LoRa's Jambalaya

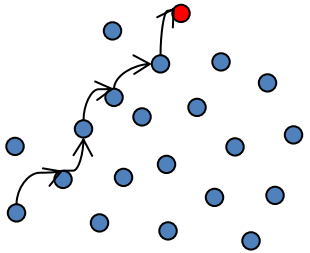
Fernando Kuipers
Delft University of Technology
May 20th, 2019
https://fernandokuipers.nl

TU Delft

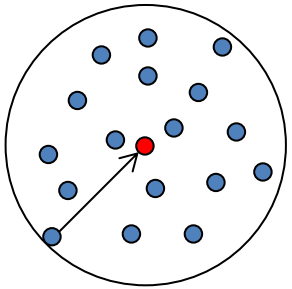
“Sense and the city”

Wireless Sensor Networks

- WSNs:
  - Multiple hops to sink
  - Many challenges due to energy constraints



- Long-range communication:
  - Direct link to sink/gateway



TU Delft

Low-Power Wide Area Networks

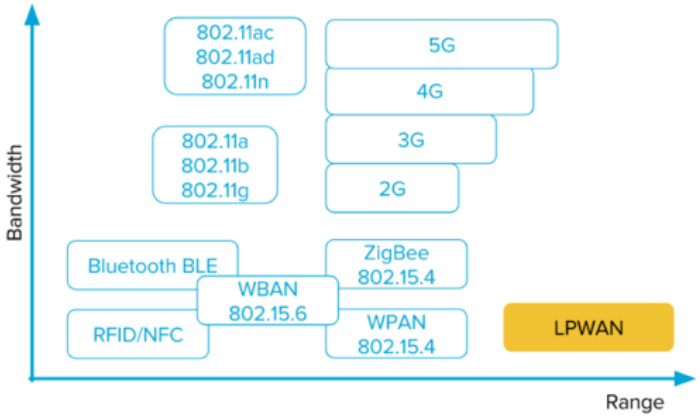
Unlicensed bands - Non 3GPP

LoRa™ sigfox

Licensed bands - 3GPP

NB-IoT Lte-M

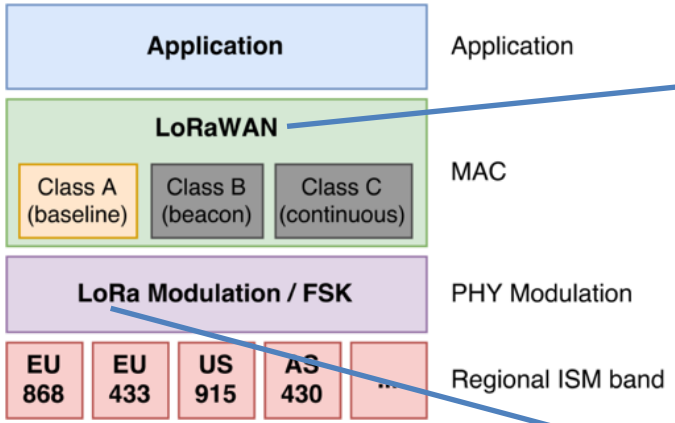
Bandwidth versus range



Use cases

TU Delft

LoRa vs LoRaWAN



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

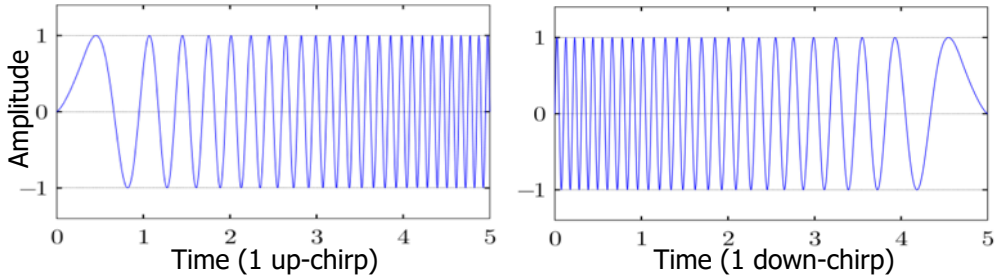
- Semtech's proprietary wireless modulation technology
- Physical layer (PHY) for long range communications
- Based on Chirp Spread Spectrum (CSS)
- Robust against multipath, Doppler shift

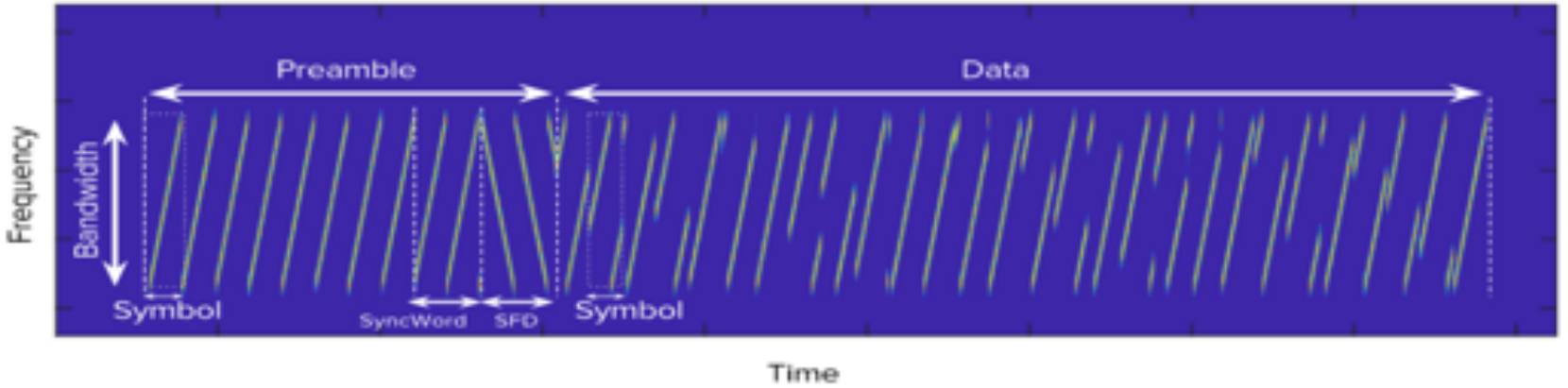
TU Delft

Chirp Spread Spectrum (CSS)

- One chirp = 1 symbol
- One chirp covers entire BW
- Frequency offset (+ wrap-around) determines symbol

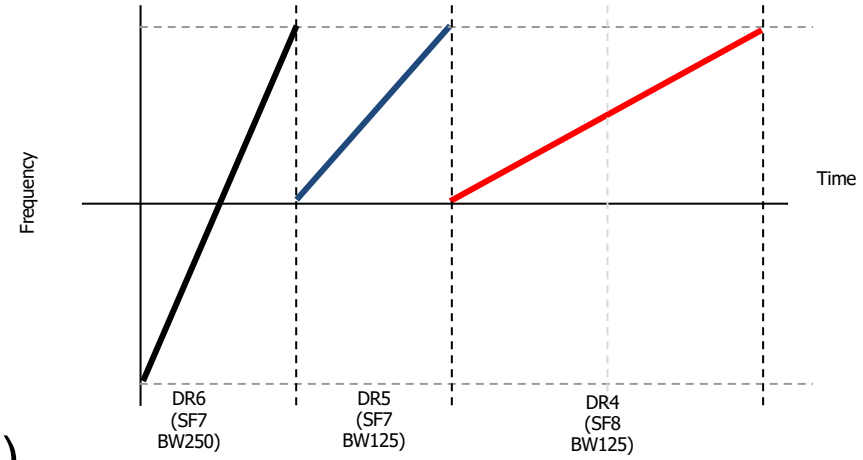
Source: https://en.wikipedia.org/wiki/Chirp_spread_spectrum.





LoRa parameters

- Data Rate (DR)
  - Spreading Factor (SF)
    1 symbol = SF bits
  - Bandwidth (BW)
- Carrier Frequency (CF)
- Coding Rate (CR)
- Transmission Power (TP)

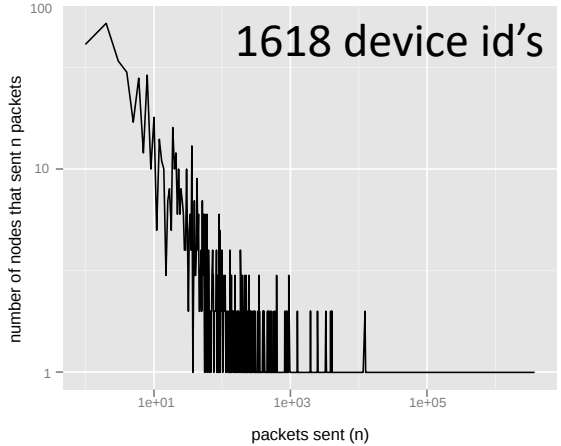


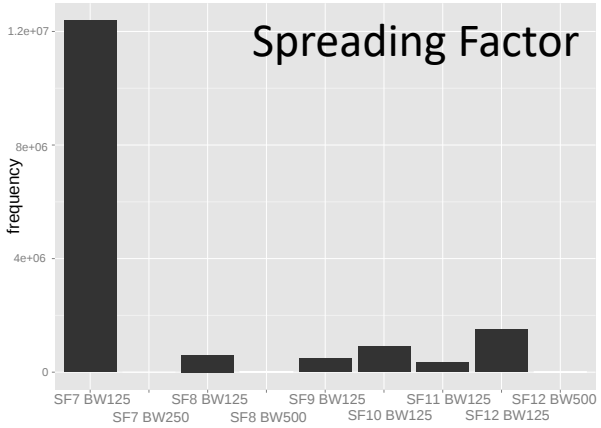
1st large-scale evaluation [1]

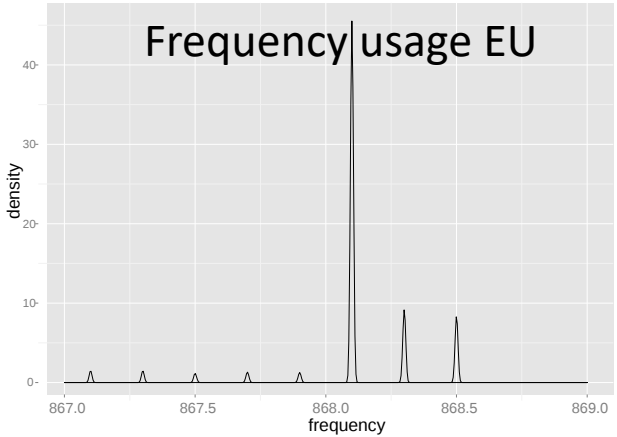
THE THINGS NETWORK

[1] N. Blenn and F.A. Kuipers, “LoRaWAN in the Wild: Measurements from The Things Network,” arXiv:1706.03086.

Results from the wild







TU Delft

Link quality

TU Delft

[2] S. Demetri, M. Zuniga, G.P. Picco, F.A. Kuipers, L. Bruzzone, and T. Telkamp, “Automated Estimation of Link Quality for LoRa: A Remote Sensing Approach,” Proc. of ACM/IEEE IPSN 2019.

How far can you go?

It depends!

hardware

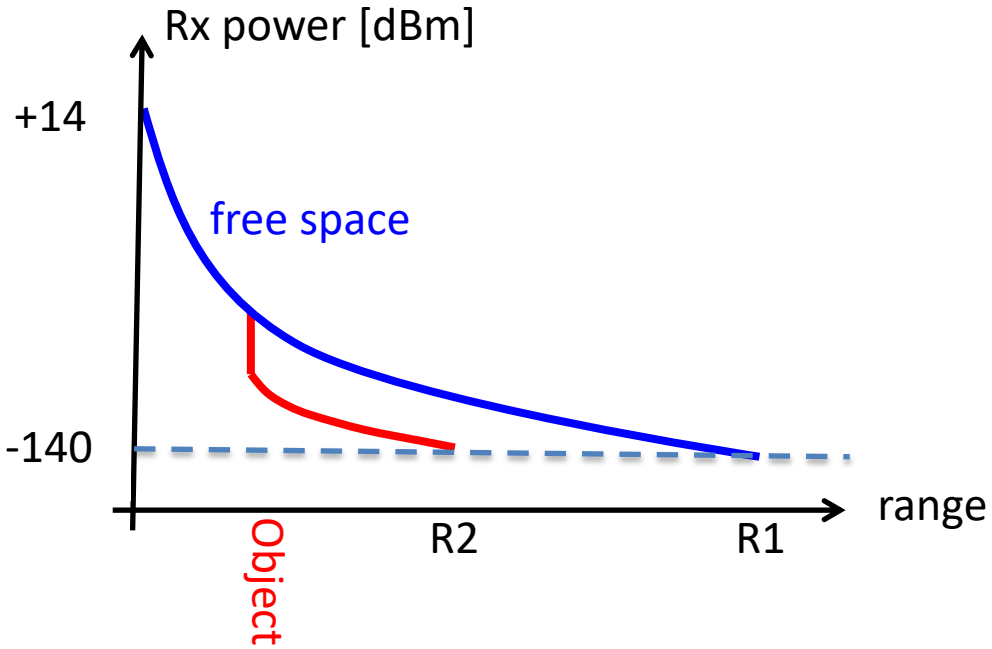
interference

mobility

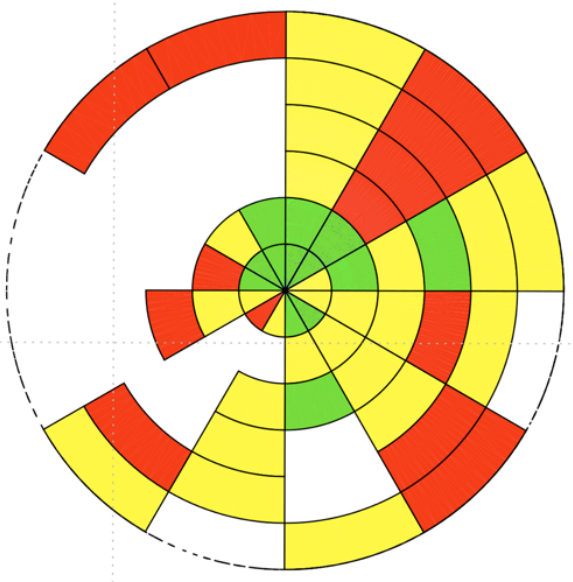
objects
in the environment

humidity

temperature



Typical gateway coverage



Measuring coverage is costly: we need an automated approach!

GOOD
> -100 dBm

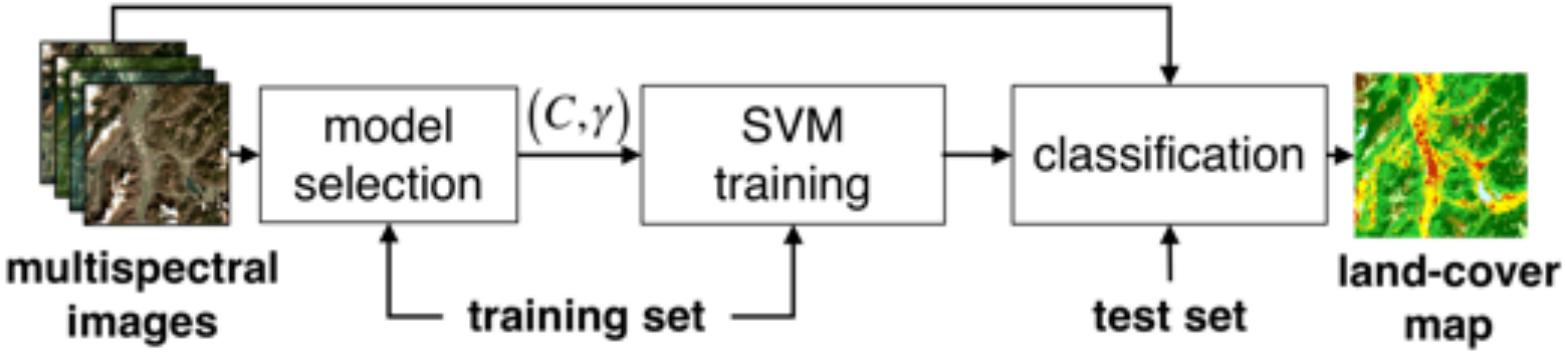
INTERMEDIATE
[-115 -100] dBm

BAD
< -115 dBm

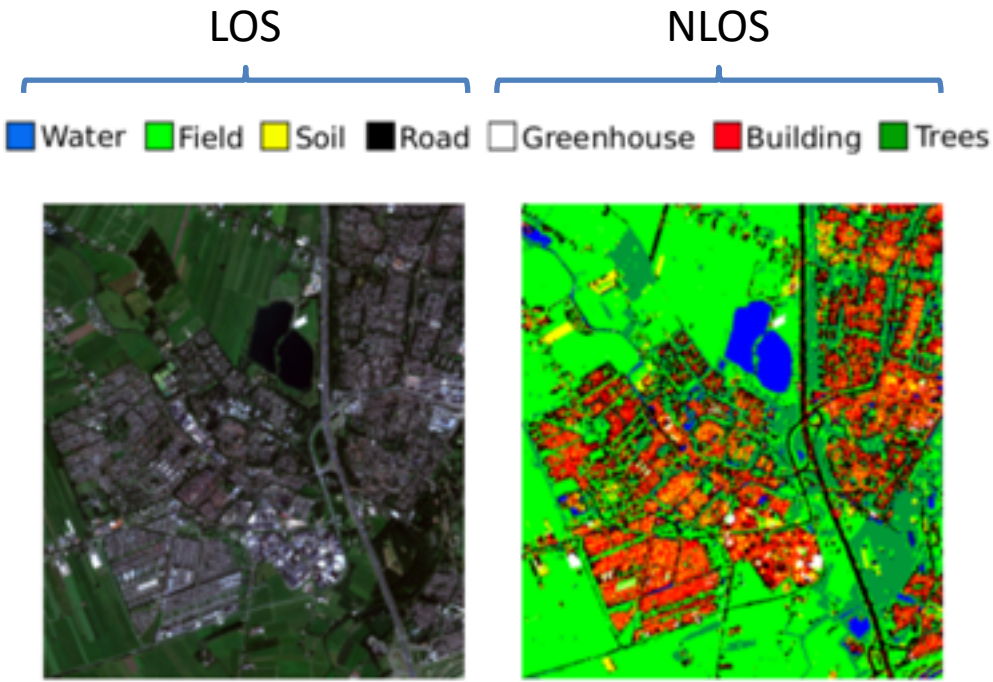
No reception

TU Delft

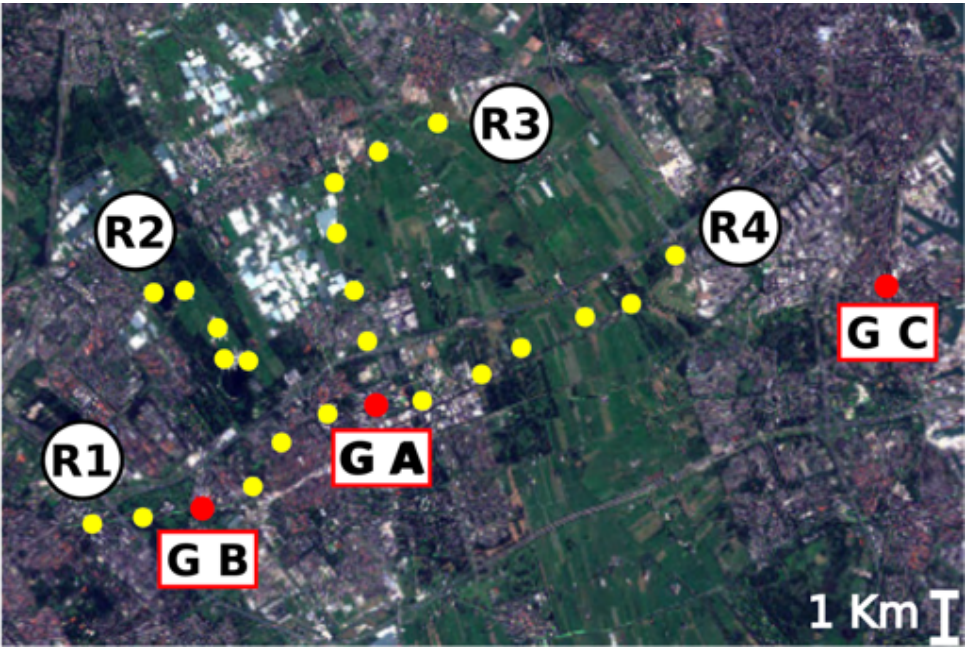
Remote sensing

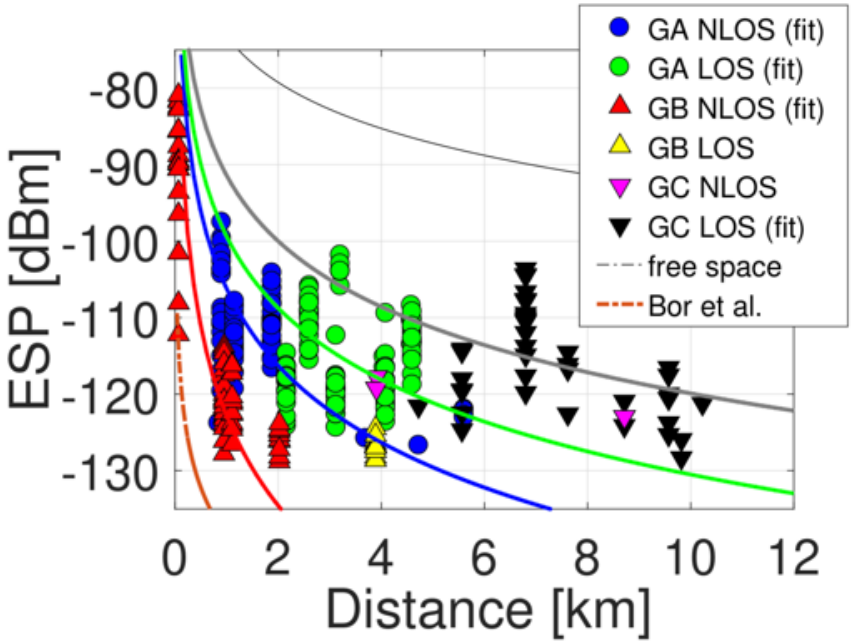


Land-cover classes



Link quality per class





TU Delft

Okumura-Hata model

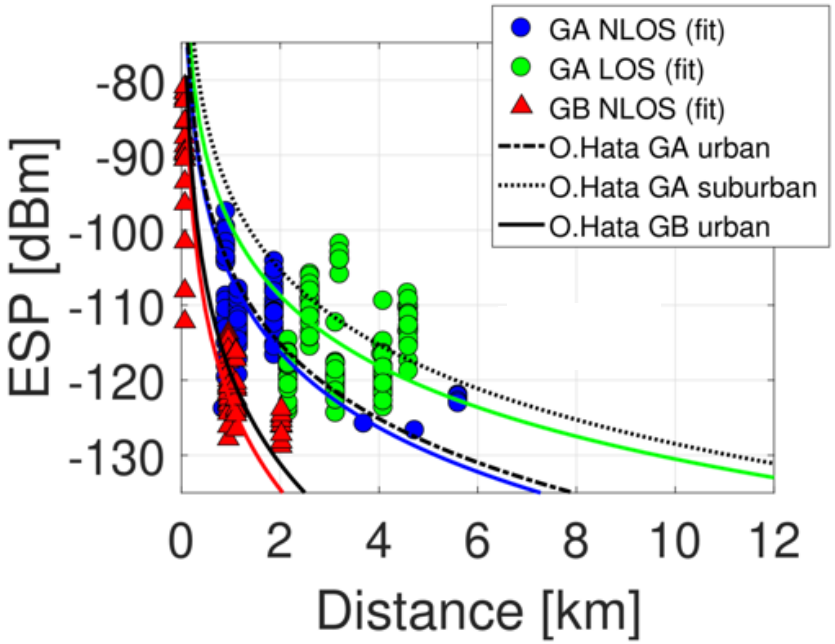
gateway height

end-device height

$$PL = f\left(H_{gw}, H_{ed}, d\right)$$

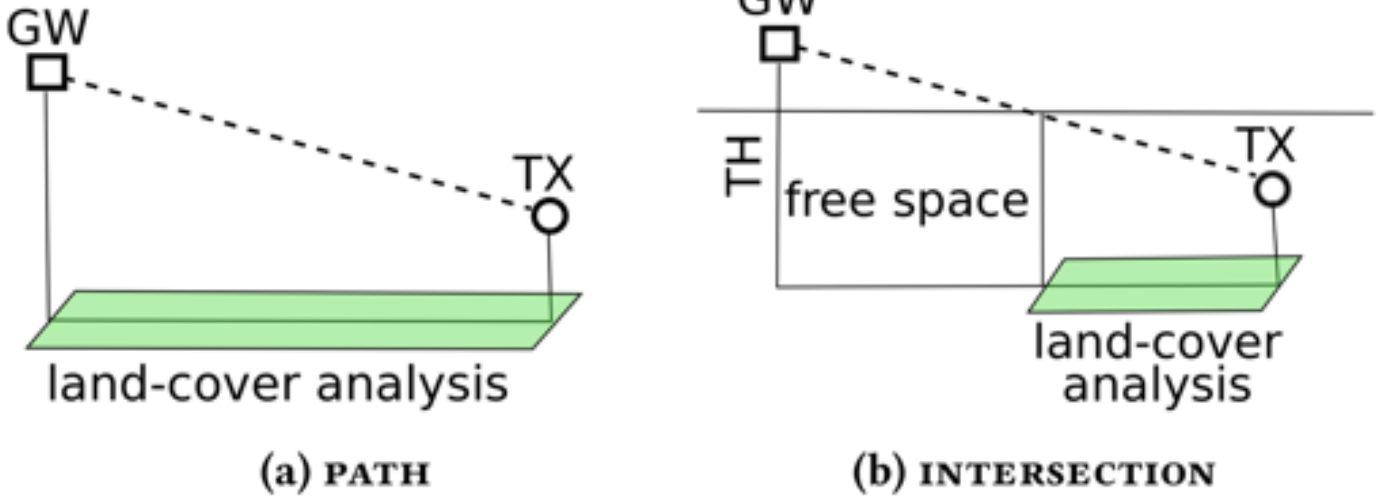
distance

① urban small city → **NLOS**
② urban large city
③ suburban → **LOS**
④ rural



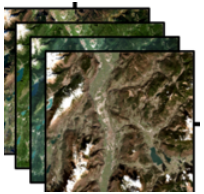
TU Delft

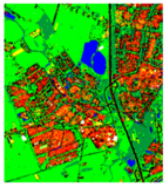
Dominant land-cover class

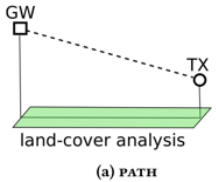


Complete tool

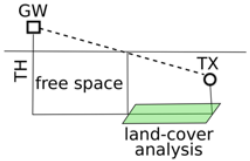
Multispectral satellite images → Land cover map → Land cover analysis → Okumura-Hata → Automatic coverage prediction





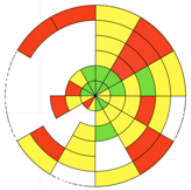


(a) PATH



(b) INTERSECTION

$$PL = f\left(H_{gw}, H_{ed}, d\right)$$



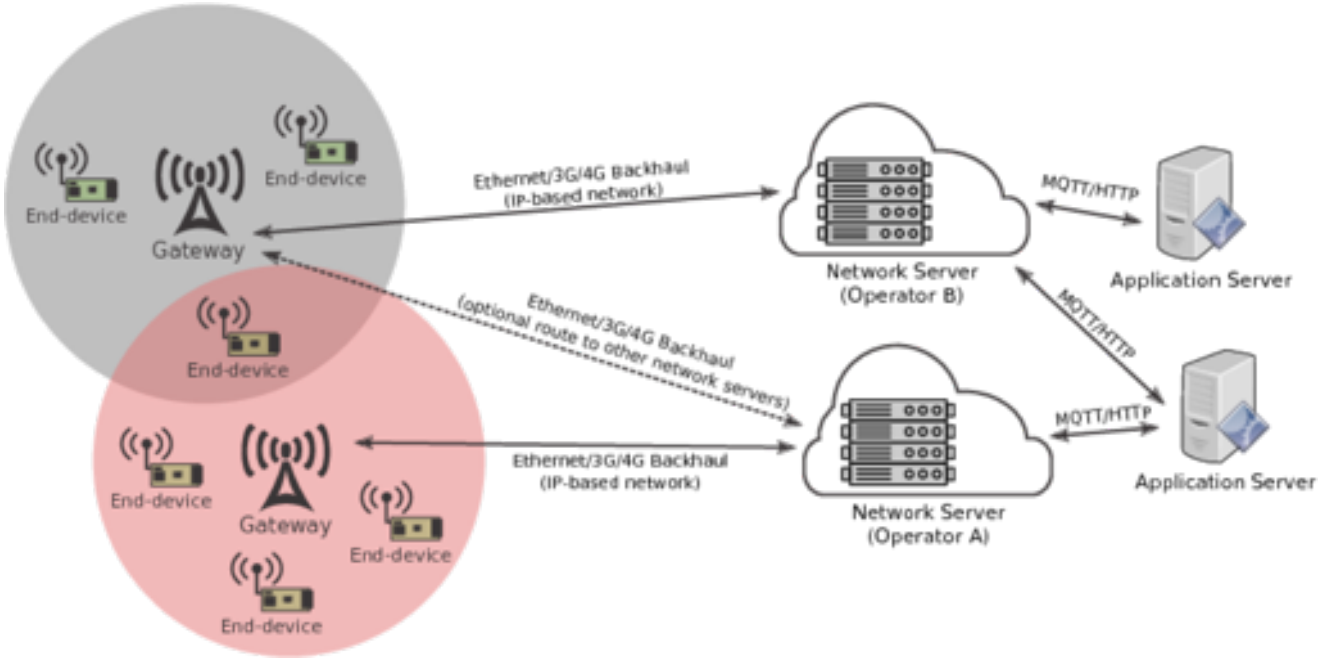
Estimation error

G_{id}	PATH		INTERSECTION		Free		Bor	
	avg	stdd	avg	stdd	avg	stdd	avg	stdd
all	8.73	6.67	8.71	6.62	32.24	10.61	33.53	10.71
1	9.73	8.01	9.64	7.69	25.66	9.93	40.58	10.59
7	7.11	5.73	6.53	5.25	32.18	6.58	33.91	6.63
8	7.90	5.36	8.03	5.56	35.68	8.36	29.92	8.31
11	10.14	5.55	9.67	5.25	42.58	8.43	22.97	8.46
13	12.28	7.22	13.63	7.69	43.22	8.28	21.97	8.17

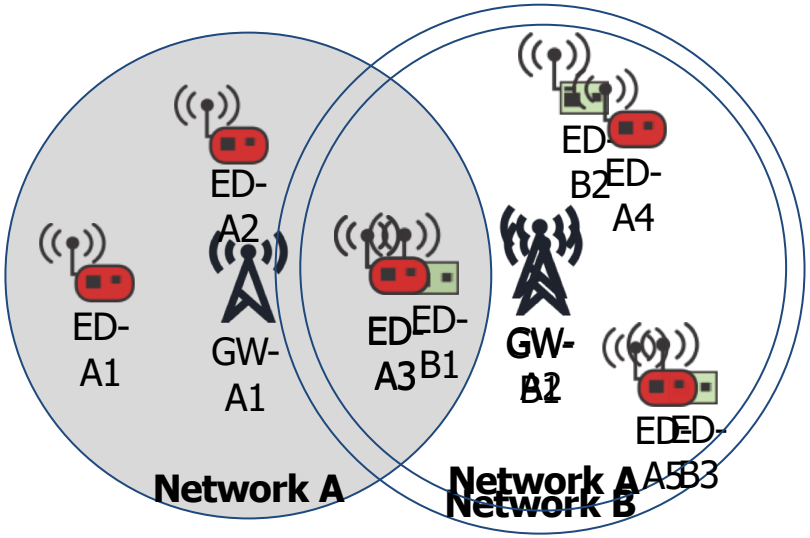
Collisions & the capture effect

[3] A. Rahmadhani and F.A. Kuipers, “When LoRaWAN Frames Collide,” Proc. of ACM WiNTECH 2018.

LoRaWAN architecture

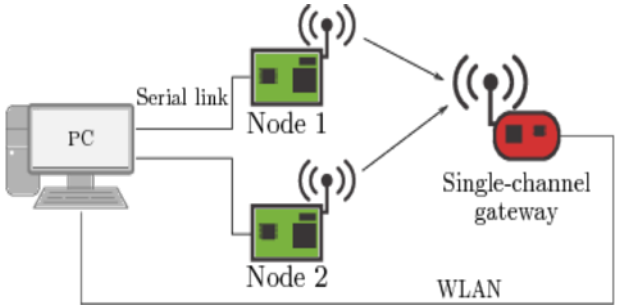


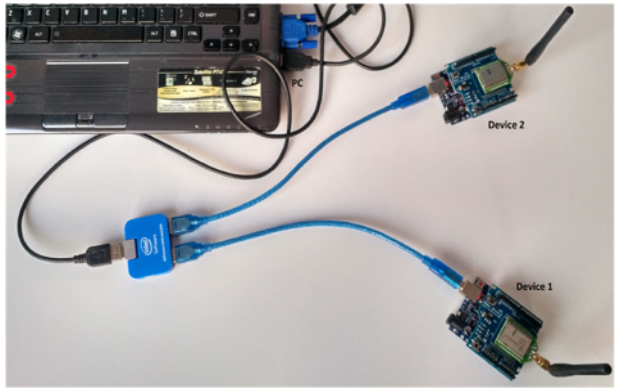
Collisions are bound to happen



Single GW experiment setup

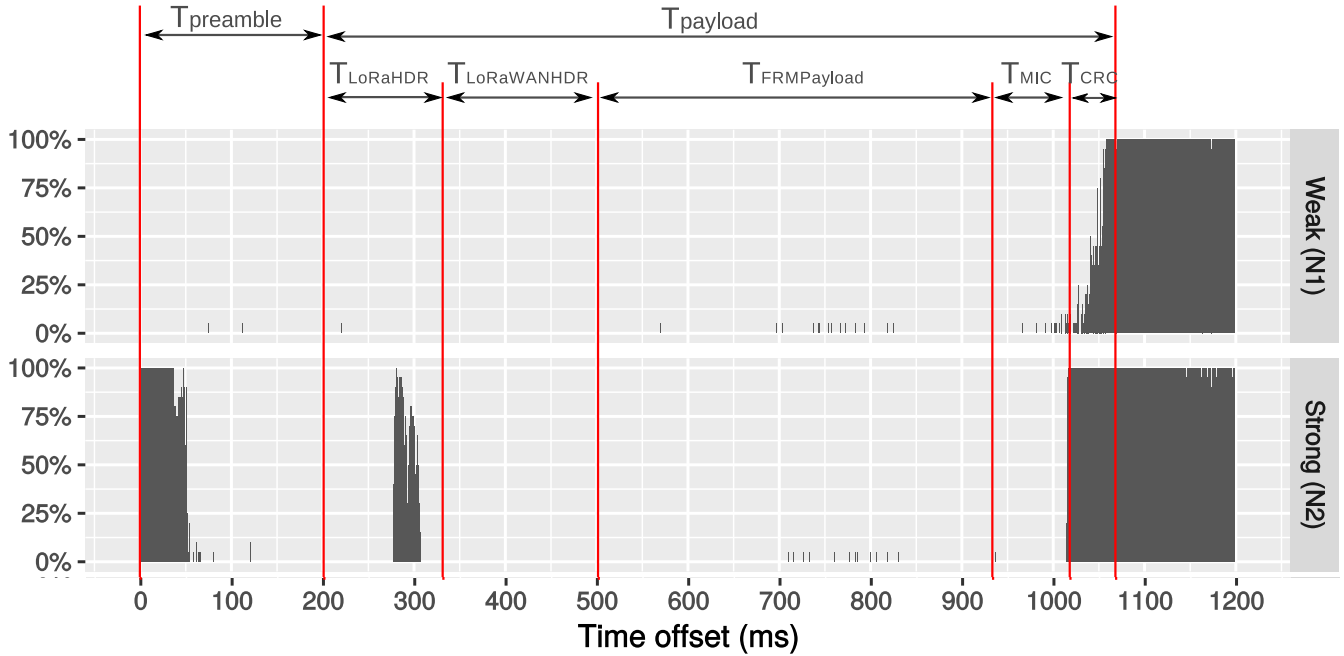
Parameters	Device 1 (N1)	Device 2 (N2)
Equal received power (TP)	2 dBm	
Different transmission powers (TP)	2 dBm	8 dBm
Time offset	0 ms	++ 1 ms (delayed)
Packets per time offset	20	
Frequency (CF)	869.7 MHz (SF11 plotted)	
Payload size	26 bytes	
Network	Private	
Distance to gateway (LOS)	5 m	
Distance to gateway (NLOS)	30 m	





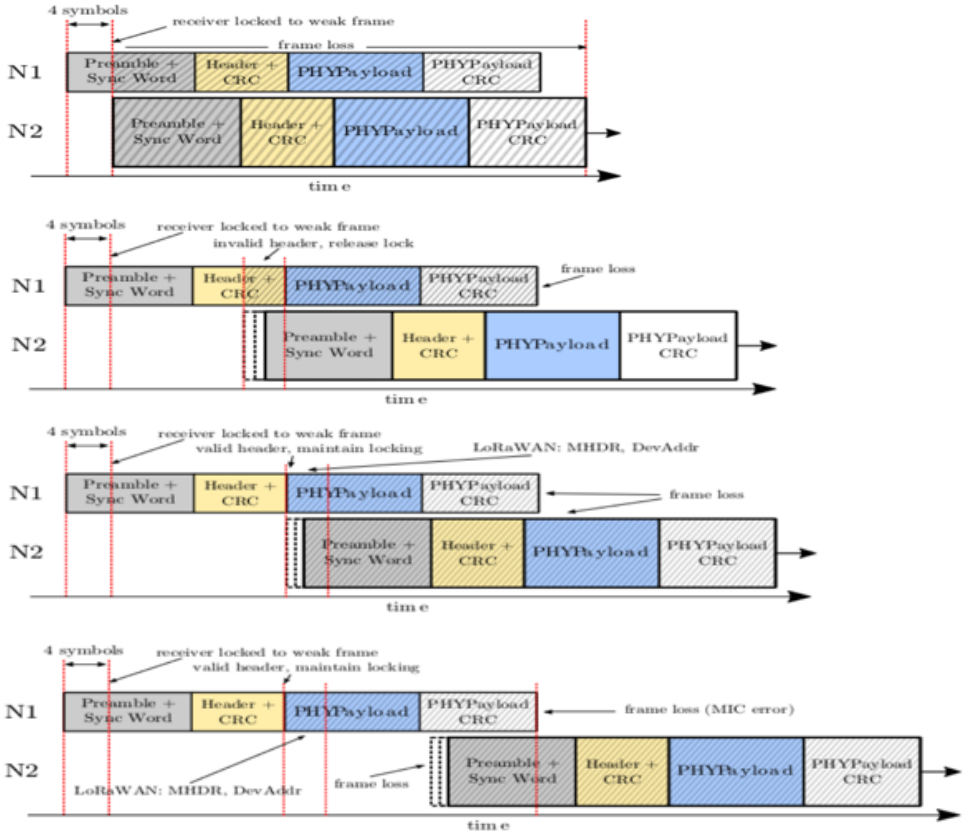
Data Extraction Rate (DER)

DER: Ratio of received frames (at application layer) to transmitted frames



Frame loss conditions

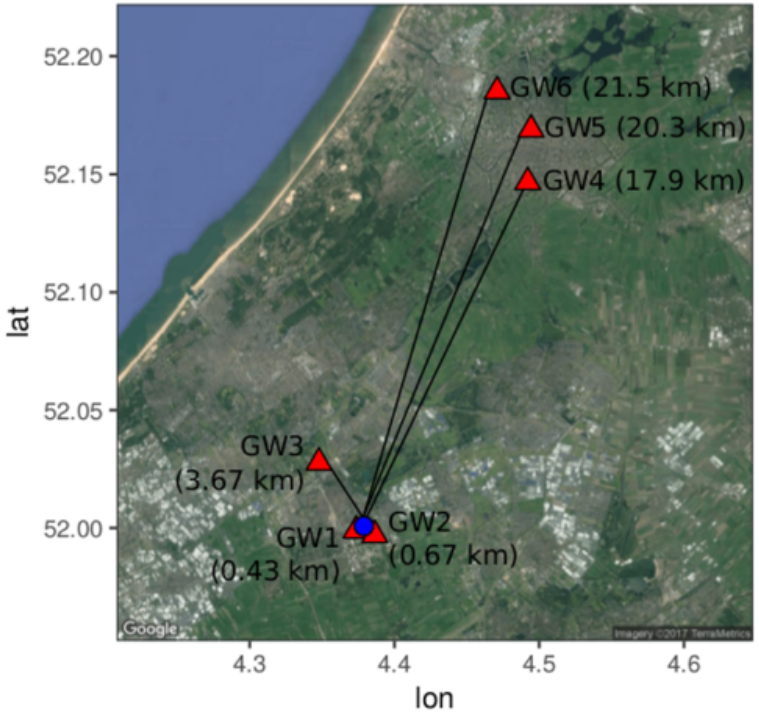
- Both frames get destroyed (preamble lock)
- Weaker frame gets destroyed, stronger frame survives (LoRa header of the weaker frame gets destroyed, receiver immediately starts reading new frame)
- Both frames get destroyed (LoRa header of the weaker frame OK, keeps lock)
- Both frames get destroyed (MIC/Payload CRC error)



TU Delft

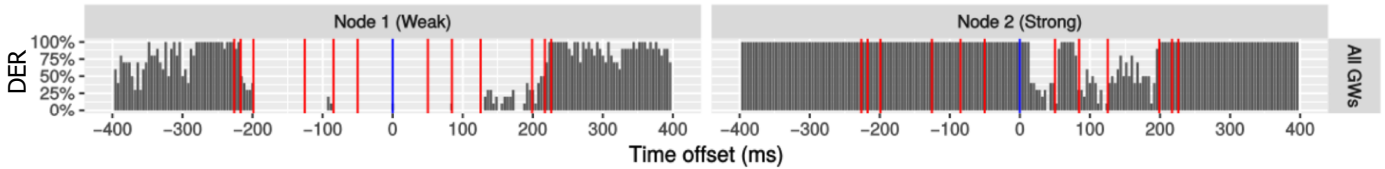
Multiple GWs experiment setup

Parameters	Device 1 (N1)	Device 2 (N2)
Same network scenario	TTN	
Different networks	TTN	KPN
Transmission power (TP)	8 dBm	14 dBm
Time offset	0 ms	++ 1 symbol (delayed)
Frequency (CF)	868.1 MHz	
Data Rate	SF9BW125	



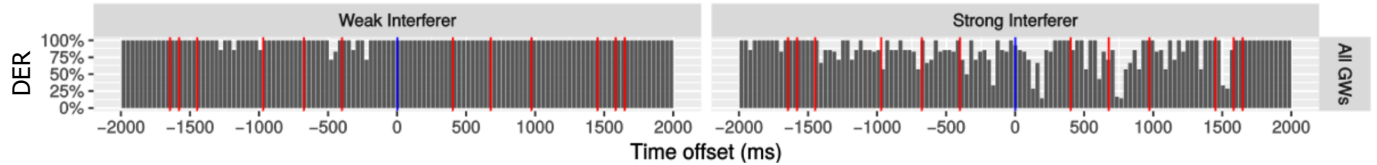
DER multiple GWs

Same network (TTN)



Different networks (TTN & KPN):

- KPN device as interferer
- KPN device received 2 new frequency channels (867.7 and 867.9 MHz) due to ADR



TU Delft

Insigths

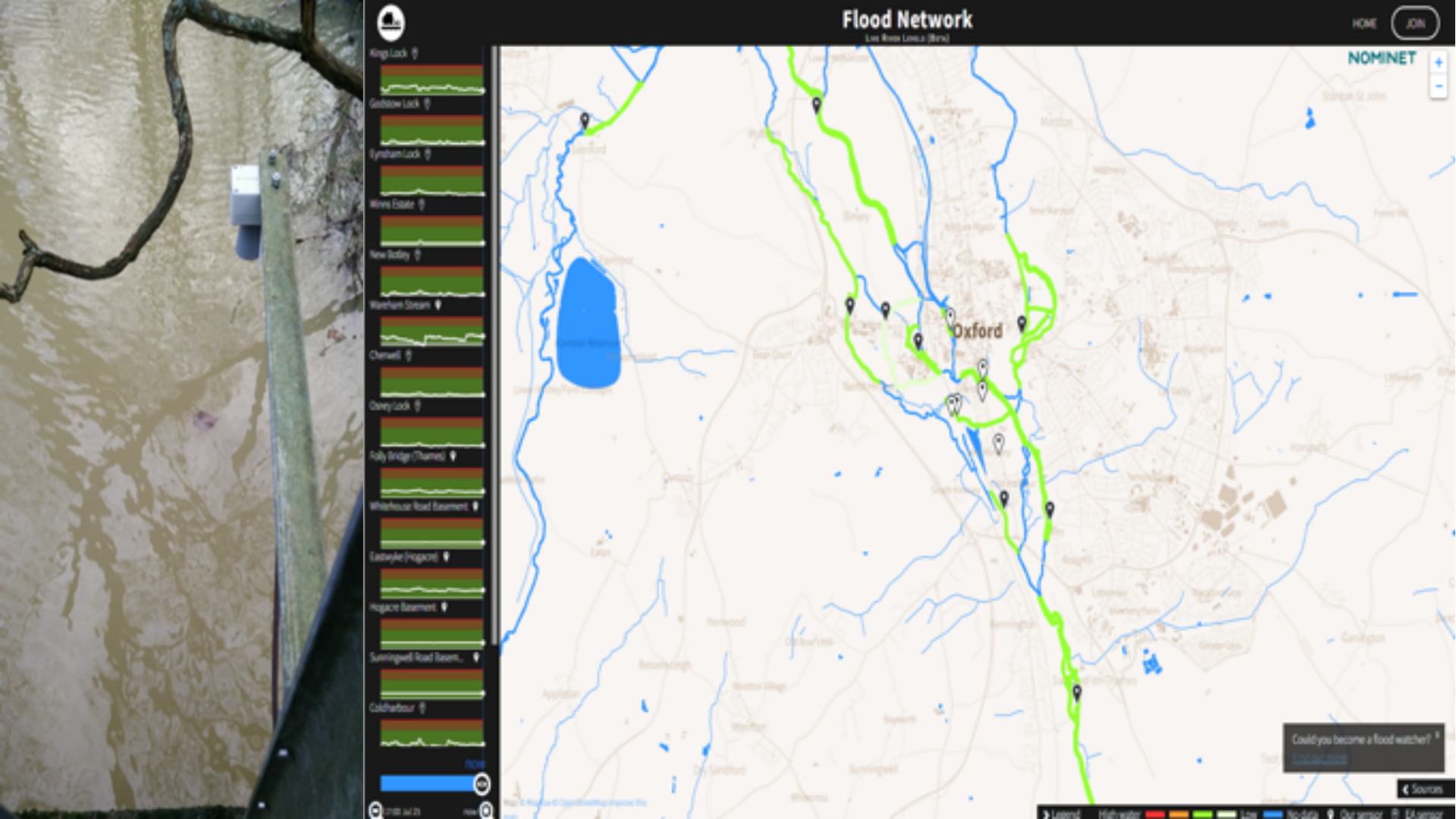
- Conditions for the capture effect to occur:
  - The stronger frame overlaps with the LoRa header of the weaker frame
  - Both frames might still be decoded whenever the stronger frame only slightly overlaps with the payload CRC of the weaker frame
- Adding more gateways improves DER:
  - Stronger signals are received by more distant gateways than weaker signals

LoRaWAN security vulnerabilities

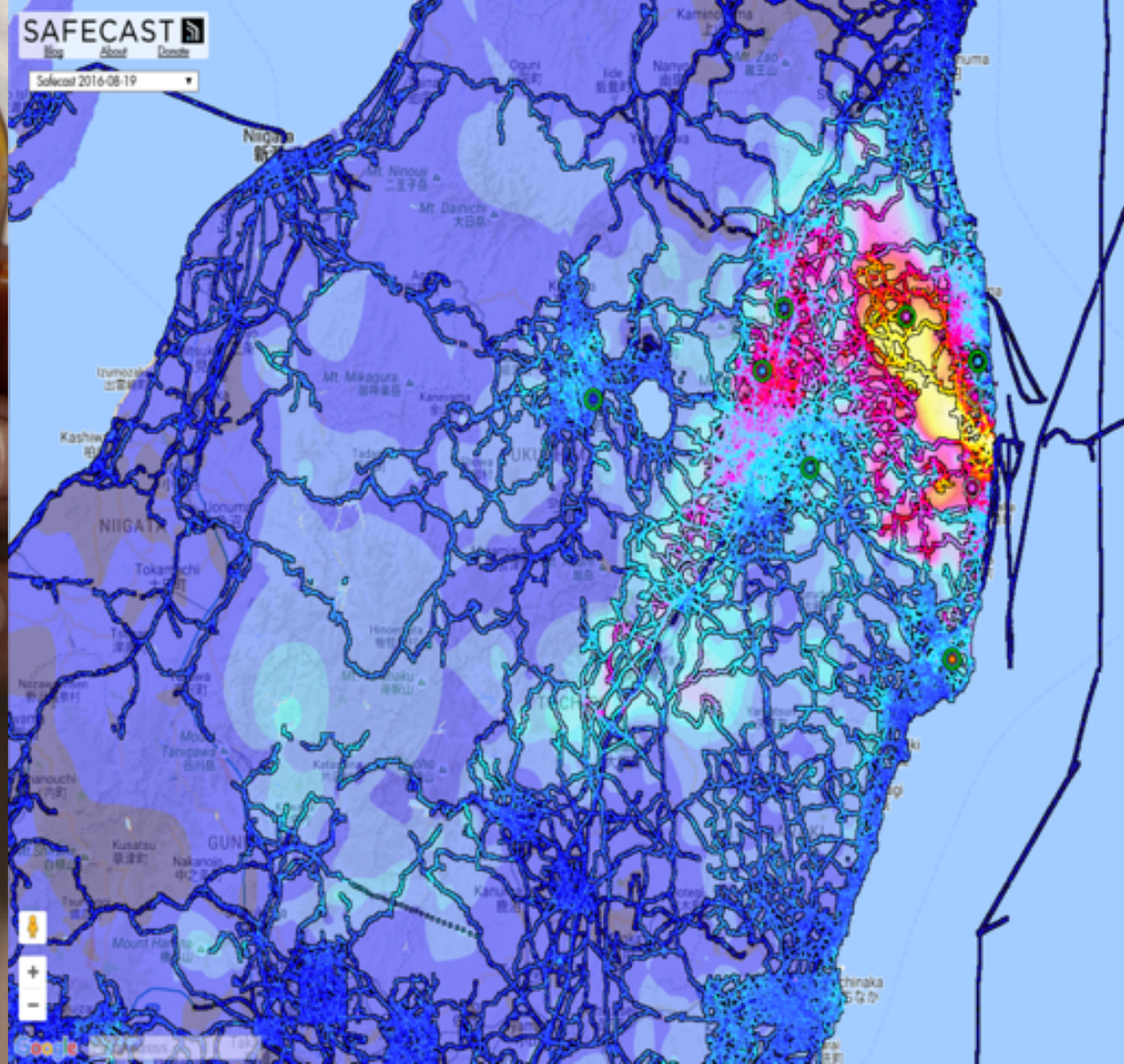
Do not try this at home ;)

TU Delft

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


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


0.144 uS/h
SAFECAST


SAFECAST
Blog
About
Donate
Safecast 2016-08-19
NIIGATA


Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

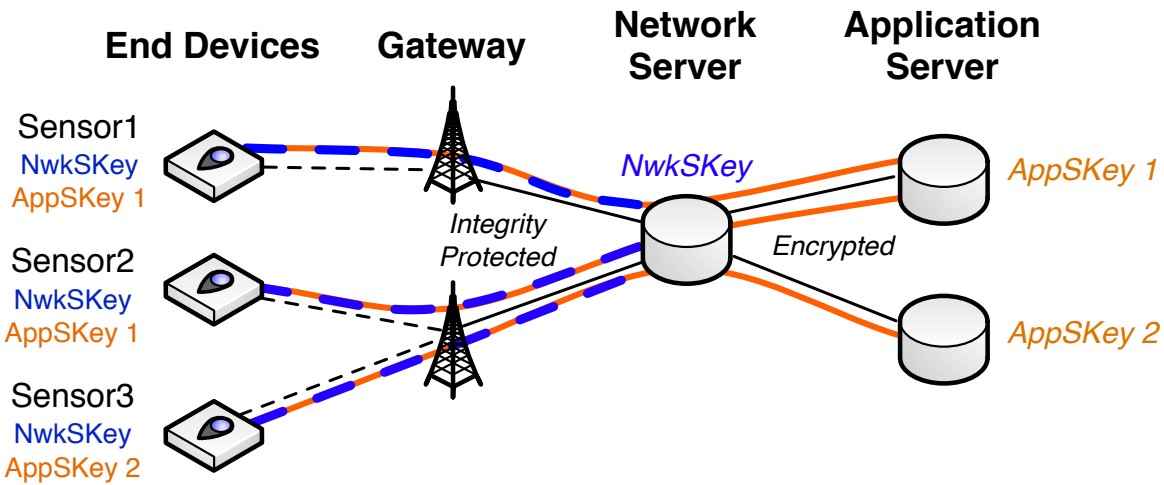

nest

TU Delft

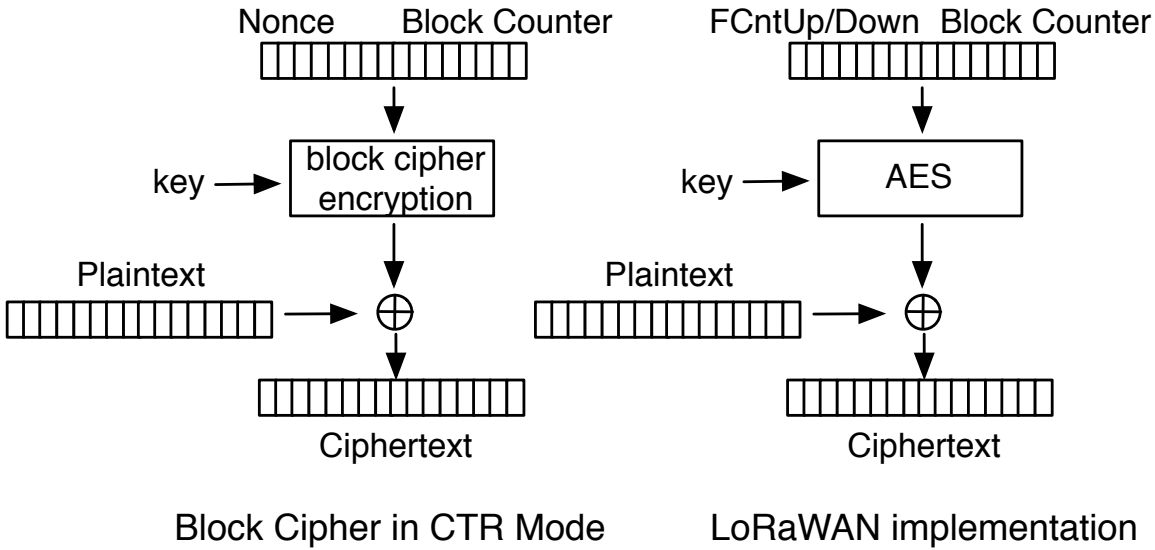
Security features of LoRaWAN

- 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

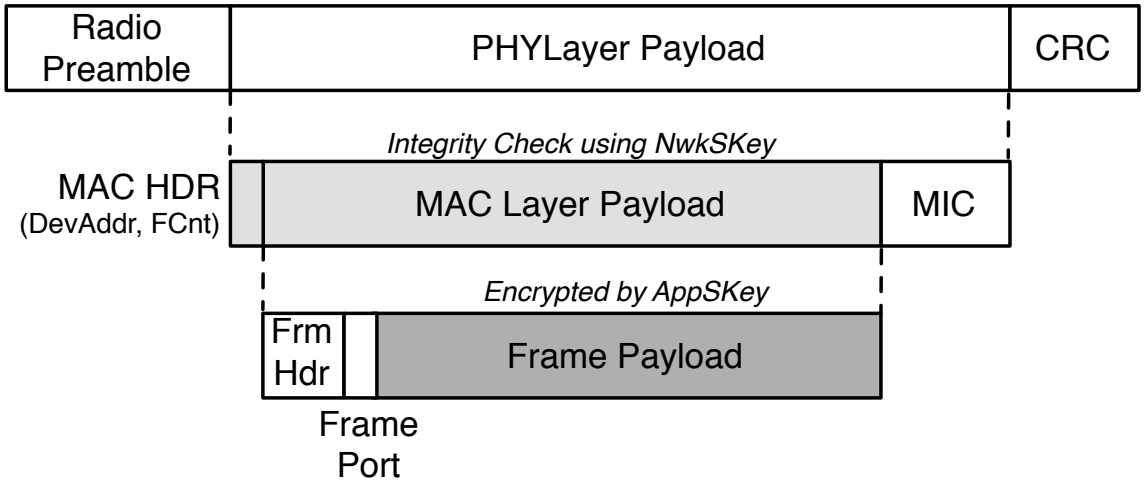


Enrollment protocol

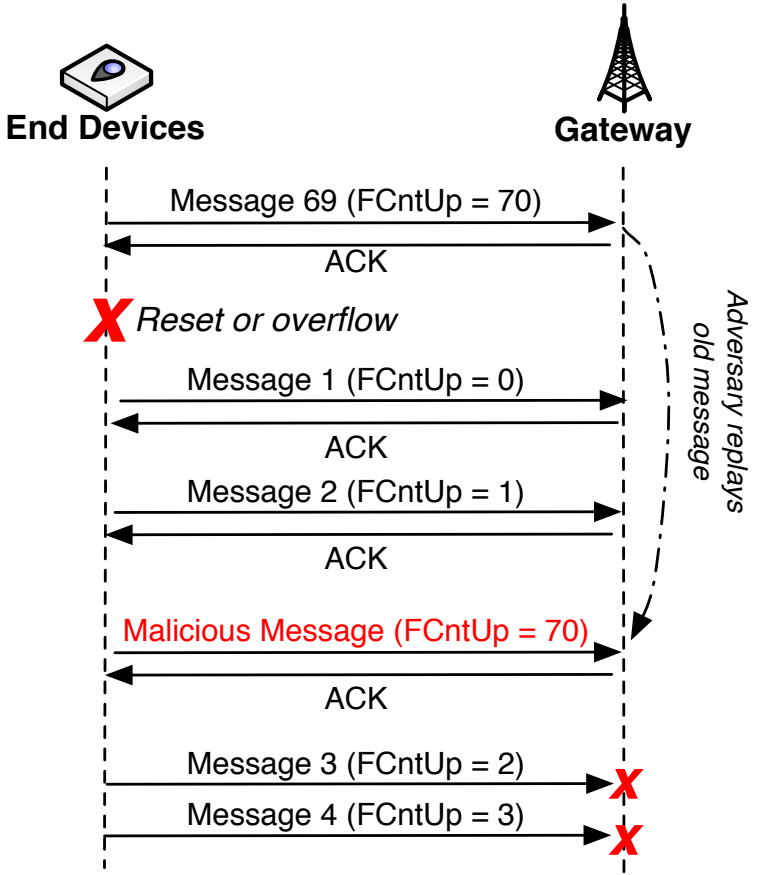
- OTAA:
  - End-device sends *Join Request*
  - Network server sends *Join Accept* with AppNonce
  - AppNonce to generate NwkSKey and AppSKey

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

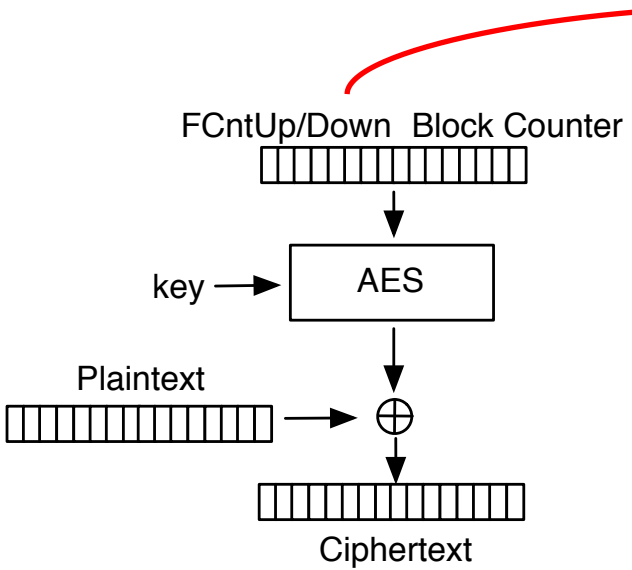
Integrity and Authenticity validation



Replay attack



Eavesdropping

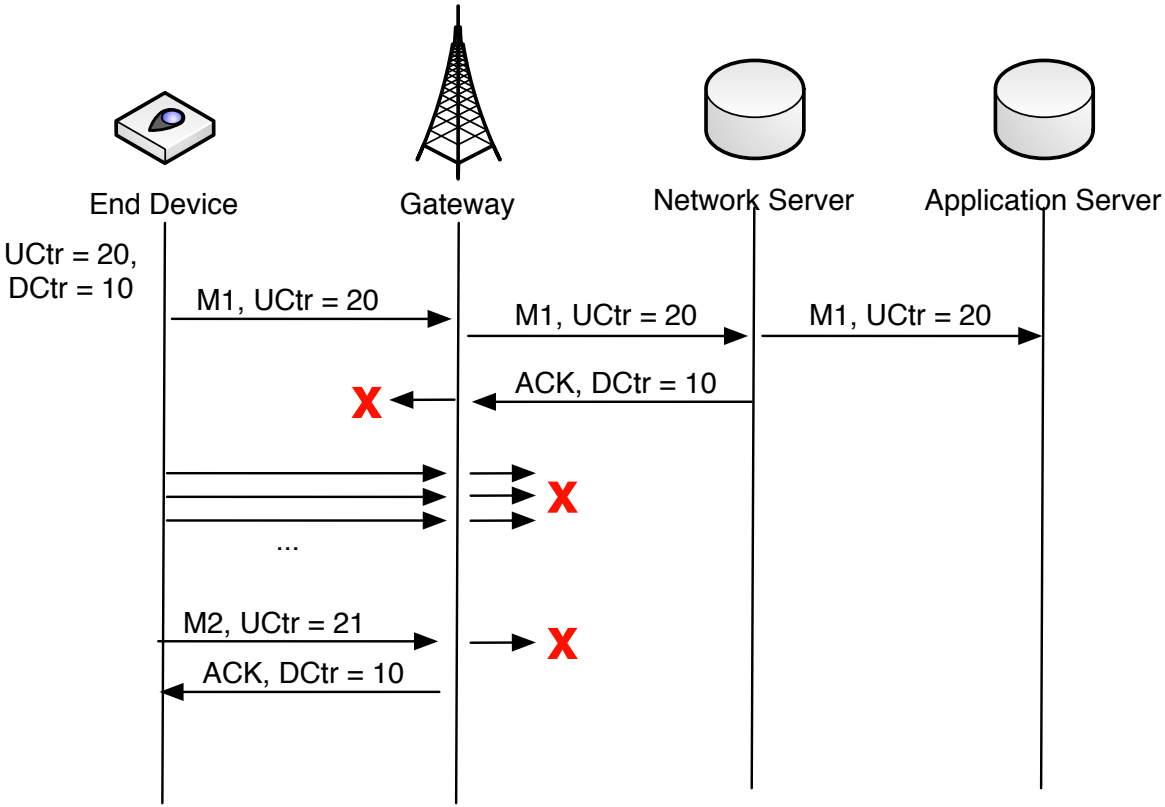


LoRaWAN implementation

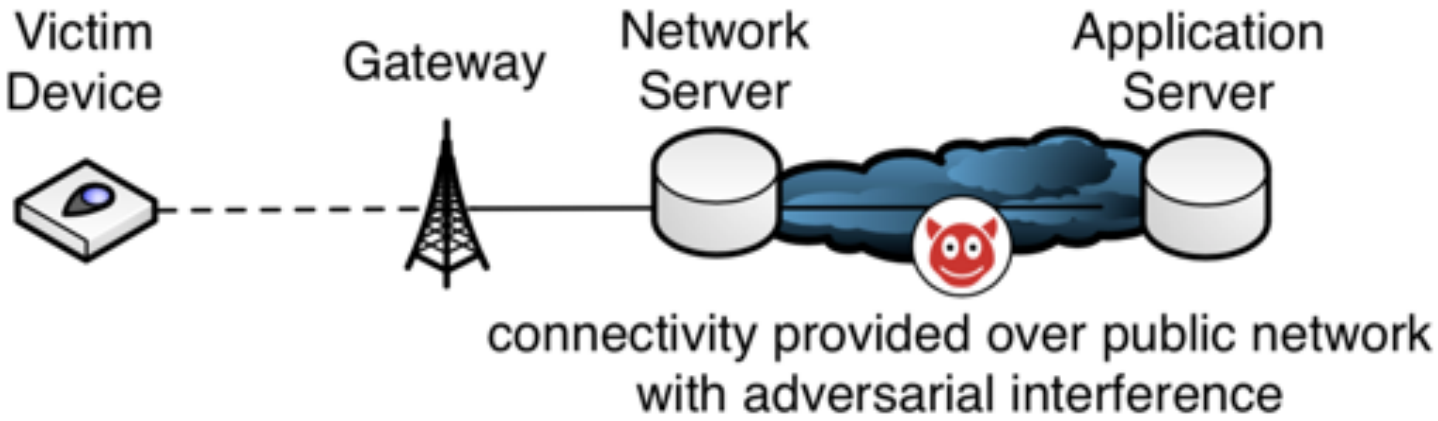
$$C_1 \oplus C_2 = (P_1 \oplus K) \oplus (P_2 \oplus K)$$
$$= P_1 \oplus P_2 \oplus \underbrace{(K \oplus K)}_{\text{cancels out}}$$
$$= P_1 \oplus P_2.$$

Guess one word to derive the other

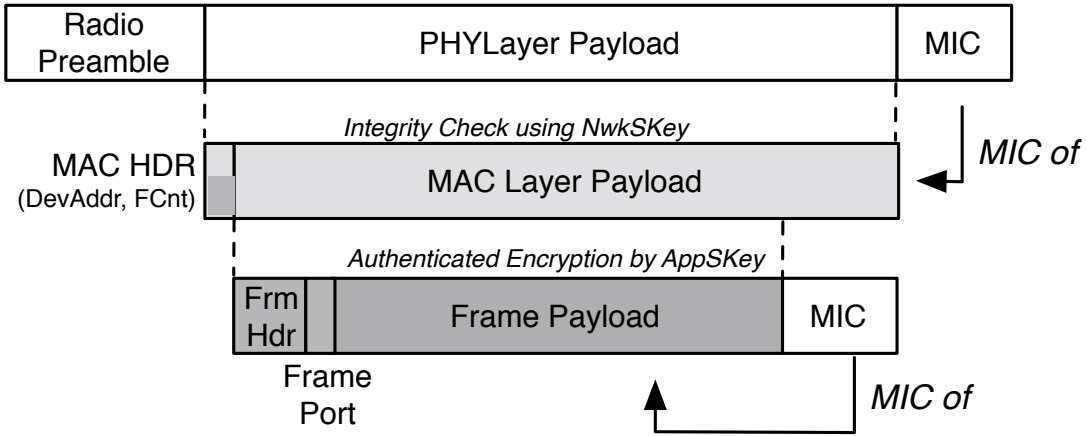
ACK spoofing



Bit flipping



Counter-measure



More info? Contact me at

Fernando Kuipers
Delft University of Technology
F.A.Kuipers@tudelft.nl
https://fernandokuipers.nl/