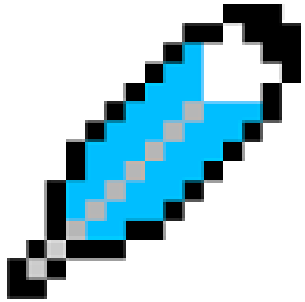


Example Presentation

Pentesting Department

David Lassig

10.August 2018

Idee

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

Figure 1: Anwendungsmöglichkeiten für LoRaWAN

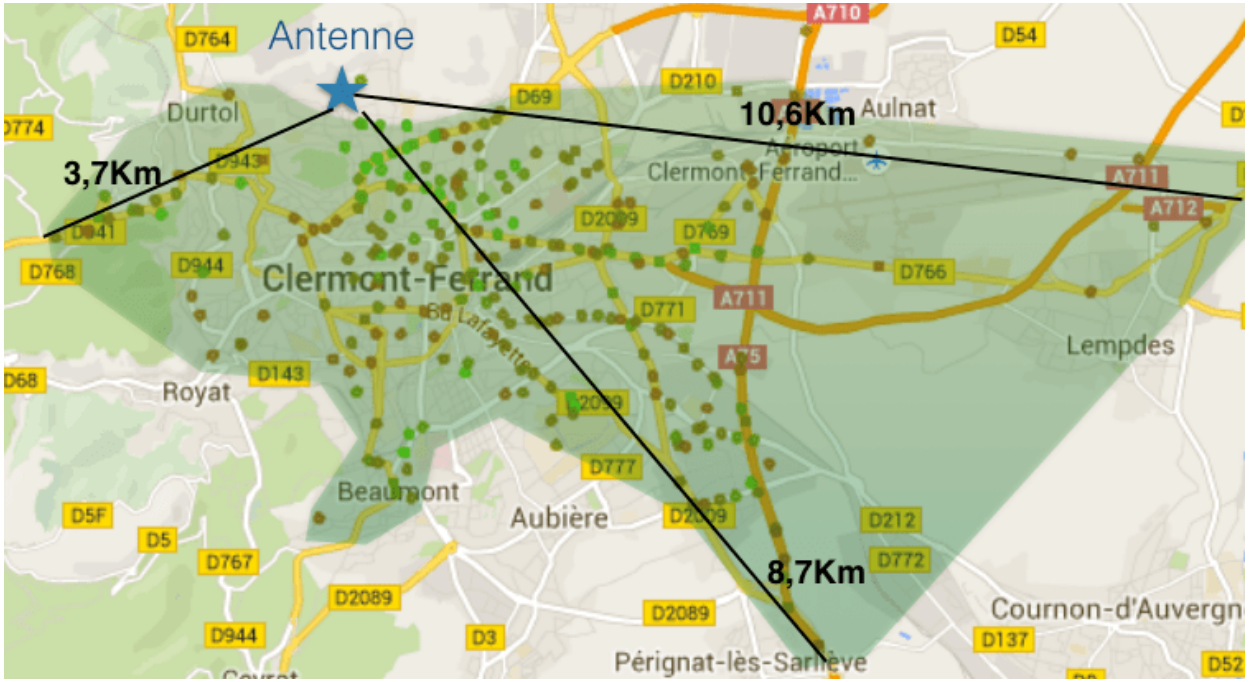


Figure 2: Beispiel Reichweite einzelner Gateway Antenne

LoRaWan101

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.

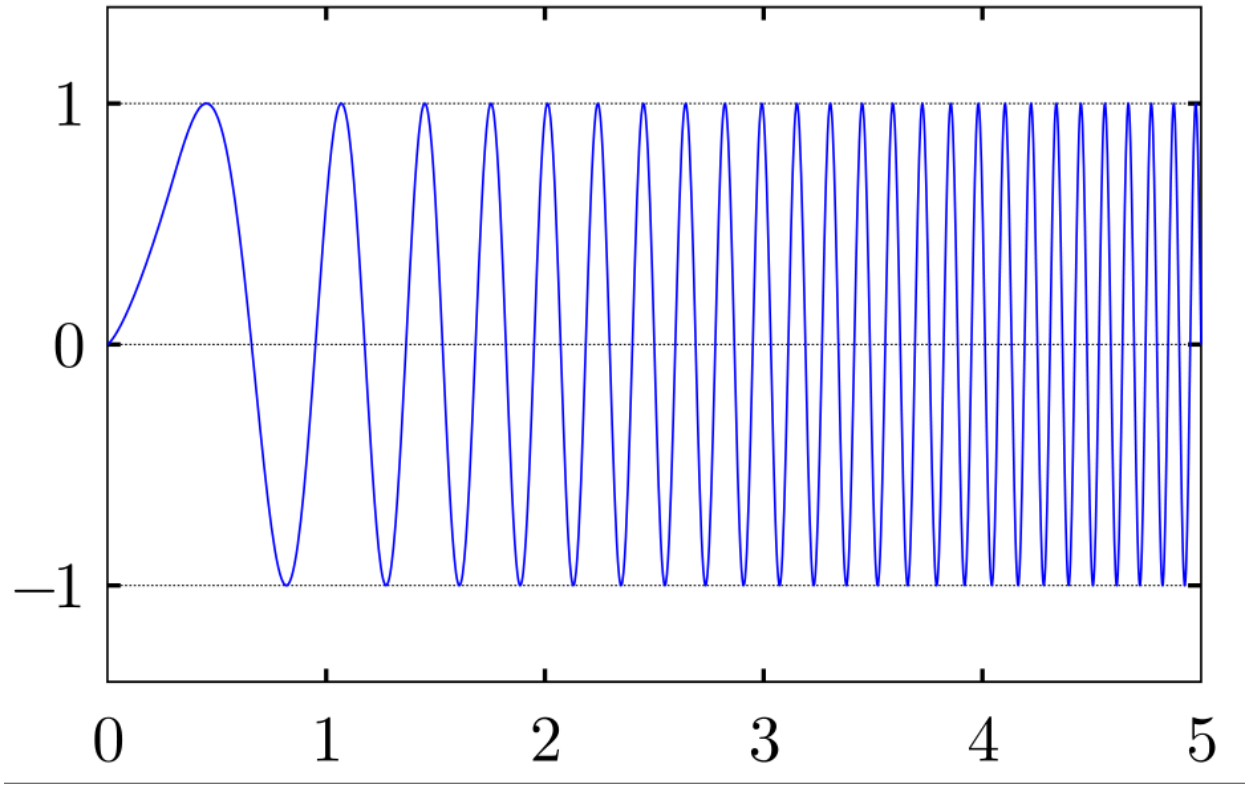
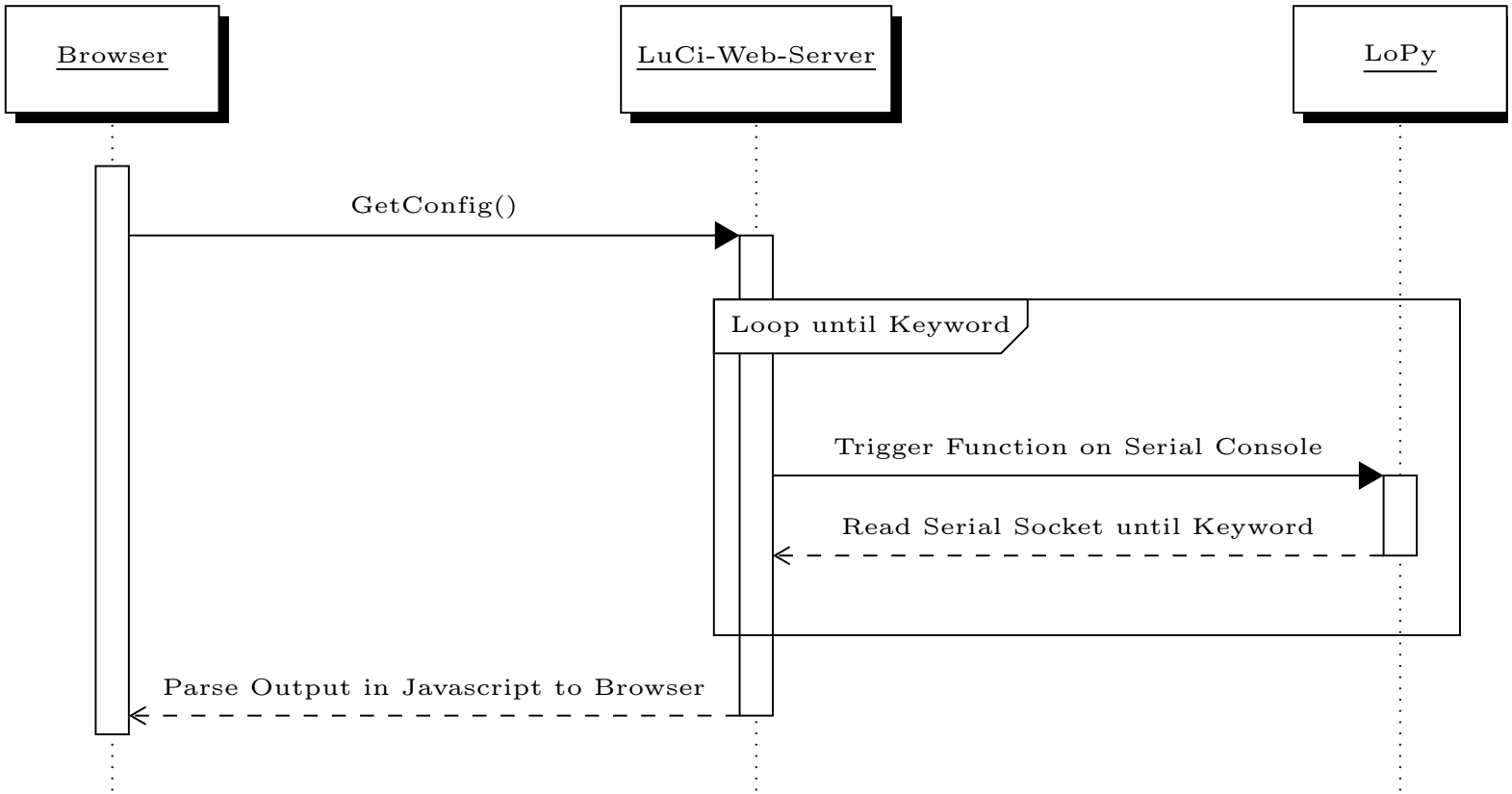


Figure 3: Beispiel eines Chirps

Umsetzung

Architecture



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)
```

Ausblick

ToDo

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