

**Workshop on LPWAN Solutions for the Internet of Things**  
**February 17-21 Makerere University, Kampala, Uganda**  
**Sebastian Büttrich (IT University of Copenhagen / NSRC)**

**Workshop on LPWAN Solutions for the Internet of Things**  
**February 17-21 Makerere University, Kampala, Uganda**  
**Sebastian Büttrich (IT University of Copenhagen / NSRC)**

# IoT – Internet of Things

within IoT

**LPWAN** – Low Power Wide Area Networks

one possible LPWAN: LoRaWAN

Physical Layer – LoRa

MAC Layer – LoRaWAN

one possible LoRaWAN: The Things Network

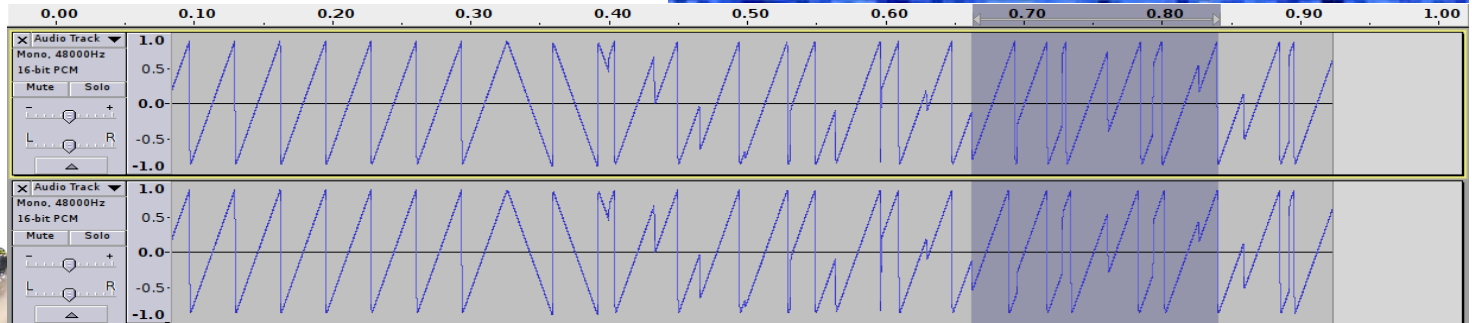
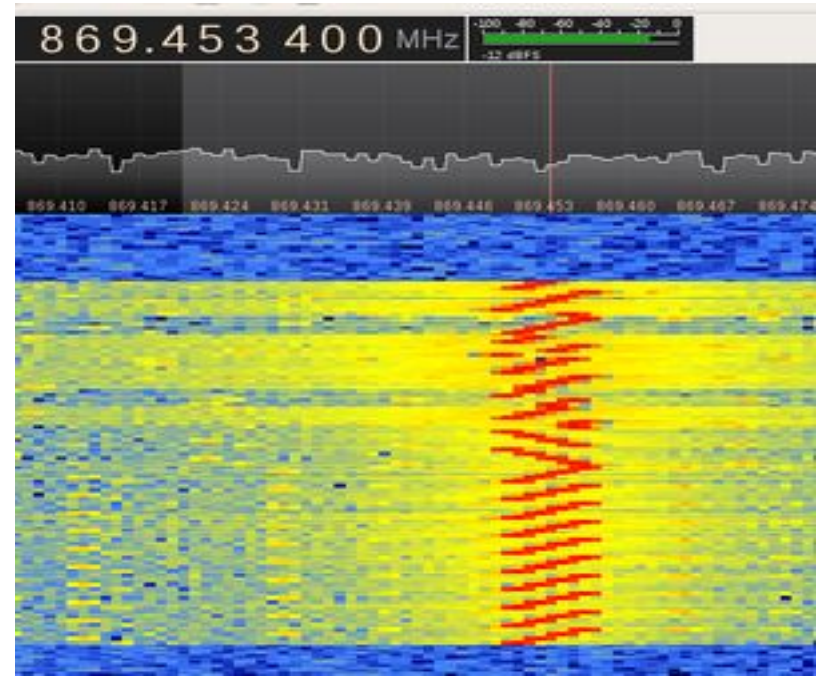


## LoRa

A proprietary radio technology,  
owned by Semtech,  
licensed to chip makers

### CSS Chirp Spread Spectrum

Often on **ISM bands** 868/915 & 433  
MHz, but not limited to those



# LoRa / recap / Spreading Factor SF

$$SF = \frac{\text{chip rate}}{\text{symbol rate}}$$

(think of it as “one bit is spread out over so and so many pulses” ... **one symbol =  $2^{SF}$** )

**Control rate CR, determines depth of forward error coding**

(Think of it as saying  
CCCAAFFFFEEE or CAFECAFECAFE  
instead of CAFE)

# LoRa / recap / Data Rate

**Data Rate depends on Bandwidth, CR, SF**

$$R_b = SF * \frac{\left[ \frac{4}{4+CR} \right]}{\left[ \frac{2^{SF}}{BW} \right]} * 1000$$

SF = Spreading Factor (6,7,8,9,10,11,12)

CR = Code Rate (1,2,3,4)

BW = Bandwidth in KHz  
(10.4,15.6,20.8,31.25,41.7,62.5,125,250,500)

Rb = Data rate or Bit Rate in bps

<http://www.rfwireless-world.com/calculators/LoRa-Data-Rate-Calculator.html>

# LoRaWan / 1

- LoRaWan is an open LPWAN standard, building on top of LoRa
- <https://www.lora-alliance.org/>



## LoRaWAN

An open specification, maintained by the LoRa-Alliance

**143** Countries with LoRaWAN® Deployments

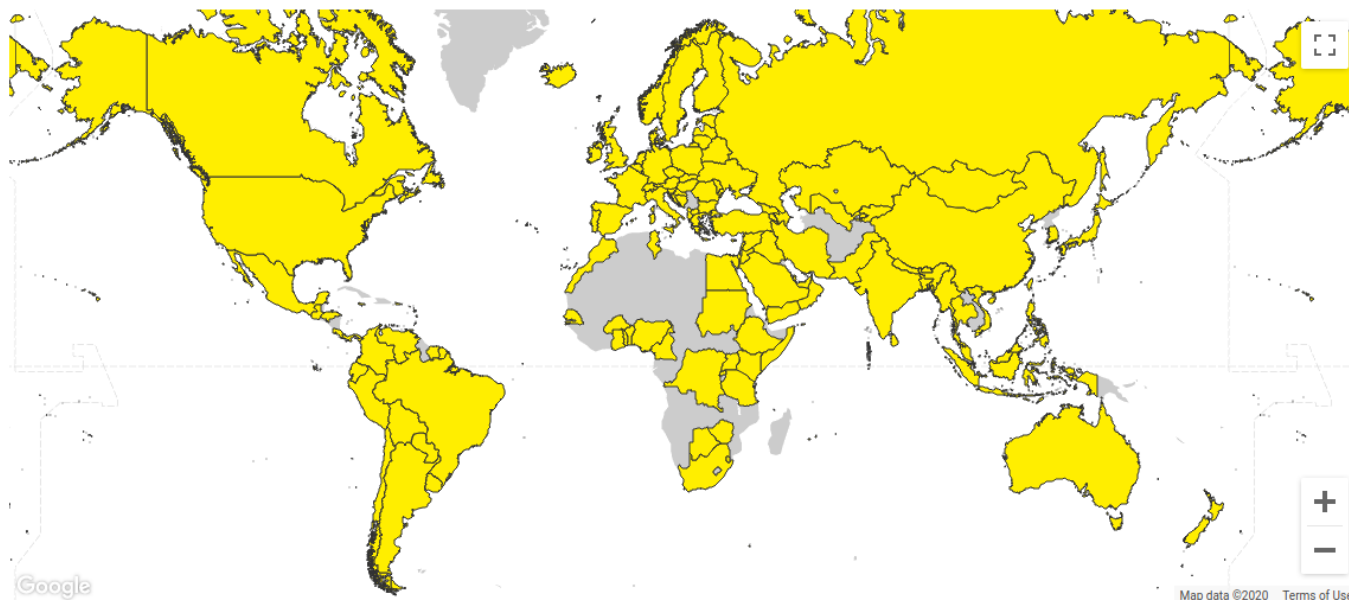
**133** Network Operators in 58 countries

**76** LoRa Alliance®  
Member Operators

LoRaWAN®  
Global Network Coverage

LoRaWAN®  
Public Network Operators

LoRaWAN®  
Open Community Networks





# LoRaWAN

A variety of commercial and community operators

**143** Countries with  
LoRaWAN® Deployments

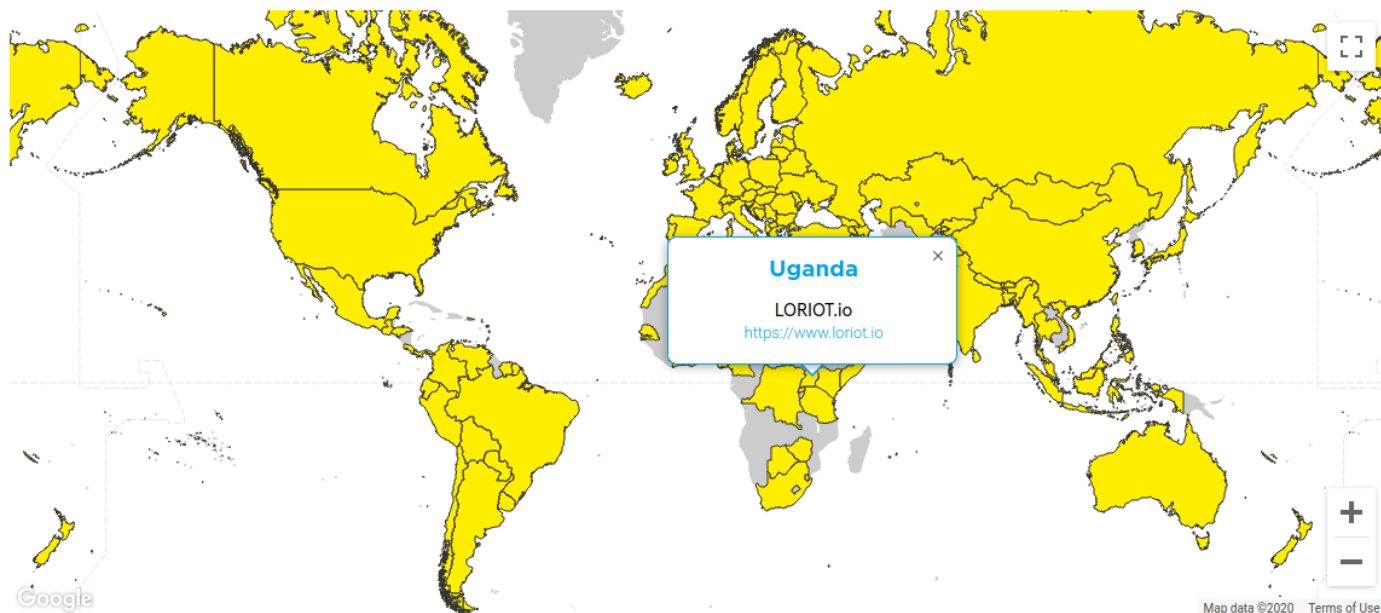
**133** Network Operators in  
58 countries

**76** LoRa Alliance®  
Member Operators

LoRaWAN®  
Global Network Coverage

LoRaWAN®  
Public Network Operators

LoRaWAN®  
Open Community Networks





## LoRaWAN specifies:

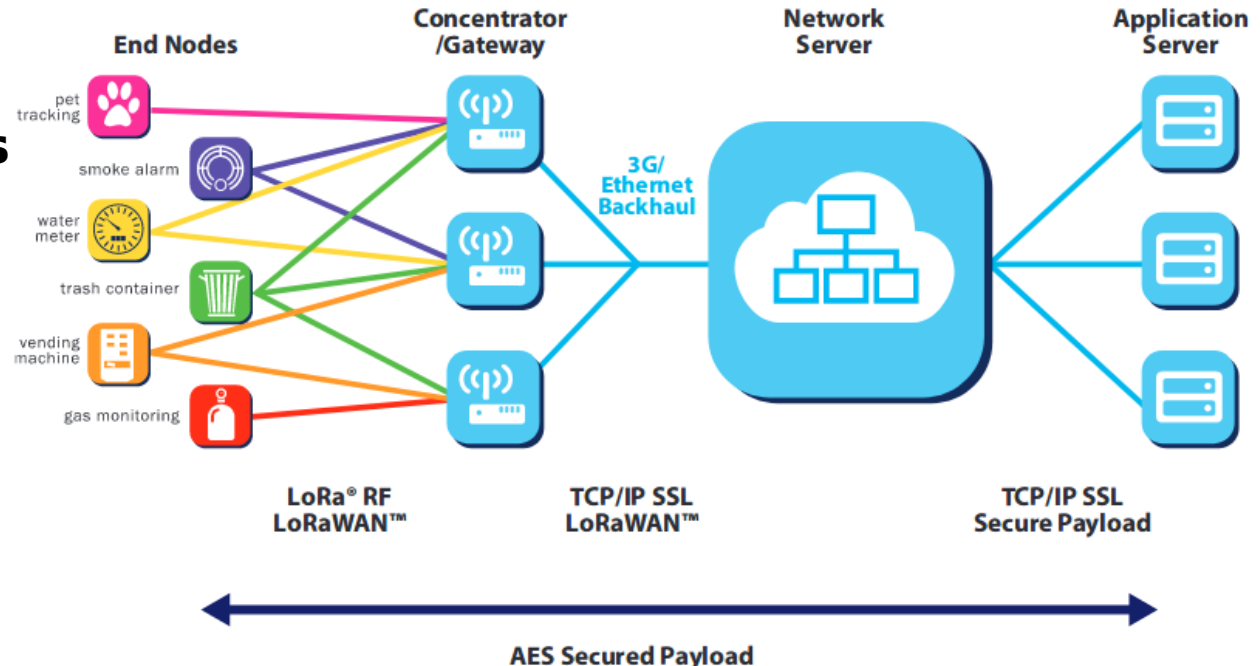
**Topology**

**Device Classes**

**Data Rates**

**Security**

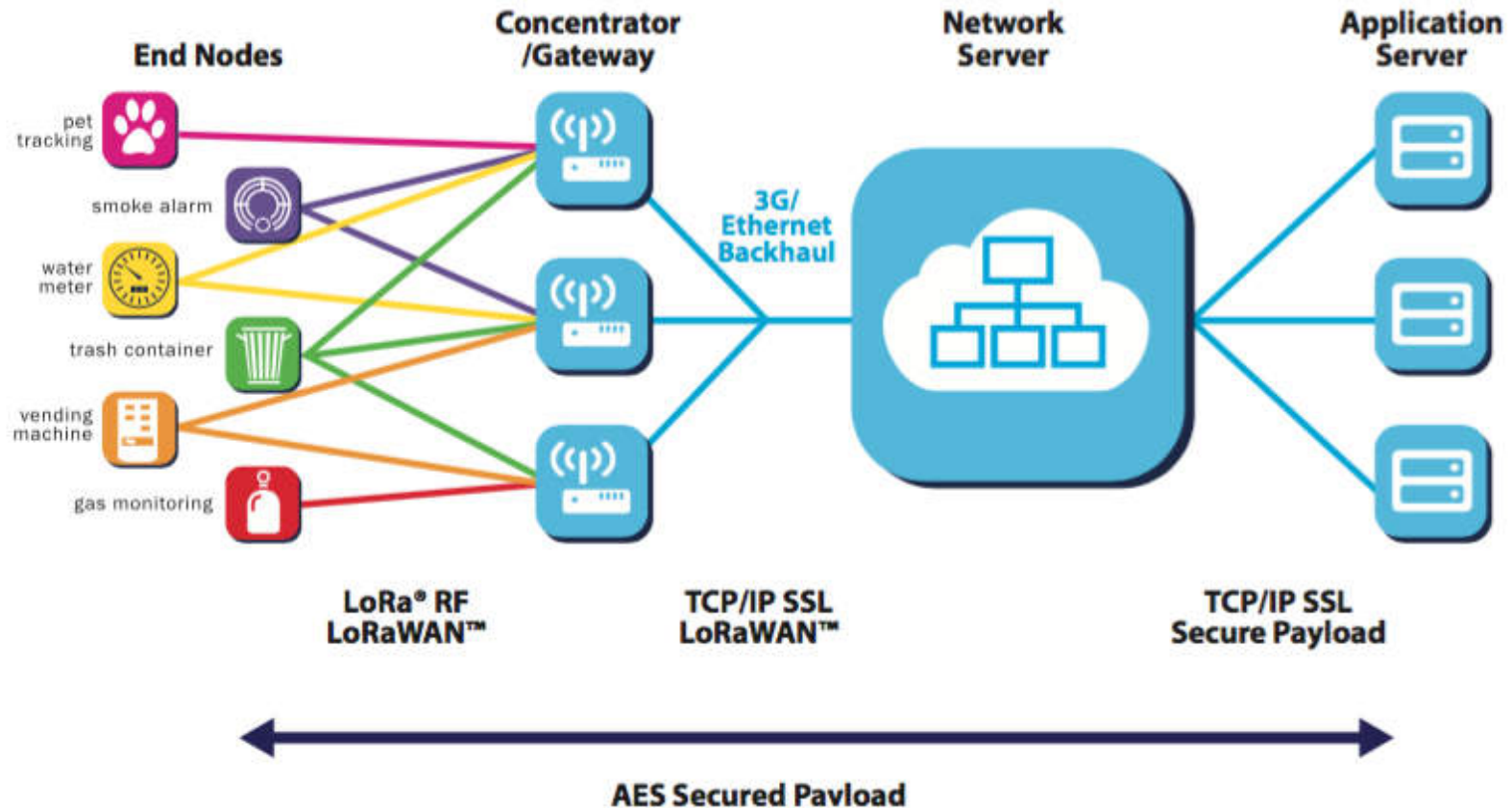
**Regional Info**



# LoRaWan / topologies & entities

- **Star-of-stars topology**
- **Gateways** are transparent bridges relaying messages between **end-devices** and a central **network server** in the backend.
- **Gateways are connected** to the network server via **standard IP connections** while end-devices use single-hop wireless communication to one or many gateways.
- All end-point communication generally **bi-directional**, supports **multicast** enabling **software upgrade over the air** or other mass distribution messages

# LoRaWan / architecture



# LoRaWan / device classes

## Device classes

**A** Battery powered, small loads, long breaks, long latency, unicast

**B** low latency, scheduled receive slots, periodic beacon from gateway, uni/multicast, higher power, 14-30 mA

**C** no latency, uni/multi, constantly receiving, power hungry

Classes can be dynamically assigned / changed

Source, Details:

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

# LoRaWan / addressing

## Devices and applications

**have a 64 bit / 8 byte unique identifier (DevEUI and AppEUI).**

**When a device joins the network, it receives a dynamic (non-unique) 32-bit / 4 byte address (DevAddr).**

Source, Details:

<https://www.thethingsnetwork.org/docs/lorawan/>

# LoRaWan / data rates

## LoRaWAN abstracts the PHY data rates of LoRa - for EU / CN:

- EU 863-870 MHz (LoRaWAN Specification (2015), Page 35, Table 14)
- CN 779-787 MHz (LoRaWAN Specification (2015), Page 44, Table 25)
- EU 433 MHz (LoRaWAN Specification (2015), Page 48, Table 31)

DataRate	Modulation	SF	BW	bit/s
0	LoRa	12	125	250
1	LoRa	11	125	440
2	LoRa	10	125	980
3	LoRa	9	125	1'760
4	LoRa	8	125	3'125
5	LoRa	7	125	5'470
6	LoRa	7	250	11'000
7	FSK 50 kbps			50'000

<https://blog.dbrgn.ch/2017/6/23/lorawan-data-rates/>

# LoRaWan / 11 / duty cycles

**LoRaWAN implements duty cycle rules made by regulators:**

In Europe, duty cycles are regulated by section 7.2.3 of the ETSI EN300.220 standard. This standard defines the following sub-bands and their duty cycles:

- g (863.0 – 868.0 MHz): 1%
- g1 (868.0 – 868.6 MHz): 1%
- g2 (868.7 – 869.2 MHz): 0.1%
- g3 (869.4 – 869.65 MHz): 10%
- g4 (869.7 – 870.0 MHz): 1%

+ duty cycle for join channel: 1%

On top of that, specific networks might have **fairplay rules**.





**THE THINGS**  
**N E T W O R K**



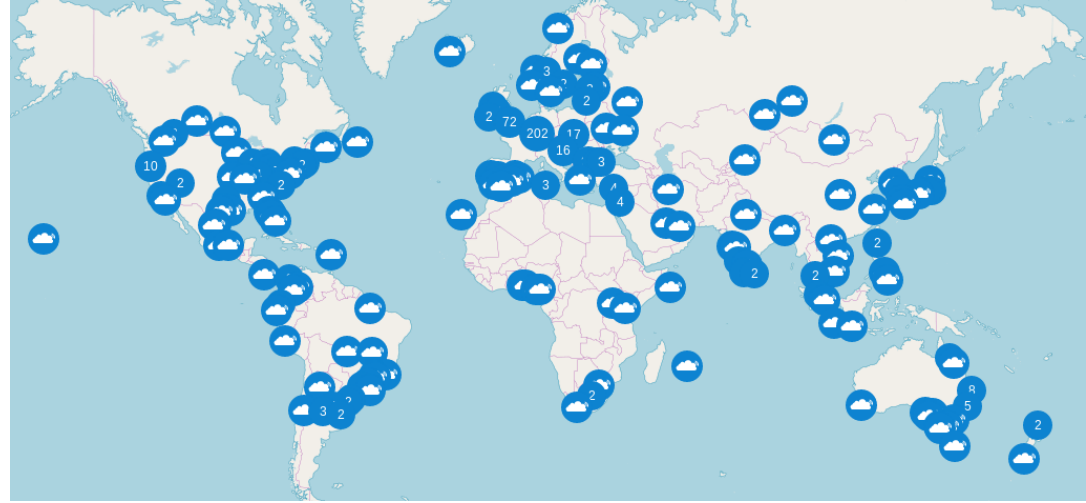
Our mission is to build a **DECENTRALIZED**,

**OPEN** and **CROWDSOURCED**

**INTERNET OF THINGS** data network

**OWNED** and **OPERATED** by its **USERS**

# The Things Network



**Anyone shall be **free** to set up "Things" and connect to "Things Gateways" that may or may not be their own.**

**Anyone shall be **free** to set up "Things Gateways" and connect to "Things Access" that may or may not be their own. Their "Things Gateways" will give [**free**] access to all "Things" in a net neutral manner, limited by the maximum available capacity alone.**

# The Things Network - Essentials



- Community project started in Netherlands, 2015
- Commercial side: The Things Industries
- Open source  *TheThingsNetwork/lorawan-stack* is licensed under the **Apache License 2.0**
- *This to some degree explains our current interest in TTN, in an educational context*
- **Great Learning resource:**  
**<https://www.thethingsnetwork.org/docs/>**

# The Things Network / Manifesto

**Everything that carries power will be connected to Internet eventually.**

**Controlling the network that makes this possible means controlling the world. We believe that this power should not be restricted to a few people, companies or nations. Instead this should be distributed over as many people as possible without the possibility to be taken away by anyone. We therefore founded "The Things Network".**

**The Things Network is an open source, free initiative with the following properties:**

**It connects sensors and actuators, called "Things", with transceivers called "Things Gateways" to servers called "Things Access".**

**The first connection is "Over The Air", the second is "Over The Net". The distributed implementation of these concepts is called "The Things Network".**

**Anyone shall be free to set up "Things" and connect to "Things Gateways" that may or may not be their own.**

**Anyone shall be free to set up "Things Gateways" and connect to "Things Access" that may or may not be their own. Their "Things Gateways" will give access to all "Things" in a net neutral manner, limited by the maximum available capacity alone.**

**Anyone shall be free to set up "Things Access" and allow anonymous connections from the Internet. Their "Things Access" will give access to all "Things Gateways" in a net neutral manner, limited by the maximum available capacity alone. Furthermore their "Things Access" will allow connection of other "Things Access" servers for the distribution of data.**

**The "Over The Air" and "Over The Net" networks shall be protocol agnostic, as long as these protocols are not proprietary, open source and free of rights.**

**Anyone who perpetrates a "Things Access" or a "Things Gateway" will do so free of charge for all connecting devices and servers.**

**Anyone making use of the network is allowed to do so for any reason or cause, possibly limited by local law, fully at own risk and realizing that services are provided "as is" and may be terminated for any reason at any moment. The use may be open for anybody, limited to customers, commercial, not-for-profit, or in any other fashion. "The Things Network" providers will not pose restrictions upon its users.**

**We invite you to sign this Manifesto, and uphold its principles to the best of your abilities.**

Source, Details:

<https://www.thingsnetwork.io/manifesto>

# THE OPEN, COLLABORATIVE NETWORK

---



**70K**

DEVELOPERS



**15M**

PACKETS ROUTED  
EVERY DAY



**100**

COUNTRIES



**950**

CITIES



**7K**

GATEWAYS

BUT THAT WAS 2019 ...

# THE OPEN, COLLABORATIVE NETWORK 2020:



**100K**

DEVELOPERS



**? M**

PACKETS ROUTED  
EVERY DAY



**149**

COUNTRIES



CITIES



**>10k**

GATEWAYS



At this moment, there are 10619 gateways up and running

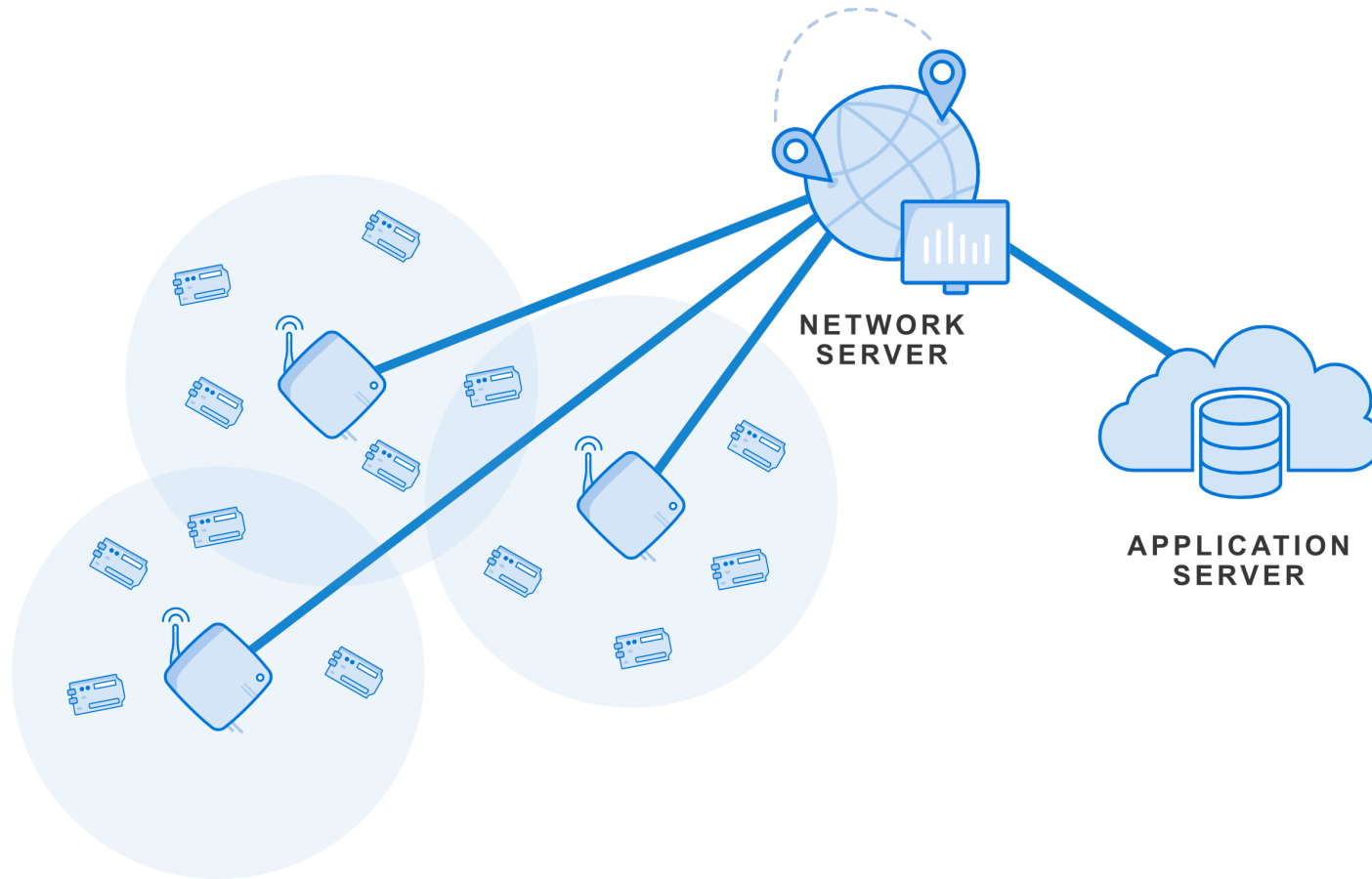






Leaflet | © OpenStreetMap contributors

# The Things Network / Simplified



## IT UNIVERSITY OF COPENHAGEN



# The Things Network / Security / Keys

Security features defined by **LoRaWAN standard**:

**Three keys: NwkSKey, AppSKey and AppKey**

AES-128 bit keys

**Challenge of key provision!**

# LoRaWan / Security / keys

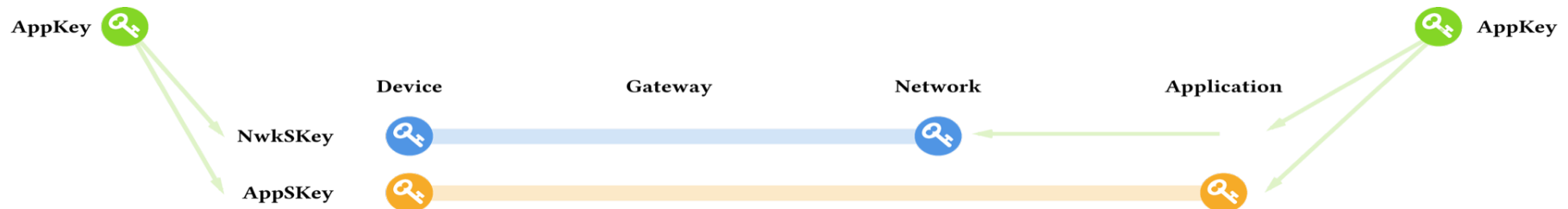
## Security measures:

three distinct 128-bit AES keys:

The **application key AppKey** is only known by the device and by the application. When a device joins the network (this is called a join or activation), an application session key **AppSKey** and a network session key **NwkSKey** are generated. The NwkSKey is shared with the network, while the AppSKey is kept private.

Source, Details:

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





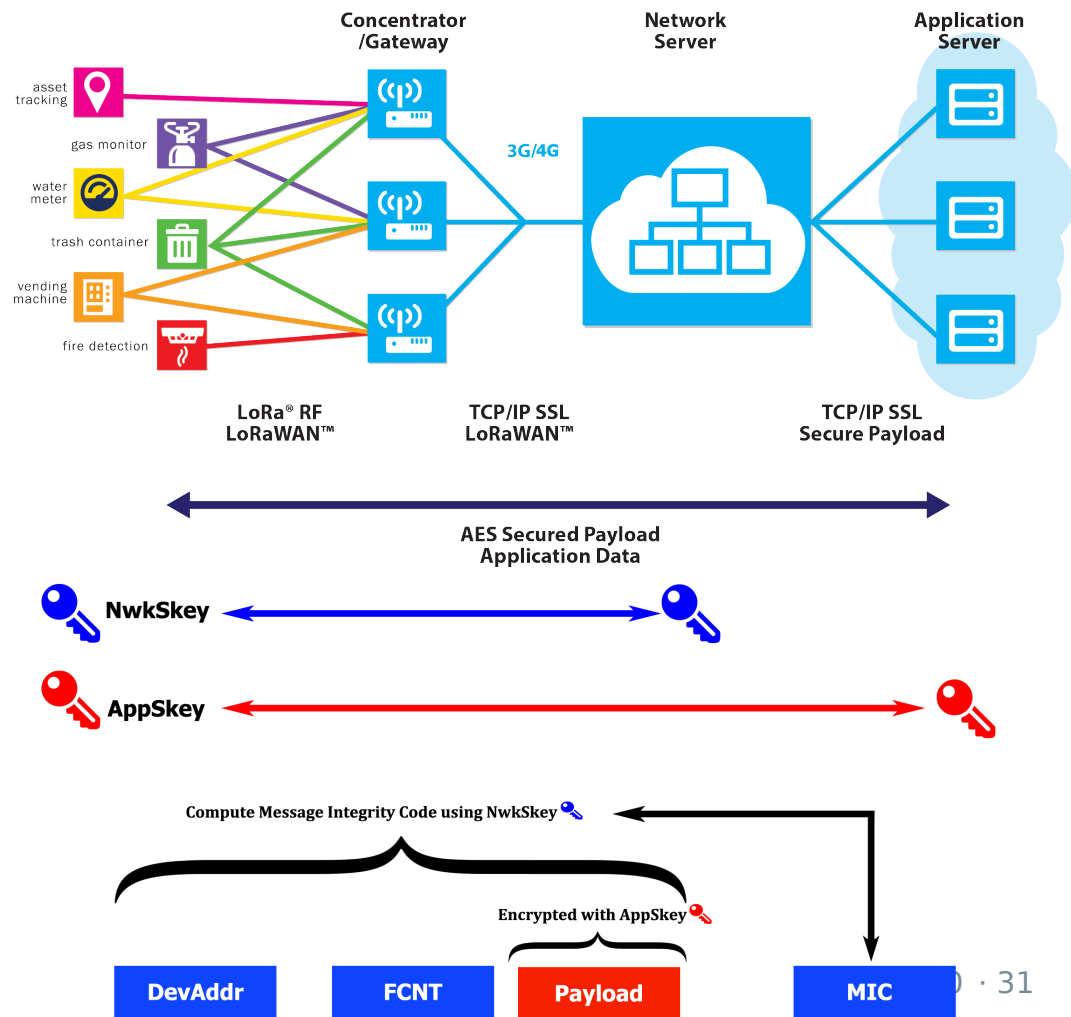
# The Things Network / Security, cntd

LoRaWAN 1.0 specifies a number of security keys: **NwkSKey**, **AppSKey** and **AppKey**. All keys have a length of 128 bits.

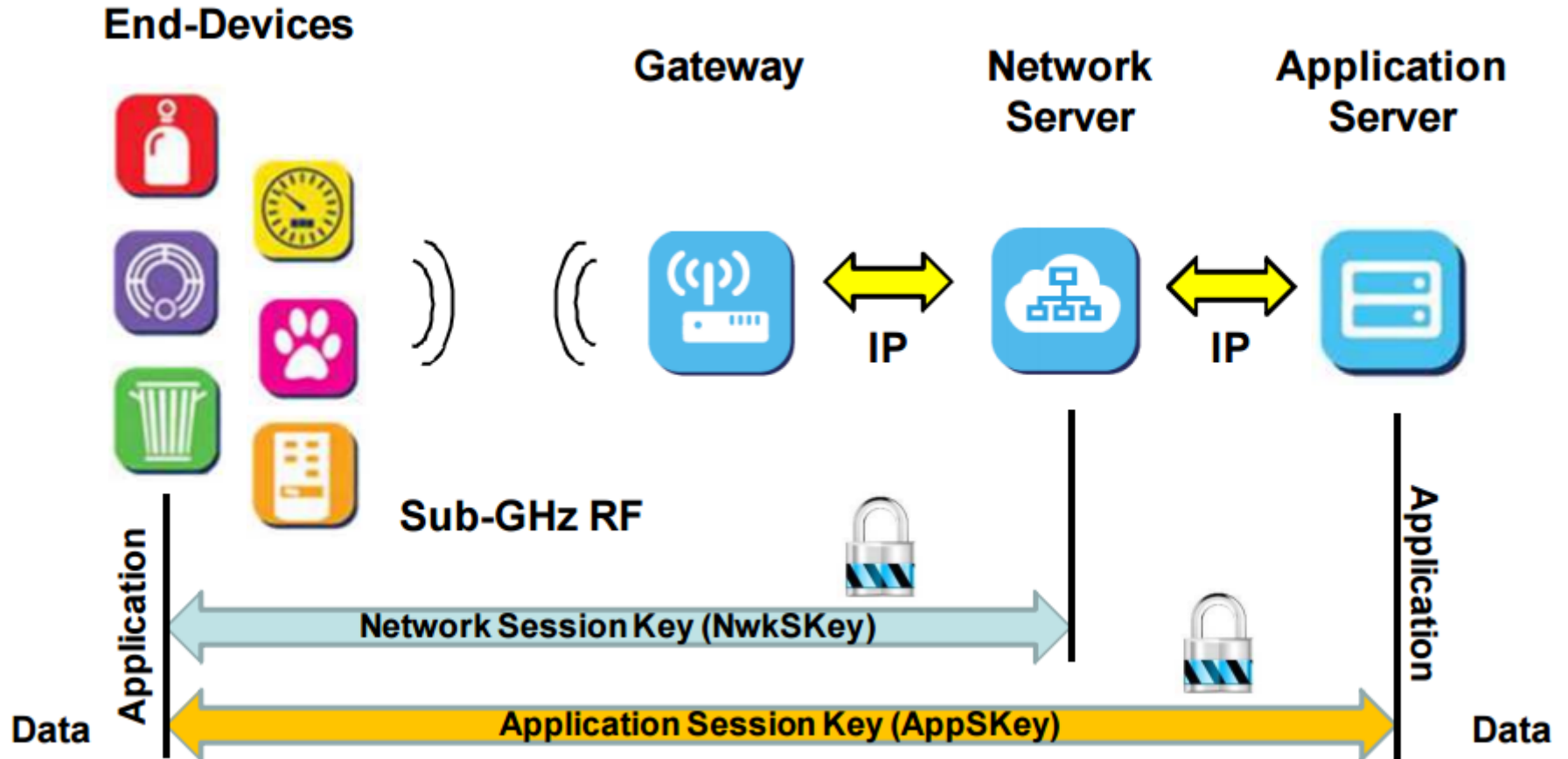
The **Network Session Key** ( **NwkSKey** ) is used for interaction between the Node and the Network Server. This key is used to check the validity of messages (MIC check). In the backend of The Things Network this validation is also used to map a non-unique device address ( **DevAddr** ) to a unique **DevEUI** and **AppEUI**.

The **Application Session Key** ( **AppSKey** ) is used for encryption and decryption of the payload. The payload is fully encrypted between the Node and the Handler/Application Server component of The Things Network (which you will be able to run on your own server). This means that nobody except you is able to read the contents of messages you send or receive.

# The Things Network / Security, cntd



# The Things Network / Security, cntd



# LoRaWan / Security / frame counter

The **frame counter in LoRaWAN** messages is a security measure used to detect **replay attacks**. After validating the MIC, the Broker checks if the Frame counter is valid. As frame counters can only increase, a message with a frame counter that is lower than the last known frame counter should be dropped. Additionally, the Broker has to verify that the gap between the last known frame counter and the counter in the message is not too big. According to the LoRaWAN specification, the maximum gap is 16384.

Source, Details:

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

# The Things Network / Security / Activation

## Two ways of activating a device:

### **OTAA Over the Air Activation**

Interactive, Join request and answer

### **ABP Activation by Personalization**

Hard coded credentials for session

# The Things Network / Security / OTAA

Dynamically activated devices (**OTAA**) use the application key (AppKey) to derive the two session keys during the activation procedure. In The Things Network you can have a default AppKey which will be used to activate all devices, or customize the AppKey per device.

What you will use, in your code:

**DevEUI, AppEUI, AppKey**

Keys will be generated on TTN server, on registration  
(but can be changed manually)

Source, Details: <https://www.thethingsnetwork.org/wiki/LoRaWAN/Security>

# The Things Network / Security / ABP

## ABP Activation by Personalization

What you will use, in your code:

**NwkSKey, AppSKey, DevAddr**

Source, Details:

<https://www.thethingsnetwork.org/wiki/LoRaWAN/Security>



# Working with The Things Network Console

## We have applications (and devices) and gateways

 **Hi, Sebastian!**

Welcome to The Things Network Console.

This is where the magic happens. Here you can work with your data. Register applications, devices and gateways, manage your integrations, collaborators and settings.



**APPLICATIONS**



**GATEWAYS**

# Working with The Things Network Console

Applications > Add Application

## We create applications

### ADD APPLICATION

#### Application ID

The unique identifier of your application on the network

uganda-workshop-2020



#### Description

A human readable description of your new app

Test application for the workshop



#### Application EUI

An application EUI will be issued for The Things Network block for convenience, you can add your own in the application settings page.

EUI issued by The Things Network

#### Handler registration

Select the handler you want to register this application to

ttn-handler-asia-se




Cancel

Add application

# Working with The Things Network Console

Applications >

 uganda-workshop-2020

## APPLICATION OVERVIEW

[documentation](#)


Application ID **uganda-workshop-2020**



Description Test application for the workshop

Created 1 minute ago

Handler ttn-handler-asia-se (current handler)

## APPLICATION EUIs

 [manage euis](#)

<>  70 B3 D5 7E D0 02 AA A0 

## In our applications, we create devices

## DEVICES


 [register device](#)

 [manage devices](#)



0 registered devices

# Working with The Things Network Console

Applications >  uganda-workshop-2020 > Devices

## A new device

Overview

Devices

Payload Formats

Integrations

Data

Settings

### REGISTER DEVICE

[bulk import devices](#)

#### Device ID

This is the unique identifier for the device in this app. The device ID will be immutable.

#### Device EUI


The device EUI is the unique identifier for this device on the network. You can change the EUI later.



0 bytes

#### App Key

The App Key will be used to secure the communication between you device and the network.



this field will be generated

#### App EUI

⌵

# Working with The Things Network Console

Gateways > Register

## A new gateway

### REGISTER GATEWAY

#### Gateway ID

A unique, human-readable identifier for your gateway. It can be anything so be creative!

uganda-test-indoors

☐ I'm using the legacy packet forwarder

Select this if you are using the legacy [Semtech packet forwarder](#).

#### Description

A human-readable description of the gateway

our first indoor gateway

#### Frequency Plan

The [frequency plan](#) this gateway will use

Europe 868MHz

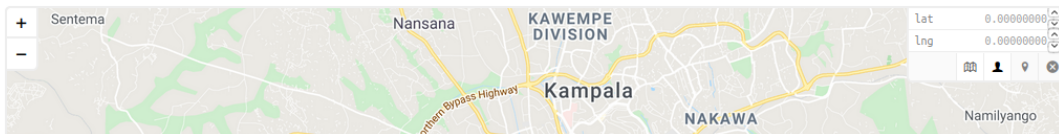
#### Router

The router this gateway will connect to. To reduce latency, pick a router that is in a region which is close to the location of the gateway.

ttn-router-eu

#### Location

The exact location of you gateway. This will be used if your gateway cannot determine its location by itself. Set a location by clicking on the map.



# Labs

- 1/ Sign on to  
<https://thethingsnetwork.org>
- 2/ Look around
- 3/ Let us know your username
- 4/ **We build and share gateways**
- 5/ Create applications
- 6/ Register devices (your LoPys)
- 7/ See the data flow!