Universität Rostock

Traditio et Innovatio

Sicherheit bei LoRaWAN

Thomas Mundt
Universität Rostock

LoRaWAN

- Netzwerk für IoT-Technik.
- Stromsparend - Mobiles Geräte kann sehr selten aktiviert werden.
- Hohe Reichweite.
- Billig.
- Alternative beispielsweise zu NarrowBand-IoT oder LTE-M.

LoRaWAN Reichweite

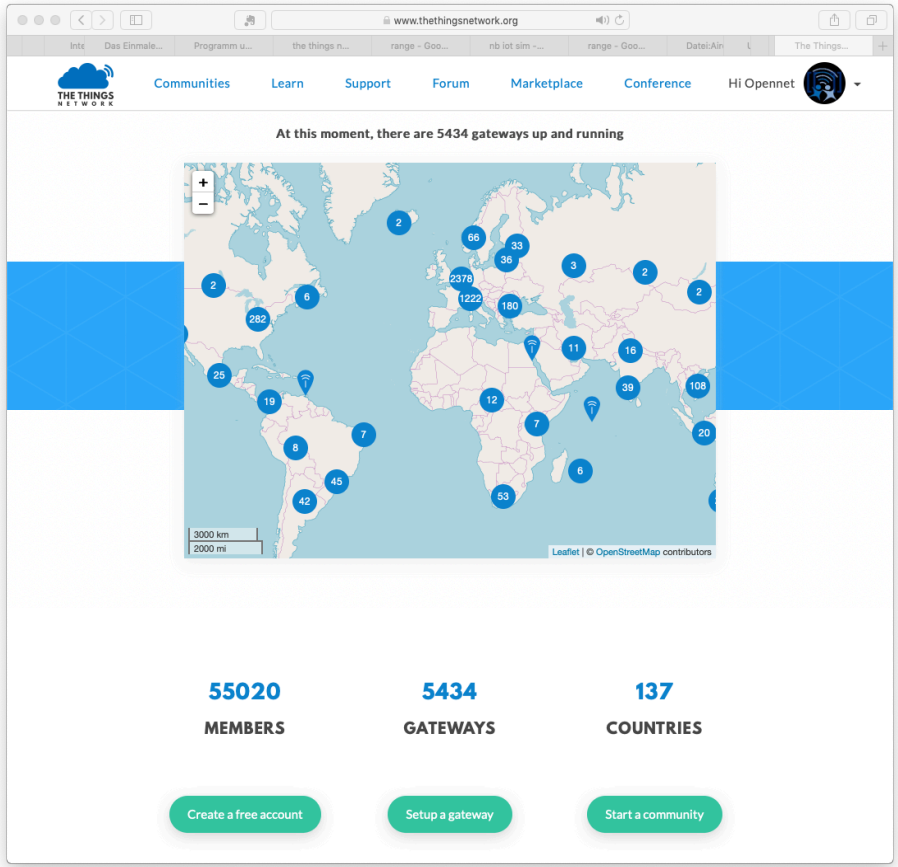
- Über 10km sind Mythos.
- In Städten typisch 2km.
- Über Land bis 10km.

LoRa - Der Physical Layer

- Chirp Modulation.
- Patentiert.
- Nicht öffentlich.
- Semtech Corp. kontrolliert den Markt. Wenige verschiedene ICs verfügbar.

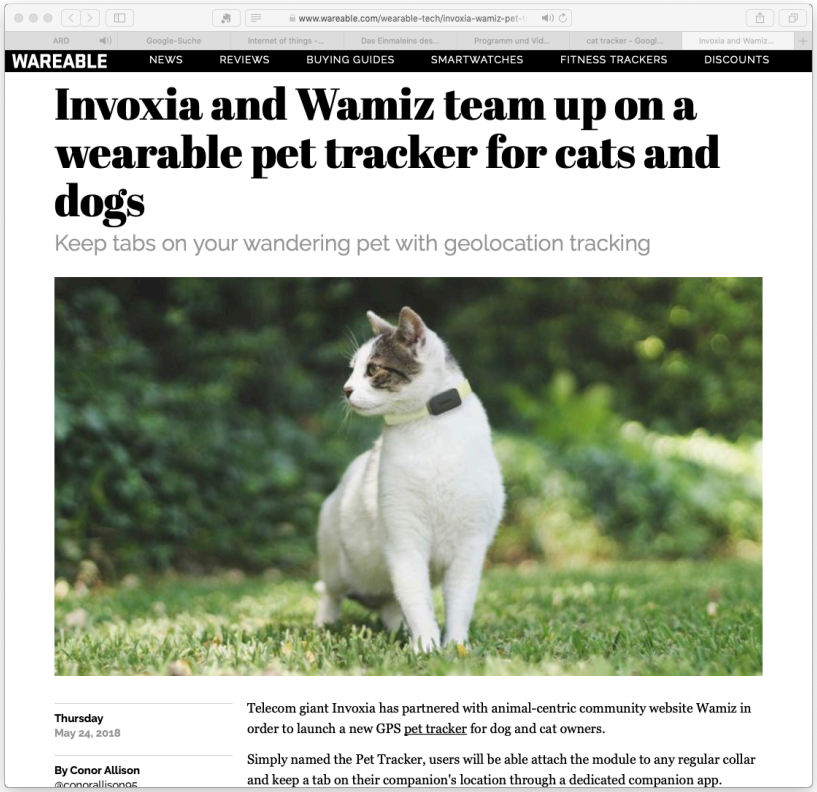
LoRaWAN

- Viele kommerzielle Netzwerkanbieter setzen auf LoRaWAN.
- Auch Community Netze global verfügbar.



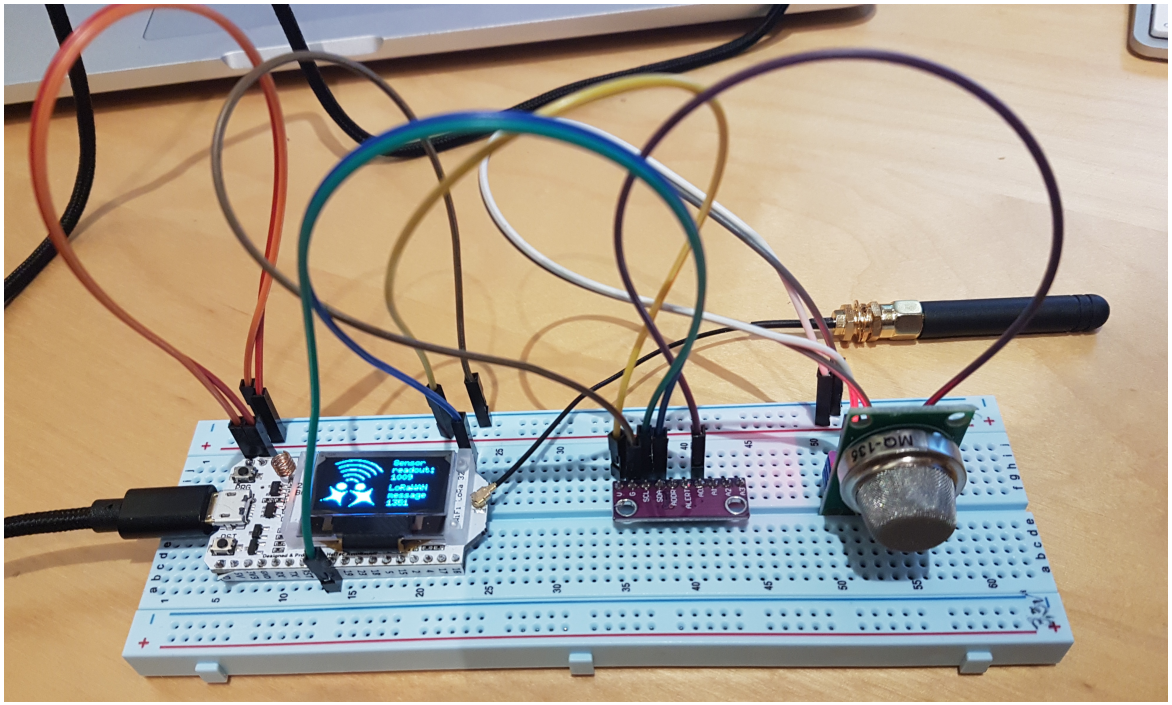
LoRaWAN Anwendungen

- IoT Sensoren und Aktoren können vielseitig eingesetzt werden.
  - Smart Cities, alles von "Katzen orten" bis "Auto wiederfinden"
  - Smart Home Anwendungen
  - Landwirtschaft
  - Überwachung / Tracker



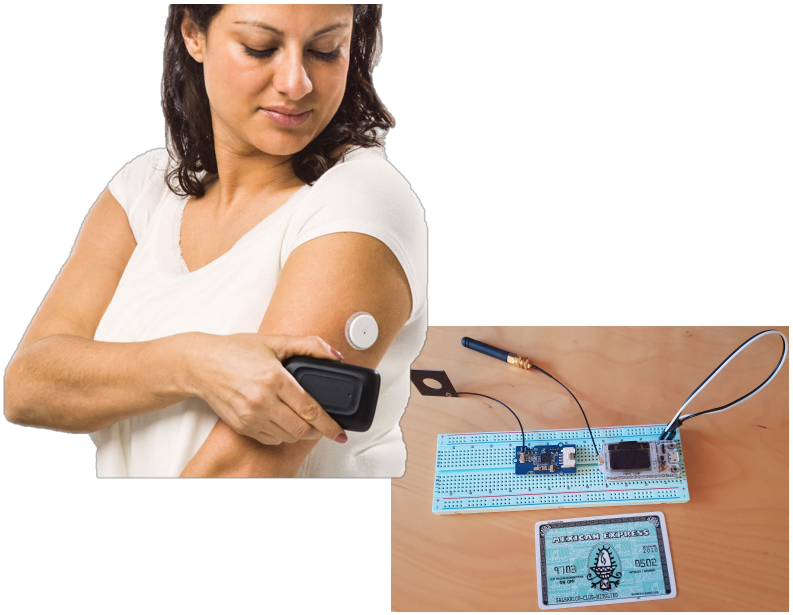
LoRaWAN Anwendungen

- Große Anzahl von Developer Boards verfügbar.
- Per Allgemeinzuteilung lizensiert.
- Verschiedene Frequenzen standardisiert.



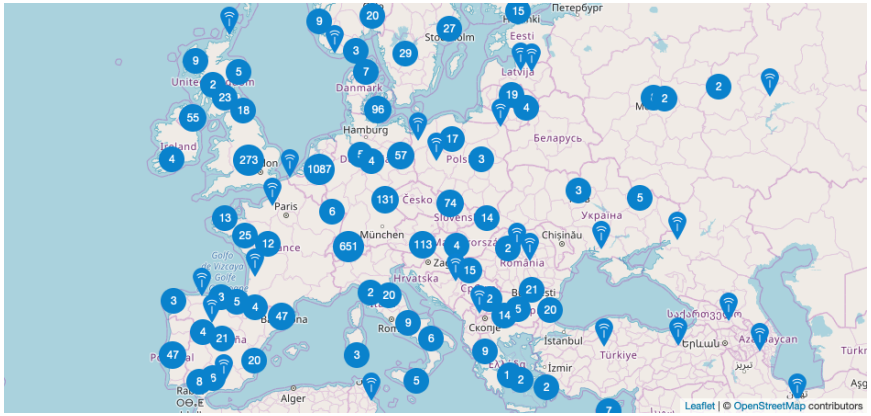
Mögliche Anwendung

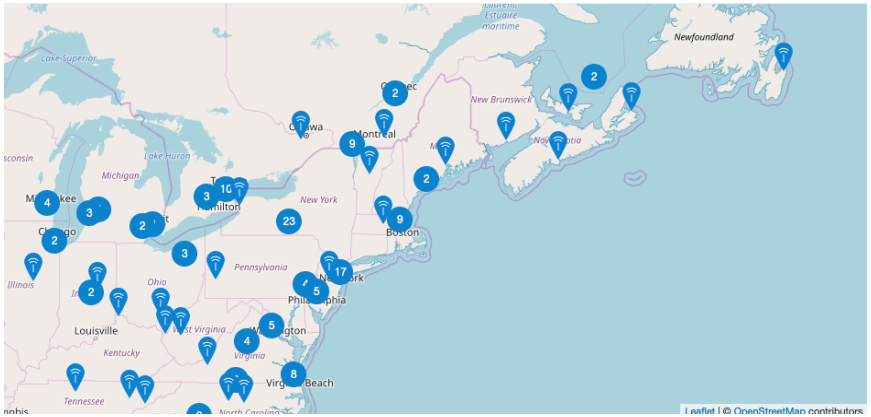
- Sicherheit ist bei bestimmten Daten besonders relevant.
- Sicherheit ist relevant, wenn Aktoren gesteuert werden können.



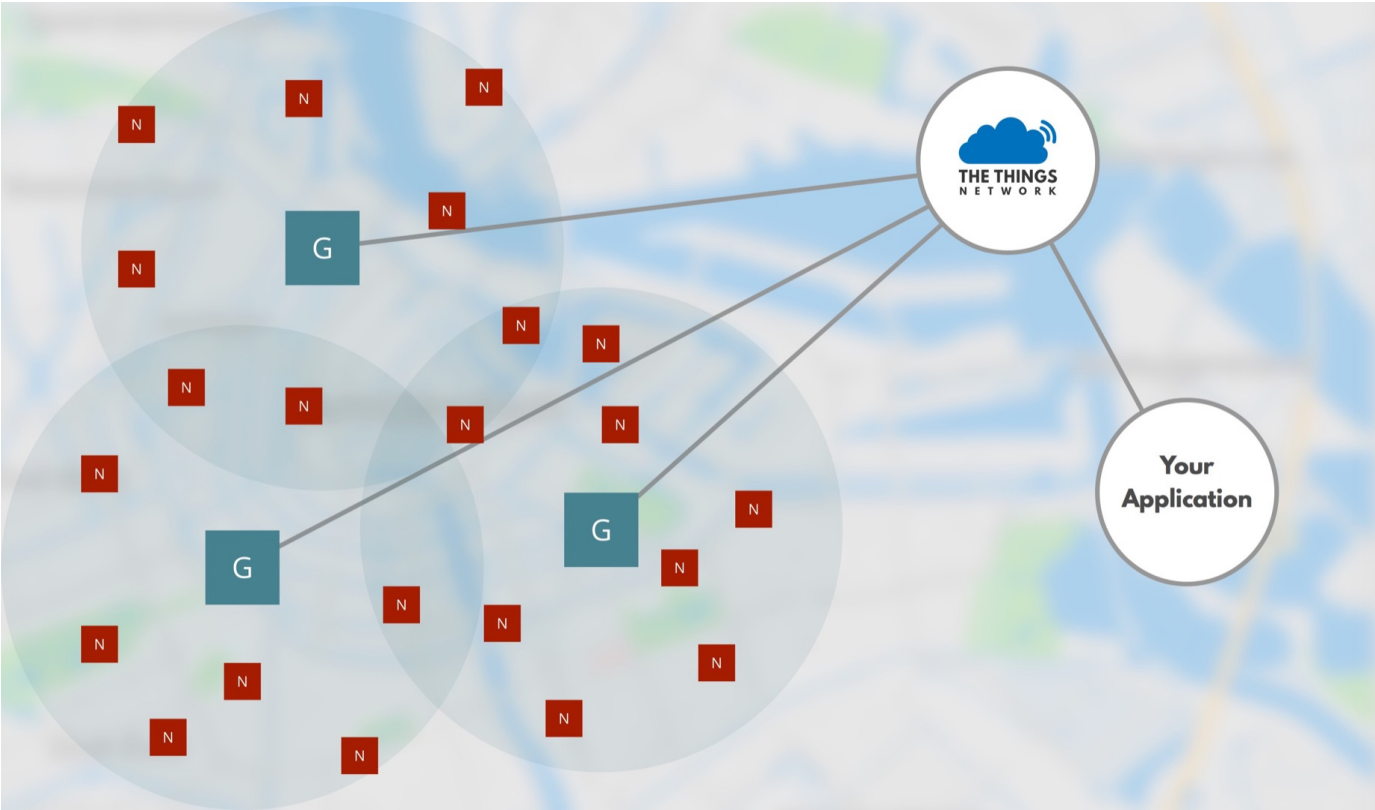
The Things Network

- LoRaWAN ist weltweit im Einsatz.
- The Things Network ist ein Community-Netzwerk, bei dem jedermann ein Radio Gateway aufstellen kann.

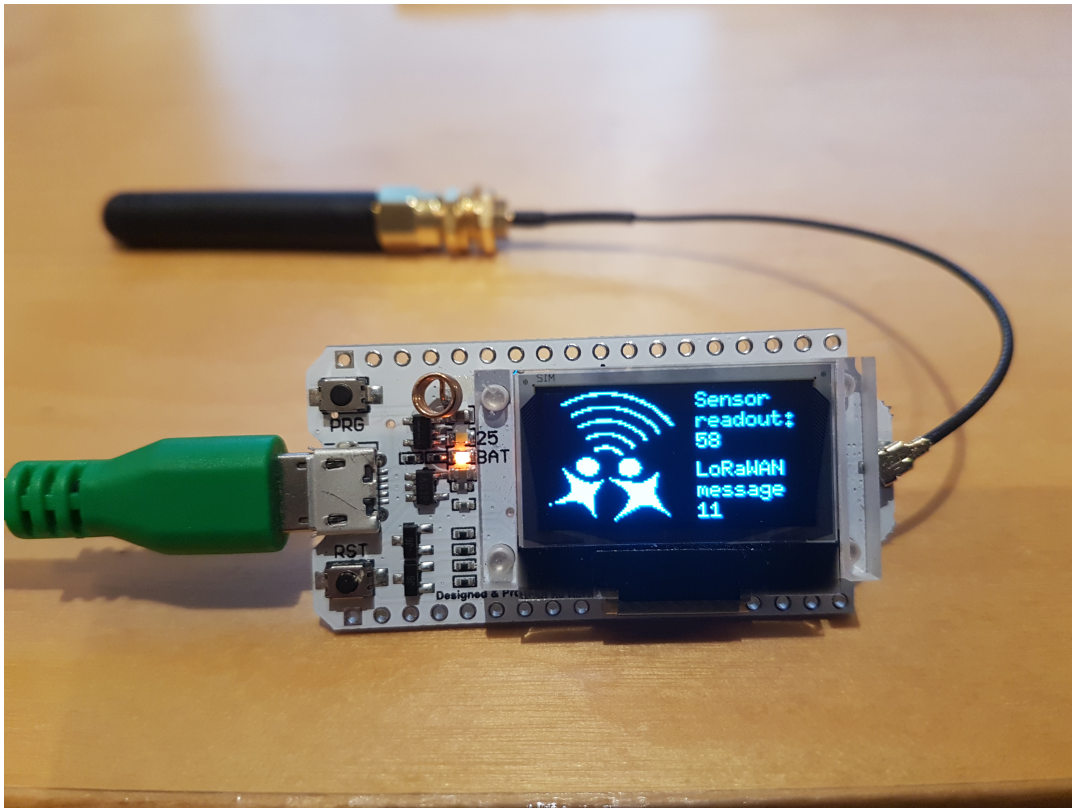


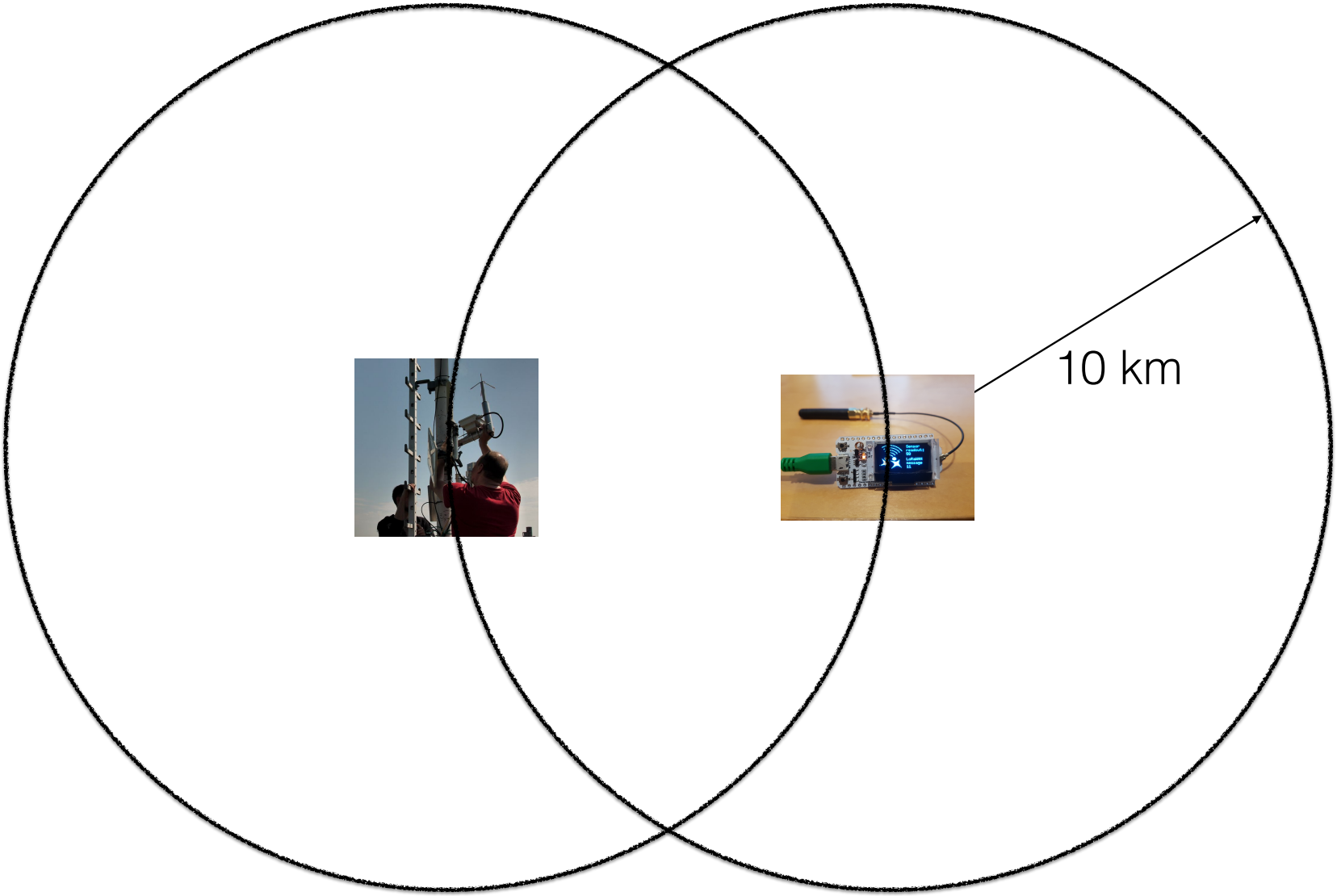


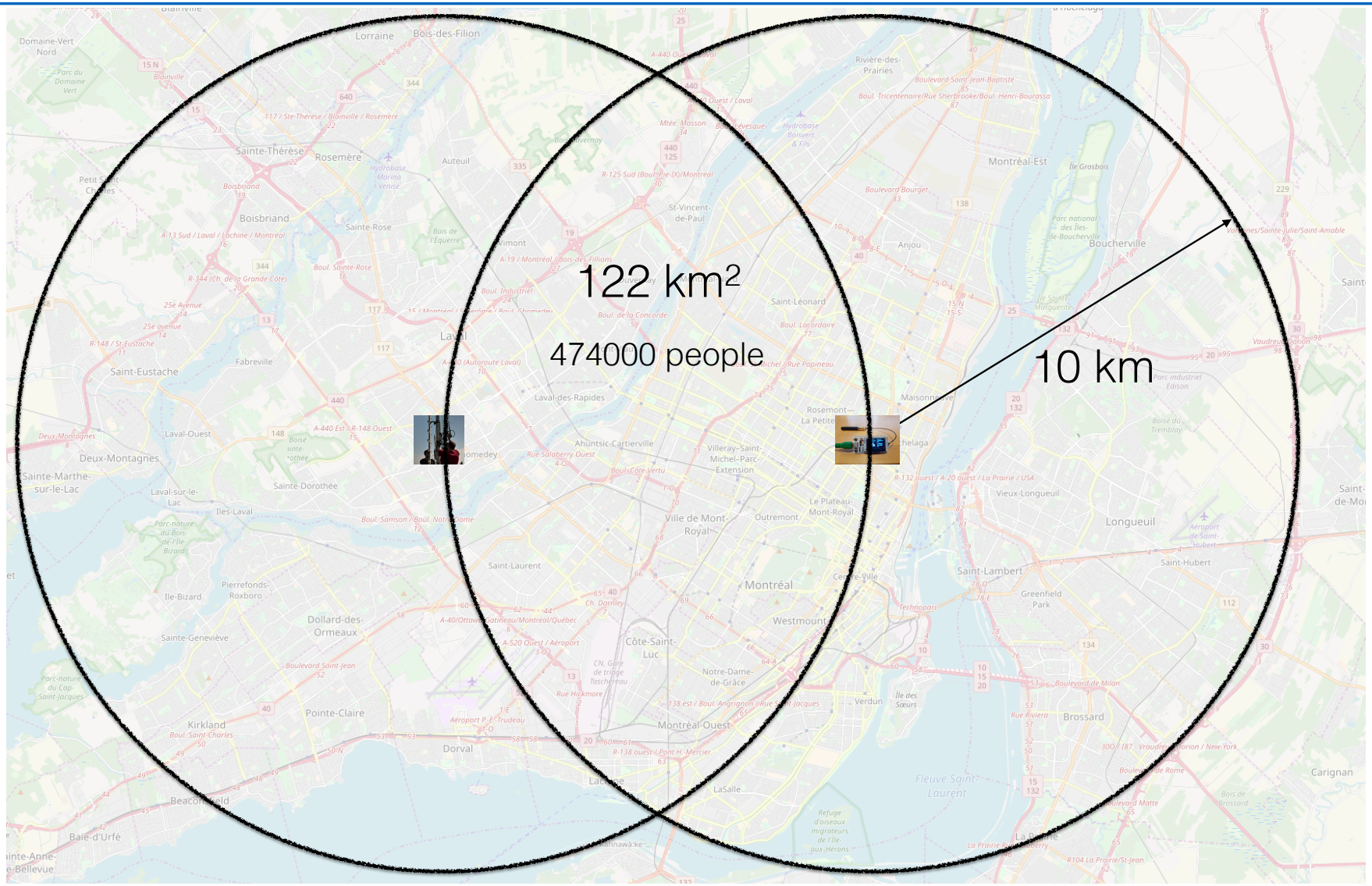
The Things Network

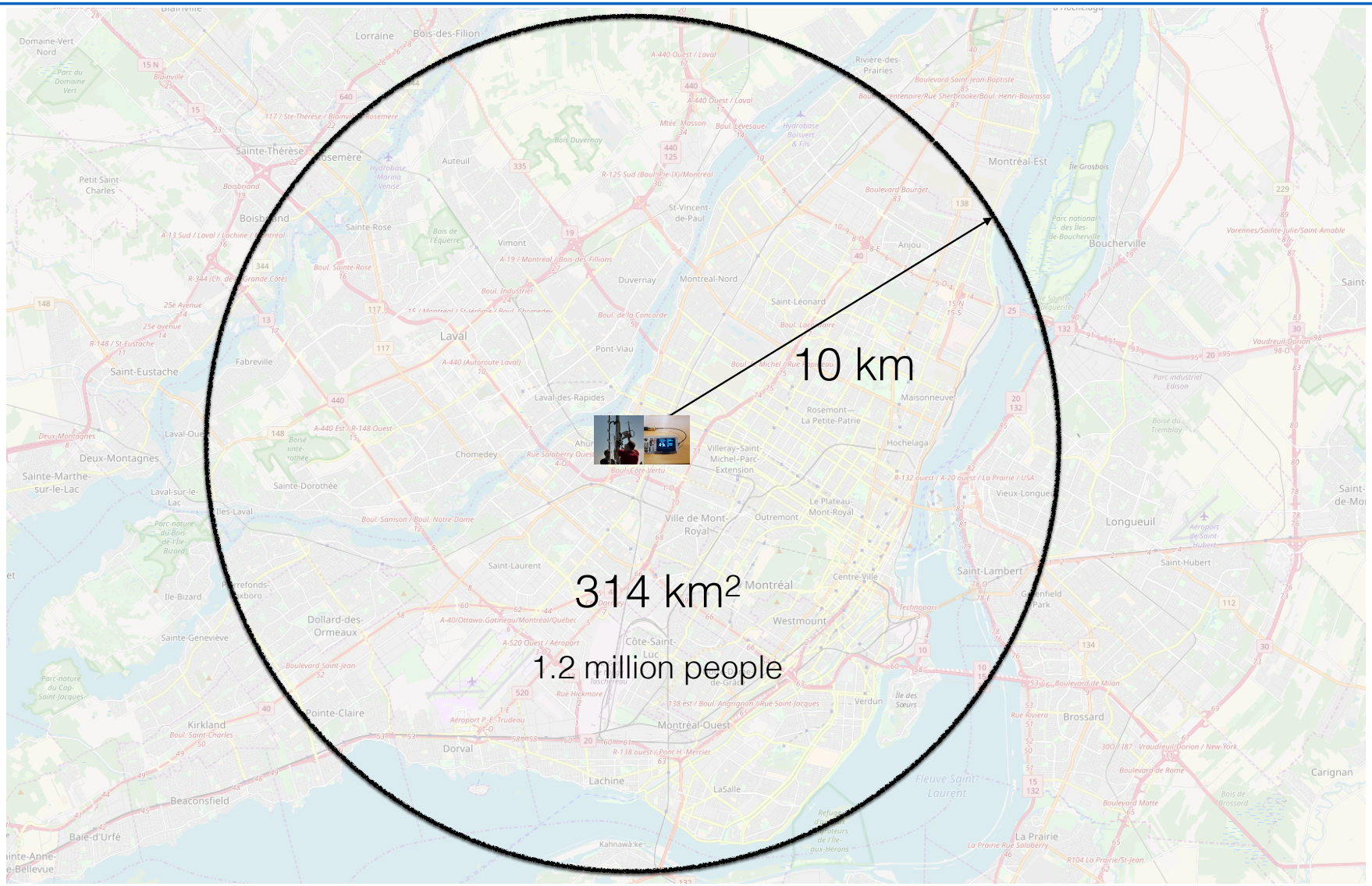


LoRaWAN



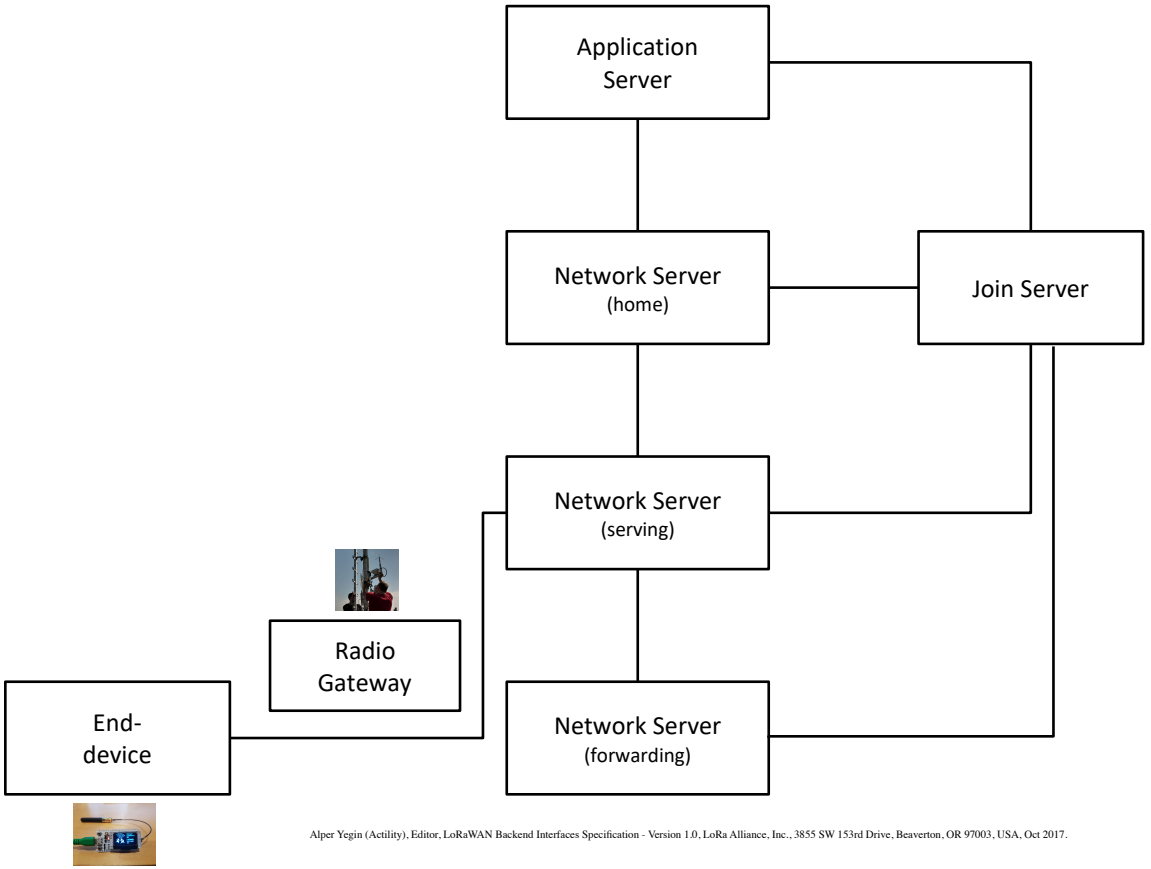

10 km


122 km²
474000 people
10 km


10 km
314 km²
1.2 million people
Montréal
Laval
Longueuil
Brossard
Lachine
Dorval
Dollard-des-Ormeaux
Pointe-Claire
Kirkland
Beaconsfield
Baie-d'Urfé
Saint-Eustache
Deux-Montagnes
Sainte-Thérèse
Boisbriand
Bois-des-Filion
Lorraine
Rosemont—La Petite-Patrie
Villeray-Saint-Michel-Parc-Extension
Ville de Mont-Royal
Westmount
Côte-Saint-Luc
Saint-Laurent
Montréal-Est
Boucherville
Saint-Lambert
Carignan
La Prairie

LoRaWAN Network Reference Model (NRM), roaming End-Device

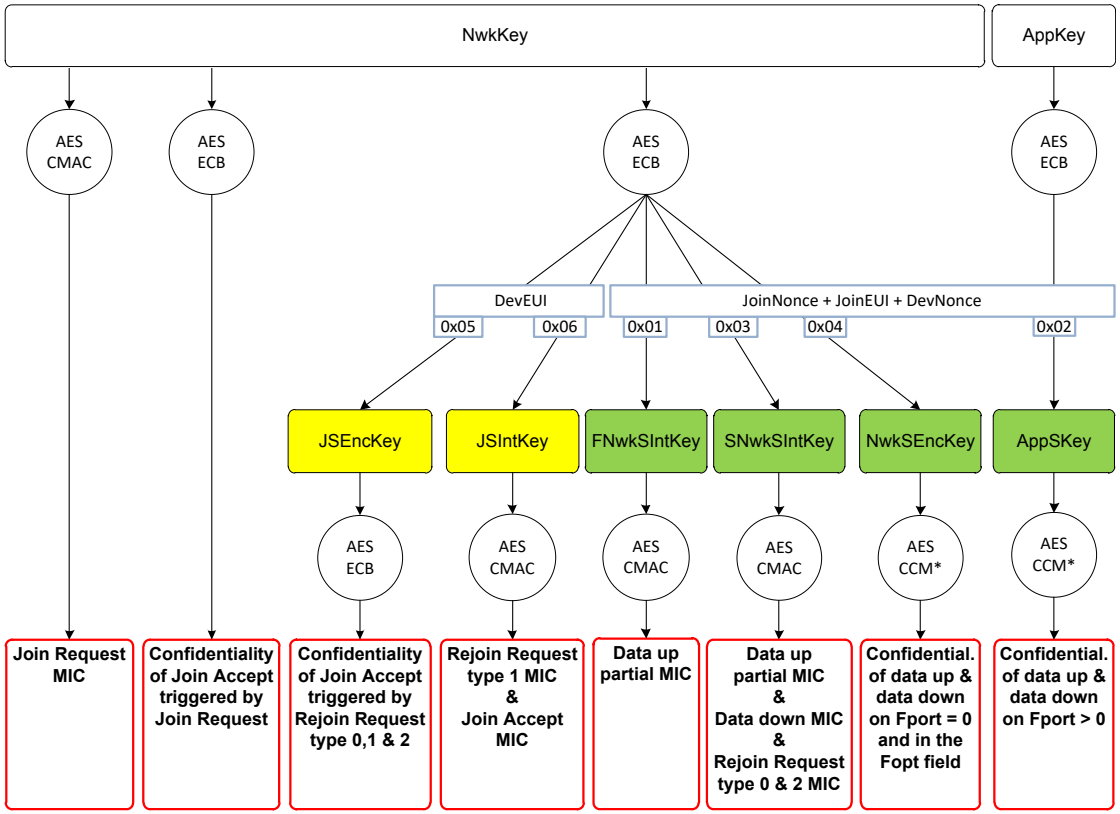
- Endgerät und Application Server kommunizieren vertraulich miteinander.
- Network Server routet Telegramme zum jeweils konfigurierten Application Server.
- Die einzige Aufgabe des Join Servers ist, eindeutige Join Nonces zu generieren.



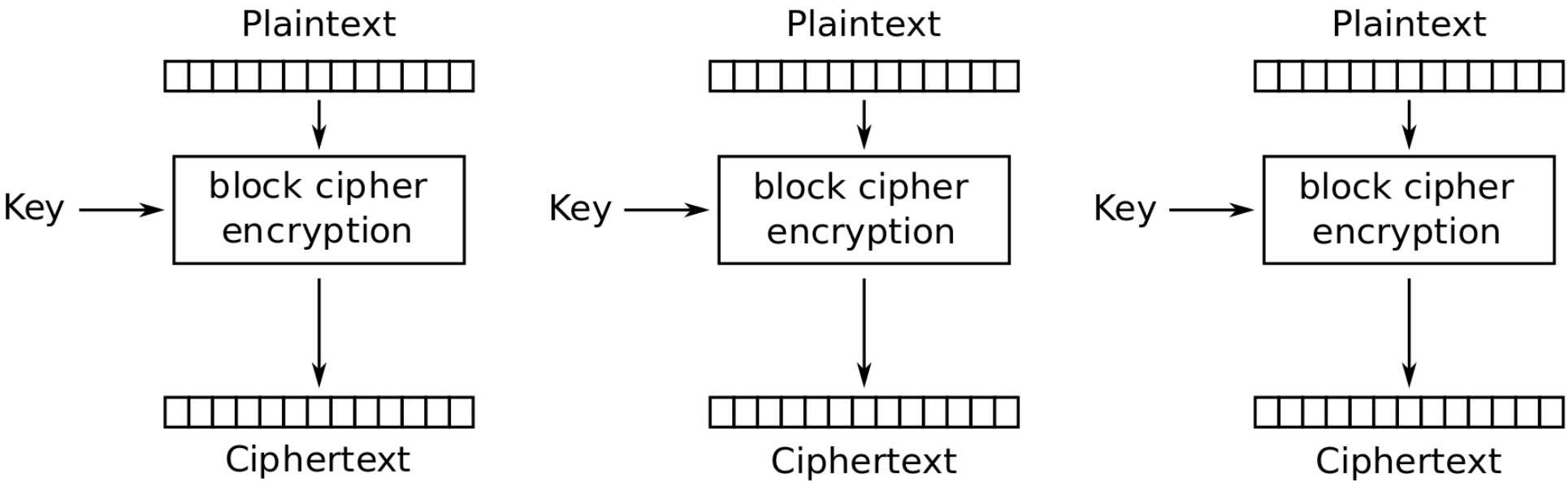
Alper Yegin (Actility), Editor, LoRaWAN Backend Interfaces Specification - Version 1.0, LoRa Alliance, Inc., 3855 SW 153rd Drive, Beaverton, OR 97003, USA, Oct 2017.

Kryptographie in LoRaWAN 1.1

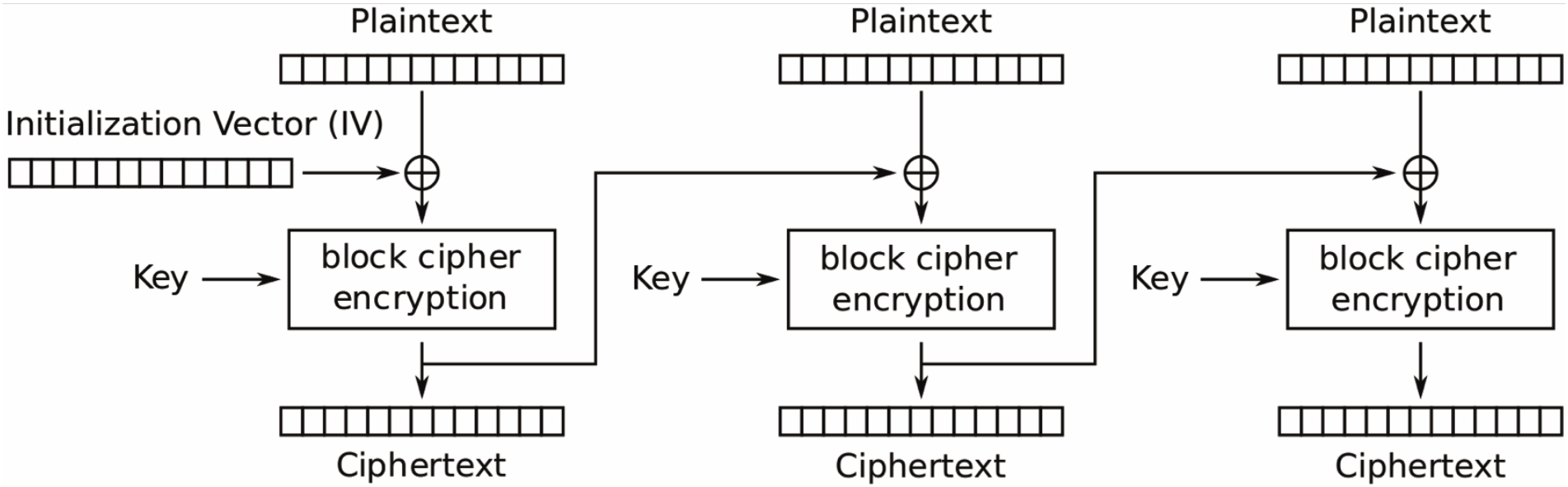
- In LoRaWAN 1.1 werden alle Geräte mit zwei Schlüsseln vorkonfiguriert.
- NwkKey und AppKey werden im End-device gespeichert.
- Verschiedene Session Keys werden von NwkKey und AppKey abgeleitet.
- Over-the-Air Activation (OTAA) oder Activation by Personalization (ABP).



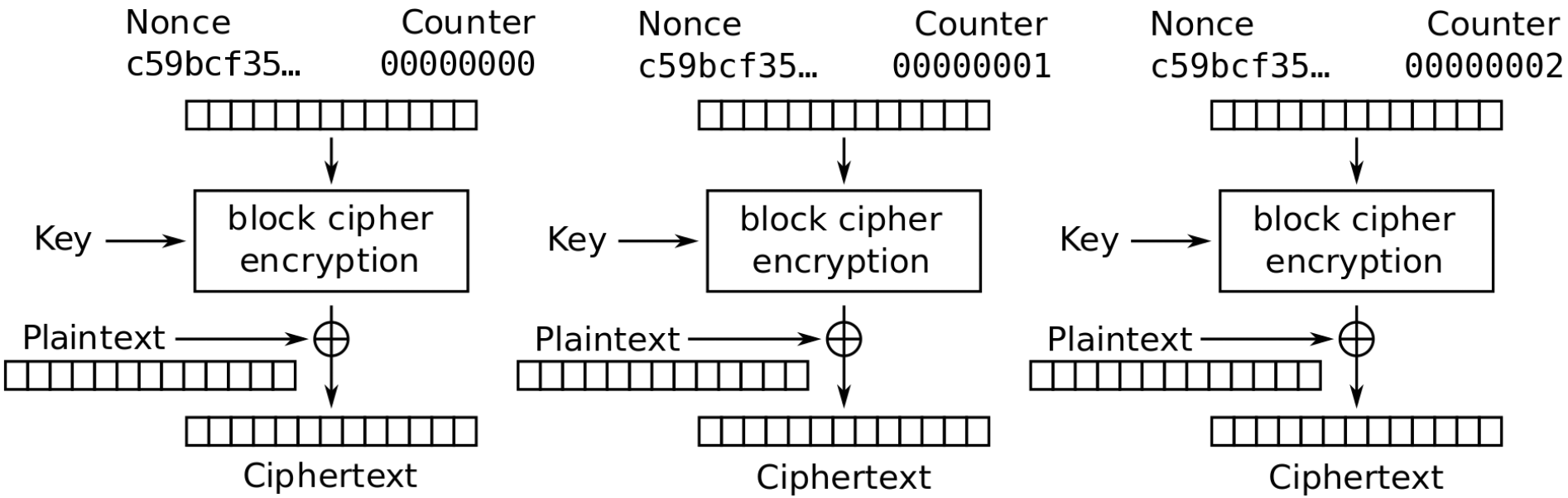
AES working modes - ECB



AES working modes - CBC

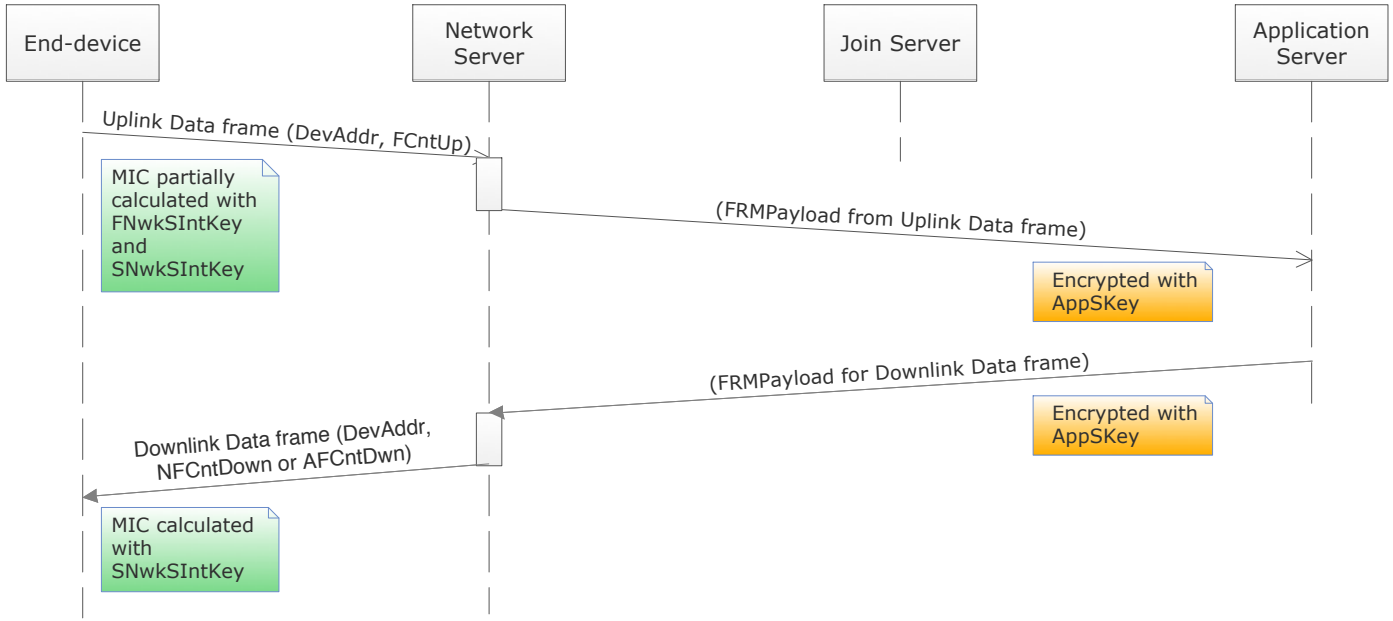


AES working modes - CCM*



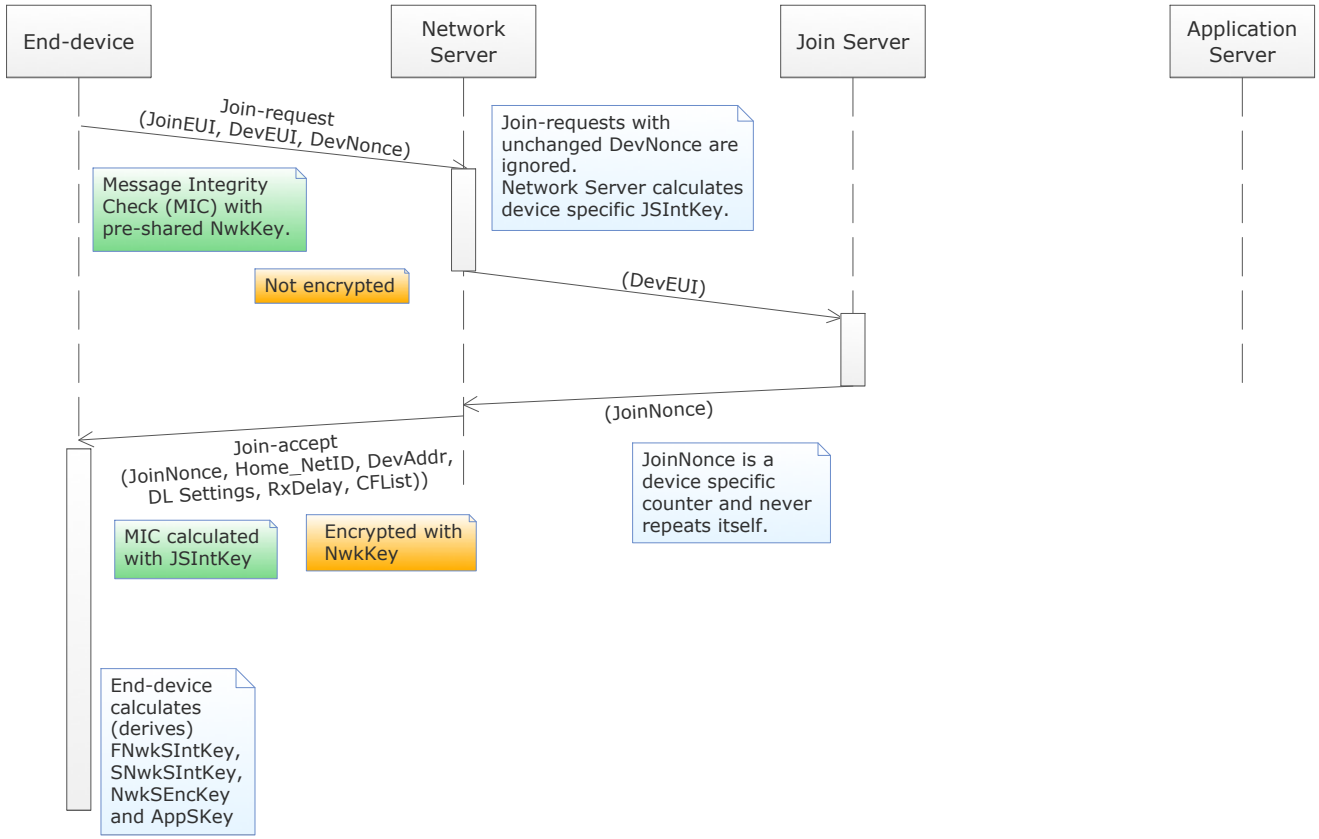
Data frames

- Data Frames werden end-to-end zwischen End-device und Application Server verschlüsselt.



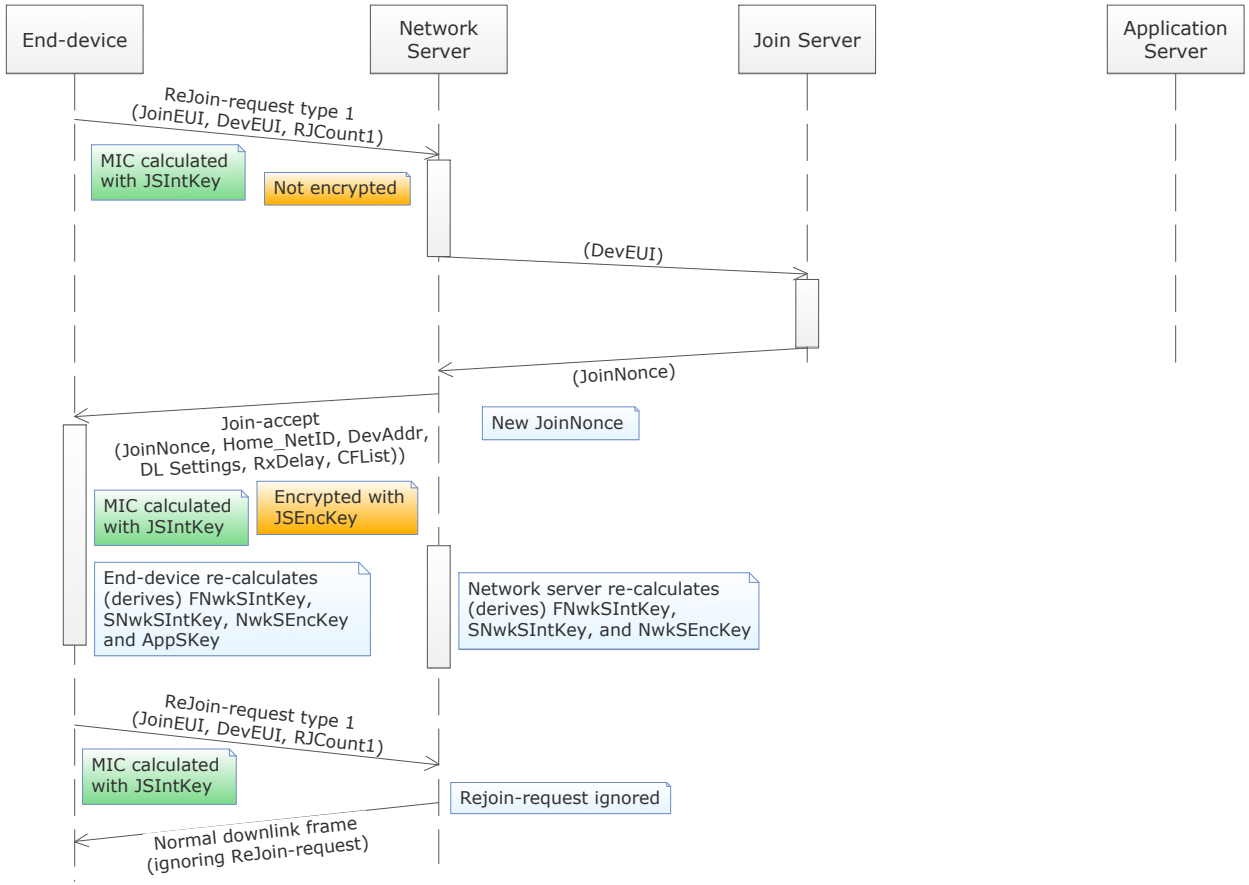
Join

- Telegram handshake, um Keys beim Over-the-Air Activation Prozess auszutauschen.



ReJoin

- Ein Gerät kann periodisch Rejoin-request-Nachrichten senden.
- Das erlaubt es dem Network Server periodisch einen neuen Session Context für ein Endgerät zu erzeugen.



Typische Angriffe

- Angriffe auf Schlüsselmaterial.
- Angriffe auf Counter und Nonces.
- Replay.
- Profiling.

Zusammenfassung

- LoRaWAN scheint vernünftig in Bezug auf Sicherheit entwickelt zu sein.
- Bis jetzt keine publizierten Sicherheitslücken.

Vielen Dank!

thomas.mundt@uni-rostock.de