Lecture #8: IoT security in non-carpeted areas

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, Etienne Khan, Ting-Han Chen

University of Twente | June 5, 2023

UNIVERSITY OF TWENTE.

SIDN LABS

Colonial Pipeline, May 2021

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

Today's agenda

- Admin
- Introduction
- Paper #1: security in LoraWAN networks
- Paper #2: Traffic Signal Control
- Feedback

UNIVERSITY OF TWENTE.
SDN LABS

Admin

UNIVERSITY OF TWENTE.

SDN LABS

Oral exams

- June 21st, 22nd, 26th, 28th, 30th, July 4th
- Sign up for a timeslot through Canvas
- 45 minutes
- Details: https://courses.sidnlabs.nl/ssi-2023/#oral-exam

UNIVERSITY OF TWENTE.
SIDN LABS

Schedule

No.	Date	Contents
1	Apr 26	Course introduction
2	May 3	Lecture: IoT and Internet Core Protocols
3	May 10	Lecture: IoT Botnet Measurements 1
4	May 17	Lecture: IoT Edge Security Systems
5	May 24	Lecture: IoT Device Security
6	May 31	Lecture: IoT Botnet Measurements 2
7	Jun 1	Guest lecture #1: Naval Systems, Dr. Sorin Iacob, Thales
8	Jun 5	Lecture: IoT Security in Non-Carpeted Areas
9	Jun 12	Guest lecture #2: Product Security for Bosch (IoT) products, Stephan van Tienen, Bosch Security Systems
10	Jun 14	Lecture: IoT Honeypots (re-sit)

UNIVERSITY OF TWENTE. SIDN LABS

Important dates

- Two summaries per lecture: before the lecture (07:00 CEST) in which the papers will be discussed
- Lab report (PDF) and required files: **Sun June 23, 2023, 23:59 CEST**
- All to be submitted through CANVAS

UNIVERSITY OF TWENTE. SDN LABS

Where are you with your lab assignment?

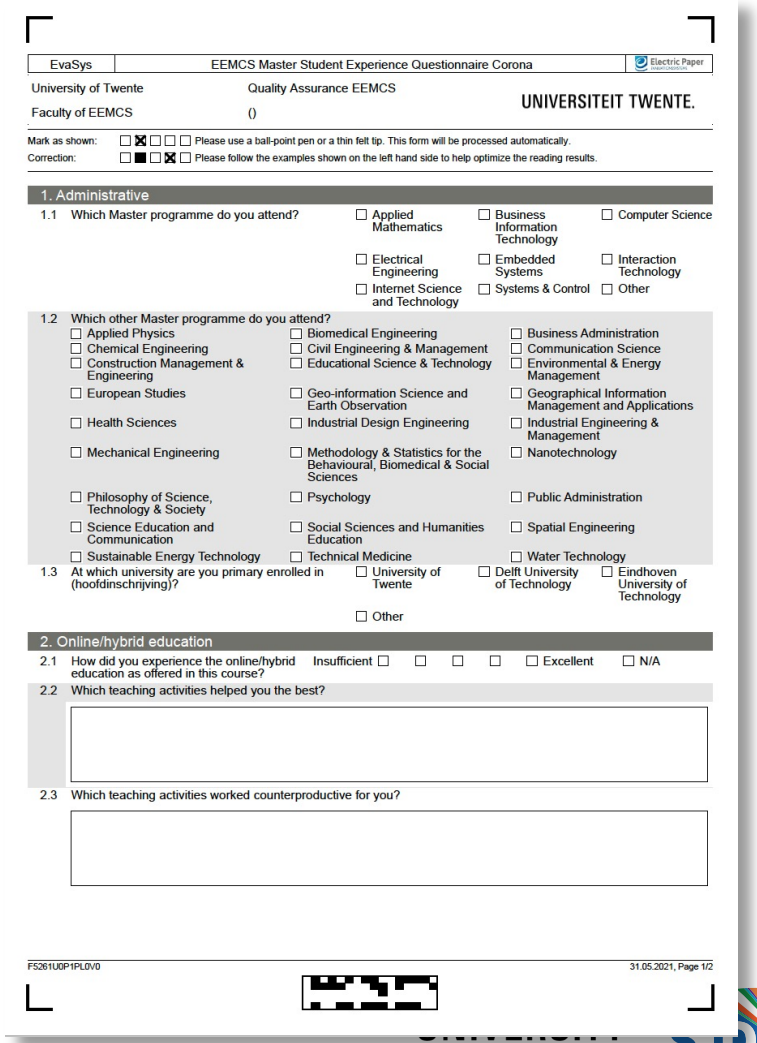
- Still trying to find the instructions on the SSI site
- Designing measurement setup
- Analyzing measurements
- Writing lab report
- Just need to click “submit” in Canvas

UNIVERSITY OF TWENTE.

SDN LABS

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 ☐ Business Information Technology ☐ Computer Science
☐ Electrical Engineering ☐ Embedded Systems ☐ Interaction Technology
☐ Internet Science and Technology ☐ Systems & Control ☐ Other

1.2 Which other Master programme do you attend?

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

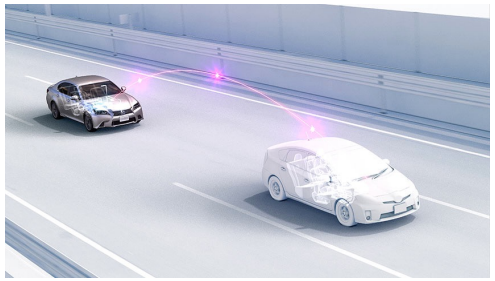
F5261U0P1PL0V0 31.05.2021, Page 1/2

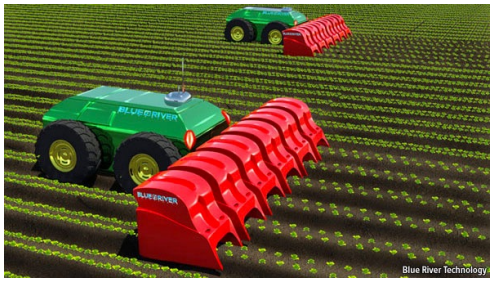
Introduction to today's lecture

UNIVERSITY OF TWENTE.

SIDN LABS

Motivation for today: IoT goes beyond carpeted areas





UNIVERSITY OF TWENTE.

SDN LABS

Today's papers

[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

[Traffic] Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z. Morley Mao, Henry X. Liu, "Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control", Network and Distributed Systems Security (NDSS) Symposium 2018, Feb 2018, San Diego, CA, USA

Today's learning objective

- After the lecture, you will be able be able to discuss technologies for non-consumer IoT applications ("non-carpeted areas"), specifically:
  - Security vulnerabilities of LoraWAN and their mitigations
  - Security risks of CV-based traffic light signaling

- 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

Did you hear about Lora and its applications?

UNIVERSITY OF TWENTE.

SIDN LABS

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

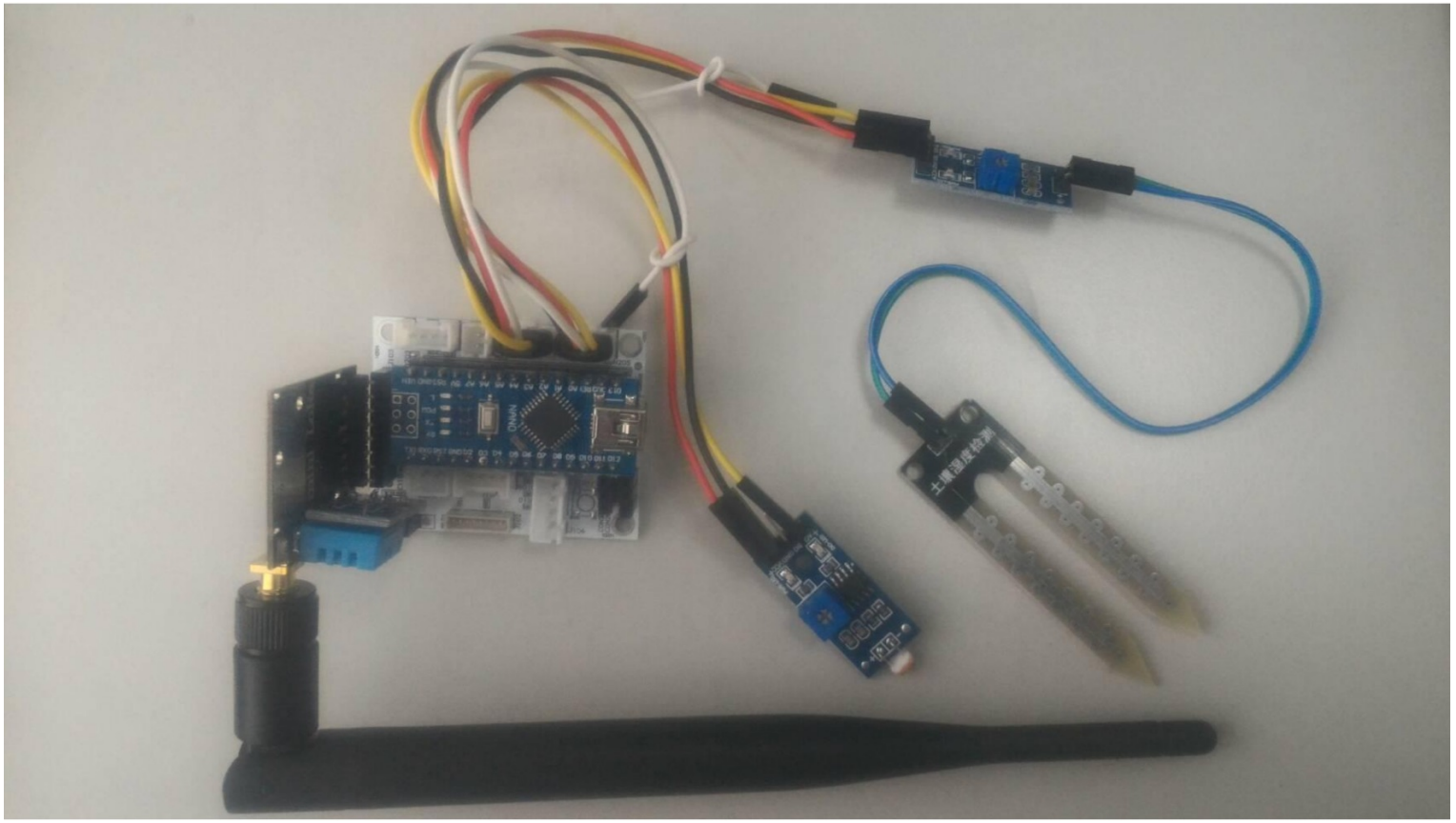
Farming

Aquaculture

UNIVERSITY OF TWENTE.

SDN LABS

LoraWAN: In a Workshop



UNIVERSITY OF TWENTE.

SDN LABS

LoraWAN: Self-made version

LASS
Location Aware
Sensor System

UNIVERSITY
OF TWENTE.

SDN LABS

LoraWAN: Long Distance, 832km as world record

公尺 = Meter, Best Record: 8km

Source: https://www.intelligentagri.com.tw/en

UNIVERSITY OF TWENTE.

STDN LABS

Deutsche Bahn is using LoraWAN, too

Picture: Johan Stokking, The Thing Industries

[Smart Train Stations with LoRaWAN - Olga Willner & Oliver Brandmüller - The Things Conference 2019 - YouTube]

UNIVERSITY OF TWENTE.

STDN LABS

Okay, how's the paper?

UNIVERSITY OF TWENTE.

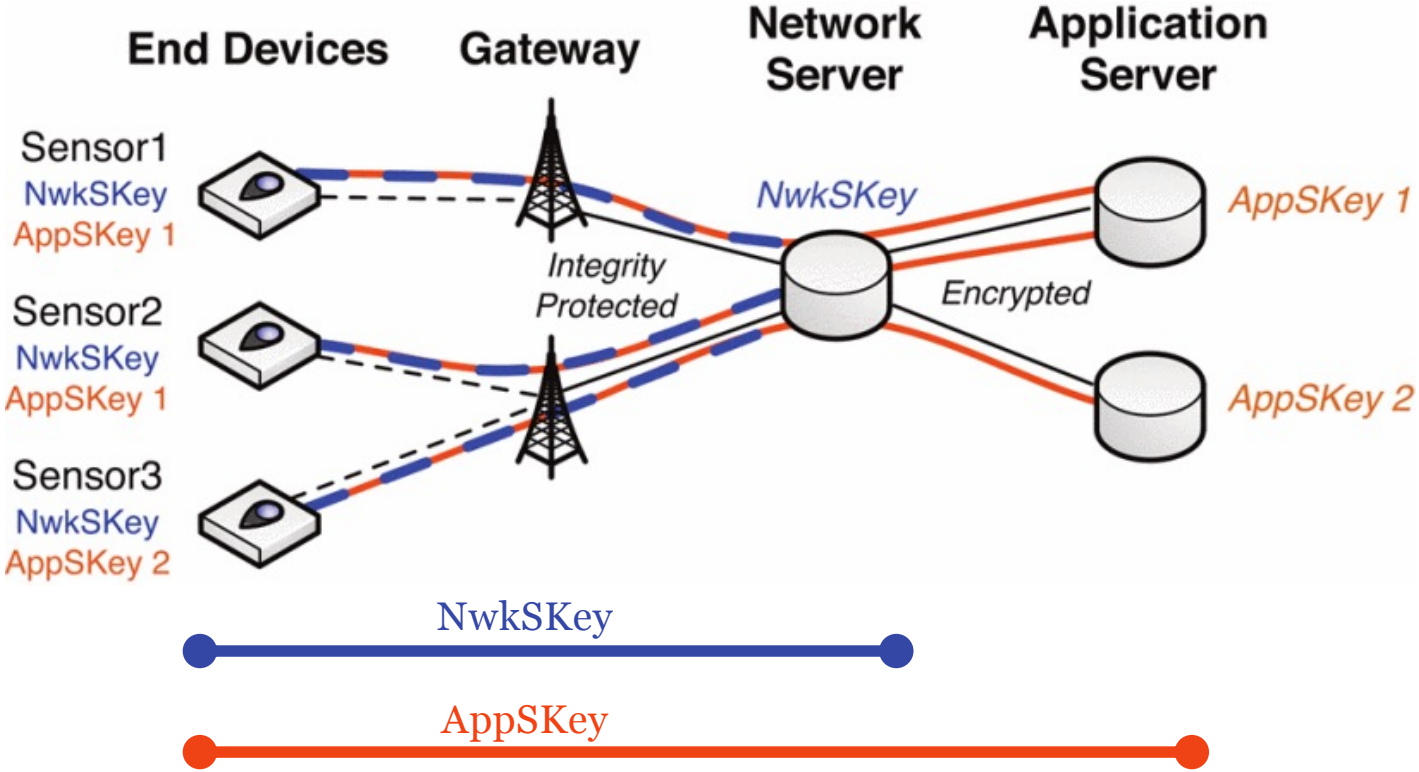
SIDN LABS

Let’s Start!

UNIVERSITY OF TWENTE.

SDN LABS

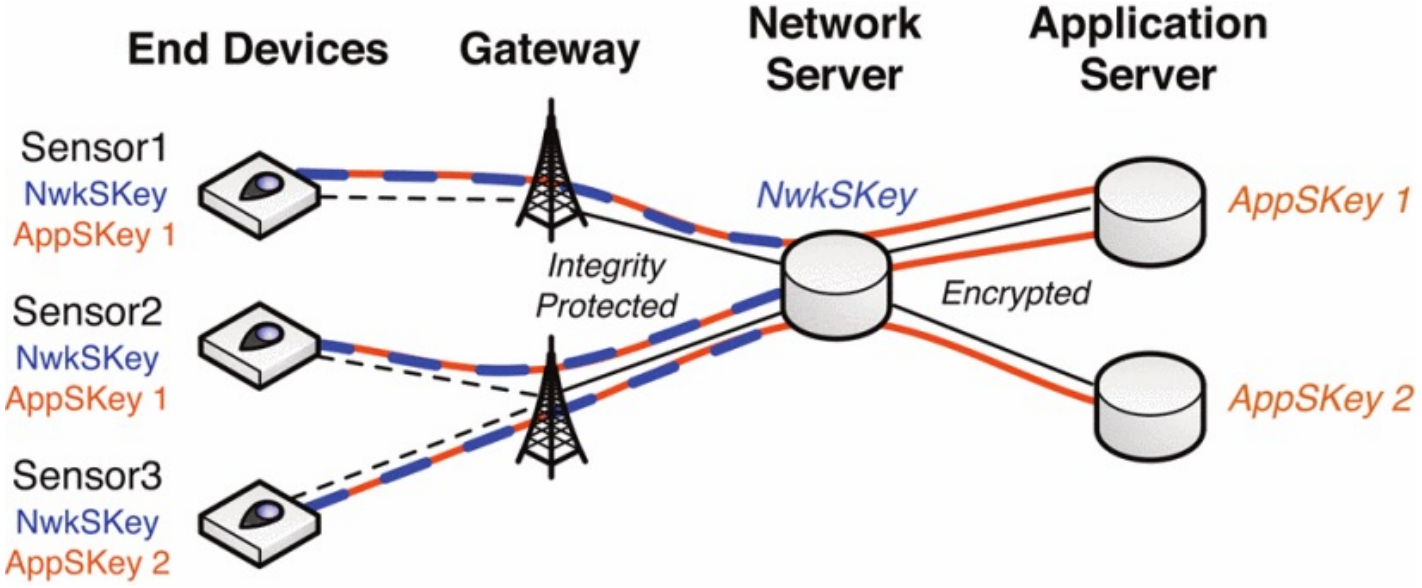
Discussion: LoraWAN roles and keys



UNIVERSITY OF TWENTE.

SDN LABS

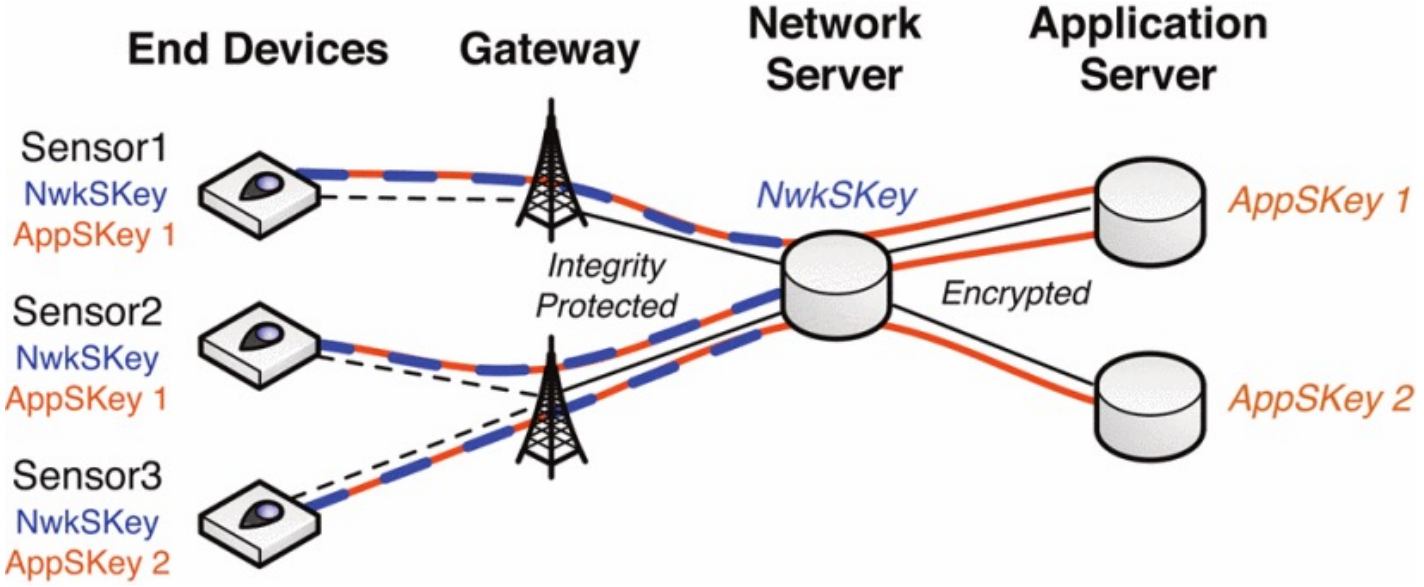
Discussion: LoraWAN roles and keys



UNIVERSITY OF TWENTE.

SDN LABS

Discussion: LoraWAN roles and keys



Network Session Key

Message Integrity & MAC Command

Application Session Key

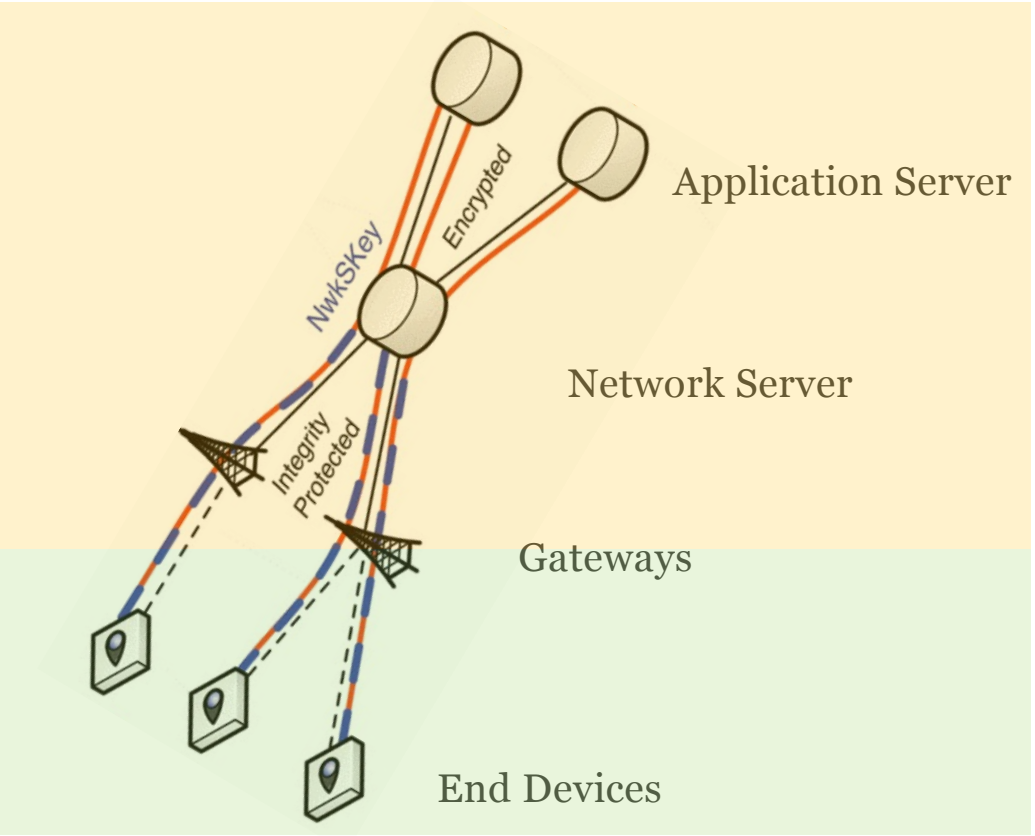
Payload Encryption & Decryption

UNIVERSITY OF TWENTE.

SDN LABS

Discussion: LoraWAN roles and keys

- Management plane
  - Key derivation (symmetric)
  - Device enrollment protocol (OTA and “personalized”)
  - Over the air firmware updates
- Data plane (packet forwarding)
  - Encryption of LoraWAN payloads
  - Message integrity verification
  - Replay protection



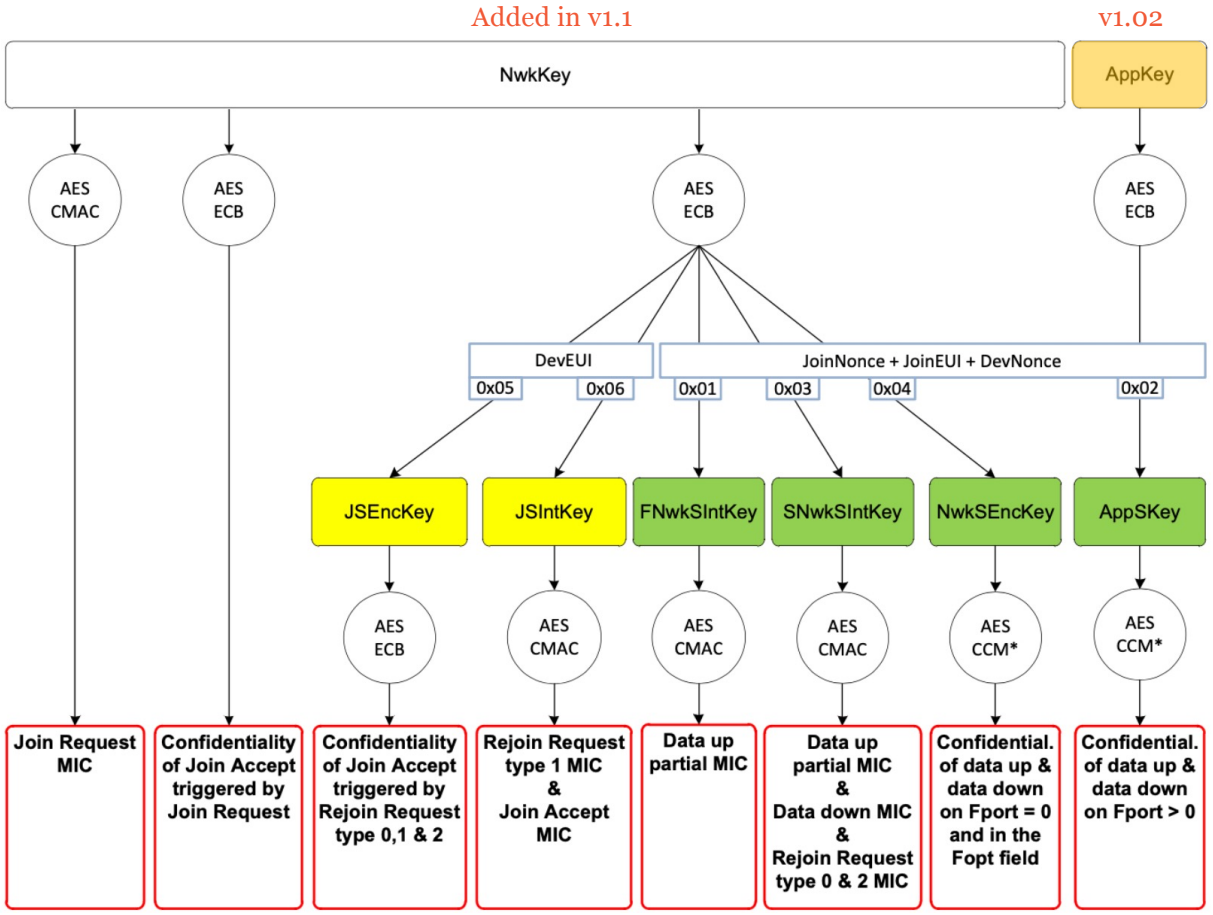
What's the root of trust in Over The Air Activation(OTAA)?

1) AppSkey
2) NwkSkey
3) Appkey
4) NwkKey

UNIVERSITY OF TWENTE.
SIDN LABS

LoraWAN key derivation

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



Picture: Johan Stokking, The Thing Industries

Which attack you like the most?

1. Replay attack for ABP-activated nodes
2. Eavesdropping
3. Bit-Flipping Attack
4. ACK spoofing
5. LoRa class B attacks

UNIVERSITY OF TWENTE.
SDN LABS

Discussion: denial of service through replay

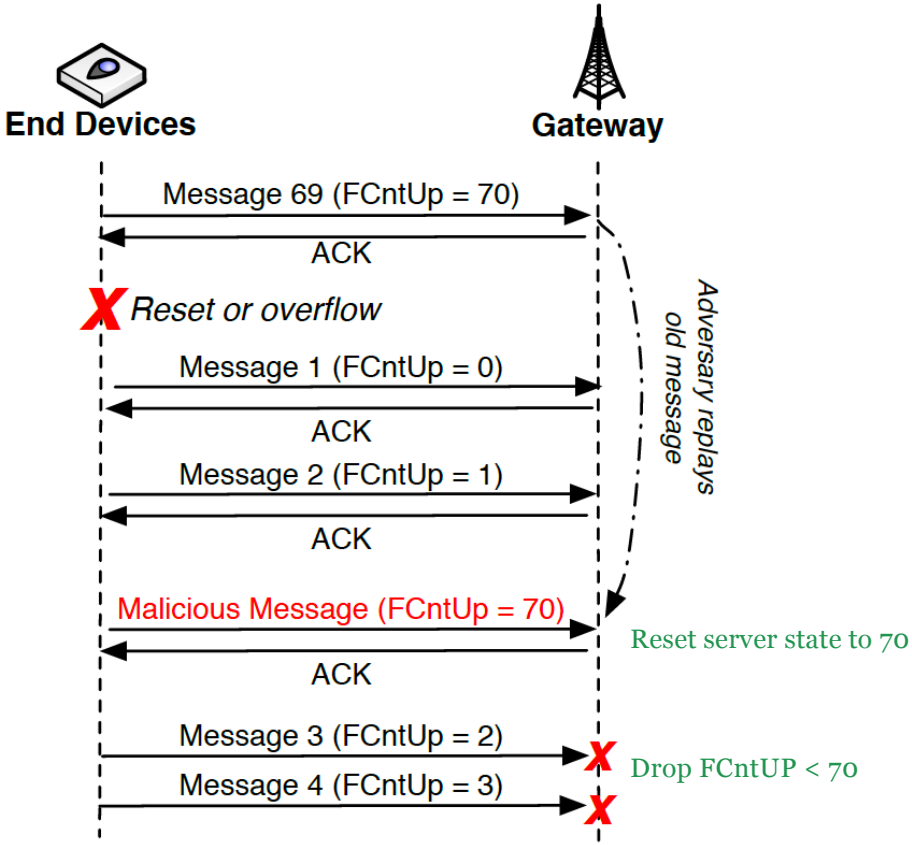


Fig. 4. An example of a replay attack for ABP.

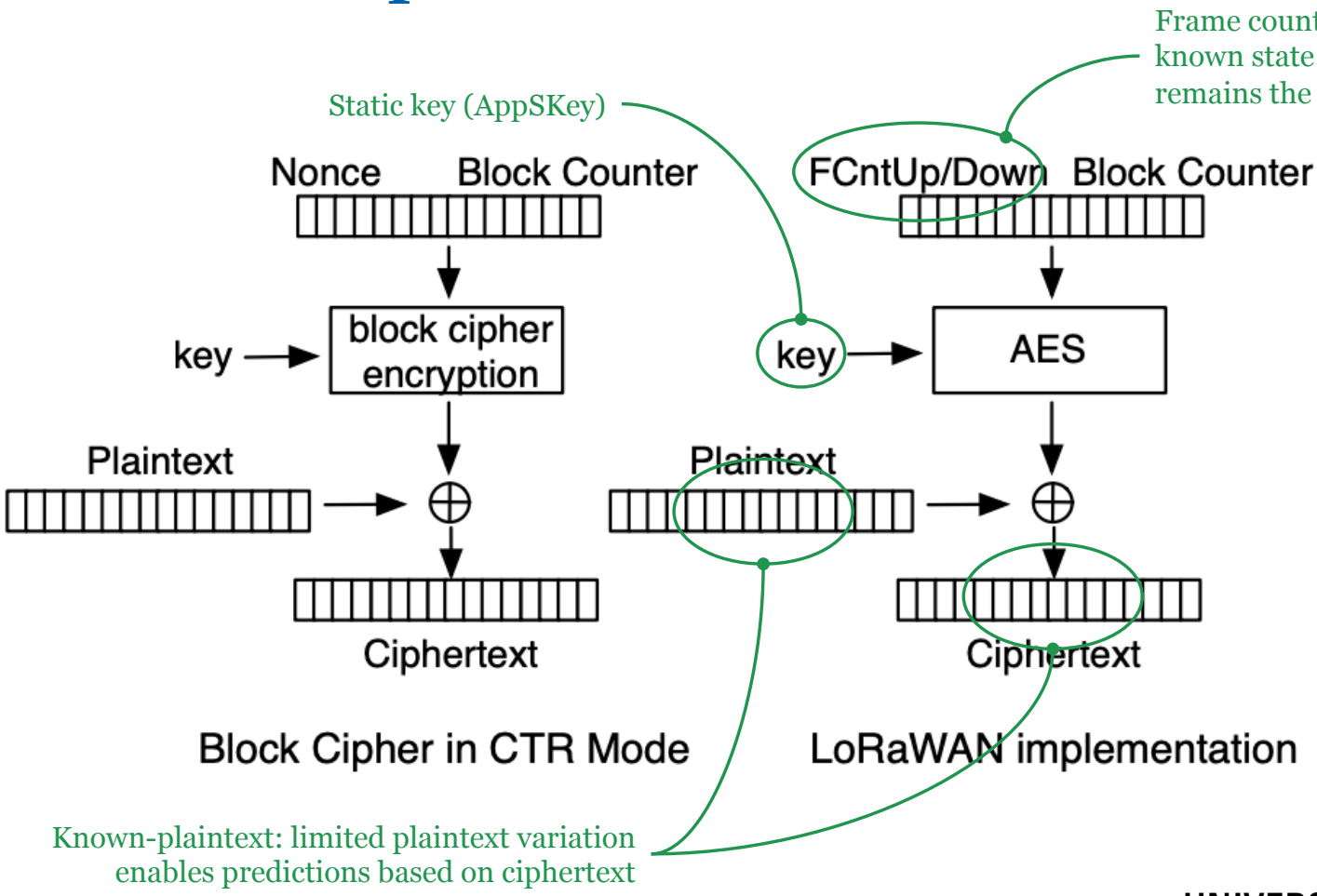
Injected message

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. SDN LABS

Discussion: known-plaintext attack

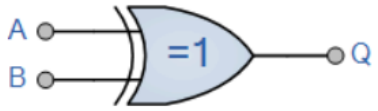


https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
https://en.wikipedia.org/wiki/Known-plaintext_attack
https://en.wikipedia.org/wiki/Block_cipher

UNIVERSITY OF TWENTE.

Discussion: Eavesdropping

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

Symbol	Truth Table		
 2-input Ex-OR Gate	B	A	Q
	0	0	0
	0	1	1
	1	0	1
	1	1	0
Boolean Expression Q = A ⊕ B	A **OR** B but NOT **BOTH** gives Q		

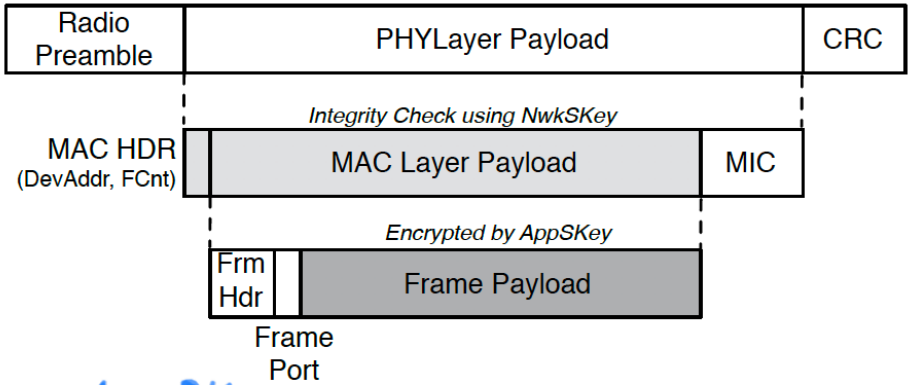
Is it worth it to get the simple messages such as temperature or humidity?
Is it important to protect those content?

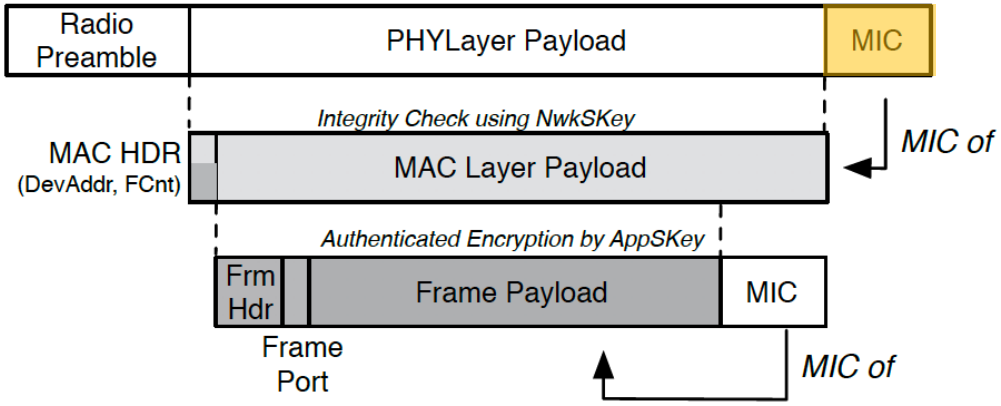
UNIVERSITY OF TWENTE. SDN LABS

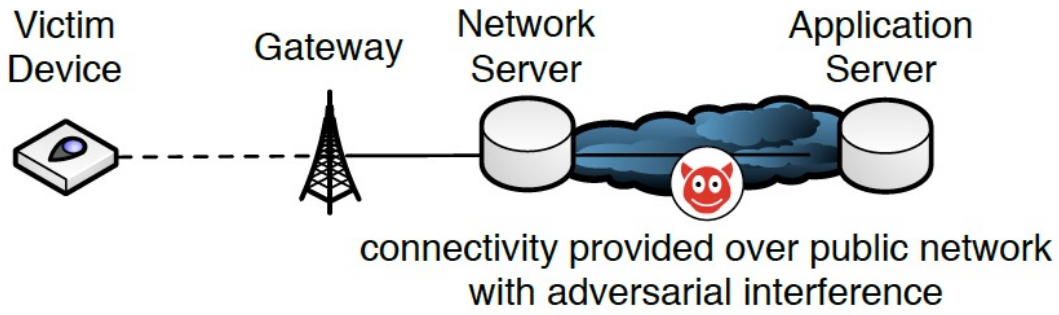
Why does LoraWAN not support end-to-end message integrity?

1) LoraWAN is a link-level technology
2) LoraWAN messages are encrypted
3) LoraWAN does not support application-level MICs
4) LoraWAN was not of attackers' interests

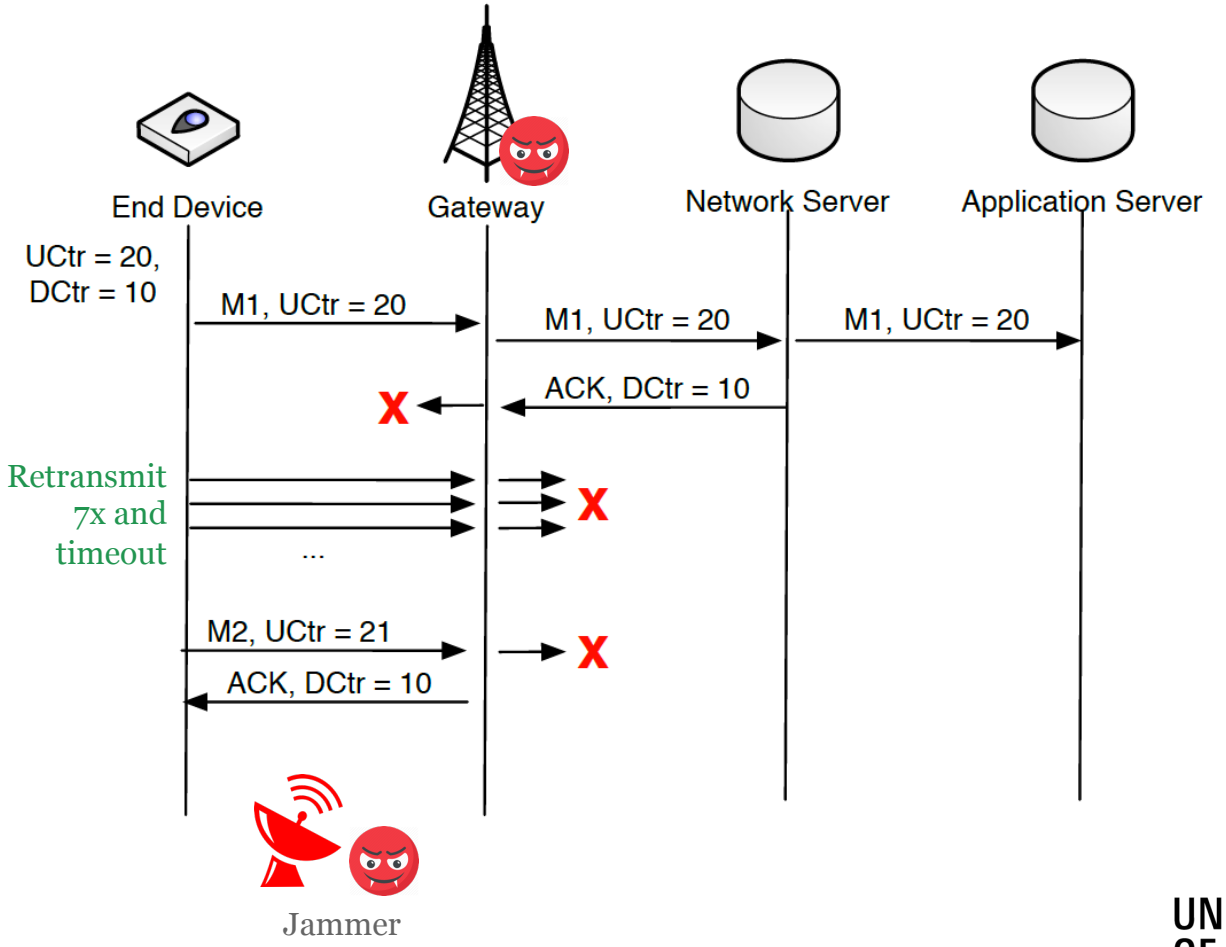
Discussion: proposed solution using 2 MICs







Discussion: ACK spoofing



UNIVERSITY OF TWENTE.

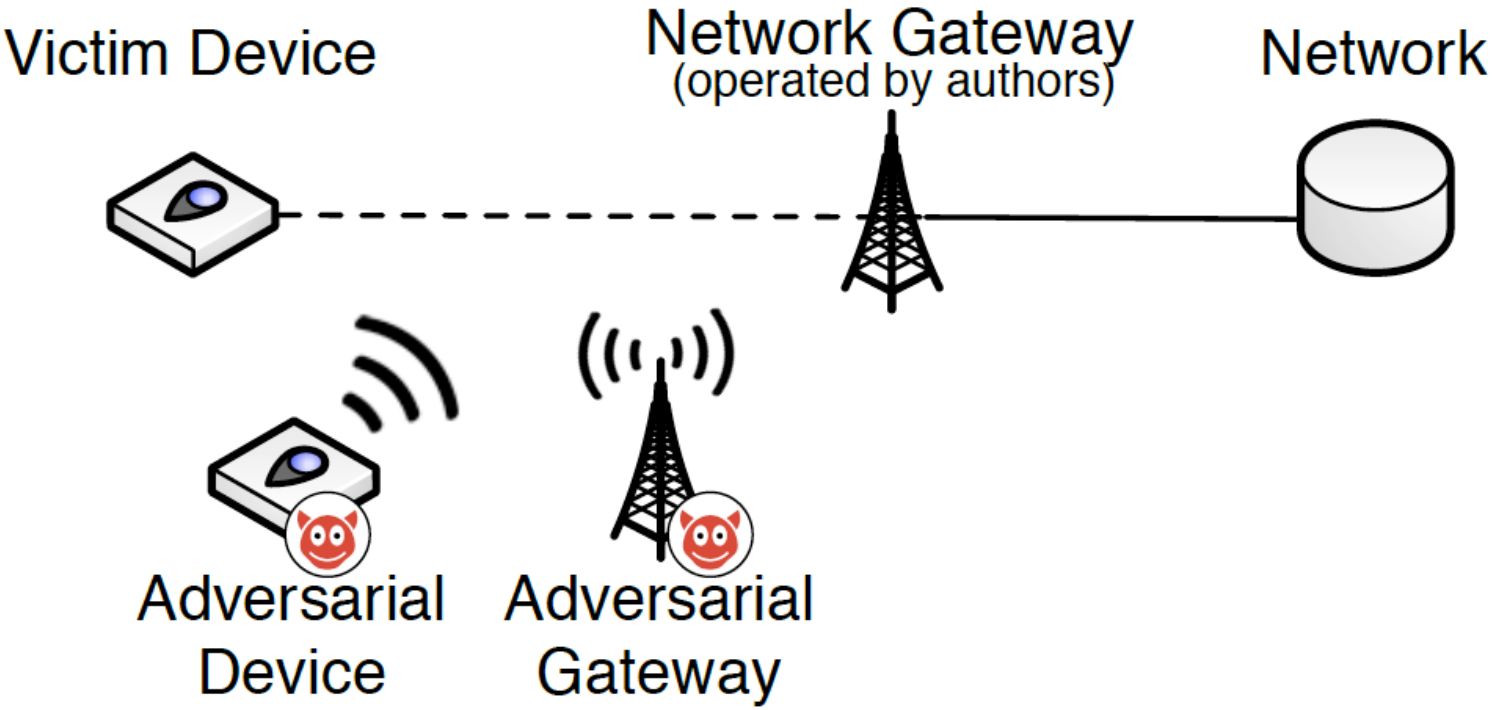
SDN LABS

How do the authors propose to extend ACK messages to tackle this problem?

1) Include a nonce signed by the gateway's private key
2) Include the frame counter value of the uplink messages
3) Accept the risk because adding more info to ACK's would be too expensive
4) Include cryptographic checksum that covers the uplink packet

UNIVERSITY OF TWENTE.
SIDN LABS

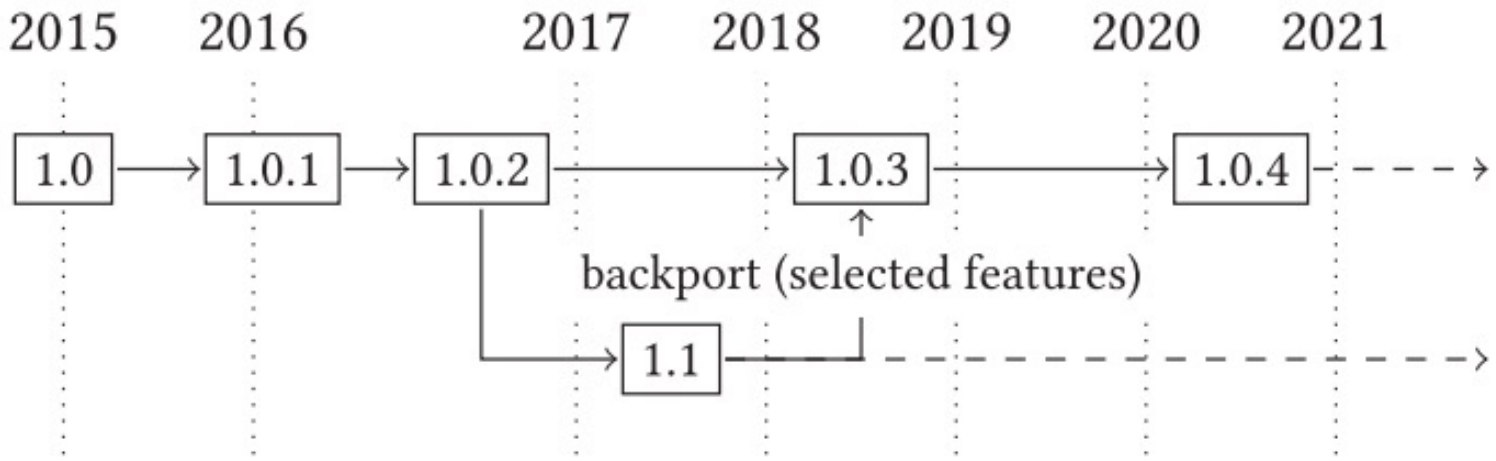
Discussion: Class B attacks - battery draining



UNIVERSITY OF TWENTE.

SDN LABS

Let's look at the version history of LoraWAN



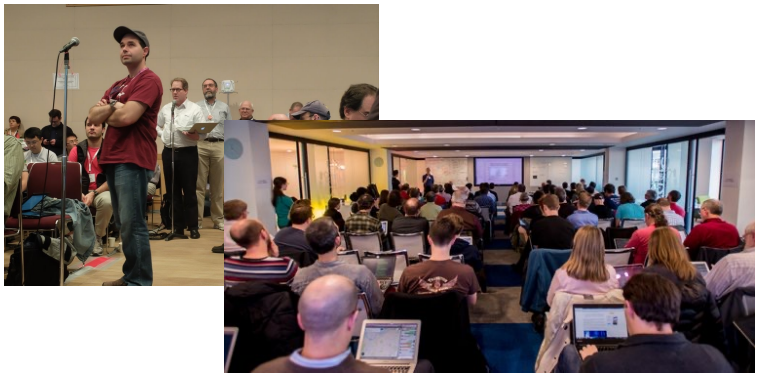
F. Hessel, L. Almon, and M. Hollick, 'LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and their Systematic Mitigation', ACM Trans. Sens. Netw., vol. 18, no. 4, p. 70:1-70:55, Mar. 2023, doi: 10.1145/3561973.

UNIVERSITY OF TWENTE.

SIDN LABS

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)



Discussion (if time permits)

- What would you do in the development process to make LoraWAN more secure? As an Engineer
- How would you update the protocol of LoraWAN regarding the features and security? As an Operator/Manufacturer

UNIVERSITY OF TWENTE.
SIDN LABS

Coffee break

UNIVERSITY OF TWENTE.
SDN LABS

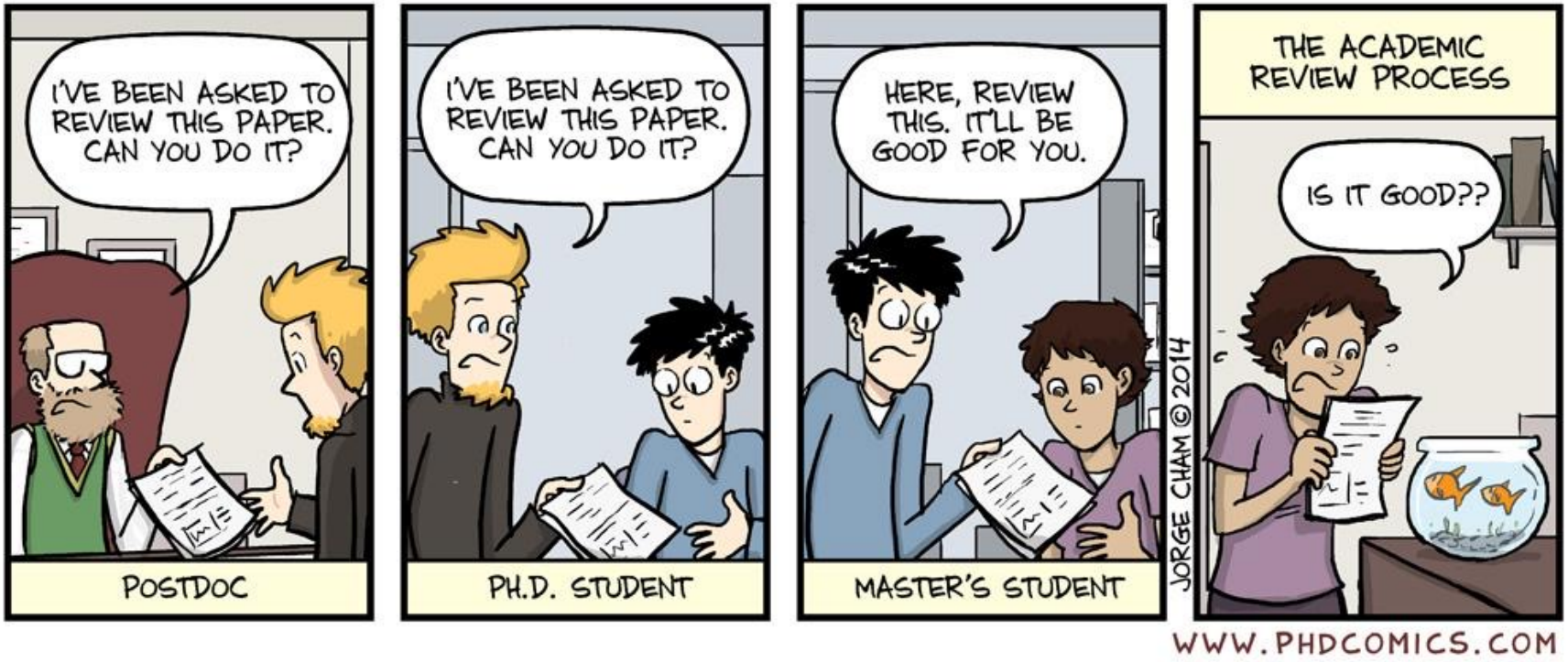
“Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control”

Network and Distributed Systems Security (NDSS) Symposium,
San Diego, CA, USA, February 2018

UNIVERSITY OF TWENTE.

SDN LABS

Your opinion



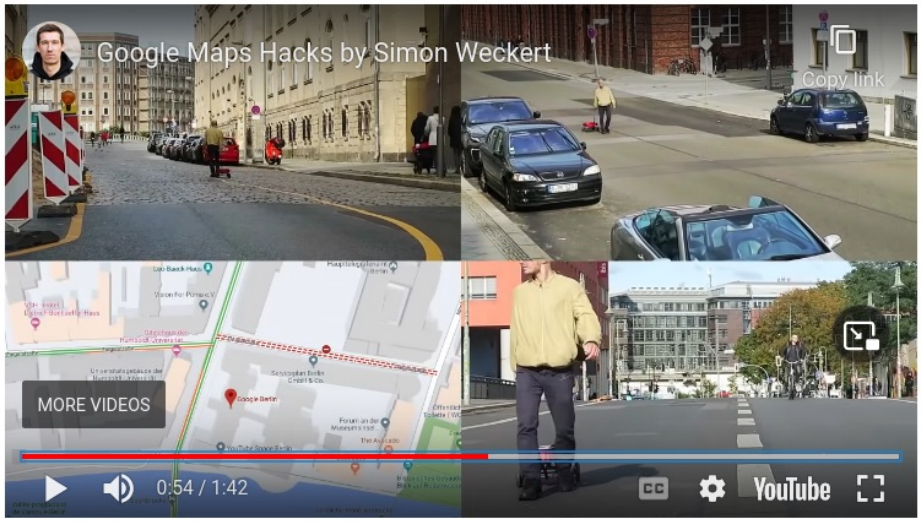
UNIVERSITY OF TWENTE.

SDN LABS

Similar hack on Google maps

Berlin artist uses 99 phones to trick Google into traffic jam alert

Google Maps diverts road users after mistaking cartload of phones for huge traffic cluster



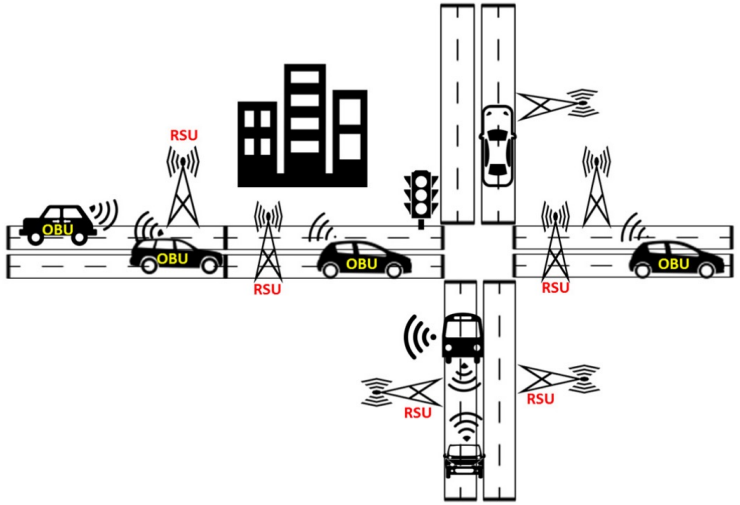
Google Maps Hacks by Simon Weckert.

Source: https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert

UNIVERSITY OF TWENTE. SDN LABS

Basic Safety Messages

"The basic safety message contains vehicle safety-related information that is periodically broadcast to surrounding vehicles." [SAE J2735]



H. Hasrouny et al., "VANet security challenges and solutions: A survey"

```
BasicSafetyMessage ::= SEQUENCE {
   -- Part I
   msgID       DSRCmsgID,                -- 1 byte

   -- Sent as a single octet blob
   blob1       BSMblob,

   --
   -- The blob consists of the following 38 packed bytes:
   --
   -- msgCnt      MsgCount,              -x- 1 byte
   -- id          TemporaryID,           -x- 4 bytes
   -- secMark     DSecond,               -x- 2 bytes

   -- pos         PositionLocal3D,
     -- lat       Latitude,              -x- 4 bytes
     -- long      Longitude,             -x- 4 bytes
     -- elev      Elevation,             -x- 2 bytes
     -- accuracy  PositionalAccuracy,    -x- 4 bytes

   -- motion      Motion,
     -- speed     TransmissionAndSpeed,  -x- 2 bytes
     -- heading   Heading,               -x- 2 byte
     -- angle     SteeringWheelAngle     -x- 1 bytes
     -- accelSet  AccelerationSet4Way,   -x- 7 bytes

   -- control     Control,
   -- brakes      BrakeSystemStatus,     -x- 2 bytes

   -- basic       VehicleBasic,
   -- size        VehicleSize,           -x- 3 bytes

   -- Part II, sent as required
   -- Part II,
   safetyExt     VehicleSafetyExtension OPTIONAL,
   status        VehicleStatus          OPTIONAL,
   }
```

Tsai, Ming-Fong, et al. "Cooperative emergency braking warning system in vehicular networks."

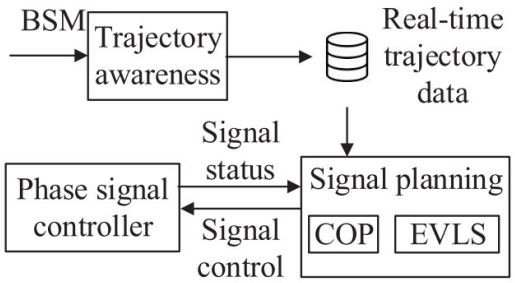
UNIVERSITY OF TWENTE.

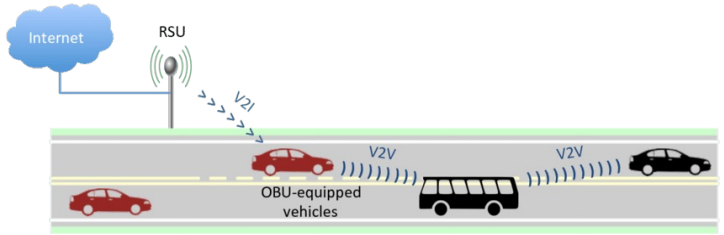
SDN LABS

Problem source

- **Hardware limitations:**
  - > Signal plan needs to be ready in a limited time
  - > Limited number of stages
  - > Not all vehicles served
  - > A plan with least unserved vehicles is chosen, then one with least total delay.

- **Penetration rate:**
  - > Not all cars are equipped with OBUs.



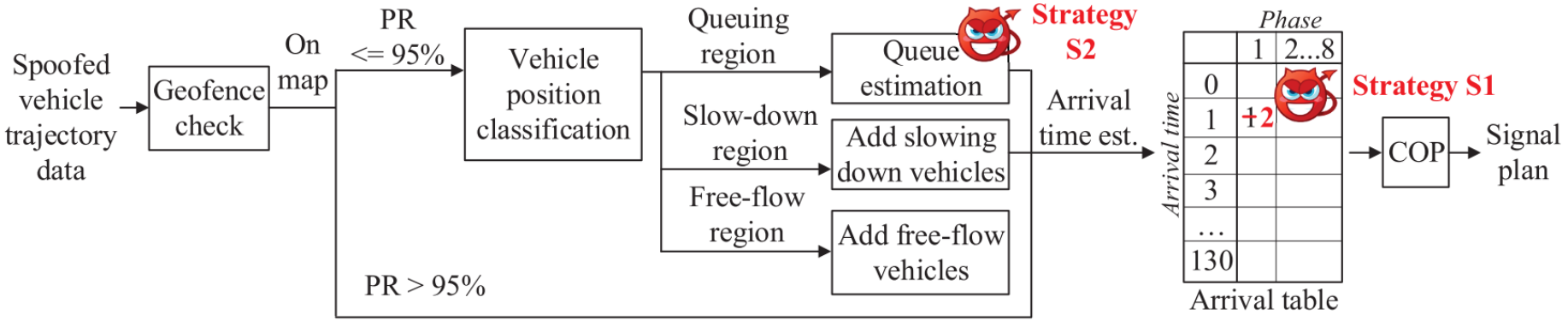


UNIVERSITY OF TWENTE.

SDN LABS

Spoofed data flow

- **S1:** Arrival time and phase spoofing (full deployment and transition period)
- **S2:** Queue length manipulation (transition period only)



Attack effectiveness

- **Full deployment:**

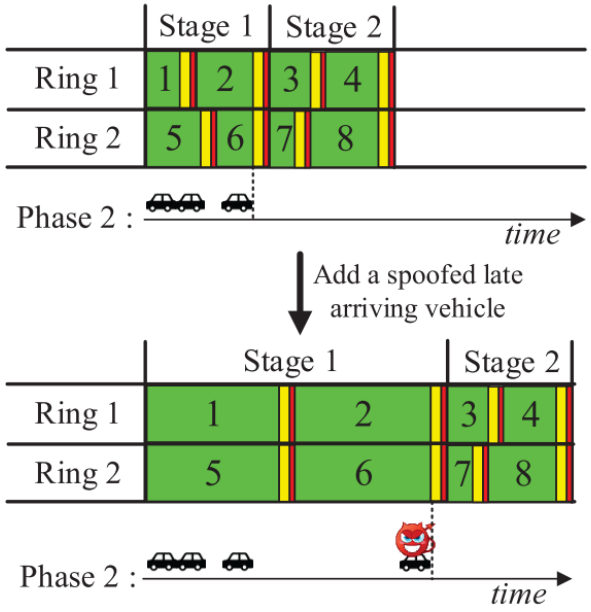
  2 stage: last vehicle advantage

  5 stage: open skipped phase + extend green light

- **Transition period**

  2 stage: last vehicle advantage (more impact because of the tgmax of preceding phases) + adding to queue length

  5 stage: open skipped phase + extend green light



UNIVERSITY OF TWENTE.

SDN LABS

Attack vectors in VANET

- This paper is specifically on congestion attacks. What other attacks in vehicular ad-hoc networks (VANET) can you think of?

- Can we disrupt traffic signal control in a different way?

UNIVERSITY OF TWENTE.
SDN LABS

Attack vectors in VANET

Table 2
Classification of Attacks based on four categories and VANET communication mode.

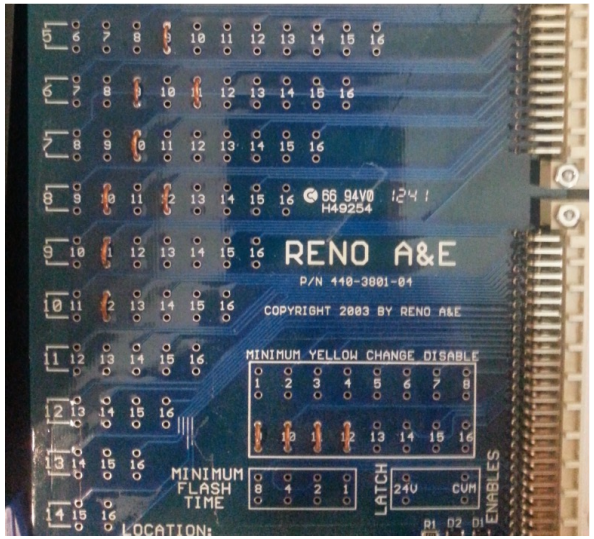
Attacks on	Attack name	Attack on VANET communication mode
Wireless interface	– Location Tracking – DoS, DDoS – Sybil – Malware and spam. – Tunnelling, Blackhole, Greyhole. – MiM – Brute force	V2V
Hardware and software	– DoS – Spoofing and forgery. – Cheating with position info (GPS spoofing). – Message suppression/ alteration/fabrication. – Replay – Masquerade – Malware and spam – MiM – Brute force	V2V, V2I
	– Sybil – Injection of erroneous messages (bogus info). – Tampering hardware – Routing, Blackhole, wormhole and Greyhole. – Timing.	V2V
Sensors input in vehicle	– Cheating with position info(GPS spoofing) – Illusion attack – Jamming attack	V2V
Infrastructure	– Session hijacking – DoS, DDoS – Unauthorized access – Tampering hardware – Repudiation – Spoofing, impersonation or masquerade	V2I and V2V

Source: H. Hasrouny et al.,
"VANet security challenges and solutions: A survey"

UNIVERSITY OF TWENTE.
SDN LABS

Malfunction management unit

- Older setup where only road sensor data is in use:
  - "With direct access to the traffic cabinet, an attacker would be able to remove fail-safe equipment and perform dangerous attacks (e.g. four-way green lights) in addition to the attacks described in this paper." [1]
  - Still possible to perform a DoS by setting all lights to red.



Source: B. Ghena et al., "Green Lights Forever: Analyzing the Security of Traffic Infrastructure"

[1] B. Ghena et al., "Green Lights Forever: Analyzing the Security of Traffic Infrastructure"

UNIVERSITY OF TWENTE. SIDN LABS

Region assignment in PR<95%

Was this clear?

> "The algorithm first finds the stopped equipped vehicle that is the farthest from the lane stop bar and uses its location as the end of the queuing region. The slow-down region started right after the queuing region, and the algorithm uses the equipped vehicle's trajectory data to judge whether it is slowing down due to an unequipped front vehicle based on a car-following model. After the slow-down region begins the free-flow region."

What if there are non-equipped cars after last equipped stopped car?

UNIVERSITY OF TWENTE. SIDN LABS

Exploit construction

> Yellow signal start

> wait 1 sec (5 secs left)

> estimate locations on map for 5 secs later

> run I-SIG without spoofing (4 secs for running I-SIG without and with spoofing in parallel, 1 sec is spared for BSM transition delay, etc.)

Attack evaluation

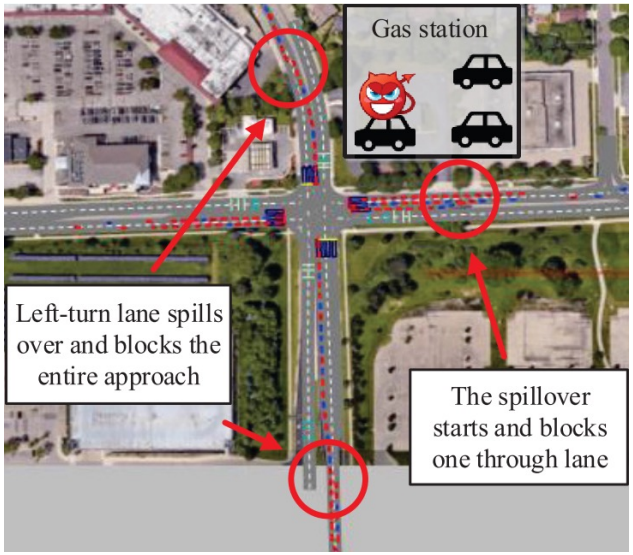
E1: Congestion attack for two-stage planning. Consistent results with vulnerability analysis.
E2: Congestion attack for five-stage planning in the full deployment period. Lower performance than vulnerability analysis, due to estimation errors nullifying attach effect.
E3: Congestion attack for five-stage planning in the transition period. Higher performance than vulnerability analysis due to cumulative blocking effect.

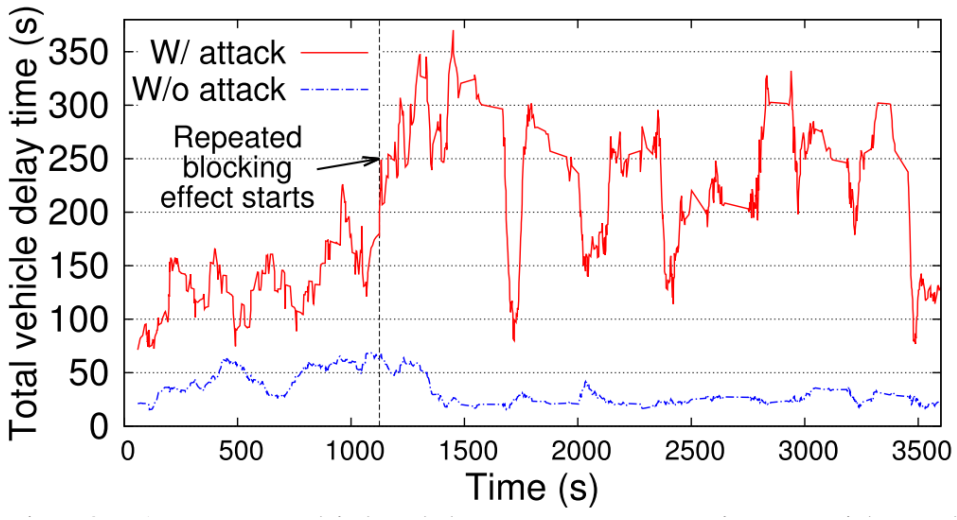
CV deployment	Full deployment		Transition period					
	100% PR		75% PR		50% PR		25% PR	
COP config.	2-S	5-S	2-S	5-S	2-S	5-S	2-S	5-S
Exploit	E1	E2	E1	E3	E1	E3	E1	E3
Ave. delay	68435.4	4695.9	64008.0	187746.0	66797.4	197410.0	56618.0	146685.0
inc. (s) & %	66.7%	4.8%	61.7%	181.6%	64.2%	193.3%	46.2%	133.2%

UNIVERSITY OF TWENTE. SDN LABS

Cumulative attack

"As shown, the delay under attack usually has an increase when the delay without attack increases. This is because when the approach is more congested without attack due to a temporarily higher demand, the congestion attack can further escalate such congestion."





UNIVERSITY OF TWENTE.

SDN LABS

Defense mechanisms?

- More powerful RSU hardware
- Returning sanity check to RSUs (traffic lights) rather than purely relying a self-declaration (e.g., using cameras and infrastructure-side sensors)
- Encrypted BSM?
- …

UNIVERSITY OF TWENTE. SDN LABS

Key Takeaways

- Security backdoors might be introduced due to implementation choices.
- Unavoidable transition period should be considered in a protocol design.
- Some sanity check on BSMs can help reduce the attack vector, e.g., use of extra road sensors as input for the traffic signaling.

Feedback

UNIVERSITY OF TWENTE.

SDN LABS

Today's objective revisited

- After the lecture, you will be able be able to discuss technologies for non-consumer IoT applications ("non-carpeted areas"), specifically:
  - Security vulnerabilities of LoraWAN and their mitigations
  - Security risks of CV-based traffic light signaling

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

Volg ons

SIDN.nl

@SIDN

SIDN

Discussion & feedback

Next lecture: **Mon Jun 12 (guest lecture), 10:45-12:30**
Topic: Product Security for Bosch (IoT) products
Room: RA 3334

UNIVERSITY OF TWENTE.

SIDN LABS