Cyber-Attacks on Electric Power System: Vulnerability and Resiliency Analysis

Lalitha Sankar
Arizona State University
PSERC Workshop, Stevenson, WA

July 13, 2015
Overview

• Electric power system is a distributed hybrid-hierarchical system.
  • top-bottom (intra-regional) and
  • lateral connections (inter-regional)

• At each level, SCADA and EMS manage and monitor the system.

• SCADA, Communication network, and Data Center will always be vulnerable to cyber attacks.
Overview

• Electric power system is a distributed hybrid-hierarchical system.
  • top-bottom (intra-regional) and
  • lateral connections (inter-regional)

• At each level, SCADA and EMS manage and monitor the system.

• SCADA, Communication network, and Data Center will always be vulnerable to cyber attacks.

• What are the consequences of cyber-attacks on the transmission system?
Motivation

- Large-scale outages are causes for concern and often involve operator error.
- Recently cyber and physical attacks have also been contributors.
Motivation

- Large-scale outages are causes for concern and often involve operator error.
- Recently cyber and physical attacks have also been contributors.

In 2003, a line out in Ohio was not conveyed in time to MISO, leading to the Northeast blackout.
**Motivation**

- Large-scale outages are causes for concern and often involve operator error.
- Recently cyber and physical attacks have also been contributors.

In 2003, a line out in Ohio was not conveyed in time to MISO, leading to the Northeast blackout.

In 2007, Aurora Generator Test shows that cyber attacks can lead to generator getting out of phase and finally exploding.
Motivation

- Large-scale outages are causes for concern and often involve operator error.
- Recently cyber and physical attacks have also been contributors.

In 2010, Stuxnet malware attacked SCADA systems, infecting 14 plants in Germany.

In 2003, a line out in Ohio was not conveyed in time to MISO, leading to the Northeast blackout.

In 2007, Aurora Generator Test shows that cyber attacks can lead to generator getting out of phase and finally exploding.
Motivation

• Attack attempt statistics collected by DHS.

DHS recorded 161 cyber attacks on the energy sector in 2013, compared to 31 in 2011.
Cyber-Attacks on EPS

- Remote hacking, firewall break-in, malware introduction, trojans/virus, false data injection, …
EPS Cyber-Attacks: The Good

• Recent cyber-attacks involve hacking into databases and learning/revealing information.

Hacking of Government Computers Exposed 21.5 Million People -- Jul. 2015, NY Times

Target Breach Involved Two-Stage Cyber-Attack
-- steal data from a machine not connected to the Internet
-- move to another machine which can send the data to an FTP (server) – Dec, 2014

• Electric Power System (EPS): does it suffice to just hack into the data networks?
EPS Cyber-Attacks: The Good

• Recent cyber-attacks involve hacking into databases and learning/revealing information.

  - Hacking of Government Computers Exposed 21.5 Million People -- Jul. 2015, NY Times
  - Target Breach Involved Two-Stage Cyber-Attack
    -- steal data from a machine not connected to the Internet
    -- move to another machine which can send the data to an FTP (server) – Dec, 2014

• Data processing at heart of EPS cyber system – data integrity has to be comprised intelligently to cause serious damage.
  • More sophisticated attacks needed to manipulate data
EPS Cyber-Attacks: The Bad

• All networks have zero day vulnerabilities (Target attack testament to that)
  • Successful attacks on communication and computer networks are inevitable

• Intelligent attacks can restrict information flows and availability for real-time response and situational awareness
  • Can combine cyber and physical attacks to create more havoc

• Well designed cyber attacks can mimic information or system loss due to natural disasters

• And will be designed to be unobservable (at least locally within the attack module)
EPS Cyber-Attacks: The Ugly

• Attacks on information sharing networks can quickly lead to cascading failures
  • Can a coordinated attack mimic the Northeast Blackout of 2003?

• Many classes of cyber-attacks – depending on sub-systems attacked
  • Generation, topology, SCADA measurements, AGC, cyber-physical attacks, substation, DER
  • All involve compromising the integrity of cyber data intelligently.

• Availability of intrusion detection decisions (during attack) and resiliency mechanisms (post-attack) crucial for human-operator based cyber systems.
  • One size fits all solution will not work
EPS: Resiliency

• Electric Power Systems are resilient systems built to withstand real-time changes to generation, dispatch, transmission and distribution failures/outages.

• But cyber-attacks and natural disasters can cause an order of magnitude large change to the system in a very short time.

• Can operators manage under partial or complete lack/loss of information?

• Need vulnerability analysis (including attack modeling)
  • What are the consequences of realistic cyber-attacks on the EPS?

• Design of resiliency mechanisms
Cyber attacks on state estimator:


Cyber-attacks on EPS: State of the Art

Cyber attacks on generation control:


Cyber attacks on topology:


Cyber-attacks on EPS: State of the Art

Cyber attacks: impact on markets:


Optimization problem for cyber attacks:

Cyber attacks consequences:


Consequences of unobservable attacks on SE and topology data:

- [1] and [3]: A congested line can be physically overloaded while appearing perfectly normal in the cyber-data
- [2]: Attacks on data-sharing between inter-areas can lead to unobservable overloads and violations.


Cyber-attacks on EPS: ASU-lead Research

- Resiliency mechanisms?

- Large complex systems are only locally unobservable
  - Modular processing can be exploited to detect anomalous and systematic data changes

- Real-time load monitoring and forecasting (machine learning), anomalous re-dispatch monitoring, real-time topology processing, …..


Motivation:

• Data sharing amongst entities in electric grid is essential for reliability.
• Successful cyber attacks on inter-area communications can have serious consequences and should be studied.
• Mimicking outage and information sharing conditions that led to the Northeast blackout in 2003.

Objectives

• Introduce a class of topology-targeted man-in-the-middle communication attacks.
• Study attack consequences using a time progression model for cyber operations.
**System Model and Attack**

- **Attacker capability:** the attacker has access to the data being shared between areas and can corrupt the data:
  - Participate in creating a line outage in one area/ be aware of such an outage
  - Corrupt the topology information shared with the other area.

- **Modeling human error:**
  - Contingency communication delays.
  - Line switch miscommunications.
Event 0:
Line outage in Area 1

Event 1:
Joint dispatch

Event 2:
Joint dispatch

Event 20:
Joint dispatch

0 \rightarrow t \rightarrow 2t \rightarrow \ldots \rightarrow 20t

Event 0:
Line outage in Area 1

Replace the updated topology with old topology

Event 1:
Joint dispatch

Both areas calculate power flow

Event 2:
Joint dispatch

1. Area 1 run local OPF
2. Area 2 run local OPF

Local generation schedule exchange

Share estimated loads

Share tie-line measurements

Share updated topology

1. Area 1 run local OPF
2. Area 2 run local OPF

Lightning represents Topology-targeted MiM attack

Information sharing

SCADA

Topology processing

State estimation

Power flow calculation

OPF Calculation
### Attack Consequences

Tie-line interchange fixed with only 10% variation.

<table>
<thead>
<tr>
<th>Feasible Case</th>
<th>Physical PF Overload</th>
<th>Cyber PF Overload</th>
<th>Non-Convergence of PF</th>
<th>No Violation Cases</th>
<th>Cyber-Physical PF Overload</th>
</tr>
</thead>
<tbody>
<tr>
<td>540</td>
<td>24.82%</td>
<td>14.26%</td>
<td>30.00%</td>
<td>23.33%</td>
<td>7.59%</td>
</tr>
</tbody>
</table>

Table: System behavior with sustained attack for IEEE 24-bus system

![Pie chart indicating attack statistics for IEEE 24-bus system](image)
Countermeasures

• Tie-line power flow mismatch: yet another countermeasure

• Immediate communication of violations between areas following power flow calculation.

• N-1 contingency analysis (over both areas) prior to attack can give a list of local elements whose outage caused the violation in neighboring area.
  • Enable external contingency list sharing between areas. (not widespread)

• Broader issue: information sharing across SEAMS crucial for resiliency and situational awareness.
Resilient Energy Management Systems

• An intelligent cyber attack decision support tool that goes hand in hand with the EMS is needed.
  • Monitors anomalous changes in a systematic manner
  • Existing intelligence in the grid (statistical, operator) etc. can be translated to intelligent machine learning algorithms

• Does PMU data provide additional resiliency?

• Are generator attacks realistic?

• Can voltage and frequency regulation as well as system dynamics be exploited to detect anomalous behavior?
Systematic Resiliency Mechanism

- Cyber attack decision support tool

![Diagram of Cyber Attack Decision Support Tool](image_url)
Questions?
Thank you!
Attack Consequences

• For area with false topology, sustained attacks cause mismatches of the physical power flow and the power flow monitored in cyber level:
  1) Prevent operators from detecting the severity of physical overload problem.
  2) Create false overload alert in cyber level, lead to mis-operation.

• In comparison with using correct topology information (both areas) for dispatch:
  1) Cause more cases with overload problem to occur during simulation time period.
  2) Increase the physical overload severity.
Tested the attack on IEEE 24-bus system and found the following consequences:

- Prevents operators from detecting the severity of physical overload problem.
- Creates false overload alert in cyber level, lead to mis-operation.
- Severe lack of convergence of OPF.
- No violation.
- Cyber-physical overload.

Attack success: % of lines with overflows: 69.08%

- critical attack cases (physical power flow > 105%) is 11.11%.