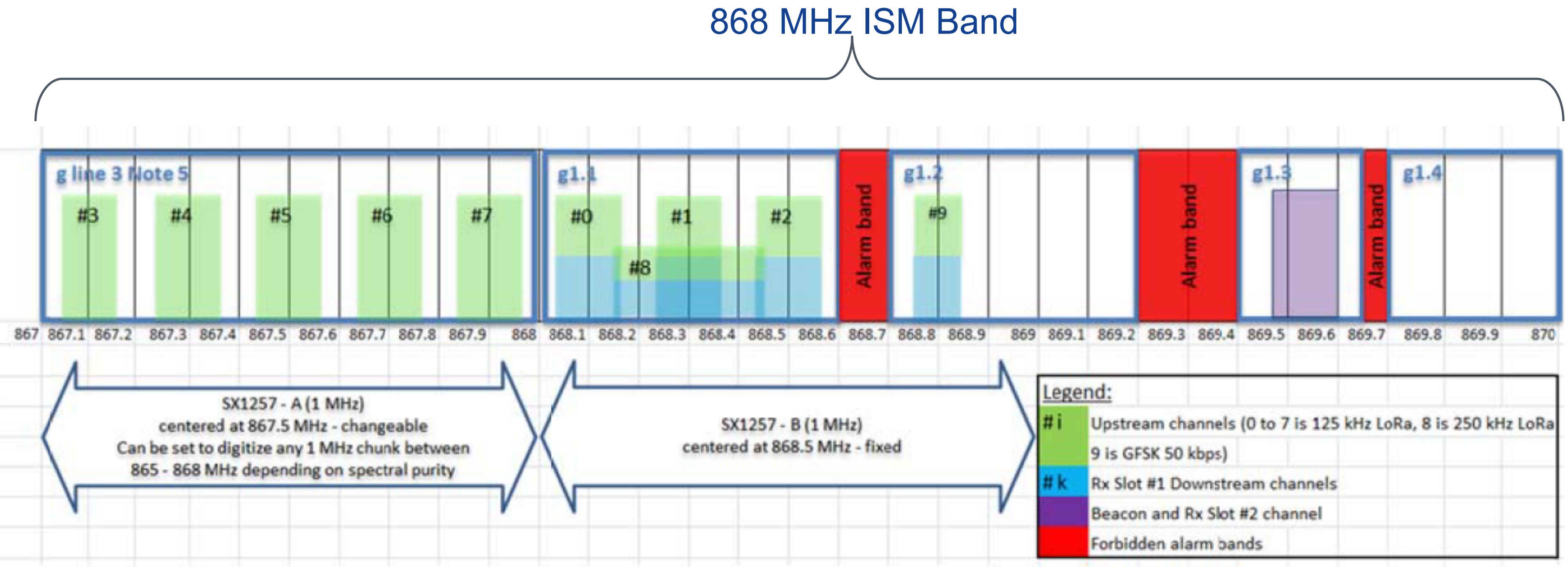
LoRa significantly improves the receiver sensitivity and, as with other spread-spectrum modulation techniques, uses the entire channel bandwidth to broadcast a signal, making it robust to channel noise and insensitive to frequency offsets caused from the use of low cost crystals.

The LoRa modulation is the physical layer (PHY).

LoRa Spectrum at 868 MHz according to ETSI spec

LoRa is a FM chirped spread spectrum (CSS) radio modulation format patented by Semtech.

LoRa is only the Physical Layer (PHY – OSI Layer 1)



SX1257 - A (1 MHz)
centered at 867.5 MHz - changeable
Can be set to digitize any 1 MHz chunk between
865 - 868 MHz depending on spectral purity

SX1257 - B (1 MHz)
centered at 868.5 MHz - fixed

Legend:

#i	Upstream channels (0 to 7 is 125 kHz LoRa, 8 is 250 kHz LoRa 9 is GFSK 50 kbps)
# k	Rx Slot #1 Downstream channels
🟪	Beacon and Rx Slot #2 channel
🟥	Forbidden alarm bands

LoRa Spectrum at 868 MHz according to ETSI spec

#	Freq (MHz)	LoRa BW	SF Range	Time allowed on this Channel per hour	Time allowed	Regulatory Regime	Max ERP
0	868.1	125k	SF 7-12	t1=36s - t2-t3-t9	t1+t2+t3+t9 < 36s/hour	g1.1	25mW or +14dB
1	868.3			t2=36s - t1-t3-t9			
2	868.5			t3=36s - t2-t1-t9			
3	867.1			t4=36s - t5-t6-t7-t8	t4+t5+t6+t7+t8 < 36s/hour	g line 3	
4	867.3			t5=36s - t4-t6-t7-t8			
5	867.5			t6=36s - t4-t5-t7-t8			
6	867.7			t7=36s - t4-t5-t6-t8			
7	867.9			t8=36s - t4-t5-t6-t7			
8	868.3	250k	SF 7	t9=36s - t1-t2-t3	t1+t2+t3+t9 < 36s/hour	g1.1	
9	868.8	GFSK 50kbps		t10=3.6s	t10<3.6s/hour	g1.2	

Information Theory – how to improve the S/N budget

Shannon/Hartley Theorem: C/B = 1.433 * S/N

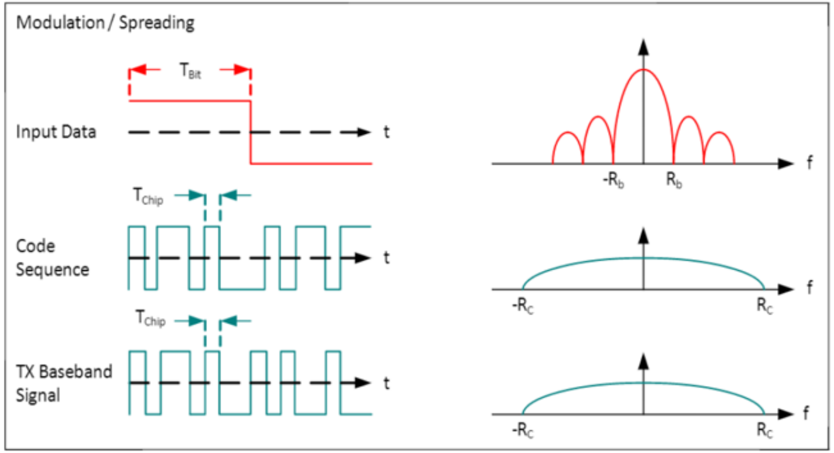
C = Channel Capacity (bits/s)
B = Channel Bandwidth (Hz)
S = Signal Power (W)
N = Noise Power (W)
S/N = Signal to Noise ratio

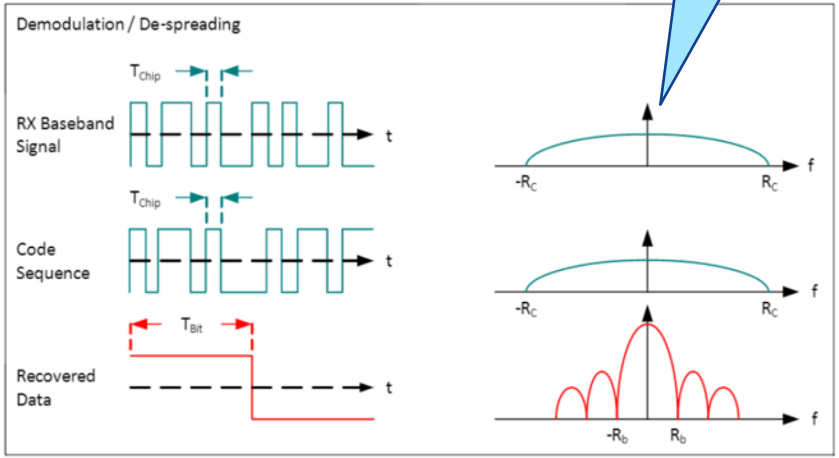
For spread spectrum applications, S/N << 1, so C/B ≈ S/N or N/S ≈ B/C

In a channel with a fixed N/S ratio to achieve error free transmission, only the transmitted bandwidth need to be increased.

Rb = bit-rate (bits/s)
Rc = chirp-rate (chirps/s)
Rb << Rc
Gp = 10 * log (Rc/Rb) (dB)

Spread Spectrum technology:
Frequency of Input Data << Frequency of Code Sequence
Modulation by multipliction of input data with code sequence.
Demodulation by multiplication of baseband signal with code sequence





More about LoRa Radio

Conclusion: with Spread Spectrum technology, we can improve the S/N ratio by increasing the BW.
For IoT, we need a cheap and practical implementation. So no highly accurate clocks but simple FM modulation and simple/fast synchronization.

For LoRa:

$$R_b = \frac{SF * BW}{2^{SF}}$$

Where:

Rb = Bit Rate (bits/s)
SF = Spreading Factor (7..12)
BW = Bandwidth (Hz)

And:

$$R_s = \frac{BW}{2^{SF}}$$

$$R_c = R_s * 2^{SF}$$

Where:

Rs = Symbol Rate (symbols/s)
Rc = Chip Rate (chirps/s)

Then:

Rc = BW (chirps/s) → one chirp is sent per second per Hz of bandwidth

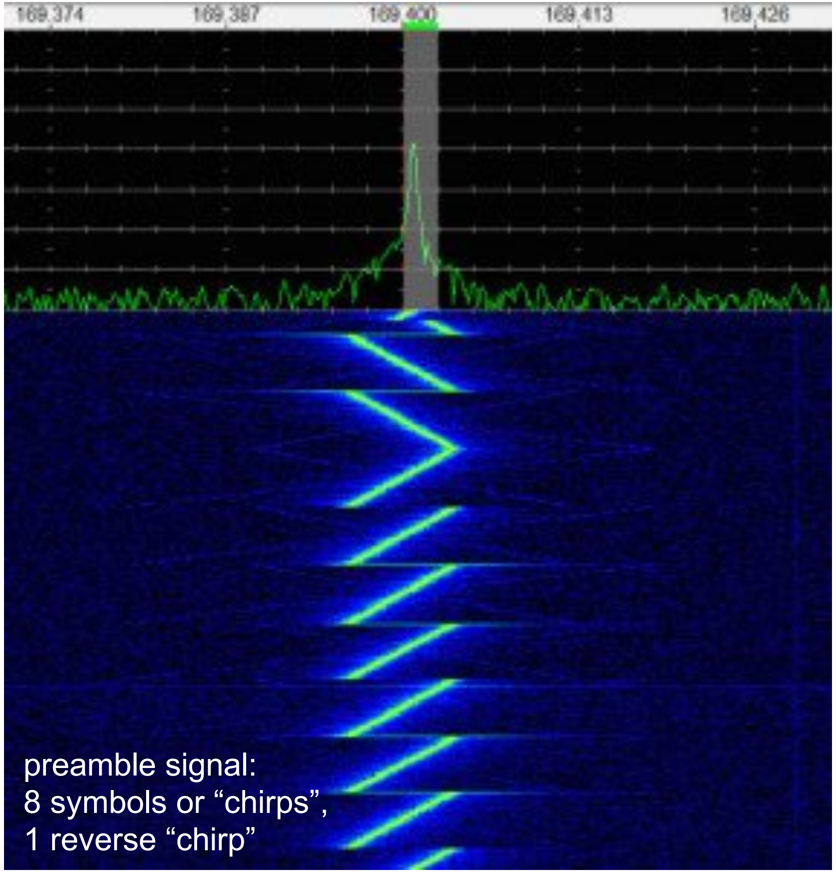
More details in:
Semtech
AN1200.22

Summary

Exchange bitrate for bandwidth returns improved signal-to-noise ratio.

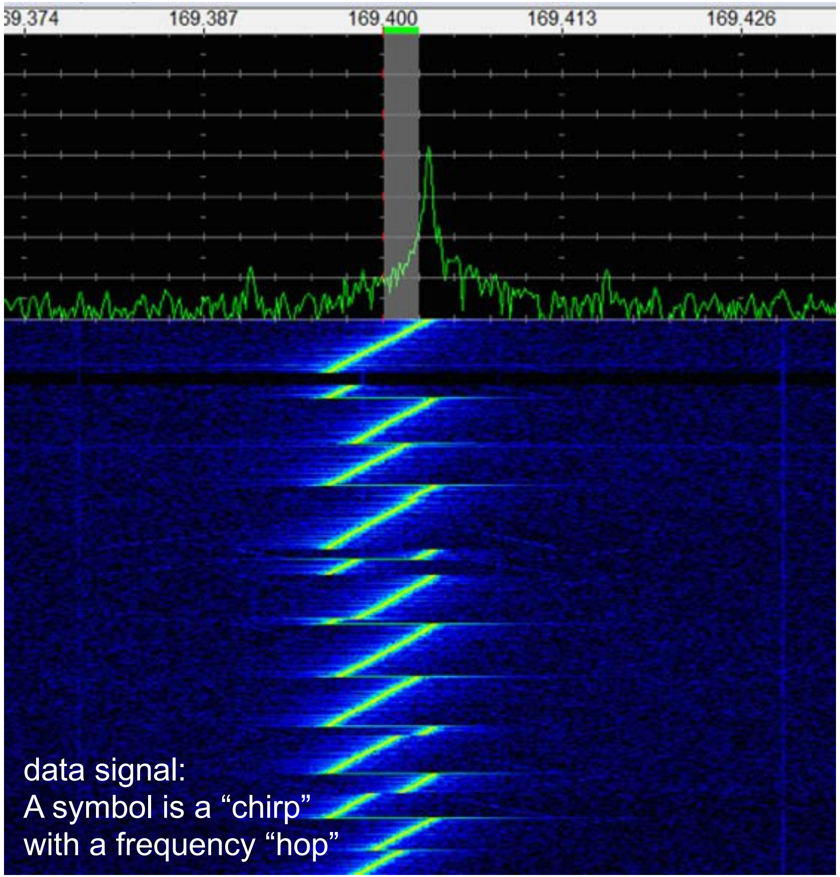
Result: Long Range and Low Power

LoRa modulation



preamble signal:
8 symbols or “chirps”,
1 reverse “chirp”

frequency



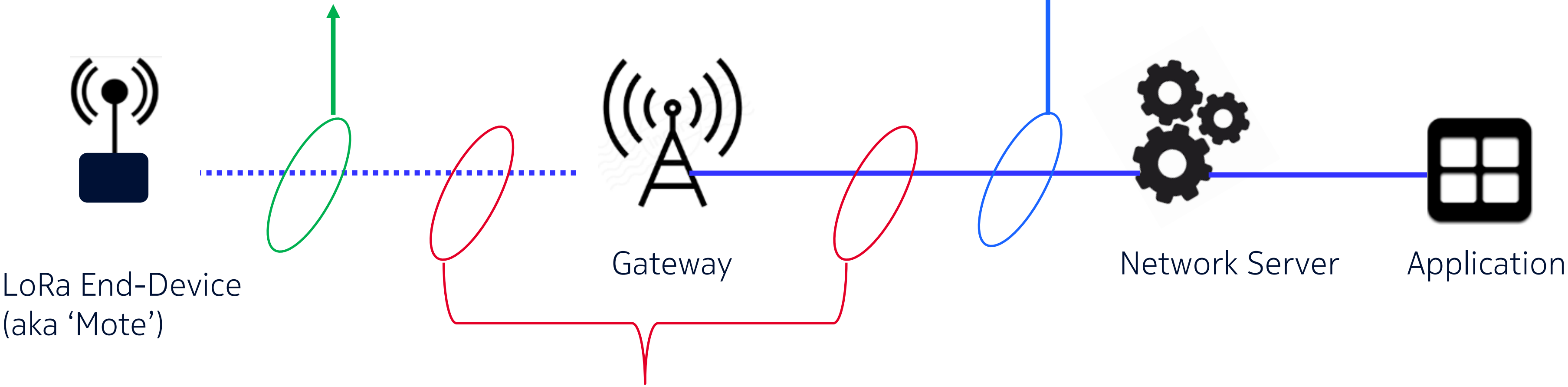
data signal:
A symbol is a “chirp”
with a frequency “hop”

frequency

level

time

What is LoRa and what is LoRaWAN



Physical layer:
LoRa modulation
radio technology

UDP/IP transport
Not standardized , Json data frame
Often referred to by the “Semtech” protocol

LoRa End-Device
(aka ‘Mote’)

Gateway

Network Server

Application

Data layer :
LoRaWAN protocol specified in:
https://www.lora-alliance.org/portals/0/specs/LoRaWAN Specification 1R0.pdf

Example of a data packet sent by the Gateway to the Network Server

LSNR – Local Signal to Noise Ratio
RSSI – Received Strength Indication

```
{"rxpk":[{
    "tmst":101662084,
    "chan":1,
    "rfch":0,
    "freq":868.300000,
    "stat":1,
    "modu":"LORA",
    "datr":"SF11BW125",
    "codr":"4/5",
    "lsnr":11.5,
    "rssi":-45,
    "size":21,
    "data":"QBfZIu4AAABb7pZcazQJD9vs7Zj6"}
]}
```

Parameters added by the gateway

Data field sent by the End-Device

What is LoRaWAN

LoRaWAN

LoRaWAN is a data link (Medium Access Control) protocol for a high capacity long range and low power star network that the LoRa Alliance is standardizing for Low Power Wide Area Networks (LPWAN).

The LoRaWAN protocol is optimized for low cost, battery operated sensors and includes different classes of End-Devices to optimize the tradeoff between network latency and battery lifetime.

It is fully bi-directional and was architected by security experts to ensure reliability and safety.

The LoRa communication with the Gateway

- The LoRa End-Device only sends information when it has to.
- Depending on the Use Case, this could be between minutes or years
- Therefore, the lifetime of the batteries depends on the Use Case

FLOOD DETECTOR
Zzz
LoRa End-Device

LoRaWAN two way communication

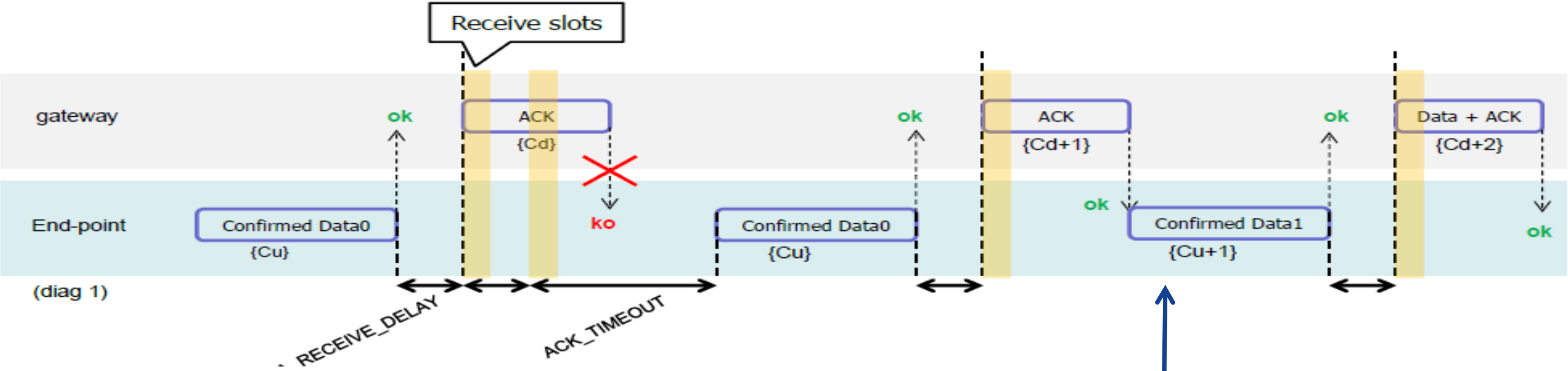
- Only when the LoRa End-Device sends data there will be a opportunity for the gateway to send information back to the End-Device. Remember that the End-Device most of the time sleeps and does not listen to radio signals (Class-A device)
- Optionally, received packets can be confirmed

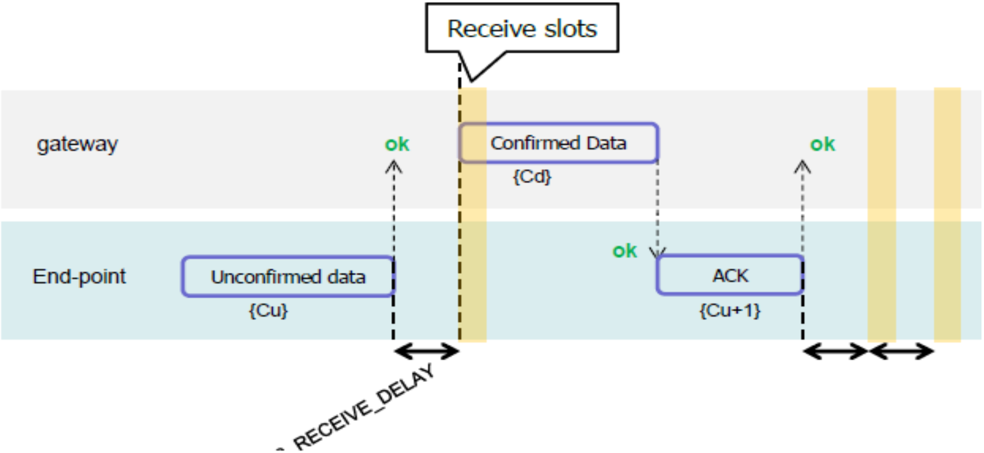
- Transmission is only one way at the time:

  - From End-Device to Gateway, and optionally
  - From Gateway to End-Device, and optionally
  - From End-Device to Gateway

→ thus not full duplex

LoRaWAN– confirmed messages





Uplink
(end-point to gateway)

Downlink
(gateway to end-point)

LoRaWAN - Confirmed messages

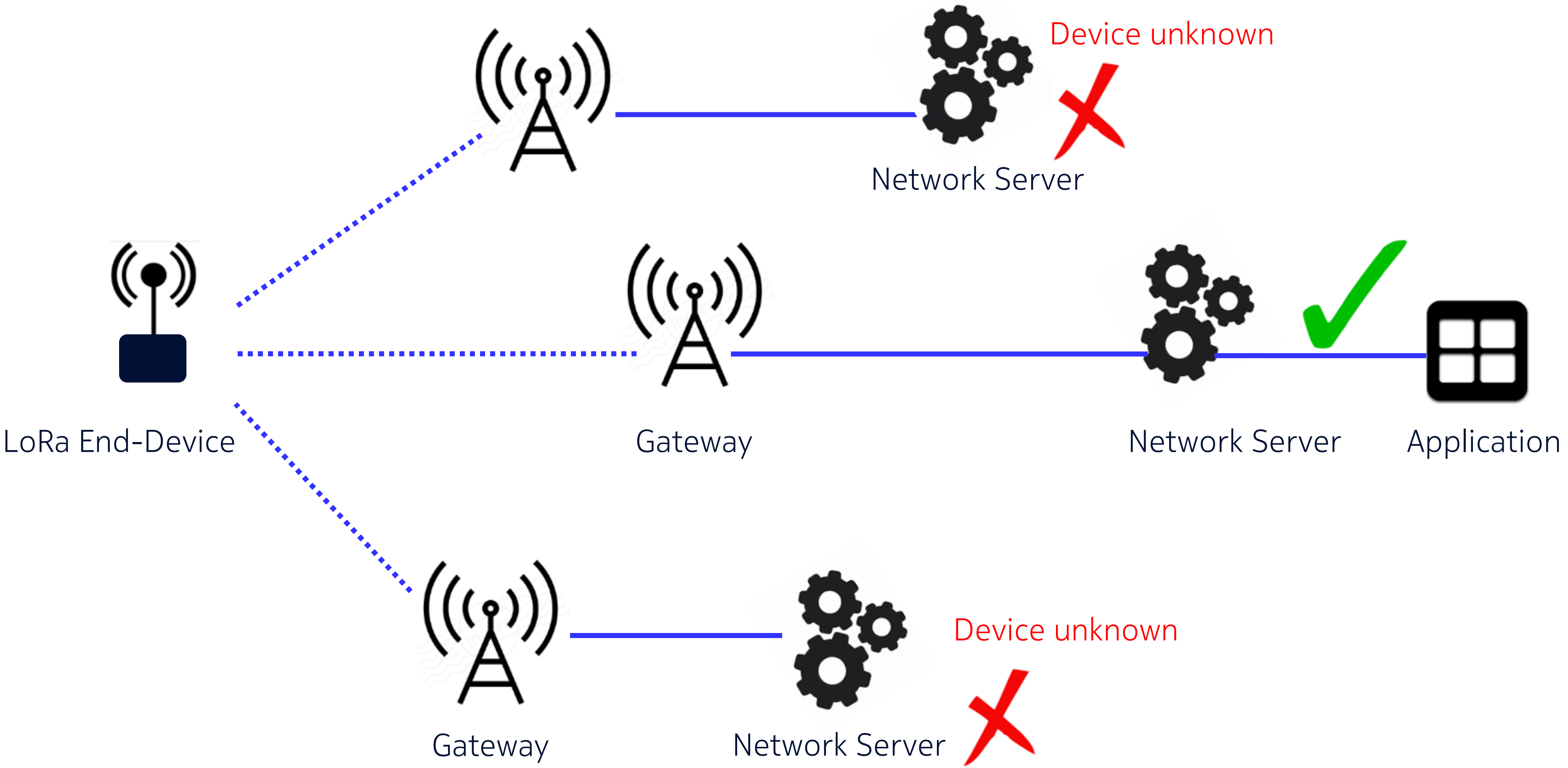
For Class A devices, radio communication is always initiated from the sensor.
Using Confirmed communication, the gateway has a chance to acknowledge the correct reception of the sensor data and also to send data to the sensor.

In this diagram, the ACK for the first packet Data0 is not received. The sensor re-transmits the packet. After reception of the ACK, the sensor listens for the Data packet from the gateway.

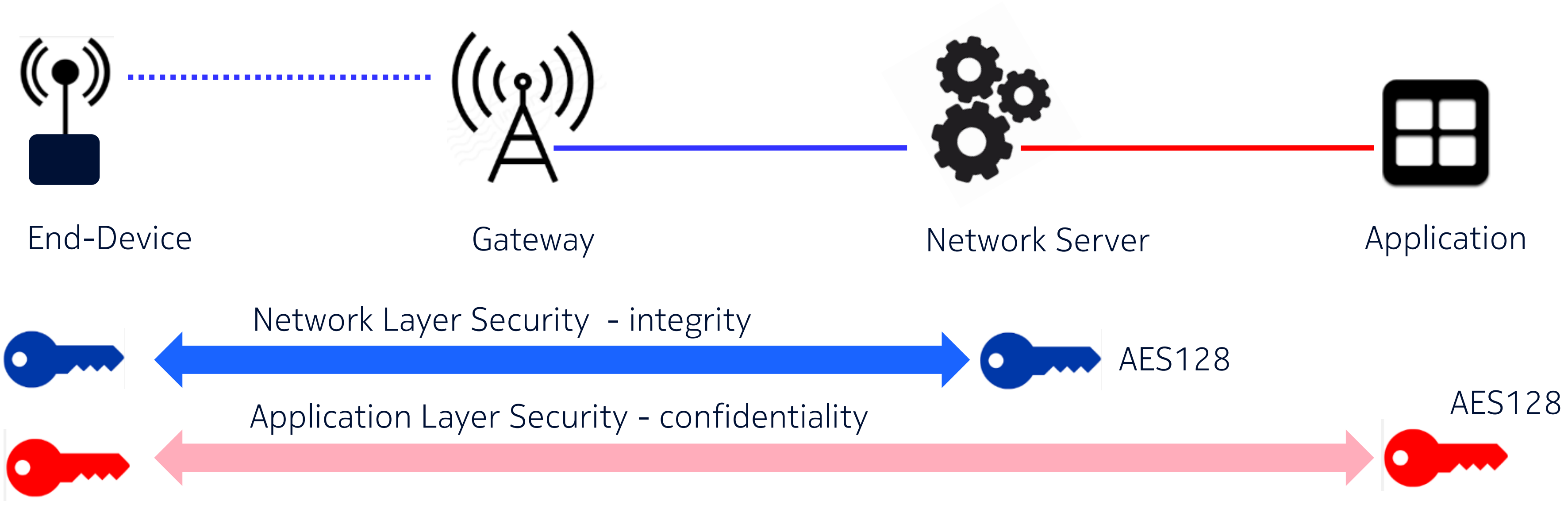
In LoRaWAN for 868 MHz ISM band,

receive_delay1 = 1 s
receive_delay2 = 2 s (must be receive_delay1 + 1 s)
join_accept_delay1 = 5 s
join_accept_delay2 = 6 s
adr_ack_limit = 64
adr_ack_delay = 32
ack_timeout = 2 ± 1 s (so 1 … 3 seconds, randomly)

The LoRa signal can be received by multiple gateways at the same time



Security Implementation



End-Device

Gateway

Network Server

Application

Network Layer Security - integrity

AES128

Application Layer Security - confidentiality

AES128

Two keys to be defined in the LoRa End-Device

- **NwkSkey**
- **AppSkey**

One key to be defined in the Network Server

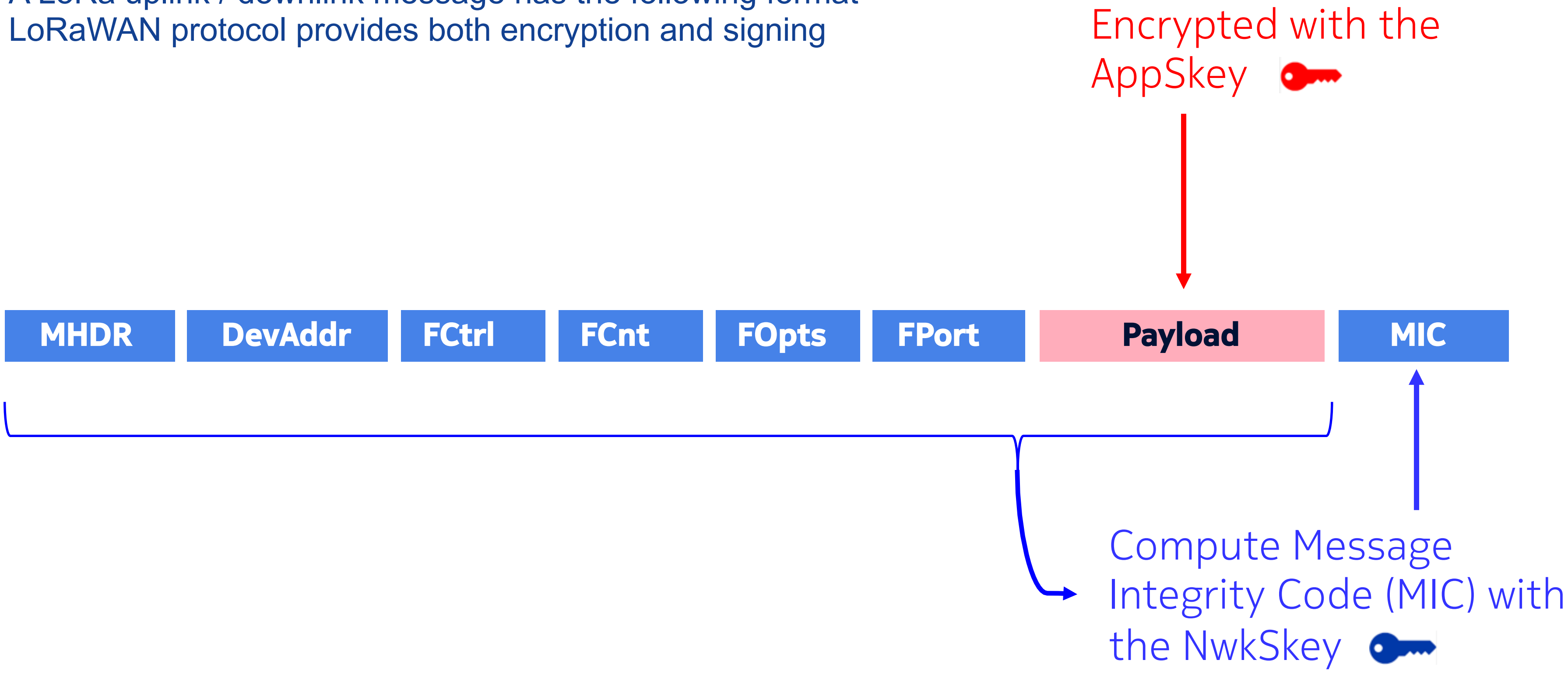
- **NwkSkey**

One key to be defined in the application

- **AppSkey**

Security – LoRa message format

A LoRa uplink / downlink message has the following format
LoRaWAN protocol provides both encryption and signing


Encrypted with the AppSkey
MHDR
DevAddr
FCtrl
FCnt
FOpts
FPort
Payload
MIC
Compute Message Integrity Code (MIC) with the NwkSkey

MIC is the integrity code for the whole packet, including the Payload

Security – Joining a End-Device to a LoRa network

- Activation by Personalization - ABP

- Over-the-Air-Activation - OTAA

Security – Activation by Personalization (ABP)

When the Activation by Personalization then:

The End-Devices are shipped / configured with the attributes:

- DevAddr (32 bits)
- AppSkey (128 bits)
- NwkSKey (128 bits)

No join message sequence over the Radio network is required, the End-Device can communicate with the Network Server and the Application Server immediately.

This ABP method is also the *weakness*, the AppSkey and NwkSKey are hard-coded in the device.

Note: When you buy a End-Device, you can configure the values with a serial interface and an application such as YAT.

Security – Over the Air Activation (OTAA)

Each End-Device is deployed with a unique 128 bit app key (AppKey) used when the End-Device sends a Join-Request.

The message is not encrypted but signed using the AppKey (integrity)
Only the AppEUI, DevEUI, DevNonce and MIC parameters are sent over the air.

AppKey = Unique value in End-Device (128b)	`3A 67 B4 92 C4 62 E0 F7 4C 52 0A 37 30 CF EA 34`
AppEUI = Application Identifier (64b)	`70 B3 D5 7E D0 00 04 A7`
DevEUI = End-Device Identifier (64b)	`00 00 00 00 EE 22 D9 17`
DevNonce = random value (16b)	`26 83`
MIC = Message integrity code (32b)	`aes128_cmac( AppKey | AppEUI | DevEui | DevNonce )`

The server will check the values and re-calculate the MIC with the AppKey. If valid the server will calculate the AppSkey and NwkSkey. The Server will respond with a Join-Accept with the following parameters:

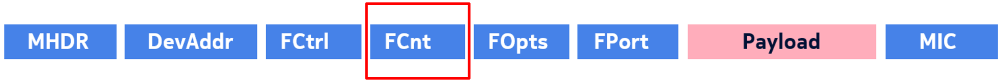
AppNonce	Generated locally on the server (24b)
NetID	Network Identity (24b)
DevAddr	End Device address (32b)
RxDelay	Configuration: Data for RF delays (8b)
CFList	Configuration: Channels to use (128b)

Encrypted using AppKey
The Network Server actually uses a decrypt operation to encrypt the Join-Accept message. The End-Device only requires an ‘encrypt’ implementation.

The End-Device calculates the AppSkey and NwkSkey using the AppNonce

Security – Additional countermeasures

To protect the LoRaWAN network from received messages being re-played and causes re-play attacks.



MHDR	DevAddr	FCtrl	FCnt	FOpts	FPort	Payload	MIC

Re-Play attacks can be detected and blocked using frame counters.

When a device is activated both the FCntUp and the FCntDown are set to 0.

Every time the device transmits an uplink message, the FCntUp is incremented, likewise for the FCcntDown when the Network Server transmits.

If either the End-Device or the Network Server receives a message with a frame counter lower than the last one, the message is ignored.

LoRa in practice

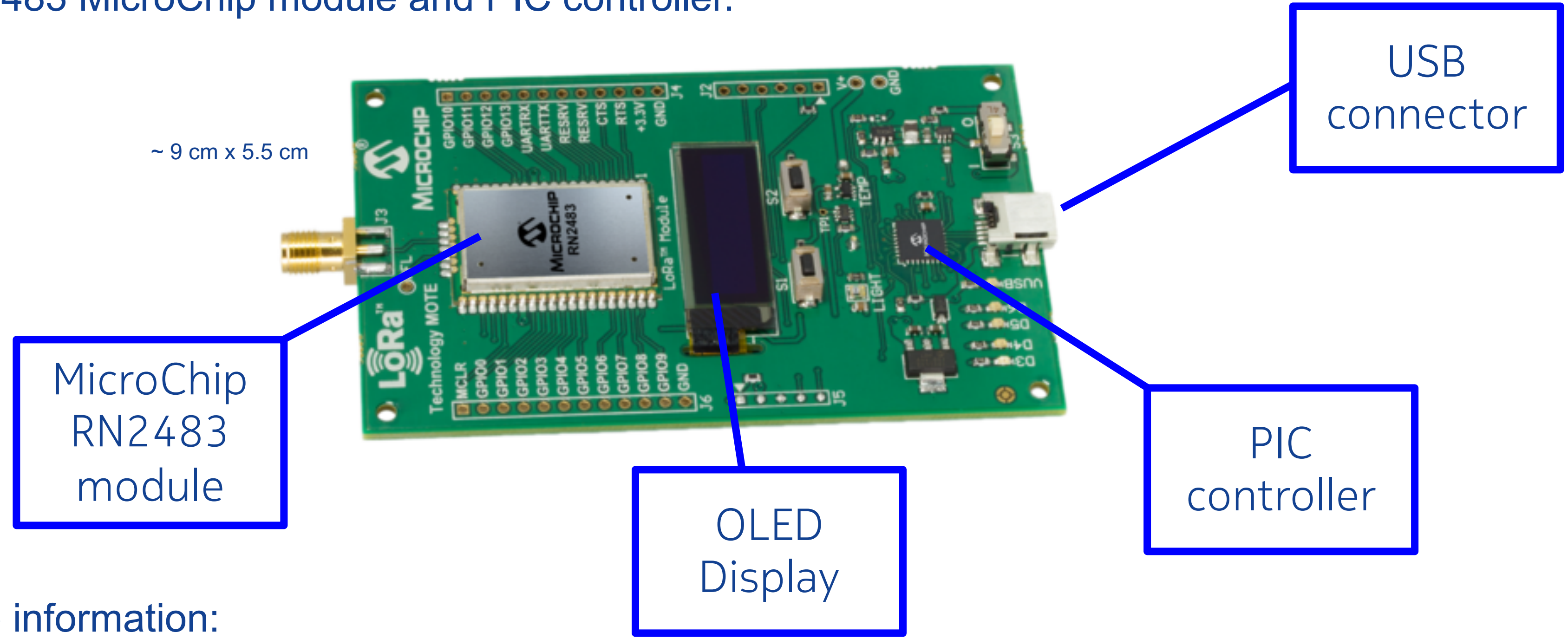
Now we understand the theory,

let’s see what LoRa can do in practice

The LoRa End-Device – How does it look like

868MHz RN2483 LoRa(TM) Technology Mote Based on the RN2483 MicroChip module and PIC controller.

~ 9 cm x 5.5 cm



USB connector

MicroChip RN2483 module

OLED Display

PIC controller

More information:

http://www.microchip.com/DevelopmentTools/ProductDetails.aspx?PartNO=dm164138

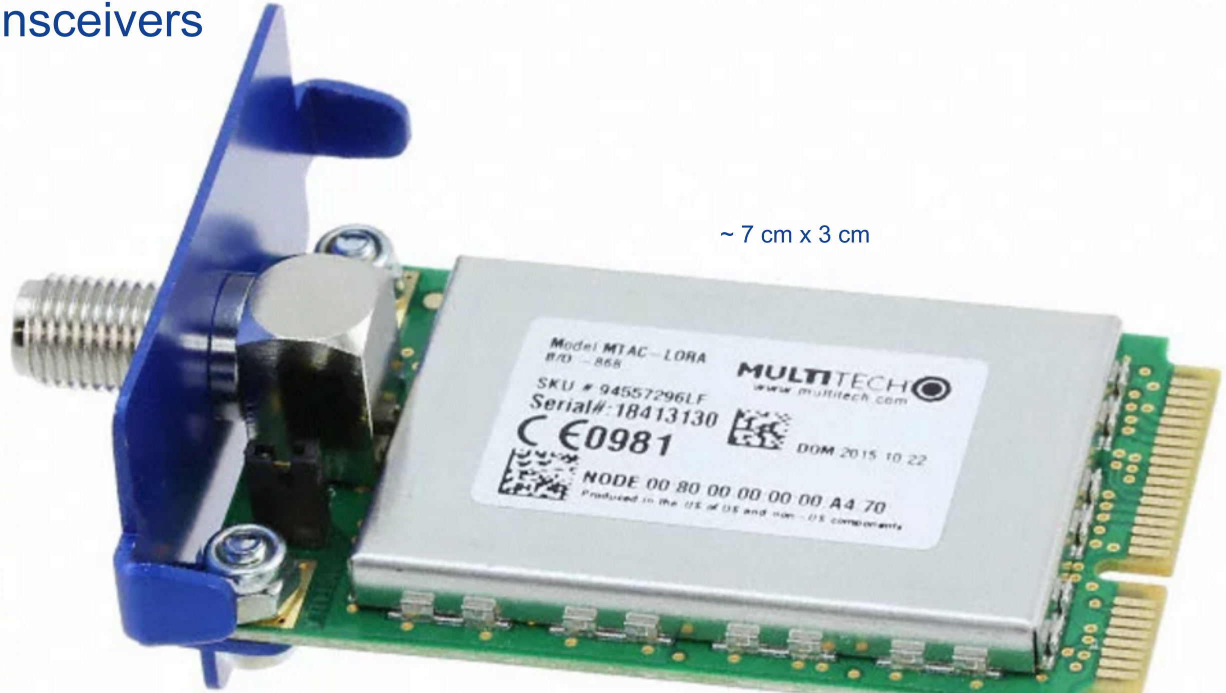
Costs: 60 Euro

The LoRa Gateway – How does it look like

Based on Multitech mCard-LORA, containing:

- 1x Semtech SX1301 Concentrator and
- 2x Semtech SX1257 I/Q Transceivers
- USB/SPI interface

Costs: 200 Euro



~ 7 cm x 3 cm

More information:

https://github.com/mirakonta/lora_gateway/wiki

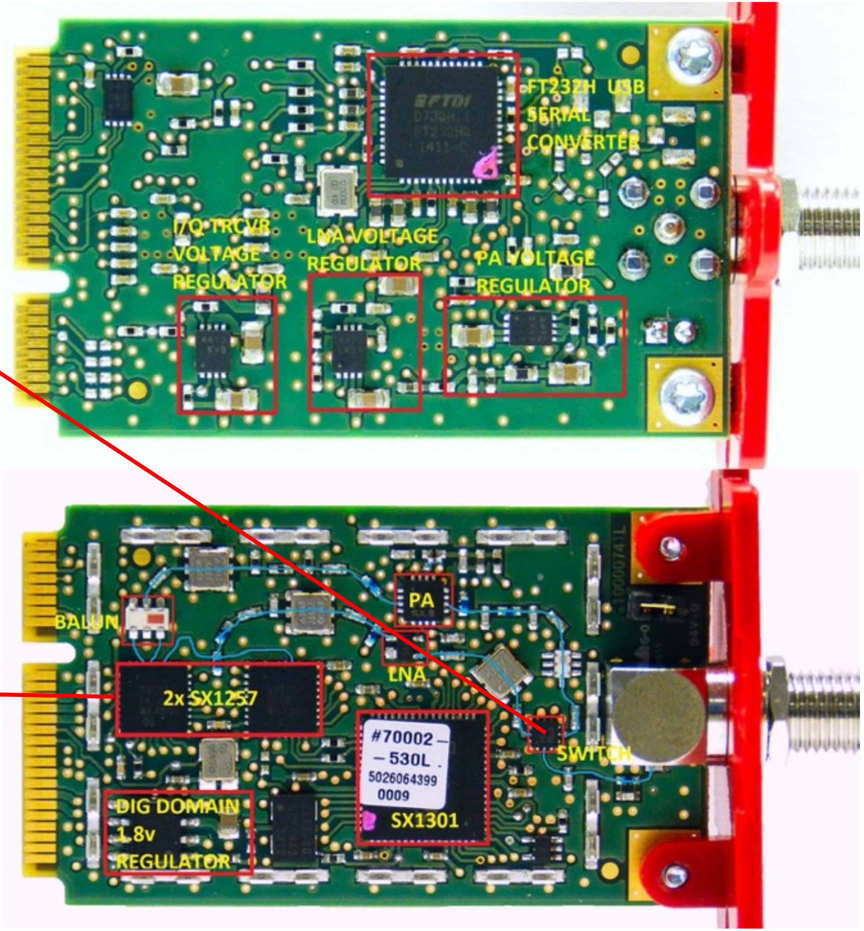
http://www.digikey.com/product-detail/en/MTAC-LORA-868/881-1243-ND/5322991

LoRa Gateway – a closer look

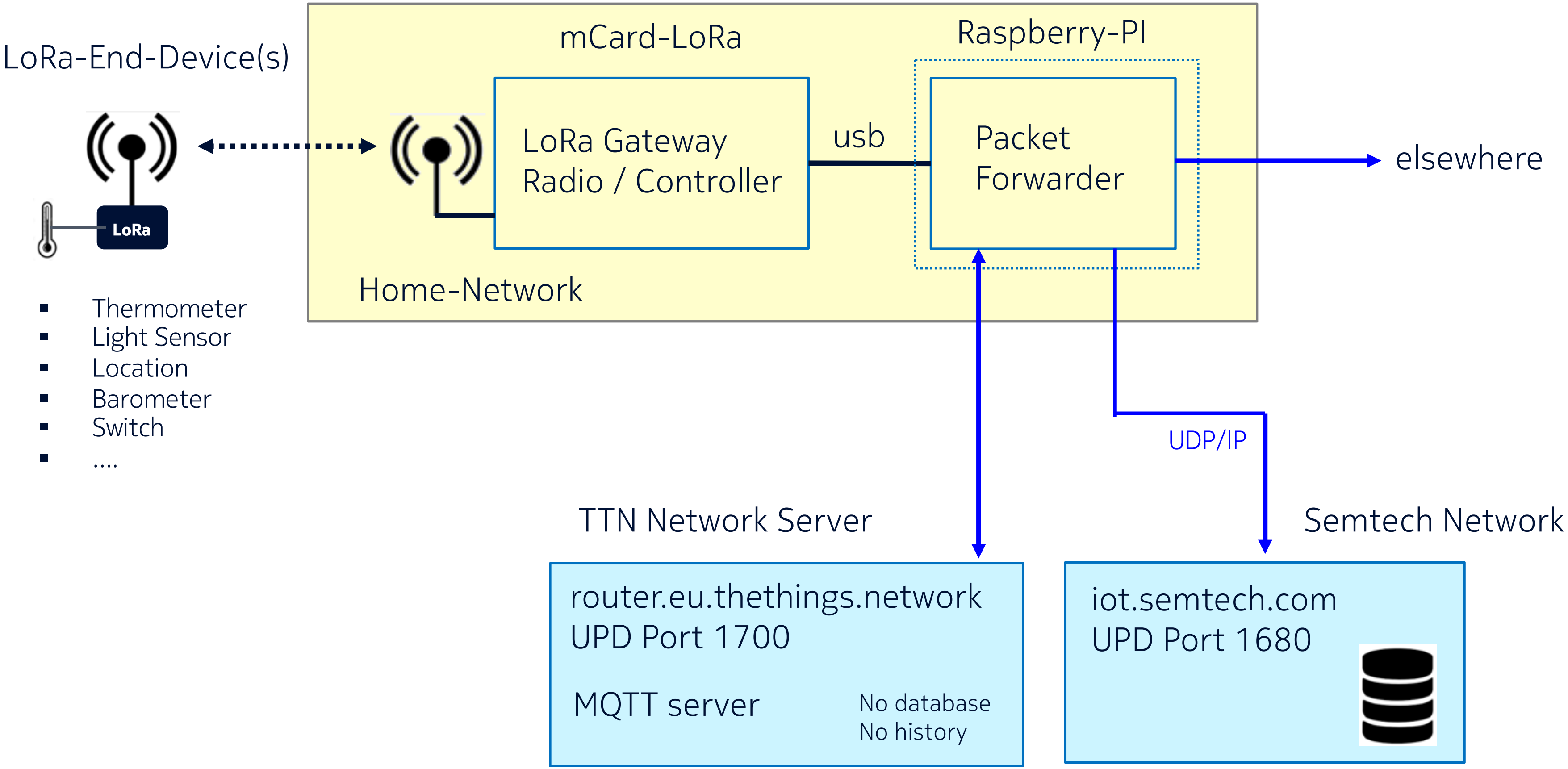
Tx/Rx switch prevents transmit power from PA to destroy sensitive LNA receiver.

As a result, only half-duplex is possible.

Because of the transceiver constraints and the required 868 MHz frequency band coverage, two transceivers are needed.


FT232H USB SERIAL CONVERTER
I/Q TRCVR VOLTAGE REGULATOR
LNA VOLTAGE REGULATOR
PA VOLTAGE REGULATOR
BALUN
PA
LNA
2x SX1257
SWITCH
DIG DOMAIN 1.8v REGULATOR
SX1301

Our setup to perform experiments (1)



LoRa-End-Device(s)

mCard-LoRa

Raspberry-PI

LoRa Gateway Radio / Controller

usb

Packet Forwarder

elsewhere

Home-Network

UDP/IP

TTN Network Server

Semtech Network

router.eu.thethings.network
UPD Port 1700

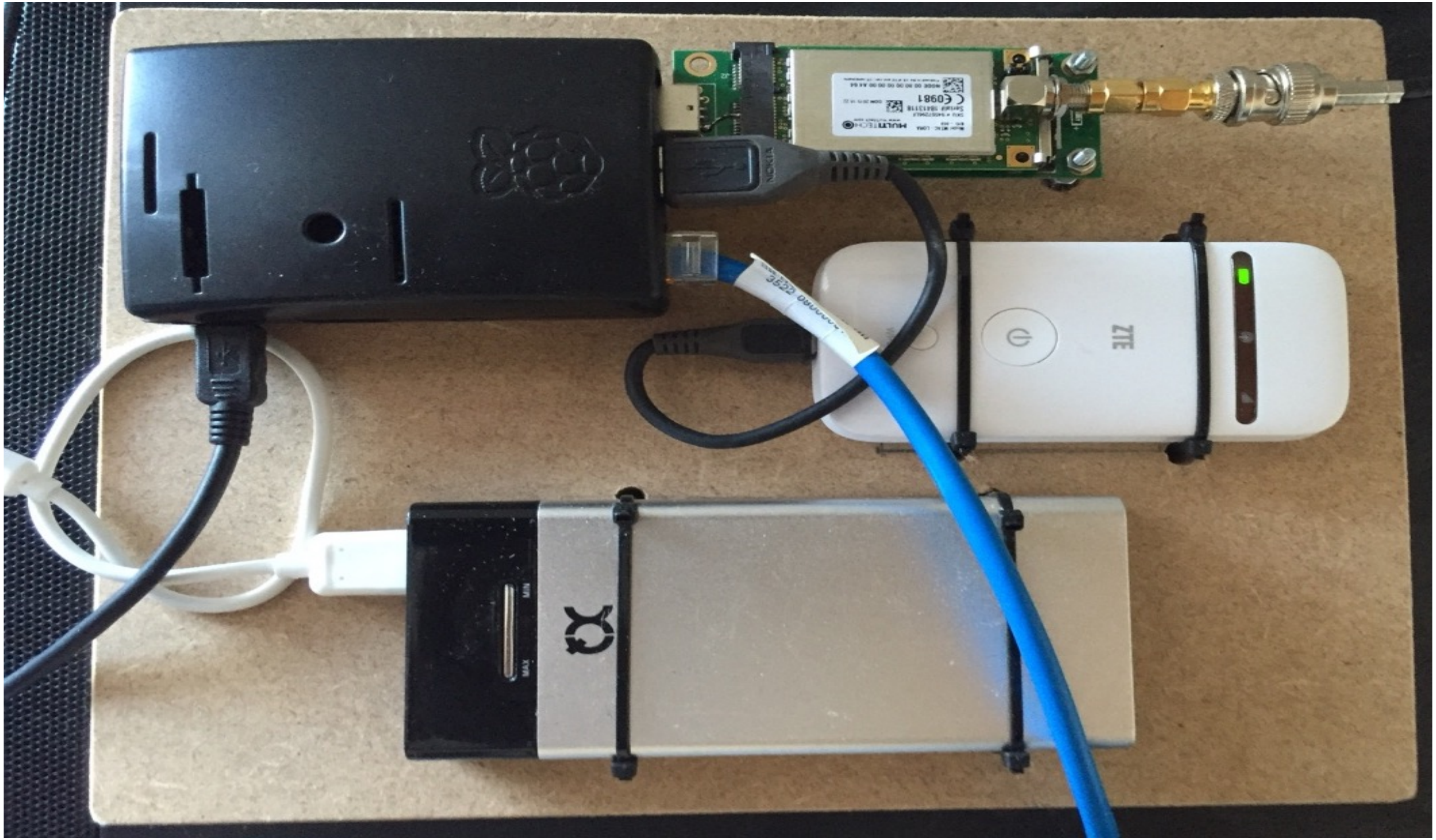
MQTT server

No database
No history

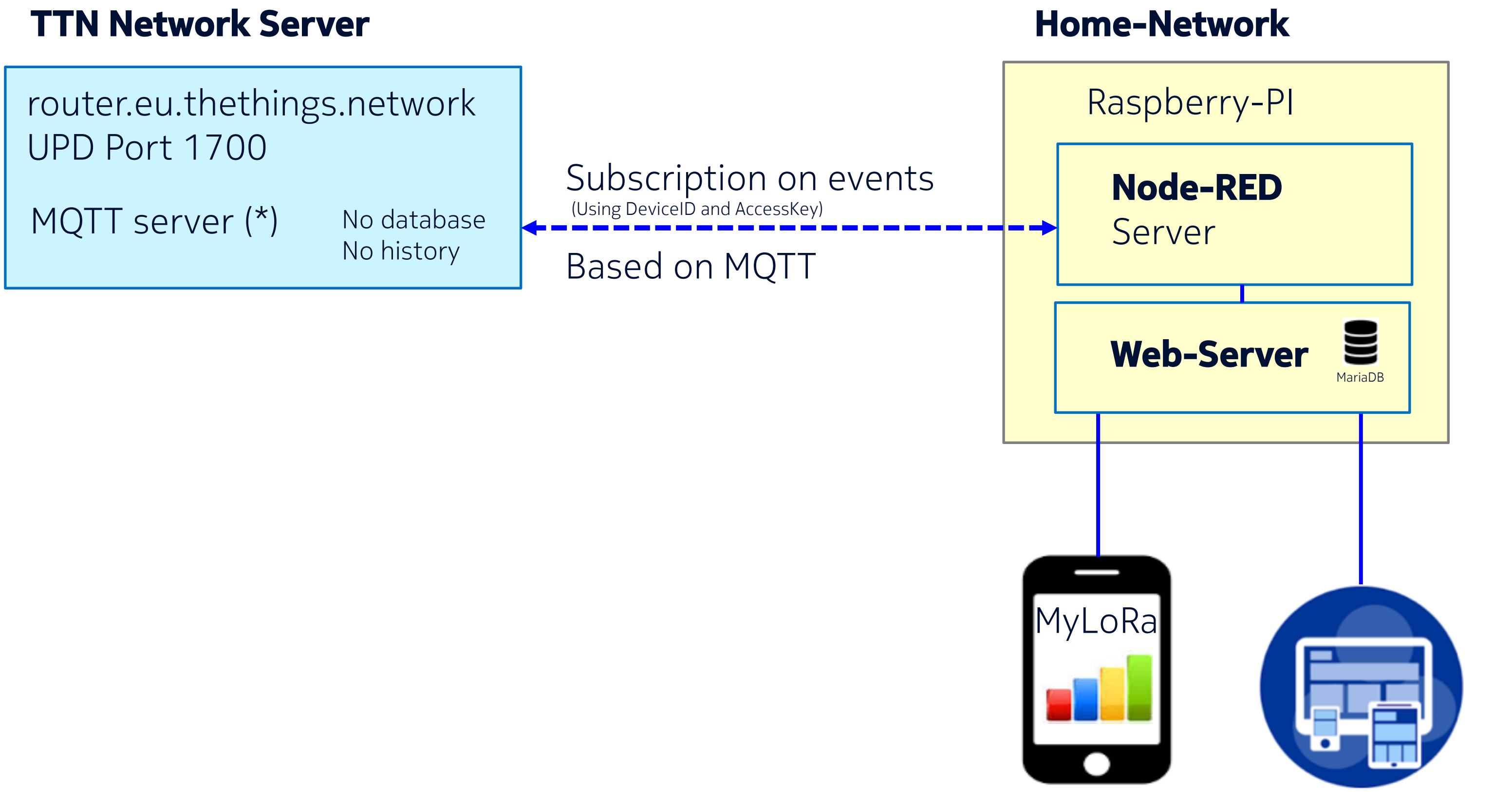
iot.semtech.com
UPD Port 1680

- Thermometer
- Light Sensor
- Location
- Barometer
- Switch
- ....

The LoRa Gateway – How does it look like



Our setup to perform experiments (2)



TTN Network Server

router.eu.thethings.network
UPD Port 1700

MQTT server (*)

No database
No history

Subscription on events
(Using DeviceID and AccessKey)

Based on MQTT

Home-Network

Raspberry-PI

Node-RED
Server

Web-Server

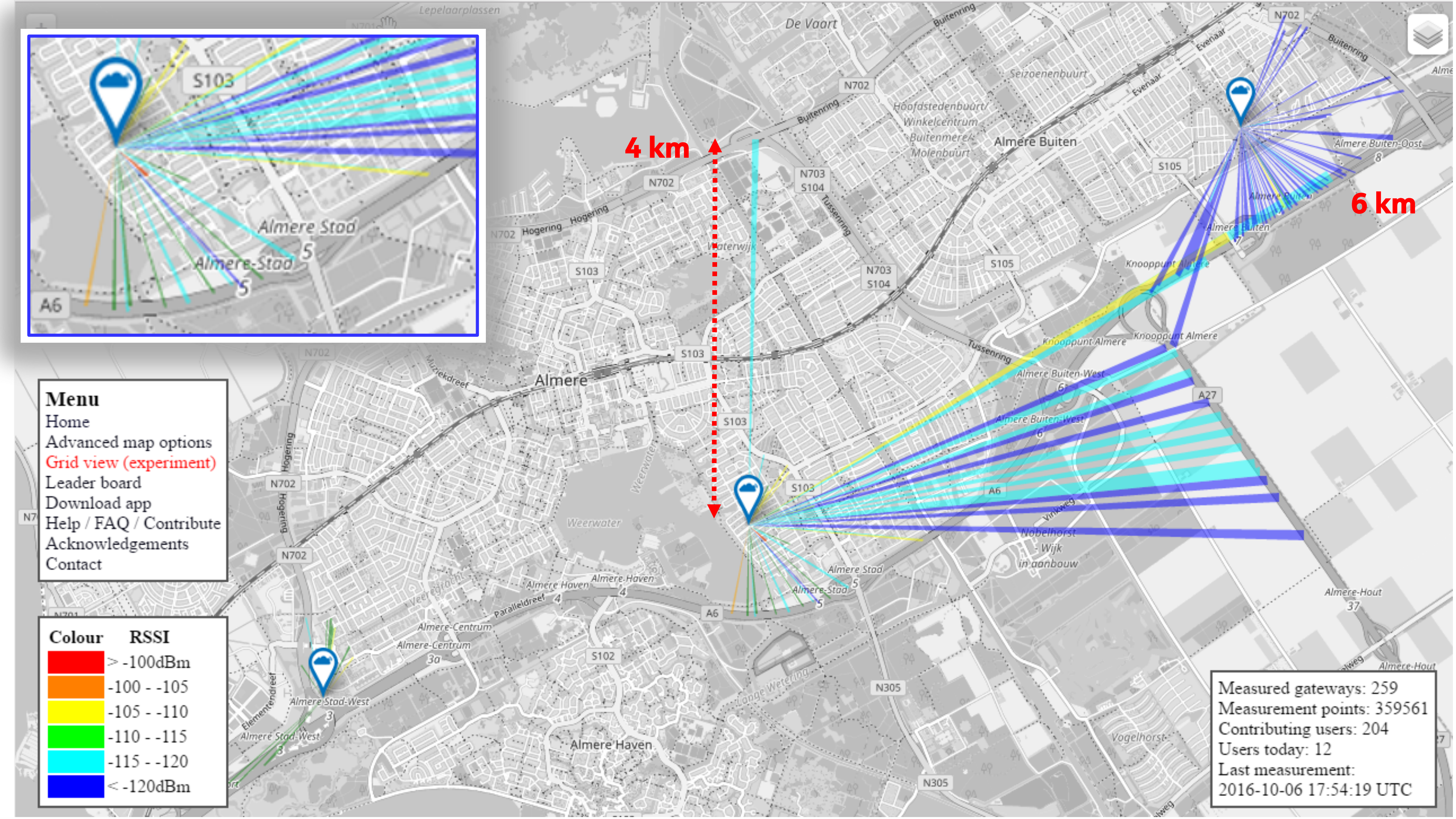
MariaDB

MyLoRa

Mobile Application

Web Application

* MQTT: Message Queuing Telemetry Transport

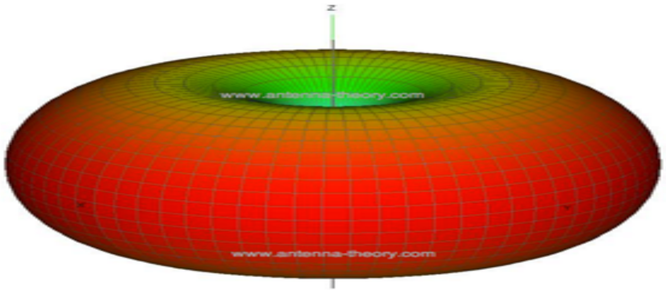


Colour	RSSI
🟥	> -100dBm
🟧	-100 - -105
🟨	-105 - -110
🟩	-110 - -115
🟦	-115 - -120
🟦	< -120dBm

Measured gateways: 259
Measurement points: 359561
Contributing users: 204
Users today: 12
Last measurement:
2016-10-06 17:54:19 UTC

Antenna considerations

The recommended gateway antenna is a ground plane antenna (omni-directional)
For example the Aurel 650200599



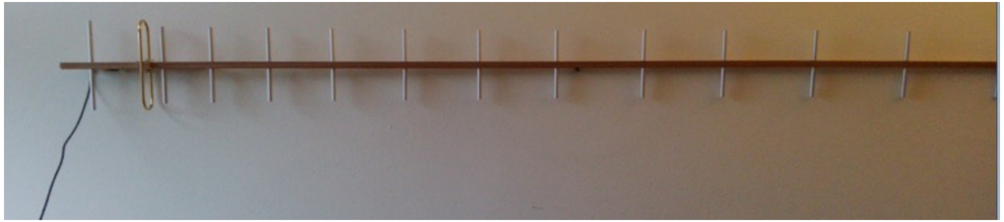
Gain: about 4 dBi (10^0.4 = 2.5x)

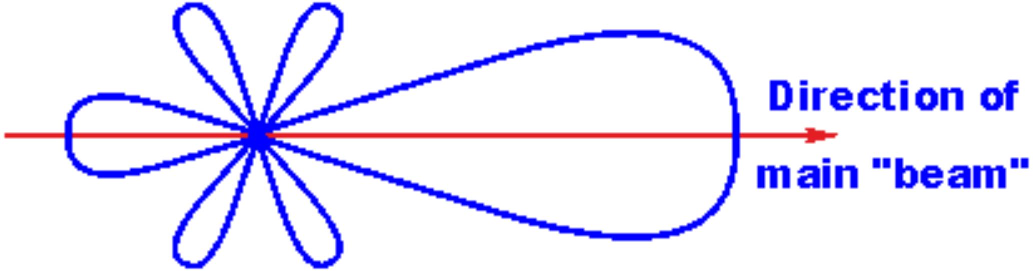
Costs: 35 Euro (conrad.nl), including 2.5 m RG58MIL coax cable
Cable has F-connector at antenna side and BNC connector at Gateway side.

Antenna considerations

Alternatively you can also make your own antenna…

Yagi, highly directional





Build instructions:
VK5DJ's Yagi Calculator
http://www.vk5dj.com/yagi.html

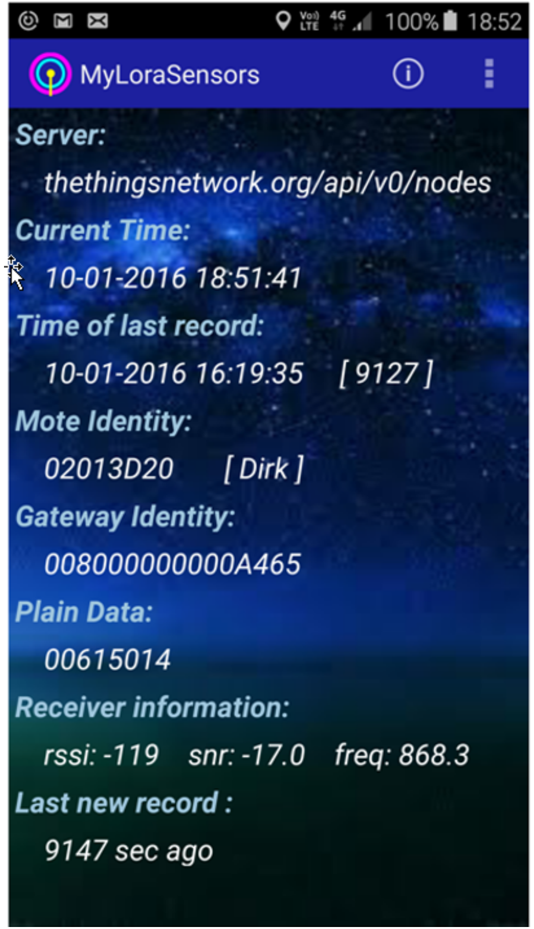
Costs: 7 Euro

Gain: 14.2 dBi (10^1.42 = 25x)
Can save energy because the radiated power can be lower

Antenna considerations

- Place the antenna as high as possible to improve the line of sight
- Place the antenna vertically polarized
- Avoid metal obstacles nearby since it will absorb radio-energy
- Make use of high quality HF cable
- The gateway impedance is 50 Ω, do not connect another impedance or you will get a bad SWR.
- Keep the cable as short as possible to avoid loss.
- Consider to mount the gateway device as close as possible to the antenna and transport the data via a USB cable to the packet-forwarder server or use UTP cable from server to internet, PoE is an option.

An Android App showing End-Device data



Server:

thethingsnetwork.org/api/v0/nodes

Current Time:

10-01-2016 18:51:41

Time of last record:

10-01-2016 16:19:35 [9127]

Mote Identity:

02013D20 [Dirk]

Gateway Identity:

008000000000A465

Plain Data:

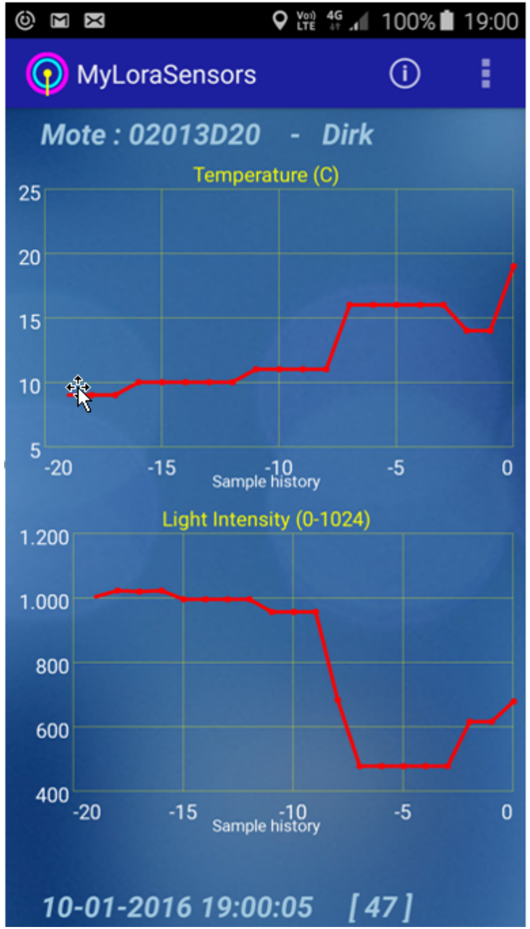
00615014

Receiver information:

rssi: -119 snr: -17.0 freq: 868.3

Last new record :

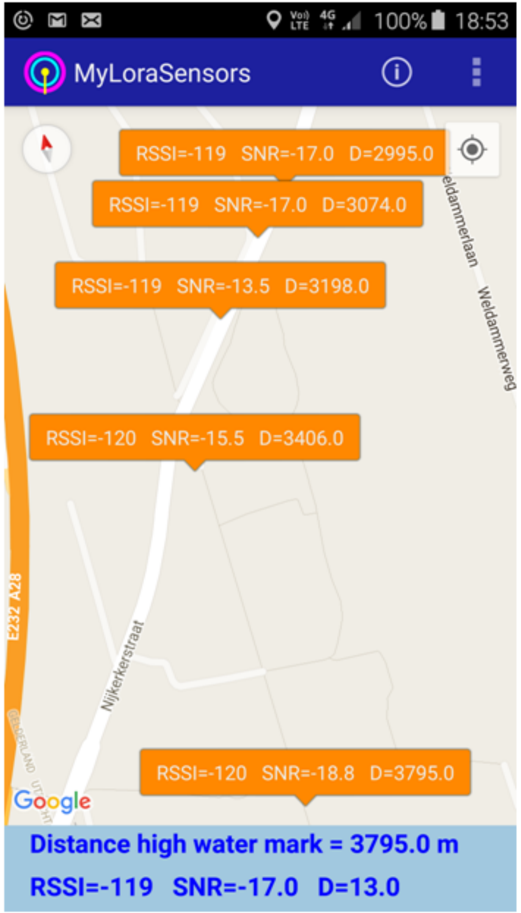
9147 sec ago



Mote : 02013D20 - Dirk

10-01-2016 19:00:05 [47]

An Android App showing End-Device data



RSSI=-119 SNR=-17.0 D=2995.0

RSSI=-119 SNR=-17.0 D=3074.0

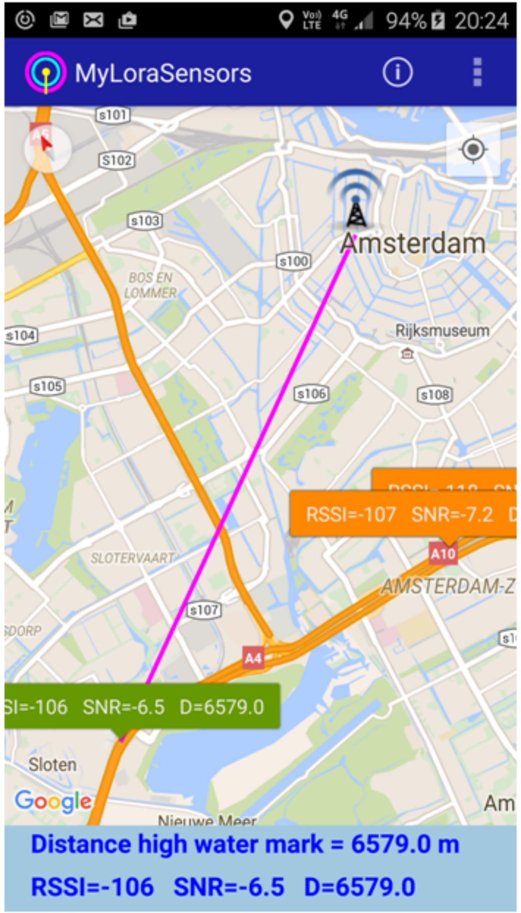
RSSI=-119 SNR=-13.5 D=3198.0

RSSI=-120 SNR=-15.5 D=3406.0

RSSI=-120 SNR=-18.8 D=3795.0

Distance high water mark = 3795.0 m

RSSI=-119 SNR=-17.0 D=13.0



RSSI=-107 SNR=-7.2 D

SI=-106 SNR=-6.5 D=6579.0

Distance high water mark = 6579.0 m

RSSI=-106 SNR=-6.5 D=6579.0

LoRa and LoRaWAN - Conclusion

- What have we learned:
  - What is LoRa Radio Modulation Technology
  - How can we build an IoT network using LoRaWAN
  - How we learn new technologies

- If you are as inspired as us, then go get your gear out and build your network for IoT

Thank you

LoRa and LoRaWAN – Demo Session

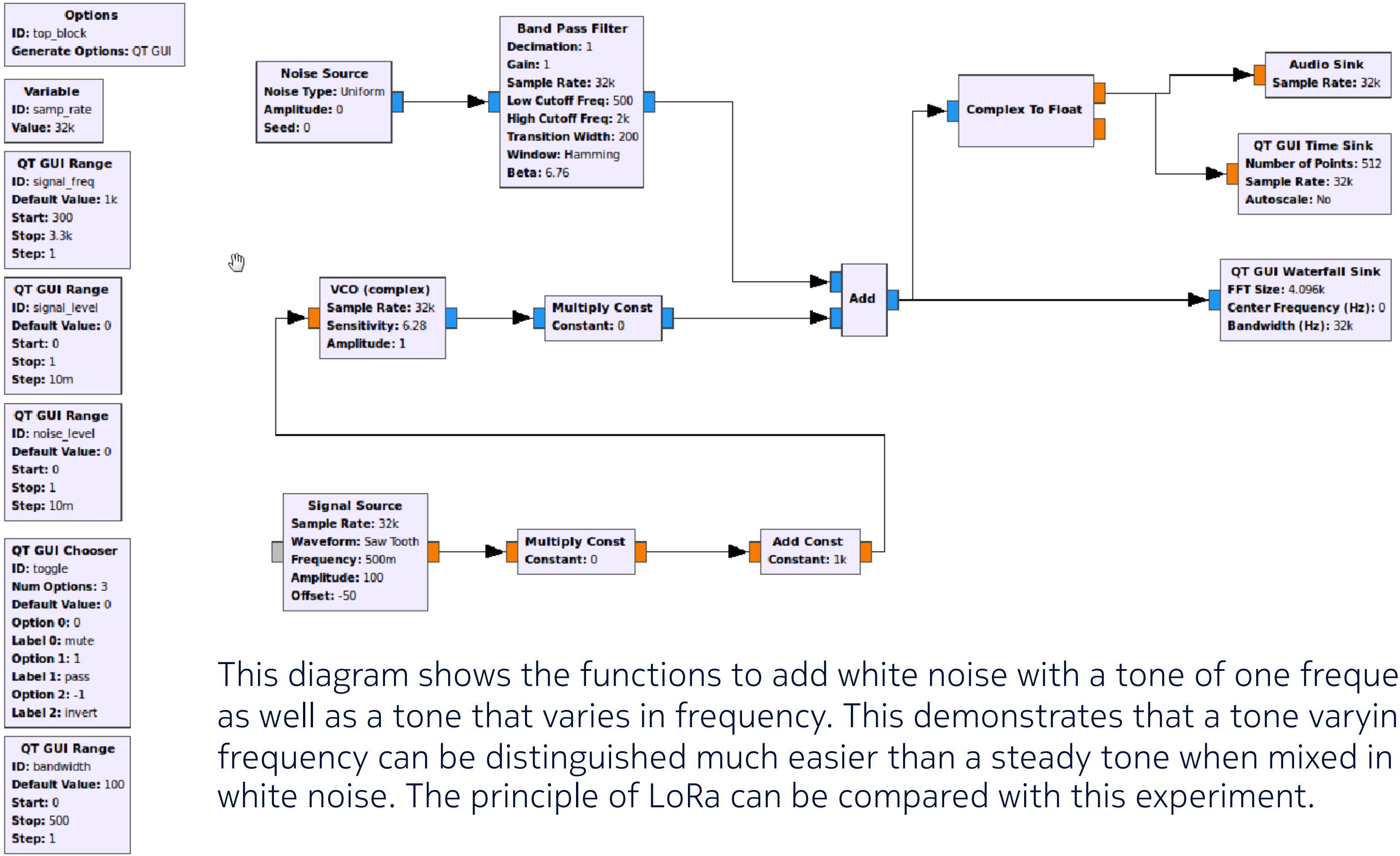
During the demo we show:

1. LoRa Radio made audible – a LoRa emulation by sound

2. Visualize LoRa Radio signals – using SDR dongle

3. LoRaWAN showcase – thermometer / light meter application

LoRa and LoRaWAN – Demo Session – LoRa Radio made audible



Options
ID: top_block
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 32k

QT GUI Range
ID: signal_freq
Default Value: 1k
Start: 300
Stop: 3.3k
Step: 1

QT GUI Range
ID: signal_level
Default Value: 0
Start: 0
Stop: 1
Step: 10m

QT GUI Range
ID: noise_level
Default Value: 0
Start: 0
Stop: 1
Step: 10m

QT GUI Chooser
ID: toggle
Num Options: 3
Default Value: 0
Option 0: 0
Label 0: mute
Option 1: 1
Label 1: pass
Option 2: -1
Label 2: invert

QT GUI Range
ID: bandwidth
Default Value: 100
Start: 0
Stop: 500
Step: 1

Noise Source
Noise Type: Uniform
Amplitude: 0
Seed: 0

Band Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 32k
Low Cutoff Freq: 500
High Cutoff Freq: 2k
Transition Width: 200
Window: Hamming
Beta: 6.76

VCO (complex)
Sample Rate: 32k
Sensitivity: 6.28
Amplitude: 1

Multiply Const
Constant: 0

Add

Complex To Float

Audio Sink
Sample Rate: 32k

QT GUI Time Sink
Number of Points: 512
Sample Rate: 32k
Autoscale: No

QT GUI Waterfall Sink
FFT Size: 4.096k
Center Frequency (Hz): 0
Bandwidth (Hz): 32k

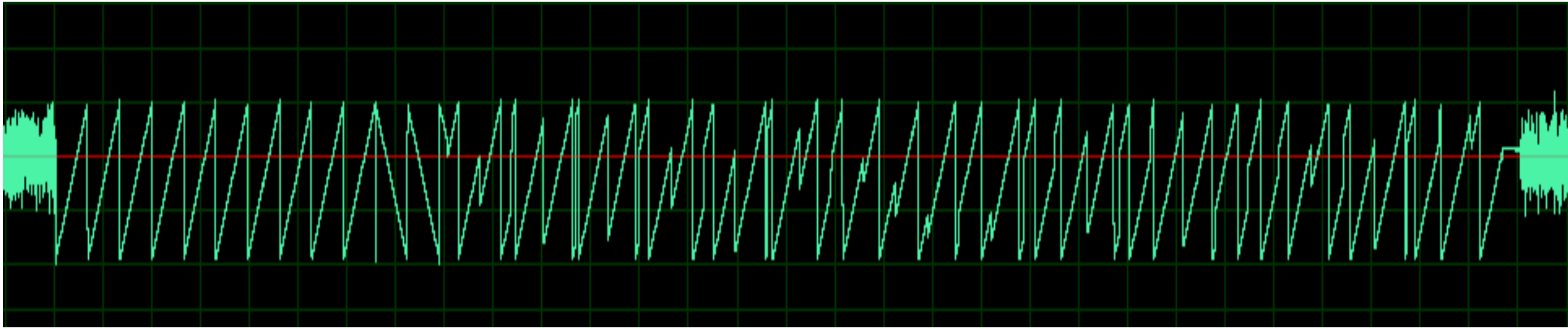
Signal Source
Sample Rate: 32k
Waveform: Saw Tooth
Frequency: 500m
Amplitude: 100
Offset: -50

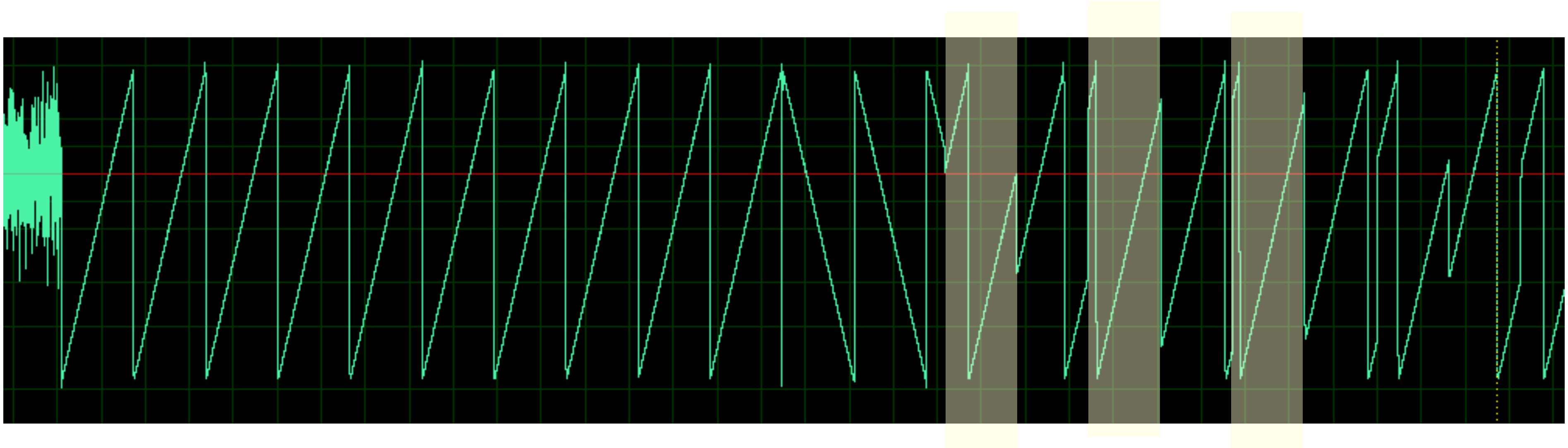
Multiply Const
Constant: 0

Add Const
Constant: 1k

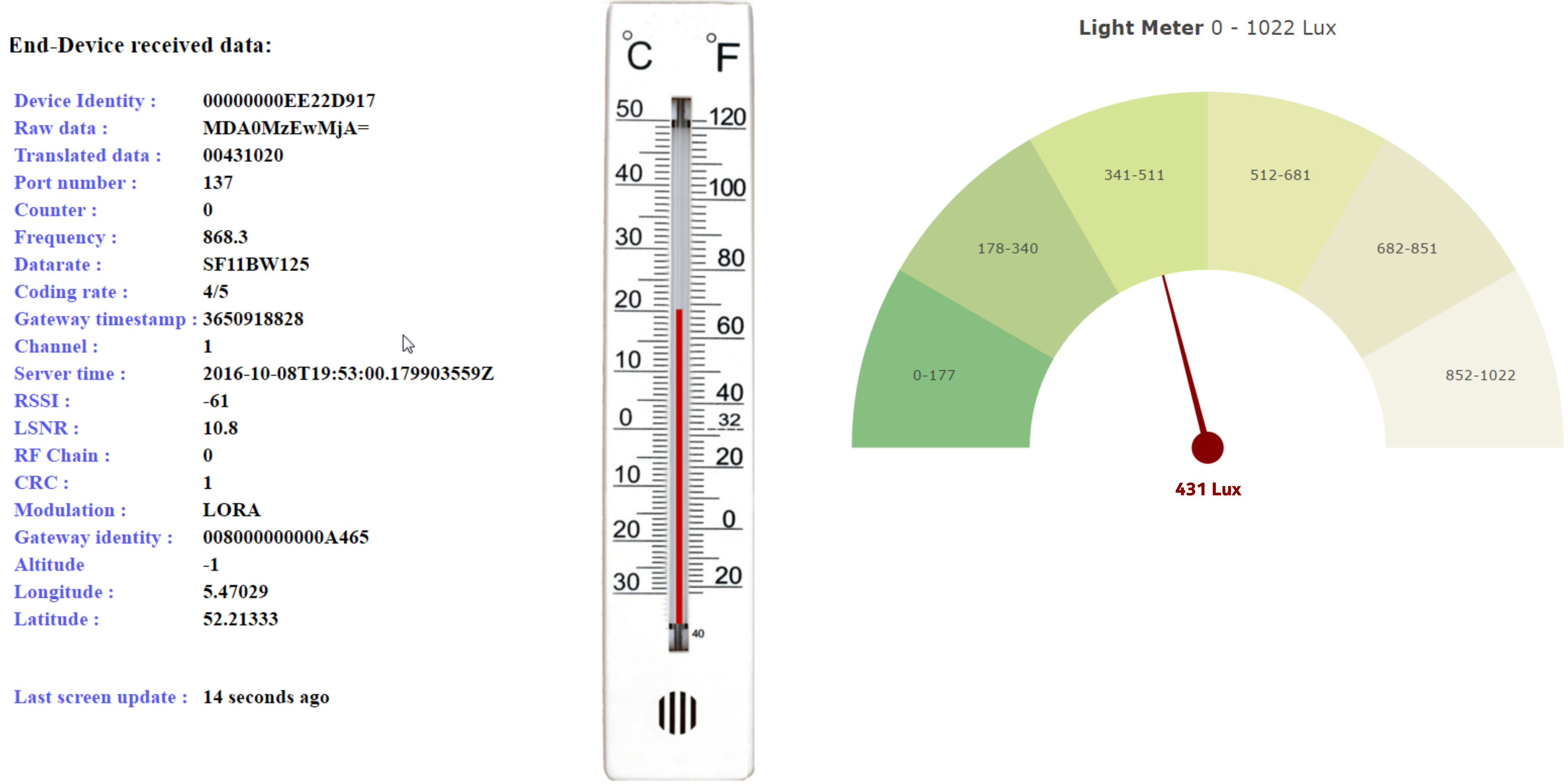
This diagram shows the functions to add white noise with a tone of one frequency as well as a tone that varies in frequency. This demonstrates that a tone varying in frequency can be distinguished much easier than a steady tone when mixed in white noise. The principle of LoRa can be compared with this experiment.

LoRa and LoRaWAN – Demo Session – Visualize LoRa Radio Signals





Website: myproxy.nl/lora shows the values of an End-Device



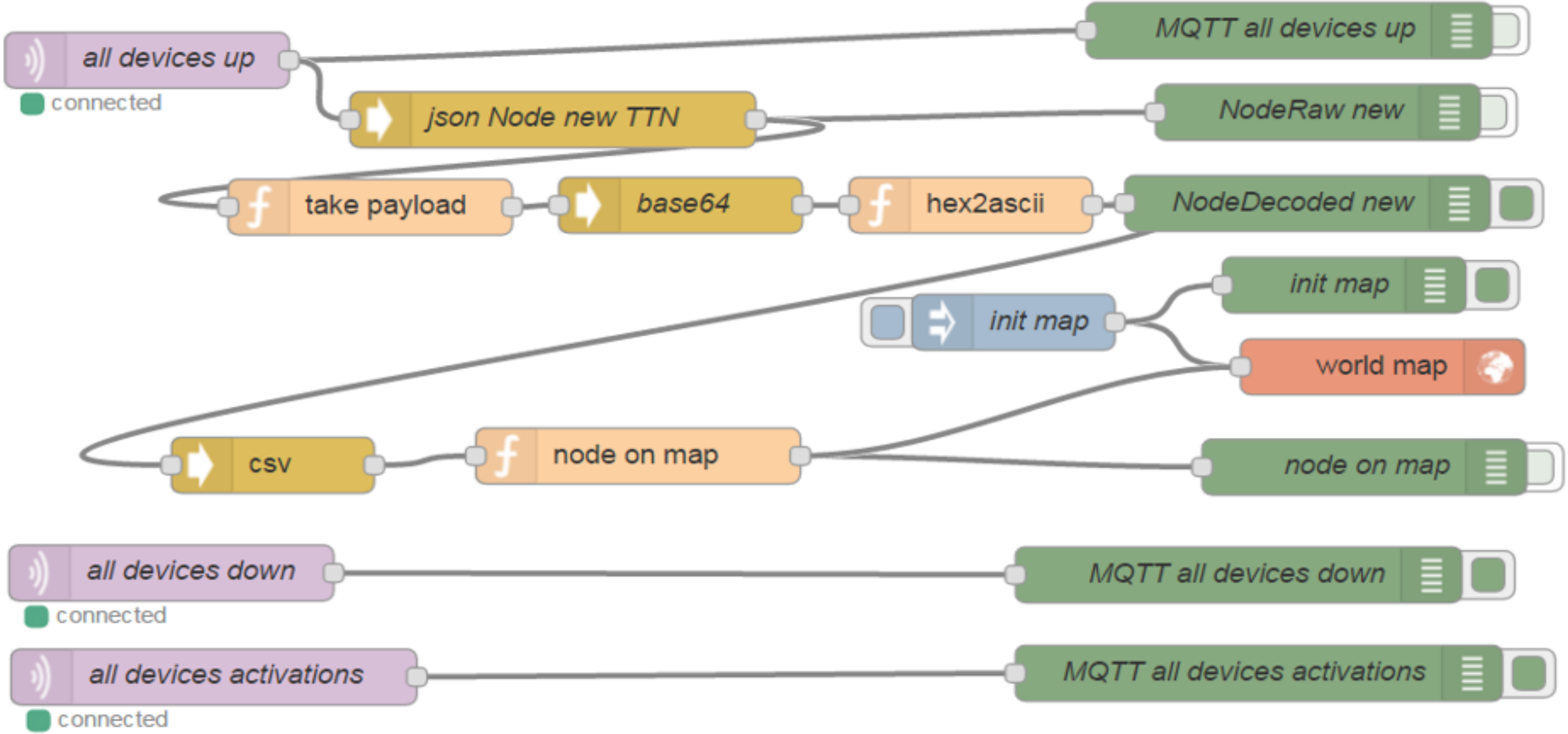
End-Device received data:

Device Identity :	00000000EE22D917
Raw data :	MDA0MzEwMjA=
Translated data :	00431020
Port number :	137
Counter :	0
Frequency :	868.3
Datarate :	SF11BW125
Coding rate :	4/5
Gateway timestamp :	3650918828
Channel :	1
Server time :	2016-10-08T19:53:00.179903559Z
RSSI :	-61
LSNR :	10.8
RF Chain :	0
CRC :	1
Modulation :	LORA
Gateway identity :	008000000000A465
Altitude	-1
Longitude :	5.47029
Latitude :	52.21333

Last screen update : 14 seconds ago

Node-RED - See http://node-red.org

Node-RED is a tool for wiring together hardware devices, APIs and online services in new and interesting ways. The below figure shows an interface example to show the sensor data received from the MQTT server.



References

Semtech

http://www.semtech.com/wireless-rf/internet-of-things/what_is_lora.html

LoRa Alliance

https://www.lora-alliance.org/What-Is-LoRa/Technology

MWR Labs Whitepaper

Independent analysis and guidance around security of LoRa and LoRaWAN - Robert Miller

Yagi Build instructions (VK5DJ's Yagi Calculator)

http://www.vk5dj.com/yagi.html