Summer Workshop on Cyber Security

Smart Grid Cyber Security (Part 1)

Dr. Hamed Mohsenian-Rad

University of California at Riverside and Texas Tech University
August 12-16, 2013

Supported by National Science Foundation
Smart Grid Cyber Security

• Smart Grid is a **Cyber Physical System**, a “hot” area!

• **Q:** What is the difference between studying

  “Cyber Security”

  and

  “Smart Grid Cyber Security”? 

A Typical Power Grid
Power Grid in the U.S.

United States transmission grid
Source: FEMA

www.geni.org
Power Grid in the U.S.
Power Grid in Texas - Generation

- South Texas Nuclear Station (Bay City, TX)
- Wind Farms (Sweetwater, TX)
- Gas Plant (Forney, TX)
Power Grid in Texas - Consumption

* It can get to around 70,000 MW in Summer!

- Load Profile is Highly **Unbalanced**.
Power Grid in Texas - Consumption

Historical Peak Load (ERCOT)

US Electricity Price ($/MWH)

* PHEVs are coming!
Some Issues

• Price of Electricity is Increasing.

• We need more generation capacity.

• Energy usage is highly unbalanced over time.

• We need a better monitoring and control.
Some Issues

• Price of Electricity is Increasing.

• We need more generation capacity.

• Energy usage is highly unbalanced over time.

• We need a better monitoring and control.
Q: What is Smart Grid?
Q: What is Smart Grid?

Short Answer:

Smart Grid = Power Grid + IT
Q: What is Smart Grid?

Short Answer:

Smart Grid = Power Grid + IT

Sensors, Smart Meters, Automation, Internet, iPhone, iPad, ...
Q: What is Smart Grid?

- Traditional Grid:
  - Markets and Operations
  - Generation
  - Transmission
  - Distribution
  - Consumption

Power Infrastructure

One-way flow of electricity

*Centralized, bulk generation*
*Heavy reliance on coal and oil*
*Limited automation*
*Limited situational awareness*
*Consumers lack data to manage energy usage*
Q: What is Smart Grid?

- Future Grid:
  - Markets and Operations
  - Generation
  - Transmission
  - Distribution
  - Consumption

  **Power Infrastructure**

  **Two-way Flow of Electricity and Information**

  **Communications Infrastructure**
Q: What is Smart Grid?

• **Future Grid:**

    ![Diagram of Future Grid Components]

    - Markets and Operations
    - Generation
    - Transmission
    - Distribution
    - Consumption
    - Power Infrastructure
    - Two-way Flow of Electricity and Information
    - Communications Infrastructure
Q: What is Smart Grid?

• According to the U.S. Department of Energy:

“Smart grid” generally refers to a class of technologies that are used to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way digital communications technologies and computer processing that has been used for decades in other industries. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumers. They offer many benefits to utilities and consumers -- mostly seen in big improvements in energy efficiency and reliability on the electricity grid and in energy users’ homes and offices.
DoE: Smart Grid as Enabling Engine

- Nationwide use of plug-in electric vehicles
- Seamless integration of renewable energy sources
- Large-scale storage
- New era of consumer choice
- 24 hours use of solar energy
- Green & Zero-net energy buildings (lighten the load)
### Smart Grid Priority Areas (NIST)

<table>
<thead>
<tr>
<th>Priority Areas to Build a Smart Grid (Identified by NIST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Demand Response and Consumer Energy Efficiency</td>
</tr>
<tr>
<td>2. Transportation Electrification</td>
</tr>
<tr>
<td>3. Renewable Power Generation</td>
</tr>
<tr>
<td>4. Energy Storage</td>
</tr>
<tr>
<td>5. Advanced Metering Infrastructure</td>
</tr>
<tr>
<td>6. Distributed Grid Management</td>
</tr>
<tr>
<td>7. Wide-Area Situational Awareness</td>
</tr>
<tr>
<td>8. Network Communications</td>
</tr>
<tr>
<td>9. Cyber Security</td>
</tr>
</tbody>
</table>
1. Demand Response

- Until large-scale energy storage becomes a reality:
  - **Balancing** Supply and Demand at **Any Time**
1. Demand Response

Peak-to-average Ratio (PAR) = \[
\frac{\text{Peak Daily Load}}{\text{Average Daily Load}}
\]

It is desired to have PAR closer to 1. (Q: Why?)

Source: ERCOT
1. Demand Response

• According to the U.S. Department of Energy:

Demand response (DR) is defined as changes in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to other incentives designed to induce lower electricity use at times of high energy usage (peak hours) or when power system reliability is jeopardized.

**Bottom line:** We want to *reduce* demand whenever needed!
1. Demand Response

• **Direct Load Control:**
  
  – Utility makes the decision
  
  – Typical Load:
    • Air conditioner
    • Water heater
    • Pumps

• **Pricing**

  – User makes the decision (automatic or manual)
1. Demand Response

- In either case we need **two-way communications**:
1. Demand Response

• In either case we need **two-way communications**:

---

**Smart Grid**

- Command / Price
- Usage Data

- (automatic or manual)

---
1. Demand Response

• **Sample pricing** options:

  - **Summer**
    - Time of Use Pricing (Toronto, ON)

  - **Winter**
    - Day-Ahead Pricing (Chicago, IL)
2. Transportation Electrification

• From Jan 2008 to June 2013:
  – Total of 116,000 plug-in electric cars are sold in the U.S.
    • Rank 1: Chevrolet Volt (36%)
    • Rank 2: Nissan Leaf (25%)
    • Another Model: Tesla S (10%)
2. Transportation Electrification

• **Q:** What if everybody charges at the same time?
2. Transportation Electrification

• Vehicle-to-Grid (V2G) Mode:

Discharge power from electric car to the grid when needed.
2. Transportation Electrification

• Charge and Discharge Coordination
2. Transportation Electrification

- Charge and Discharge Coordination

![Smart Grid Diagram]
3. Renewable Power Generation

- U.S. electricity generation by energy source:

![Graph showing electricity generation by energy source with the following percentages:
- Coal: 44.9%
- Natural Gas: 23.4%
- Nuclear: 20.3%
- Hydroelectric: 6.9%
- Conventional: 3.6%
- Petroleum: 1.0%
- Other Renewables: 3.6%

![Bar graph showing carbon footprints for different energy sources with Coal having the highest carbon footprint followed by Gas, Biomass, PV, Marine, Hydro, Wind, and Nuclear having the least.]}
3. Renewable Power Generation

• Various renewable generation options:
3. Renewable Power Generation

- **Main challenge**: intermittency and fluctuations

Clouds over the DeSoto PV site. Irradiance in a cloudy day.
3. Renewable Power Generation

• Main **challenge**: intermittency and fluctuations

Wind Speed in Lubbock, TX

Wind Turbine Power Generation Curve
3. Renewable Power Generation

• Main **challenge**: intermittency and fluctuations
  
  – Recall that we should always **match** supply and demand.
  
  – We need:
    
    • Sensors for **real-time monitoring**
    
    • **Prediction** methods
    
    • **Automation**
3. Renewable Power Generation

- Main **challenge**: intermittency and fluctuations
  - Recall that we should always **match** supply and demand.
  
- We need:
  - Sensors for **real-time monitoring**
  - **Prediction** methods
  - **Automation**
4. Energy Storage

• Two approaches to integrate renewable resources:

- Renewable Generators
- Fast Responding Generators (Coal & Gas)
4. Energy Storage

- **Two approaches** to integrate renewable resources:

  - Renewable Generators
  - Fast Responding Generators (Coal & Gas)
4. Energy Storage

- **Two approaches to integrate renewable resources:**

![Diagram showing renewable generators, storage charge, and discharge](image.png)
4. Energy Storage

• Various storage options:
4. Energy Storage

• **Coordination** across renewables and storage units:
5. Advanced Metering

• First, consider traditional (not smart!) meters:

* Reading on June 1, 2013 = 093735 kWh
* Reading on July 1, 2013 = 092779 kWh

Usage = 093735 - 092779 = 956 kWh

Bill = 956 kWh x 11.44 c/kWh = $109.37
5. Advanced Metering

• Problem with traditional (not smart!) meters:
  
  – They do NOT take into account time of use!
  
  – The only price model they can support is a flat rate
  
  – What is the incentive to reduce load at peak-hours?
  
  – We cannot support demand response.
5. Advanced Metering

• Therefore, we need a **smart meter**: 

![Smart Meter Image]

<table>
<thead>
<tr>
<th>Time</th>
<th>kWh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Hours</td>
<td></td>
</tr>
</tbody>
</table>

**Load Profile**

Monthly Reading: $30 \times 24 \times 4 = 2880$ Values
5. Advanced Metering

• Therefore, we need a **smart meter**:

**Load Profile**

- **Monthly Reading**: $30 \times 24 \times 4 = 2880$ Values

**Peak Hours**

**Time**
6. Distributed Grid Management

• Power grid is a large and complex network / circuit.

• It is becoming even more complex:
  – Distributed and Renewable Generation
  – Storage Systems
  – Demand Response and Electric Vehicles
  – New Services and Market Options
6. Distributed Grid Management

- Regional System Operators (CAISO, ERCOT, PJM, ...):

CAISO
6. Distributed Grid Management

• We need **distributed** control systems at all levels:
6. Distributed Grid Management

- And they should be able to communicate:
6. Distributed Grid Management

**Example**: grid management at distribution level:

- Substation
- Transformer
- Controller
- Sensors
- Smart Meters
- Rooftop PV Panels
- Batteries
- Protection System
6. Distributed Grid Management

• **Example**: grid management at distribution level:

  – Issues:
    • Fault Detection
    • Disruption Management
    • Substation Congestion Control
    • Voltage Control
    • Power Loss Control
    • Integrating
      – Renewable Resources
      – Storage
      – Electric Vehicles
6. Distributed Grid Management

• **Example**: grid management at distribution level:

  – Issues:
    • Fault Detection
    • Disruption Management
    • Substation Congestion Control
    • Voltage Control
    • Power Loss Control
    • Integrating
      – Renewable Resources
      – Storage
      – Electric Vehicles

Local Response
Self Healing
Avoid Ripple Effect

Smart Grid
7. Wide-Area Situational Awareness

• Before we make a control of management decision:

  – We need to know what is going on in this huge circuit!
7. Wide-Area Situational Awareness

• A key sensor in wide area monitoring:

  – Phasor Measurement Unit (PMU)

\[ V_i = |V_i| \angle \theta_i \]
7. Wide-Area Situational Awareness

- We usually compare Phasors at different locations:

![Diagram showing comparison of phasors at different locations with time-stamped data.](image)
7. Wide-Area Situational Awareness

- PMUs are synchronized using GPS systems (Q: Why?):
  - 24 Satellites in 12 hour orbit times
  - Time-stamps will be synchronized.

PMUs are also called synchrophasors.
7. Wide-Area Situational Awareness

- PMUs are new technologies and highly accurate:

![PMU Measurements](image1.png)

![SCADA Measurements](image2.png)
7. Wide-Area Situational Awareness

• **Example**: PMUs can show how a fault was propagated.

• Therefore, we can **diagnose** the source of the fault!
7. Wide-Area Situational Awareness

• The phase magnitudes are important.

• But what matters most is the phase difference.
  
  – It indicates the power flow on a transmission line.
  
  – Inter-connected systems are typically synchronized.

  • Phase difference between any two points should be small.

    (Otherwise, something is wrong!)
7. Wide-Area Situational Awareness

- **Example**: August 14, 2003 Northeast Blackout
7. Wide-Area Situational Awareness

• **Example**: August 14, 2003 Northeast Blackout

  • 12:15:00 EDT: Some operation error in Northern Ohio
  • 13:31:00 EDT: The Eastlake, Ohio generating plant **shuts down**
  • 16:05:57 EDT: Last point blackout could have been **prevented!**
  • 16:13:00 EDT: A total of **256 power plants** are offline

    • Restoration: It took up to **6 days** in some locations.
7. Wide-Area Situational Awareness

• **Example**: August 14, 2003 Northeast Blackout

  – About **55 million people** were affected in the U.S. and Canada

Downtown Toronto

Evening of August 14, 2003
7. Wide-Area Situational Awareness

- Some applications of PMUs and Situational Awareness
  - Quickly respond to emergencies
  - Prevent disturbance propagation
  - Planned islanding, if needed
  - Limited scope load shedding, if needed
  - Faster system restoration
7. Wide-Area Situational Awareness

- Some applications of PMUs and Situational Awareness
  - Quickly respond to emergencies
  - Prevent disturbance propagation
  - Planned islanding, if needed
  - Limited scope load shedding, if needed
  - Faster system restoration
8. Communications Networks

• The choice of communication technology depends on
  – Distance
    • In-home
    • Neighborhood
    • Distribution Network
    • Transmission Network
    • Inter-connection
  – Data rate
8. Communications Networks

- Wireless communications:
  - Zigbee
  - WiFi
  - WiMax
8. Communications Networks

• Wired communications:
  – Ethernet / Internet
  – Power Line (PLC)
  – Dedicated Lines
8. Communications Networks

Smart Grid = IT + Power Grid

Ref: www.nazeleno.cz
Q: How about Cyber Security?

• Power grid is a
  – Huge
  – Complex
  – Critical
  – Expensive

infrastructure.

• Can IT technologies make the power grid vulnerable?