Cyber security in the Smart Grid: Survey and challenges

Presented by Linn Eirin Paulsen

What is the paper about?

The paper presents a survey of the cyber security issues in the Smart Grid.

The goal is to provide an understanding of security vulnerabilities and solutions.

It focuses on security objectives and requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architecture in the Smart Grid.

Objectives and requirements for cyber security

SMART GRID SECURITY OBJECTIVES:

Availability, integrity and confidentiality are the most important objectives, in that order. Cited from NIST Smart Grid.

CYBER SECURITY REQUIREMENTS:

Attack detection and resilience operations: Because the SG features a relatively open communication network over large areas, it’s difficult to ensure that every node is invulerable. The network needs to detect and identify abnormal incidents due to attacks. Also the network must have ability to continue operations in the presence of attacks.

Objectives and requirements for cyber security

Identification, authentication and access control: The network infrastructure has millions of users an devices, so identification and authentication is key. Strict access control is necessary. Every node in the SG must have basic encryption.

Secure and efficient communication protocols: In particular in transmission and distribution systems, message delivery requires time-criticality and security.These to contradict each other, optimal tradeoffs are required to balance communication.

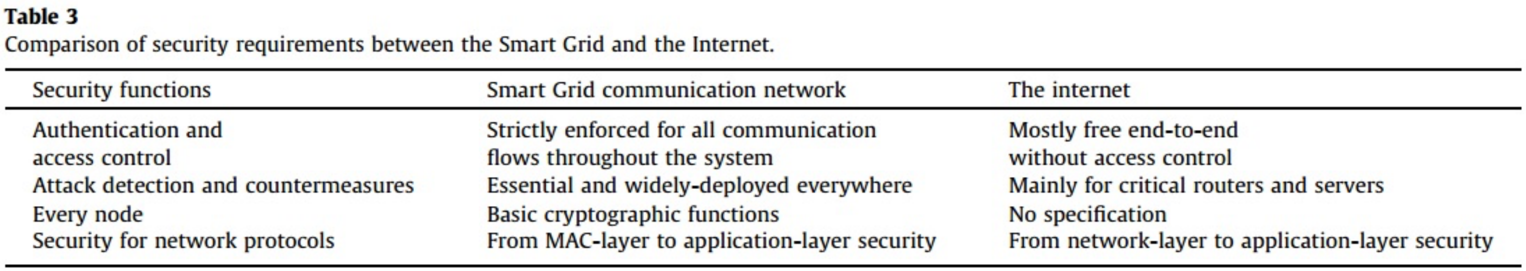

Table 3
Comparison of security requirements between the Smart Grid and the Internet.

Security functions	Smart Grid communication network	The internet
Authentication and access control	Strictly enforced for all communication flows throughout the system	Mostly free end-to-end without access control
Attack detection and countermeasures	Essential and widely-deployed everywhere	Mainly for critical routers and servers
Every node	Basic cryptographic functions	No specification
Security for network protocols	From MAC-layer to application-layer security	From network-layer to application-layer security

Network security threats in the Smart Grid

SMART GRID USE CASES WITH CRITICAL SECURITY REQUIREMENTS

Existing work focuses on power substation systems or SCADA systems. The NIST report recommends use cases for security consideration.

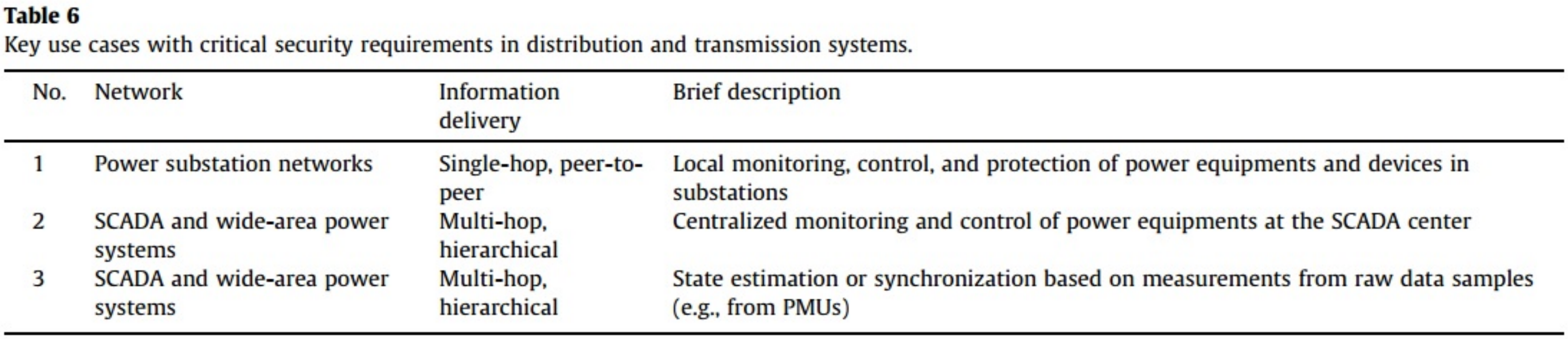

Table 6
Key use cases with critical security requirements in distribution and transmission systems.

No.	Network	Information delivery	Brief description
1	Power substation networks	Single-hop, peer-to-peer	Local monitoring, control, and protection of power equipments and devices in substations
2	SCADA and wide-area power systems	Multi-hop, hierarchical	Centralized monitoring and control of power equipments at the SCADA center
3	SCADA and wide-area power systems	Multi-hop, hierarchical	State estimation or synchronization based on measurements from raw data samples (e.g., from PMUs)

Network security threats in the Smart Grid

KEY FINDINGS

1 – The distribution and transmission system: Three important scenarios (table 6) with distinct communicaiton requirements and security vulnerabilites. Also, critical timing requirements limit the use of strong security solutions.

2 – The AMI system: Messages are none-time critical, availability is less important than integrity and confidentiality.

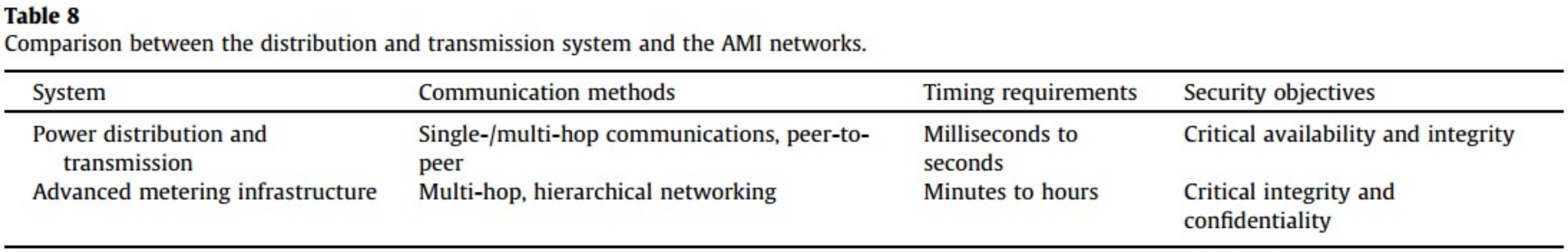

Table 8
Comparison between the distribution and transmission system and the AMI networks.

System	Communication methods	Timing requirements	Security objectives
Power distribution and transmission	Single-/multi-hop communications, peer-to-peer	Milliseconds to seconds	Critical availability and integrity
Advanced metering infrastructure	Multi-hop, hierarchical networking	Minutes to hours	Critical integrity and confidentiality

Network countermeasures

KEY FINDINGS: Packet-based detection schemes (can ble implemented in every layer to measure the transmission result for each packet and discover potential attacks by identifying an increase of packet transmission failures) can be used on many applications in the SG. Rate-limiting and filtering are effective attack mitigation methods. Current anti-jamming communications schemes are easily applied to AMI. DoS attack detection may still be based on existing frameworks, the research challenge lies in the differences between packet transmission on data networks and message delivery in th SG. The design of attack detection must be effectiv to trime-critical distribution and transmission networks. Jamming-resilient and delay-efficient transmission schems must be designed for secure communication in wireless bases distribution and transmission systems.

Cryptographic countermeasures

KEY FINDINGS: Case studies show that symmetric key cryptography is a better choice for real time IED communications in power distribution and transmission systems. We see that the IEC 62351 recommendation, RSA, is not ready to be used in time-critical communication between practical embedded devices for power systems. Tradeoff between security and latency. The initial results indicate that HMAC-based and HORS-based schemes can be potential solution candidates for authentication in the SG. But fine-graines protocols need to be developed for different applications because of the timing requirements in power systems.

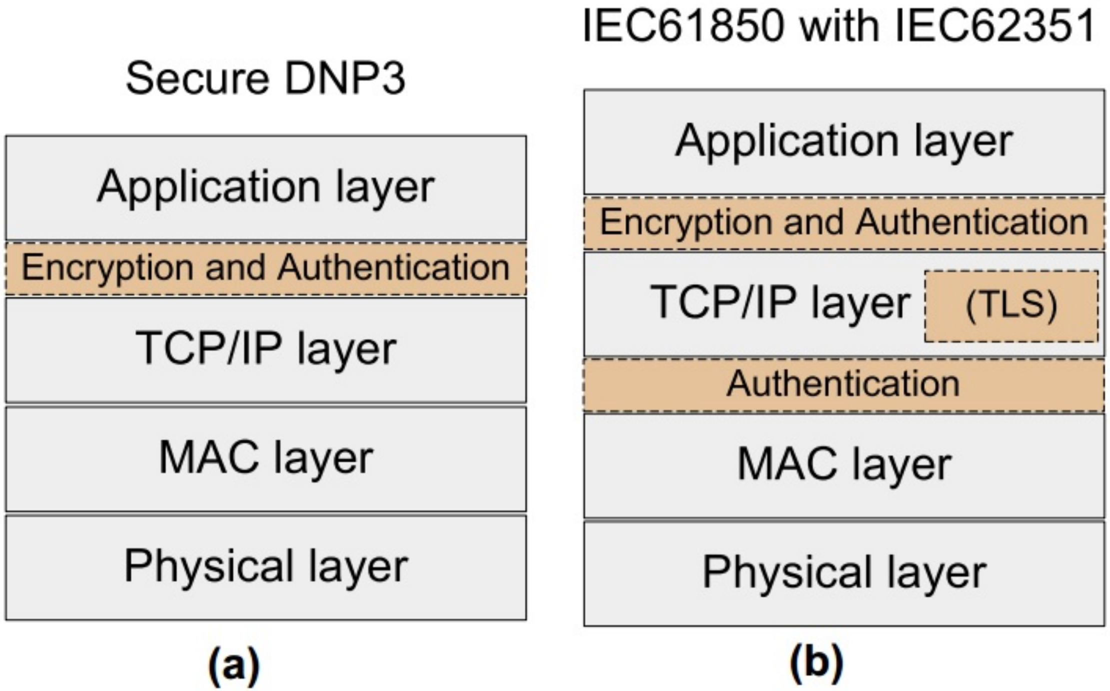

Fig. 9. Secure DNP3 and IEC 61850 with IEC 62351.

Design of secure network protocols and architectures

KEY FINDINGS: At the network and transport layers, power systems rely on Internet security mechanisms such as TLS and IPSec. This means that current power devices must use Interne security protocols to communicate in mulit-hop communications networks for wide-area power systems. Such mechanisms may not be the optimal solution for delay-oriented power systems. Should design new network/transport-layer protocols to achieve secure and efficient end-to-end delivere for wide area power systems in the SG. Designing strong data encryption schemes along the aggregation path is also a chellenge in the SG.

Discussion and remaining challenges

The survey features use case studies to analyze potential security attacks in different systems for the SG. They also offer first-hand experimental results on real world power devices. There are distinct features of different SG domains, which means a security solution may be applicable to one domain but not the others. They offer a overview of the remaining challenges in the SG security research. In the Generation/Transmission/Distribution domains, attack detection, mitigation authentication and key management are challenging issues, because of the large network scale and demanding requirements.

Conclusion: Cyber security in teh SG is still under development . It requires fine-grained security solutions designed specifically for distinct network applications.

Evaluation

The paper reviews many parts of the Smart Grid, maybe focus should be narrowed to some parts. Hard to keep track at the different types of attacks in different layers in different parts of the Smart Grid.

They do not address privacy, it seems it is not important.