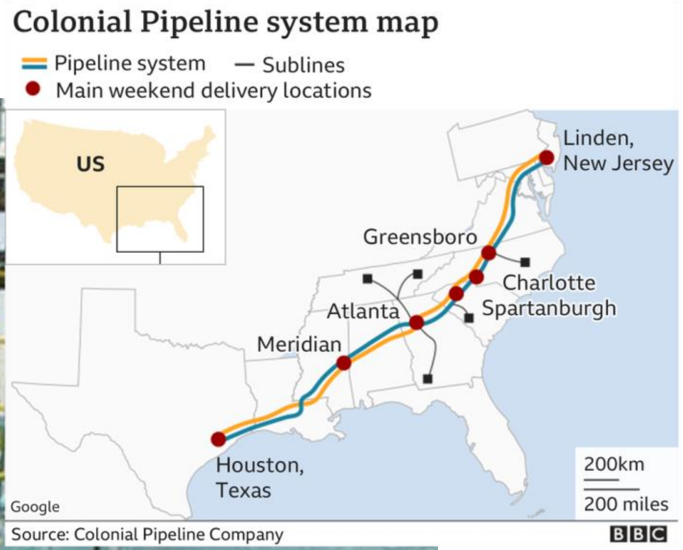
Lecture #6: IoT security in non-carpeted areas

Antonia Affinito, Etienne Khan, Ting-Han Chen, and Cristian Hesselman

University of Twente | June 12, 2024

Colonial Pipeline, May 2021



Colonial Pipeline system map

Source: Colonial Pipeline Company

https://www.bbc.com/news/technology-57063636

Today’s agenda

- Admin
- Introduction to today’s lecture
- Paper #1: security in LoraWAN networks
- Paper #2: privacy of opportunistic networks
- Feedback

Admin

Important dates

- Lab report (PDF) and required files: **Wed Jun 19, 9 AM CEST**
- Written exam: **Wed July 3, 13:45-15:45** ⚠
- Alle summaries and lab reports to be submitted through CANVAS

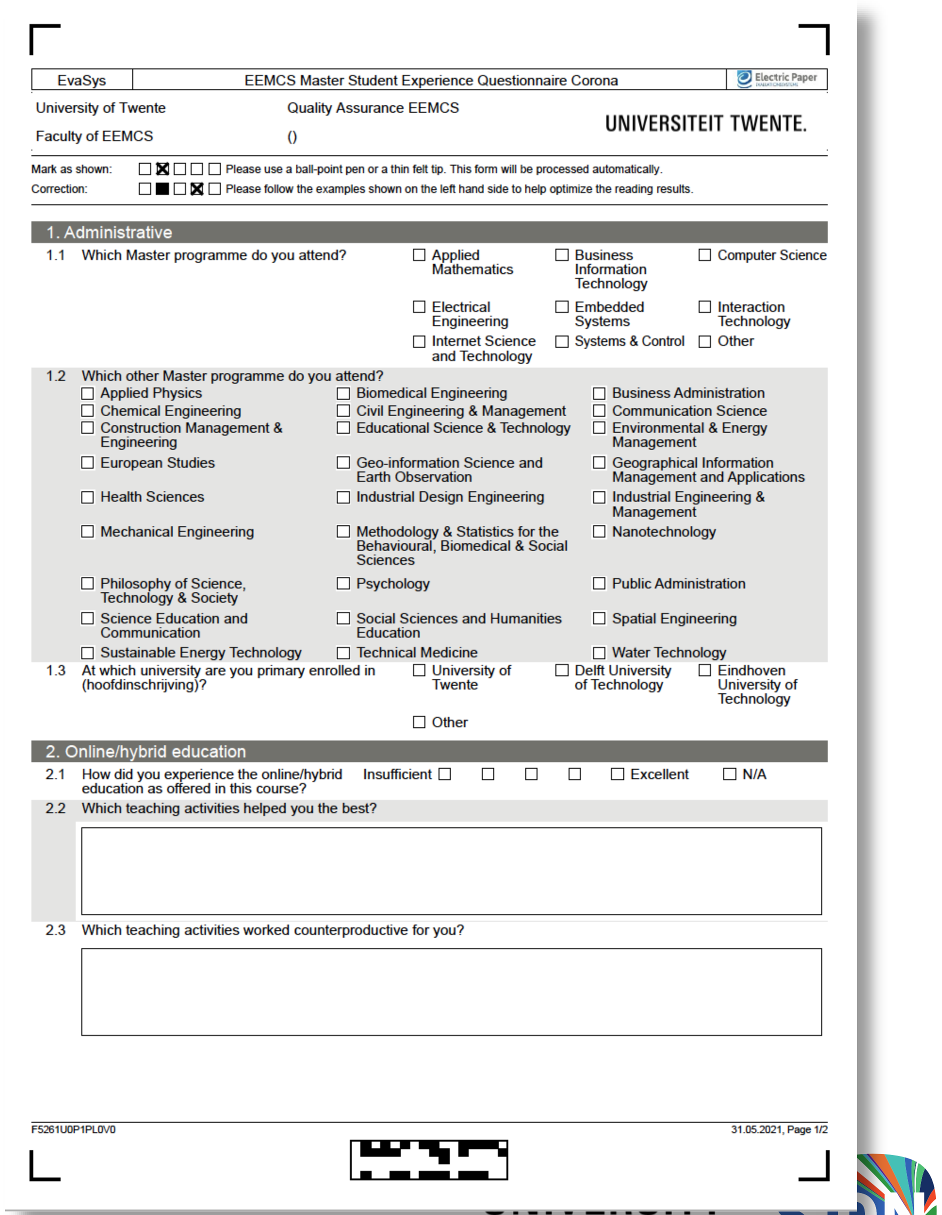
Interactive lectures, so please speak up!

Schedule

Lecture	Date	Contents
R1	May 1	Course introduction
R2	May 8	IoT and Internet Core Protocols
G1	May 14	How the core of the Internet works
R3	May 15	IoT Edge Security Systems
	May 22	No lecture (as several of your teachers will be in Dresden :)
R4	May 29	IoT Botnet Measurements 1
R5	Jun 5	IoT Botnet Measurements 2
R6	Jun 12	IoT Security in Non-Carpeted Areas
G2	Jun 14	Security in the new digital world – the Internet of Things
R7	Jun 19	IoT Device Security
	Jun 26	No lecture (so you can study for the exam :)

Official feedback forms

- Survey by EEMCS Quality Assurance folks
- Will be sent out on in the next week or so
- Please fill it out, your feedback is **crucial** for us to further improve the course!
- Next year's students will thank you for it ;-)
- We'll let you know how we handled your feedback



EvaSys	EEMCS Master Student Experience Questionnaire Corona	Electric Paper

University of Twente — Quality Assurance EEMCS

Faculty of EEMCS — ()

UNIVERSITEIT TWENTE.

Mark as shown: □ ☒ □ □ □ Please use a ball-point pen or a thin felt tip. This form will be processed automatically.

Correction: □ ■ □ ☒ □ Please follow the examples shown on the left hand side to help optimize the reading results.

1. Administrative

1.1 Which Master programme do you attend?

□ Applied Mathematics
□ Electrical Engineering
□ Internet Science and Technology
□ Business Information Technology
□ Embedded Systems
□ Systems & Control
□ Computer Science
□ Interaction Technology
□ Other

1.2 Which other Master programme do you attend?

□ Applied Physics
□ Chemical Engineering
□ Construction Management & Engineering
□ European Studies
□ Health Sciences
□ Mechanical Engineering
□ Philosophy of Science, Technology & Society
□ Science Education and Communication
□ Sustainable Energy Technology
□ Biomedical Engineering
□ Civil Engineering & Management
□ Educational Science & Technology
□ Geo-information Science and Earth Observation
□ Industrial Design Engineering
□ Methodology & Statistics for the Behavioural, Biomedical & Social Sciences
□ Psychology
□ Social Sciences and Humanities Education
□ Technical Medicine
□ Business Administration
□ Communication Science
□ Environmental & Energy Management
□ Geographical Information Management and Applications
□ Industrial Engineering & Management
□ Nanotechnology
□ Public Administration
□ Spatial Engineering
□ Water Technology

1.3 At which university are you primary enrolled in (hoofdinschrijving)?

□ University of Twente
□ Delft University of Technology
□ Eindhoven University of Technology
□ Other

2. Online/hybrid education

2.1 How did you experience the online/hybrid education as offered in this course? Insufficient □ □ □ □ □ Excellent □ N/A

2.2 Which teaching activities helped you the best?

2.3 Which teaching activities worked counterproductive for you?

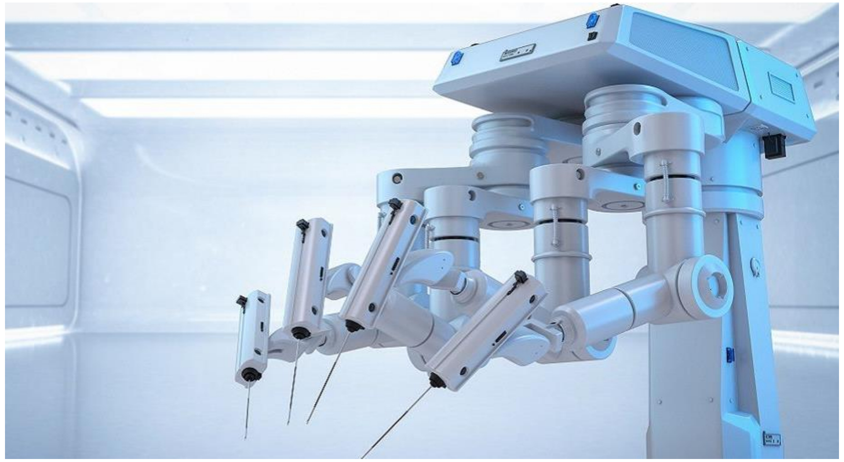
F5261U0P1PL0V0 — 31.05.2021, Page 1/2

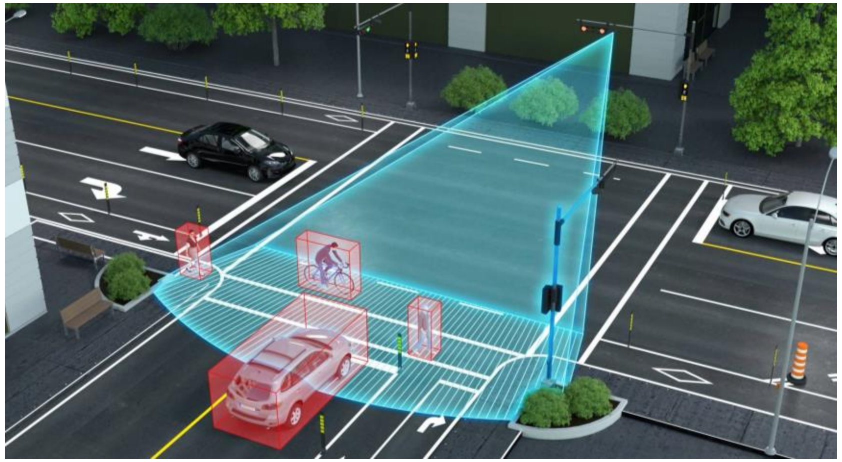
Introduction to today’s lecture

https://www.youtube.com/watch?v=-7xg3DQyOXw

Example: remote truck driving

Motivation for today: IoT goes beyond carpeted areas





But first: group discussion for a broader perspective

- What security and privacy requirements does IoT in “non-carpeted areas” put on the underlying networks?
- What would the impact be on software engineering, hardware engineering, regulation, liability, and so forth?
- Split up in groups of around 5 and discuss!
- Take 5 minutes ☺

So that’s why we selected today’s papers for you

[Lora] X. Wang, E. Karampatzakis, C. Doerr, and F.A. Kuipers, “Security Vulnerabilities in LoRaWAN”, Proc. of the 3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, Florida, USA, April 17-20, 2018

[Sidewalk] T. Despres, S. Patil, A. Tan, J.-L. Watson, and P. Dutta, “Where the sidewalk ends: privacy of opportunistic backhaul”, 15th European Workshop on Systems Security (EuroSec22), Rennes France, April 2022

Today’s learning objective

- After the lecture, you will be able to discuss the security and privacy challenges of IoT networks for “non-carpeted areas”

- Contributes to SSI learning goal #1: “Understand IoT concepts and applications, security threats, technical solutions, and a few relevant standardization efforts in the IETF”

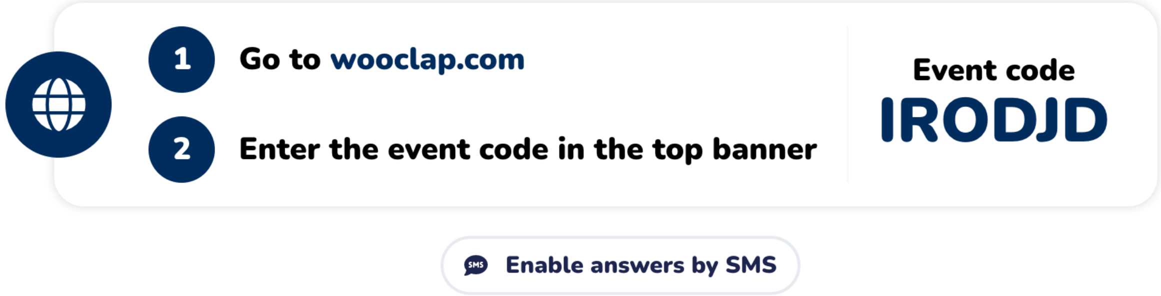
“Security Vulnerabilities in LoRaWAN”

3rd ACM/IEEE International Conference on Internet-of-Things Design and Implementation (IoTDI), Orlando, Florida, USA, April 17-20, 2018

UNIVERSITY OF TWENTE.

SIDN LABS

Get your phones ready!



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

IRODJD

Enable answers by SMS

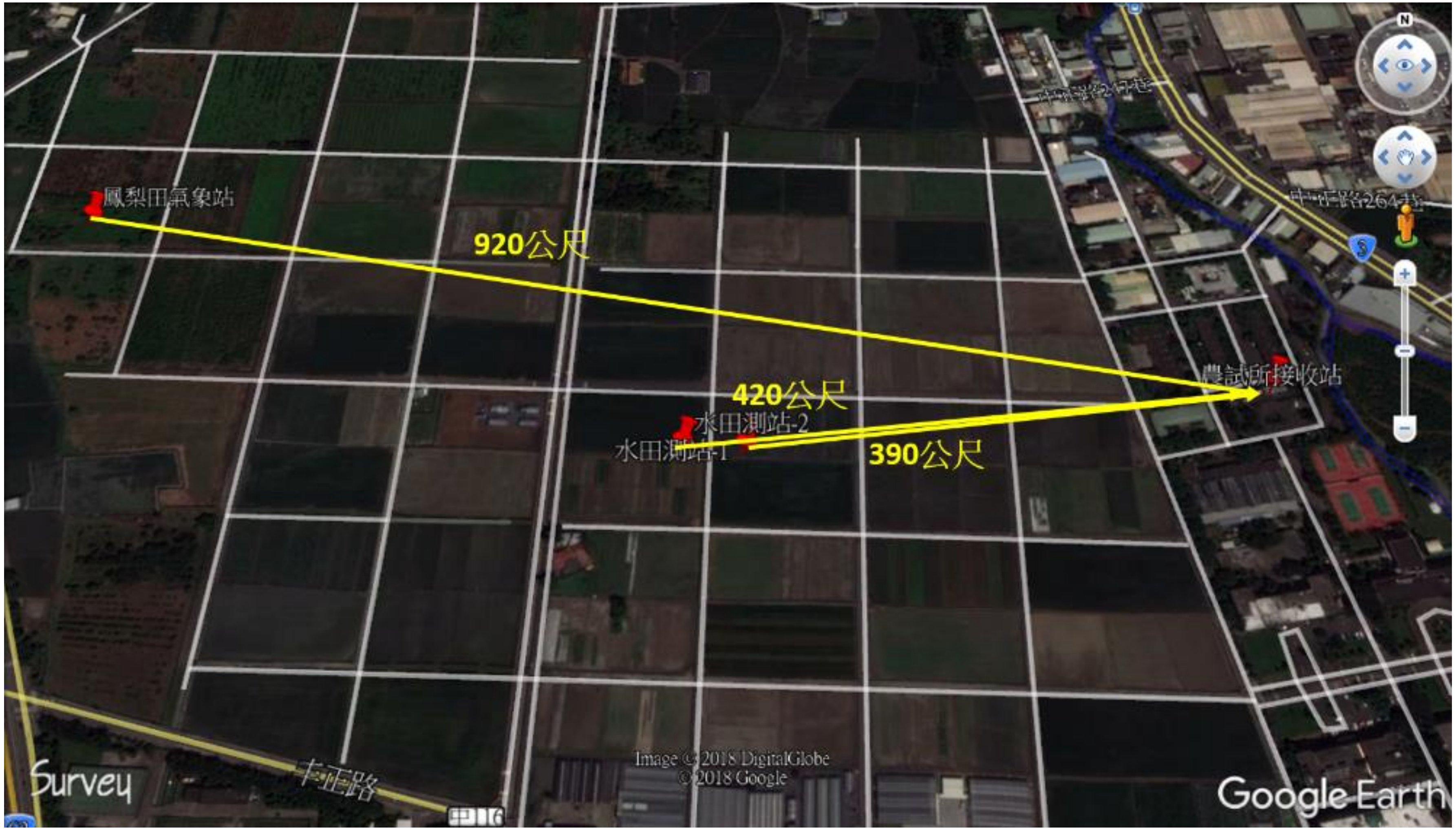
What struck you about the paper?

LoraWAN: low-power, wide-area network, low bitrate

Deutsche Bahn is using LoraWAN, too

https://www.thethingsindustries.com/stories/deutsche-bahn/
https://www.youtube.com/watch?v=7zXNnb2qr6s

Long distance communications

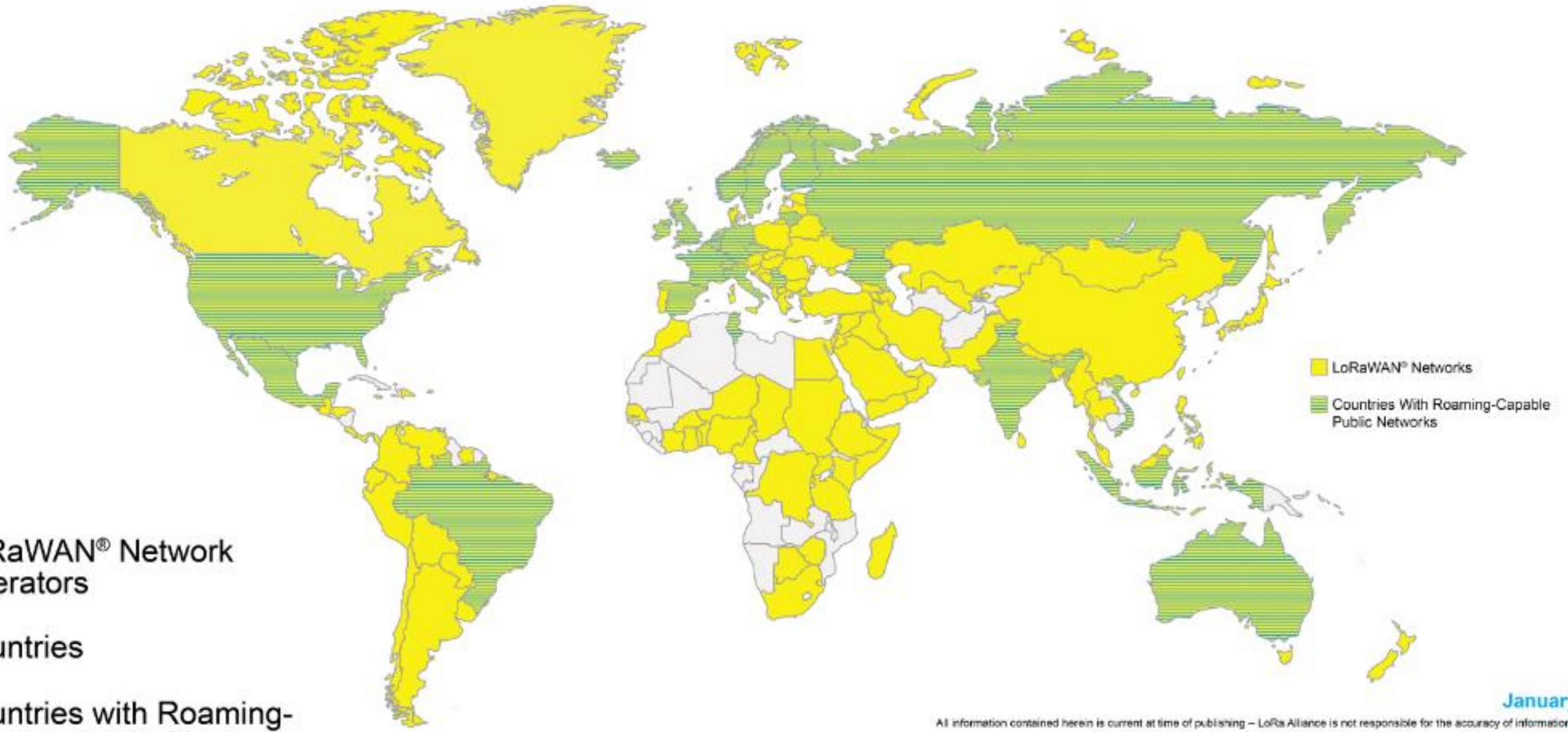


公尺 = meter, record: 8km (832 km is the world record)
Source: https://www.intelligentagri.com.tw/en

Coverage worldwide

Availability of LoRaWAN® Networks and Roaming Capability

LoRa Alliance®



150 LoRaWAN® Network Operators

163 Countries

27 Countries with Roaming-Capable Public Networks

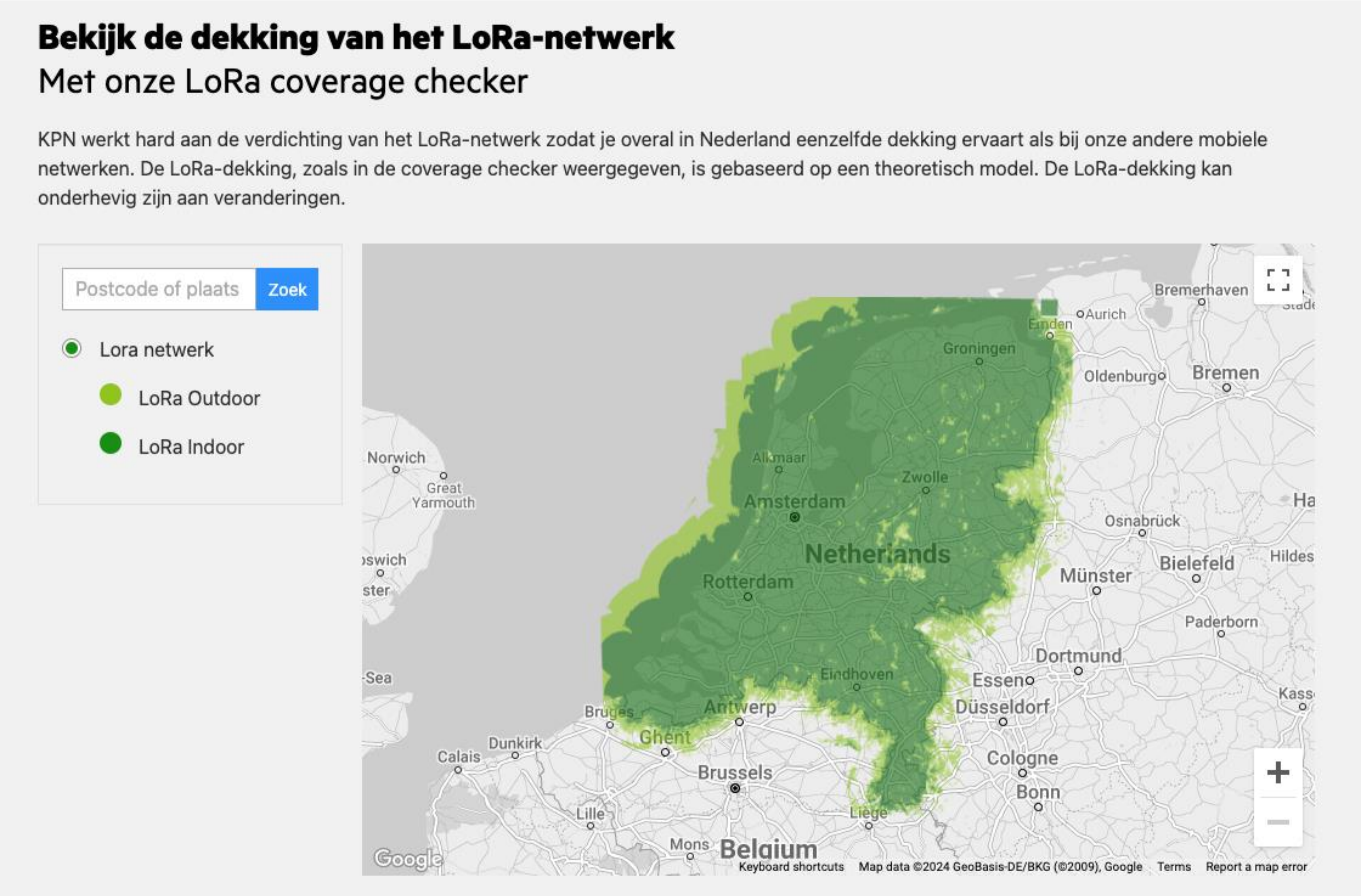
January 2021

All information contained herein is current at time of publishing – LoRa Alliance is not responsible for the accuracy of information presented.
Yellow color indicates presence of a public network, which may or may not include full nationwide coverage.
Blue lines indicate presence of a roaming-capable public network, does not indicate which networks it currently has roaming agreements with.

UNIVERSITY OF TWENTE.

SIDN LABS

Coverage in the Netherlands (KPN)



Bekijk de dekking van het LoRa-netwerk

Met onze LoRa coverage checker

KPN werkt hard aan de verdichting van het LoRa-netwerk zodat je overal in Nederland eenzelfde dekking ervaart als bij onze andere mobiele netwerken. De LoRa-dekking, zoals in de coverage checker weergegeven, is gebaseerd op een theoretisch model. De LoRa-dekking kan onderhevig zijn aan veranderingen.

Postcode of plaats | Zoek

◉ Lora netwerk

● LoRa Outdoor

● LoRa Indoor

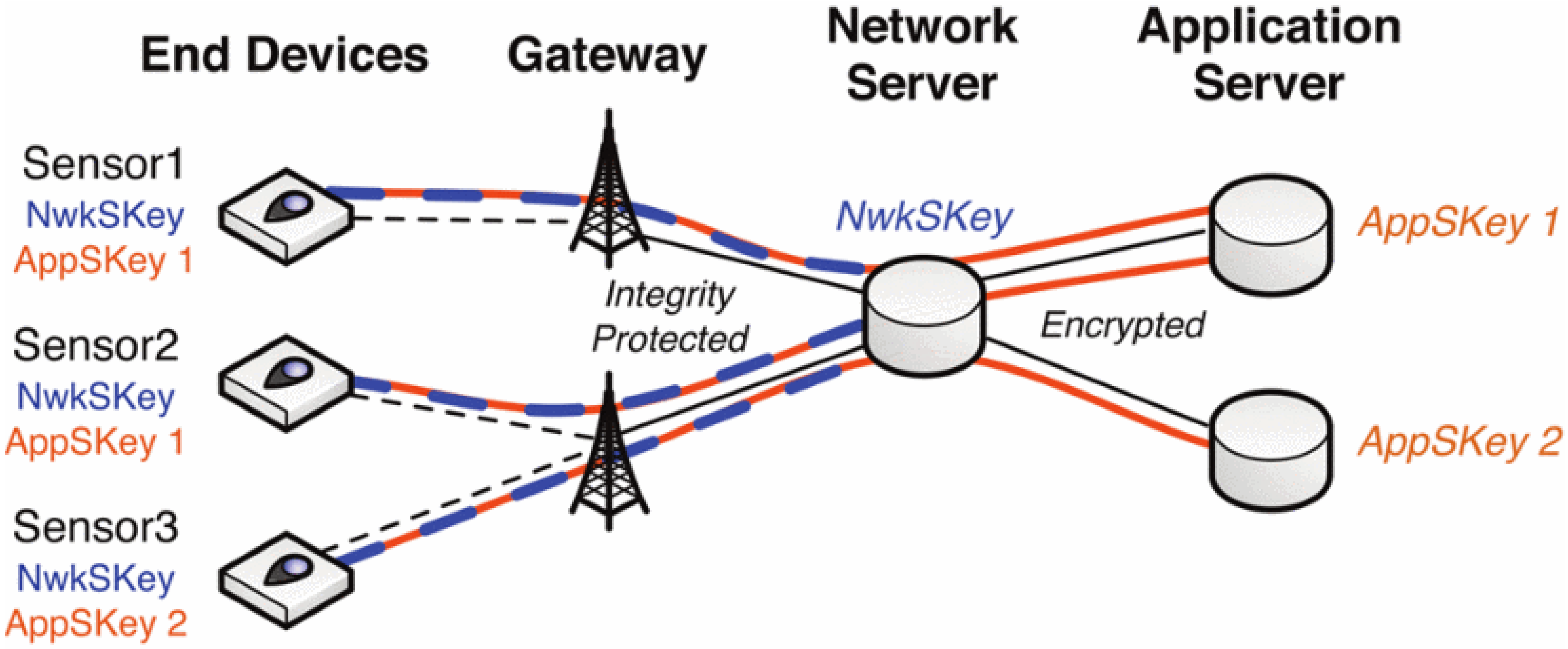
LoraWAN: key components

LoraWAN sensor (e.g., temperature)

LoraWAN gateway

LoraWAN bridge (e.g., for ModBus)

Discussion: LoraWAN roles and keys



Network Session Key

message integrity

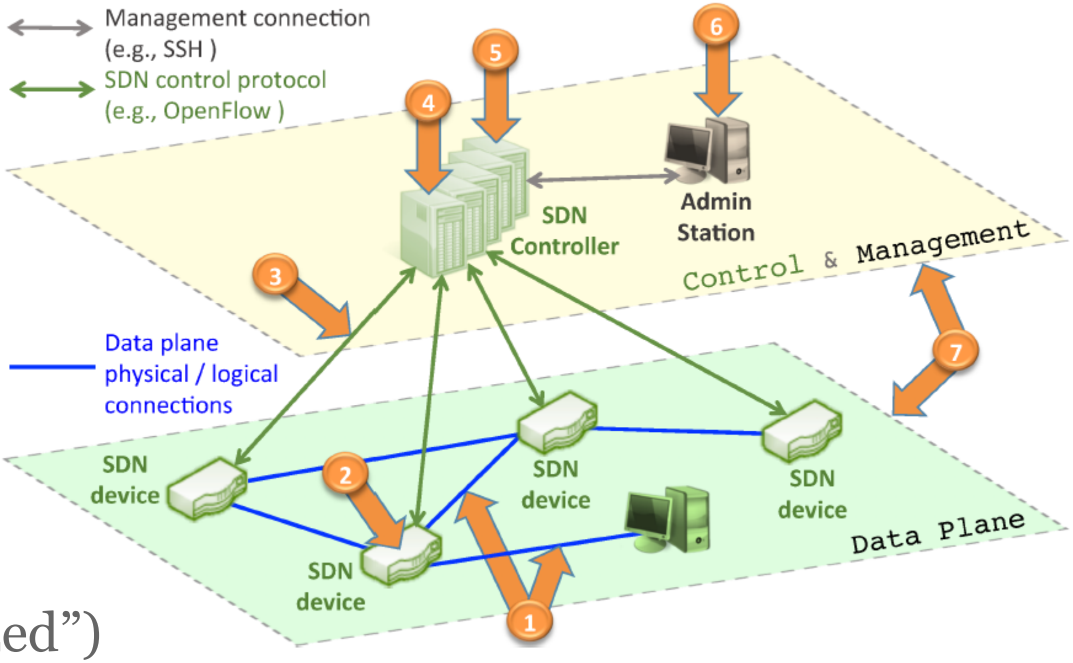
Application Session Key

payload encryption & decryption

Key security functions

- Data plane (packet forwarding)
  - Encryption of LoraWAN payloads
  - Message integrity verification
  - Replay protection

- Management plane
  - Key derivation (symmetric)
  - Device enrollment protocol (OTA and "personalized")
  - Over the air firmware updates


Management connection (e.g., SSH)
SDN control protocol (e.g., OpenFlow)
Data plane physical / logical connections
1
2
3
4
5
6
7
SDN Controller
Admin Station
Control & Management
SDN device
SDN device
SDN device
SDN device
Data Plane

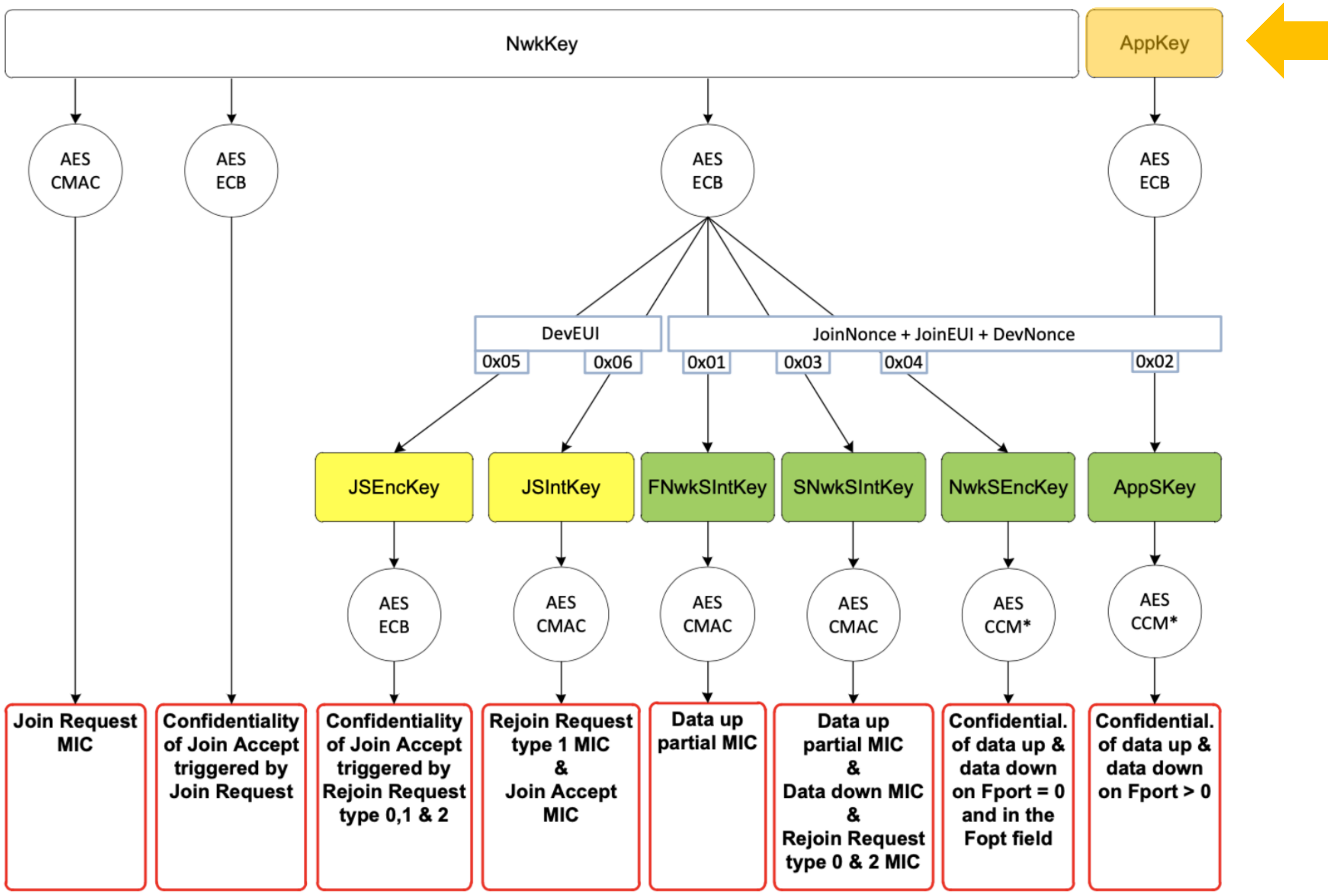
Source: D. Kreutz, F. M. V. Ramos, P. Verissimo, HotSDN'13, August 16, 2013, Hong Kong, China.

LoraWAN key derivation

v1.1: logical separation between network and application operator (Oct 2017)

Added in v1.1

v1.02



NwkKey

AppKey

Provisioned

AES CMAC

AES ECB

AES ECB

AES ECB

DevEUI

JoinNonce + JoinEUI + DevNonce

0x05

0x06

0x01

0x03

0x04

0x02

JSEncKey

JSIntKey

FNwkSIntKey

SNwkSIntKey

NwkSEncKey

AppSKey

AES ECB

AES CMAC

AES CMAC

AES CMAC

AES CCM*

AES CCM*

Join Request MIC

Confidentiality of Join Accept triggered by Join Request

Confidentiality of Join Accept triggered by Rejoin Request type 0,1 & 2

Rejoin Request type 1 MIC & Join Accept MIC

Data up partial MIC

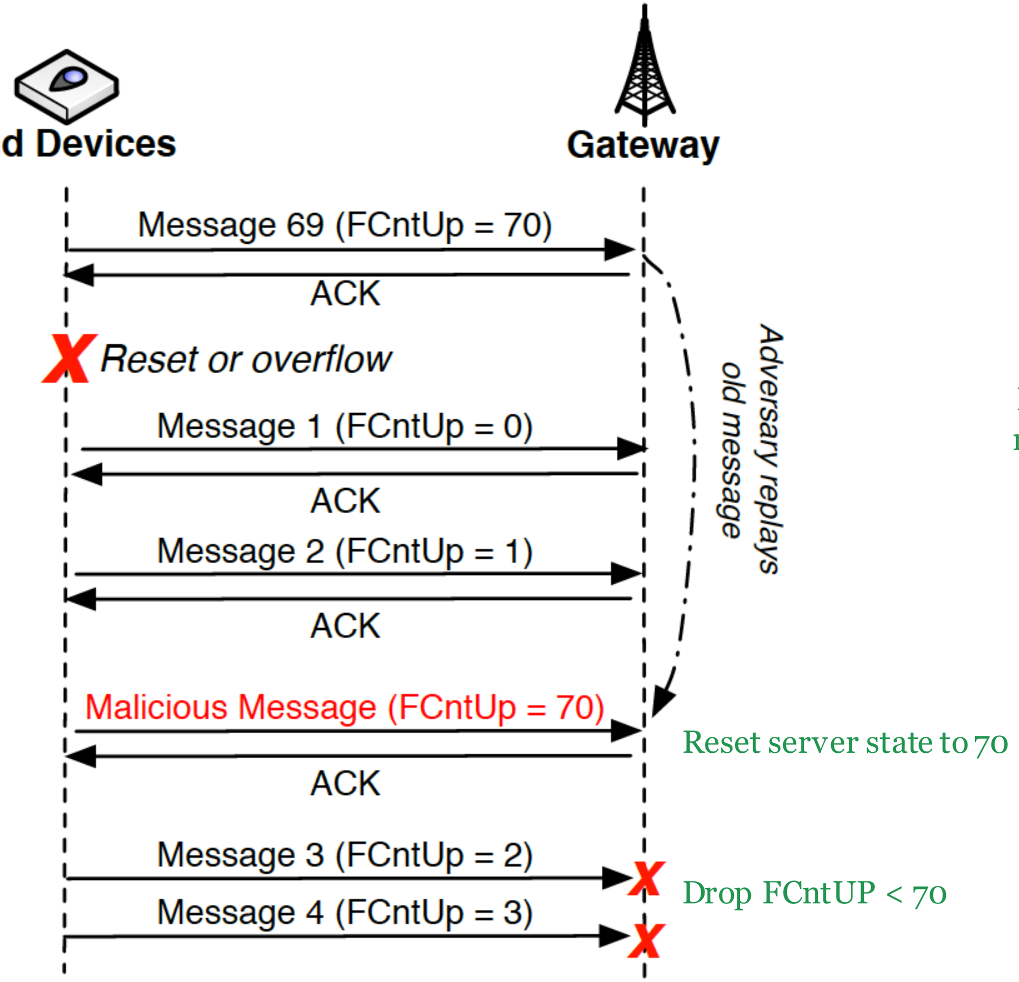
Data up partial MIC & Data down MIC & Rejoin Request type 0 & 2 MIC

Confidential. of data up & data down on Fport = 0 and in the Fopt field

Confidential. of data up & data down on Fport > 0

Picture: Johan Stokking, The Thing Industries

Discussion: denial of service through replay

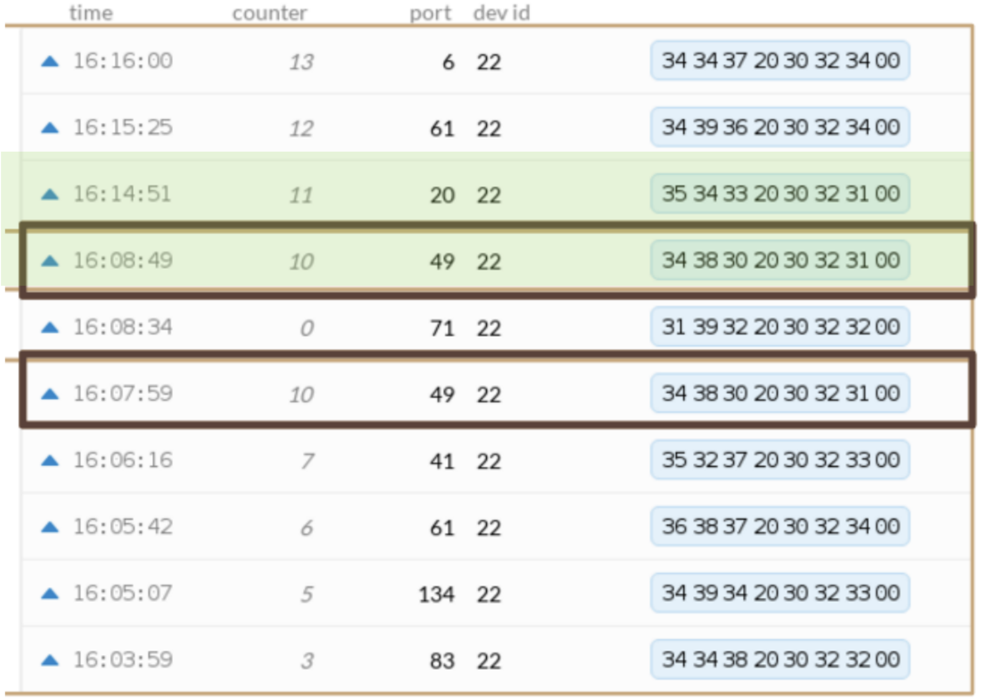


Reset server state to 70

Drop FCntUP < 70

Fig. 4. An example of a replay attack for ABP.

Injected message



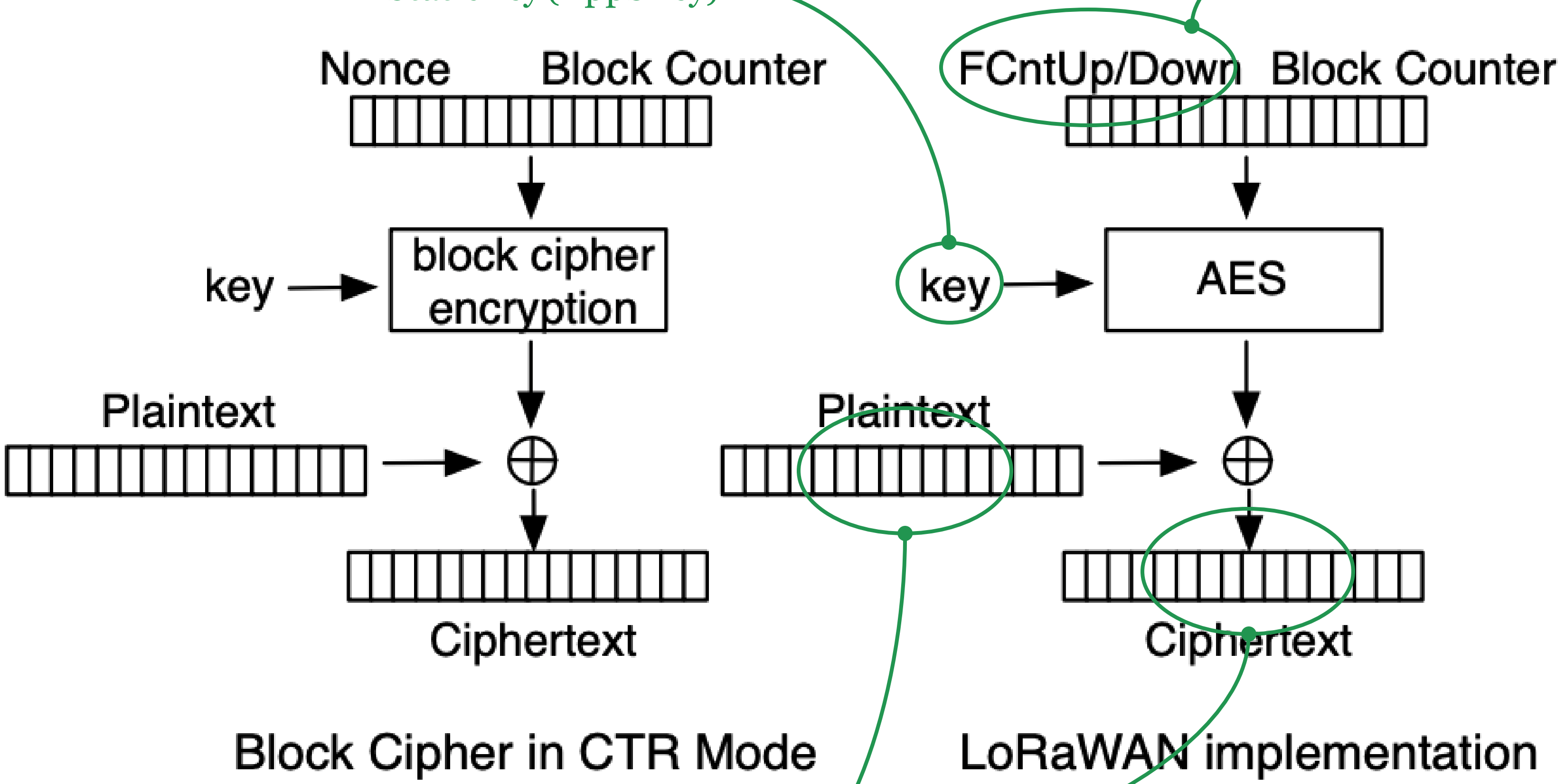
time	counter	port	dev id	
▲ 16:16:00	13	6	22	34 34 37 20 30 32 34 00
▲ 16:15:25	12	61	22	34 39 36 20 30 32 34 00
▲ 16:14:51	11	20	22	35 34 33 20 30 32 31 00
▲ 16:08:49	10	49	22	34 38 30 20 30 32 31 00
▲ 16:08:34	0	71	22	31 39 32 20 30 32 32 00
▲ 16:07:59	10	49	22	34 38 30 20 30 32 31 00
▲ 16:06:16	7	41	22	35 32 37 20 30 32 33 00
▲ 16:05:42	6	61	22	36 38 37 20 30 32 34 00
▲ 16:05:07	5	134	22	34 39 34 20 30 32 33 00
▲ 16:03:59	3	83	22	34 34 38 20 30 32 32 00

Fig. 7. Log file of the victim's server.

UNIVERSITY OF TWENTE.

SIDN LABS

Discussion: known-plaintext attack



Block Cipher in CTR Mode

LoRaWAN implementation

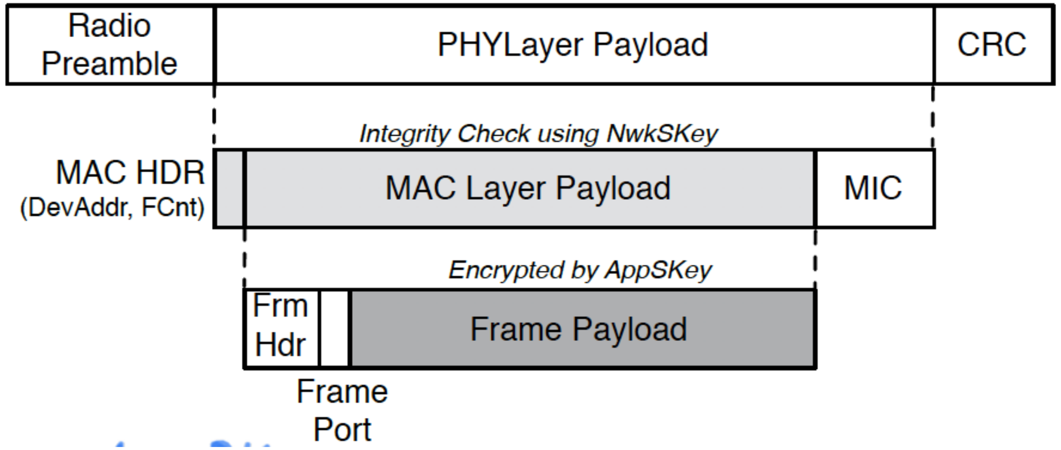
Static key (AppSKey)

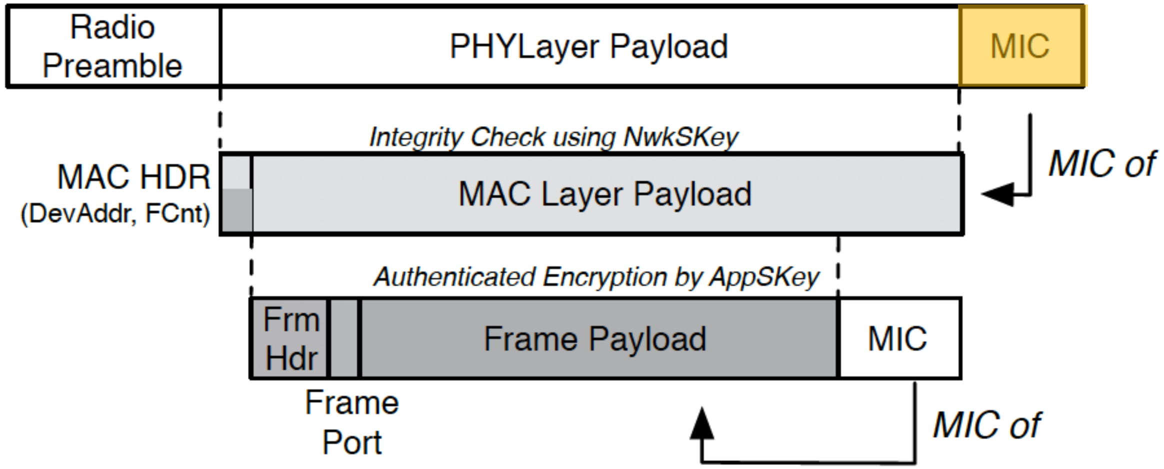
Frame counter, can be reset to a known state (0) while AppSKey remains the same

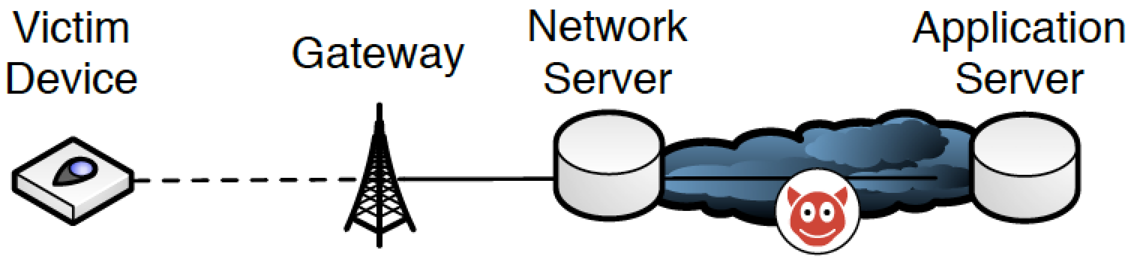
Known-plaintext: limited plaintext variation enables predictions based on ciphertext

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
https://en.wikipedia.org/wiki/Known-plaintext_attack
https://en.wikipedia.org/wiki/Block_cipher

Discussion: proposed solution using 2 MICs

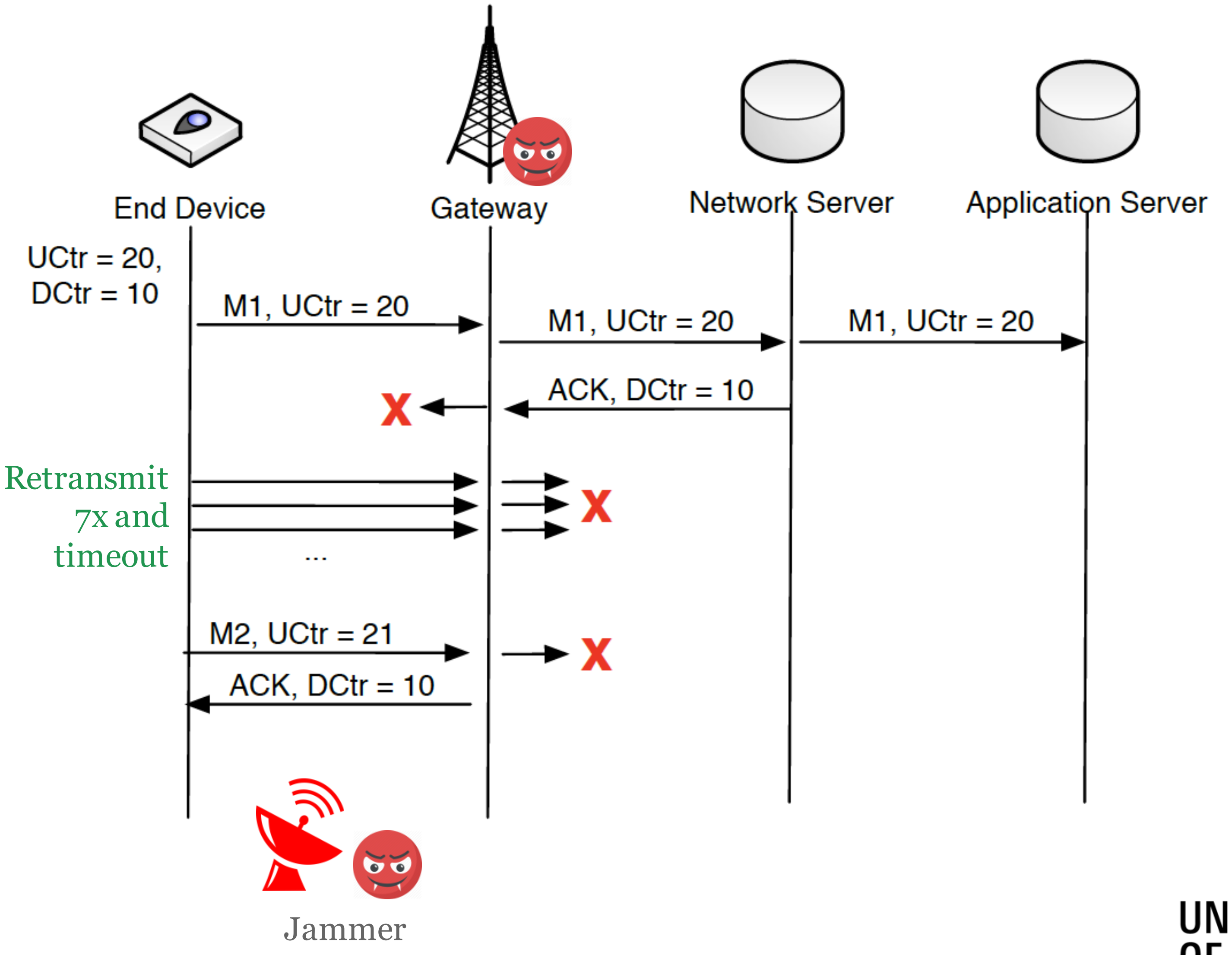




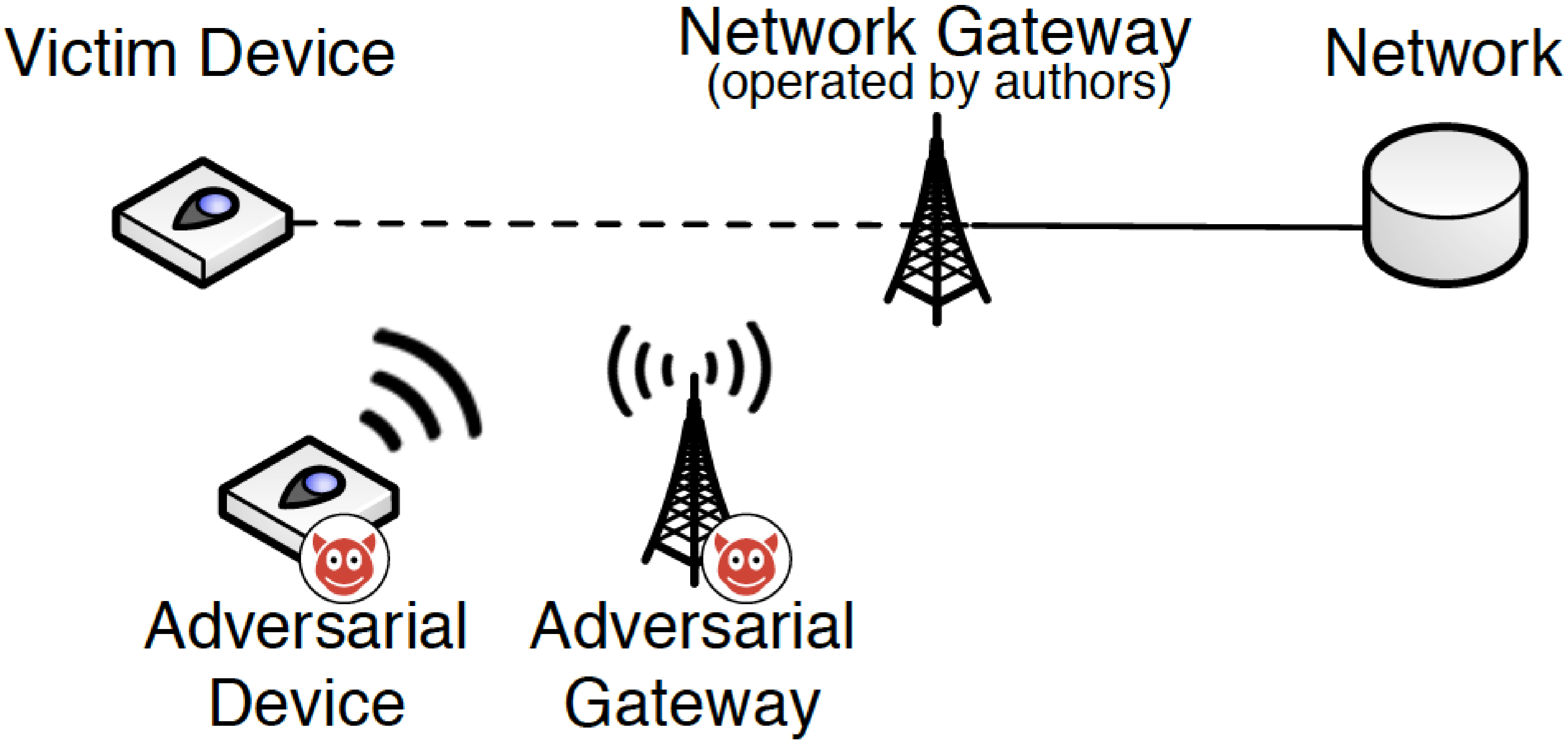


connectivity provided over public network
with adversarial interference

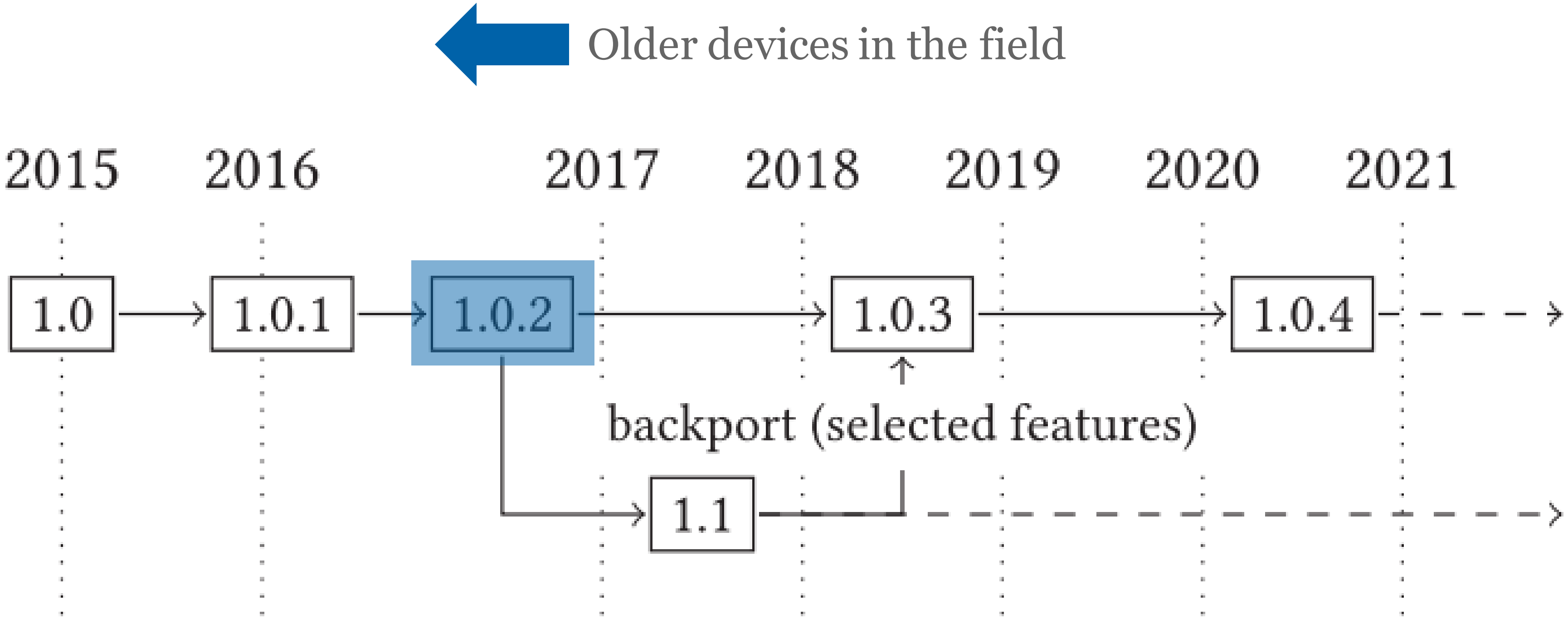
Discussion: ACK spoofing



Discussion: class B attacks (battery draining)



Let’s look at the version history of LoraWAN



F. Hessel, L. Almon, and M. Hollick, ‘LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation’, ACM Trans. Sens. Netw., vol. 18, no. 4, p. 70:1-70:55, Mar. 2023, doi: 10.1145/3561973.

Open standardization (vs. more closed like LoraWAN)

IETF®

Key takeaways

- Designing network security protocols is challenging

- Attacks can have a physical component, such as jamming or device resets

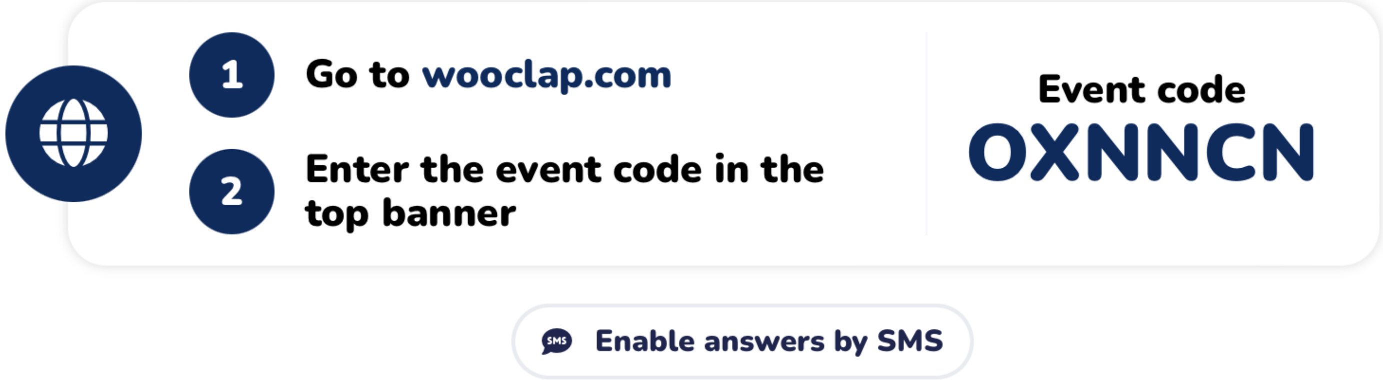
- Highlights the importance of an open protocol development process (cf. IETF)

Coffee break

“Where the sidewalk ends: privacy of opportunistic backhaul”

15th European Workshop on Systems Security (EuroSec22), Rennes France, April 2022

Get your phones ready!



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

OXNNCN

Enable answers by SMS

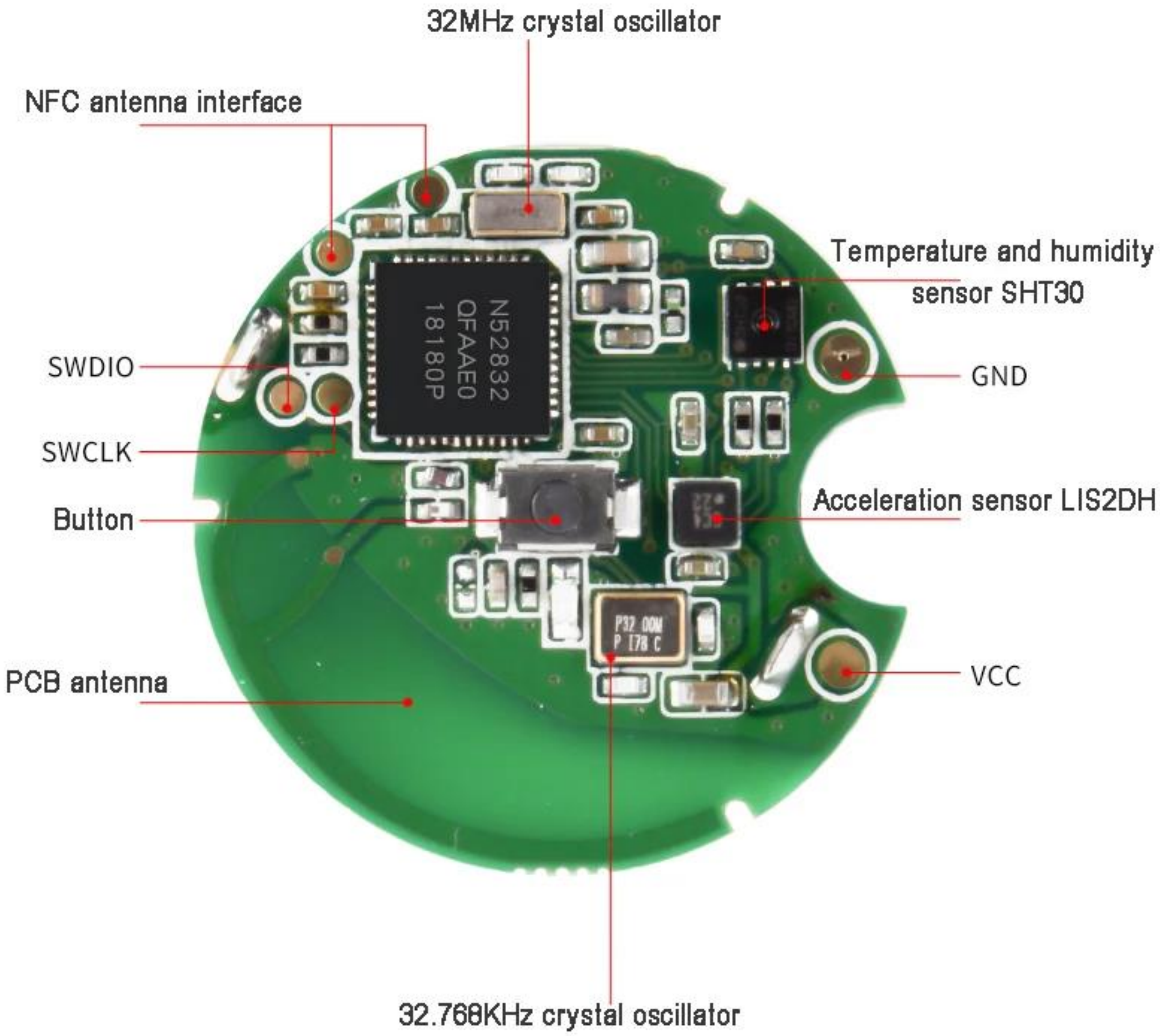
What struck you about the paper?

What are Opportunistic Networks and Backhaul?

UNIVERSITY OF TWENTE.

SIDN LABS

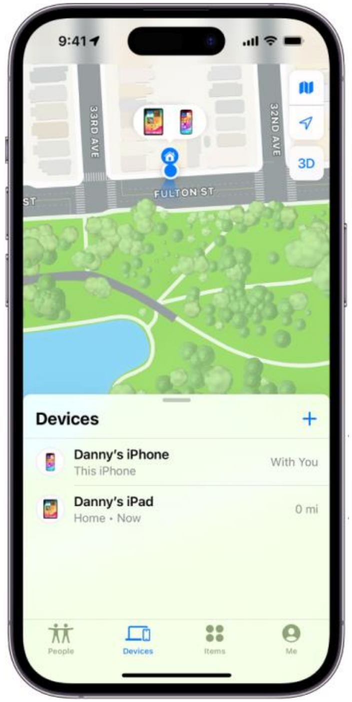
De beste Bluetooth Tags



Opportunistic mesh networks

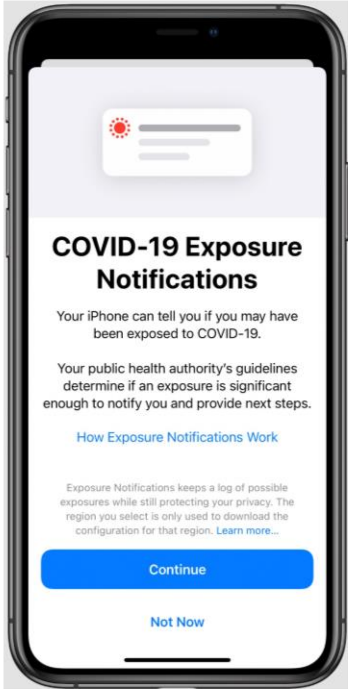
- Data mule: a vehicle providing data communication in remote areas
- Find My: crowd source device-tracking feature with BLE advertisements
- Exposure Notifications: Covid-19 notification based on BLE beacons

How is your experience and opinions on such applications?



Devices +

Danny's iPhone This iPhone	With You
Danny's iPad Home • Now	0 mi



COVID-19 Exposure Notifications

Your iPhone can tell you if you may have been exposed to COVID-19.

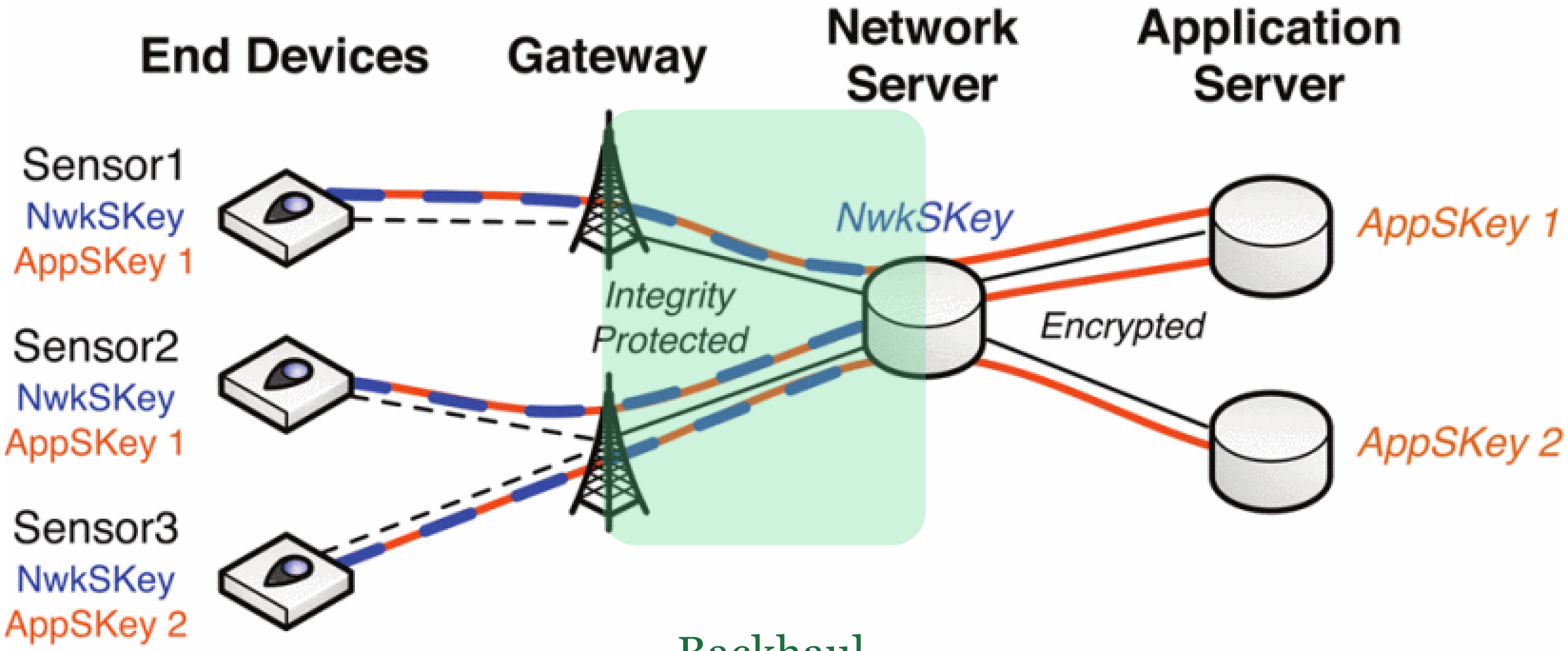
Your public health authority's guidelines determine if an exposure is significant enough to notify you and provide next steps.

How Exposure Notifications Work

Exposure Notifications keeps a log of possible exposures while still protecting your privacy. The region you select is only used to download the configuration for that region. Learn more...

Backhaul as a service

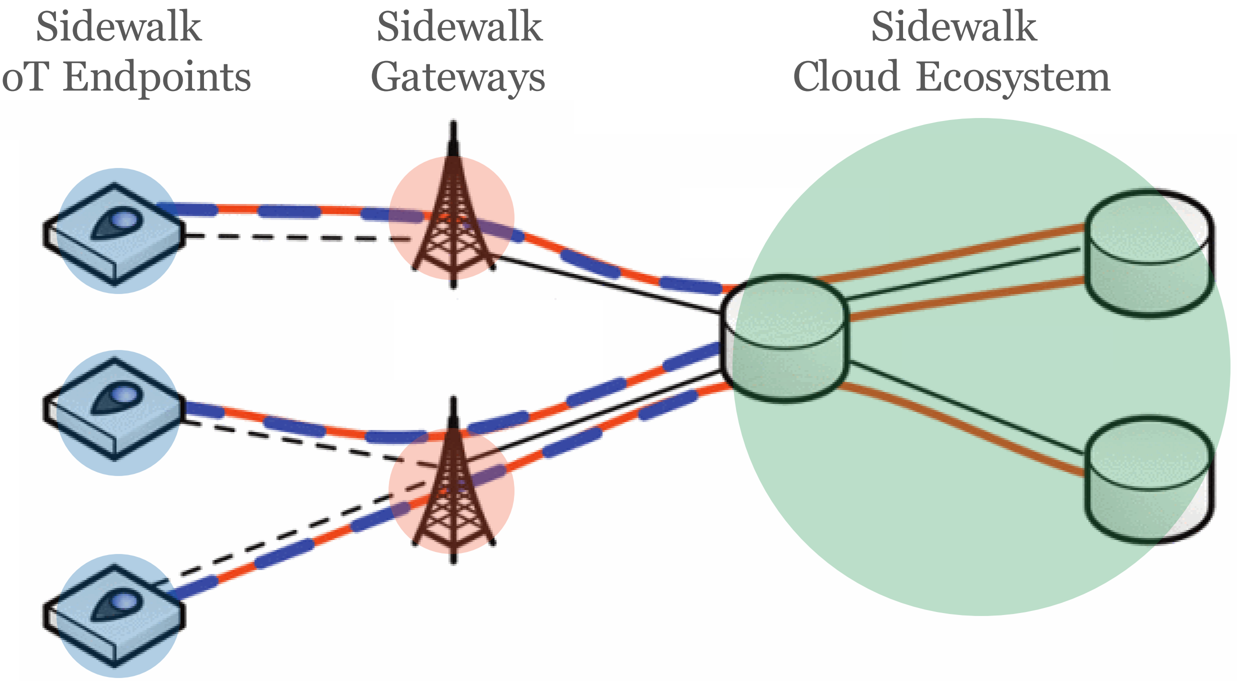
- Gateway-Centric Design using BLE, LoRA, or other low power wireless protocol



Backhaul
Ethernet, LTE, Satellite, etc

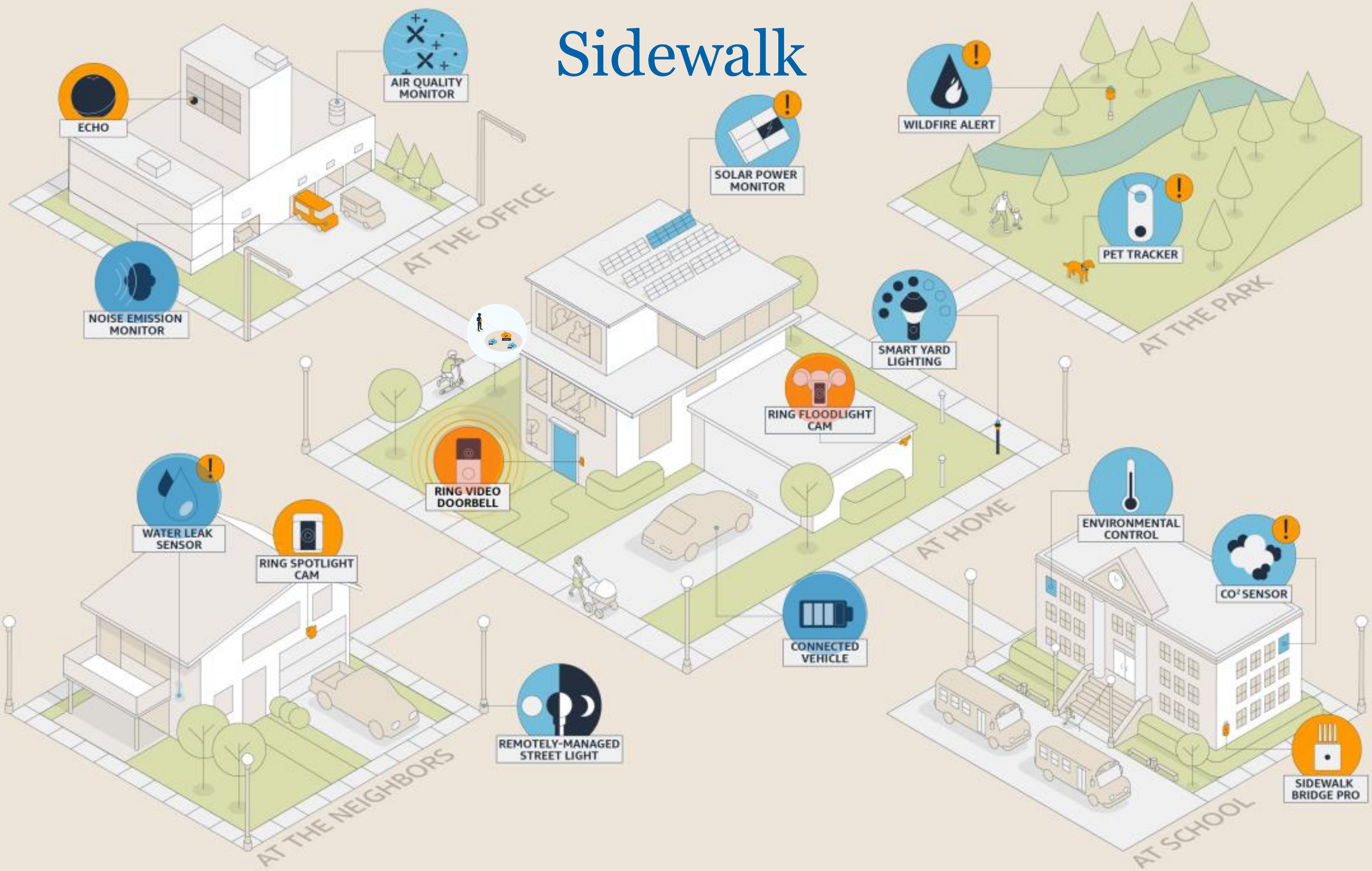
Amazon Sidewalk Architecture

- Amazon Sidewalk use BLE and LoRA. Sidewalk gateways can be Echo



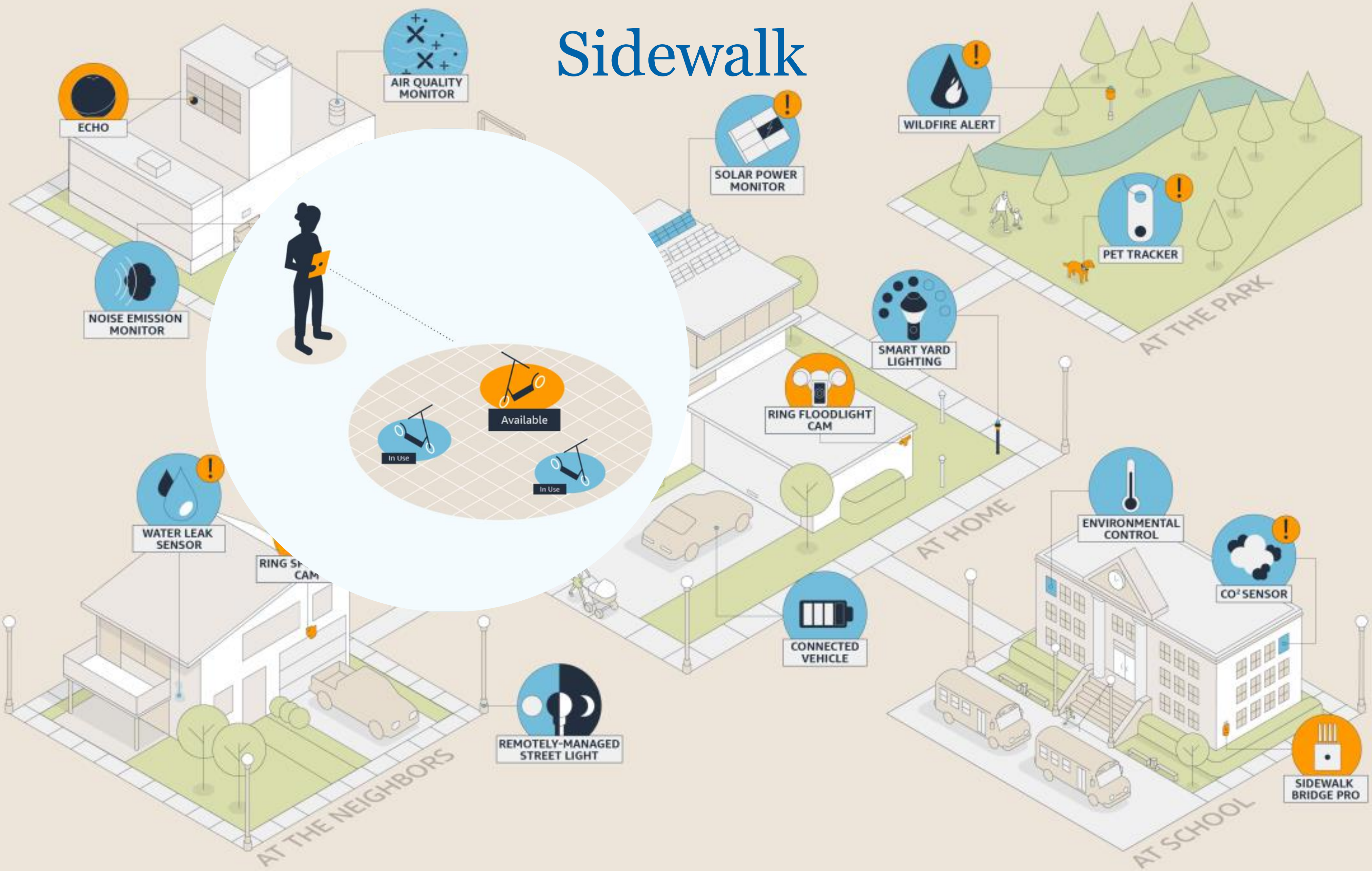
https://docs.aws.amazon.com/iot-wireless/latest/developerguide/amazon-sidewalk-overview.html
https://docs.sidewalk.amazon/introduction/sidewalk-how-works.htmlHZPRPBGX

Sidewalk



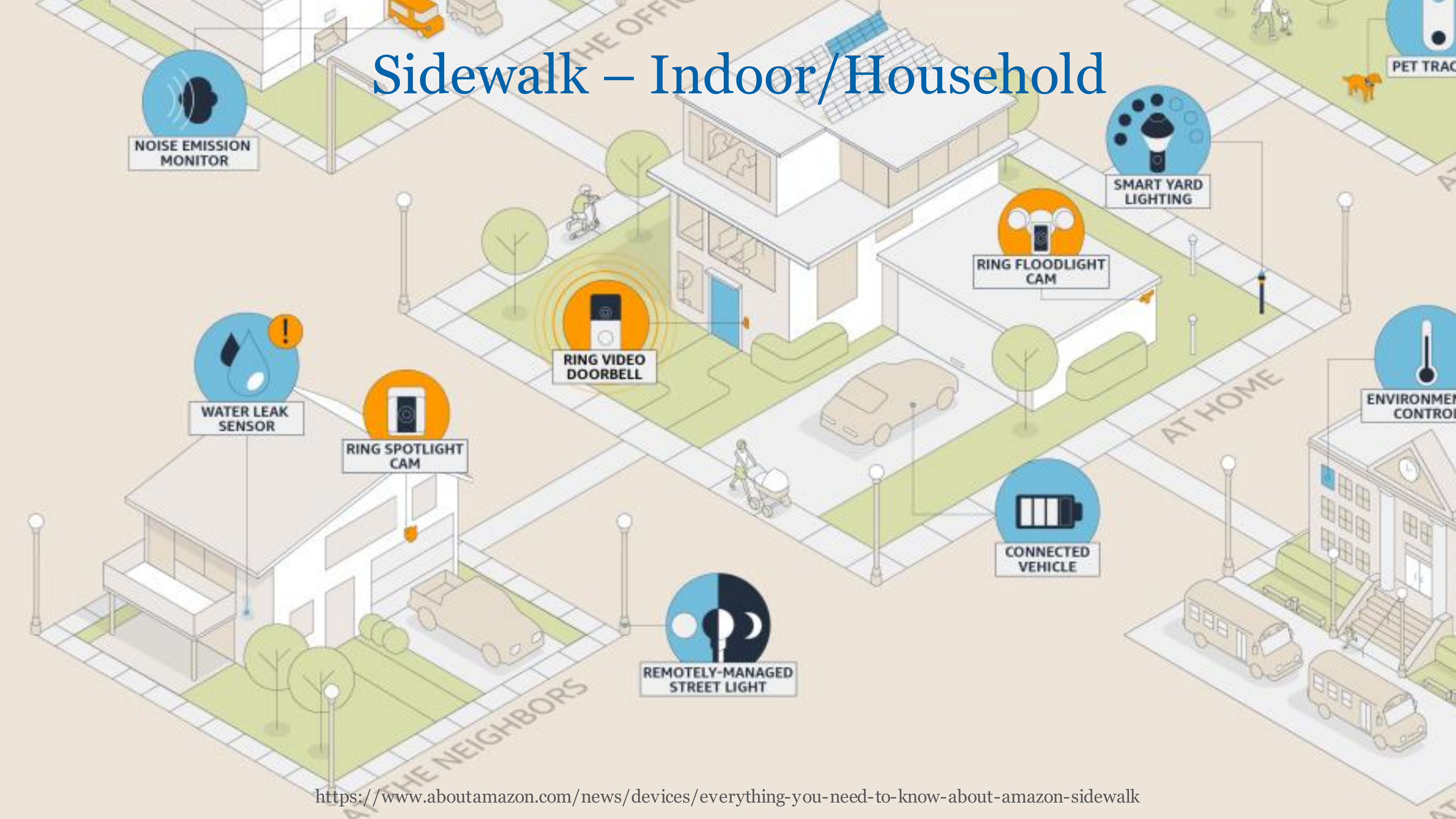
https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

Sidewalk



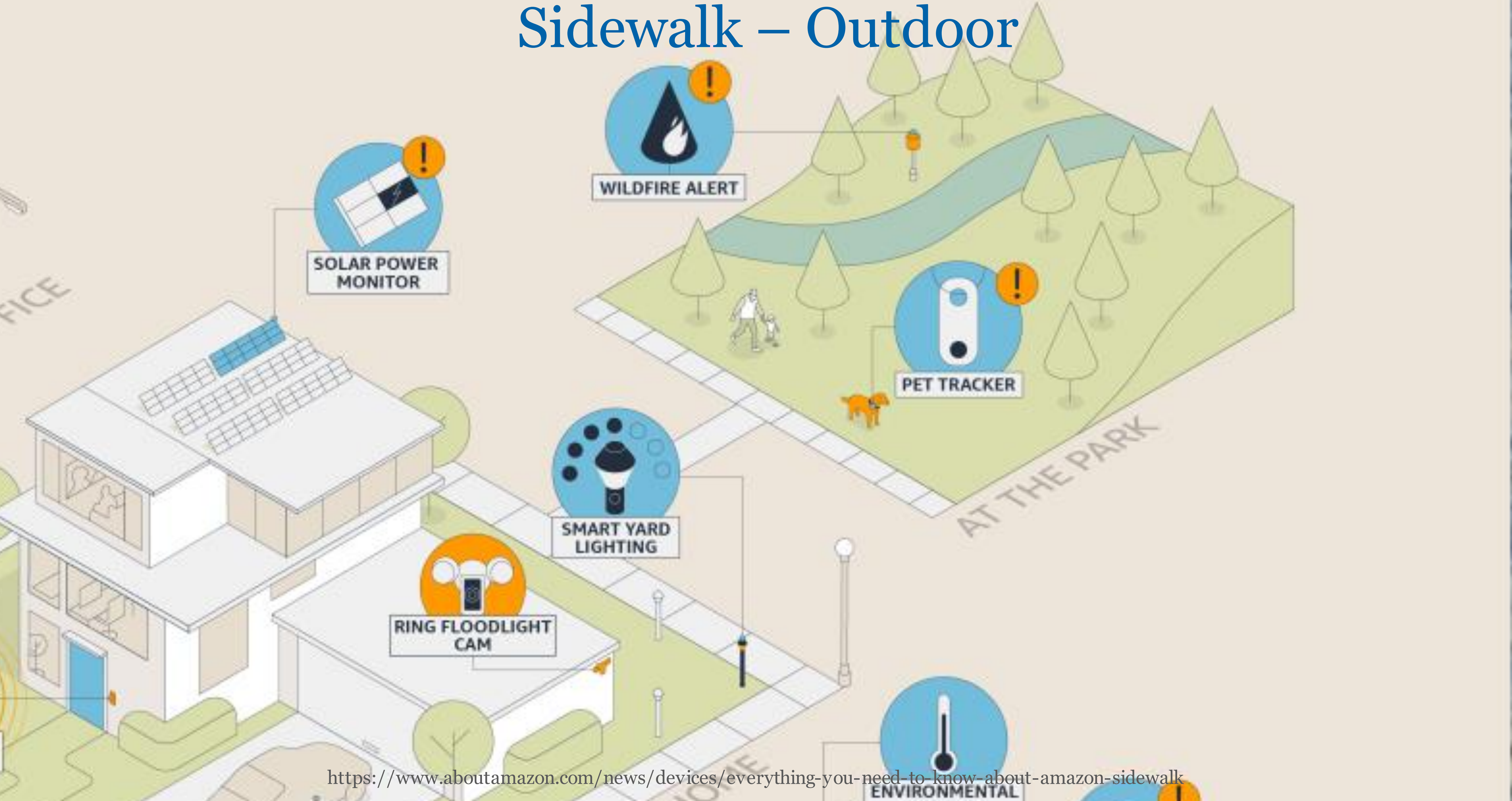
https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

Sidewalk – Indoor/Household



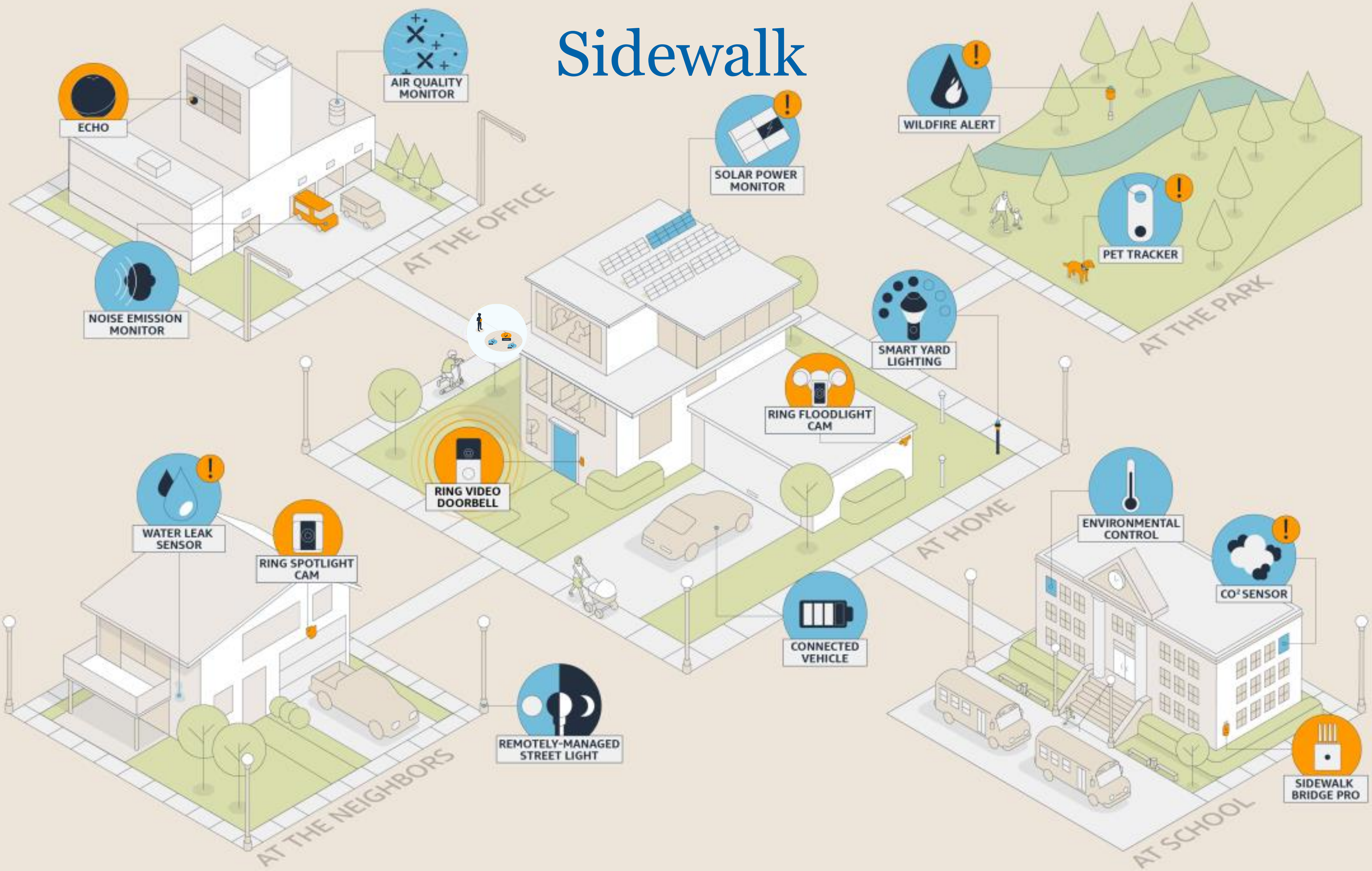
https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

Sidewalk – Outdoor

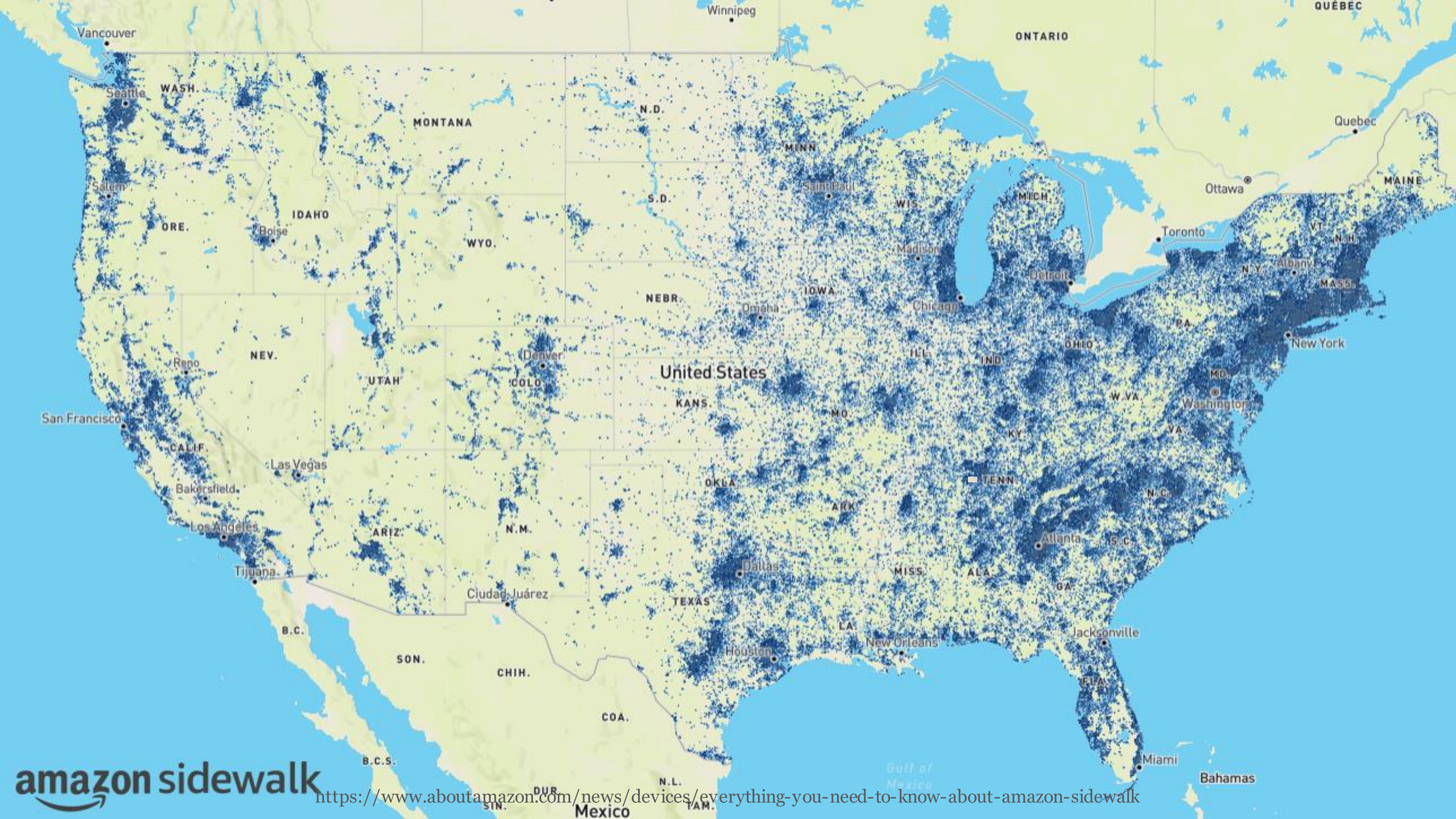


https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

Sidewalk



https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk



amazon sidewalk

https://www.aboutamazon.com/news/devices/everything-you-need-to-know-about-amazon-sidewalk

Sidewalk collects routing metadata

“At a central network server for each payload”

- “Authenticates the gateway being used and records recently-used gateways for bidirectional communication”
- “Collects endpoint identifiers to authenticate devices”
- “Keeps gateways time-synchronized to generate correct payload timestamps”
- “Is given the desired server destination for the application data”
- “Device IDs are kept to enable bidirectional communication”

“Several encryption layers and rotating transmission identifiers protect Sidewalk communication, no guarantees can be made on how Amazon handles user metadata”

Amazon Sidewalk Privacy and Security Whitepaper
https://www.amazon.com/gp/help/customer/display.html?nodeId=GRGWE27XHZPRPBGX
Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Proof of Concept

Simulated pedestrian mobility

Microsoft GeoLife mobility dataset

Routing Metadata

Devices and Gateways

Proof of Concept

Simulated pedestrian mobility

Microsoft GeoLife mobility dataset

Routing Metadata

Devices and Gateways

Proof of Concept

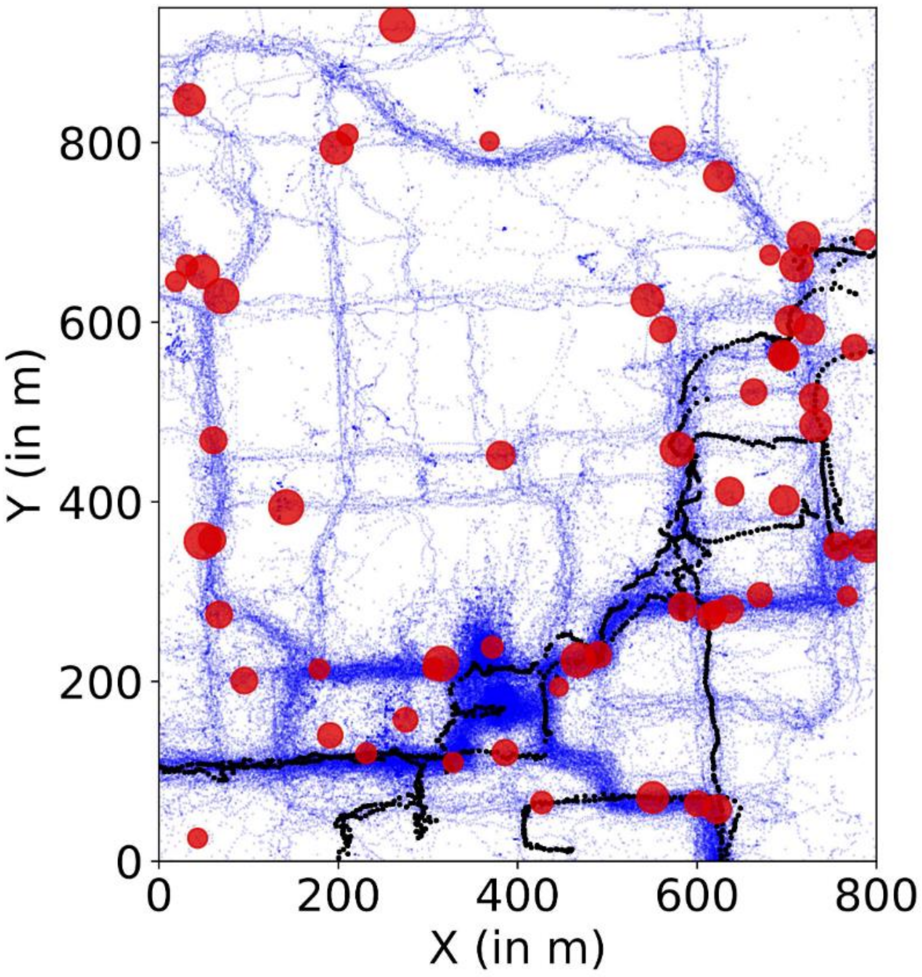
Simulated pedestrian mobility

- Microsoft GeoLife mobility dataset

Routing Metadata

- Device and Gateway identities
- Transmission time

Locations of Devices and Gateways



Microsoft GeoLife mobility dataset

What do you think about the dataset?

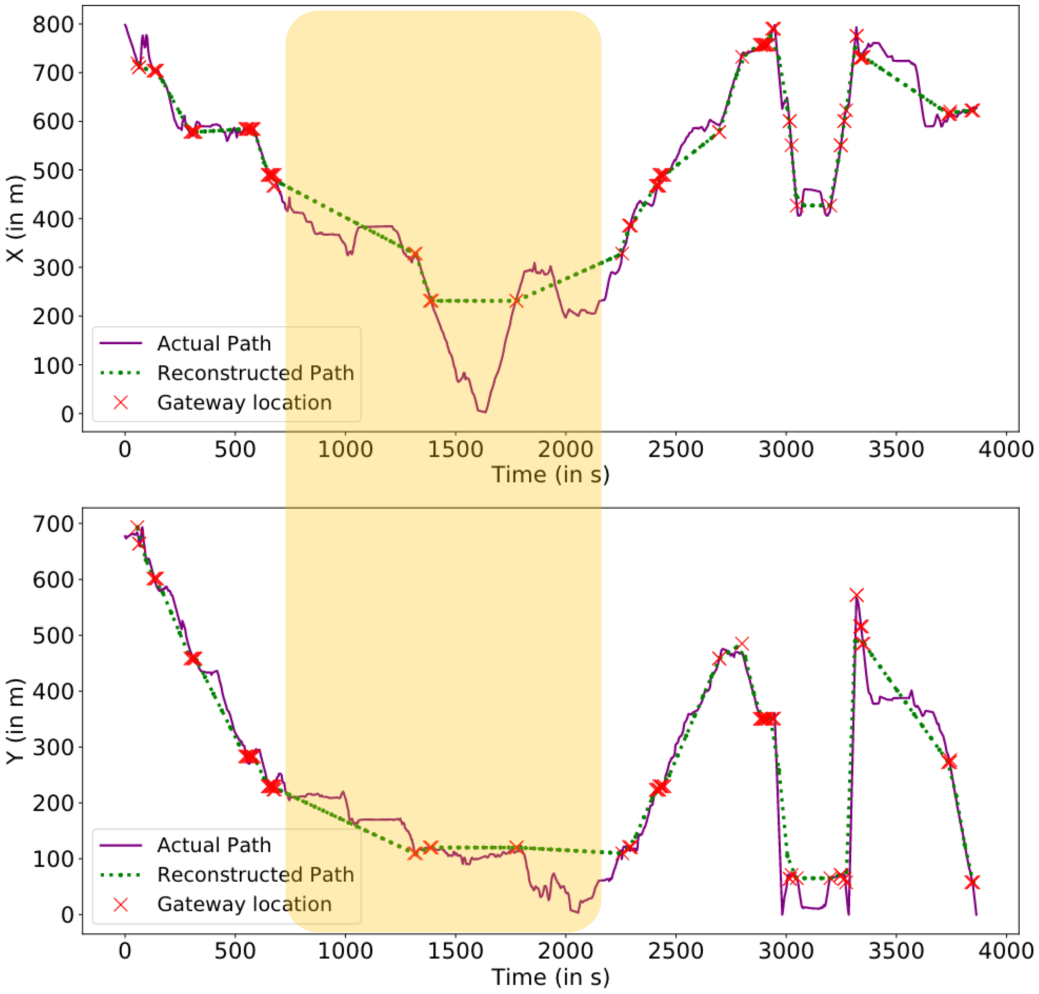
Can we do this at University of Twente?

What are Pros and Cons to collect such data?

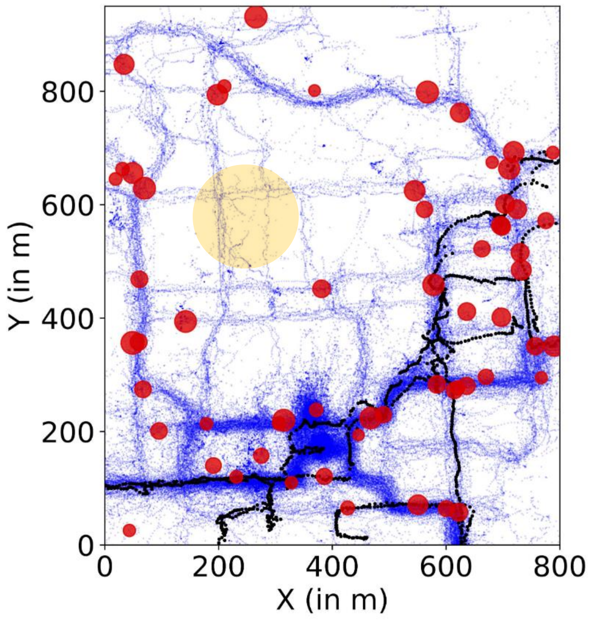
Will you agree to participate in a similar experiment?

https://www.microsoft.com/en-us/research/publication/geolife-gps-trajectory-dataset-user-guide/

Location-based reconstruction



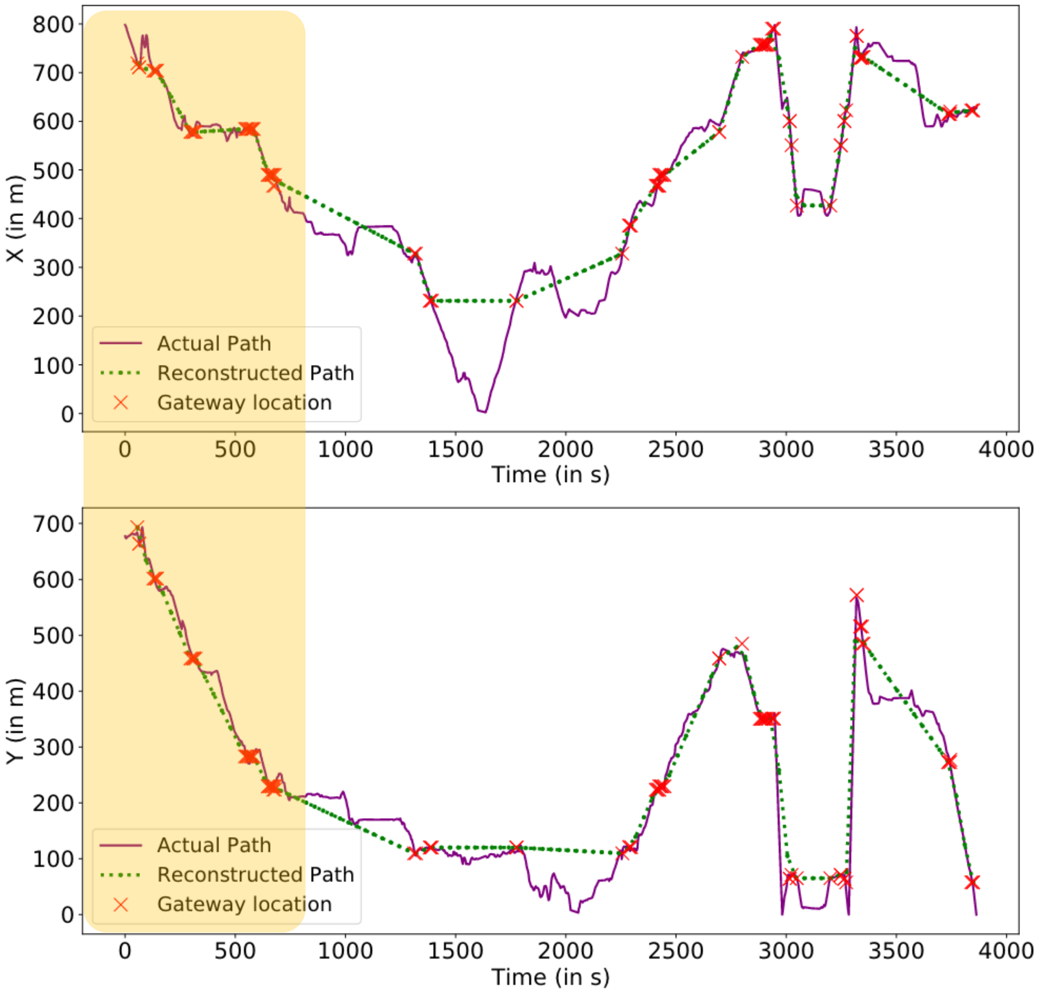
- All backhaul gateways are known
- A single mobile device
- Linear splines
- 800-2200 secs, gateways are sparse
- What else do you see? Problems? Methods?



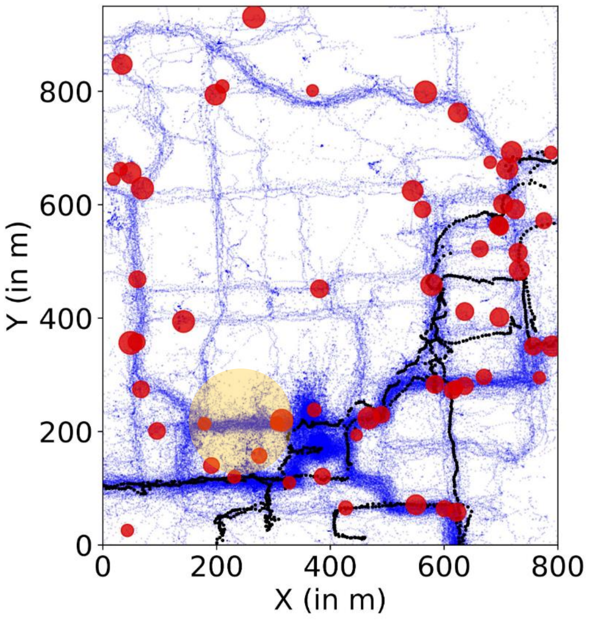
UNIVERSITY OF TWENTE.

SIDN LABS

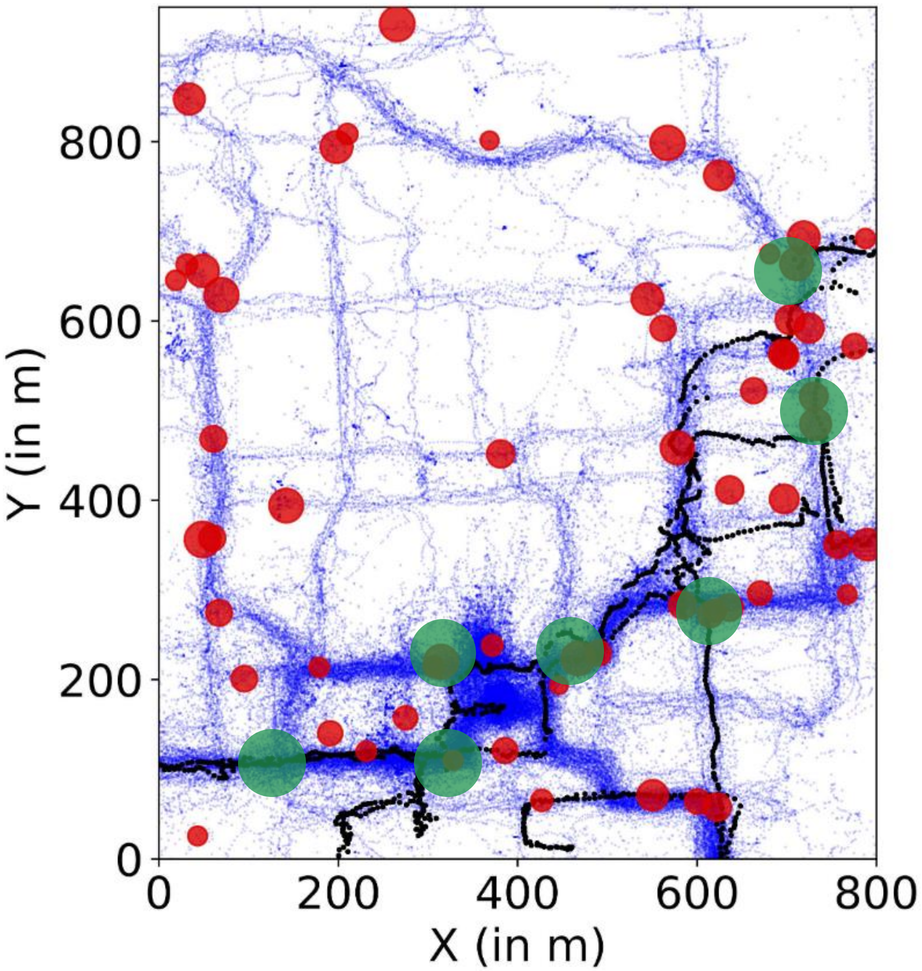
Location-based reconstruction



- All backhaul gateways are known
- A single mobile device
- Linear splines
- 800-2200 secs, gateways are sparse
- What else do you see? Problems? Methods?



Metadata-based reconstruction

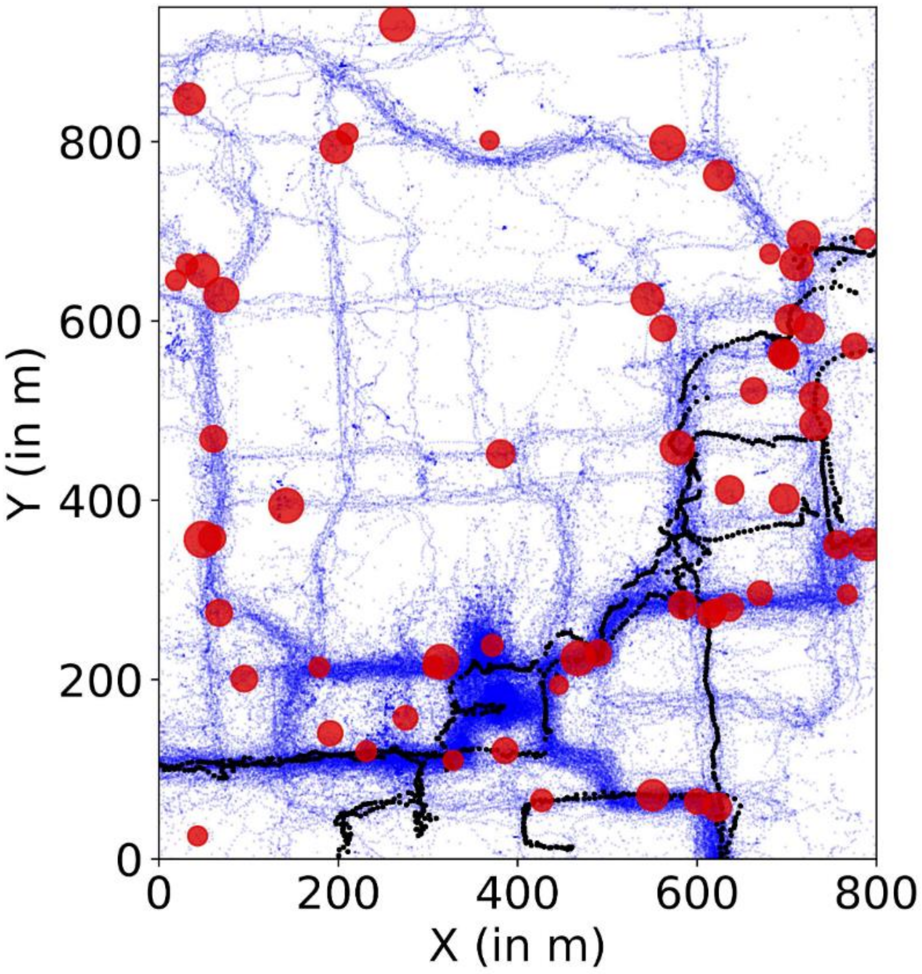


"An adversarial network provider can reconstruct the movement of endpoints through that area over time, but they can also derive an estimated position for the other gateways"

- A few gateways at known locations with high traffic flow
- Estimating pairwise distances
- Triangulating positions of other gateways

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Metadata-based reconstruction



"An adversarial network provider can reconstruct the movement of endpoints through that area over time, but they can also derive an estimated position for the other gateways"

- A few gateways at known locations with high traffic flow
- Estimating pairwise distances
- Triangulating positions of other gateways

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Metadata-based reconstruction

Estimating pairwise distances

- “Specifically, for each trace p_i , we calculate the list of time differences $(t_{k_1} - t_{k_2})$ between connections made with gateways g_{j1}, g_{j2} for connection times t_{k_1} and t_{k_2} that occurred within two minutes of each other”
- “Since we want an accurate straight-line distance between gateways in order to conduct triangulation, we select the 5^{th} percentile value of $(t_{k_1} - t_{k_2})$ for each pair of gateways to use as the time distance estimate, avoiding noise”
- “We ignore any trace that does not see at least three unique gateways, as traces with only two or less gateways do not provide any meaningful information about relative distance between gateways”
- “Of the 1034 traces we started with, only 637 of them passed by at least three unique gateways, with the other 397 traces being too short or walking in too sparsely populated areas to interact with enough gateways.”
- “Our data validates our assumption - standard deviation of the velocities of the endpoints we used tend to be around 1 m/s”

Metadata-based reconstruction

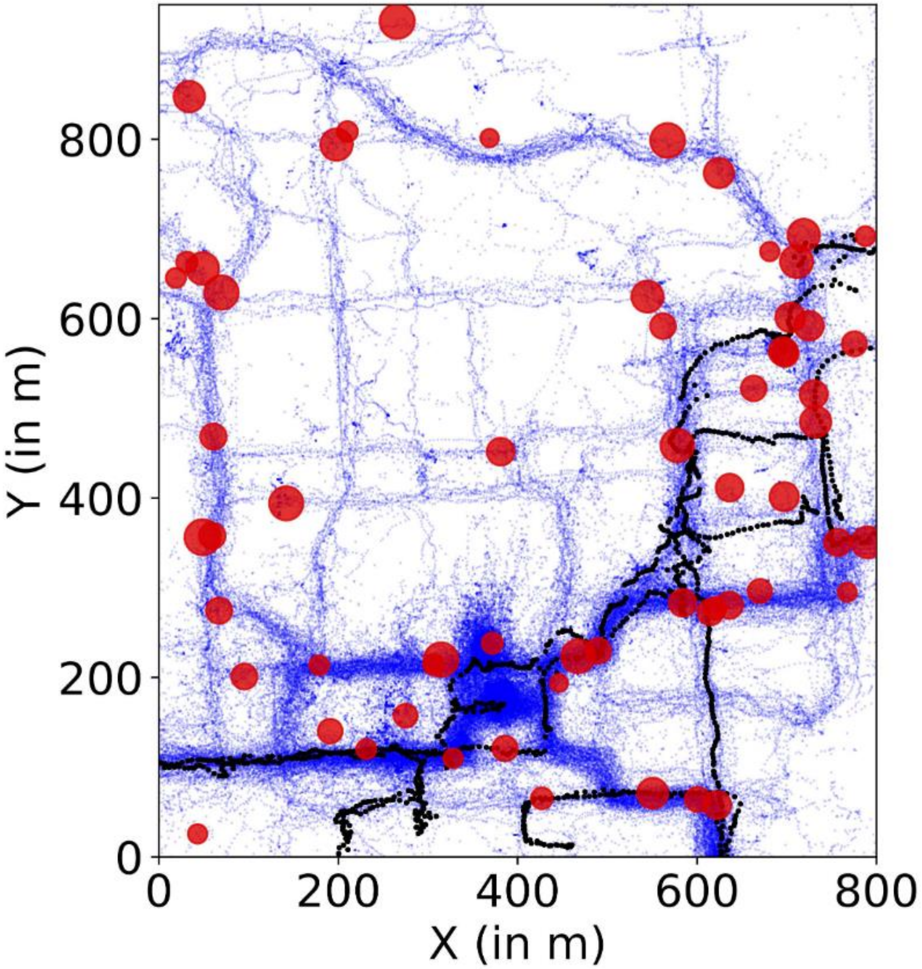
Estimating pairwise distances

- “For each trace p_i , we check every two minutes time $(t_{k1} - t_{k2})$”
- “We select the 5^{th} percentile value of $(t_{k1} - t_{k2})$ to avoid noise and get a straight-line distance”
- “We ignore any trace that does not see at least three unique gateways to get useful results”
- “The velocities of the endpoints we used tend to be around 1 m/s”

“Known gateway locations should be chosen intelligently. More mobility data allows for more accurate reconstructions.”

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Metadata-based reconstruction



Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

"An adversarial network provider can reconstruct the movement of endpoints through that area over time, but they can also derive an estimated position for the other gateways"

- A few gateways at known locations with high traffic flow
- Estimating pairwise distances
- Triangulating positions of other gateways

Metadata-based reconstruction

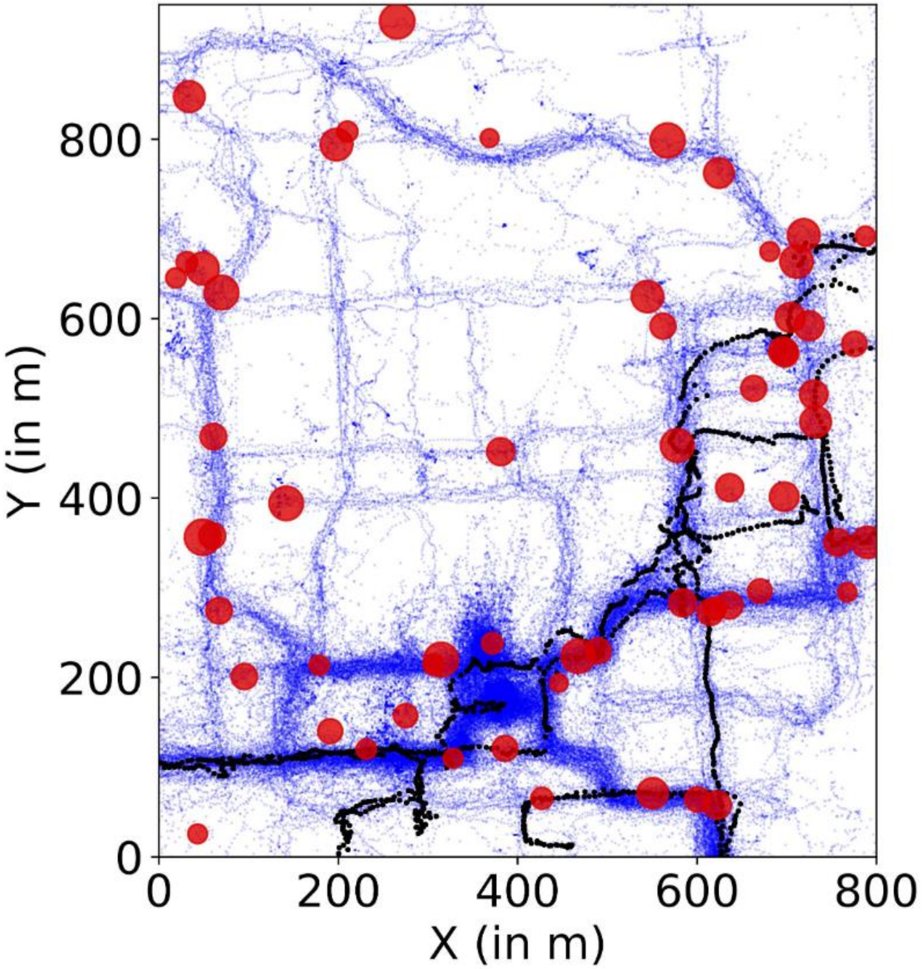
Triangulating positions of other gateways

- “We do this through iterative least squares optimizations on *unknown* gateways until the positions stabilize.”
- “To avoid local minima, we instantiate the predicted position values randomly, run 20 predictions with randomized initial positions, and select predictions that minimize the loss”

$$\min_{pos(g_{j_u})} \sum_{j \in \{0,\ldots,75\}} \left(||pos(g_{j_u}) - pos(g_j)||_2 - D[j_u, j]\right)^2$$

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Metadata-based reconstruction



"An adversarial network provider can reconstruct the movement of endpoints through that area over time, but they can also derive an estimated position for the other gateways"

- A few gateways at known locations with high traffic flow
- Estimating pairwise distances
- Triangulating positions of other gateways
- Results

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Discussion

- Metadata Privacy
  Tradeoffs of using private information retrieval (PIR)
- Accountability
  bidirectional communication
- Scalability
  database sharding and differential privacy

Discussion

- Metadata Privacy
  Tradeoffs of using private information retrieval (PIR)
  - “Data-packet source identifiers and timing data should be treated as sensitive information”
  - Anonymous Communication Systems
  - “Hiding timing metadata by batching uploads to a cloud system at a set frequency”
- Accountability
  bidirectional communication
- Scalability
  database sharding and differential privacy

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Discussion

- Metadata Privacy
  Tradeoffs of using private information retrieval (PIR)
- Accountability
  bidirectional communication
  - “Read public PIR allows for authentication and tracks the volume of data.”
  - “The network provider can charge users based on the amount of their data that is transmitted.”
  - “One data transfer writing to many rows of the PIR database makes it vulnerable to DoS attack.”
  - “To set up a bidirectional anonymous communications scheme to share location based deny lists.”
- Scalability
  database sharding and differential privacy

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Discussion

- **Metadata Privacy**
  Tradeoffs of using private information retrieval (PIR)
- **Accountability**
  bidirectional communication
- **Scalability**
  database sharding and differential privacy
  - "Stricter privacy guarantees resulting in higher computation, memory, and bandwidth cost."
  - "Adding noise locally at the gateway can avoid using cover traffic in exchange for a measurable privacy loss and additional latency."
  - "Uses of differential privacy must take into account a degrading privacy budget with repeated uploads from repetitive human behavior."

Where the Sidewalk Ends: Privacy of Opportunistic Backhaul
https://dl.acm.org/doi/abs/10.1145/3517208.3523757

Key takeaways

- Security and privacy concerns of opportunistic networks
- Basics of devices and gateway localization by reconstruction with routing metadata
- Potential solutions to handle Metadata Privacy, Accountability, and Scalability.

Wrap-up

Guest lecture:

Fri June 14, 10:45-12:30

Next regular lecture:

Wed June 19, 10:45-12:30

Topic: IoT Device Security

Dr. Antonia Affinito | a.affinito@utwente.nl
Prof. Cristian Hesselman | c.e.w.hesselman@utwente.nl

UNIVERSITY OF TWENTE.

SIDN LABS