The Sequential Attack against Power Grid Networks

Yihai Zhu, Jun Yan, Yufei Tang, Yan (Lindsay) Sun, Haibo He

Presenter: Yan (Lindsay) Sun
Associate Professor at
University of Rhode Island
Email: yansun@ele.uri.edu
Massive Blackouts

- **The Electric Grid**
  - Critical infrastructure
  - Complicated cyber-physical systems
  - Experiences of power outages

- **Massive Blackouts**
  - Large-scale power outage
  - Affecting millions of people
  - Tremendous economic loss

- **Northeast Blackout in 2003**
  - 50 million people
  - 10 billion U.S. dollar

Northeast blackout of 2003
Main Causes

Exterior reasons of blackouts affecting at least 50,000 customers between 1984 and 2006. Data from NERC records. [2]
Media Report

- **Truthstream Media** (August 30, 2013)
  
  “The former DHS chief Janet Napolitano says: Cyber Attack Will Bring Down Power Grid: ‘When Not If’ ”

- **The Wall Street Journal** (February 5, 2014)
  
  “Assault on California Power Station Raises Alarm on Potential for Terrorism”
Two Real-life Cases

❖ Case I: The attack from an individual
  ▪ On Oct. 6, 2013, a man attacked a high-voltage transmission line near Cabot, Arkansas, USA.
  ▪ 10,000 customers lost power as a result.

❖ Case II: The attack from a team
  ▪ At the mid night on Apr. 16, 2013, a team of armed people shot on a transmission substation near San Jose, California, USA.
  ▪ 17 giant transformers were knocked out, and this substation was closed for a month.
Power Grid Information Collection

- Ways of Information Collection
  - Online tools
  - Purchasing the grid’s information
  - Hacking or spying

- Online tools are useful to collect the topological information.
  - Google Maps
  - Online websites
    - Topology of the high-voltage transmission lines in U.S.
Outline

- Background
- Related Work
- The Sequential Attack
  - Motivation & Challenge
  - Cascading Failure Simulator
  - A Case Study
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work
Outline

- Background
- Related Work
- The Sequential Attack
  - Motivation & Challenge
  - Cascading Failure Simulator
  - A Case Study
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work
Related Work

Vulnerability Analysis of Power Grids

- Cascading Models\(^{[10,11,12]}\)
- Contingency Analysis\(^{[12]}\)
- Cyber Vulnerability Analysis\(^{[15]}\)
- Defense Analysis\(^{[16]}\)
- Attack Analysis:
  - The simultaneous attack\(^{[13,14]}\)
  - The sequential attack
Outline

➢ Background
➢ Related Work
➢ The Sequential Attack
  ➢ Motivation and Challenge
  ➢ Cascading Failure Simulator
  ➢ A Case Study
  ➢ Vulnerability Analysis
  ➢ Metric Study
➢ Summary & Future Work
The Sequential Attack

❖ Motivation

- The attackers are able to launch multiple-target attacks sequentially, but not simultaneously.
- Provide a new angle to conduct the vulnerability analysis of power transmission systems.

❖ Challenges

- Developing the cascading failure simulator
- Mimicking sequential attacks
- Conducting vulnerability analysis
- Studying metrics to find strong sequential attacks
Cascading Failure Simulator

- **DC power-flow model**
- **Blackout size → damage**
- **Ten steps**
  - Step 1: Initialization
  - Step 2: Apply an attack,
  - Step 3: Check "Stop simulator",
  - Step 4: Redispatch power and recalculate power flows,
  - Step 5: Check "Overloading",
  - Steps 6, 7, 8: Trip one overcurrent line,
  - Step 9: Check "More Attacks",
  - Step 10: Evaluate damage.

Flowchart of cascading failure simulator
IEEE 39 Bus System

< #: Node Index  G#: Generator Index  ↓: Demand Node
A Case Study

- A case study on the combination of lines 26 and 39
  - The simultaneous attack: upper subplot
  - The sequential attack: lower subplot
  - Blue-star points stand for a line trip.

- Observation
  - The sequential attack can discover new vulnerability of power systems.
Vulnerability Analysis

❖ Concept
  ▪ Test benchmark: IEEE 39 bus system that has 39 substations and 46 transmission lines.
  ▪ Damage evaluation: Blackout size ($\lambda$)
  ▪ Analysis on transmission lines

❖ Demonstration
  ▪ Two-line combinations: 1035
  ▪ For each two-line combination, obtaining
    • Its sequential attack strength: $\lambda_{seq}$
    • Its simultaneous attack strength: $\lambda_{sim}$
  ▪ Plot $\lambda_{seq}$ v.s. $\lambda_{sim}$ to reveal the relationship between the sequential attack and the simultaneous attack.
  ▪ Each dot in the figure represents an two-line combination.
**Discovery**

- **Red dots**
  - These dots represent that the non-vulnerable combination of links that corresponds to a weak simultaneous attack can become highly vulnerable when the sequential attack is considered.

- **Three categories**
  - Category II: the sequential attack is much stronger than the simultaneous attack.
  - There are more strong sequential attacks than strong simultaneous attacks

\[
\begin{align*}
\text{Category I: } & \lambda_{seq} - \lambda_{sim} \leq \theta \\
\text{Category II: } & \lambda_{seq} - \lambda_{sim} > \theta \\
\text{Category III: } & \lambda_{seq} - \lambda_{sim} < -\theta \\
\text{When: } & \theta = 0.1
\end{align*}
\]
More experiments and analysis on three-line or four-line combinations

- Two-line combination: 1035 (Category I: 85.6%, Category II: 13.14%, Category III: 1.26%)
- Three-line combinations (15,180)
- Four-line combinations (163,185)

Observation

- The sequential attack can be stronger than the simultaneous attack.
- As k increases, Category II becomes increasingly dominant.
**Metric Study**

- **Goal**
  - It is to study existing metrics to find whether metric(s) can help to reduce the search space for finding strong sequential attacks.

- **Four existing metrics**
  - **Metric 1**: Random selection, determining candidate links by randomly choosing among all links.
  - **Metric 2**: Generator-connection, selecting the links that are connected with generators as candidate links.
  - **Metric 3**: Degree, choosing candidate links by ranking degree values of links from high to low.
  - **Metric 4**: Load, choosing candidate links by ranking load values of links from high to low.
Experiment

- 11 lines for Metric 2, because 11 lines are originally connected with generators.
- 11 lines for Metrics 3 and 4.
- Conducting $k$-line sequential attacks, where $k$ is set be 2, 3, 4, 5 and 6, respectively.
- Randomly choosing $k$ lines for each metric.
- 1000 times and average results.

Observation

- Metric 4: load
  - Strong performance
  - Reducing search space
Summary & Future Work

- **Summary**
  - Discover the sequential attack scenario against power transmission systems.
  - Discover many new vulnerabilities.
  - Investigate four existing metrics on reducing the search space to find strong sequential attacks.

- **Future Work**
  - Investigate the sequential attack on substations.
  - Investigate the sequential attack strategy.


The simultaneous attack versus the sequential attack

- **The simultaneous attack**
  - Conduct multiple removals simultaneously.

- **The sequential attack**
  - Conduct multiple removals in the predefined sequence.
Summary of typical works in studying the attacks against power systems

<table>
<thead>
<tr>
<th>Attack Strategy</th>
<th>Single-node Synchronous</th>
<th>Multiple-node Synchronous</th>
<th>Multiple-node Sequential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random removal [25]</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Search-based approaches [4]</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Attack metrics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Degree [25]</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Load [21]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>RIF [9]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LDV [10]</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Geographic information [12]</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RG [11]</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Proposed work</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
## Models of Cascading Failures

<table>
<thead>
<tr>
<th>Models of Cascading Failures</th>
<th>Models of Cascading Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CASCADE mode</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Randomly choosing load values between a range</strong></td>
</tr>
<tr>
<td><strong>Overloading when the load exceeds a threshold.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Wang-Rong model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Using the degree to calculate load</strong></td>
</tr>
<tr>
<td><strong>Overloading when the load exceeds the capacity.</strong></td>
<td><strong>The capacity is proportional to the initial load.</strong></td>
</tr>
<tr>
<td><strong>Motter-Lai model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Calculating the betweenness as the load</strong></td>
</tr>
<tr>
<td><strong>Overloading when the load exceeds the capacity</strong></td>
<td><strong>The capacity is proportional to the initial load.</strong></td>
</tr>
<tr>
<td><strong>Betweenness model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Calculating the betweenness to calculate the load</strong></td>
</tr>
<tr>
<td><strong>Overloading when the load exceeds a threshold.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Efficiency model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Calculating the betweenness as the load.</strong></td>
</tr>
<tr>
<td><strong>Overloading components can be recovered.</strong></td>
<td><strong>Network efficiency</strong></td>
</tr>
<tr>
<td><strong>Extended model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Identical components</strong></td>
<td><strong>Calculating the extended betweenness as the load, based on PTDFs.</strong></td>
</tr>
<tr>
<td><strong>Overloading when the load exceeds the capacity.</strong></td>
<td><strong>Net-ability</strong></td>
</tr>
<tr>
<td><strong>Hines model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Substation type</strong></td>
<td><strong>Line impedance</strong></td>
</tr>
<tr>
<td><strong>DC power flows</strong></td>
<td><strong>Calculating DC power flows</strong></td>
</tr>
<tr>
<td><strong>Generation dispatch and load shedding</strong></td>
<td><strong>Trip lines due to overheat.</strong></td>
</tr>
<tr>
<td><strong>Blackout Size</strong></td>
<td></td>
</tr>
<tr>
<td><strong>OPA model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Substation type</strong></td>
<td><strong>Line impedance</strong></td>
</tr>
<tr>
<td><strong>DC power flows</strong></td>
<td><strong>Calculating DC power flows</strong></td>
</tr>
<tr>
<td><strong>Probability of line failure</strong></td>
<td><strong>Generation dispatch and load shedding</strong></td>
</tr>
<tr>
<td><strong>Trip lines with probability.</strong></td>
<td><strong>Both fast and slow dynamics</strong></td>
</tr>
<tr>
<td><strong>Hidden failure model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Substation type</strong></td>
<td><strong>Line impedance</strong></td>
</tr>
<tr>
<td><strong>DC power flows</strong></td>
<td><strong>Calculating DC power flows</strong></td>
</tr>
<tr>
<td><strong>Probability of line failure</strong></td>
<td><strong>Generation dispatch and load shedding</strong></td>
</tr>
<tr>
<td><strong>Trip lines with probability.</strong></td>
<td><strong>Hidden failures</strong></td>
</tr>
<tr>
<td><strong>Manchester model</strong></td>
<td><strong>Topology</strong></td>
</tr>
<tr>
<td><strong>Substation type</strong></td>
<td><strong>Line impedance</strong></td>
</tr>
<tr>
<td><strong>AC power flows</strong></td>
<td><strong>Calculating AC power flows</strong></td>
</tr>
<tr>
<td><strong>Tripping lines</strong></td>
<td><strong>System convergence</strong></td>
</tr>
<tr>
<td><strong>Fast dynamics</strong></td>
<td></td>
</tr>
</tbody>
</table>
Attackers and Means of Attacks

**Attackers**
- Disgruntled individuals
- Terrorist teams
- Computer hackers
- Energy companies
- Hostile Countries

**Attacker can be from inside and outside.**

**Attackers can well organize the attacks, aiming to cause large damage.**

**Means of Attacks**
- Physical sabotages
  - Failing down poles that support high-voltage transmission lines.
  - Cutting a tree to fail a line
  - Fire on substations
  - Air force attacks
  - EMP attacks
  - Etc.

- Cyber intrusions
  - Cyber attacks
  - Cyber worms
  - Etc.
Cyber Attacks

Simulated Cyber Attack

- Name: Aurora Generator Test
- Participants: Idaho National Laboratories (INL) and Department of Homeland Security, USA
- Time: 2007
- Object: A large diesel-electric generator
- Procedure: Researchers sent malicious commands to force the generator overheat and shut down.
- Results: the generator was completely destroyed.
- Effects: Cyber vulnerabilities of many generators that are currently in use in USA.
Commercially Available

Bay Area power grid

Platts.com

GIS raw data