Resilient, crowd-sourced LPWAN infrastructure using blockchain

CryBlock'18, Munich, Germany

Arnaud Durand <arnaud.durand@unifr.ch>
Pascal Gremaud <pascal.gremaud@unifr.ch>
Jacques Pasquier <jacques.pasquier@unifr.ch>

University of Fribourg
Department of Informatics
Software Engineering Group

June 15, 2018

Decentralized LPWAN Infrastructure

Overview

*We built a scalable, decentralized **IoT-network** using a **distributed ledger**.*

Agenda

- Project goal
- LPWAN
- LoRaWAN
- Activation process
- Roaming
- Security model
- Smart contract
- Limitations
- Using our project

Decentralized LPWAN Infrastructure

Project goals

Low-Power Wide Area Networks relies (mostly) on telecom operators which are a single point of failure.

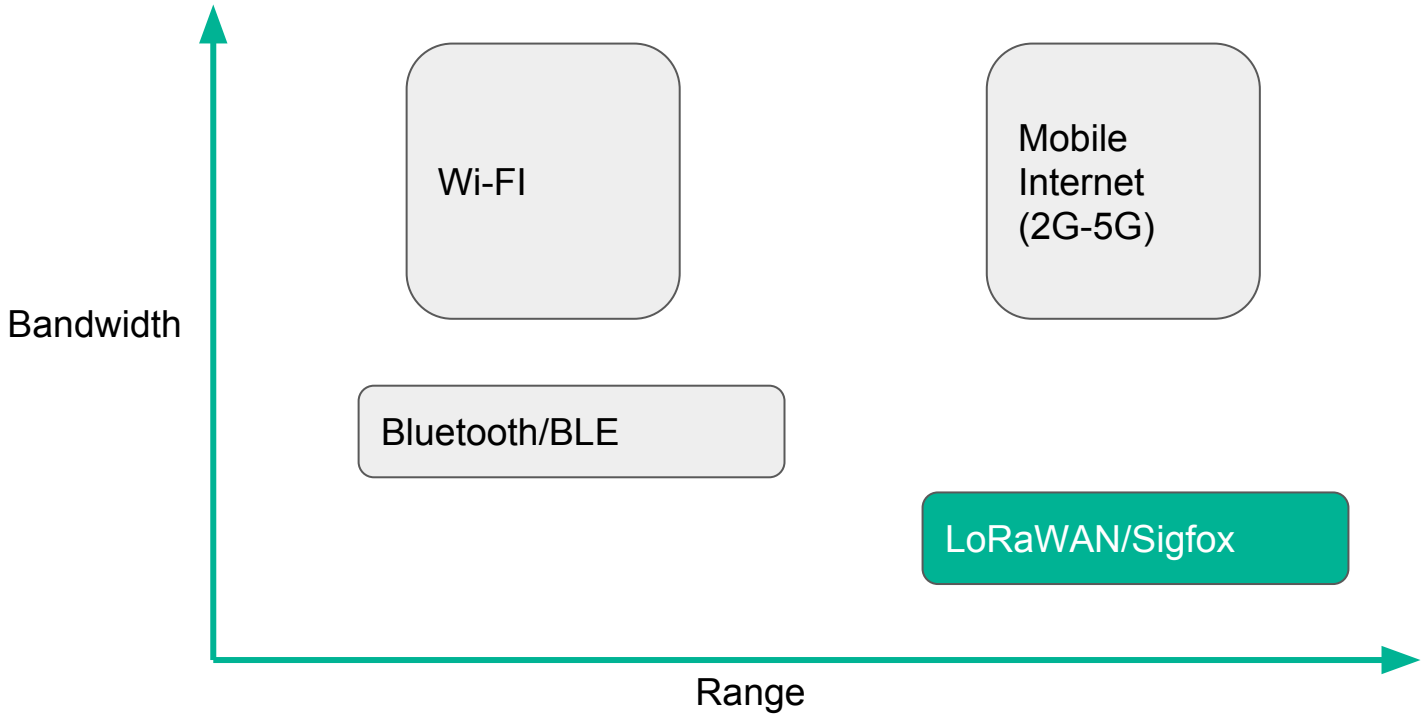
Project goals

- Create a decentralized LPWAN infrastructure
- Build a network server resolver using a public blockchain.
- Demonstrate such an architecture using LoRaWAN.

Low-Power Wide-Area Network

LPWAN

- Long-range sub-gigahertz radio links
- Star topologies



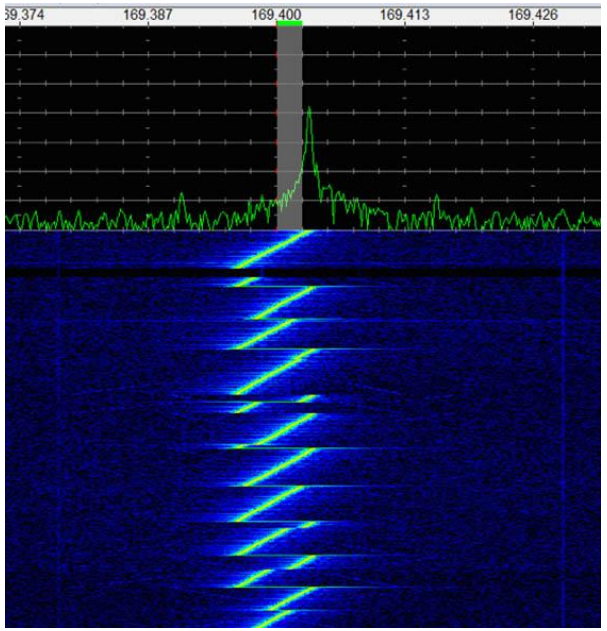
LoRa

Very **long-range** transmission with **low power** consumption

- > 10km in rural areas
- Uses licence-free sub-gigahertz frequency
  - 433Mhz and 868Mhz in Europe
- Chirp modulation
- Runs for years on a coin cell battery

		1 pkt/day	1 pkt/15 min
SF	*Size (bytes)*	*Battery lifetime (years)*	
7	5	5,7	5,2
7	10	5,7	5,1
9	5	5,7	4,3
9	10	5,7	4,0
12	5	5,6	1,8
12	10	5,6	1,7

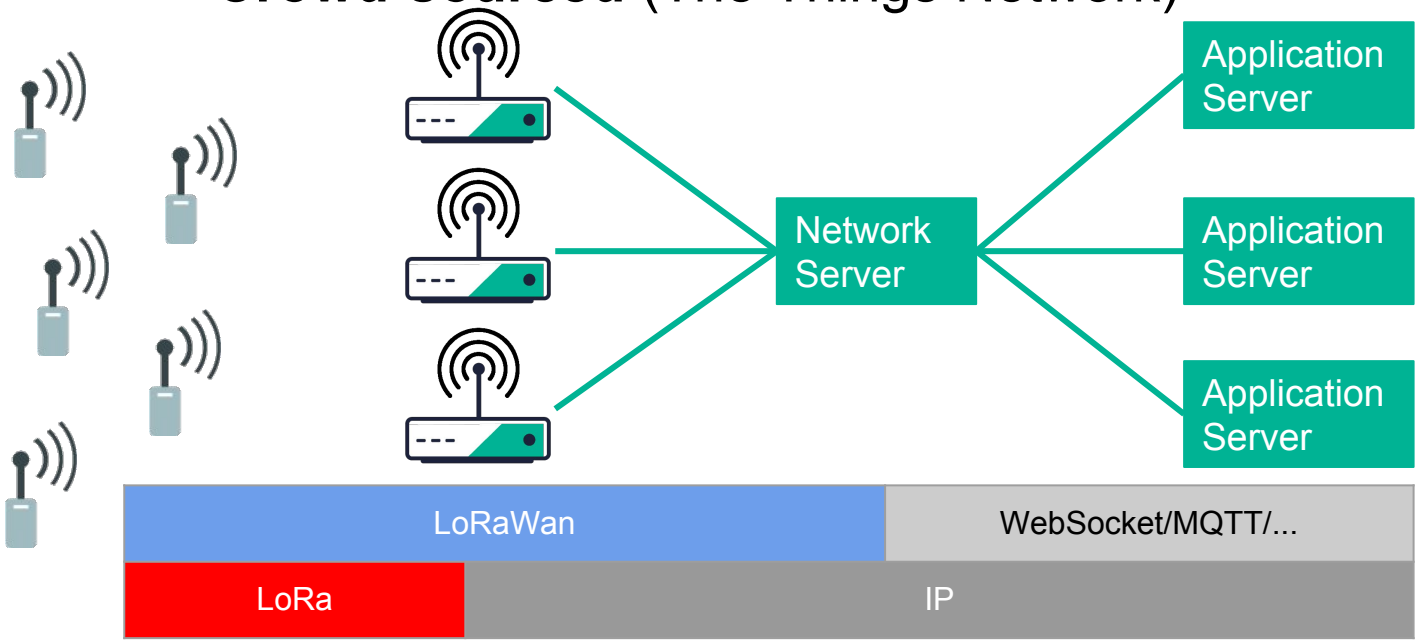
[1]



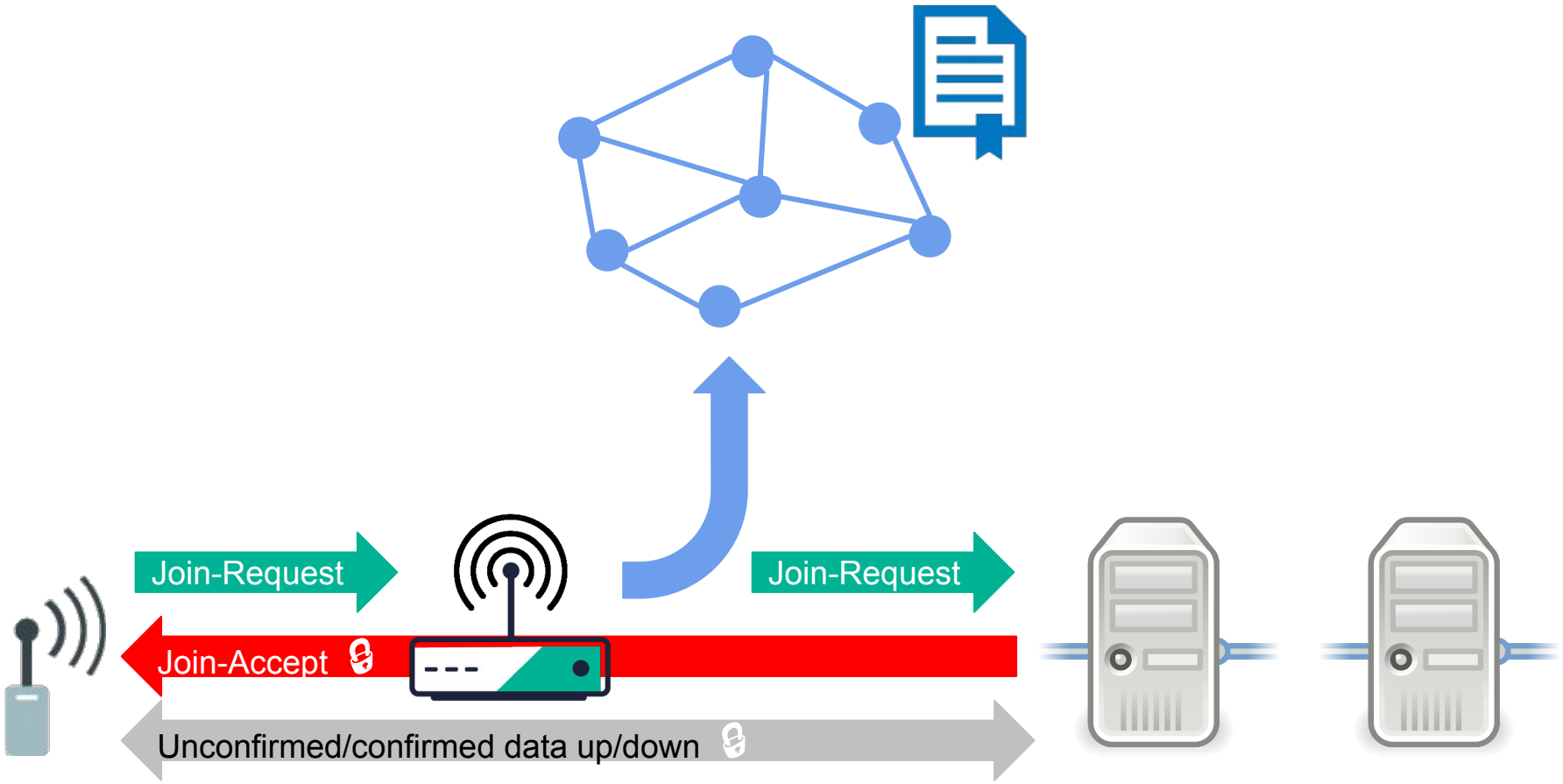
LoRaWAN

- LoRaWAN is a **MAC layer** on top of LoRa
- Enables LoRa devices to connect to a wide area network
- Network types
  - Private vs. commercial
  - **Crowd-sourced** (The Things Network)

Application Layer	
LoRaWAN	MAC
LoRa	PHY
EU868 | US915 | ...	RF



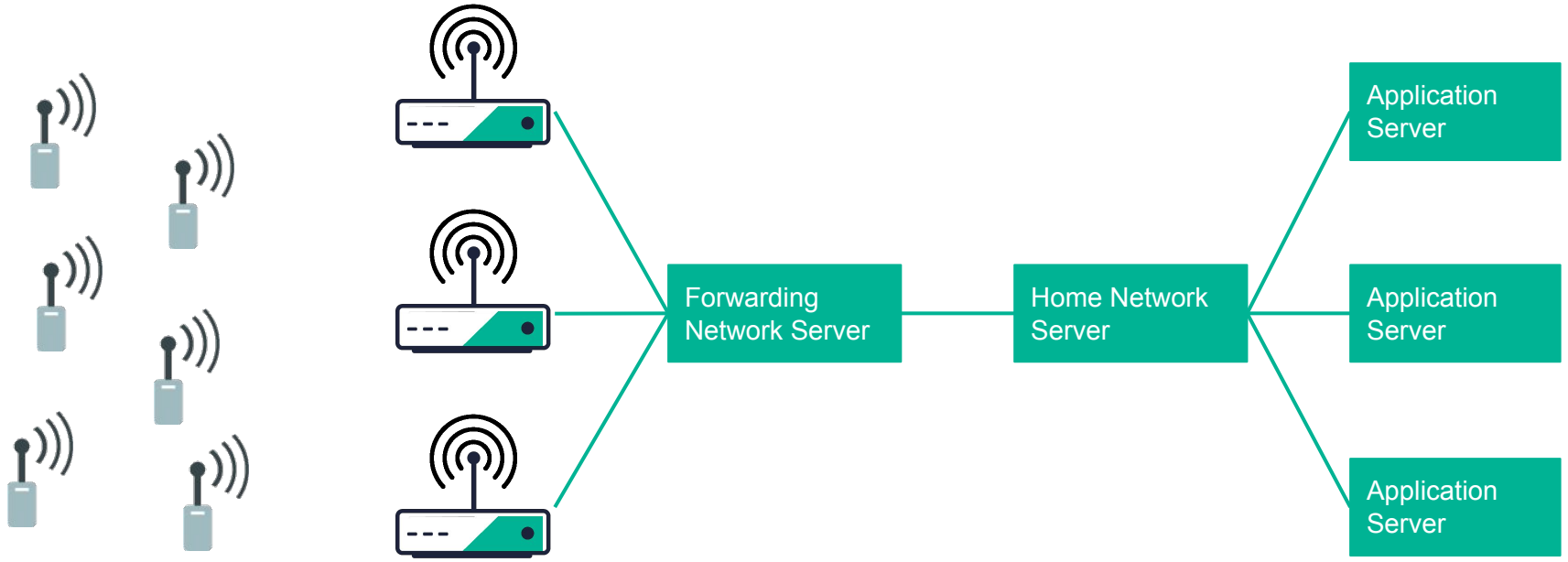
Activation process



Passive Roaming

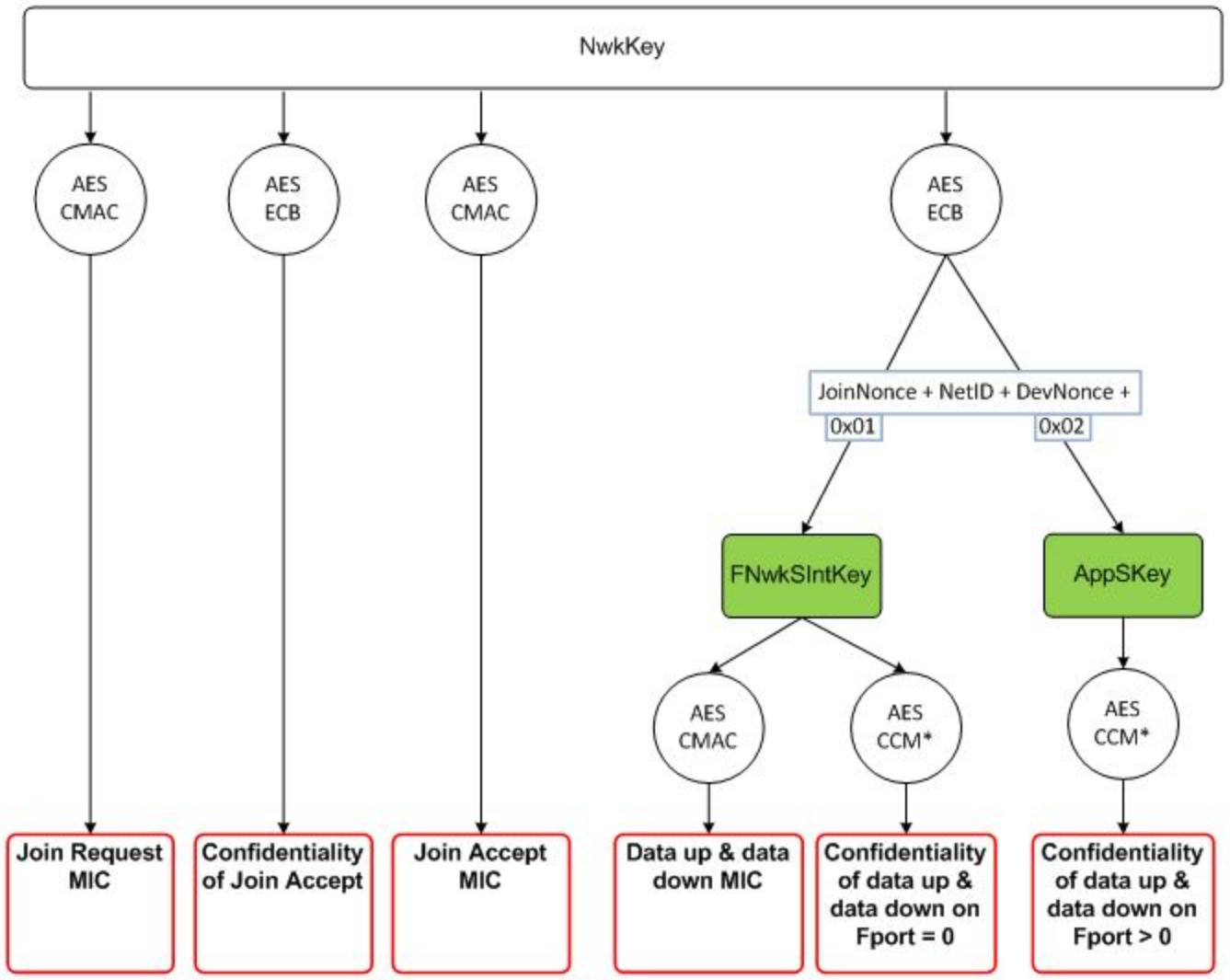
Roaming enables connectivity between devices connected to a foreign network and the home network.

- Passive vs. active roaming



- Home network servers are typically operated by telecom operator

Security Model



[2]

JoinEUI Smart Contract

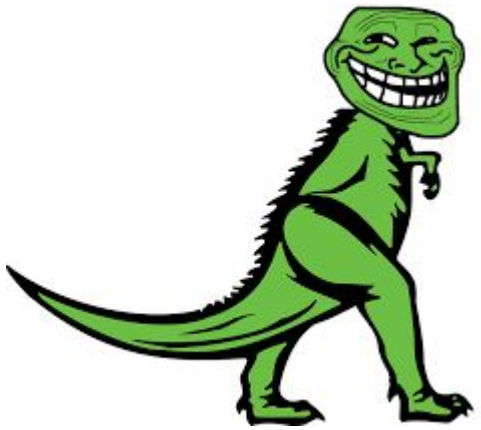
- Replaces LoRa Alliance registry
- Runs on the Ethereum Mainnet
- Generates “join” server identifiers
  - JoinEUI = keccak256($block_N$||$JoinEUI_{i-1}$)

Operation	Gas	Transaction fee (fiat)*
registerJoinEUI()	48947	$0.26738
setIpv4()	42275	$0.23096
getAddress(uint64 joinEui)	0	$0

*June 8, 2018 (Mainnet)

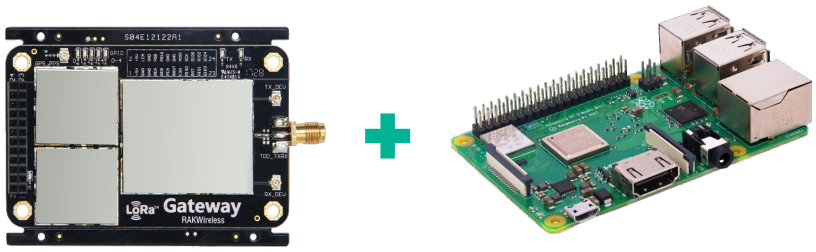
Limitations

- LoRaWAN uses only symmetric keys (AES + CMAC)
- Cannot securely map Join-Accept (🔑) messages to device addresses
- Known attack
  - Collect metadata remotely
- Mitigations
  - Replace LoRaWAN with a new protocol that uses digital signatures



Want to try our project?

- Code is fully open source (Python + Solidity)
  - https://github.com/DurandA/lora-peer
  - https://github.com/DurandA/lorawan-parser
- Required hardware
  - Gateway



  - End-device

References

[1] https://www.link-labs.com/blog/what-is-lora
[2] Lorawan 1.1 specification. Technical report, LoRa Alliance