Lecture #8: IoT Network Security

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

University of Twente | June 10, 2020

UNIVERSITY OF TWENTE.

SIDN LABS

Paper summaries

- You must have handed in your two summaries BEFORE this lecture
- You can use the summaries during the oral exam (“open book”)
- You **cannot** complete SSI without submitting 12 paper summaries!
- If you have done 12, you don’t need to provide summaries next week (but do attend the lecture :-)

UNIVERSITY OF TWENTE.

SIDN LABS

Interactive Lecture

- Goal: enable you to learn from each other and further increase your understanding of the papers (contributes to preparing yourself for the oral exam)

- Format:
  1. We'll ask someone to provide their **opinion** of the paper
  2. Summary by teachers (put any questions in the chat)
  3. Questions: discussion starters and fact questions
  4. Discussion (use your mic)
  5. We may ask someone specific to start the discussion

- Experimental format resulting from Corona pandemic, please provide feedback!

UNIVERSITY OF TWENTE. SIDN LABS

Today's papers: IoT network security

[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

[PHY] S. Naz Islam, Z. Baig, and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures", IEEE Transactions on Industrial Informatics, Vol. 15, Issue 12, Dec. 2019

“Security Vulnerabilities in LoRaWAN”, April 2018

X. Wang, E. Karampatzakis, C. Doerr, and F.A. Kuipers

UNIVERSITY OF TWENTE.

SIDN LABS

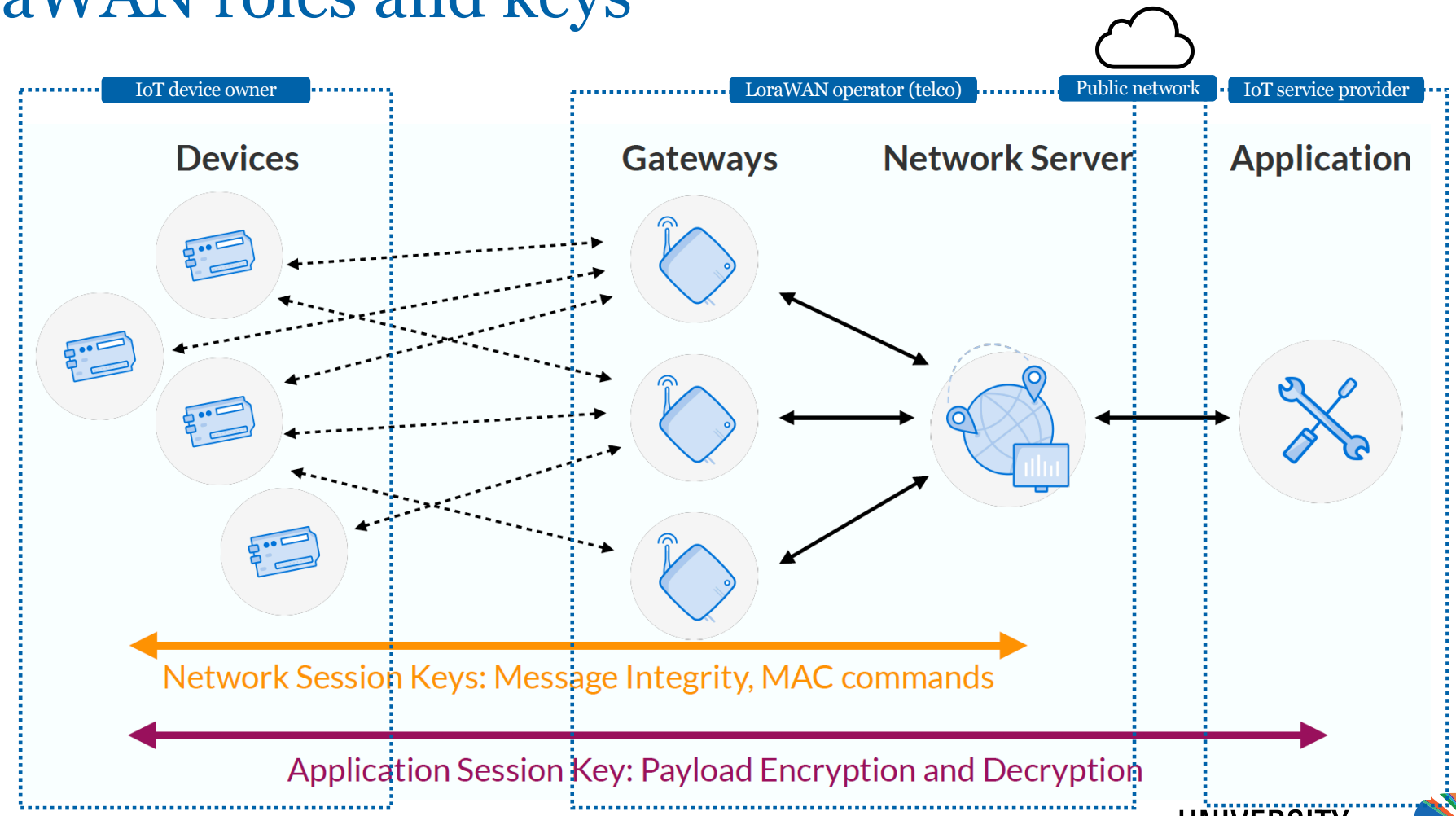
Quiz: warming up

What classical definition of security does the paper use?

A. Communication, Information, and Authority
B. Confidentiality, Integrity, and Availability
C. Authentication, Authorization, and Accounting
D. Stability, Resilience, and Transparency

UNIVERSITY OF TWENTE.

LoraWAN roles and keys



Picture: Johan Stokking, The Thing Industries

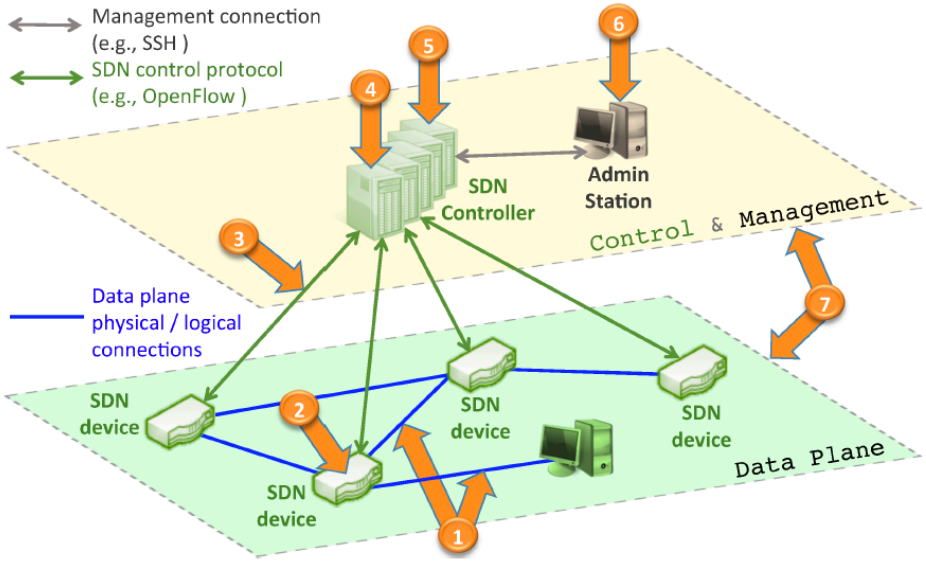
UNIVERSITY OF TWENTE.

SDN LABS

Key security functions

- Data plane (packet forwarding)
  - Encryption (counters)
  - Authentication of LoraWAN sources (MIC)
  - Message integrity verification (MIC)
  - Replay protection (counters)

- Management plane
  - Key derivation (symmetric)
  - Device enrollment protocol (OTAA and ABP)
  - Over the air firmware updates (guest lecture)



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

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: over-the-air activation

What's the root of trust in OTAA mode?

A. AppSKey

B. NwkSKey

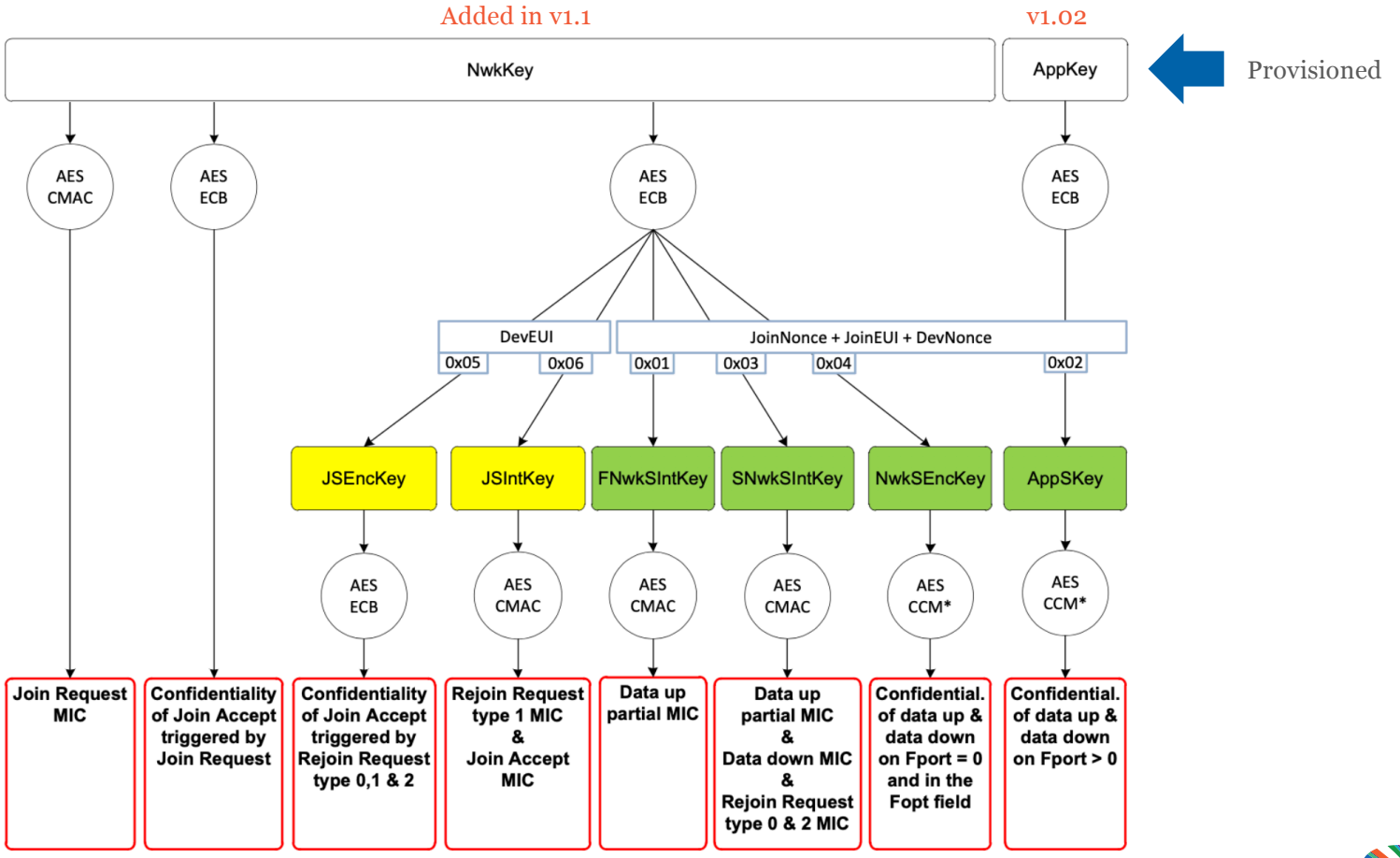
C. AppKey

D. NwkKey

UNIVERSITY OF TWENTE.

SIDN LABS

LoraWAN key derivation



Picture: Johan Stokking, The Thing Industries

UNIVERSITY OF TWENTE.

SDN LABS

Denial of Service through replay

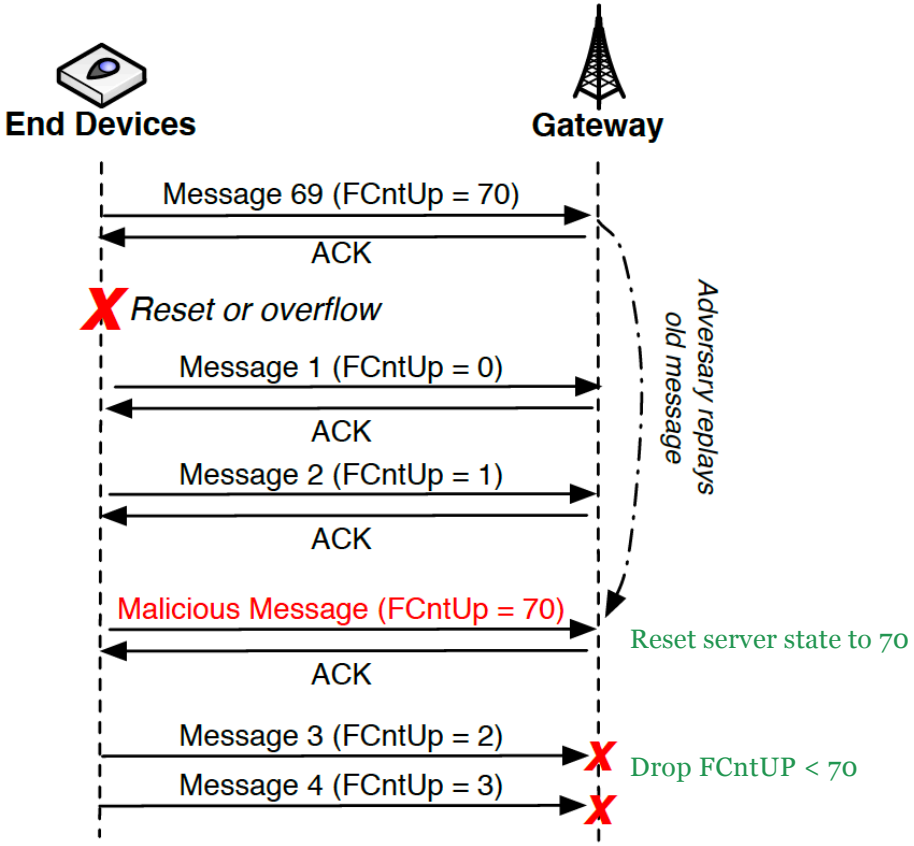


Fig. 4. An example of a replay attack for ABP.

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: eavesdropping

What's the root cause of an eavesdropping attack?

A. LoraWAN nodes use their message counters to encrypt messages
B. LoraWAN nodes use limited payload sizes
C. LoraWAN nodes use known formats for their messages
D. LoraWAN nodes use a block cipher in counter mode

Quiz: eavesdropping

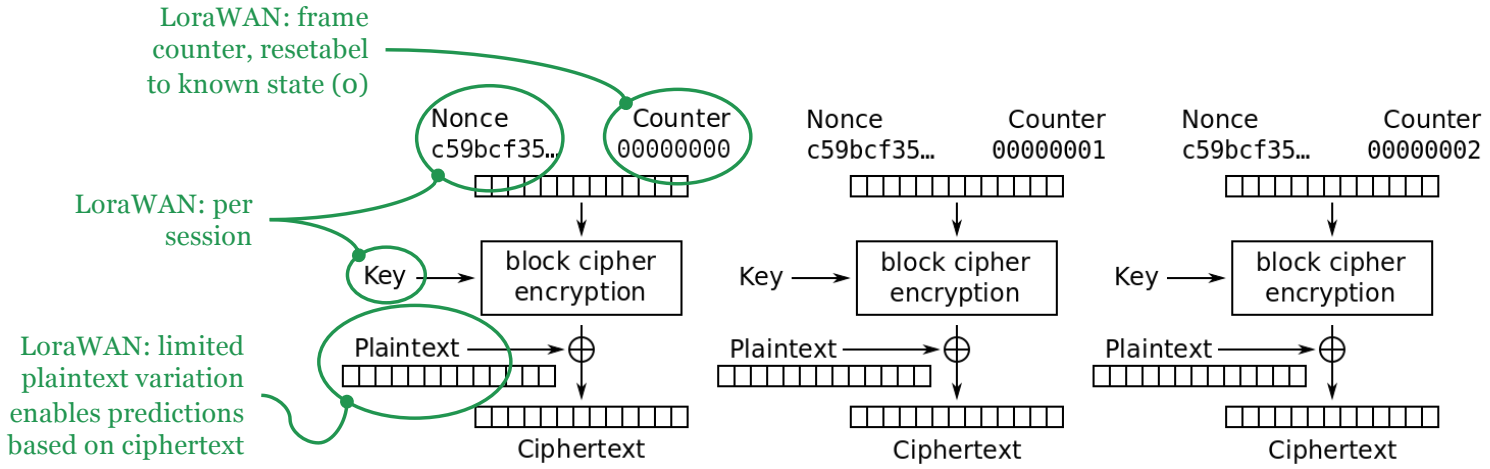
What's the root cause of an eavesdropping attack?

A. LoraWAN nodes use their message counters to encrypt messages

B. LoraWAN nodes use limited payload sizes

C. LoraWAN nodes use known formats for their messages

D. LoraWAN nodes use a block cipher in counter mode



Counter (CTR) mode encryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

UNIVERSITY OF TWENTE.

SDN LABS

Quiz: message integrity

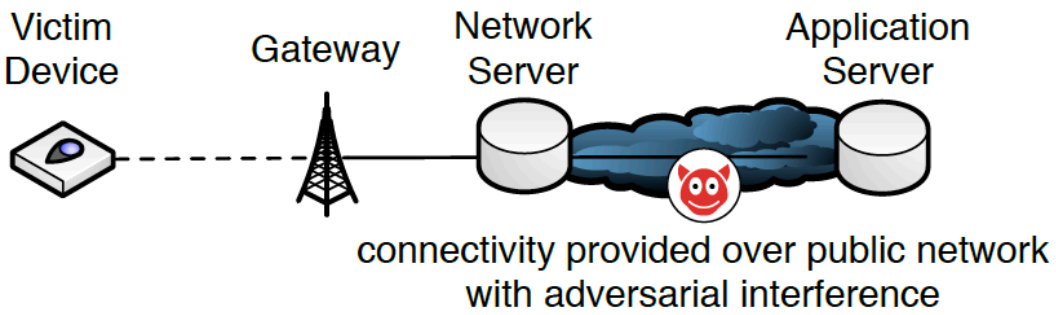
Why does LoraWAN not support end-to-end message integrity?

A. LoraWAN is a link-level technology

B. LoraWAN messages are encrypted

C. LoraWAN do not have an application-level MIC

D. LoraWAN messages can be subject to a routing hijack

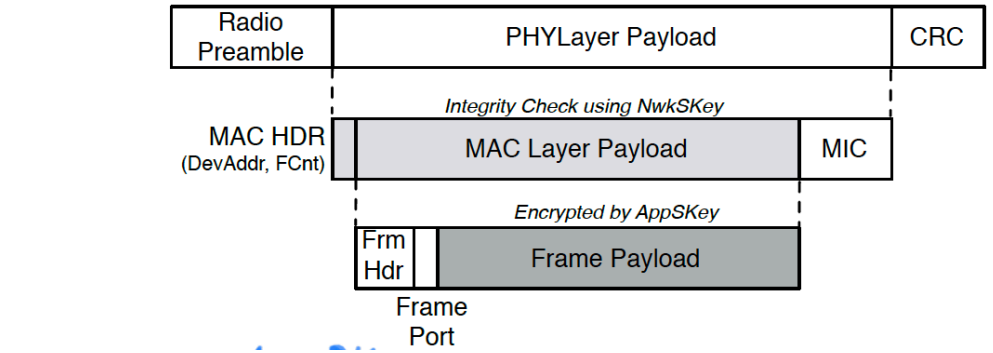


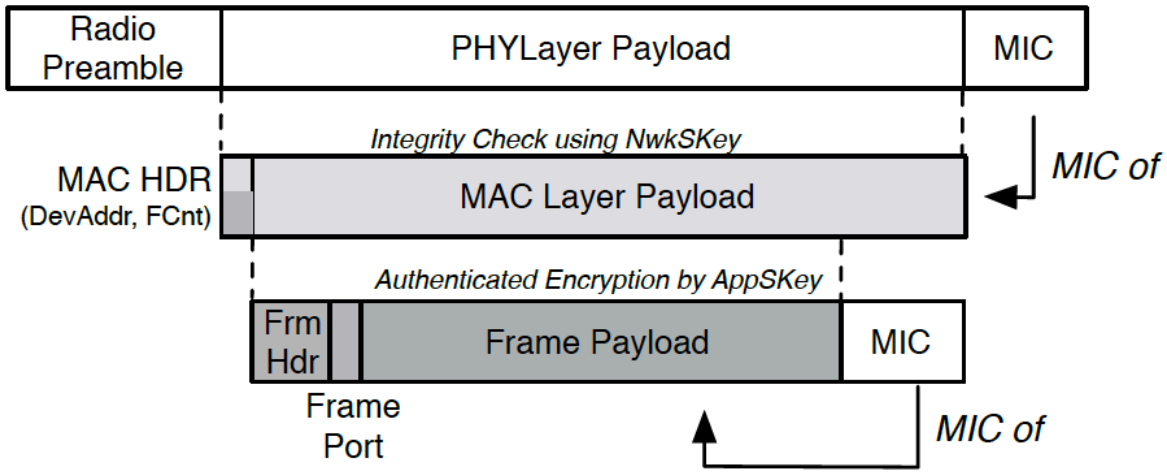
UNIVERSITY OF TWENTE.

SDN LABS

Proposed solution: 2 MICs

Why would they have not used an application-level MIC initially?

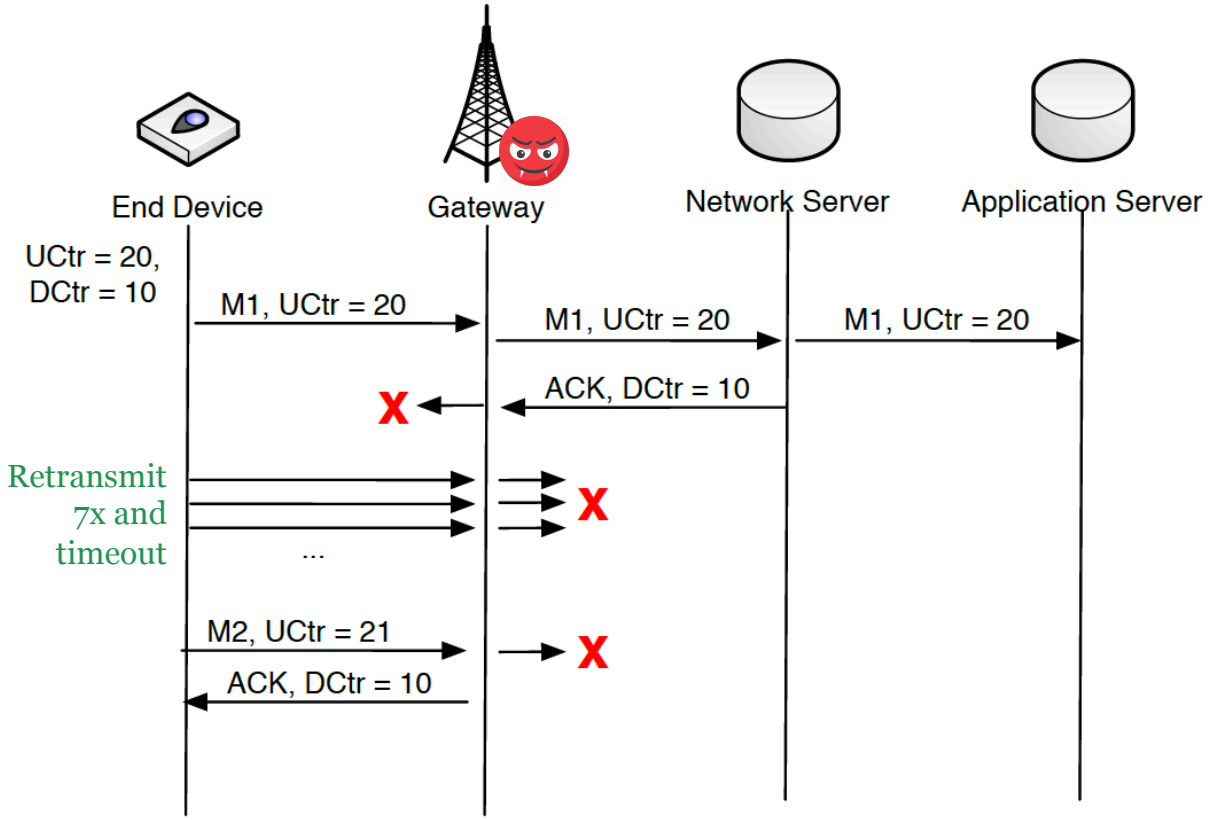




VERSITY OF TWENTE.

SDN LABS

ACK spoofing



UNIVERSITY OF TWENTE.

SDN LABS

Quiz: ACK spoofing

The fundamental problem with the ACK spoofing attack is that ACKs do not indicate which message they confirm. How do the authors propose to extend ACK messages to tackle this problem?

A. Include a nonce signed by the gateway's private key

B. Include the frame counter value of the uplink message

C. Include cryptographic checksum that covers the uplink packet

D. Accept the risk because adding more info to ACKs would be too expensive

Key takeaways

- Designing network security protocols is challenging
- Many different corner cases that folks will exploit
- My “favorite” attacks
  - Content guessing based on typical packet content (small messages, known data formats, etc.)
  - Remote battery draining

UNIVERSITY OF TWENTE. SIDN LABS

Discussion

- What would you do to better in the development process to make LoraWAN more secure?
  - IETF-like standardization?
  - Formal verification?
  - Open source implementation?
  - …

UNIVERSITY OF TWENTE. SIDN LABS

Physical Layer Security for the Smart Grid:

Vulnerabilities, Threats, and Countermeasures

UNIVERSITY OF TWENTE.

SDN LABS

Opening question: This paper was easy to understand

- True
- False

UNIVERSITY OF TWENTE.

SDN LABS

Cont.: Some of the proposed solutions were too obvious (ie. use encryption)

- True
- False

UNIVERSITY OF TWENTE.

SDN LABS

Motivation

- Smart energy grids are made up of two broad components
  - The traditional electricity grid
  - Data communication layer
- Up until now, only specific vulnerabilitie were investigated
  - Moreover, the physical layer threats were n considered

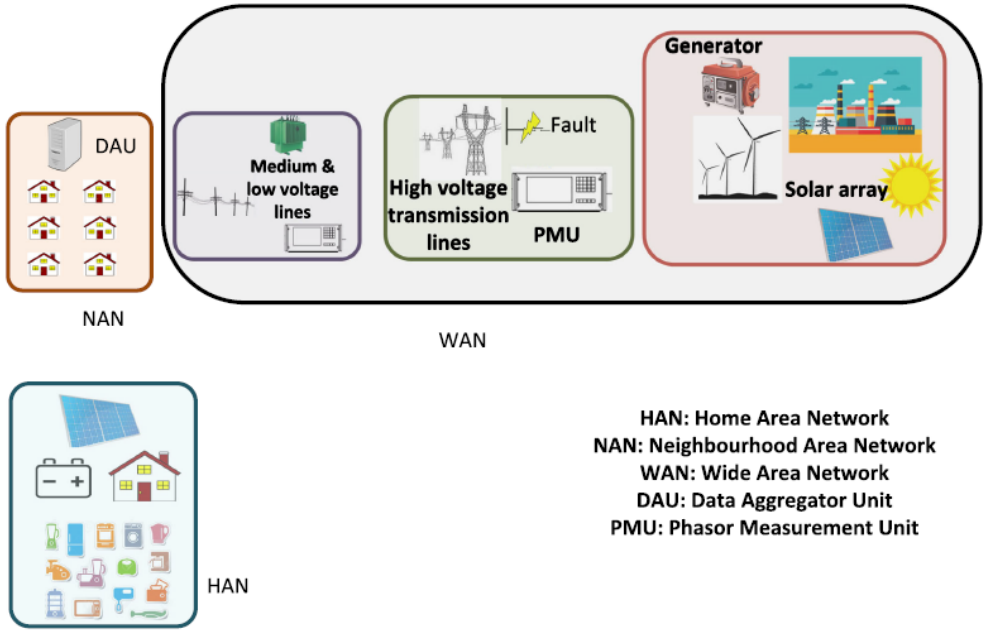
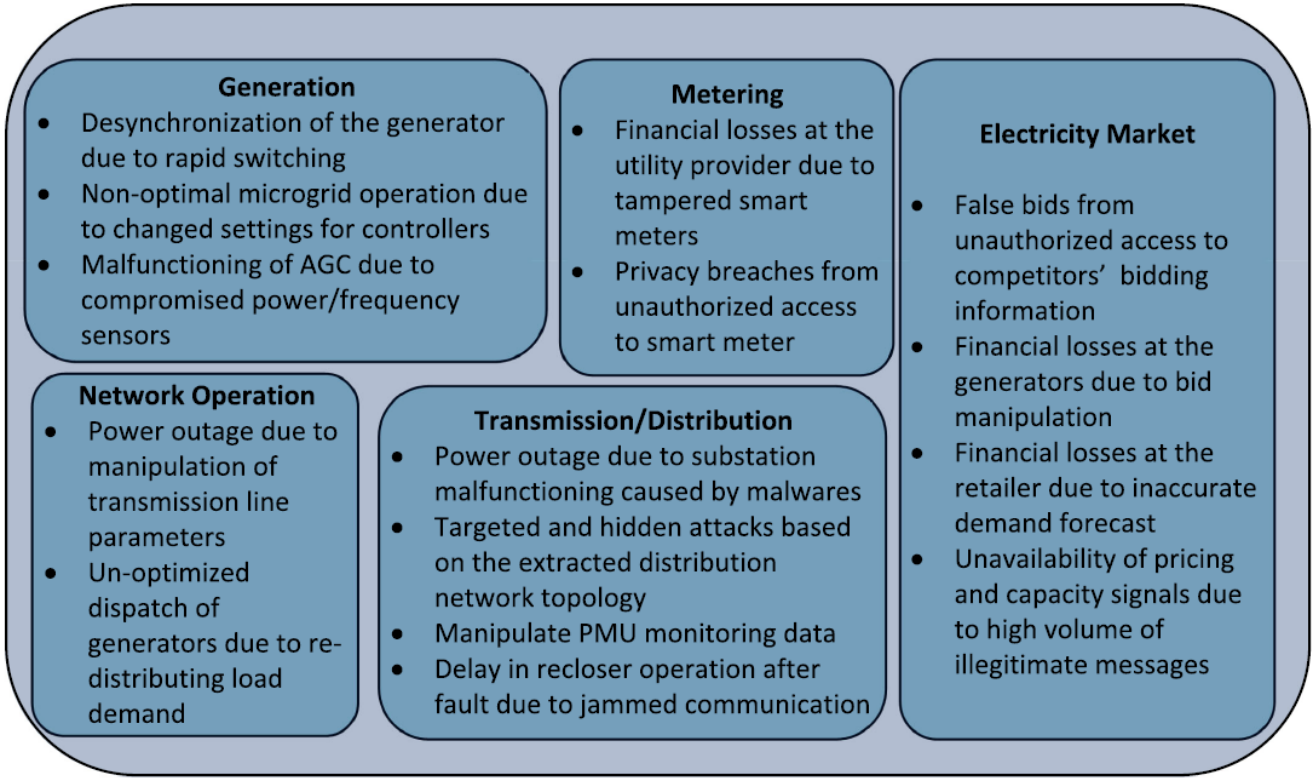


Fig. 1. Smart energy system.

UNIVERSITY OF TWENTE.

SDN LABS

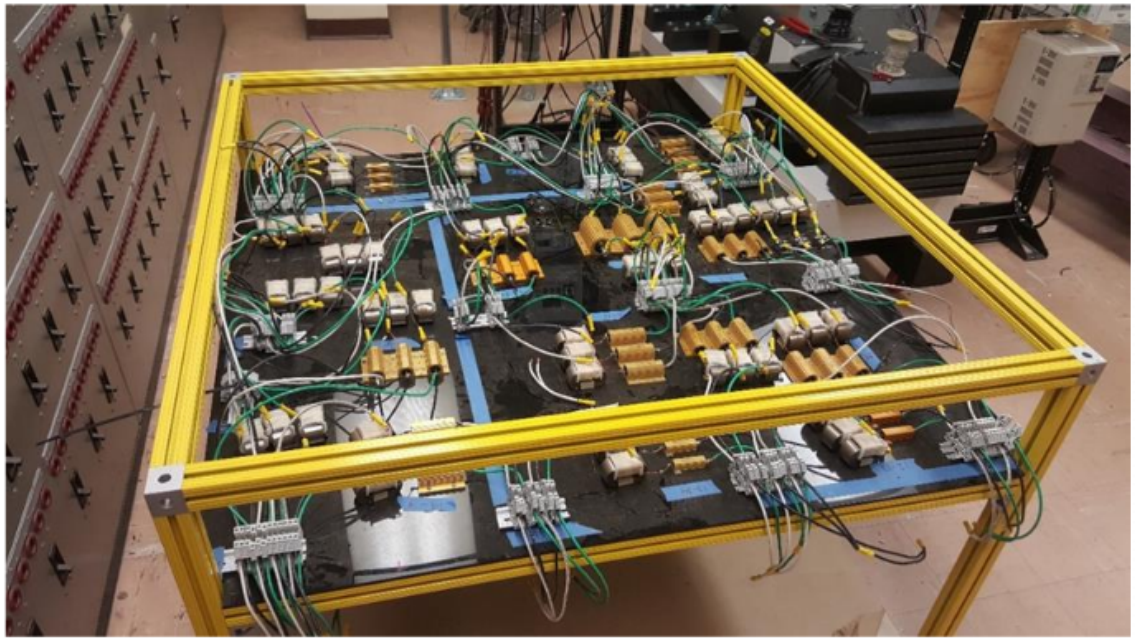
SECURITY VULNERABILITIES OF SMART ENERGY SYSTEMS

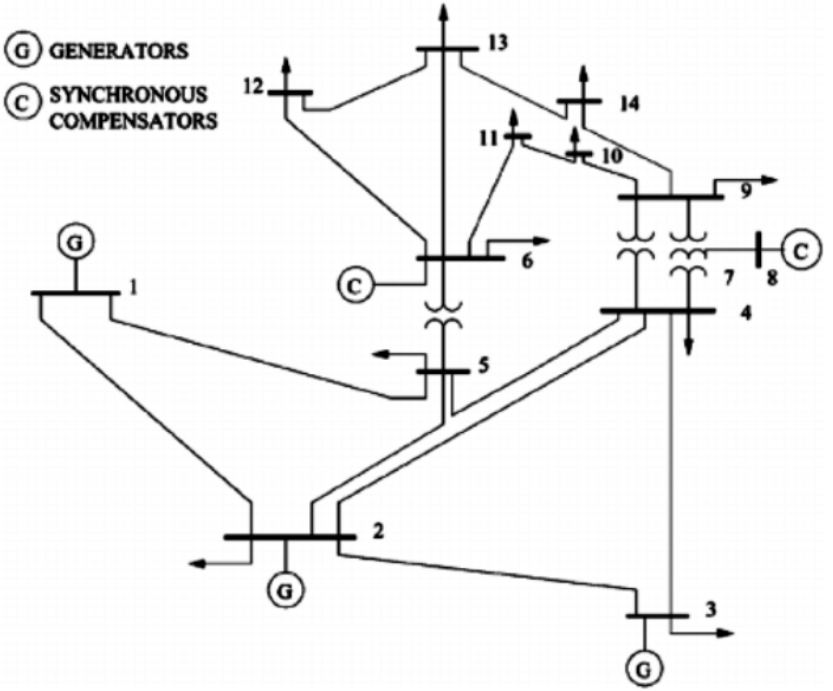


UNIVERSITY OF TWENTE.

SDN LABS

IEEE 14 Bus Power System

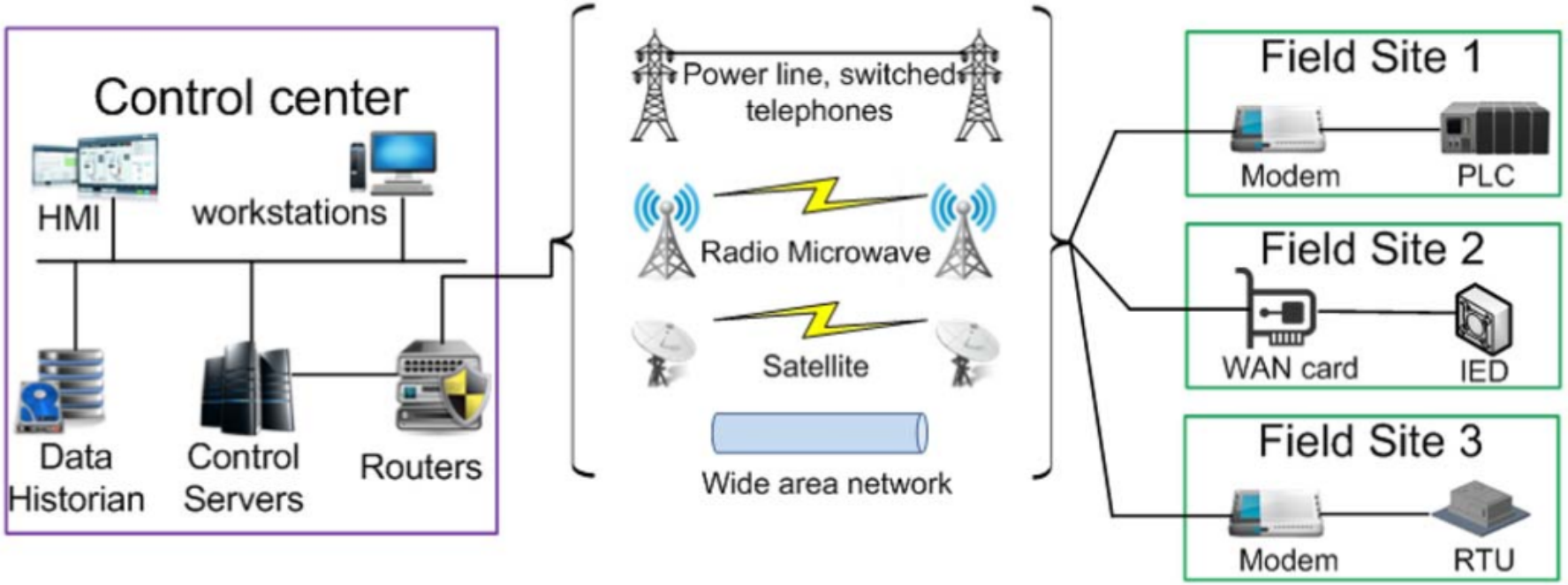




UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems



UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

- IoT-enabled smart grids connect various smart grid components, including smart meters, controllers, DAUs, PMUs, PDCs, and fault isolators over the Internet, to enable ubiquitous connectivity.
- As a result, these IoT-enabled smart grid devices and corresponding communication links expose an increasing number of vulnerabilities.

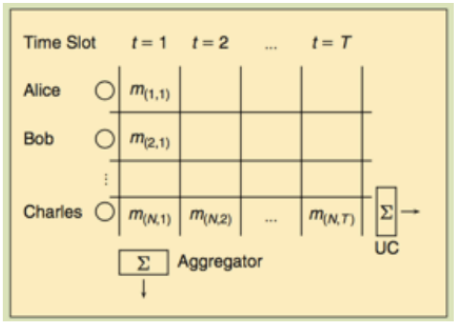
UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

Data Aggregation

public ← $M = \sum_{i=1}^{N} m_i$ → private



- Setting:
  - Service provider
  - Aggregator(s) (*optional)
  - Customers: e.g. households
- Questions: Can we compute aggregated data without learning individual consumption?
  - Spatial?
  - Temporal?
  - Missing data?
  - in different security models

TU Delft

UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

Homomorphic Encryption

$$E_{pk}(m_1) \otimes E_{pk}(m_2) = E_{pk}(m_1 \oplus m_2)$$

Encrypted/Ciphertext Domain

Plaintext Domain

TU Delft

UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

Paillier Encryption Scheme

- Additively Homomorphic
- Another one, Okamoto-Uchiyama

$$n = pq \qquad g^n \equiv 1 \bmod n^2 \qquad r \in \mathbb{Z}_n^*$$

$$\lambda = lcm(p-1, q-1) \qquad L(x) = \frac{x-1}{n}$$

$$E_{pk}(m) = g^m r^n \bmod n^2$$

$$D_{sk}(c) = \frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n$$

UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

Additive Homomorphism

$$
\begin{aligned}
E_{pk}(3, r_1) \times E_{pk}(5, r_2) &= g^3 \cdot r_1^n \times g^5 \cdot r_2^n \bmod n^2 \\
&= g^{3+5} \cdot (r_1 \cdot r_2)^n \bmod n^2 \\
&= E_{pk}(3+5, r_1 r_2)
\end{aligned}
$$

TU Delft

UNIVERSITY OF TWENTE.

SDN LABS

Physical Layer Security For Smart Energy Systems

ET12: Modified Paillier Encryption

$$\text{Alice: } \mathcal{F}_{pk}(m_{1,t}) = g^{m_{1,t}} \cdot r^{n_1} \bmod n^2,$$
$$\text{Bob: } \mathcal{F}_{pk}(m_{2,t}) = g^{m_{2,t}} \cdot r^{n_2} \bmod n^2,$$
$$\text{Charles: } \mathcal{F}_{pk}(m_{3,t}) = g^{m_{3,t}} \cdot r^{n_3} \bmod n^2,$$

$$n_1 + n_2 + n_3 = n$$

$$\prod_i \mathcal{F}_{pk}(m_i) = g^{\sum_i m_{i,t}} \cdot r^{\sum_i n_i} \bmod n^2$$
$$= g^{\sum_i m_{i,t}} \cdot r^n \bmod n^2 := \mathcal{E}_{pk}\left(\sum_i m_{i,t}\right).$$

- In practice, you need time-stamps
- Cryptographic tools: Paillier, Hash, PRF
- Cannot deal with missing data (external party needed)

UNIVERSITY OF TWENTE.

SDN LABS

Discussion

- What do you think?

- (Completely open discussion)

UNIVERSITY OF TWENTE.

SDN LABS

Volg ons


SIDN.nl


@SIDN


SIDN

Discussion & feedback

Next lecture: **Wed Jun 17, 10:45-12:30**
Topic: IoT edge security systems (re-sit)
Everyone welcome to attend!

UNIVERSITY OF TWENTE.

SIDN LABS