LoRa, LoRaWAN, and the challenges of long-range networking in shared spectrum

Cognitive Radio Platform NL, december 2015

Thomas Telkamp

Contents

- LPWAN
- LoRa modulation
- Hardware
- LoRaWAN protocol
- Deployment models
- Long-range networking in shared spectrum

LoRa, LoRaWAN, LPWAN…?

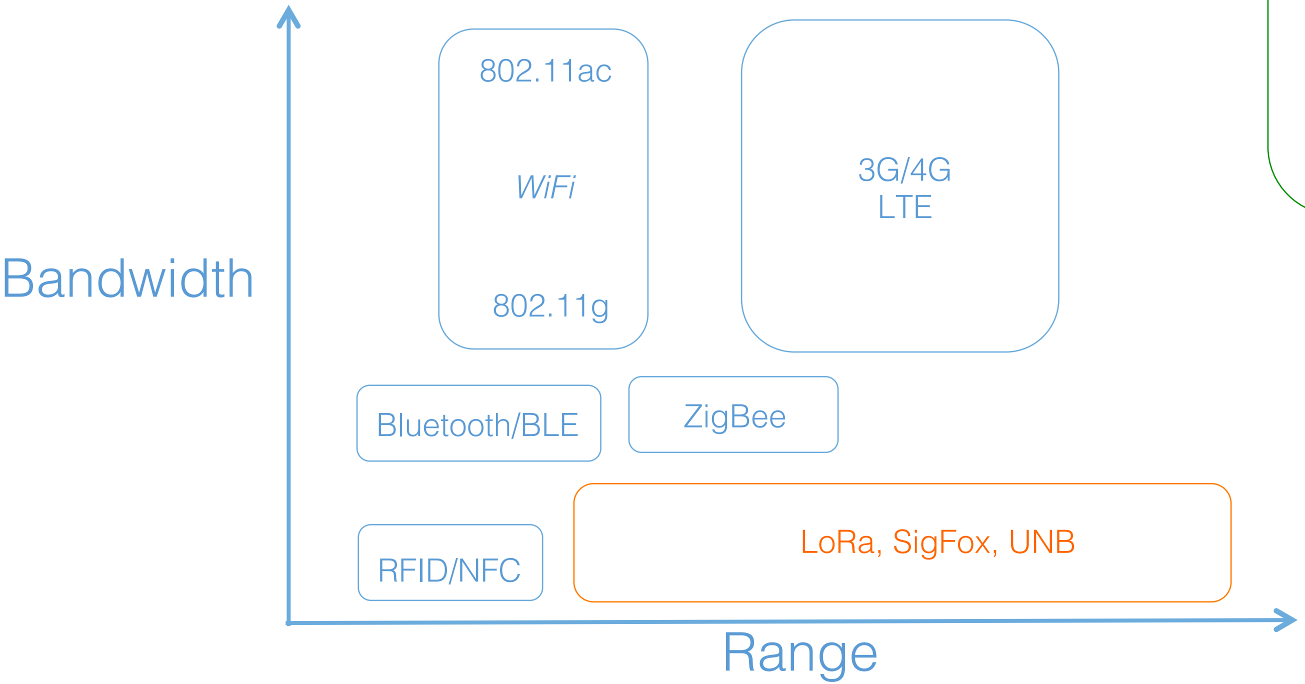
- LPWAN name for Low Power Wide-Area Network
  - a wireless wide area network technology that is specialized for interconnecting devices with low-bandwidth connectivity, focusing on range and power efficiency.
- Mostly unlicensed (but regulated) spectrum under 1 GHz (433, 868, 915 MHz)
- Multiple solutions, including:

SIGFOX

One network A billion dreams

LoRa™

Bandwidth vs Range



- Long Distance
- High Speed
- Low Power

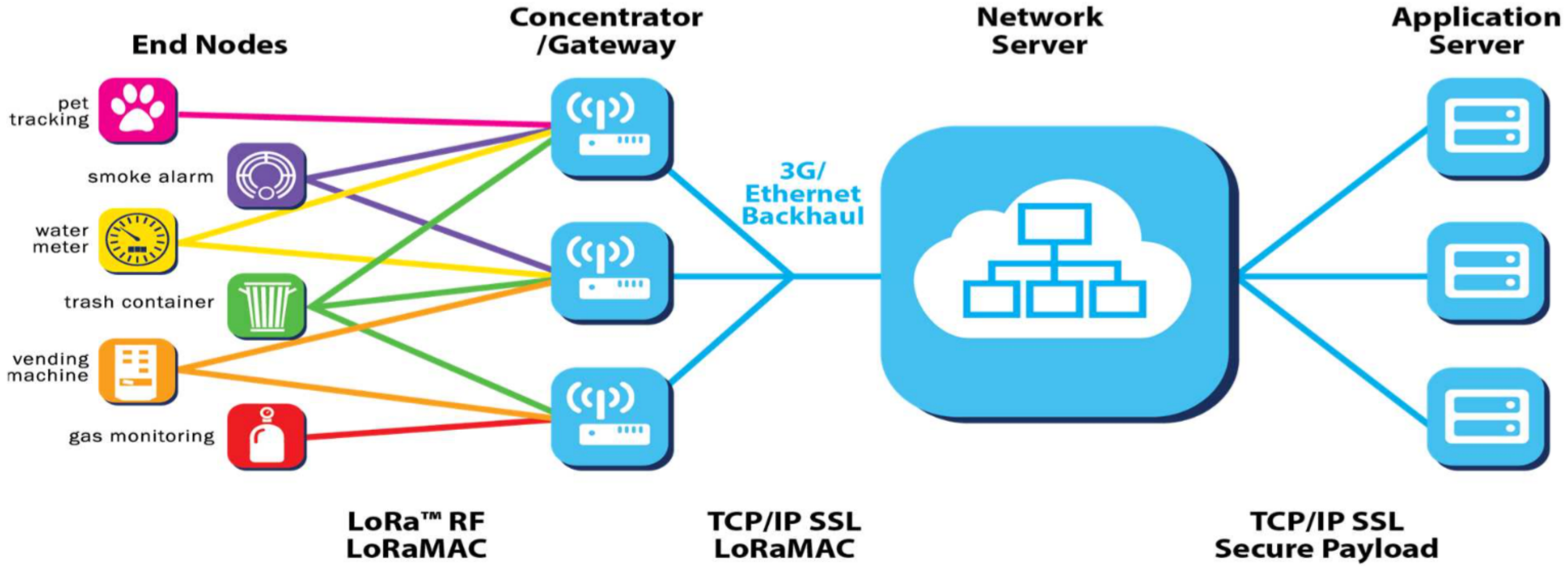
Pick 2…

What is LoRa?

- Wireless modulation technology
- Physical layer for long range communications
- Low bandwidth
- Low battery usage
- Operates in the license-free ISM bands all around the world
    - 433, 868, 915 Mhz
    - Regulated (power, duty-cycle, bandwidth)
    - EU: 0.1% or 1% per sub-band duty-cycle limitation (per hour)
- Sensitivity: -142 dBm
- Link budget (EU): 156 dB

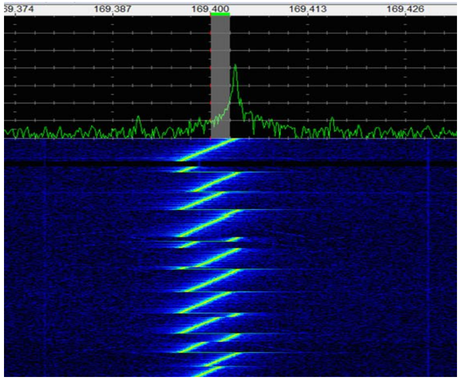
What is LoRaWAN?

- Communications protocol and architecture that utilizes the LoRa physical layer
- Data rates are defined that range from 300bps to 5.5kbps
  - with two high-speed channels at 11kbps and 50kbps (FSK modulation)
- Supports
  - secure bi-directional communication,
  - mobility
  - localization.

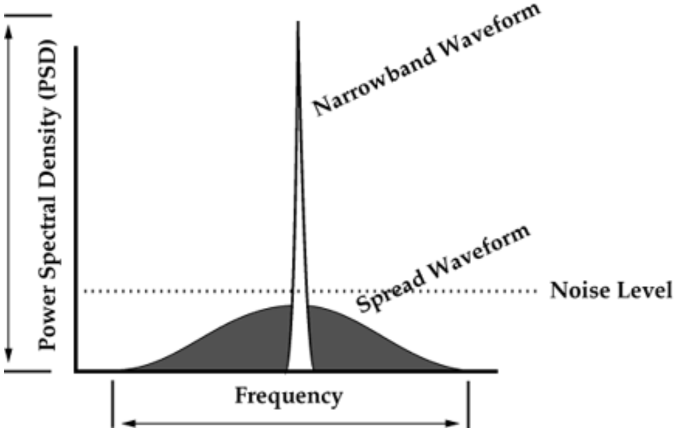

End Nodes
Concentrator /Gateway
Network Server
Application Server
pet tracking
smoke alarm
water meter
trash container
vending machine
gas monitoring
3G/ Ethernet Backhaul
LoRa™ RF
LoRaMAC
TCP/IP SSL
LoRaMAC
TCP/IP SSL
Secure Payload

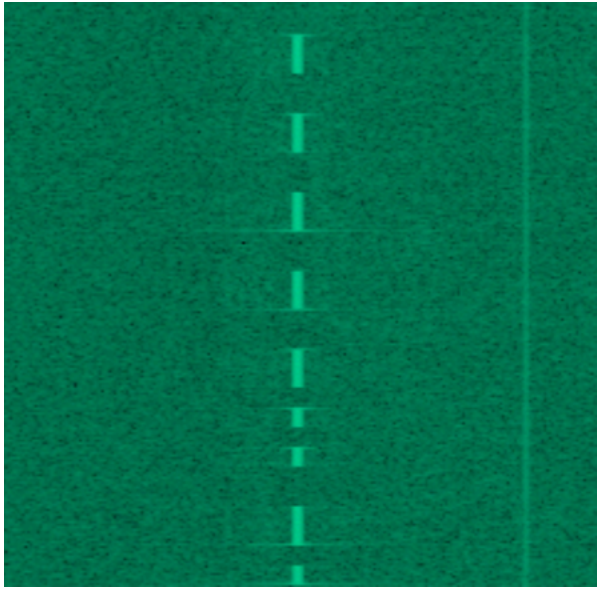
LoRa Modulation

LoRa characteristics

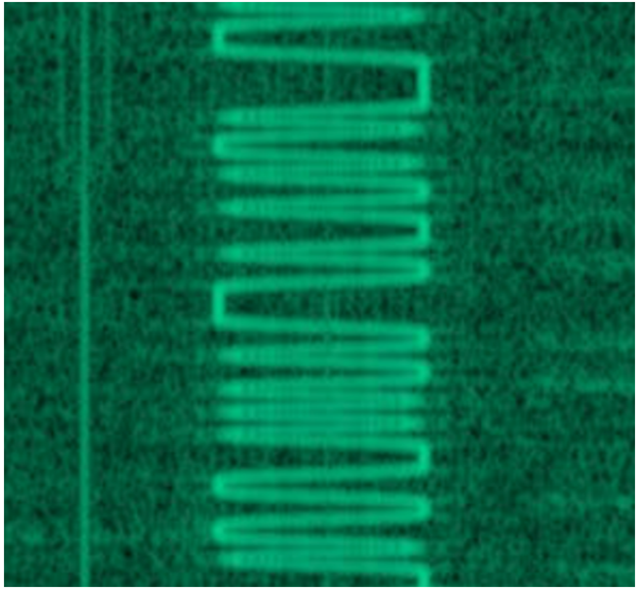


- A variation of chirp spread spectrum (CSS)
- Transmit power in EU 868 Mhz band is mostly limited to 14 dBm (=25 mW)
- Increase reach by increasing energy per bit:
  - Transmit power
  - Modulation rate
- LoRa uses Spreading Factors to set the modulation rate (SF7 to SF12)
- Robust to interference, multipath, and fading
- Developed by Cycleo, a French company acquired by Semtech in 2012
- IP requires less than 50k gates

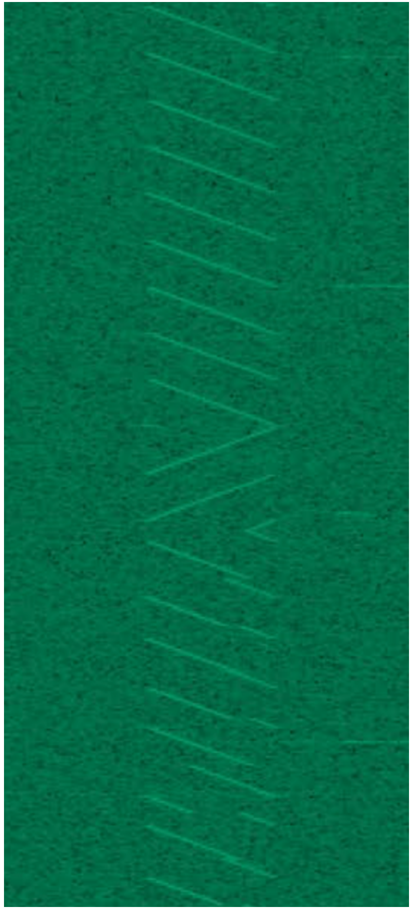




On-Off Keying



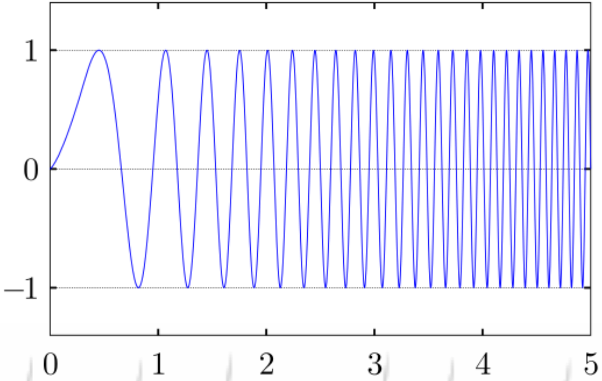
Frequency-shift Keying

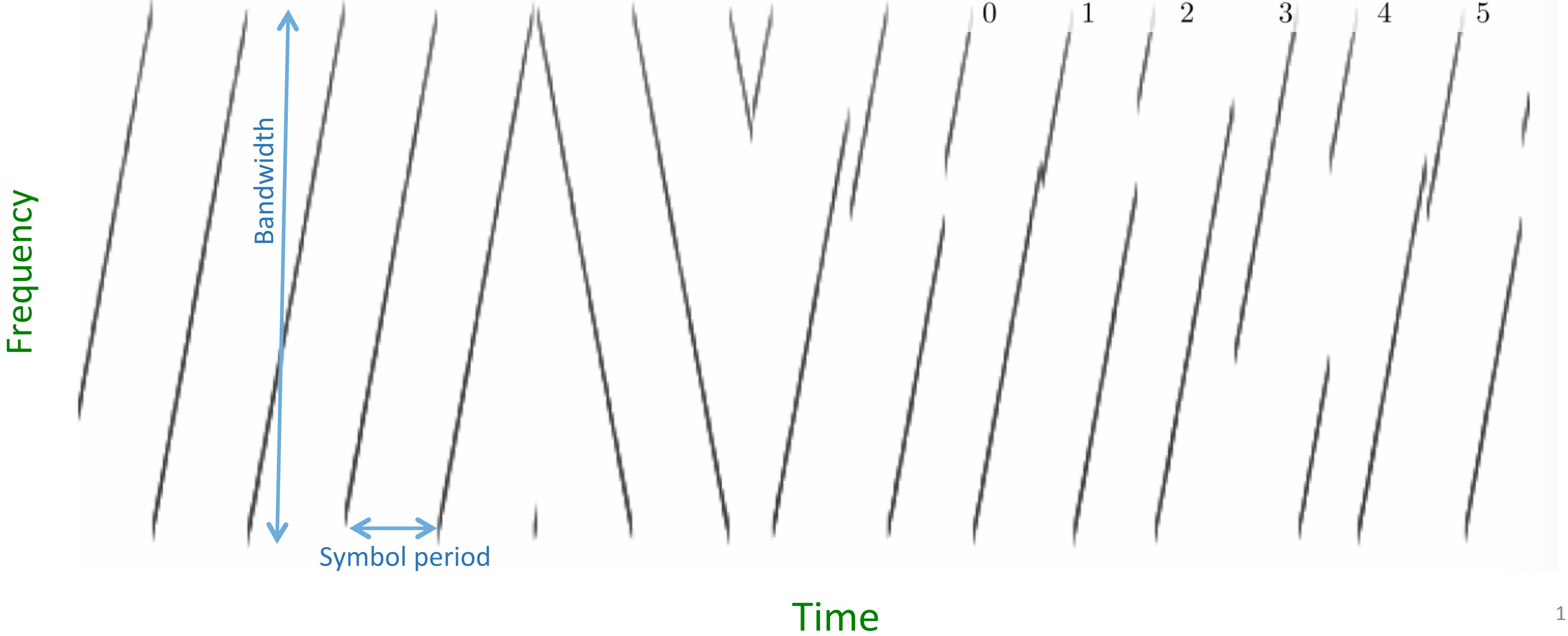


LoRa

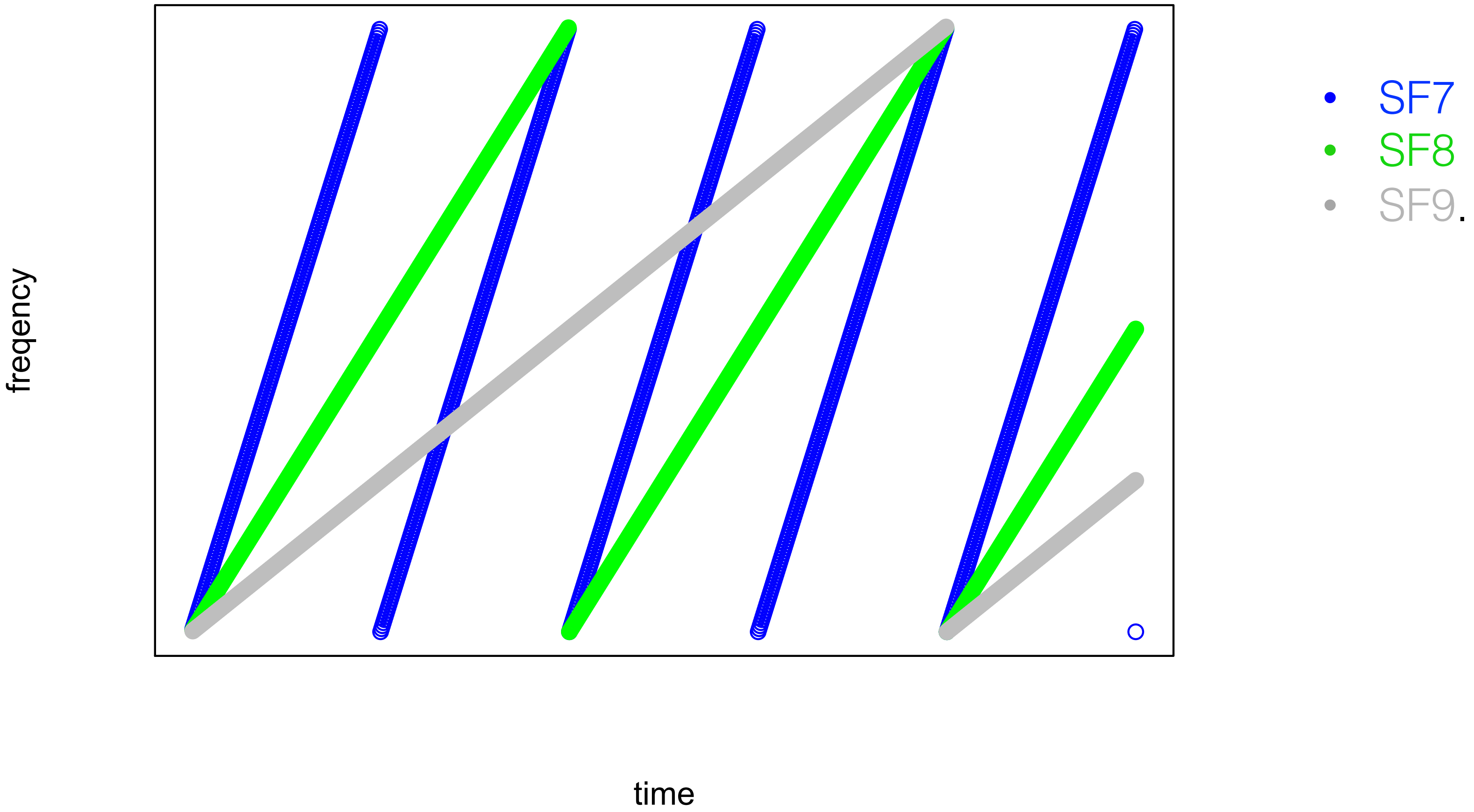
Source: Matt Knight

Time domain (1 chirp):

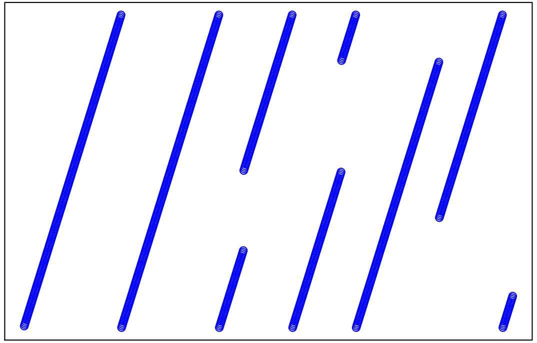




Spreading Factors

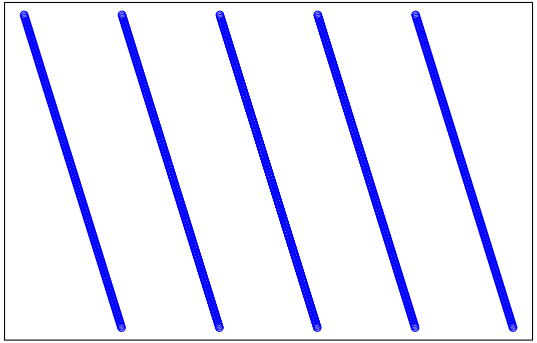


LoRa Demodulation (SF7)



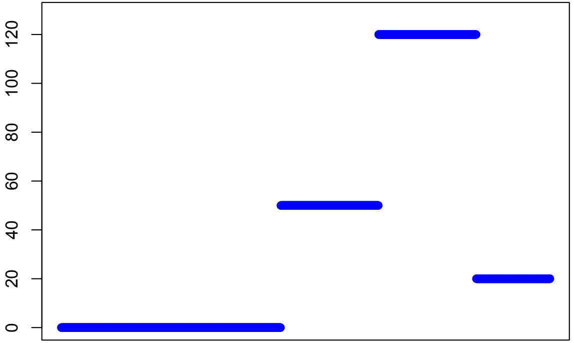
Received Lora signal

x



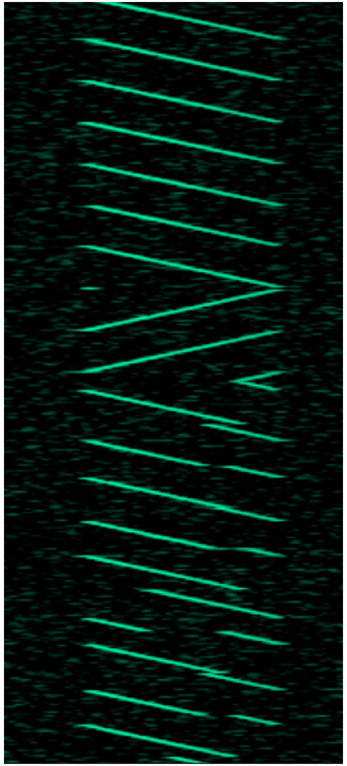
Inverse chirp

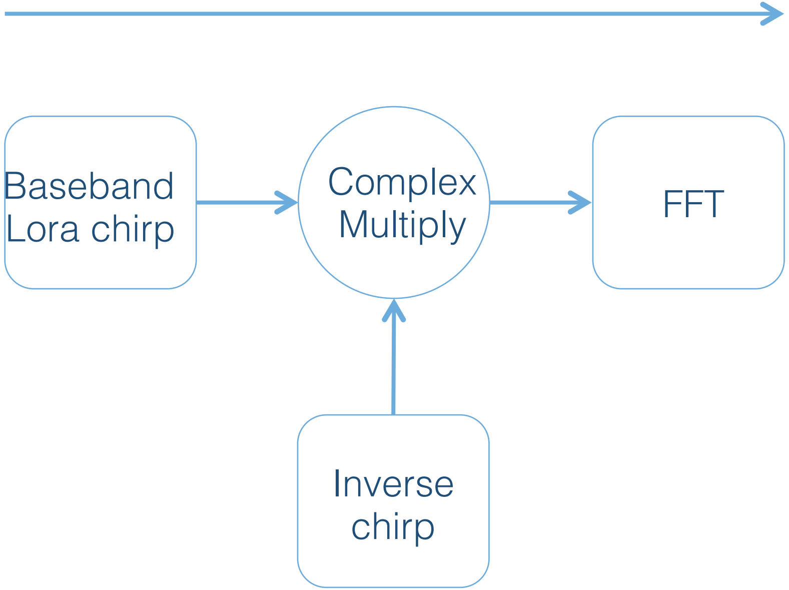
=

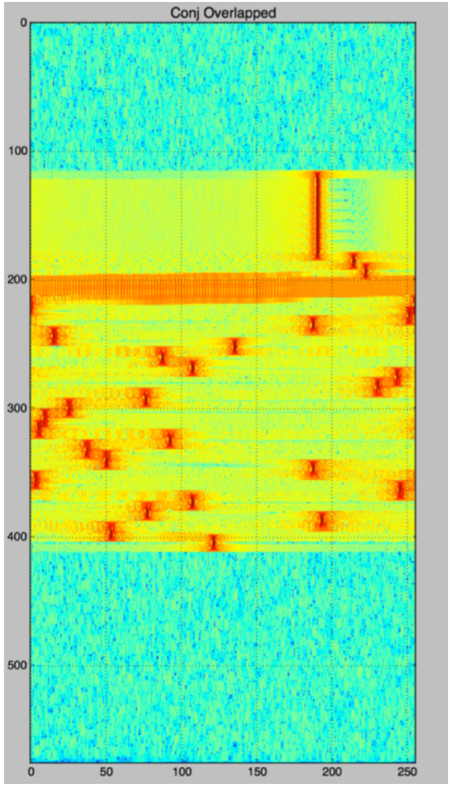


Decoded symbols

LoRa Demodulation

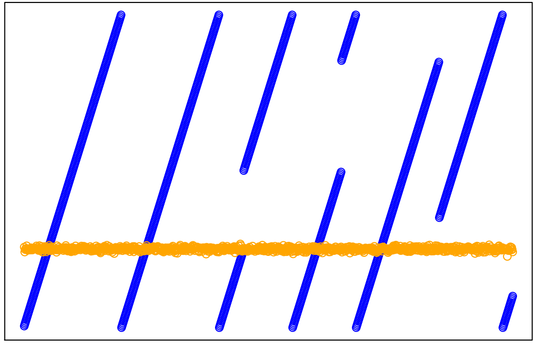






Source: Matt Knight

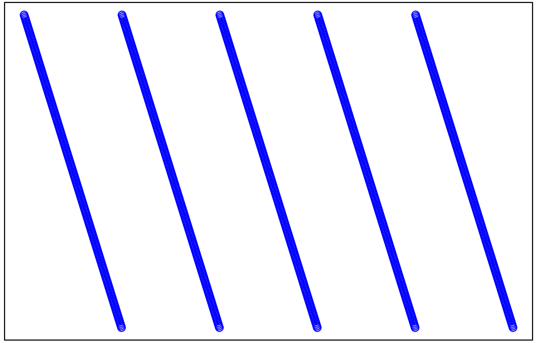
LoRa Demodulation



Received Lora signal

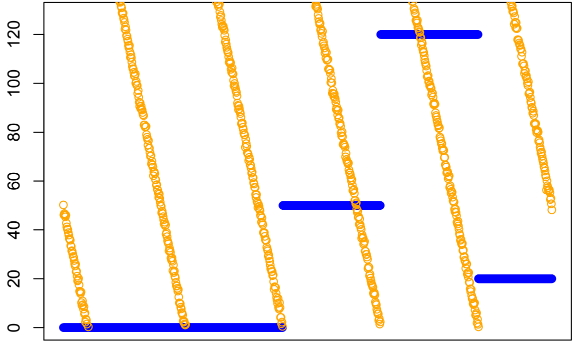
Narrowband interferer

X



Inverse chirp

=



Decoded symbols

Co-channel interference rejection

Spreading factor	Constant envelope interferer (FSK, GFSK, …)	Noise like interferer (OFDM, QAM, …)
SF7	-12.5 dB	-9.5 dB
…	…	…
SF12	-25 dB	-22 dB

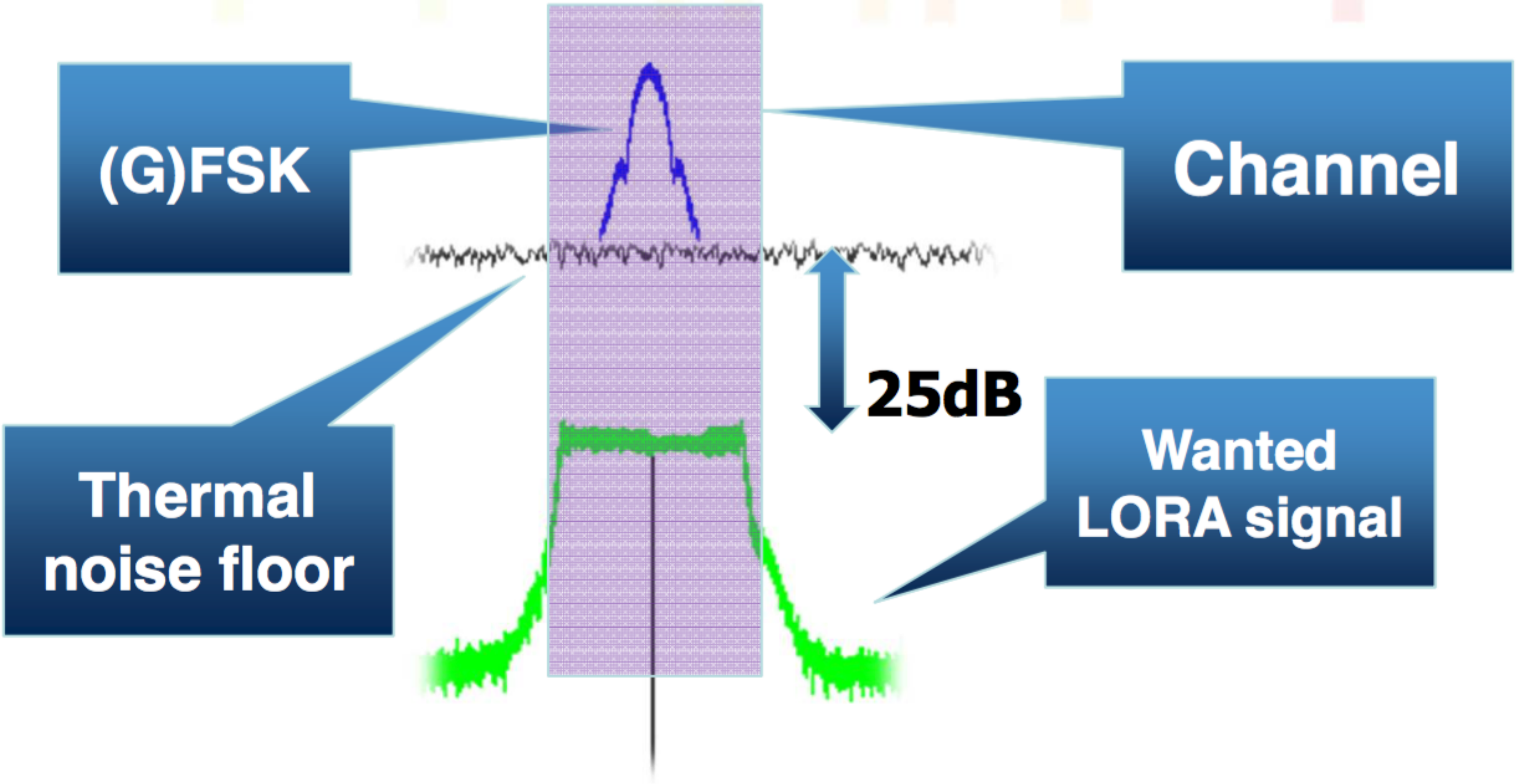
LoRa specifics

- Symbol rate: $R_s = \frac{BW}{2^{SF}}$

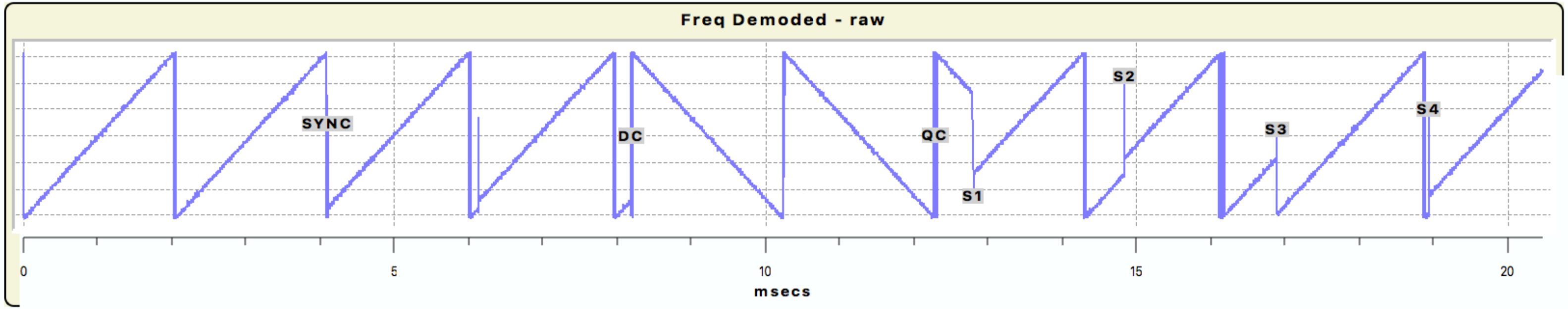
- *SF* bits per symbol

- Bit rate: $R_b = SF\frac{BW}{2^{SF}}$

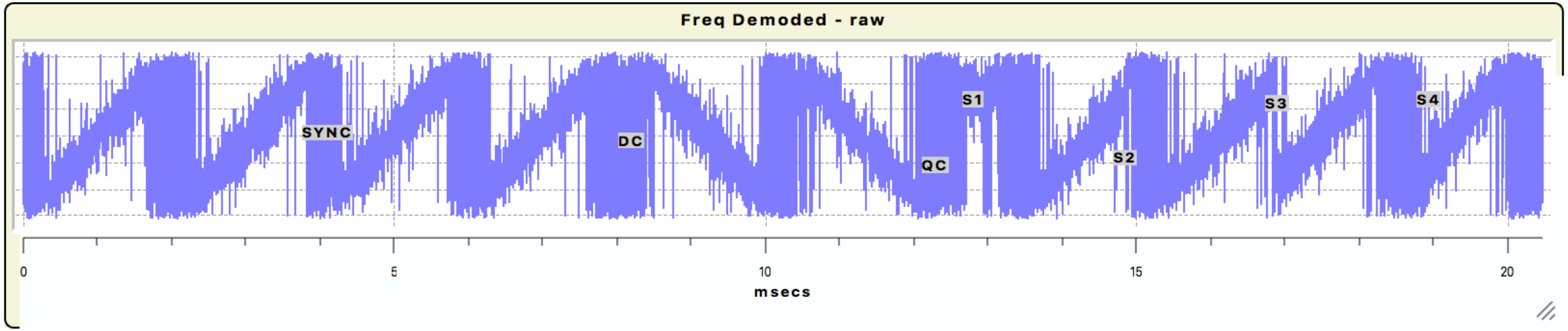
- Data whitening, Interleaving, Forward Error Correction



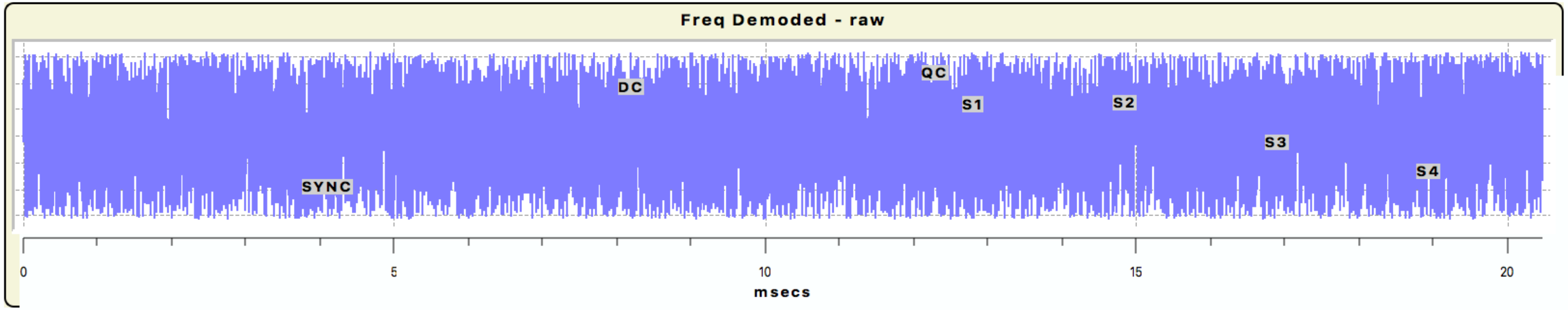
Source: Semtech



Freq Demoded - raw



Freq Demoded - raw

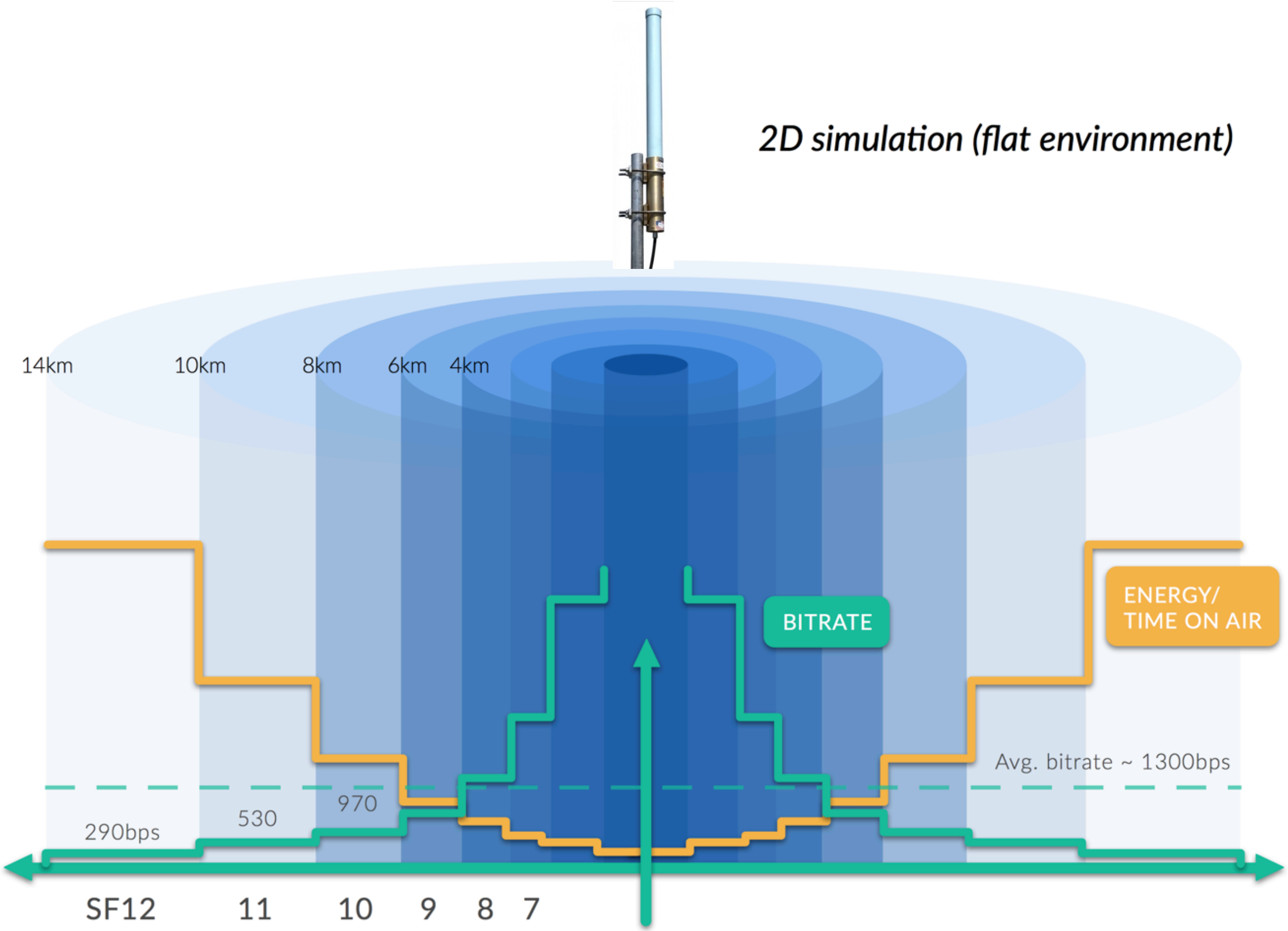


Freq Demoded - raw

LoRa Spreading Factors (125kHz bw)

Spreading Factor	Chips/symbol	SNR limit	Time-on-air (10 byte packet)	Bitrate
7	128	-7.5	56 ms	5469 bps
8	256	-10	103 ms	3125 bps
9	512	-12.5	205 ms	1758 bps
10	1024	-15	371 ms	977 bps
11	2048	-17.5	741 ms	537 bps
12	4096	-20	1483 ms	293 bps

2D simulation (flat environment)



Benefits of LoRa CSS

- Simple to implement (Constant Envelope Modulation)
    - Low acquisition time (compared to DSSS)
- Very resistant to both in-band and out-of-band interference
- High immunity to multipath and fading
- Doppler shift resistant
    - Moving devices
    - High clock tolerance (e.g. 30 ppm crystal!)
- Good sensitivity
- LoRa reception is simple (symmetrical up/down budget)
- Downside: not terribly spectrum efficient

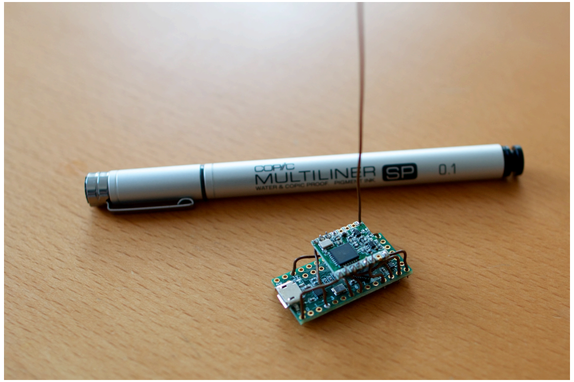
Hardware

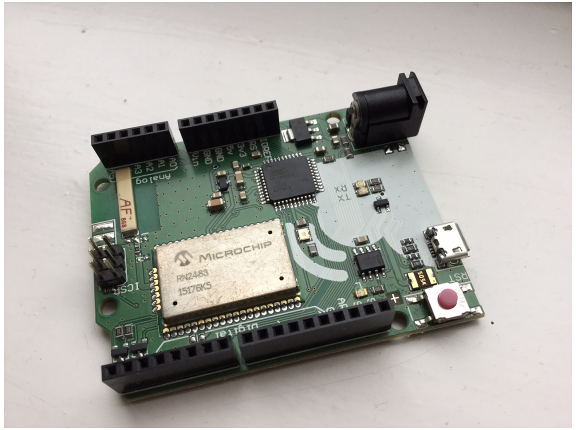
Device chips

- SX1276 -- 137 MHz to 1020 MHz Low Power Long Range Transceiver
    - SX1272 -- 860 MHz to 1020 MHz
- FSK, GFSK, MSK, GMSK, OOK and LoRa modulation
- +20 dBm or +14 dBm (high efficiency PA)
- Channel activity detection (CAD) mode
    - designed to detect a LoRa preamble on the radio channel with the best possible power efficiency

Devices

COPIC
MULTILINER SP 0.3
WATER & COPIC PROOF. PIGMENT INK
MICROCHIP
RN2483
1528HHJ

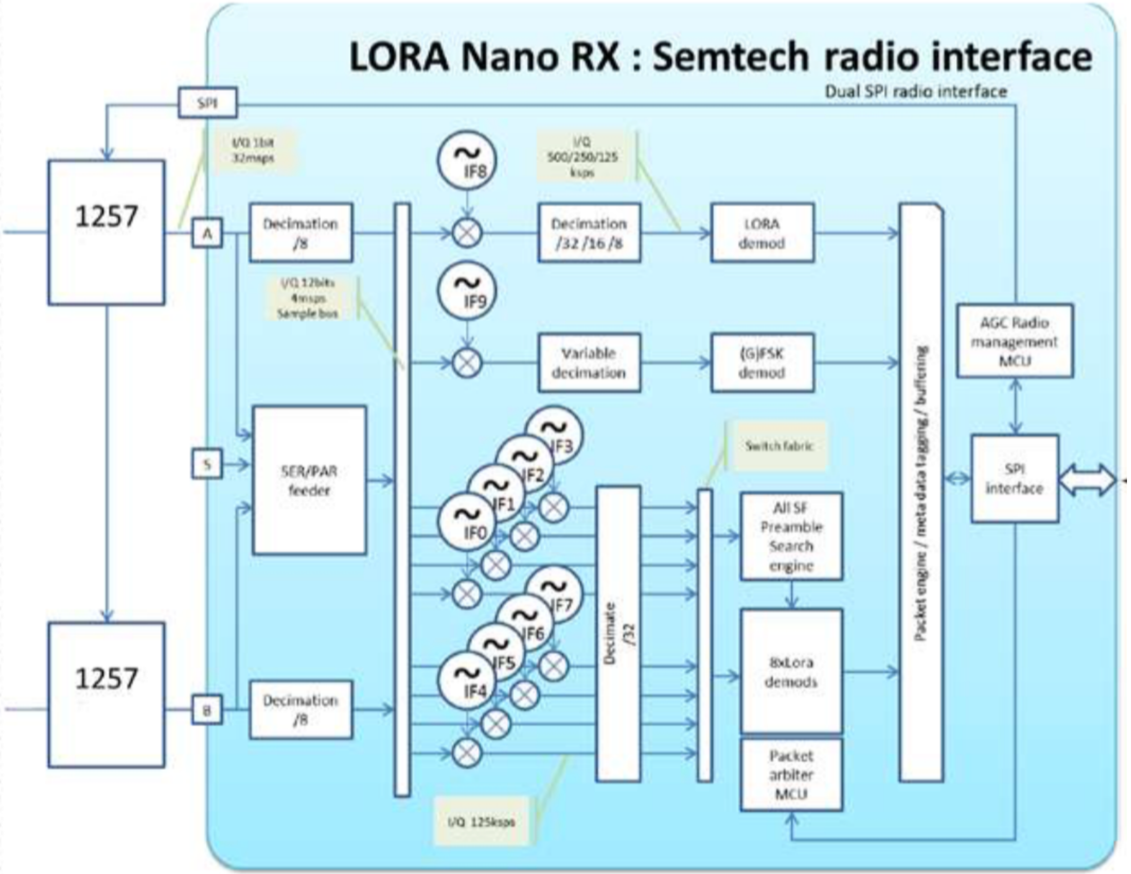

COPIC
MULTILINER SP 0.1


MICROCHIP
RN2483
1517GKS
Analog
TX
RX

Gateway:
SX1301 (DSP) + 2x SX1257 (RF)

SX1301

- Base Band processor
- 2x SX1257 RF front-end
- 8 separate 125 kHz LoRa channels
- One high speed 250 kHz LoRa channel
- One high speed 200 kHz GFSK channel
- Emulates 49 LoRa demodulators
- SX1308 for femto gateway

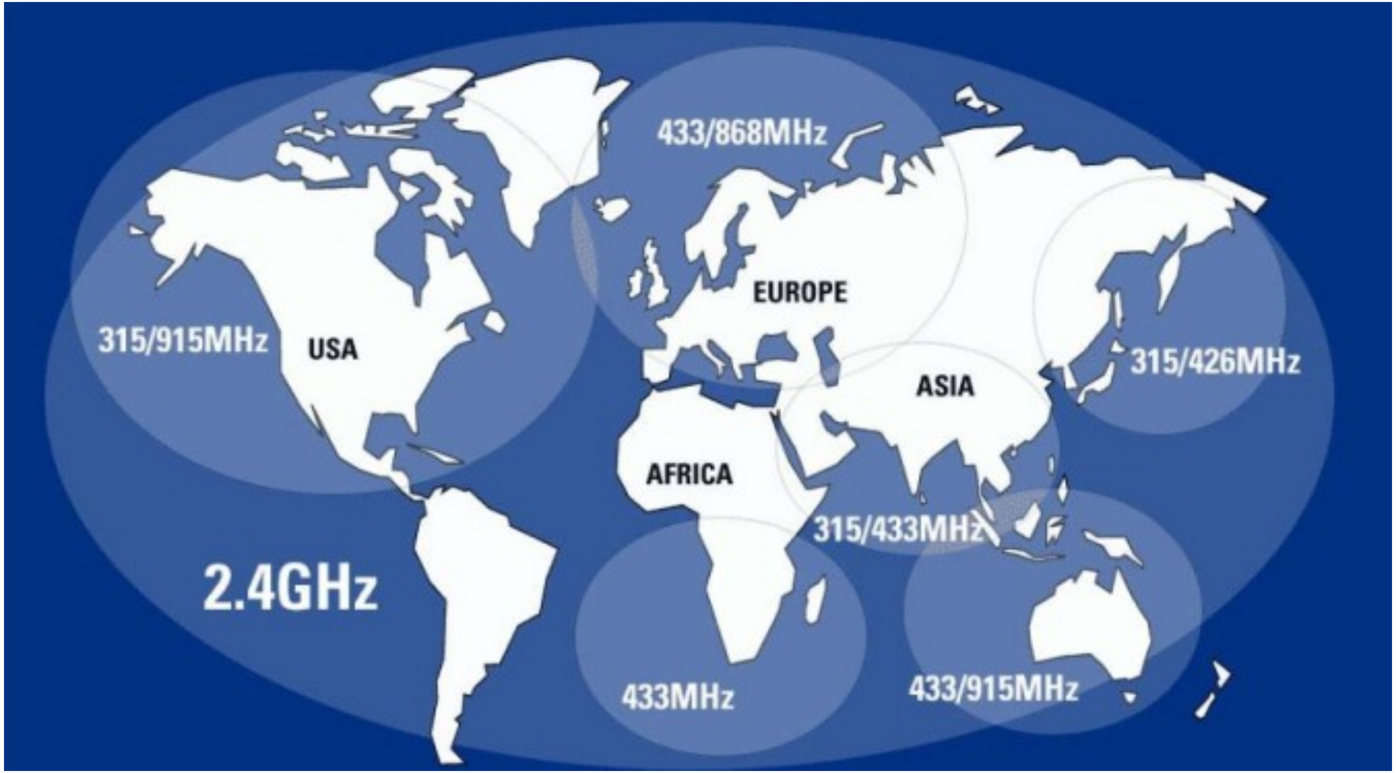


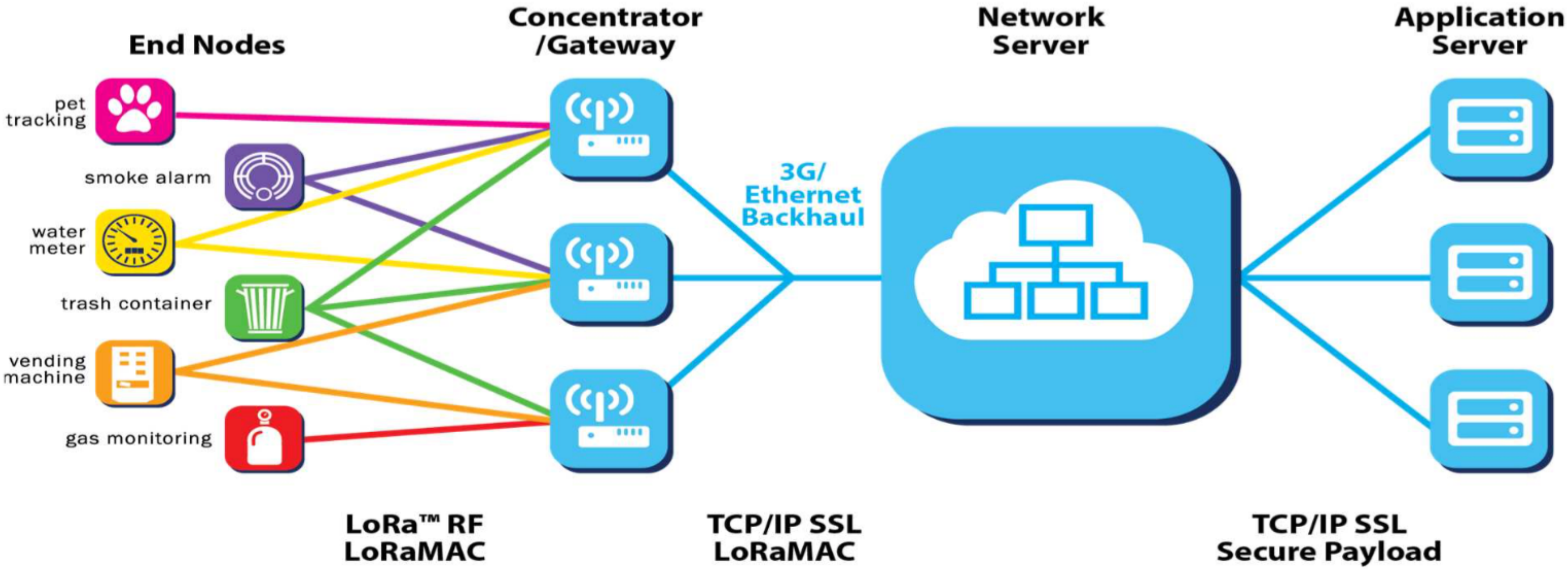
LoRaWAN Protocol

LoRaWAN

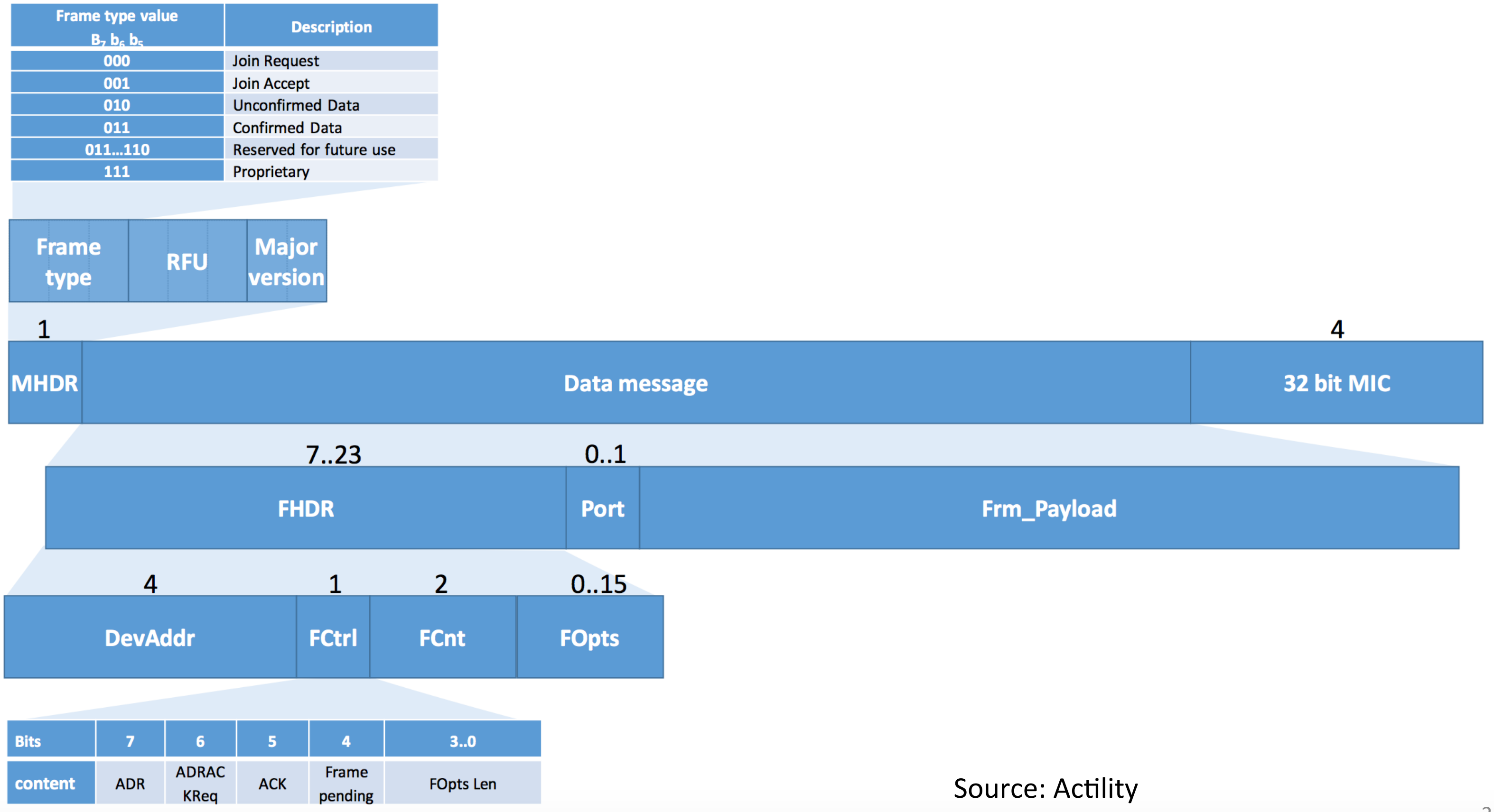
- Protocol standardized by the LoRa Alliance
- Current version: 1.0
  - 1.0.2 upcoming, with extra frequency plans
  - 1.1 next major release
- https://www.lora-alliance.org
  - LoRaWAN 1.0 Specification
  - White papers
- For use in global ISM bands:
  - EU_863_870
  - US_902_928
  - CN779-787, EU433, AU915-928, CN470-510, AS923, KR920-923

Global ISM bands




End Nodes
Concentrator /Gateway
Network Server
Application Server
pet tracking
smoke alarm
water meter
trash container
vending machine
gas monitoring
3G/ Ethernet Backhaul
LoRa™ RF LoRaMAC
TCP/IP SSL LoRaMAC
TCP/IP SSL Secure Payload

LoRaWAN frame



Frame type value B_7 b_6 b_5	Description
000	Join Request
001	Join Accept
010	Unconfirmed Data
011	Confirmed Data
011…110	Reserved for future use
111	Proprietary

Frame type	RFU	Major version

1		4
MHDR	Data message	32 bit MIC

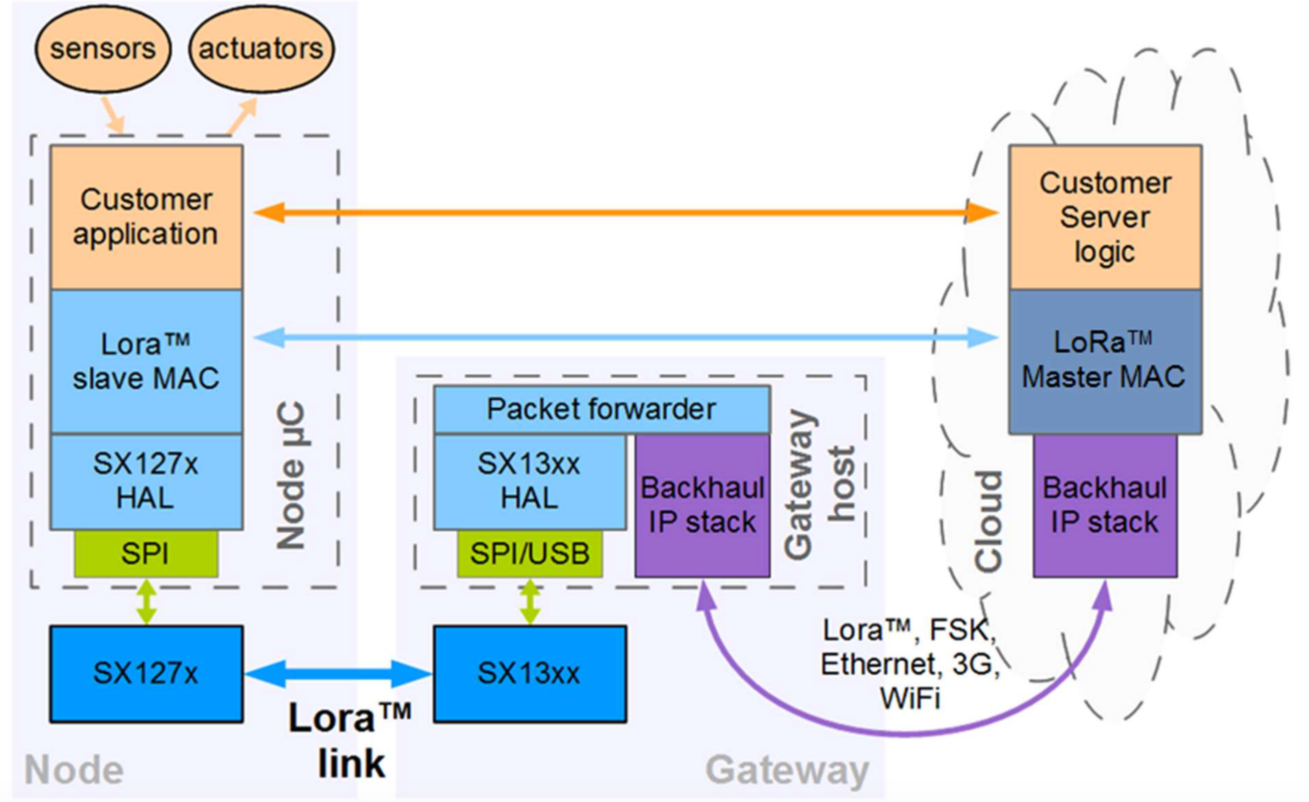
7..23	0..1	
FHDR	Port	Frm_Payload

4	1	2	0..15
DevAddr	FCtrl	FCnt	FOpts

Bits	7	6	5	4	3..0
content	ADR	ADRACKReq	ACK	Frame pending	FOpts Len

Source: Actility

LoRaWAN architecture



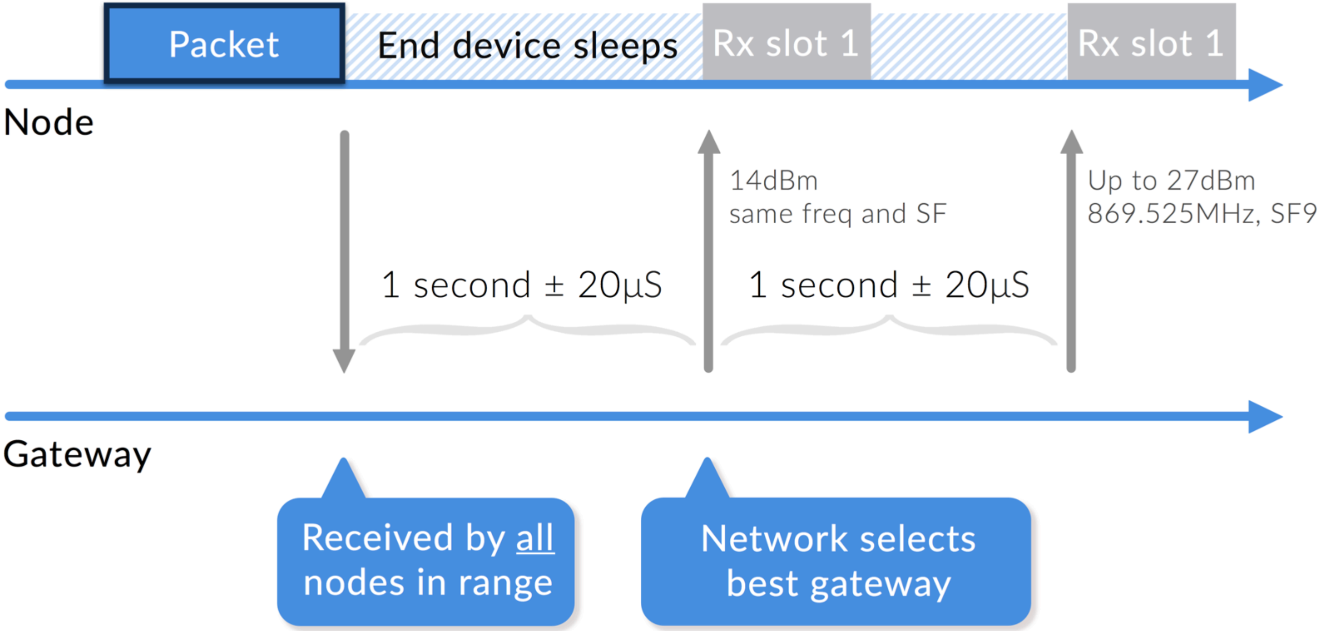
Gateway RX data format

```
{"rxpk":
[{
   "tmst":87485028,
   "time":"2016-12-06T11:15:50.763950Z",
   "chan":6,
   "rfch":0,
   "freq":867.700000,
   "stat":1,
   "modu":"LORA",
   "datr":"SF9BW125",
   "codr":"4/5",
   "lsnr":-11.8,
   "rssi":-118,
   "size":29,
   "data":"QDABAUCA3CMBnpi48xb25eMnX2iH5sA/8RqLqNg="
   }]
}
```

LoRaWAN device classes

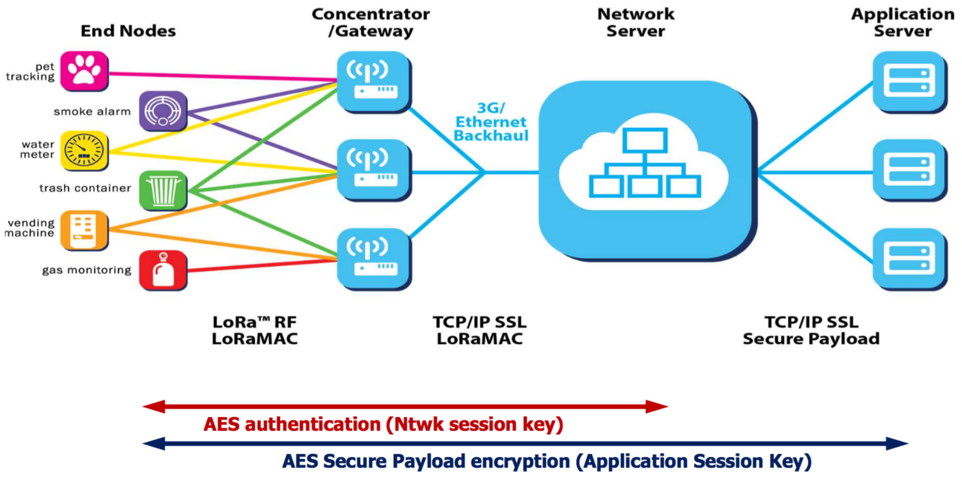
- Three classes of devices have been defined, to address specific application requirements:
  - Class A: Each device's uplink transmission is followed by two short downlink receive windows.
  - Class B: In addition to the Class A functionality, Class B devices open extra receive windows at scheduled times.
  - Class C: These devices have a continuous open receive widow, except when transmitting.

LoRaWAN Class A

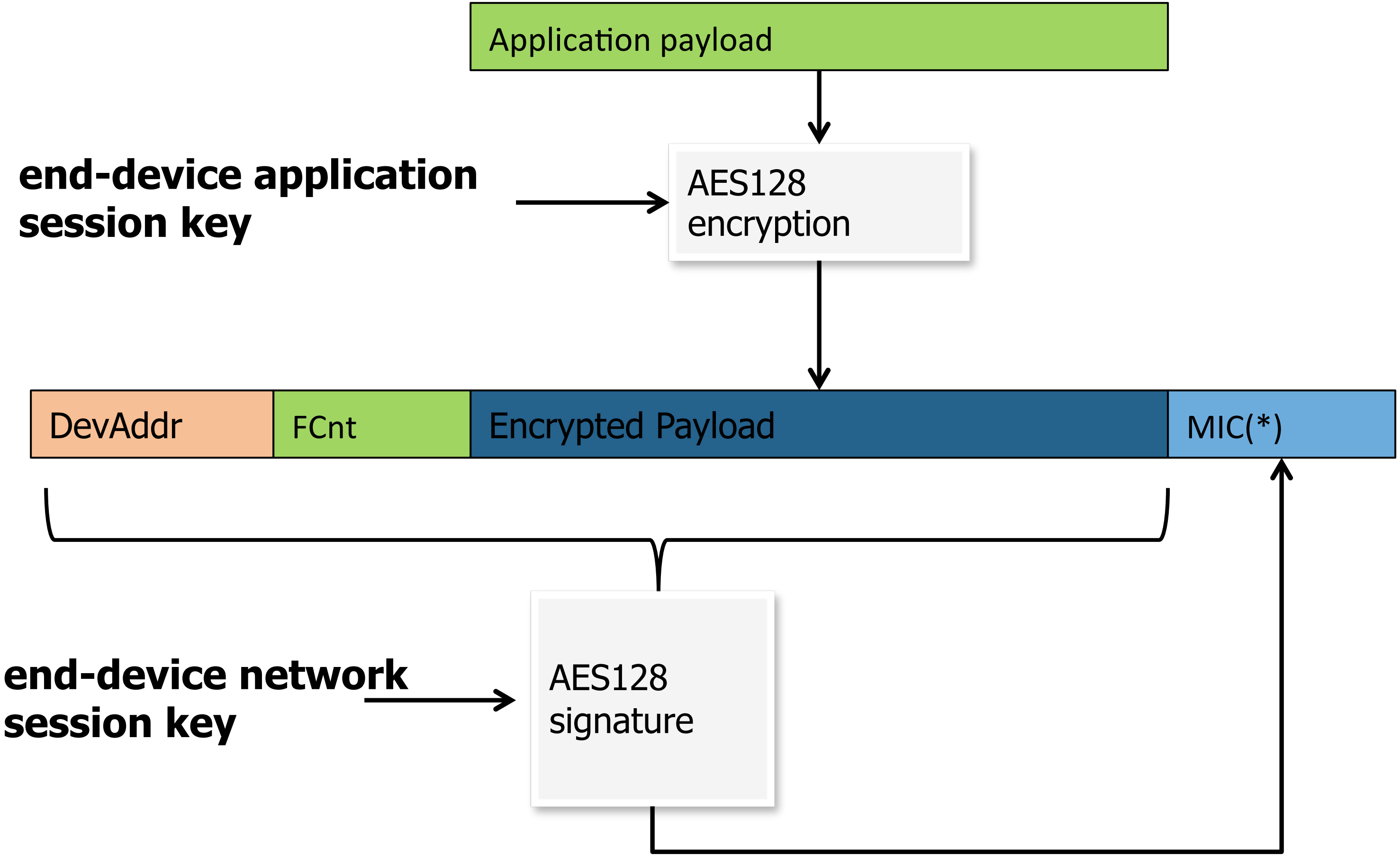


THE THINGS NETWORK

LoRaWAN security



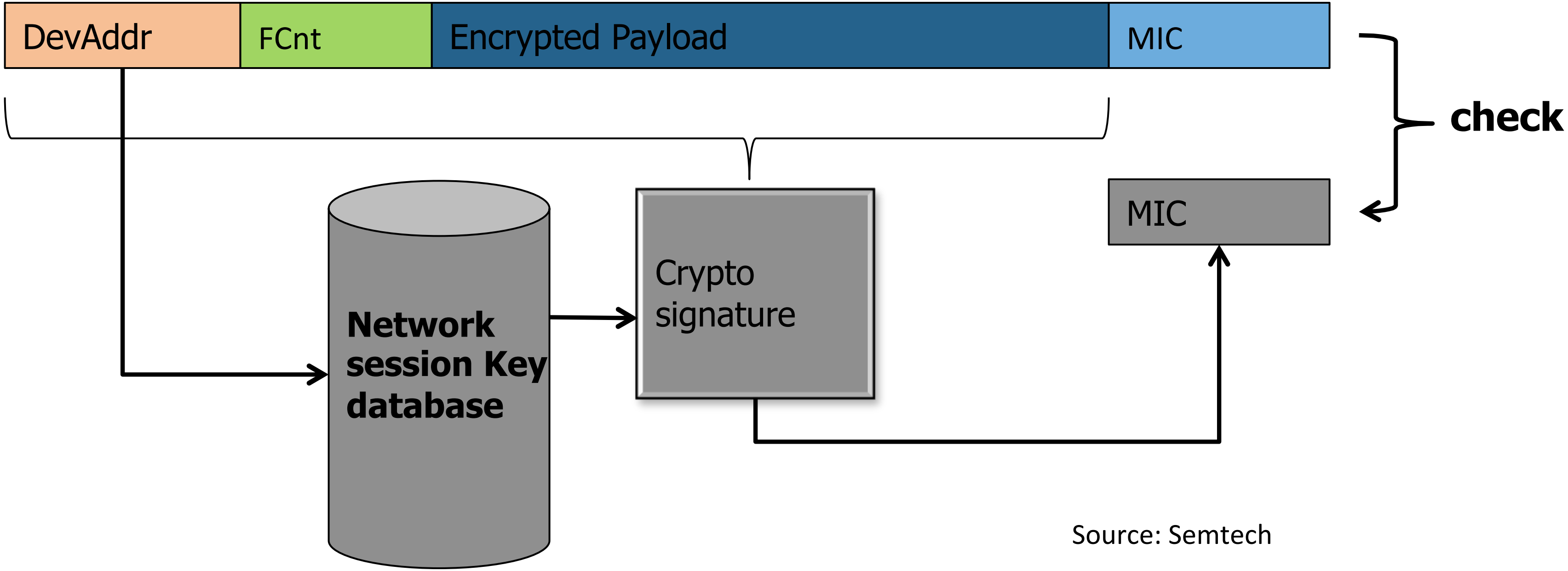
- Two layers of security:
  - Network (nwkSkey)
  - Application (appSkey)
- AES 128 (128 bit key length)
- The network security authenticates the node in the network
  - Message Integrity Check (MIC)
- The application layer of security ensures the network operator does not have access to the application data.
- Sensitive data can optionally be encrypted on top of this with a stronger algorithm.



(*) MIC = Message Integrity Check

Source: Semtech

- 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



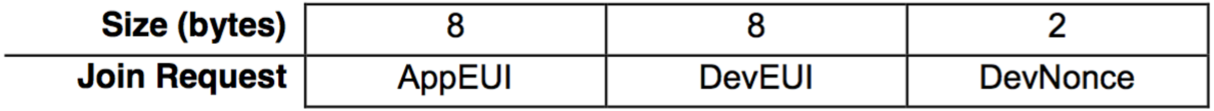
Source: Semtech

LoRaWAN security

- Activation by Personalization or Over The Air (OTAA)
- Personalization:
  - Fixed device addresses and security keys
  - Simple
  - Vulnerable to replay attacks (after a reset)
- Over The Air Activation
  - New security session keys can be generated from a shared secret
  - Enables roaming

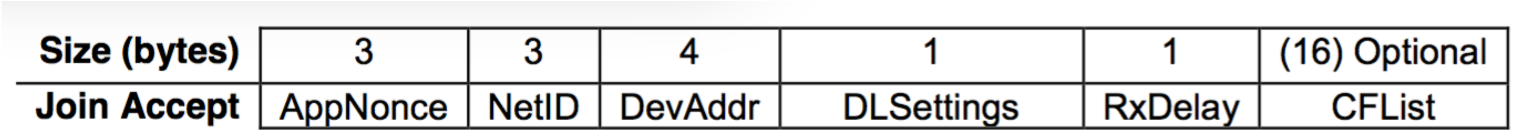
Join Process

- Device is provisioned with DevEUI (64 bits), AppEUI (64 bits), and AppKey (128 bits)
- Device sends join request message:



Size (bytes)	8	8	2
Join Request	AppEUI	DevEUI	DevNonce

- Network server calculates the session keys:
  - NwkSKey = aes128_encrypt(AppKey, 0x01 | AppNonce | NetID | DevNonce | pad16)
  - AppSKey = aes128_encrypt(AppKey, 0x02 | AppNonce | NetID | DevNonce | pad16)
- Network server send join accept message:

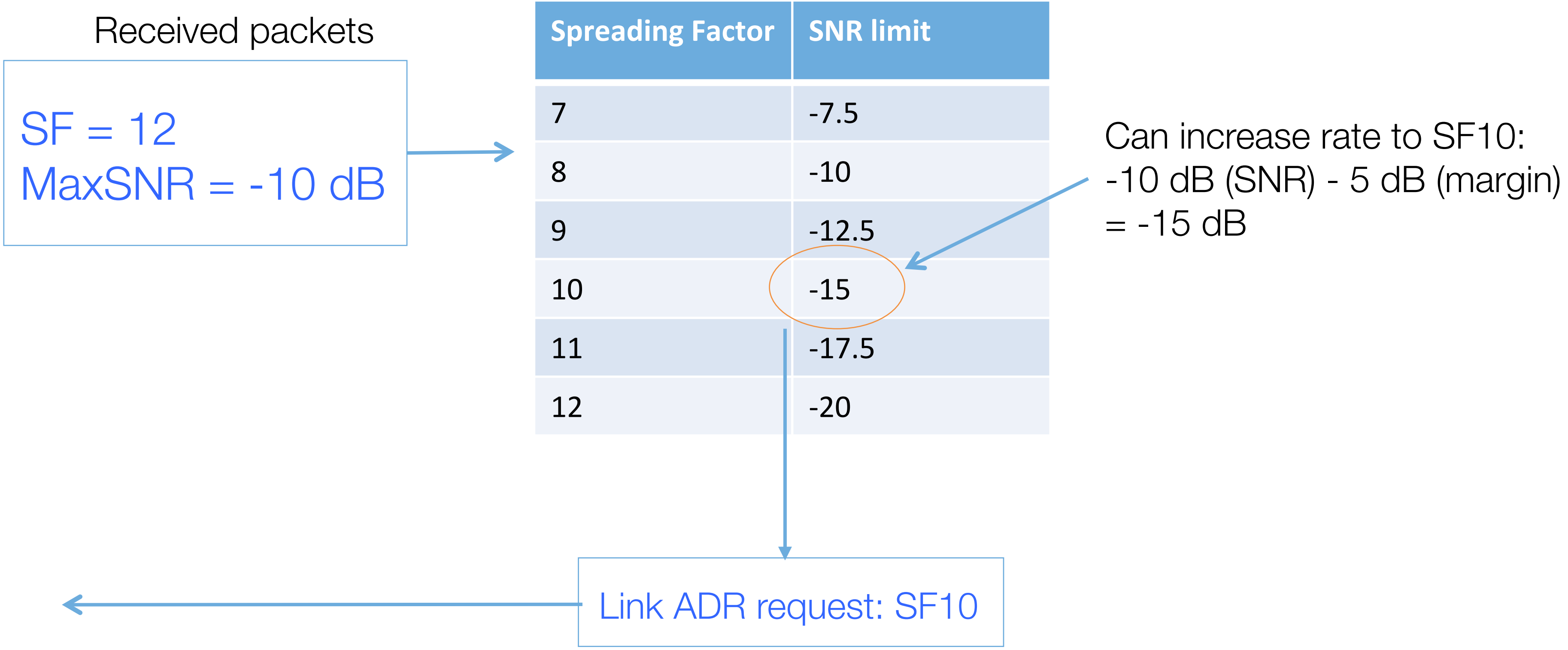


Size (bytes)	3	3	4	1	1	(16) Optional
Join Accept	AppNonce	NetID	DevAddr	DLSettings	RxDelay	CFList

LoRaWAN scalability

- Gateways listen on 8 frequencies
- All SF per frequency
    - Can receive concurrently two different SF on the same frequency
- In case of collision, packet with strongest signal gets decoded (generally)
- Two dedicated high-speed channels (10 kbps and 50 kbps)
- Adaptive Data Rate (ADR), see next slide
- In case of congestion, scale by adding gateways
    - Nodes get closer to the gateway
    - Due to ADR, spreading factors will be reduced
    - More capacity: multiplicative!

Adaptive Data Rate (ADR) mechanism



Received packets

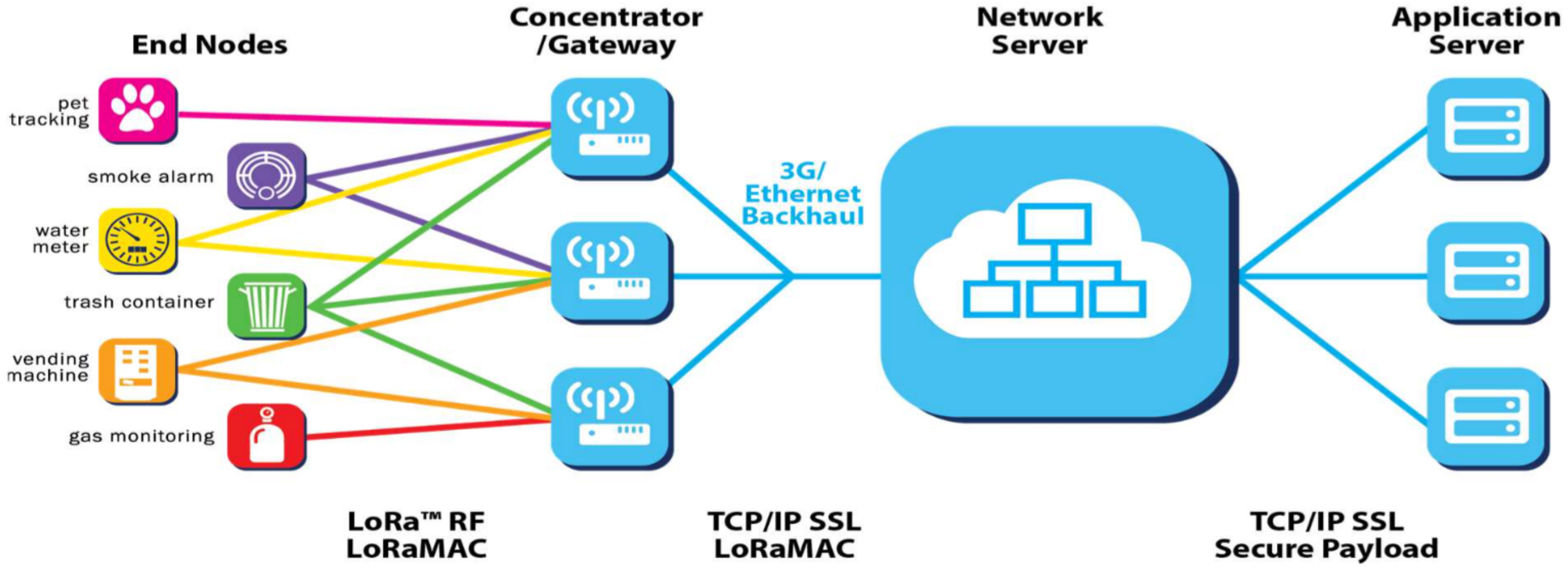
SF = 12
MaxSNR = -10 dB

Spreading Factor	SNR limit
7	-7.5
8	-10
9	-12.5
10	-15
11	-17.5
12	-20

Can increase rate to SF10:
-10 dB (SNR) - 5 dB (margin)
= -15 dB

Link ADR request: SF10

Deployment models

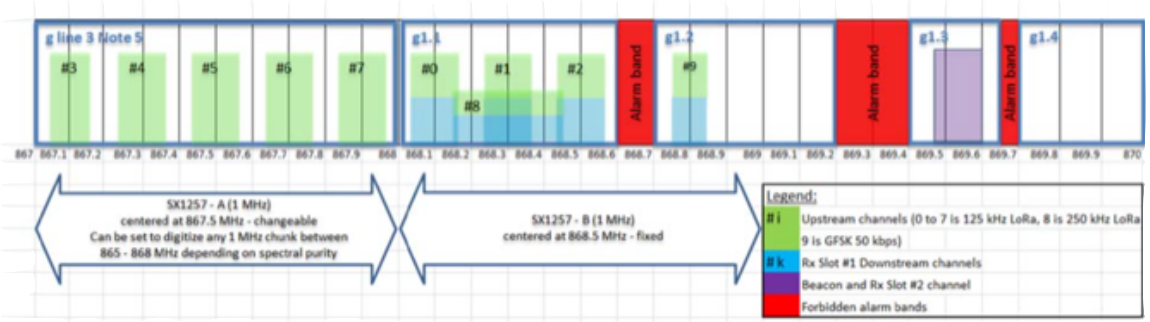

End Nodes
Concentrator /Gateway
Network Server
Application Server
pet tracking
smoke alarm
water meter
trash container
vending machine
gas monitoring
3G/ Ethernet Backhaul
LoRa™ RF LoRaMAC
TCP/IP SSL LoRaMAC
TCP/IP SSL Secure Payload

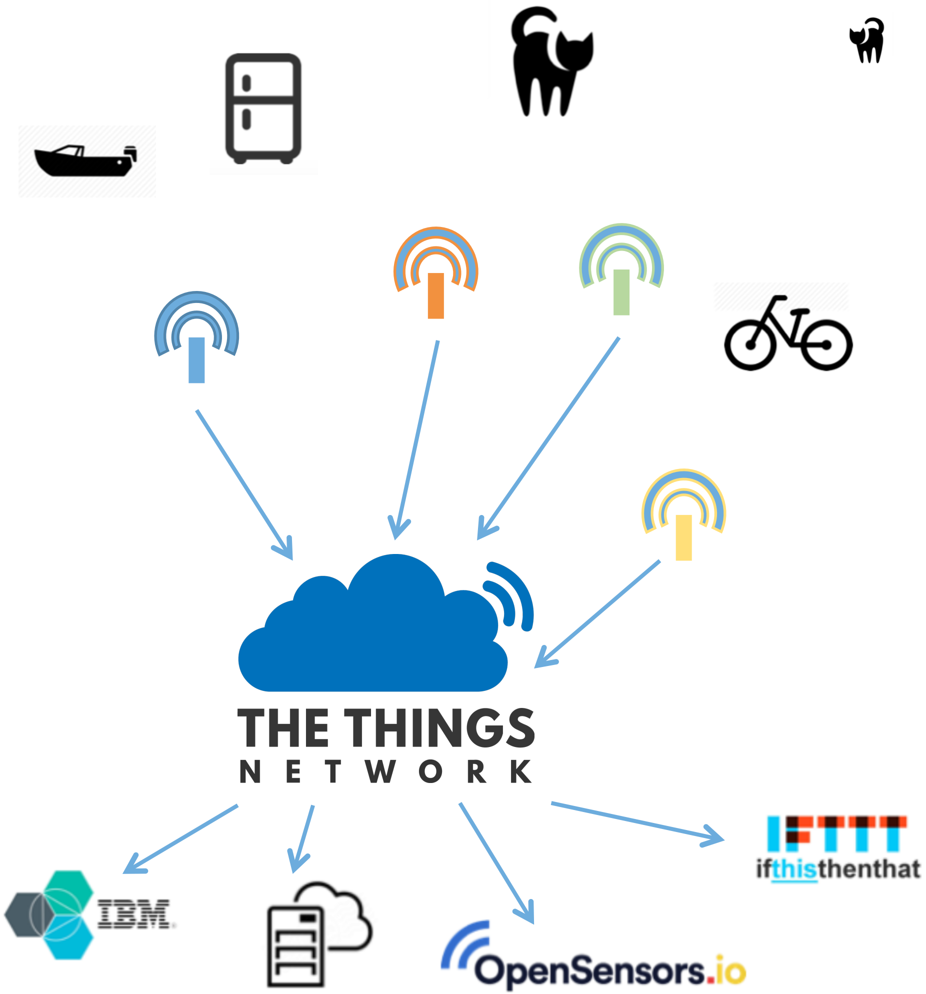
Private vs Public Network

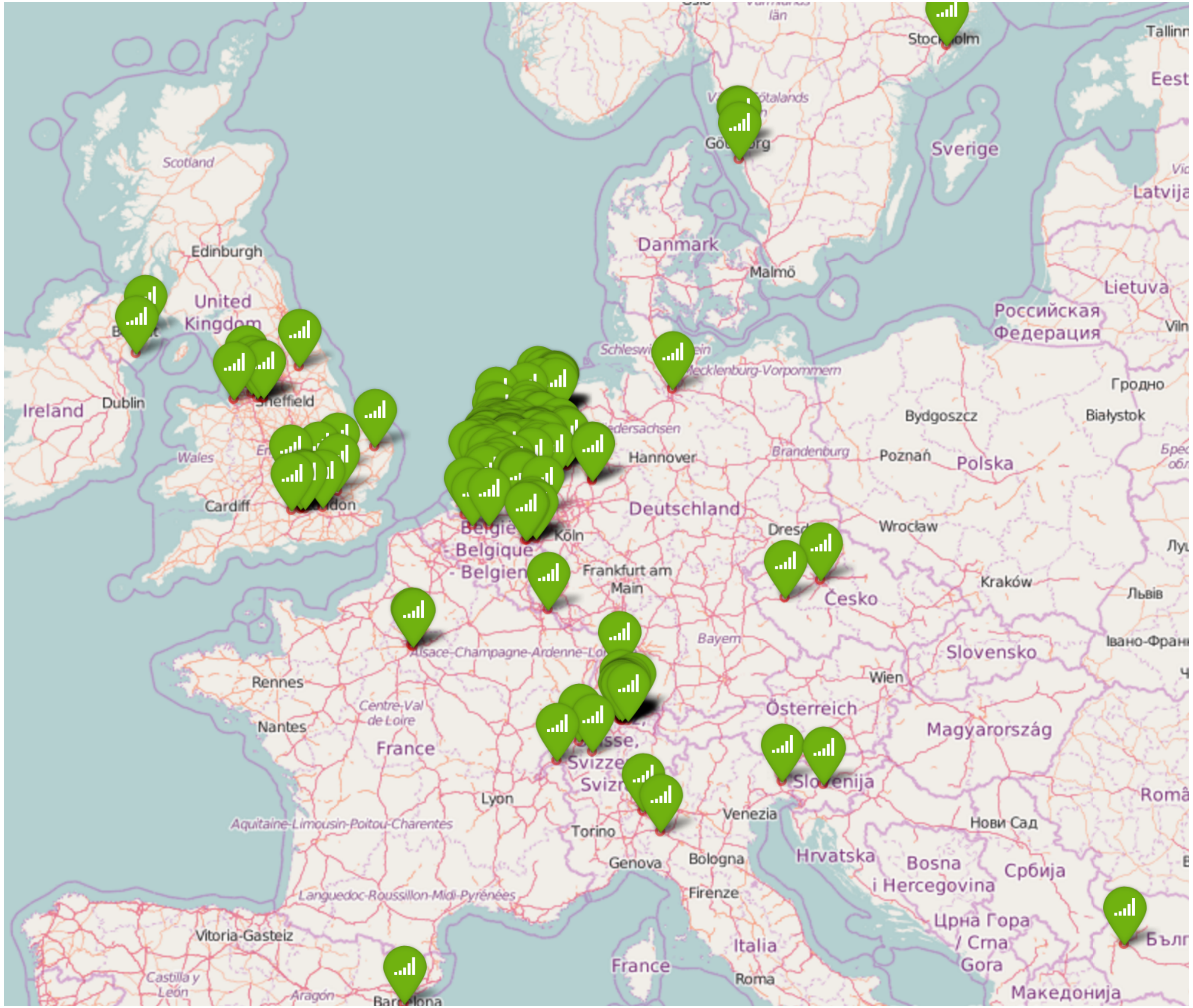
- Private Network
    - Individually managed
    - Specific deployments: geographically bound
- Centralized Public Network
    - Telecom operator managed network
    - Large geographical coverage
    - Fully managed
    - Roaming
- Distributed/Cooperative Public Network
    - No single owner, no single point of control
    - E.g. The Things Network
    - Internet model

The Things Network

- Global community LoRaWAN network
- No “single point of control”
- End-to-end encryption
- No country borders
- Overlapping device-addresses
- Uses recently released sub-band g1, line 3, Note 5




THE THINGS
NETWORK
IBM
IFTTT
ifthisthenthat
OpenSensors.io


Värmlands län
Stockholm
Tallinn
Eesti
Västra Götalands län
Göteborg
Sverige
Latvija
Scotland
Edinburgh
Danmark
Malmö
Lietuva
United Kingdom
Российская Федерация
Viln
Belfast
Schleswig-Holstein
Mecklenburg-Vorpommern
Ireland
Dublin
Sheffield
Гродно
Bydgoszcz
Białystok
Niedersachsen
Wales
Brandenburg
Poznań
Polska
Hannover
Cardiff
London
Deutschland
België - Belgique - Belgien
Köln
Dresden
Wrocław
Frankfurt am Main
Kraków
Львів
Česko
Alsace-Champagne-Ardenne-Lorraine
Bayern
Slovensko
Rennes
Wien
Centre-Val de Loire
Nantes
Österreich
Magyarország
France
Suisse, Svizzera, Svizra
Slovenija
Lyon
Venezia
Român
Нови Сад
Aquitaine-Limousin-Poitou-Charentes
Torino
Genova
Bologna
Hrvatska
Bosna i Hercegovina
Србија
Firenze
Languedoc-Roussillon-Midi-Pyrénées
Црна Гора / Crna Gora
Vitoria-Gasteiz
Italia
France
Бълг
Castilla y León
Aragón
Barcelona
Roma
Македонија

Core Components

Gateway

Send data to and receive data from nodes

Broker

Decoupling from Router and Application Handler

Application Handler

Decryption, deduping, works on behalf of apps

Router

Routes raw packets from gateways to brokers

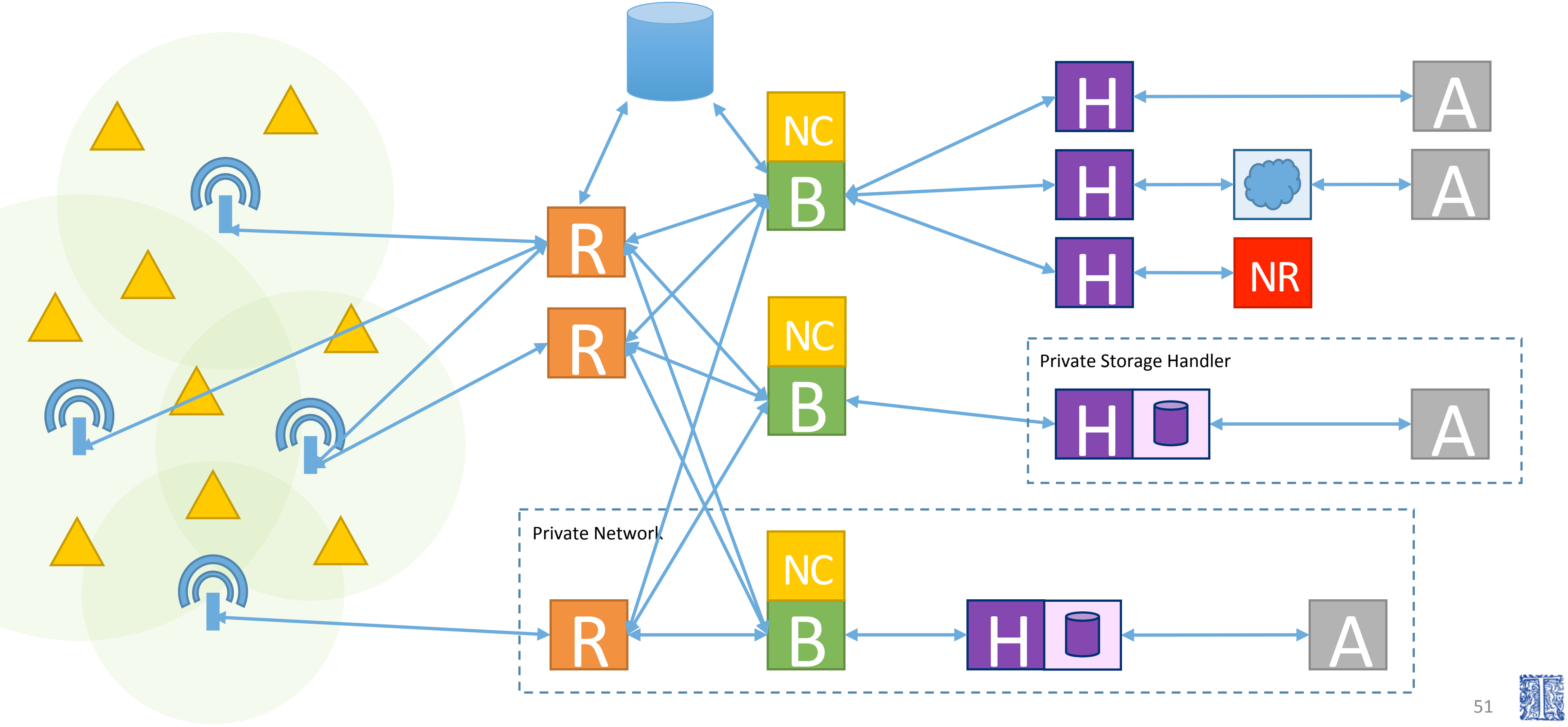
Network Controller

Node state: data rate and frequency management

Application

User application

Public and Private Networking



Long-range networking in shared spectrum

LoRaWAN observations

- LoRa designed for use in ISM band: interference tolerant

- Due to uncoordinated transmission, system can’t sustain a high load (‘ALOHA-like’)
- Maintain reception duty-cycle under 10% (per channel)
- Manage load by densifying the network: cheap gateways
- Additional benefit: more downlink capacity (half-duplex gateways)

- Is this good use of the (ISM) spectrum?
- How does LoRa affect other long-range technologies?

Optimizations

- Adaptive Data Rate
    - Manage spreading factor and transmission power
- Geography based channel allocation (use certain frequencies in some places but not in others)
- Listen Before Talk

Alternative LPWAN technologies

- SigFox
  - (Ultra) narrowband DBPSK uplink
  - 100Hz uplink channels (random!) in 200 kHz band
  - 12 bytes packets, 3x repetition
  - GFSK downlink (600 baud)
  - Gateways and servers managed by SigFox
- LinkLabs Symphony Link
  - LoRa based, but synchronized/slotted
  - Not for public networking
- Other
  - Ingenu, 802.11ah, Waviot, Weightless-N, -P, etc.

3GPP

- LTE Cat-M1
  - ‘LTE-Light’
  - Smaller front-end (1.4Mhz), half-duplex, 1 antenna
  - Cheaper chipset
  - Power Saving Mode and Extended Discontinuous Reception
  - Questions/Issues: cost, IPR, actual battery usage

- LTE Cat-NB, NB-IOT
  - Not LTE
  - 200 kHz bands: stand-alone, guard-band, in-band
  - Questions/Issues: deployment, IPR, cost, battery, mobility, sim-card (?)

Commons

- Elinor Ostrom, “Governing the Commons”
- “Tragedy of the commons” can be prevented if a commons is bound by *people*, *place*, and *rules*

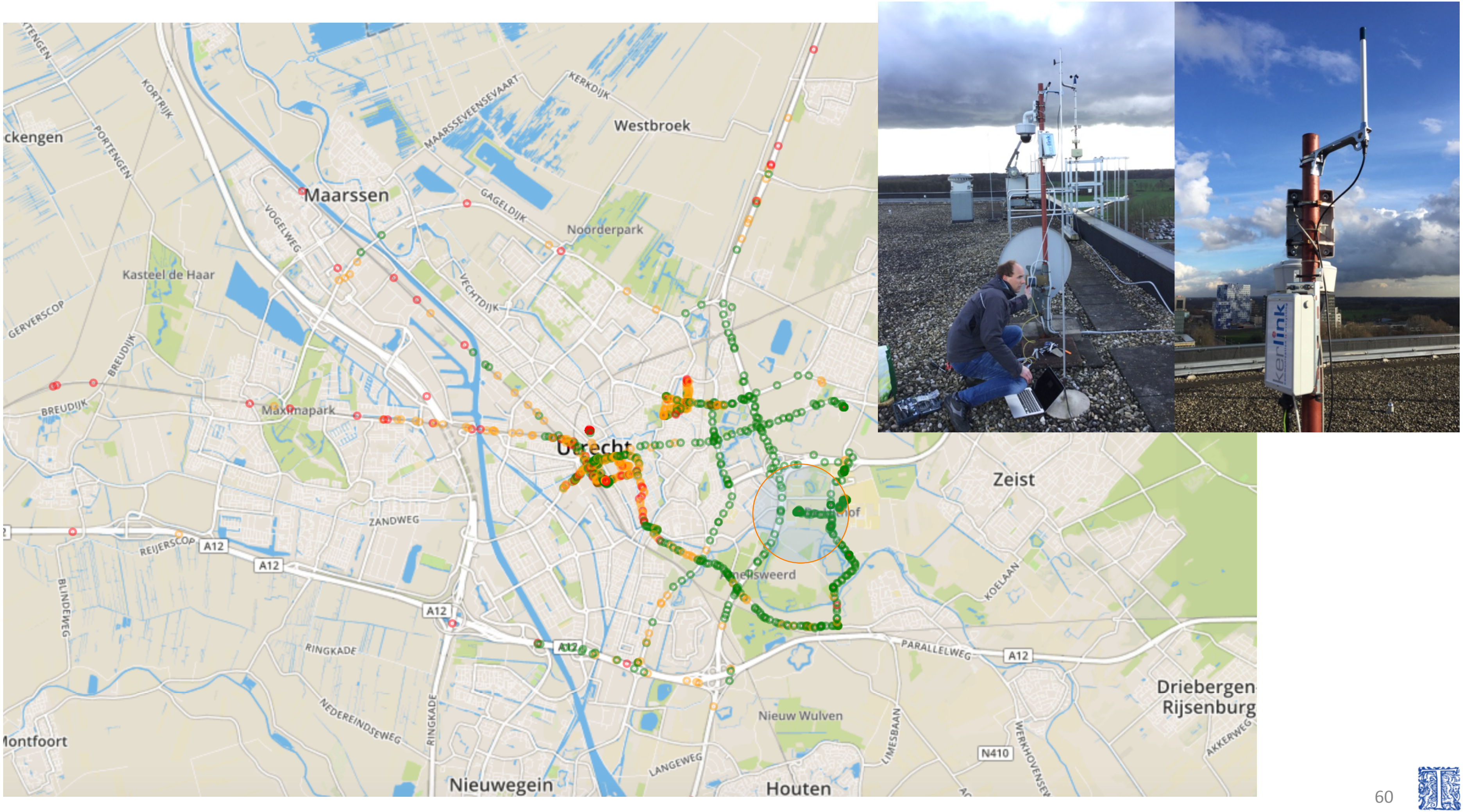
- ISM band for SRD is regulated for uncooperative users
    - Limit power and duty-cycle to limit influence of a single user

- But for long-range networking this is different. Users:
    - are related to each other (could be grouped)
    - have common objectives
    - could develop and maintain rules that maximize total gain

What can we do?

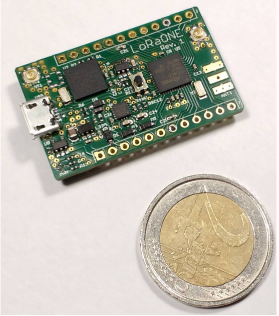
- Recent (lpwan) IoT research reports (Dialogic, Stratix, Figo, Strict, etc.) signal potential problems, but do not provide significant solutions (or directions) other than managing the problem itself by raising awareness, additional spectrum, stricter rules, monitoring, etc.
- What can we learn from Cognitive Radio, Commons models, and available data for future use of license-exempt spectrum?
- For example, simple CR capabilities
  - Mix LoRa (CSS) with narrowband and have devices and the network make smart decisions, to optimize performance and efficiency
    - E.g. Ultra-Narrowband for uplink, LoRa for downlink
  - Measure and share frequency usage
  - Multi dimensional metrics?
- Can we start experimenting with technical and policy solutions in current license-exempt spectrum, to build a case for future allocations?

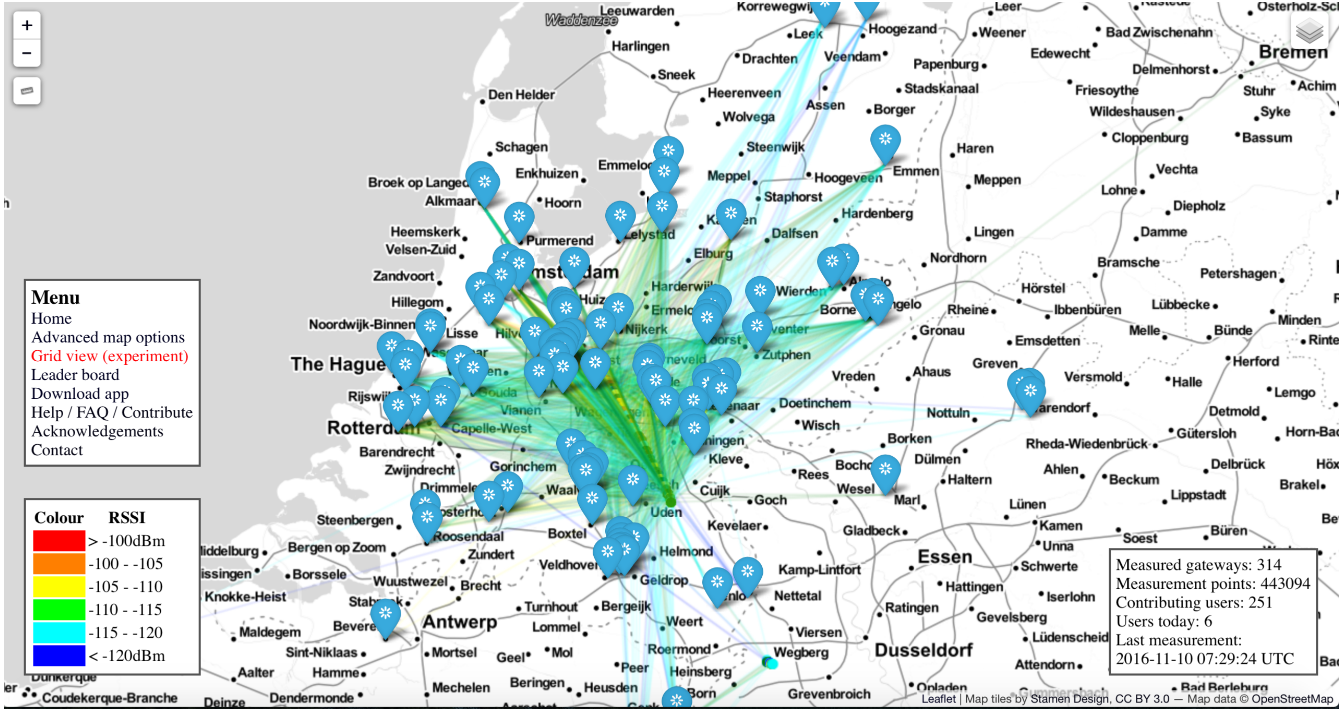
Extra material



ckengen
KORTRIJK
PORTENGEN
MAARSSEVEENSEVAART
KERKDIJK
Westbroek
Maarssen
GAGELDIJK
Noorderpark
VOGELWEG
Kasteel de Haar
VECHTDIJK
GERVERSCOP
BREUDIJK
BREUDIJK
Maximapark
Utrecht
Zeist
ZANDWEG
REIJERSCOP
A12
A12
A12
A12
A12
nellsweerd
hof
BLINDEWEG
RINGKADE
KOELAAN
PARALLELWEG
Driebergen-
Rijsenburg
Nieuw Wulven
NEDEREINDSEWEG
RINGKADE
LIMESBAAN
N410
WERKHOVENSEW
AKKERWEG
lontfoort
Nieuwegein
LANGEWEG
Houten
kerlink

SODAQ balloon flight (>14km altitude)





Menu
Home
Advanced map options
Grid view (experiment)
Leader board
Download app
Help / FAQ / Contribute
Acknowledgements
Contact

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

Measured gateways: 314
Measurement points: 443094
Contributing users: 251
Users today: 6
Last measurement:
2016-11-10 07:29:24 UTC

Leaflet | Map tiles by Stamen Design, CC BY 3.0 — Map data © OpenStreetMap

Max. number of gateway for a single message: 84
Max. distance: 325 km