Summer Workshop on Cyber Security

Smart Grid Cyber Security (Part 2)

Dr. Hamed Mohsenian-Rad

University of California at Riverside and Texas Tech University
July 14 - 18, 2014

Supported by National Science Foundation
Smart Grid Cyber Security

• IT technologies can make the grid *smart*!
  – Real time monitoring (PMUs, Smart Meters)
  – Advanced information analysis (Big Data)
  – Automated control (Self-healing, Smart Actuators)

• They also make the grid *vulnerable*!
Smart Grid Cyber Security

• USA TODAY on July 11, 2013:

Spooked by NSA, Russia reverts to paper documents!
... officials at Kremlin recently ordered 20 typewriters.
Smart Grid Cyber Security

• In smart grid, we are doing the opposite:

• Can the 2003 blackout happen again, intentionally?
Privacy and Security Concerns

• For the rest of this workshop we will study

  “Privacy”

  and

  “Security”

• These are different but related smart grid issues.
Smart Meters and Privacy

- **Q**: What is the difference between these two?

  - Traditional Meter

  - Smart Meter
Smart Meters and Privacy

- **Q:** What is the difference between these two?

  - Traditional Meter → Total Load
  - Smart Meter → Load Profile
Smart Meters and Privacy

• Residential load profile:

![Power Consumption Chart]

- Peak: 7.18 kW
- Mean: 0.49 kW
- Total Consumption: 11.8 kWh
Smart Meters and Privacy

- Residential load profile:

  Peak: 7.18 kW
  Mean: 0.49 kW
  Total Consumption: 11.8 kWh

Power Consumption (kW)

Time of Day

refrigerator, Toaster, Heating Cycles, Hob Heaters, Over Preheating, Kettle, Washing Machine, Kettle
Smart Meters and Privacy

• Every home appliance has a load signature.

• The load profile can reveal your life style.

• Q: Does it concern you?

• See: http://www.youtube.com/watch?v=8JNFr_j6kdI
Smart Meters and Privacy

• Example 1: Criminals can use the data
  • To schedule burglary
    • They can figure out if you are not at home.
    • House alarm systems have their own signature
  • Pre-identify what items they want to steal.
    • Plasma TVs have their own signature.
    • Laptop computers have their own signature
Smart Meters and Privacy

• **Example 2: Privacy violation**

  • Your *living pattern* can be revealed
    
    • When you wake up.
    
    • When you take shower
    
    • When you watch TV

  • You can even tell what TV program / movie is watched!
    
    • Fluctuations at brightness of movies → Load changes!
Smart Meters and Privacy

• **Example 3**: Healthcare companies can
  
  • Determine which **medical devices** you used.
    
    • Pre-existing conditions
    
    • Different insurance rate

• **Example 4**: Your landlord can tell
  
  • How many people live here. When you have a party!
Smart Meters and Privacy

• Here we are facing two problems:
Smart Meters and Privacy

• To avoid third party access to the metering data:
  – Data encryption at smart meters.
  – Message authentication at utility servers.

• Typical security solutions, just like Credit Card data!
Smart Meters and Privacy

- **Q:** How about protection against utilities?
  - You may not want the utilities to know your life style.
    - They may sell your information!
  - But they **do** need to know your load profile!

- **Q:** Is there any cyber security solution?
Smart Meters and Privacy

• Local **renewable generation** can help mask data

\[ \text{Meter reading} = \text{Load} - \text{Local Renewable Generation} \]

**Stochastic Nature**
Smart Meters and Privacy

• Another solution is to use local batteries

\[
\text{Meter reading} = \text{Load} - \text{Battery Discharge} + \text{Battery Charge}
\]

• Set the charging schedules to hide signatures!
Smart Meters and Privacy

• Our key message so far:

Combine Power Systems and Information Systems Solutions.
Cyber Security Concerns

• Privacy is a valid concern for consumers.

• But there are also some serious security concerns:
  – What if hackers *alter* Smart Meter and PMU data?
  – What if hackers *take control* of automation system?
  – ...

Cyber Attacks against Smart Grid

- In smart grid, **all sectors** interact via two-way communications:
Cyber Attacks against Smart Grid

- In smart grid, all sectors interact via two-way communications:

![Diagram showing the interaction between Generation, Distribution & Control, and Consumption through Communications Infrastructure and different types of cyber attacks.](image-url)
Cyber Attacks against Smart Grid

- In smart grid, all sectors interact via two-way communications:

  - Cyber Attack (Type I)
  - Cyber Attack (Type II)
  - Cyber Attack (Type III)

Easier to Hack

- Generation
- Distribution & Control
- Consumption
Cyber Attacks against Smart Grid

- In smart grid, **all sectors** interact via two-way communications:

  - **Cyber Attack (Type I)**
  - **Cyber Attack (Type II)**
  - **Cyber Attack (Type III)**

![Diagram showing communications infrastructure and types of cyber attacks affecting smart grid components: Generation, Distribution & Control, Consumption. The diagram illustrates the flow of communications and highlights that larger scale to be effective.]
Cyber Attacks against Smart Grid

- In smart grid, all sectors interact via two-way communications:

  - Cyber Attack (Type I)
  - Cyber Attack (Type II)
  - Cyber Attack (Type III)

Hacking a Power Plant = Hacking Multiple Thousands of Meters
Type I Cyber Attacks

• This type of attacks affect the operation of generators.

• Turning off/on a generator can imbalance supply and demand.

• Generally speaking:
  
  – Supply < Demand  \[\rightarrow\]  Frequency < Nominal
  
  – Supply > Demand  \[\rightarrow\]  Frequency > Nominal

• Ripple effect is usually a major problem in such cases.
Type I Cyber Attacks

• Although such attacks are complex and need resources:
  
  In January 2008, the Central Intelligence Agency reported knowledge of four disruptions, or threatened disruptions, by hackers of the power plants for four cities [Amin 2010].

• We need to highly protect access to power plants:
  
  – Physical Access
  
  – Cyber Access
Type I Cyber Attacks

• Any remote access should be controlled by firewalls:

• Consider both remote data and *local* measurements.
Type II Cyber Attacks

- Attacks against distribution and control systems.
Type II Cyber Attacks

- Attacks against distribution and control systems.
Type II Cyber Attacks

- Attacks against distribution and control systems.

Control & Monitoring Centers

Sensors

Actuators
Type II Cyber Attacks

- Attacks against *distribution and control* systems.

Control & Monitoring Centers

Sensors

Actuators
Type II Cyber Attacks

- Attacks against distribution and control systems.
Type II Cyber Attacks

- Attacks against *distribution and control* systems.
Hacking PMUs

• Q: Any suggestion on hacking a PMU?
Hacking PMUs

• **Q**: Any suggestion on hacking a PMU?

• Department of Homeland Security released a report in July 2013 about *GPS Systems vulnerabilities to jamming attacks*.  

* Example: Newark Airport Incident in 2010.*
Hacking PMUs

• **Q:** Any suggestion on hacking a PMU?

• With invalid time-stamp, GPS data is *useless* or *misleading*.
Hacking Network Devices

• A similar attack can be designed against network equipment.

• We need to do source and message authentication.
False Data Injection Attacks

• We need to do our best to protect sensor data.

• But what if an attack goes through?

• Power Systems Solution:

PMUs readings should add up!
False Data Injection Attacks

• The power grid is a circuit governed by rules of physics!

\[ P_{31} + P_{32} + L_3 = 0 \]

\[ P_{31} = B_{31}(\theta_3 - \theta_1) \]

\[ P_{32} = B_{32}(\theta_3 - \theta_2) \]

• What you observe at different locations should be **consistent**!
False Data Injection Attacks

- **Example**: It is not enough to just hack PMU 1:
  - PMUs 4 and 6 need to be hacked too.
  - Or the attack will be detected!
False Data Injection Attacks

- **Operator’s Viewpoint**: Operator has limited resources.
  - Only 5 PMUs can be protected.
  - Which ones?
  - This is a “hot” problem.
False Data Injection Attacks

- **Attacker’s Viewpoint**: Attacker has limited resources.
  - Only 2 PMUs can be hacked at a time.
  - Which ones?
  - This is a “hot” problem.
False Data Injection Attacks

- **Attacker’s Viewpoint**: Attacker has limited resources.
  - Only 2 PMUs can be hacked at a time.
  - Which ones?
  - This is a “hot” problem.

Combine Power Systems & Information Systems Solutions.
Type III Cyber Attacks

- A Type III attack affects the load sector.
  - One of the standard Type III attacks is “load altering attack”.

- Load altering attack is an attack against demand response.

- **Q**: Can you guess how this attack may work?
Load Altering Attacks

• There is a growing interest towards using **automated** energy management systems that respond to time-varying prices:

\[ x_a \text{ : Energy consumption schedule for appliance } a. \]
Load Altering Attacks

• There is a growing interest towards using automated energy management systems that respond to time-varying prices:

\[ x_a \]: Energy consumption schedule for appliance \( a \).
Load Altering Attacks

• There is a growing interest towards using automated energy management systems that respond to time-varying prices:

\[ x_a : \text{Energy consumption schedule for appliance } a. \]
Load Altering Attacks

• There is a growing interest towards using automated energy management systems that respond to time-varying prices:

\[ x_a \] : Energy consumption schedule for appliance \( a \).
Load Altering Attacks

• There is a growing interest towards using automated energy management systems that respond to time-varying prices:

\[ x_a : \text{Energy consumption schedule for appliance } a. \]
Load Altering Attacks

• Assume that a hacker compromises the price data:
  • Sent to hundreds of thousands of ECS devices.

• A large number of users jump into the low price hour.
  • This can cause a load spike at an already peak hour.
  • Price signals have to be source authenticated.
Load Altering Attacks

- A sudden spike in load demand for 1 million users

= 

- A sudden shot down of multiple generation units!

- It resembles Denial of Service attacks with botnets!
Combined Cyber Physical Attacks

• Having a mix of
  • Type I
  • Type II
  • Type III

Cyber attacks combined with
  • Physical attacks.

Needs a lot of Resources
Can cause major damage
Conclusions and Summary

• Smart Grid is a cyber physical system:
  
  • IT Technologies in
    
    – Generation
    
    – Distribution and Transmission
    
    – Control and Monitoring
    
    – Consumption
Conclusions and Summary

• All these sectors become vulnerable to cyber attacks.
  • Type I to Type III Cyber Attacks

• Attacks can involve both
  • Cyber elements.
  • Physical elements
Conclusions and Summary

- Most effective security solutions are combined:
  - **Power Systems**: Understanding Power Grid
  - **Information Systems**:
    - Message Encryption
    - Message Authentication
    - Source Authentication
    - ...

References

• Please refer to the references at the end of these files:

  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_1_Power_Systems.pdf
  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_2_Smart_Grid.pdf
  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_3_Communications.pdf
  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_4_Demand_Response.pdf
  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_5_Renewable_Power.pdf
  • http://www.ee.ucr.edu/~hamed/Smart_Grid_Topic_6_Wide_Area_Measurement.pdf