Lecture #9: IoT security in non-carpeted areas

Cristian Hesselman, Elmer Lastdrager, Ramin Yazdani, and Etienne Khan

University of Twente | June 16, 2022

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

Admin

UNIVERSITY OF TWENTE.

SDN LABS

Oral exams

- Thu Jun 23 (on campus), Fri Jul 1 (online), Fri Jul 8 (on campus)
- Sign up for a timeslot through Canvas
- 45 minutes
- Details: https://courses.sidnlabs.nl/ssi-2022/#oral-exam

Schedule

No.	Date	Contents
1	Apr 26	Course introduction Guest lecture #1: IoT and SPIN
2	May 11	Lecture: IoT security risks and challenges
3	May 18	Lecture: IoT Botnet Measurements
4	May 24	Guest lecture #2: Intro to cyber-physical systems (Jeroen Gaiser, Rijkswaterstaat)
5	May 25	Lecture: IoT Malware Analysis
6	Jun 1	Lecture: IoT Edge Security Systems
7	Jun 7	Lecture: IoT Device Security
8	Jun 14	Guest lecture #3: Strengthening the IoT Ecosystem: Privacy Preserving IoT Security Management (Dr Anna Maria Mandalari, Imperial College London)
9	Jun 15	Lecture: IoT in Non-Carpeted Areas
10	Jun 22	Lecture: IoT Honeypots (re-sit)

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 26, 2022, 23:59 CEST**
- All to be submitted through CANVAS

UNIVERSITY OF TWENTE.

SDN LABS

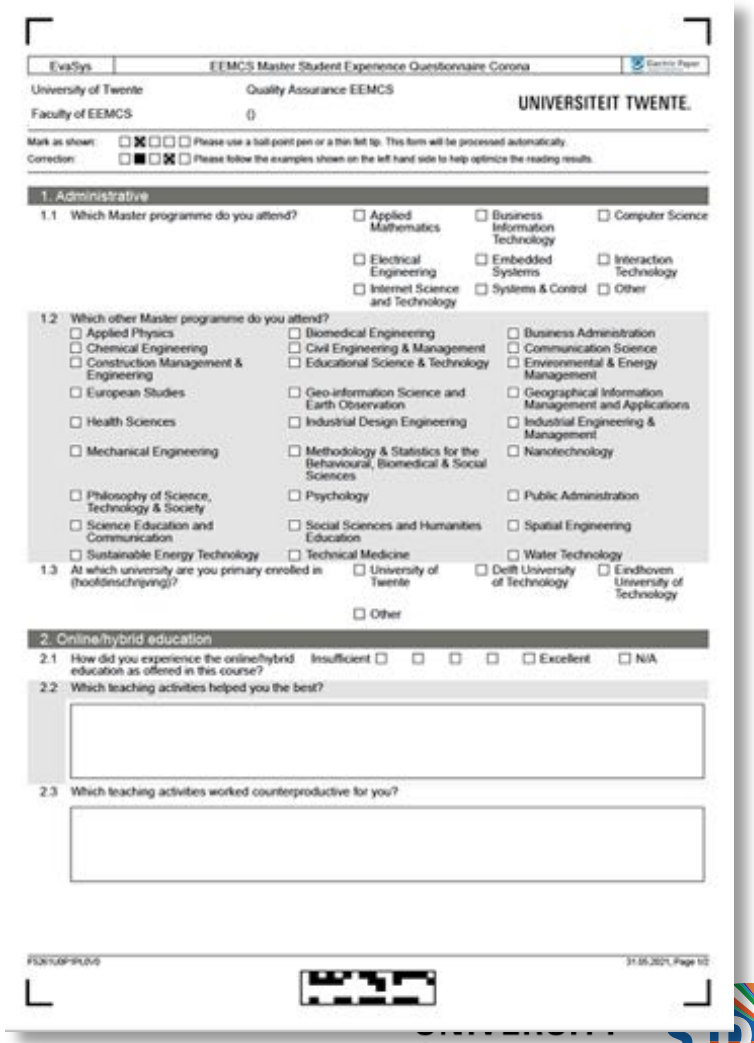
Where are you with your lab assignment?

- 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.

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

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?

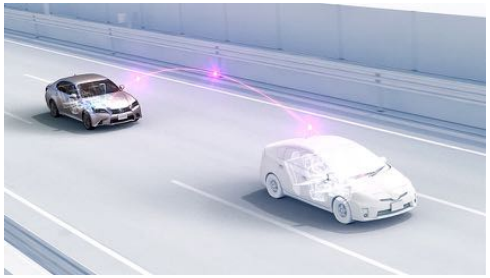
2.3 Which teaching activities worked counterproductive for you?

Introduction to today's lecture

UNIVERSITY OF TWENTE.

SDN 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 remote-controlled traffic lights

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

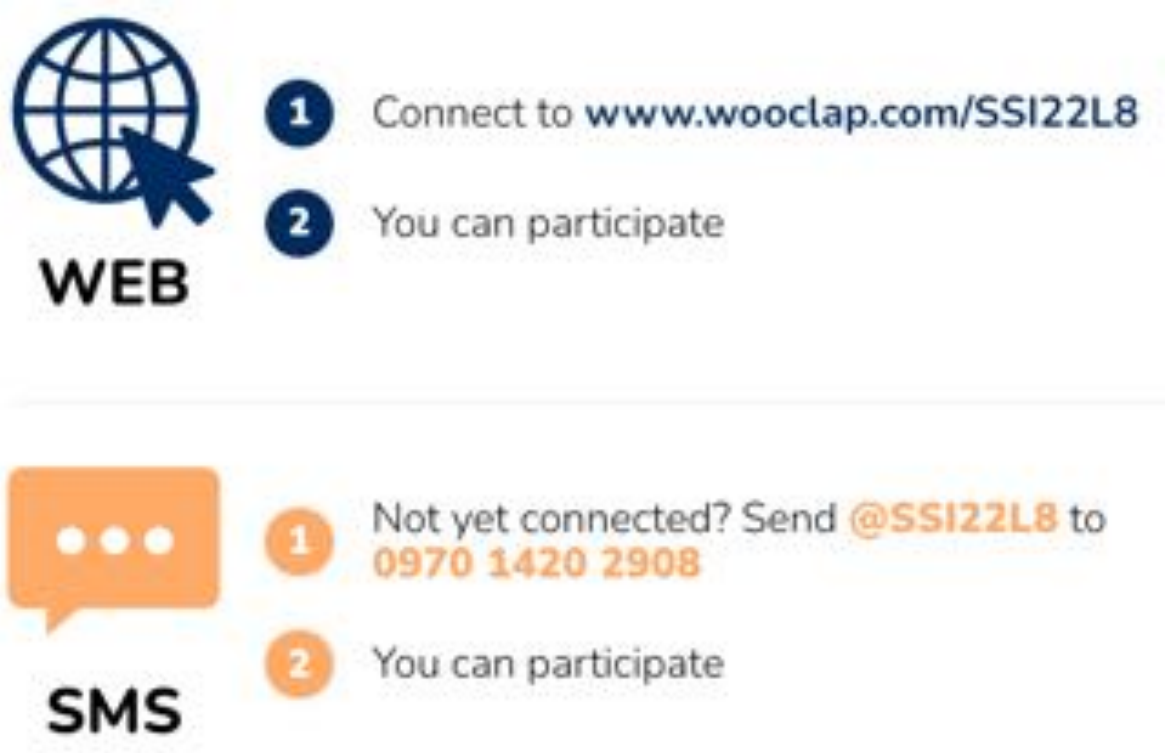
“Security Vulnerabilities in LoRaWAN”

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

Wooclap quizzes (max three)



Multiple-choice questions: 30 seconds
Open questions: 1.5 minutes

LoraWAN: low power, wide area, low bitrate comms

LoraWAN temperature sensor

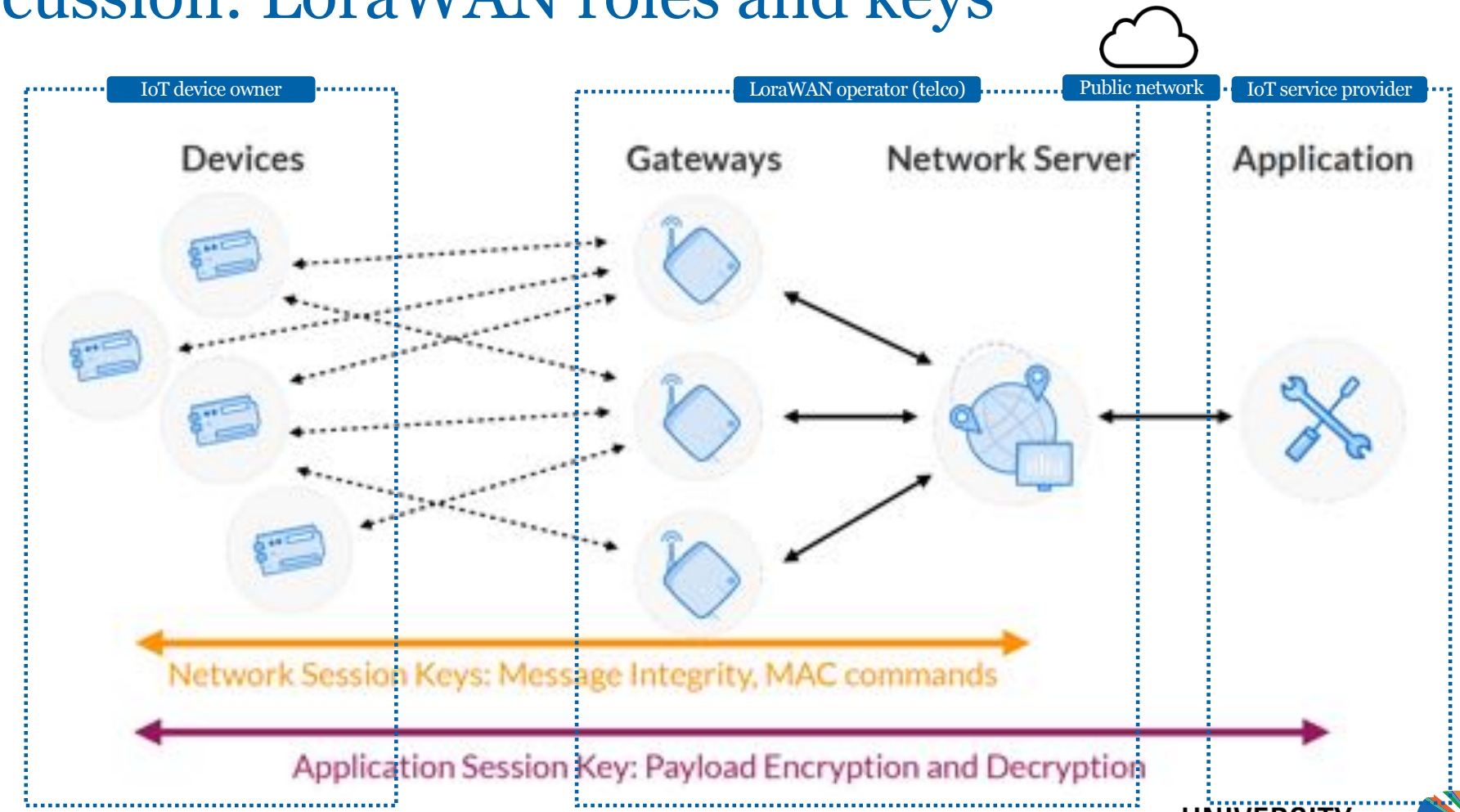
Modbus-over-LoraWAN bridge

LoraWAN gateway

UNIVERSITY OF TWENTE.

SDN LABS

Discussion: LoraWAN roles and keys

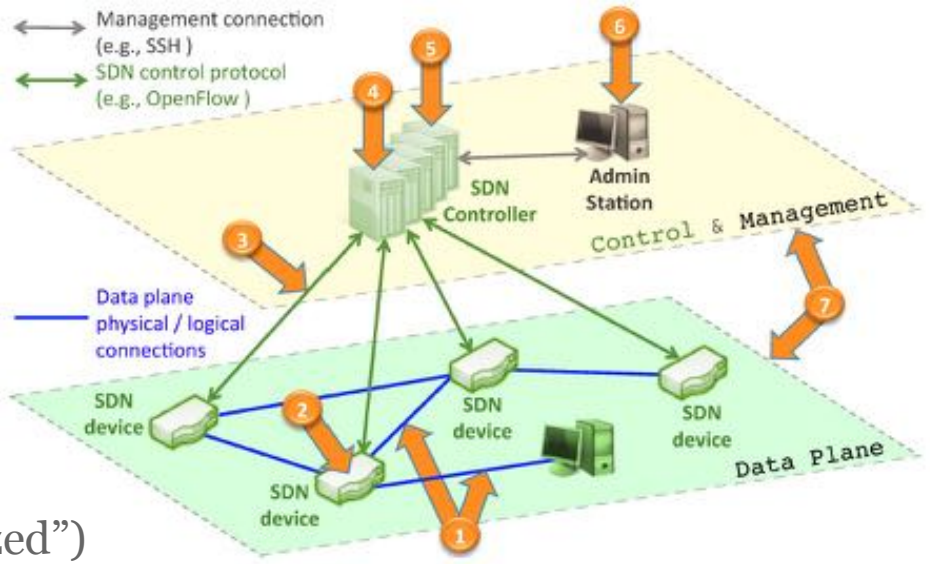


Picture: Johan Stokking, The Thing Industries

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

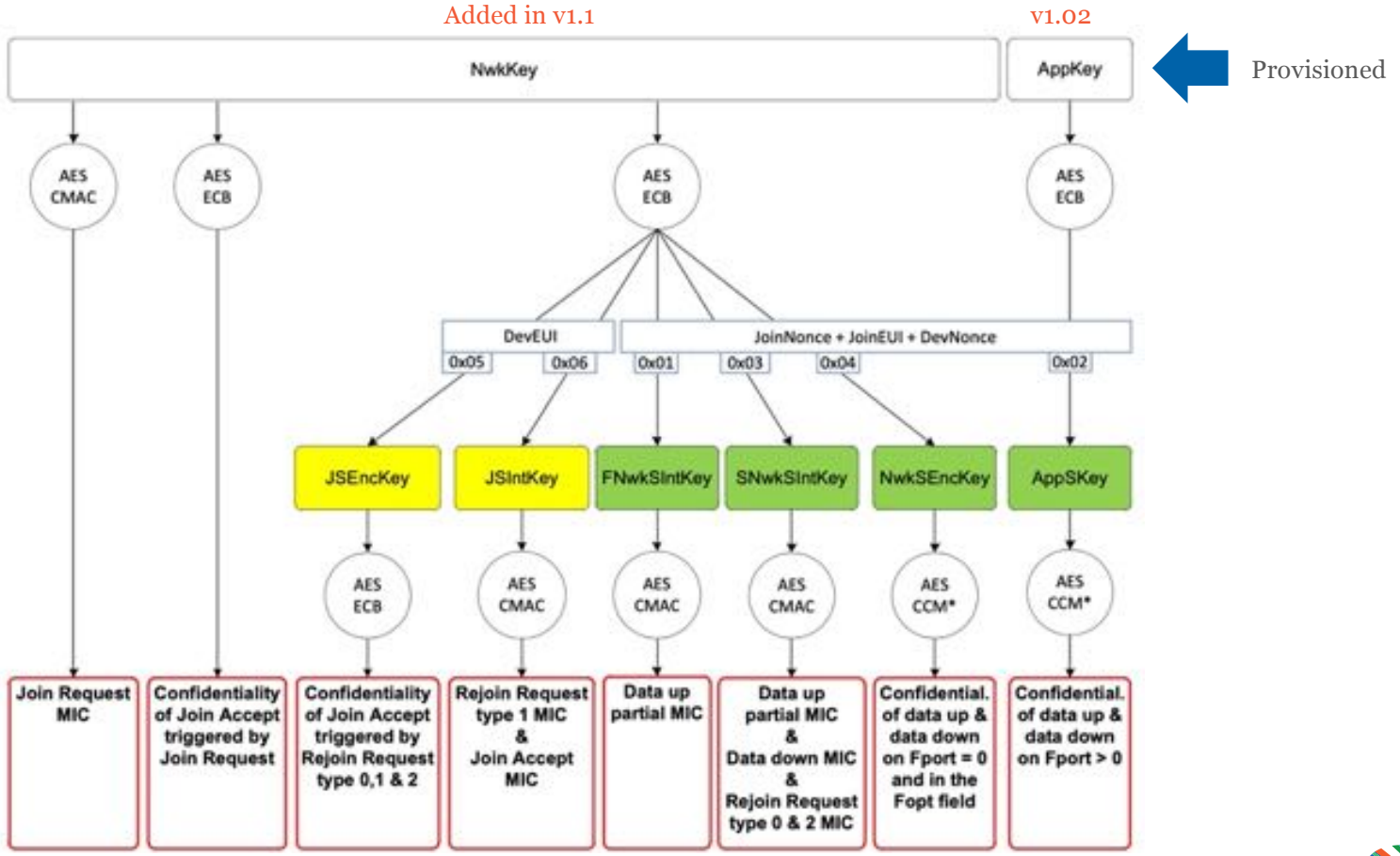


Source: D. Kreutz, F. M. V. Ramos, P. Verissimo, HotSDN’13, August 16, 2013, Hong Kong, China.

UNIVERSITY OF TWENTE. SDN LABS

LoraWAN key derivation

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



Picture: Johan Stokking, The Thing Industries

Discussion: denial of service through replay

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.

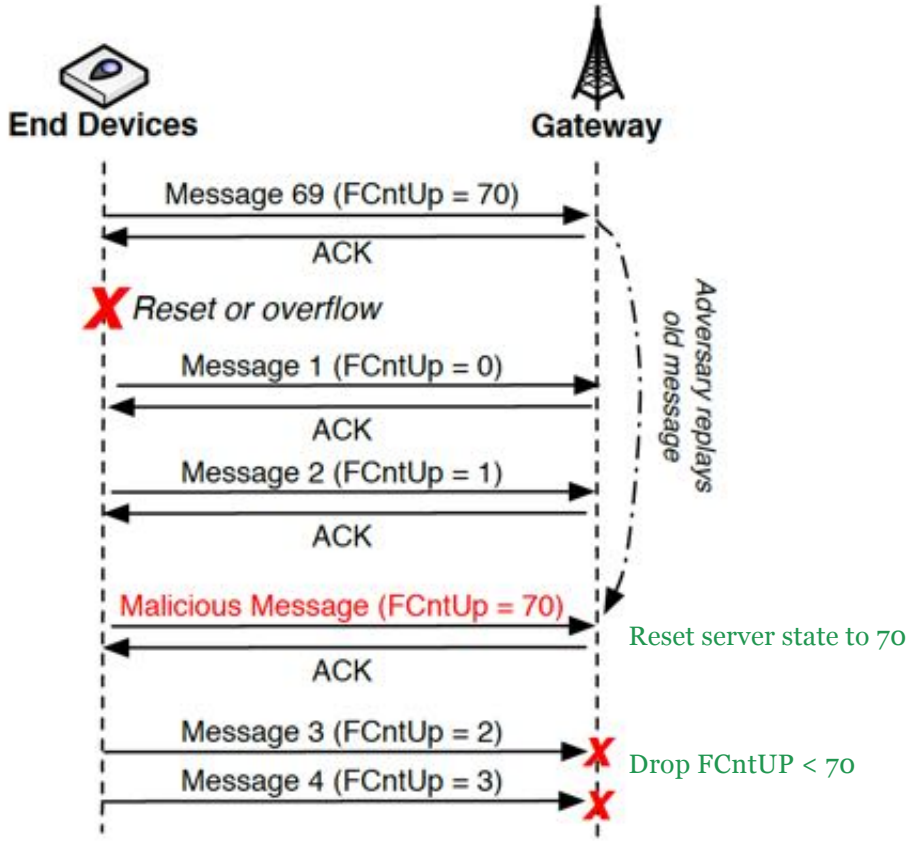
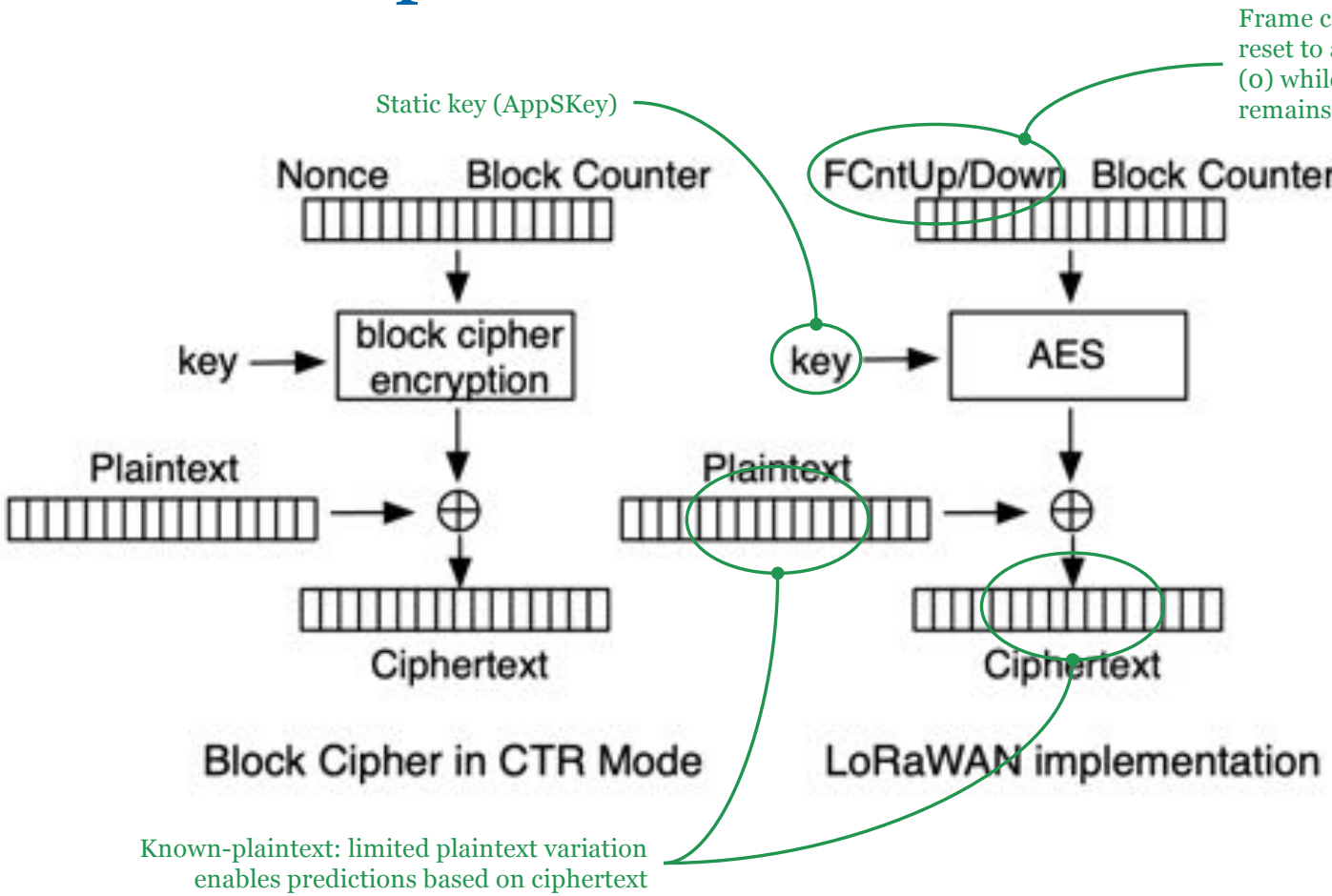


Fig. 4. An example of a replay attack for ABP.

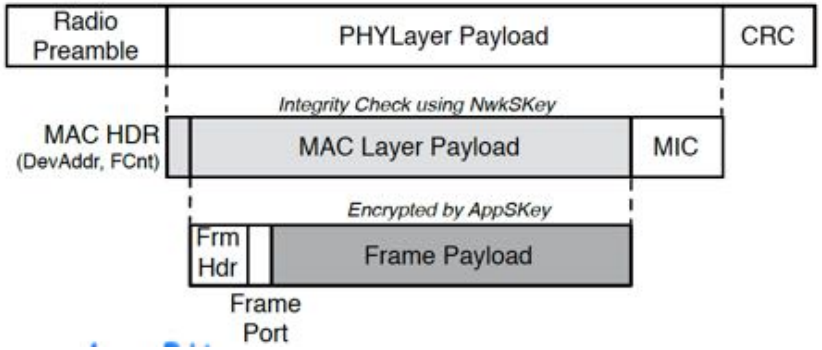
Discussion: known-plaintext attack

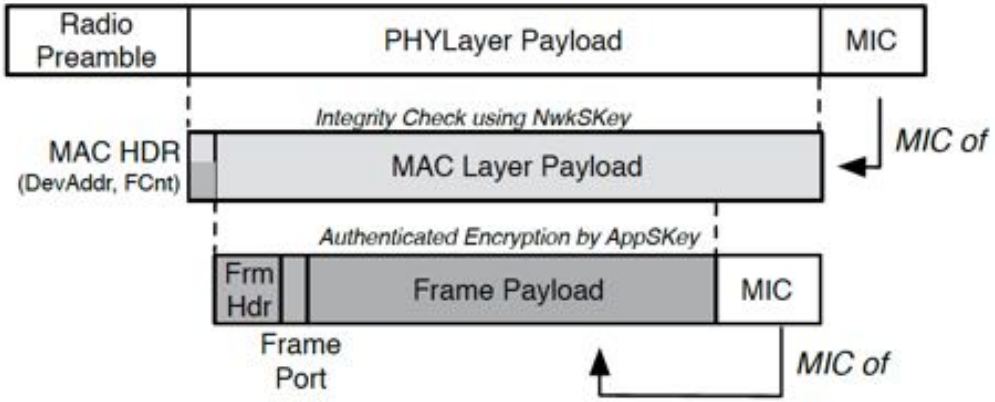


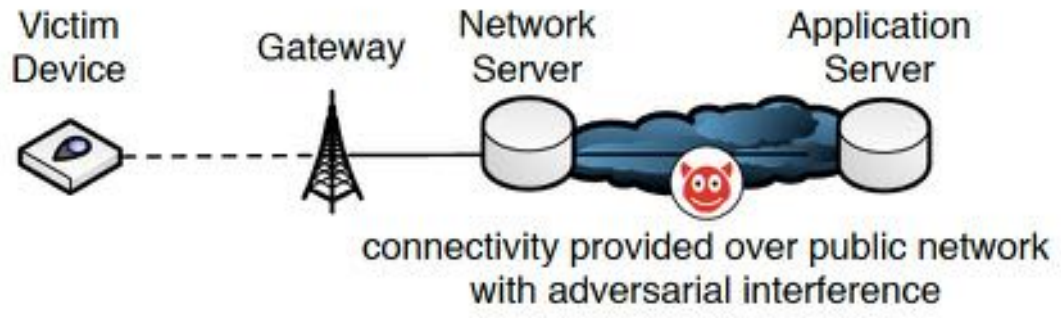
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
https://en.wikipedia.org/wiki/Known-plaintext_attack
https://en.wikipedia.org/wiki/Block_cipher

UNIVERSITY OF TWENTE.
SDN LABS

Discussion: proposed solution using 2 MICs



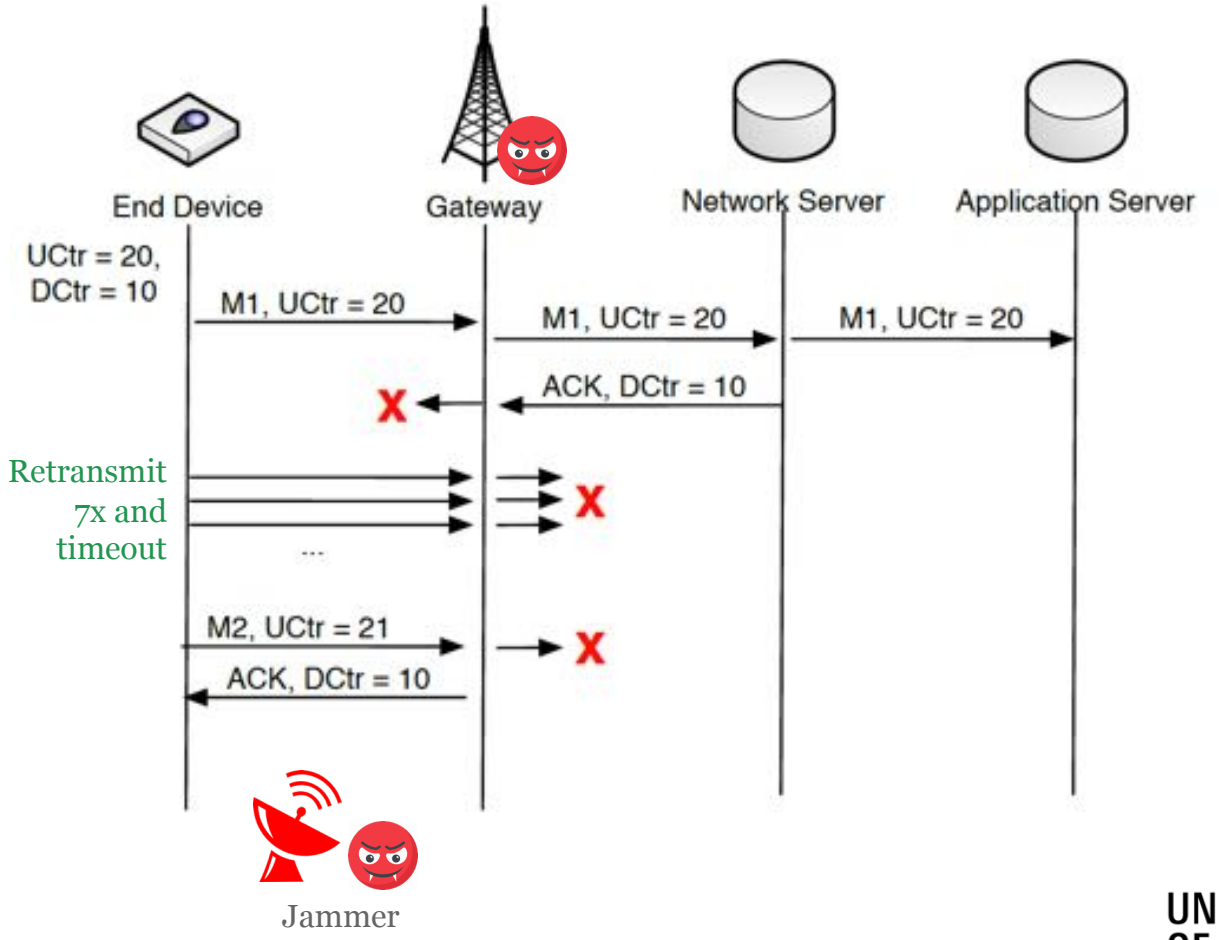




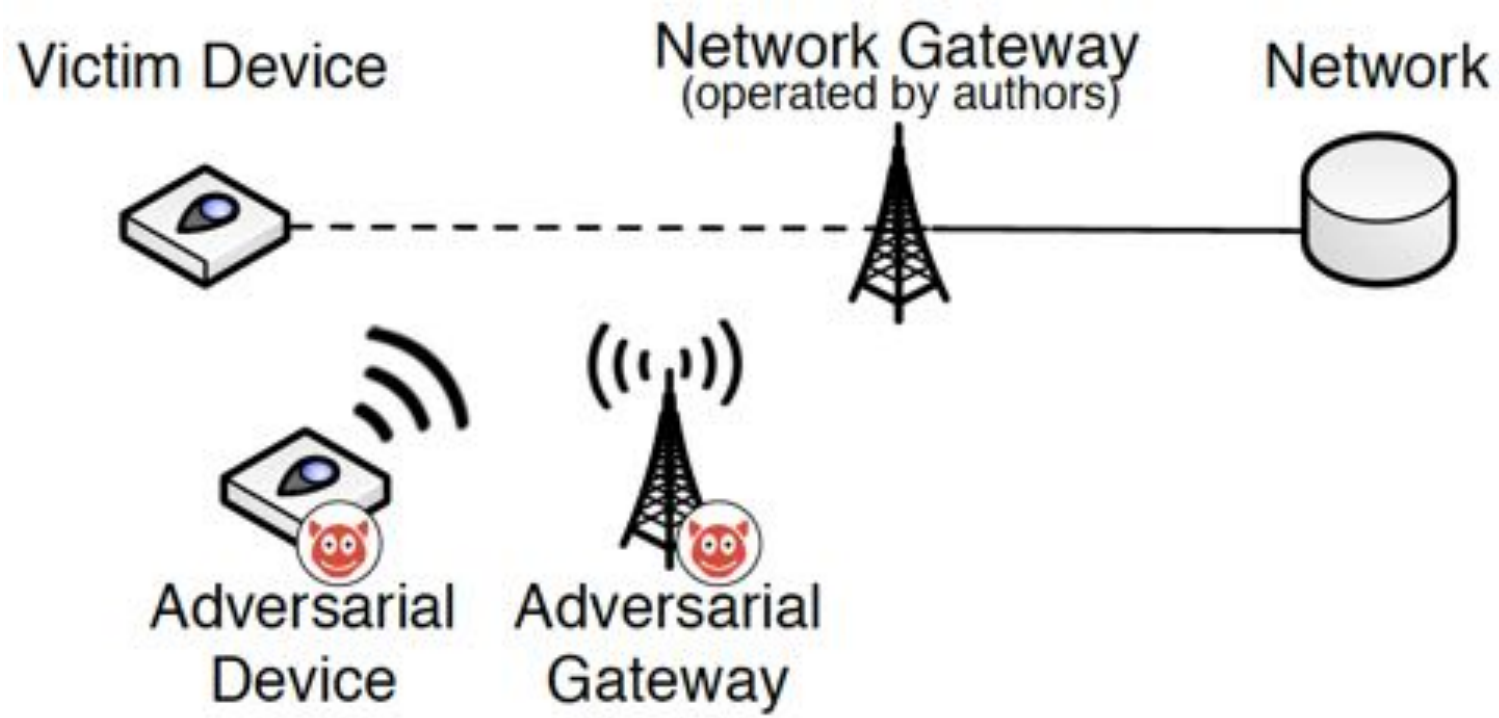
UNIVERSITY OF TWENTE.

SDN LABS

Discussion: ACK spoofing



Discussion: battery draining

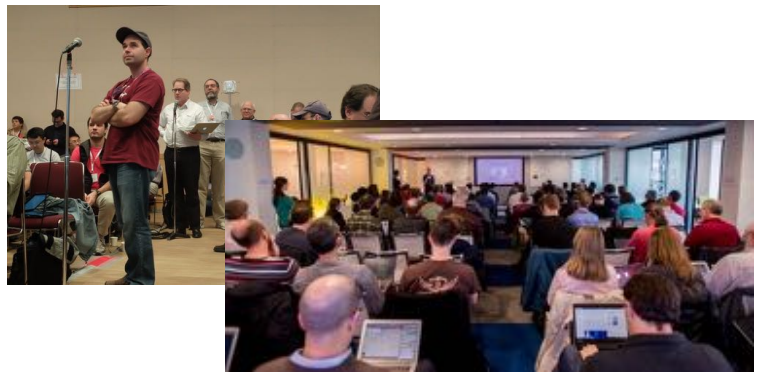


UNIVERSITY OF TWENTE.

SDN LABS

Key takeaways

- Designing network security protocols is challenging work
- Attacks can have a physical component, such as jamming or device resets
- Highlights the importance of an open protocol development process (cf. IETF)
- My “favorite”: remote battery draining



Discussion (if time permits)

- What would you do to better in the development process to make LoraWAN more secure?

Coffee break

UNIVERSITY OF TWENTE.

SDN LABS

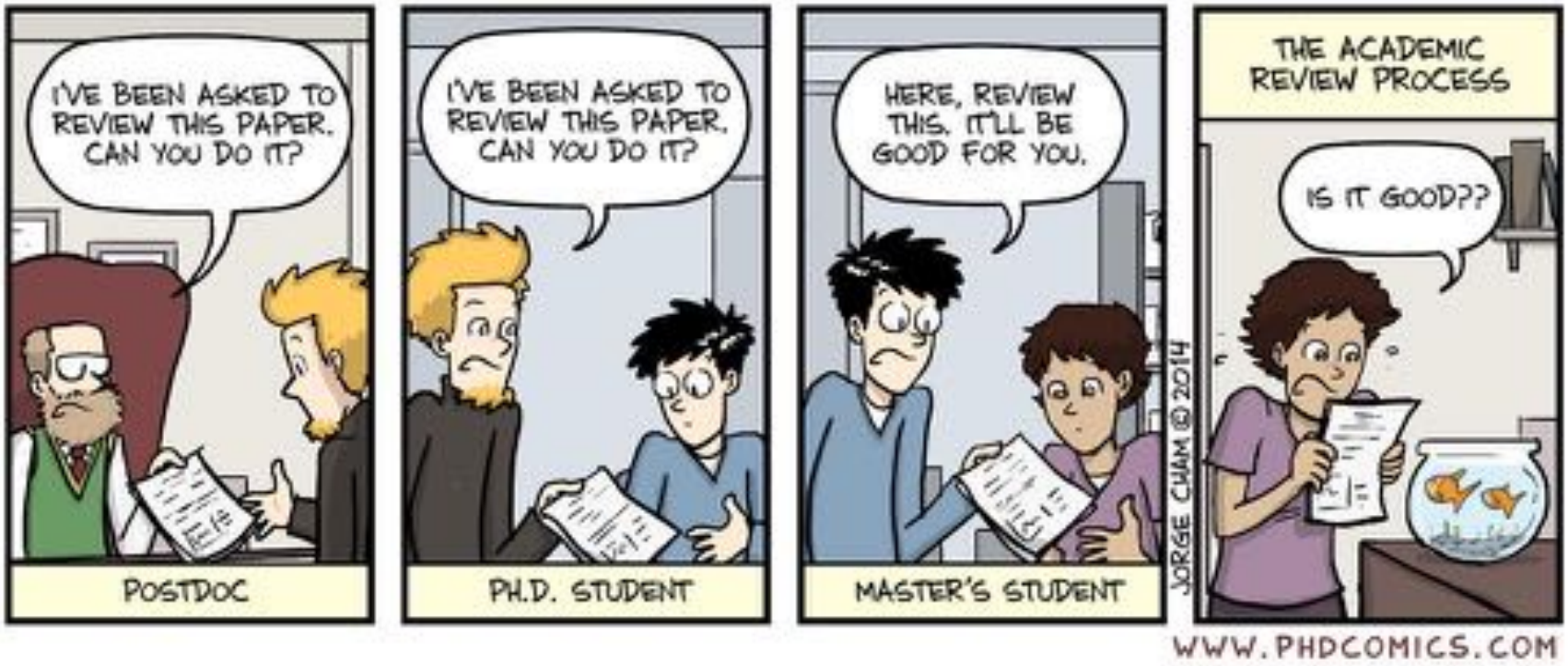
“Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control”

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

UNIVERSITY OF TWENTE.

SDN LABS

Your opinion



UNIVERSITY OF TWENTE.

SIDN 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

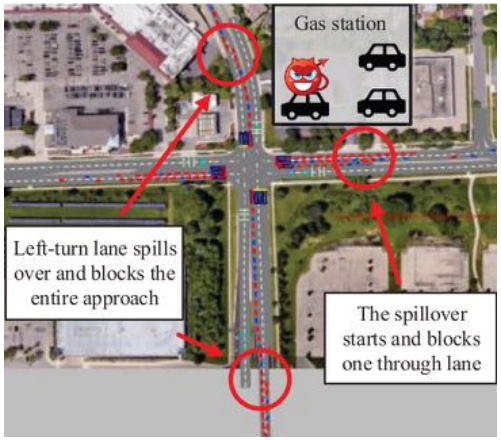
Google Maps Hacks by Simon Weckert.

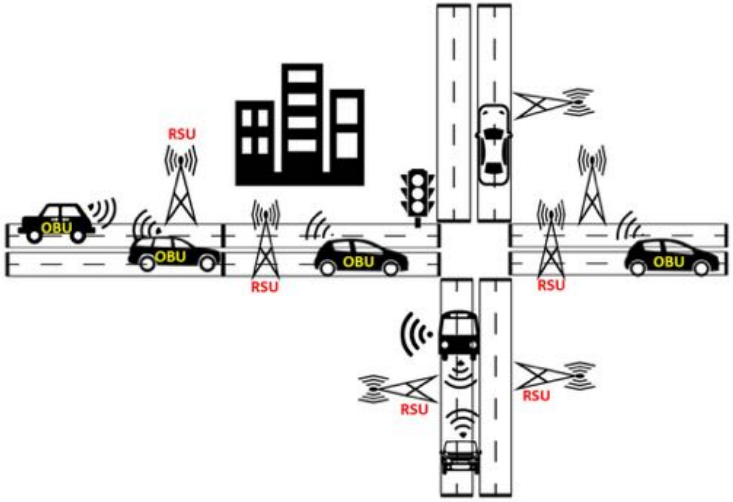
Source: https://www.theguardian.com/technology/2020/feb/03/berlin-artist-uses-99-phones-trick-google-maps-traffic-jam-alert

UNIVERSITY OF TWENTE. SDN LABS

Basic Safety Messages

"Safety applications center on the **basic safety message (BSM)**, a packet of data that contains information about **vehicle position, heading, speed, and other information relating to a vehicle's state and predicted path**." -ITS





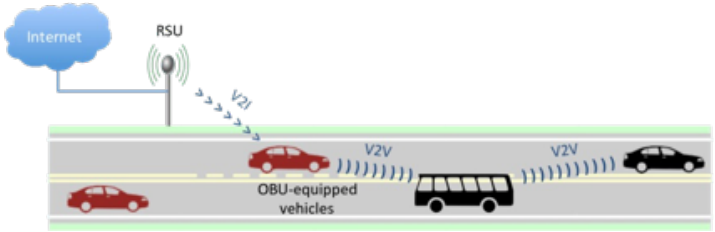
Source: H. Hasrouny et al., "VANet security challenges and solutions: A survey"

UNIVERSITY OF TWENTE. SDN LABS

Problem source

- **Hardware limitations:** Signal plan needs to be ready in a limited time

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

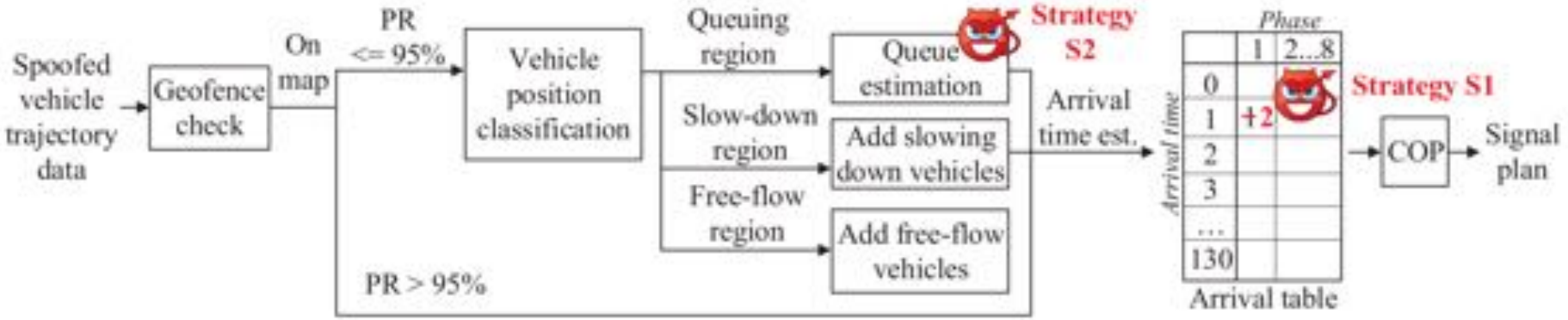


UNIVERSITY OF TWENTE.

SDN LABS

Spoofed data flow

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



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? (hint: GPS spoofing)

Attack vectors in VANET

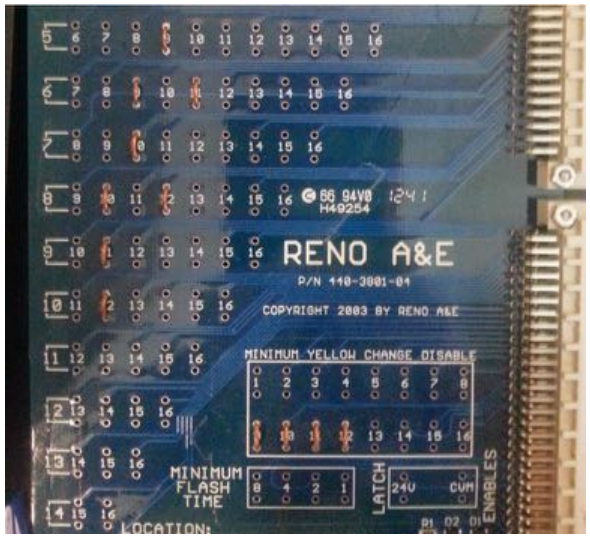
Table 2
Classification of Attacks based on four categories and VANET communication mode.

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"

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 at-tacks (e.g. four-way green lights) in addition to the attacks described in this paper." *
  - 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"

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

UNIVERSITY OF TWENTE. SIDN LABS

Attack effectiveness

- **Full deployment:**

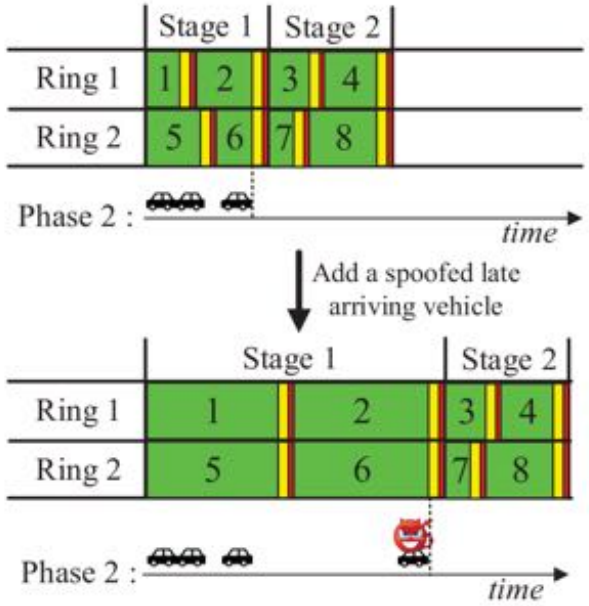
  2 stage: last vehicle advantage

  5 stage: open skipped phase + extend green light

- **Transition period**

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

  5 stage: open skipped phase + extend green light



Last vehicle advantage

- How is this exactly done?
- What is transmitted in the spoofed BSM?

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?

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, they spare 1 sec for BSM transition delay, etc.)

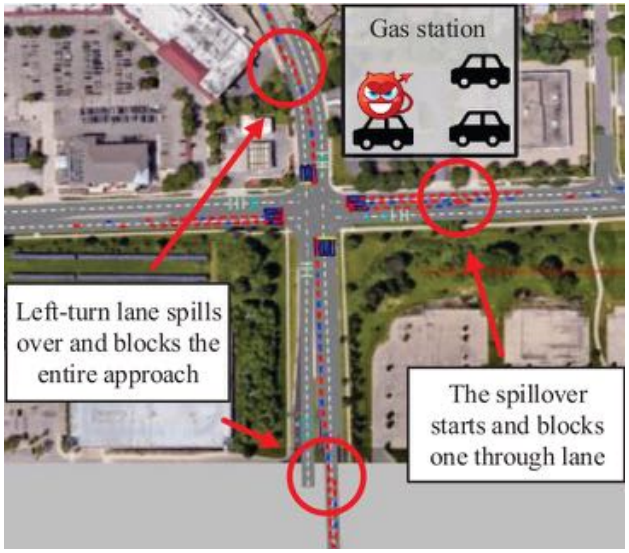
Attack evaluation

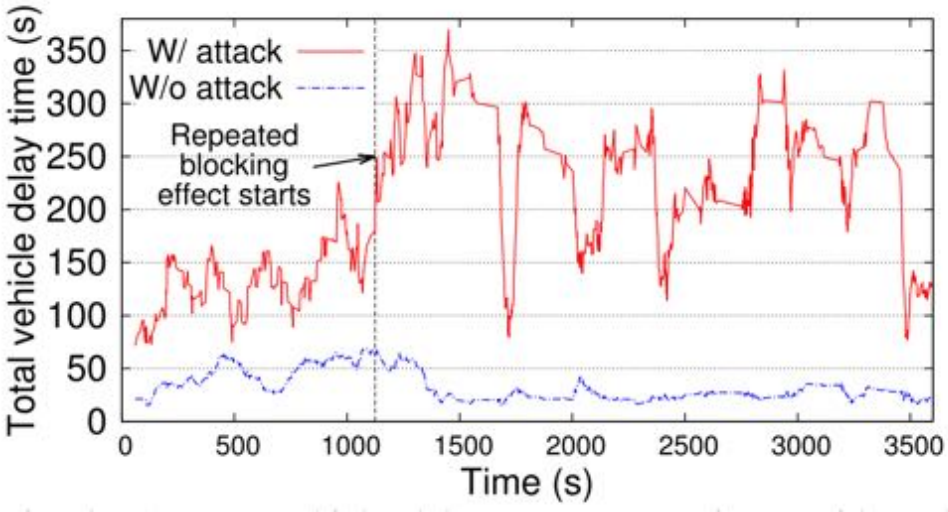
E1: Congestion attack for two-stage planning
E2: Congestion attack for five-stage planning in the full deployment period (lower performance than vulnerability analysis)
E3: Congestion attack for five-stage planning in the transition period (higher performance than vulnerability analysis)

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





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)
- …

Lessons Learned

- 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
  - Measurement techniques to detect ICS systems that are connected to the Internet but shouldn't

- 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: **Wed Jun 22 (resit), 10:45-12:30**
Topic: IoT honeypots
Note: we'll be back in VR 583

UNIVERSITY OF TWENTE.

SIDN LABS