Example Presentation

Pentesting Department

David Lassig

10.August 2018

Inhaltsübersicht

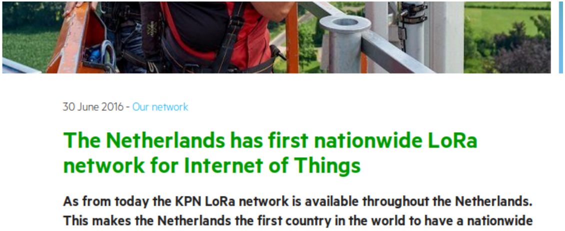
1 Idee

2 LoRaWan101

3 Umsetzung

4 Ausblick

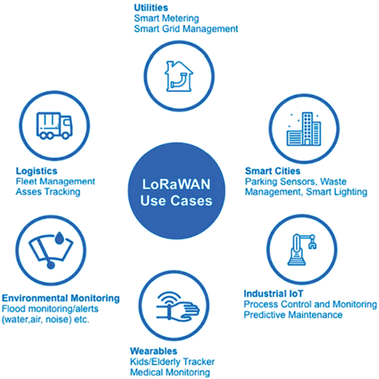
Initiator



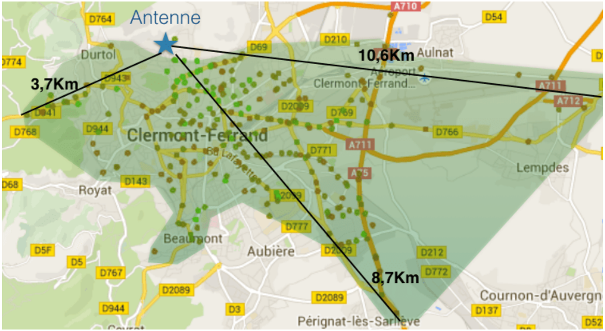
30 June 2016 - Our network

The Netherlands has first nationwide LoRa network for Internet of Things

As from today the KPN LoRa network is available throughout the Netherlands. This makes the Netherlands the first country in the world to have a nationwide



Anwendungsmöglichkeiten für LoRaWAN



Beispiel Reichweite einzelner Gateway Antenne

Inhaltsübersicht

1 Idee

2 LoRaWan101

3 Umsetzung

4 Ausblick

Was ist LORA?

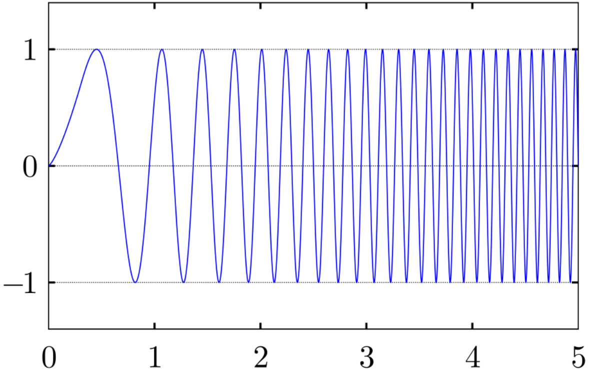
Funkgebundene Modulation zur Kommunikationsverbindung über Langstrecke in LPWAN[1] (Layer 1) zur Optimierung von

- Batterielebensdauer
- Robustheit
- Entfernung
- Kosten

[1] Low-Power, Wide-Area-Network

Modulation

- LoRa benutzt CSS für robuste Übertragung.



Beispiel eines Chirps

Inhaltsübersicht

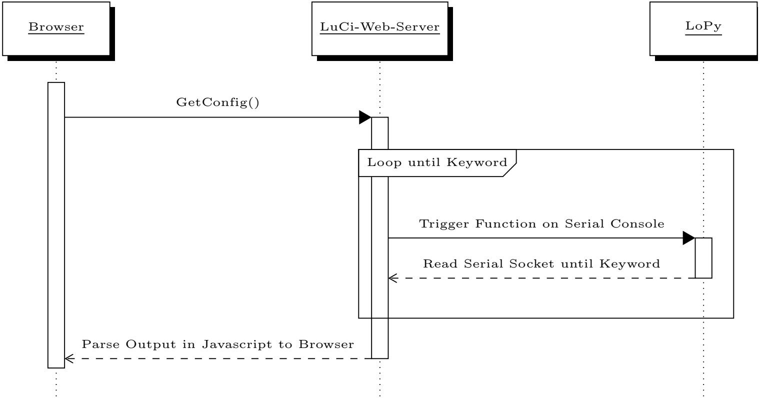
1 Idee

2 LoRaWan101

3 Umsetzung

4 Ausblick

Architecture


Browser
LuCi-Web-Server
LoPy
GetConfig()
Loop until Keyword
Trigger Function on Serial Console
Read Serial Socket until Keyword
Parse Output in Javascript to Browser

Set up RX

```
def set_up_rx(self):

    if not self.create_lora():
        self.pdeb("Lora Socket failed")
    else:
        self.pdeb("Lora Socket Raw RX succesfully created")
        if self.basemode == "master":
            self.s.settimeout(10)
    time.sleep(1)
```

Receive Mode

```
def receive_mode(self):
    try:
        msg = ""
        self.set_up_rx()
        while(True):
            result = self.receive()
            if result == 2: # receive part
                msg += self.msg
                self.send("ack",self.cb_output_payload)
                time.sleep(1)
            if result == 1: #receive finish
                msg += self.msg
                self.out_msg(msg,self.last_device_id)
                self.send("ack",self.cb_output_payload)
                time.sleep(1)
                self.mode = "tx"
                time.sleep(1)
                break
            if result == 0: # wrong device_id
                self.pdeb("Not our cup of tea")
                time.sleep(1)
                break
    except socket.timeout:
        self.pdeb("Master got Receiver Timeout, changing back to TX")
        self.mode = "tx"
```

Inhaltsübersicht

1 Idee

2 LoRaWan101

3 Umsetzung

4 Ausblick

ToDo

- “Protokollhärtung” - Wiederholtes Senden von Paketen
- Datenhaltung und Auswertung im Webserver
- Wechsel auf andere Hardwareplattform (Dragino)
- Wechsel auf andere Modulation ???