# Security vulnerabilities in LoRaWAN

Fernando Kuipers
https://fernandokuipers.nl

TU Delft

# Low-Power Wide Area Networks

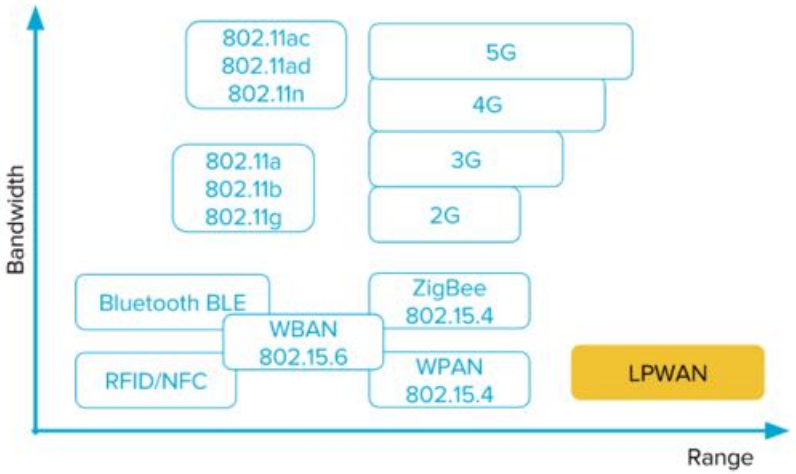
**Unlicensed bands - Non 3GPP**

LoRa™ sigfox

**Licensed bands - 3GPP**

NB-IoT Lte-M

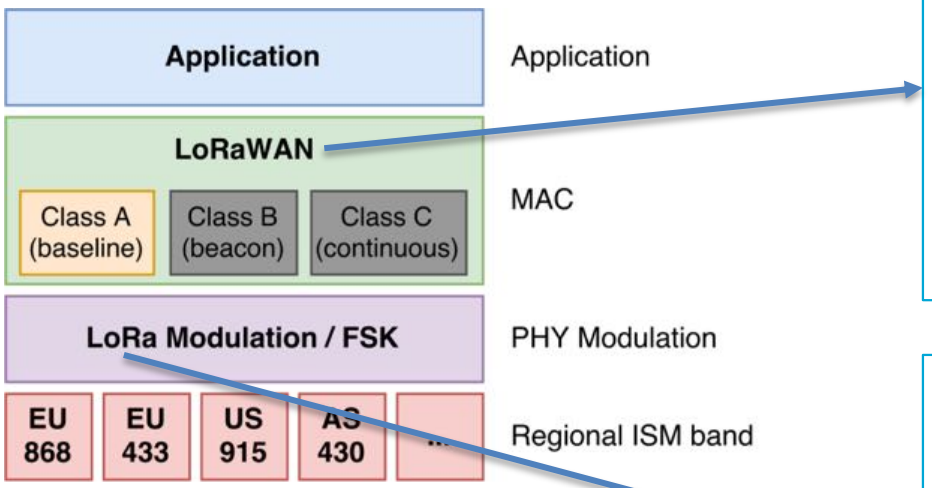
Bandwidth versus range




Use cases


TU Delft

# LoRa vs LoRaWAN

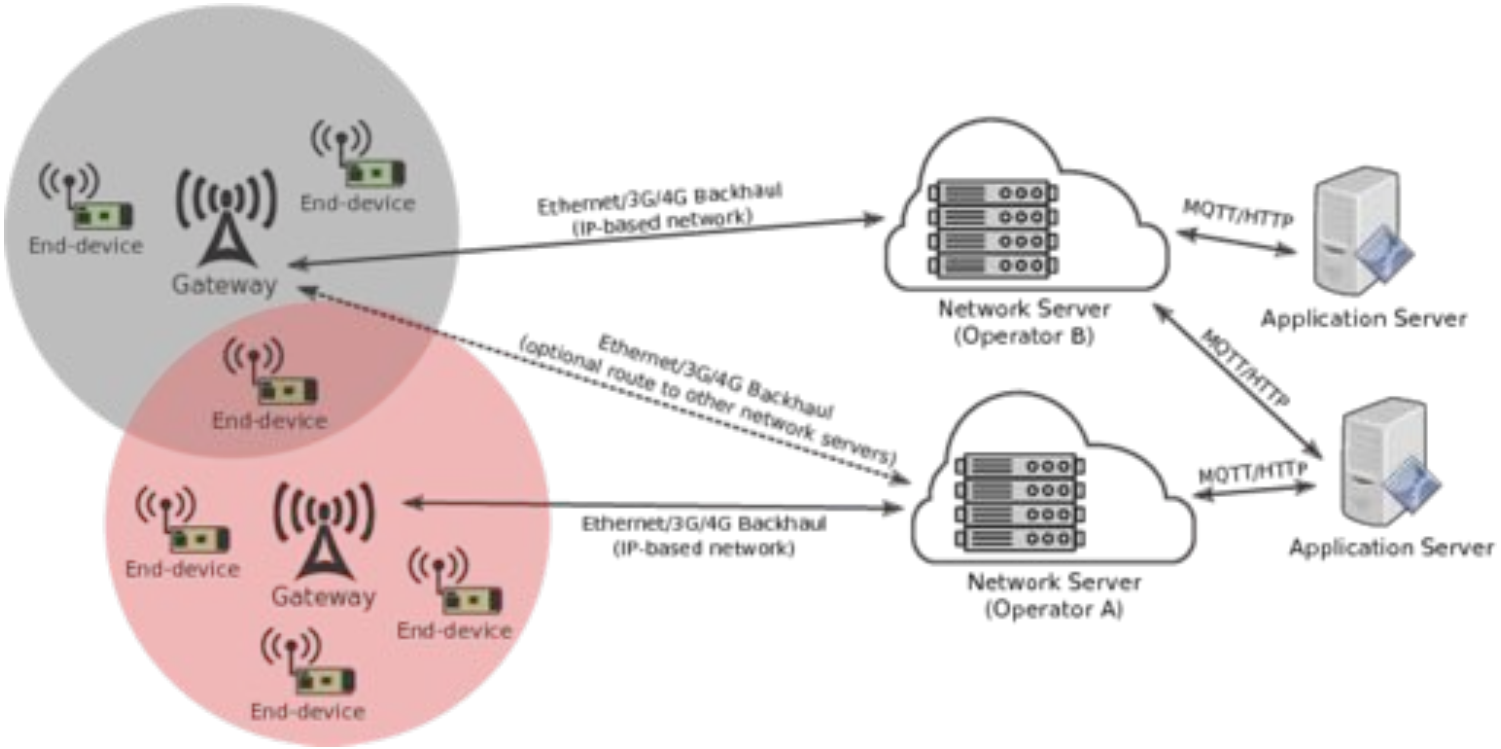


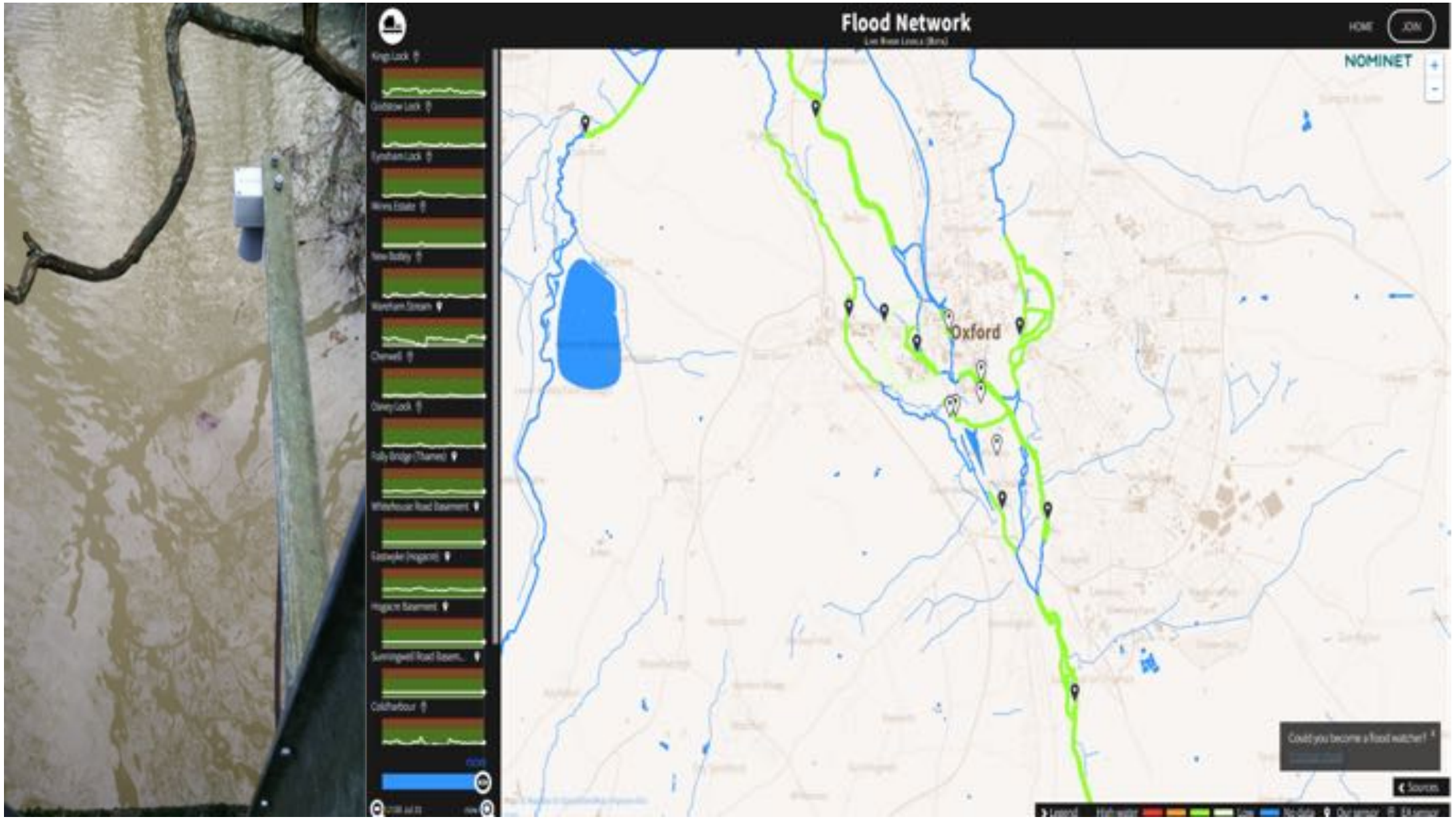

- Communication protocol (MAC) and architecture for LoRa/FSK
- Specified by LoRa Alliance
- LoRaWAN version
  - Common: 1.0.2 (July 2016)
  - Recent: 1.1 (October 11, 2017)

- Semtech's proprietary wireless modulation technology
- Physical layer (PHY) for long range communications
- Based on Chirp Spread Spectrum (CSS)
- Robust against multipath, Doppler shift

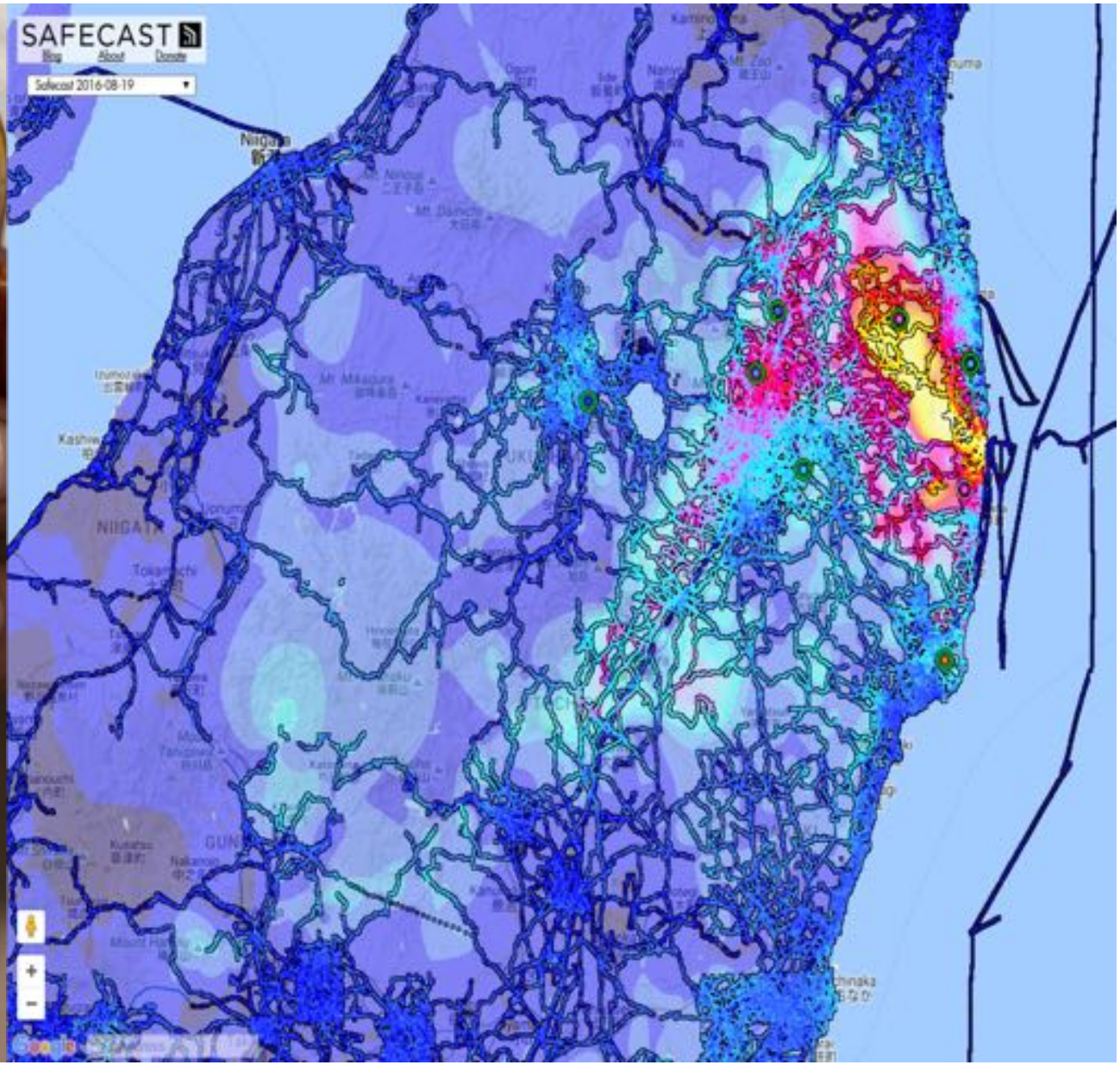
TU Delft

# LoRaWAN architecture




Flood Network
HOME
JOIN
NOMINET
Oxford
Could you become a flood watcher?
Sources

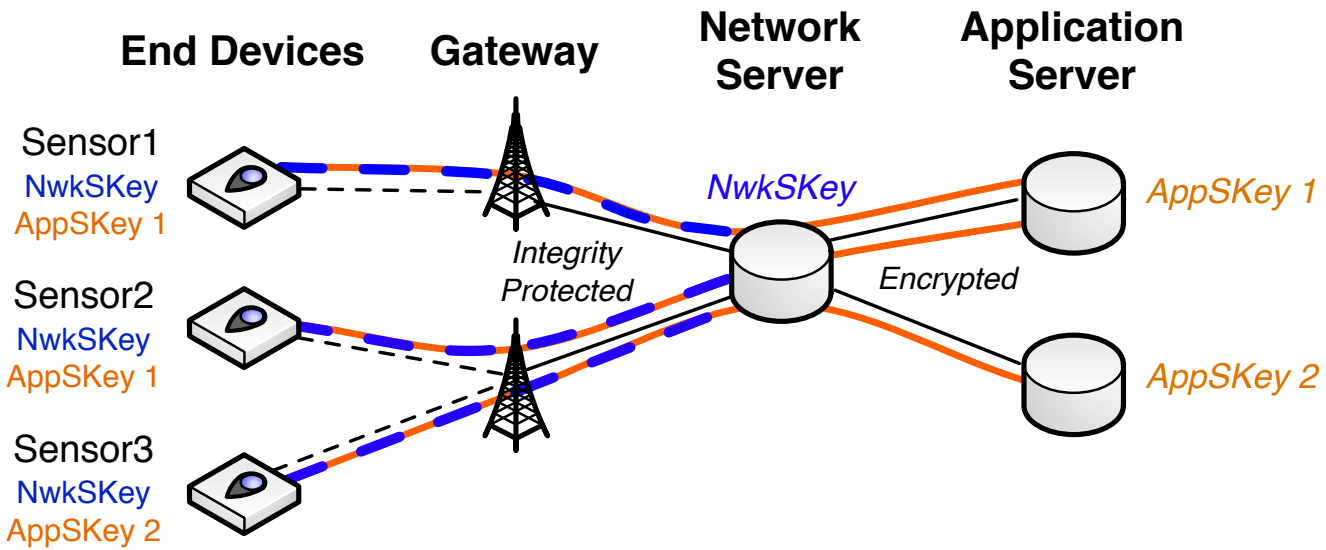

0.144 uSv/h
SAFECAST


SAFECAST
Blog
About
Donate
Safecast 2016-08-19
NIIGATA

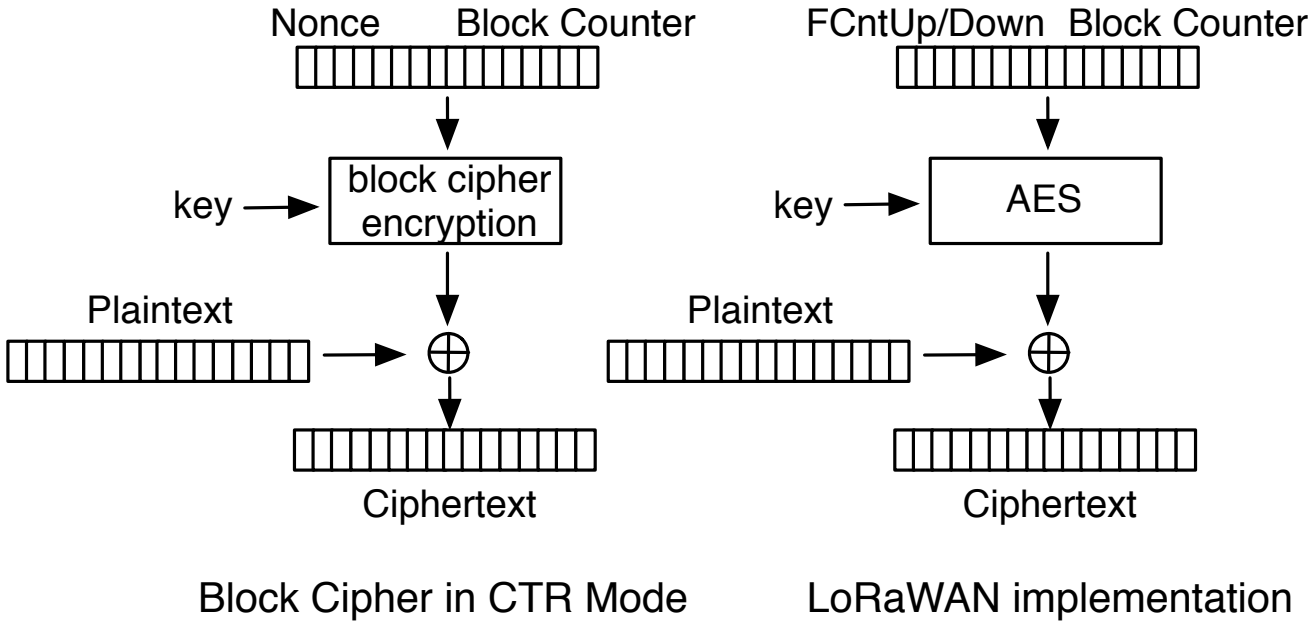
# Security features of LoRaWAN

- Channel confidentiality
  - Network and application keys
  - End-to-end encryption
- Enrollment protocol
  - Activation by Personalization (ABP)
  - Over-the-Air Activation (OTAA)
- Integrity and authenticity validation
  - Message Integrity Code (MIC)

# Channel confidentiality



# Encryption by AppSKey




Block Cipher in CTR Mode

LoRaWAN implementation

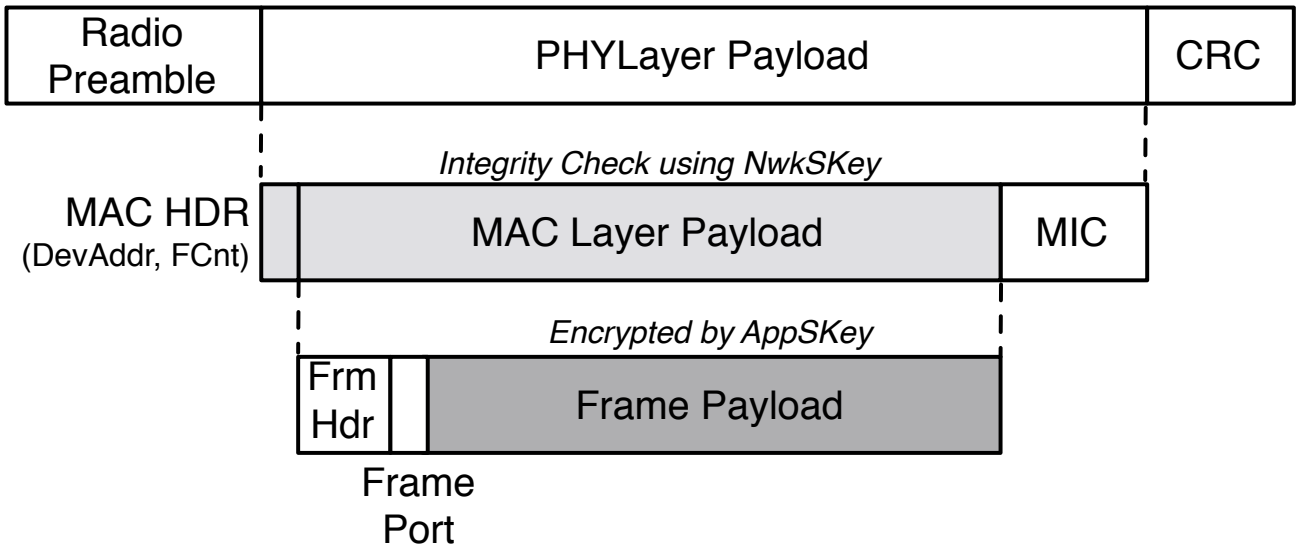
TU Delft

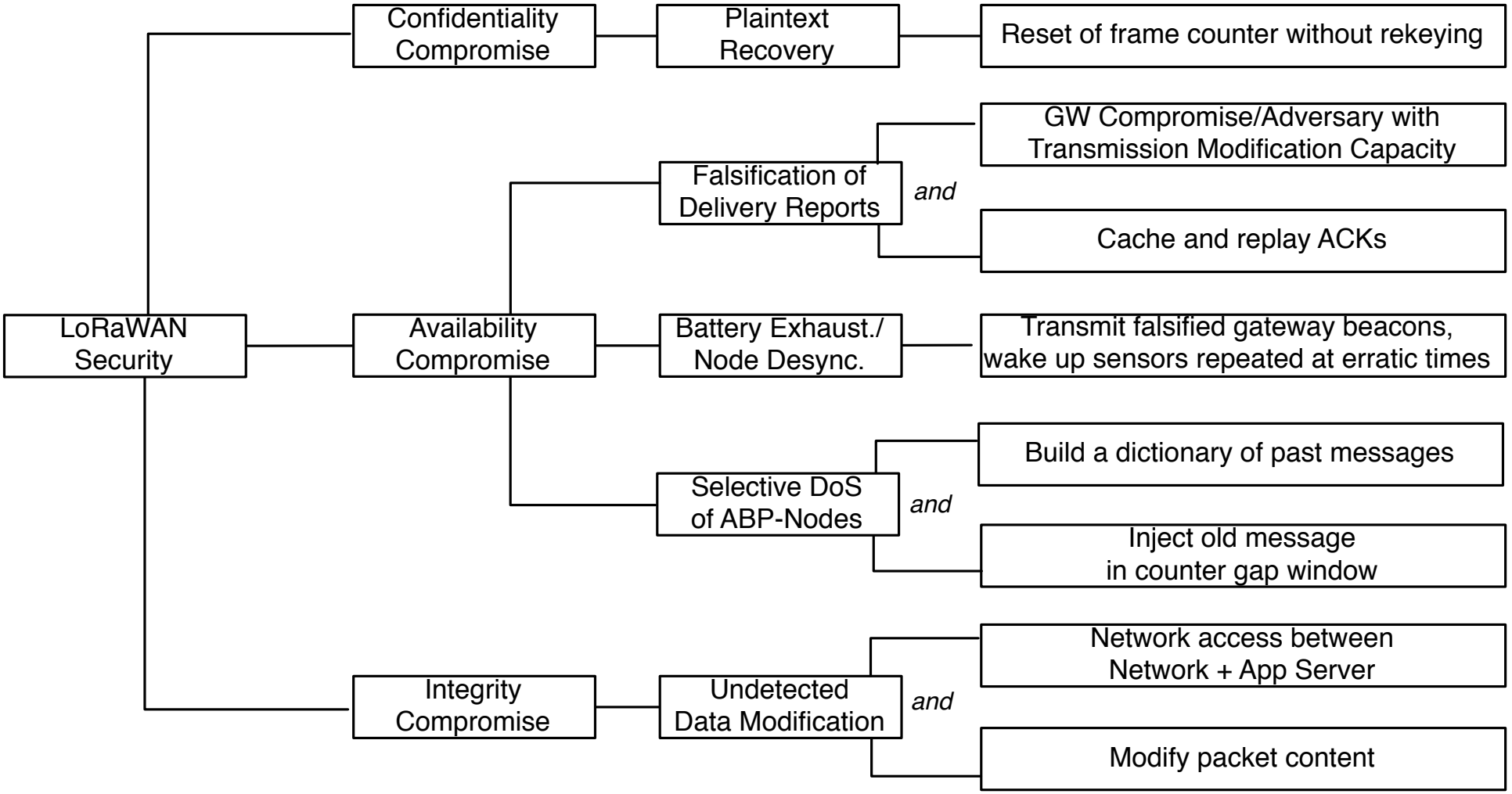
# Enrollment protocol

- OTAA:
  - End-device sends *Join Request*
  - Network server sends *Join Accept* with AppNonce
  - AppNonce to generate NwkSKey and AppSKey

- ABP:
  - No exchange of join messages
  - NwkSKey and AppSKey pre-assigned

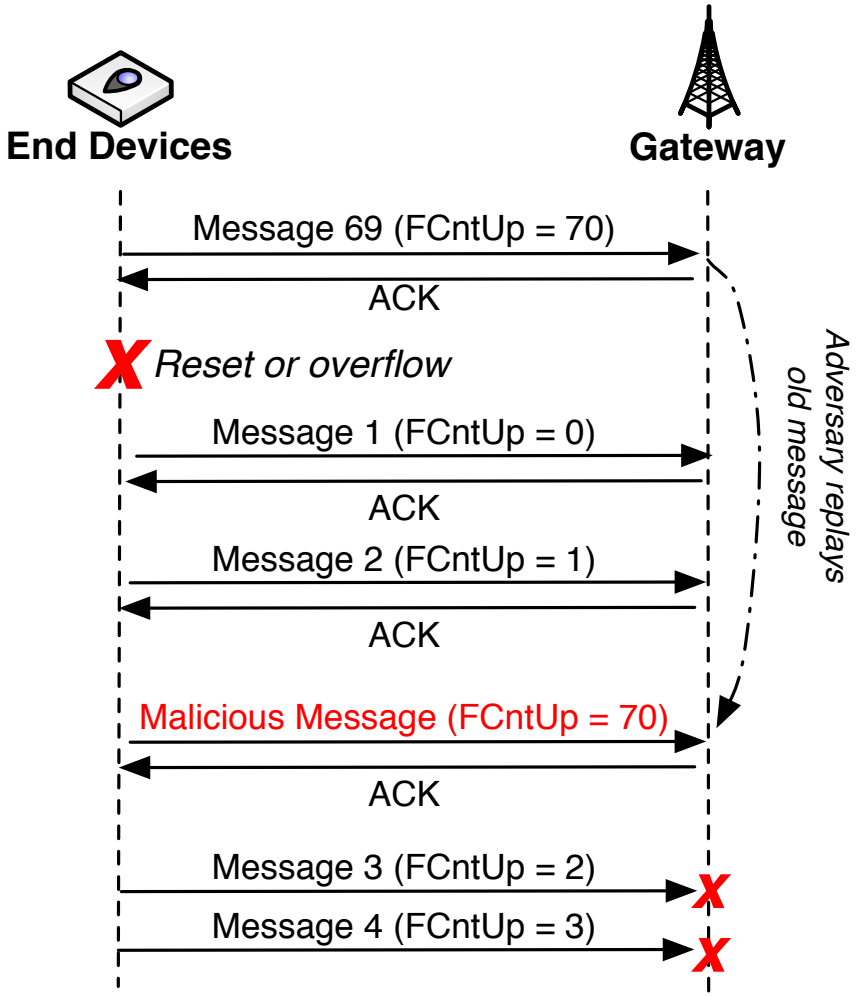
# Integrity and Authenticity validation

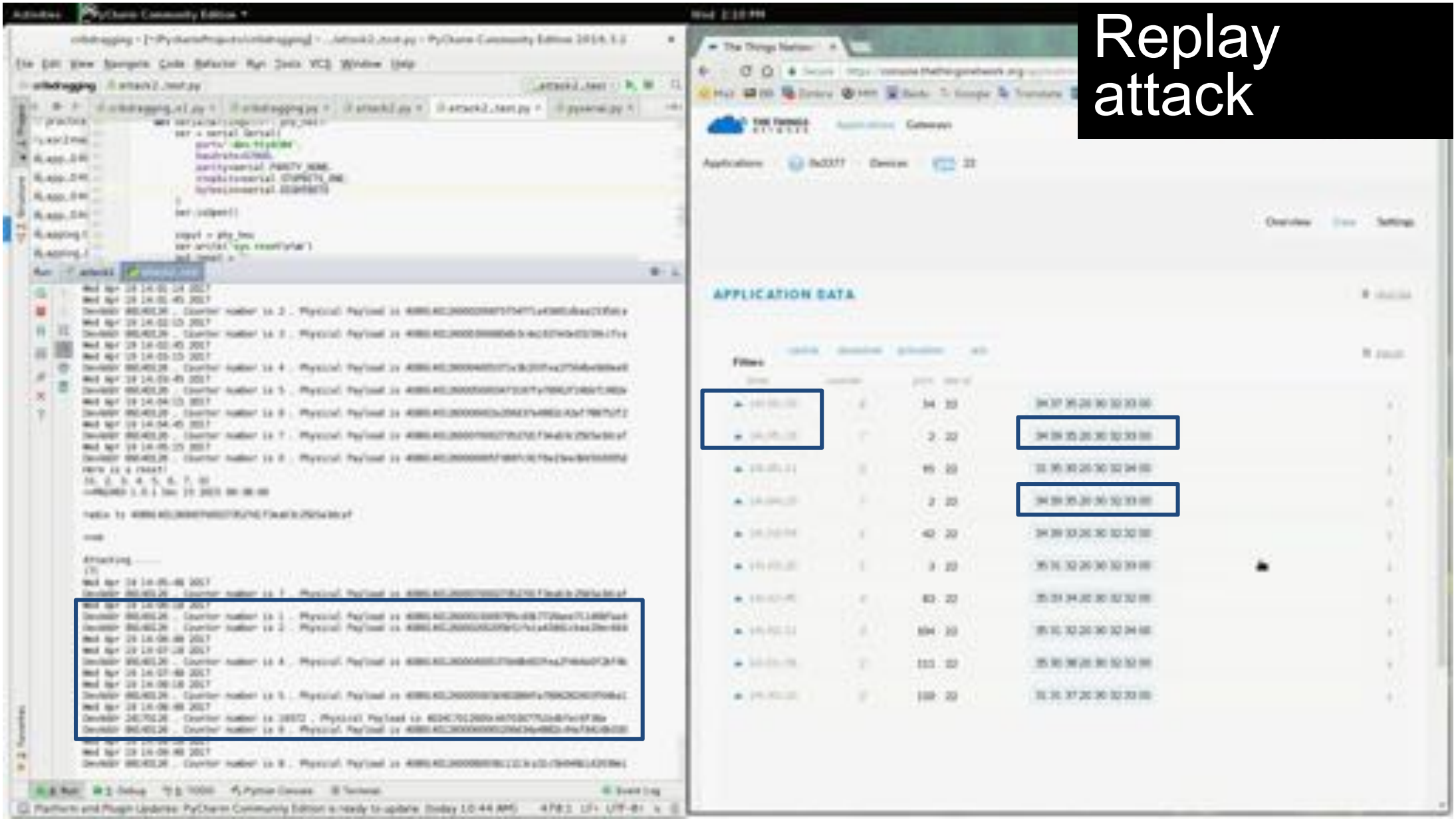



LoRaWAN Security
Confidentiality Compromise
Plaintext Recovery
Reset of frame counter without rekeying
Availability Compromise
Falsification of Delivery Reports
and
GW Compromise/Adversary with Transmission Modification Capacity
Cache and replay ACKs
Battery Exhaust./ Node Desync.
Transmit falsified gateway beacons, wake up sensors repeated at erratic times
Selective DoS of ABP-Nodes
and
Build a dictionary of past messages
Inject old message in counter gap window
Integrity Compromise
Undetected Data Modification
and
Network access between Network + App Server
Modify packet content

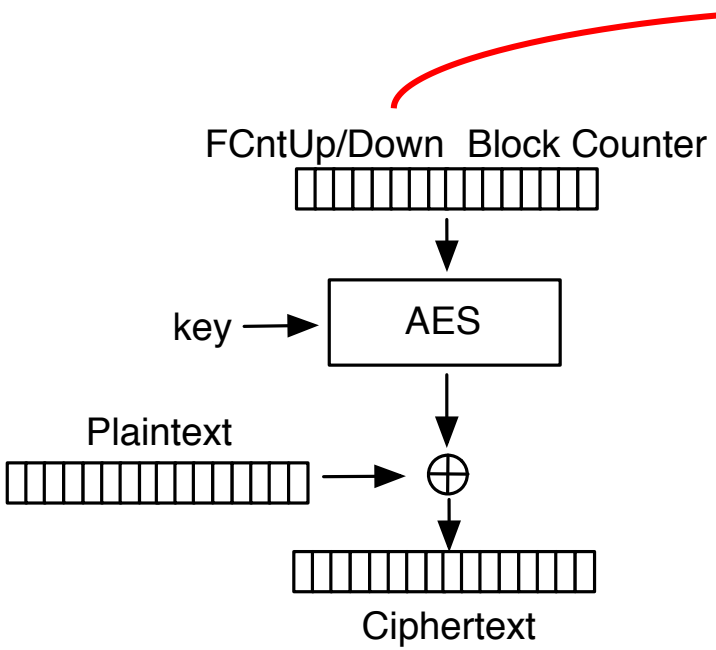
TU Delft

# Replay attack




Replay
attack
APPLICATION DATA

# Eavesdropping




LoRaWAN implementation

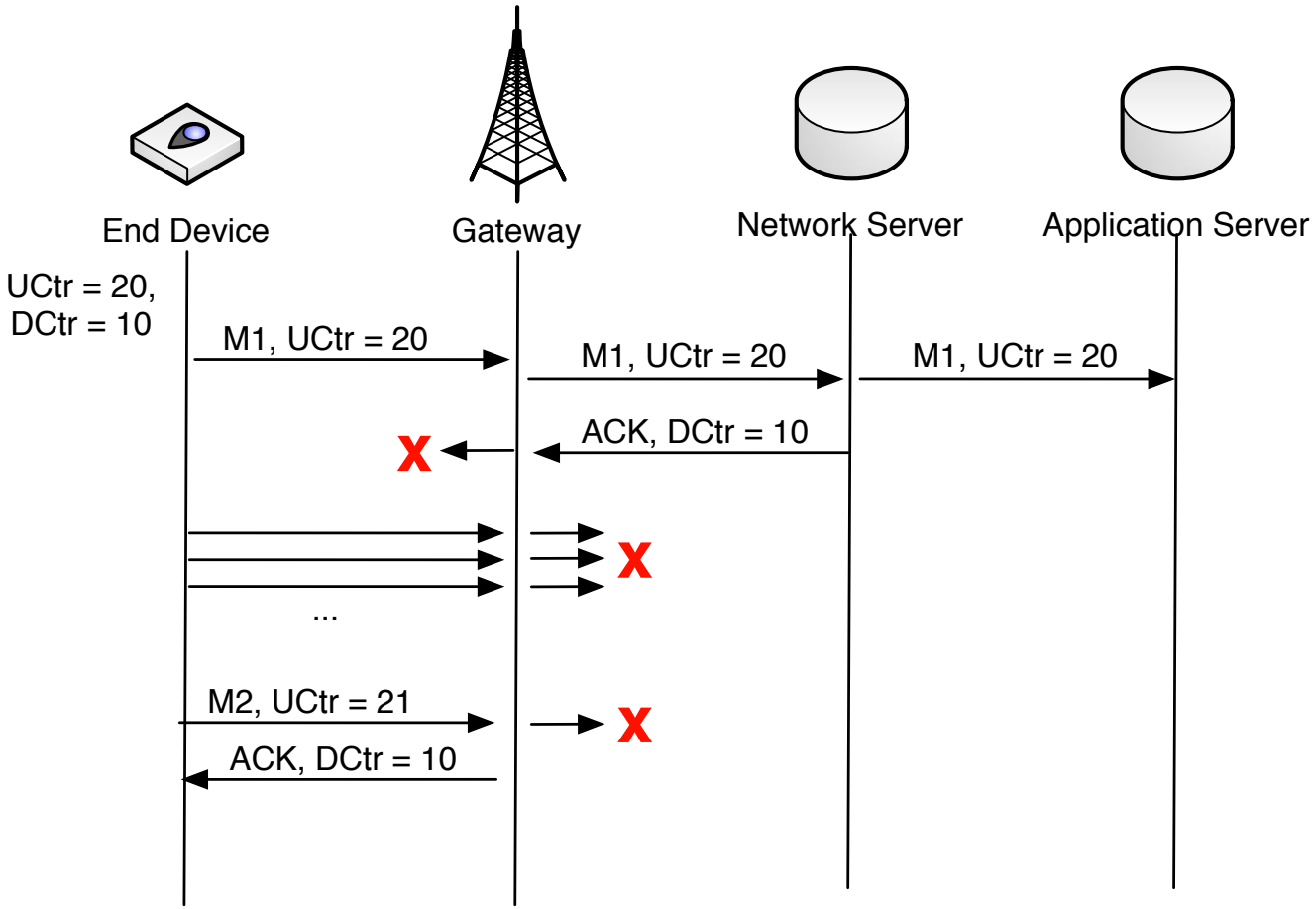
If FCnt is re-used

$$C_1 \oplus C_2 = (P_1 \oplus K) \oplus (P_2 \oplus K)$$
$$= P_1 \oplus P_2 \oplus \underbrace{(K \oplus K)}_{\text{cancels out}}$$
$$= P_1 \oplus P_2.$$

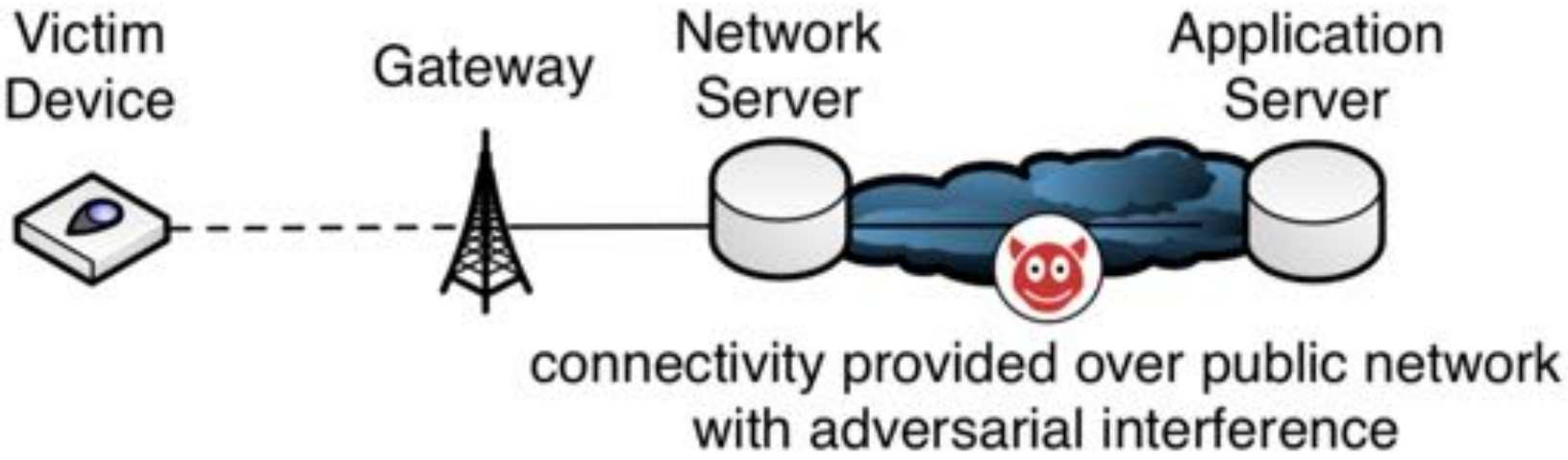
Guess one word to derive the other

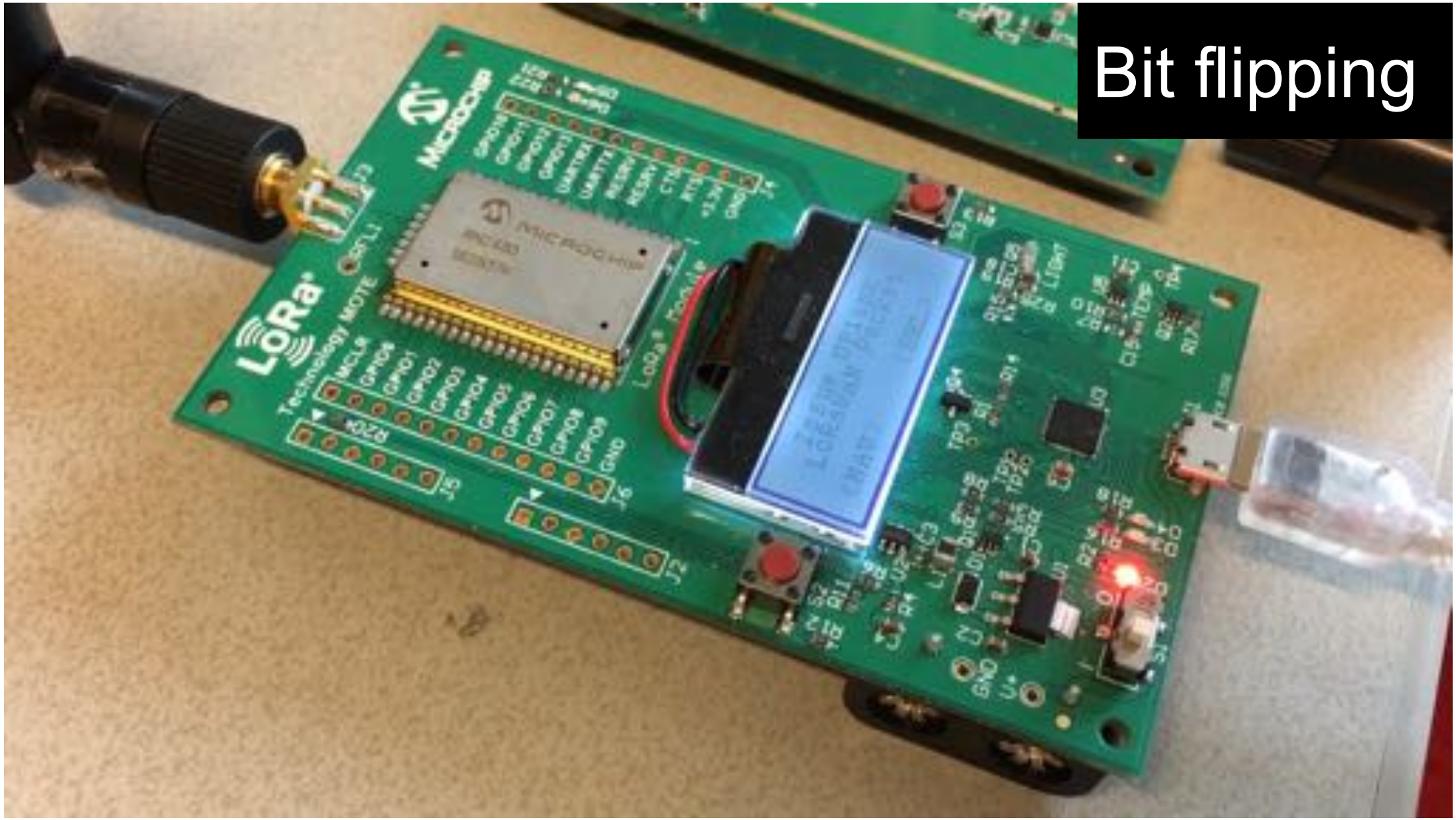
TU Delft

# ACK spoofing

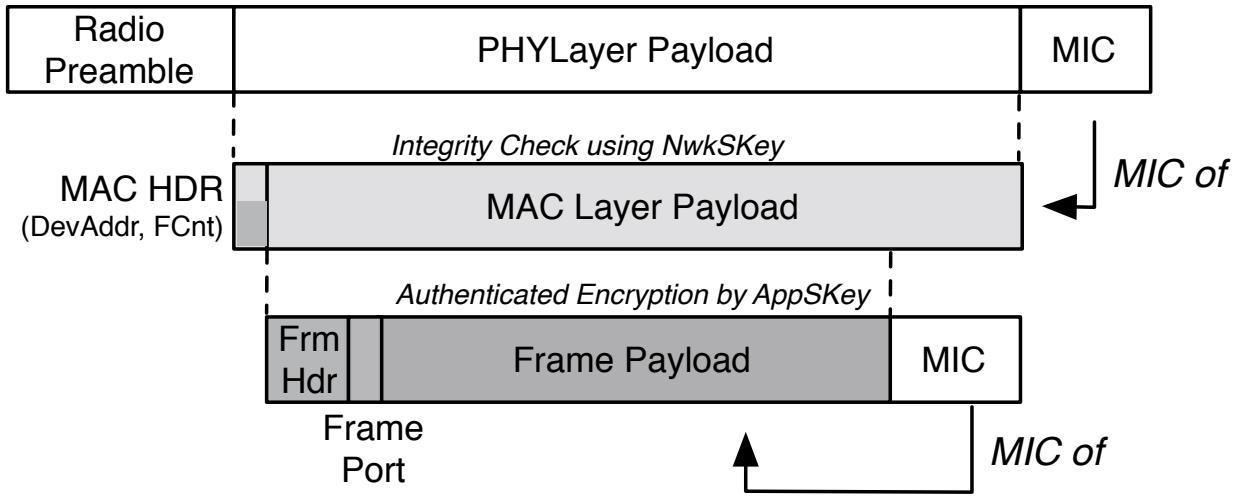


# Bit flipping




Bit flipping
LoRa
MICROCHIP

# Counter-measure



# More attacks and counter-measures in our paper

TU Delft

X. Wang, E. Karampatzakis, C. Doerr, and F.A. Kuipers, “Security Vulnerabilities in LoRaWAN,” ACM/IEEE IoTDI, 2018.