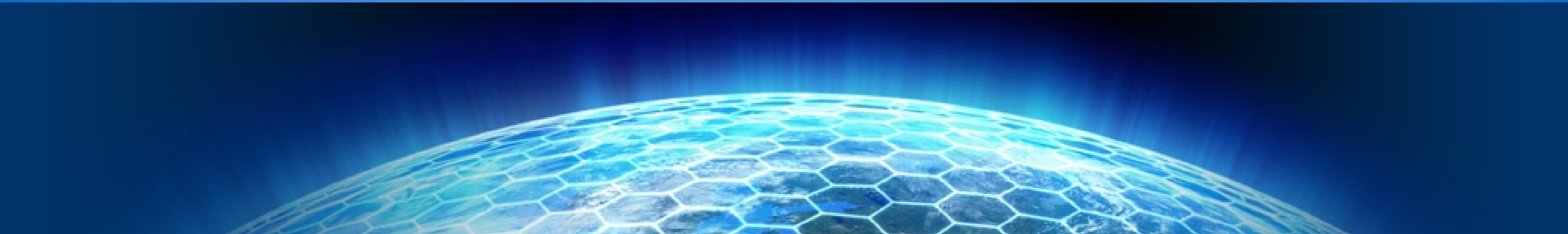
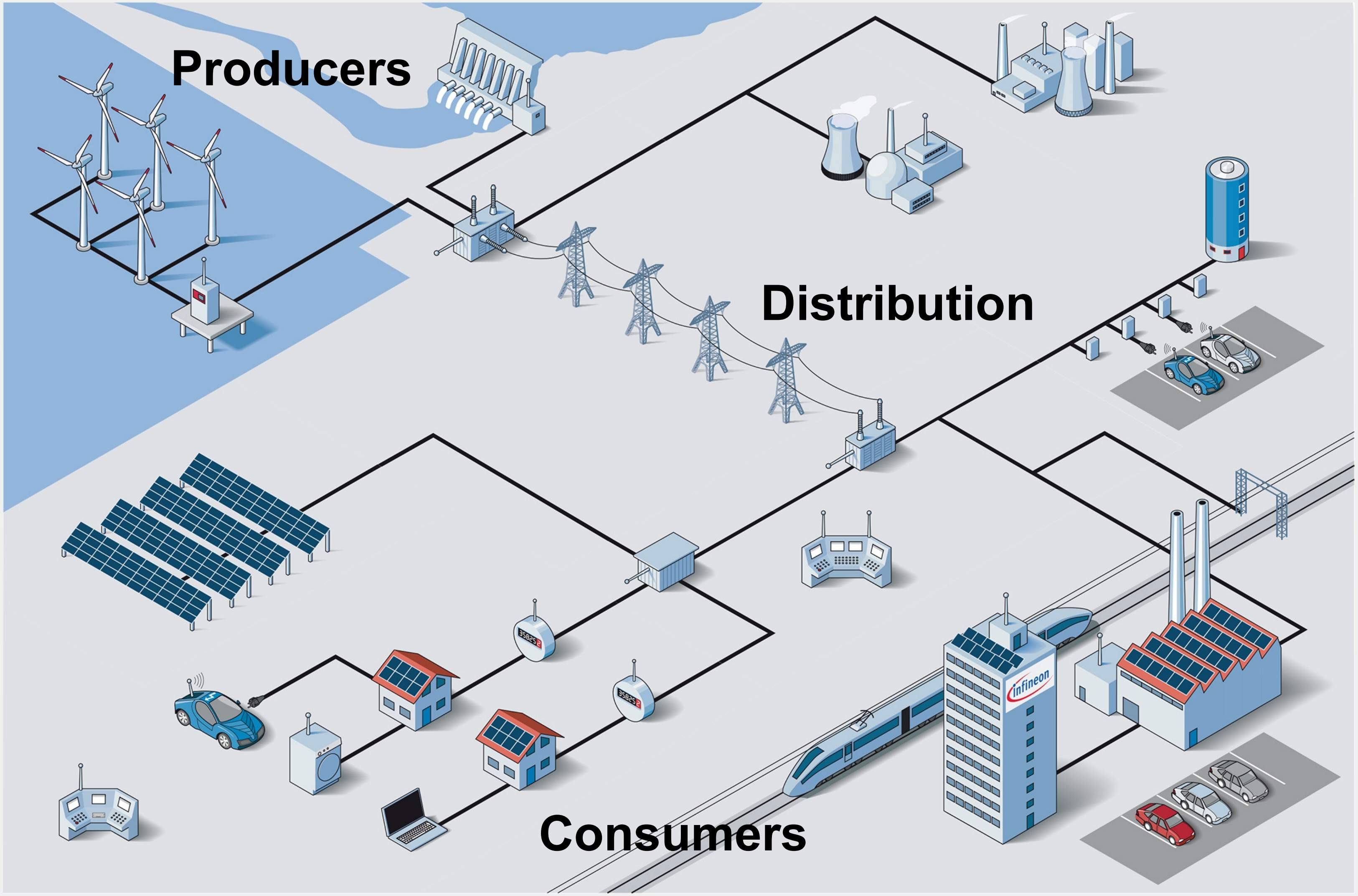
ICT Support for Adaptiveness and (Cyber)security in the Smart Grid (DAT300) 2014

Challenges for IT-Security in Smart Grids

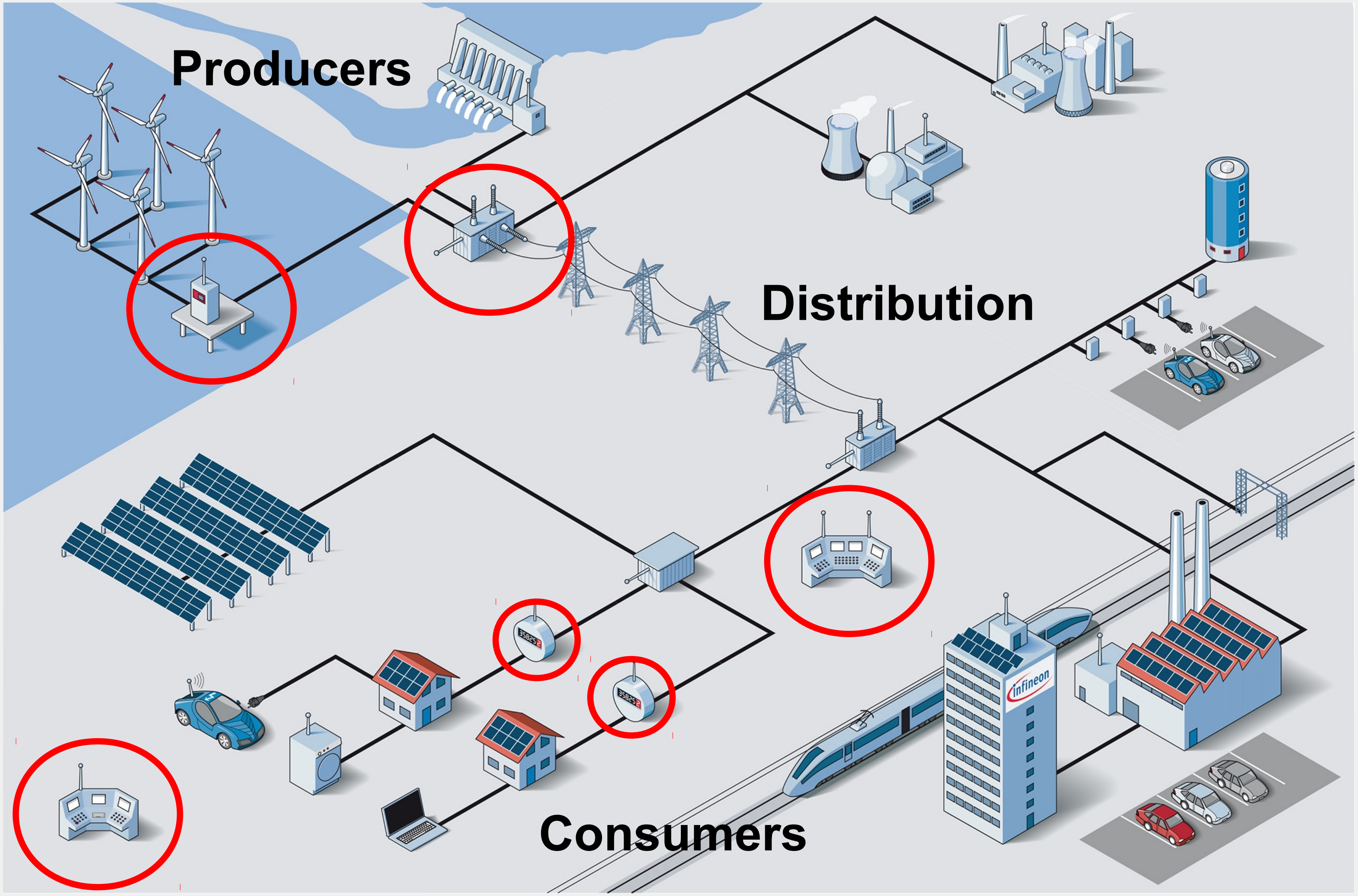
Daniel Hausknecht



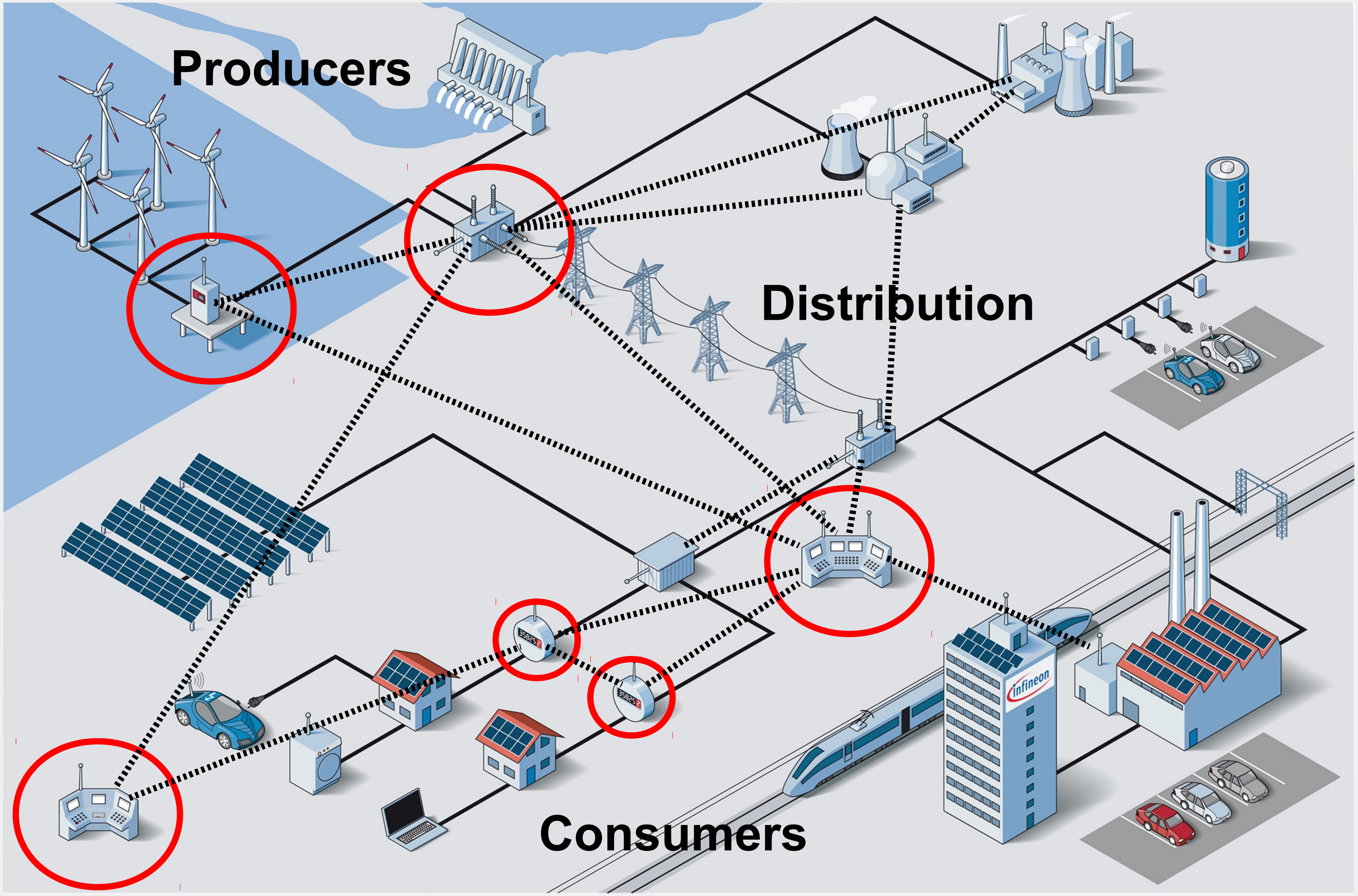
The Smart Grid



The Smart Grid



The Smart Grid



The Communication in the Smart Grid

DNP3:

- Developed 1993 out of need
- No security measurements

IEC 61850:

- ”Defines the communication between IEDs in the substation and the related system requirements”
- Security in separate *IEC 62351* (work in progress)

Internet vs. Smart Grid

	Internet	**Smart Grid**
Performance metric:	Throughput, fairness	Reliable, real-time
Traffic model:	Self-similarity, “power-law”	periodic
Timing requirement:	Delay: 100ms - secs	Delay: 3ms - mins
Communication model:	Client-server, peer-to-peer	Top-down, bottom-up
Protocol stack:	IPv4 / IPv6	IPv6, heterogeneous

Outline

1. **Smart Grid Overview**
2. **Security Objectives**
    a. Availability
    b. Confidentiality
    c. Integrity
3. **Recent Exemplary Approach**

Availability

"A wizard is never late,
he arrives precisely when he means to!"

- Accessability within a reasonable amount of time
- Attacks:
  - Denial of Service (DoS) attacks
  - In Smart Grids: message delaying

Availability

- Frequency hopping
- Firewalls
- Intrusion Detection Systems (IDS)
- Authentication
- Network topology (e.g. alternative paths)

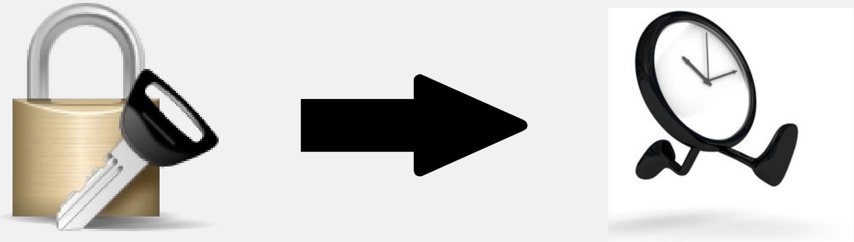
Confidentiality

Preserving restrictions on information access

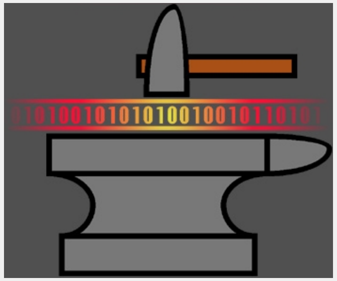
Attack: eavesdropping, e.g., account number

Countermeasure: encryption

- Shared key (symetric)
- Public key (asymetric)



Integrity

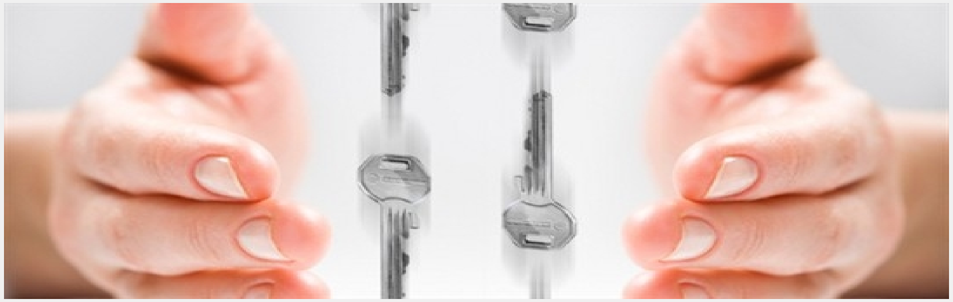


Preservation of data or system

Attacks: message forging/spoofing, device takeover

Countermeasures:

- Detection of misbehaviour → IDS
- Message authentication → key management



Exemplary Recent Approach

”Smart Grid Mesh Network Security Using Dynamic Key Distribution With Merkle Tree 4-Way Handshaking”

(B. Hu et al., IEEE Trans. Smart Grid 5(2): 550-558 (2014))

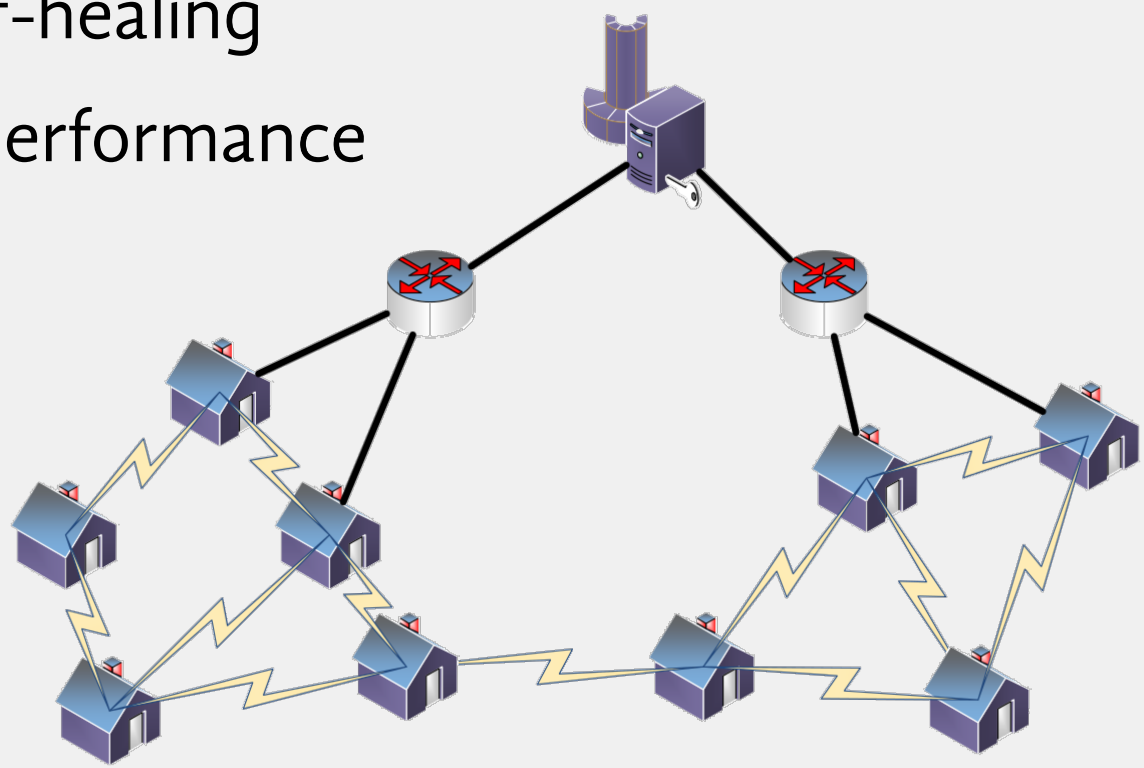
1. *The Network Setting*
2. *Dynamic Key Disribution*
3. *Evaluation*

The Network Setting

Multigate communication network [1)]

- Resilienct, self-healing
- Throughput performance

→ availability



1) H. Gharavi et al: Multigate Communication Network for Smart Grid. Proceedings of the IEEE 99(6), 2011

Dynamic Key Distribution [1)]

Problem of static key management:

- What if key is disclosed / cracked?
- How long does it take to detect it and to fix it?

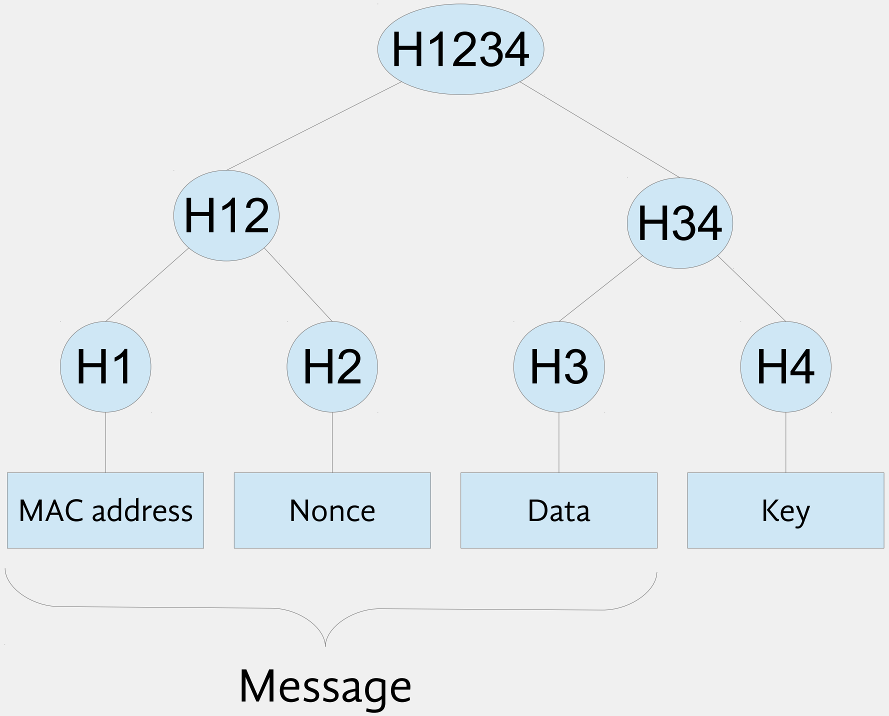
Dynamic Key Distribution:

- Frequent key updates reduce time for exploits

1) H. Gharavi et al: Dynamic key refreshment for smart grid mesh network security. ISGT 2013: 1-6

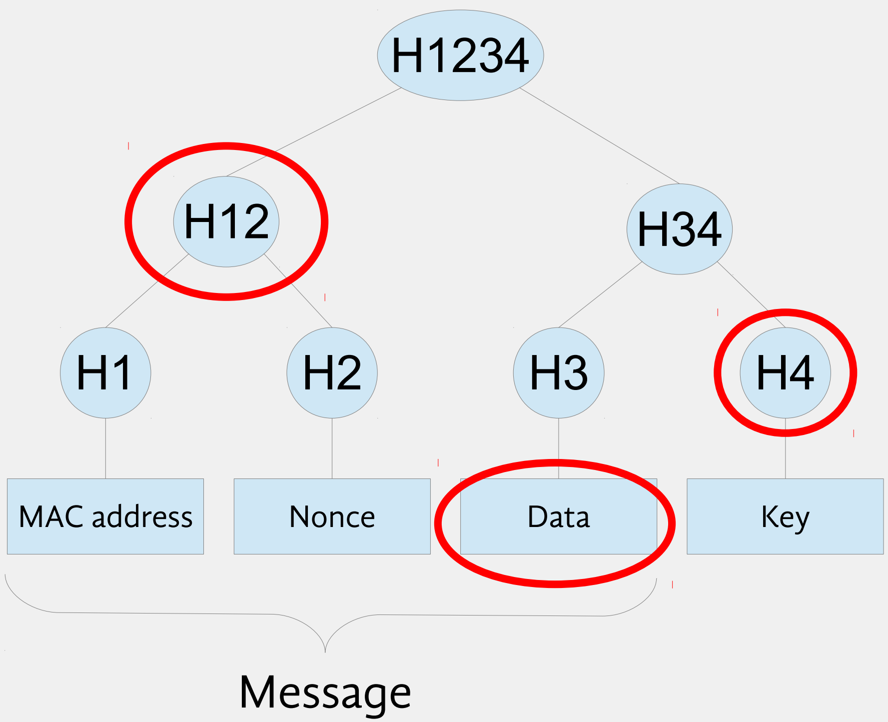
More Efficient Integrity

Merkle trees to improve performance for message integrity checks:



More Efficient Integrity

Merkle trees to improve performance for message integrity checks:



Paper Reflection

Selected because it sounded relevant to the topic

Addresses details of multiple previous works

Does not introduce them properly

I personally doubt their competence in security

- e.g., encryption through hashing

Summary

Internet technology vs. Smart Grid challenges

Smart Grid security properties:

- **Availablity**
- **Confidentiality**
- **Integrity**

Smart Grid getting more secure