Cyber Security and Privacy Issues in Smart Grids

Acknowledgement: Slides by Hongwei Li from Univ. of Waterloo

References

- **Main Reference**
  - Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. **"Cyber Security and Privacy Issues in Smart Grids,"** IEEE Communications Surveys & Tutorials, 2012.
- **In Brief**
  - U.S. NIST, "**Guidelines for smart grid cyber security** ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

NIST: National Institute of Standard and Technology

University of Waterloo

Outline

1. Reference model for the smart grid
2. Security issues
3. Privacy issues
4. Future research directions

3

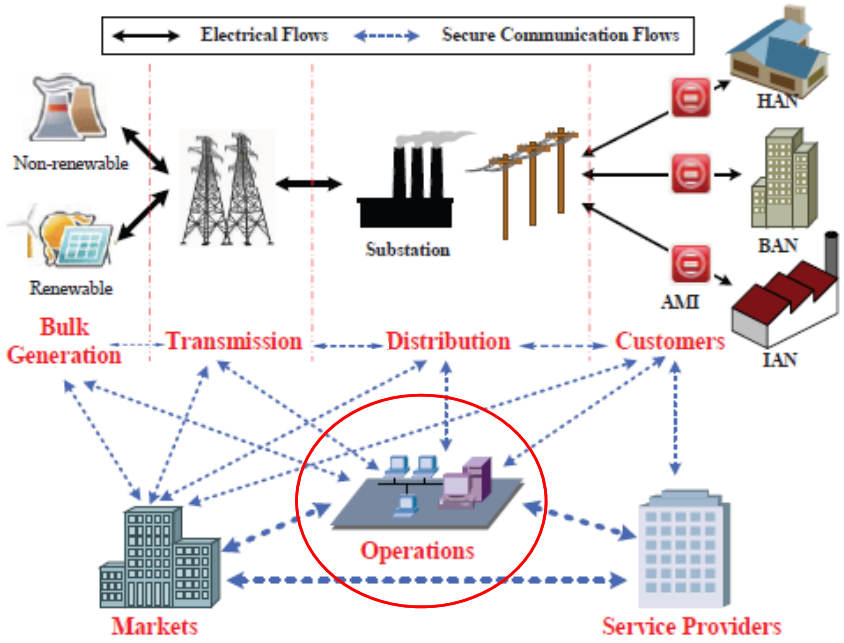


Fig. 1. NIST reference model for the smart grid

4

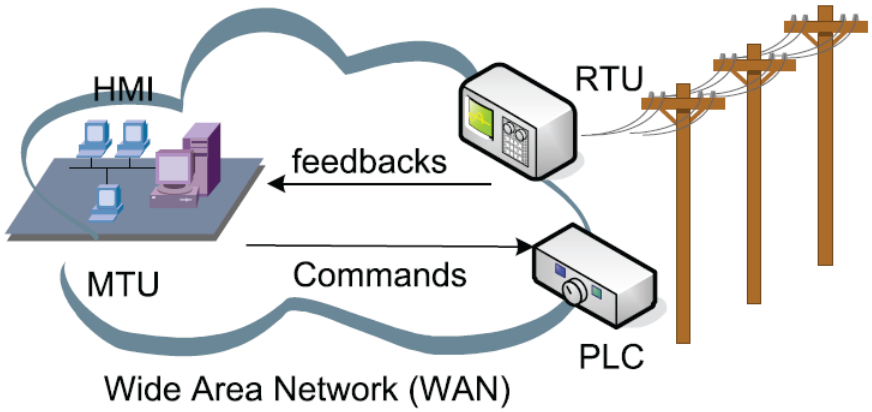
SCADA: an important component of operations

- SCADA (Distribution Supervisory Control and Data Acquisition)
  - A type of control system that transmits individual device status, manages energy consumption by controlling the devices.
  - Allows operators to directly control power system equipment.

The main goal of SCADA

- Helping the grid reduce operation and maintenance costs and ensure the reliability of the power supply.

5



MTU: Master Terminal Unit HMI: Human Machine Interface

RTU: Remote Terminal Unit PLC: Programmable Logic Controller

Field data interface devices: Including RTU and PLC, et al.

Fig. 3. A typical SCADA architecture

6

SCADA Security Issues-1

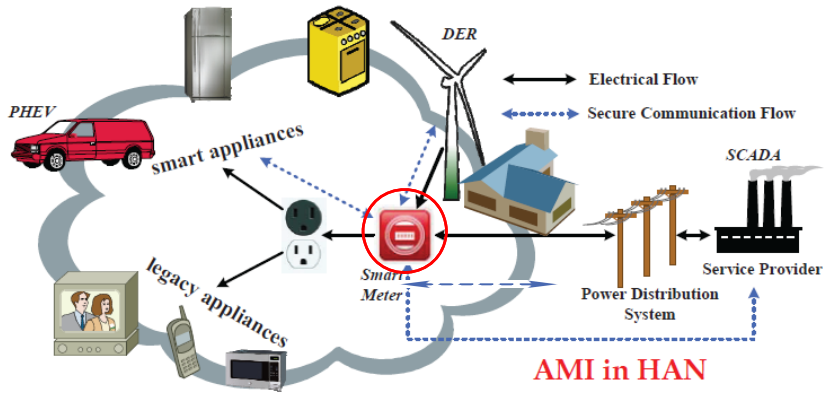
- Distribution control commands and access logs are critical for SCADA systems. Intercepting, tampering, or forging these data damages the grid.
  - Possible solutions: Ensure all commands and log files are accurate and secure.
- Synchronizing time-tagged data in wide areas is essential; without it the safety and reliability of the SCADA system cannot be achieved.
  - Possible solutions: Use a common time reference for time synchronization.

7

SCADA Security Issues-2

- Every decision of SCADA comes from the analysis of the raw data based on a reasonable model. Improper models may mislead operator actions. In addition, different vendors using distinct SCADA models will disrupt the consistency of the grid.
  - Possible solutions: So far, no.
- Other security issues ?

8



PHEV; Plug-in Hybrid Electric Vehicle DER: Distributed Energy Resource

HAN: Home Area Network AMI: Advanced Metering Infrastructure

Fig. 2. A use case of AMI in HAN

9

University of Waterloo

Smart Meter Security

- Meters may suffer physical attacks such as battery change, removal, and modification.
- Functions like remote connect/disconnect meters and outage reporting may be used by unwarranted third parties.
- Customer tariff varies on individuals, and thus, breaches of the metering database may lead to alternate bills.

Possible solutions

- Ensure the integrity of meter data.
- Detect unauthorized changes on meter.
- Authorize all accesses to/from AMI networks.
- Secure meter maintenance.

10

Customer Interface Security

- Home appliances can interact with service providers or other AMI devices. Once manipulated by malicious intruders, they could be unsafe factors in residential areas.
- Energy-related information can be revealed on the communication links. Unwarranted data may misguide users' decision.

Possible solutions

- Access control to all customer interfaces.
- Validate notified information.
- Improve security of hardware and software upgrade.

11

PHEV Security

- PHEV can be charged at different locations. Inaccurate billings or unwarranted service will disrupt operations of the market.

Possible solutions

- Establish electric vehicle standards [1].

[1] U.S. NIST, "Guidelines for smart grid cyber security ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

12

Anomaly detection-1: Temporal Information

- Unsecured time information may be used for replay attacks and revoked access which has a significant impact on many security protocols.
- Timestamps in event logs may be tampered by malicious people.

Possible solutions

- Use Phasor Measurement Units (PMUs) to ensure accurate time information.
- Adopt existing forensic technologies to ensure temporal logs are accurate.

13

Anomaly detection-2: Data & Service

- RTUs may be damaged in various ways. The accuracy of transmitted data and the quality of services therefore can not be guaranteed.

Possible solutions

- Utilize fraud detection algorithms and models used in credit card transaction monitoring[1].

[1] U.S. NIST, "Guidelines for smart grid cyber security ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

14

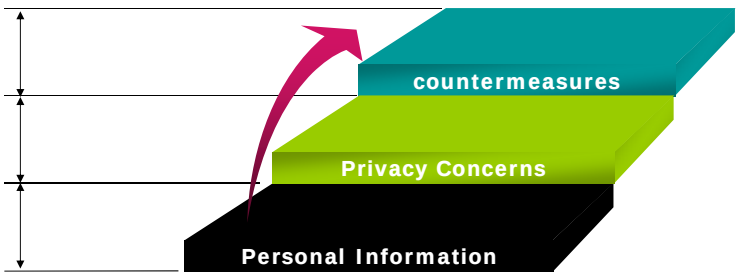
Demand Response

What is the demand response?

- Smart grid allows customers to shift load and to generate and store energy based on near real-time prices and other economic incentives.
- Customers can also sell surfeit stored energy back to the grid when the price is high.
- Such demand-response mechanisms help the grid balance power supply and demand, thus enhancing the efficiency of power usage.

15

Privacy Issues on Smart Grid



16

Personal Information

- NIST guidelines have provided a list of personal information that may be available through the smart grid as follows[1]:
  - Name: responsible for the account
  - Address: location to which service is being taken
  - Account number: unique identifier for the account
  - Meter IP, Meter reading, current bill, billing history
  - Lifestyle; when the home is occupied and it is unoccupied, when occupants are awake and when they are asleep, how many various appliances are used, etc.
  - DER: the presence of on-site generation and/or storage devices, operational status, net supply to or consumption from the grid, usage patterns.
  - Service Provider: identity of the party supplying this account, relevant only in retail access markets.

[1] U.S. NIST, "Guidelines for smart grid cyber security ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

17

Privacy Concerns

- Energy consumption data obtained by a third part may disclose personal information without one's permission[1].
  - Firstly, data in the smart meter and HAN could reveal certain activities of home smart appliances, e.g., appliance vendors may want this kind of data to know both how and why individuals used their products in certain ways.
  - Secondly, obtaining near real-time data regarding energy consumption may infer whether a residence or facility is occupied, what they are doing, and so on.
  - Thirdly, personal lifestyle information derived from energy use data could be valuable to some vendors or parties, e.g., vendors may use this information for targeted marketing, which could not be welcomed by those targets.
  - . . .

[1] U.S. NIST, "Guidelines for smart grid cyber security ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

18

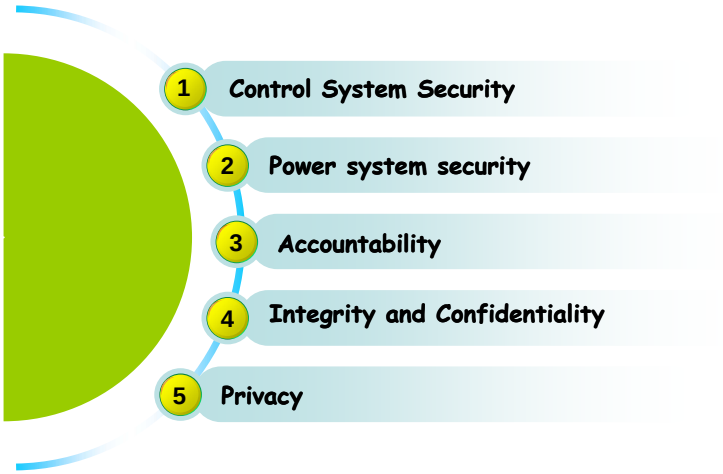
Countermeasures

- NIST proposed some countermeasures to address privacy issues in smart grid [1].
  - An organization should ensure that information security and privacy policies exist and are documented and followed. Audit functions should be present to monitor all data accesses and modifications.
  - Before collecting and sharing personal information and energy use data, a clearly-specified notice should be announced.
  - Organizations should ensure the data usage information is complete, accurate, and relevant for the purposes identified in the notice.
  - Personal information in all forms, should be protected from unauthorized modification, copying, disclosure, access, use, loss, or theft.
  - . . .

[1] U.S. NIST, "Guidelines for smart grid cyber security ," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

19

Future Research Directions



20

Control System Security

- Industrial control normally does not do too much about security. In recent years, people pay some attention to control systems security to protect power generation, transmission and distribution.
- Co-designs of control and security in smart grids will be interesting topics in the future.

[1] Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, 2012.

21

Power System Security

- Besides cyber security, vulnerabilities in physical power grid should also be further explored and studied. Since new devices will be largely deployed, no one can guarantee the power line itself is 100% secure.

[1] Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, 2012.

22

Integrity and Confidentiality

- Integrity and confidentiality are two main aspects for computer and network security design.
- Naturally, they are still essential for securing the smart grids. For example, integrating with huge numbers of DERs may incorporate with distributed database management and cloud computing technology.
- Whether or not we could adopt current solutions to provide integrity and confidentiality for smart grid is a future research direction.

[1] Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, 2012.

23

Privacy

- Privacy issues in cyber security may be addressed by adopting newly anonymous communication technologies.
- Current approaches to anonymize traffic in general networks will cause overhead problems or delay issues. For some time-critical operations, limited bandwidth and less connectivity features in the smart grid may hinder the implementation of anonymity.

[1] Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, 2012.

24

University of Waterloo

Accountability

- As a complement, accountability is required to further secure the smart gird in terms of integrity, confidentiality and privacy.
- Even if a security issue presents itself, the built-in accountability mechanism will determine who is responsible for it. Once detected, some problems can be fixed automatically through the predefined program, while others may provide valuable information to experts for evaluation.

[1] Liu, J. and Xiao, Y. and Li, S. and Liang, W. and Chen, C. "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, 2012.

25