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

THE UNIVERSITY OF RHODE ISLAND NEST C I S A

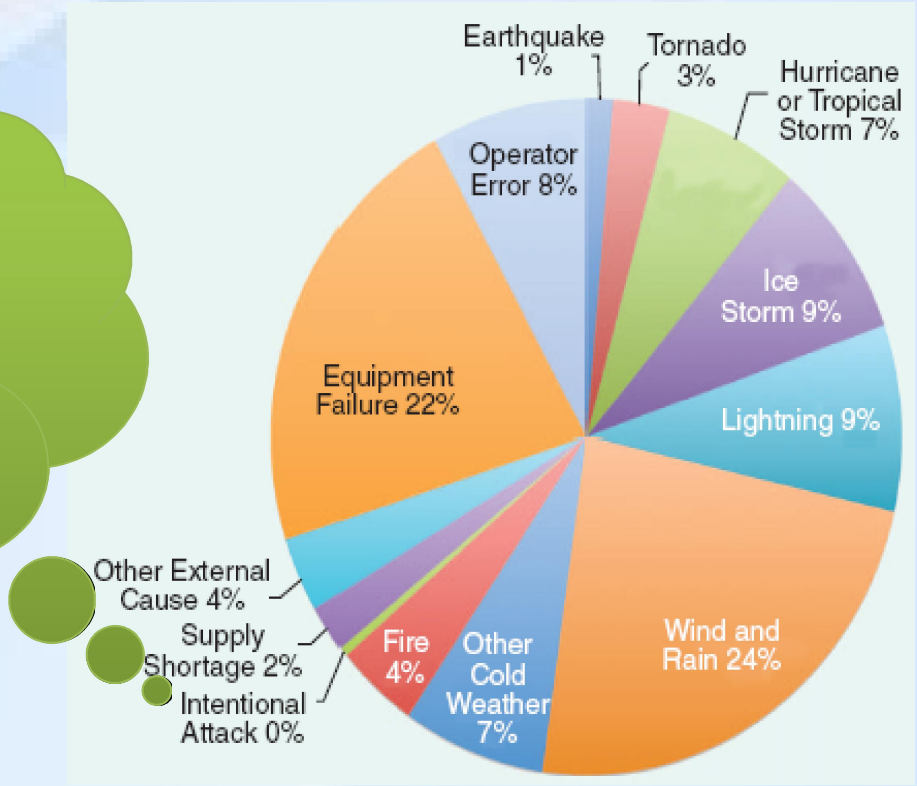
Massive Blackouts

- **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** [1]
  - 50 million people
  - 10 billion U.S. dallor

Northeast blackout of 2003

Main Causes

Attack



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)

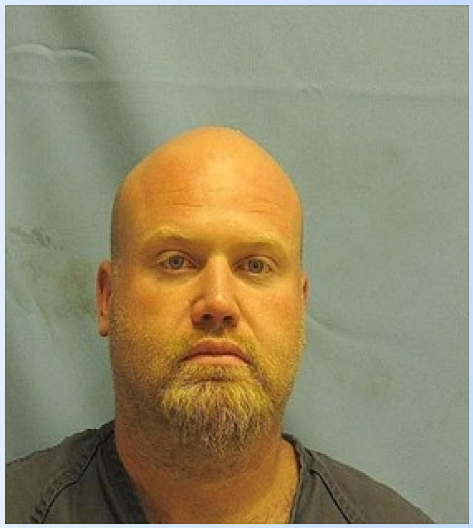
  "The former DHS chief Janet Napolitano says: Cyber Attack Will Bring Down Power Grid: 'When Not If' "

- **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.



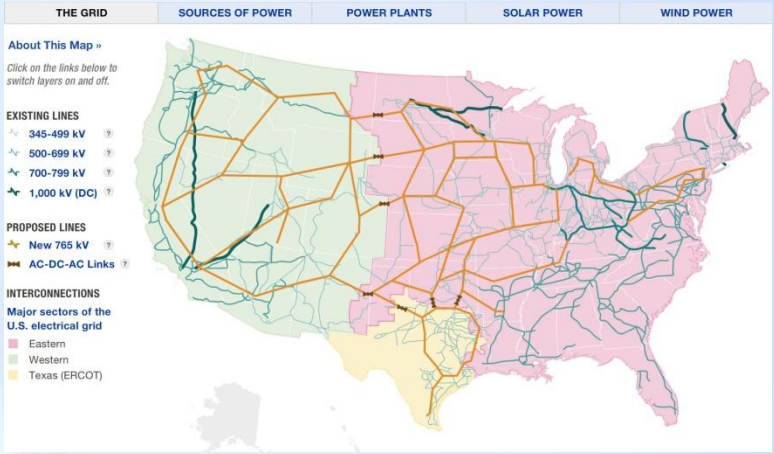
Jason Woodring

- **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.

Substation from Google Map



Visualizing the U.S. Electric Grid

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

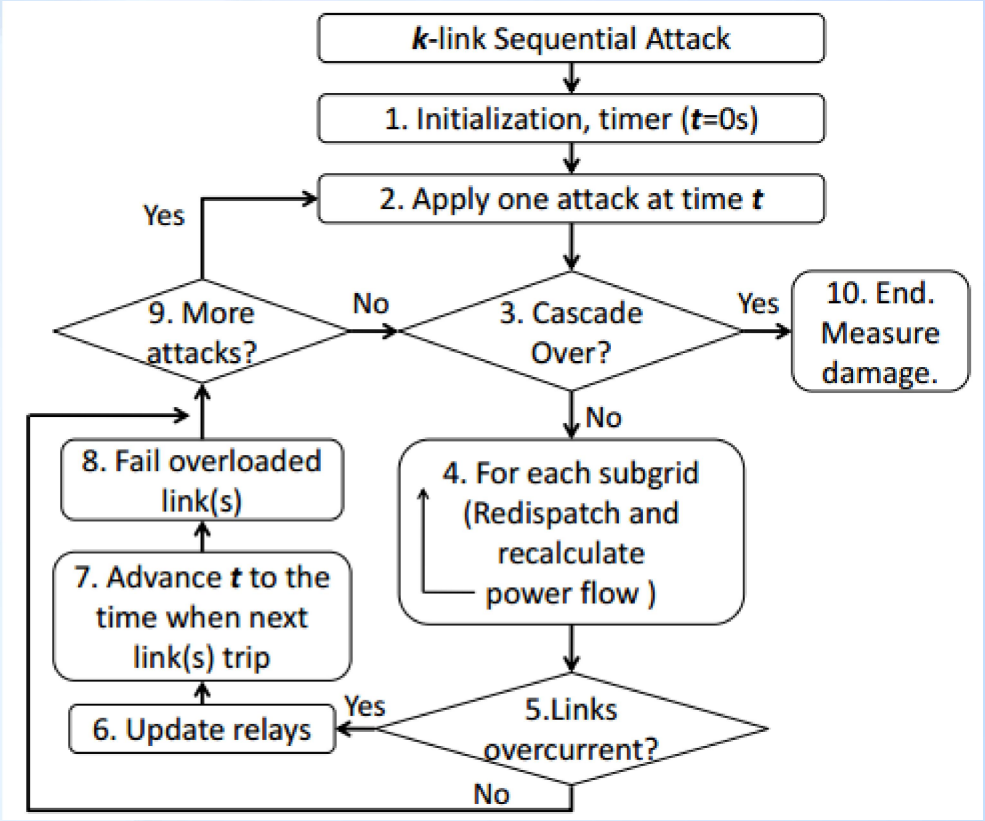
- Background
- Related Work
- The Sequential Attack
  - Motivation and Challenge
  - Cascading Failure Simulator
  - A Case Study
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work

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

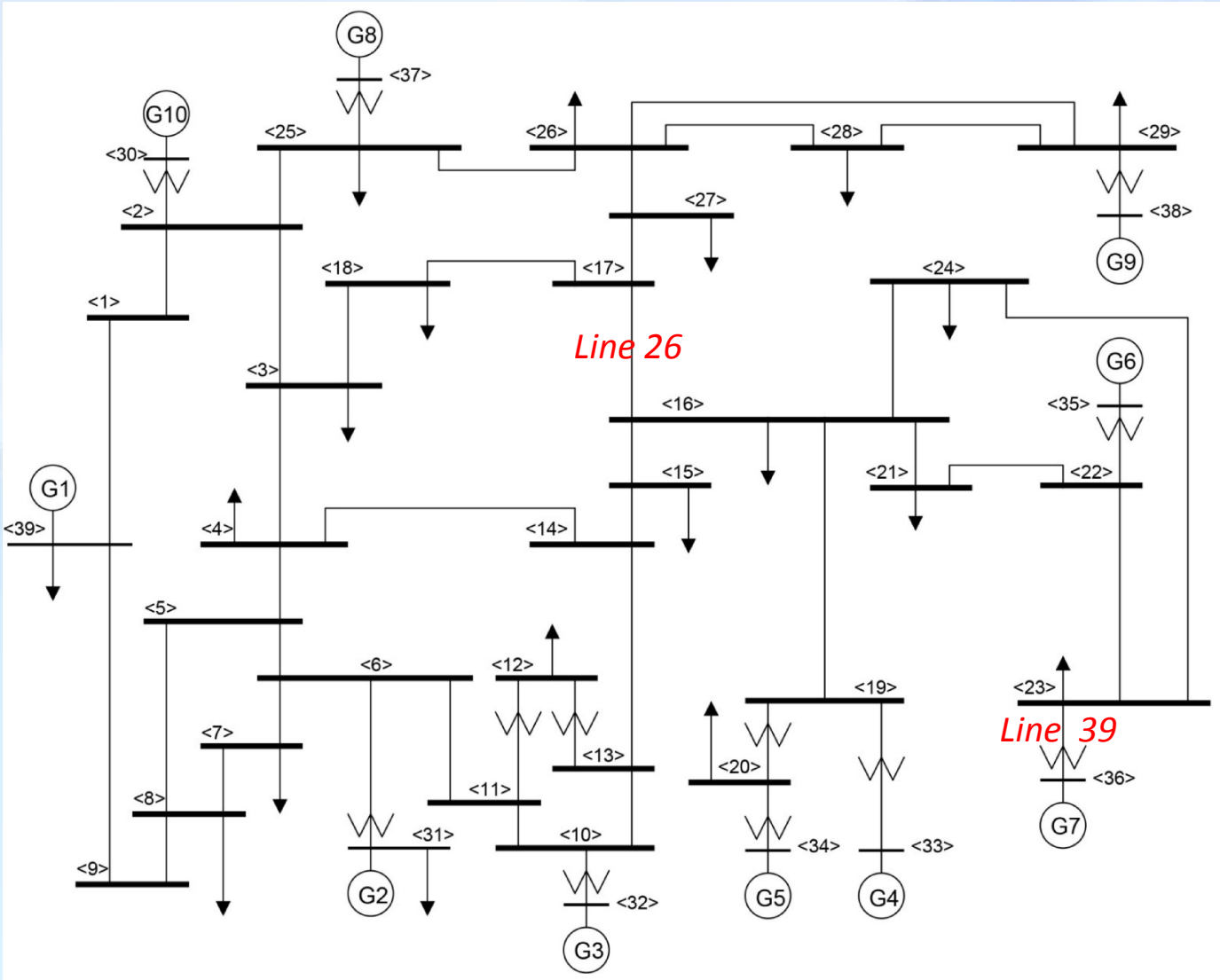
Cascading Failure Simulator

- **DC power-flow model**
- **Blackout size → damage**
- **Ten steps**
  - Step 1: Initialization
  - Step 2: Apply an attack,
  - Step 3: Check "Stop simulator",
  - Step 4: Redispath 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

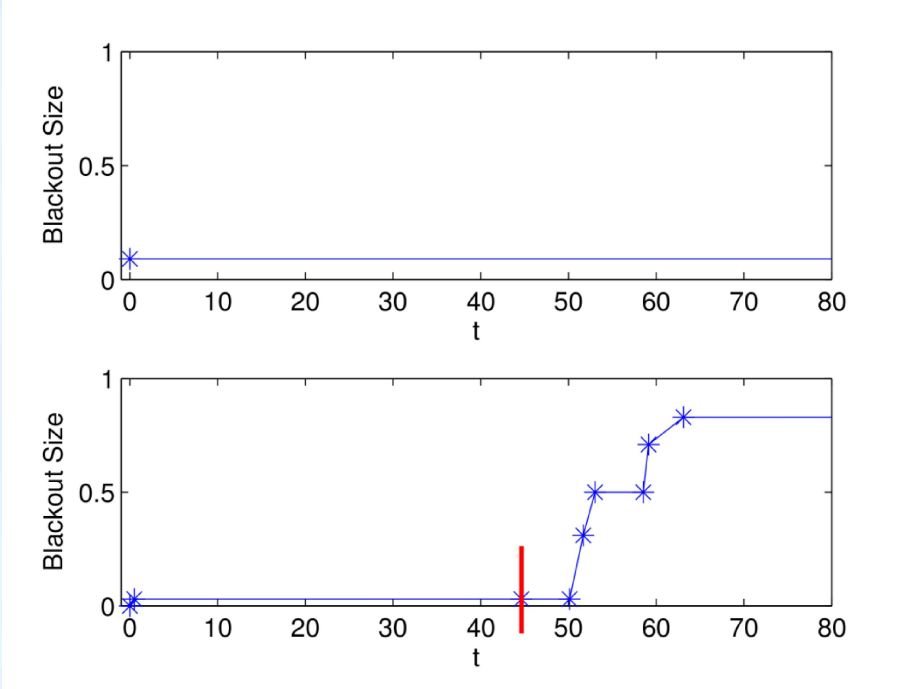
IEEE 39 Bus System



< #>: 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.



The case study

Vulnerability Analysis

❖ Concept

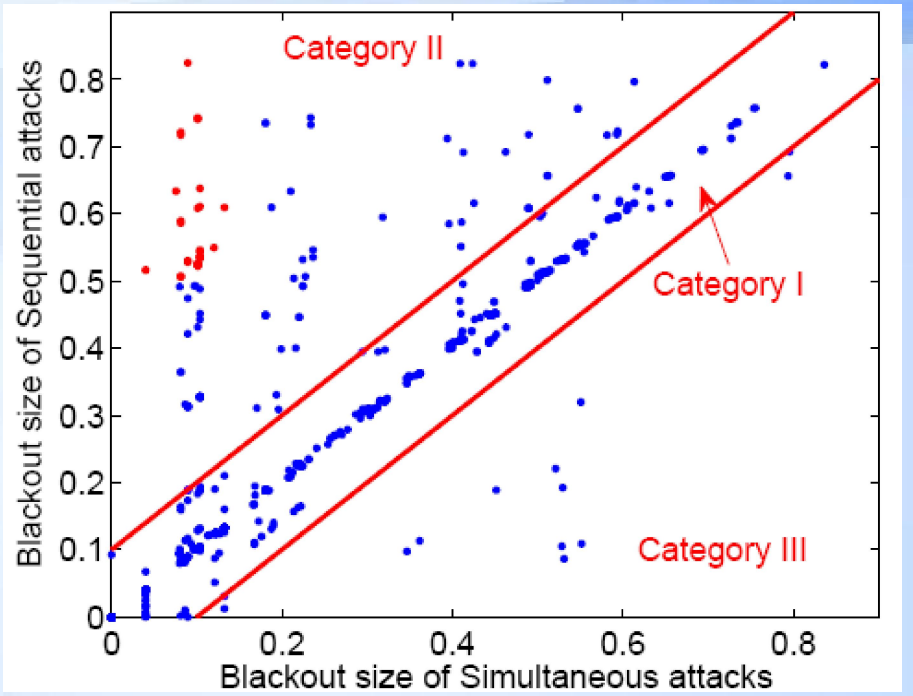
- Test benchmark: IEEE 39 bus system that has 39 substations and 46 transmission lines.
- Damge evaluation: Blackout size (λ)
- Analysis on transmission lines

❖ Demonstration

- Two-line combinations : 1035
- For each two-line combination, obtaining
  - Its sequential attack strength: λ_{seq}
  - Its simultaneous attack strength: λ_{sim}
- Plot λ_{seq} v.s. λ_{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 reprent 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



Relationship between the sequential attack and the simultaneous attack

$$\begin{cases} \text{Category I}: |\lambda_{seq} - \lambda_{sim}| \le \theta \\ \text{Category II}: \lambda_{seq} - \lambda_{sim} > \theta \\ \text{Category III}: \lambda_{seq} - \lambda_{sim} < -\theta \\ When: \theta = 0.1 \end{cases}$$

k-link	Category I	Category II	Category III
$k = 2$	85.6%	**13.14%**	1.26%
$k = 3$	69.57%	**28.83%**	1.6%
$k = 4$	52.45%	**46.24%**	1.32%

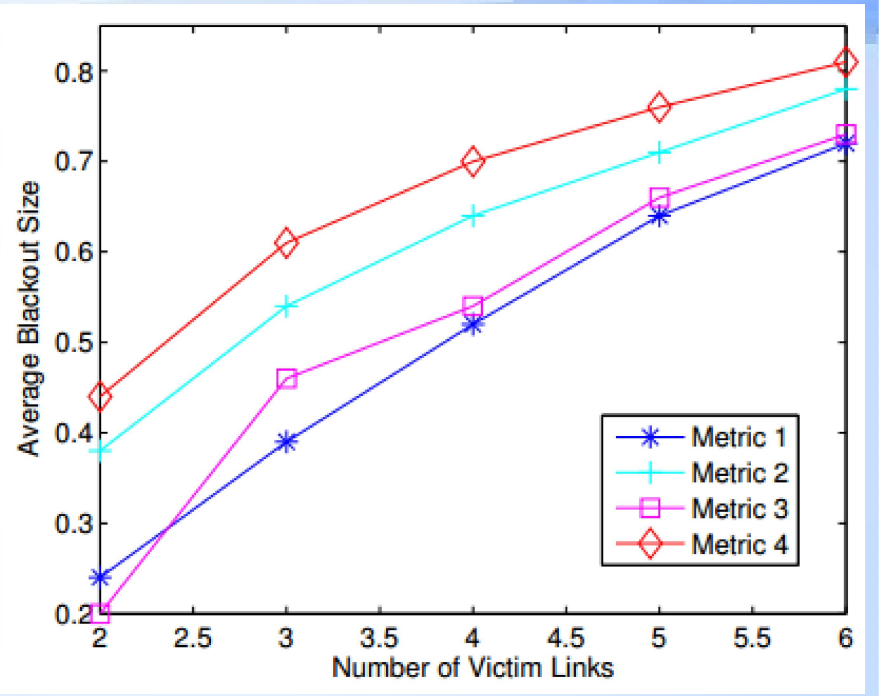
- **More experiments and analysis on three-line or four-line combinations**
  - Two-line combination: 1035 (Category I: 85.6%, Category II: 13.14%, Category III: 1.26%)
  - Three-line combinations (15,180)
  - Four-line combinations (163,185)
- **Observation**
  - The sequential attack can be stronger 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 chooing ***k*** lines for each metric.
- 1000 times and average results.



Performance Comparison

❖ Observation

- Metric 4: load
  - Strong performance
  - Reducing search space

Comparison of the search space between metric 1 and metric 4

	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$
Metric 1 $\binom{46}{k}$	1,035	15,180	163,185	1,370,754	9,366,819
Metric 4 $\binom{11}{k}$	55	165	330	462	462

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.

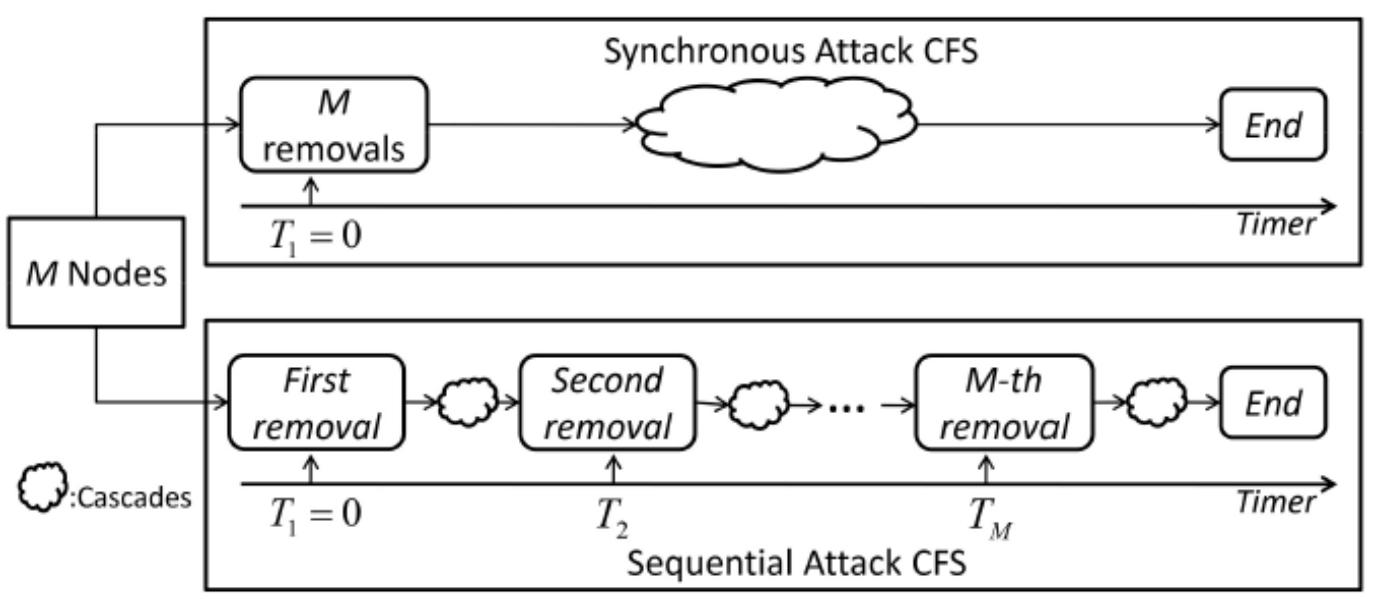
Reference

1. U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.
2. Paul Hines, “Cascading failures in power grids”, IEEE Potentials, vol. 28, no. 5, pp. 24–30, 2009
3. “FBI, joint terrorism task force arrest suspect in arkansas power grid attacks," 2013. [Online]. Available: http://www.forbes.com/
4. R. Smith, "Assault on california power station raises alarm on potential for terrorism," Feb.18 2014. [Online]. Available: http://online.wsj.com/
5. C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, ”Intruders in the grid,“ IEEE Power and Energy Magazine, vol. 10, no. 1, pp. 58{66, Jan. 2012.
6. M. Levine, “Outgoing dhs secretary janet napolitano warns of serious cyber attack, unprecedented natural disaster," Aug.27 2013. [Online]. Available: http://abcnews.go.com/.
7. “Small-scale power grid attack could cause nationwide blackout, study says,” Mar.13 2014. [Online]. Available: FoxNews.com
8. J. Tollefson, “US electrical grid on the edge of failure," Nature News and Comment, Aug.25 2013
9. A. Kredo, “U.S. electric grid inherently vulnerable to sabotage," Apr.8 2014. [Online]. Available: http://freebeacon.com/author/adam-kredo/

10. S. Mei, X. Zhang, and M. Cao, Power Grid Complexity. Beijing: Tsinghua University Press, 2011.
11. E. Bompard, D. Wu, and F. Xue, “Structural vulnerability of power systems: A topological approach,” Electrical Power Systems Research, vol. 81, pp. 1334–1340, 2011.
12. M. Vaiman, et al, “Risk assessment of cascading outages: Methodologies and challenges," IEEE Transactions on Power Systems, vol. 27, no. 2, pp. 631-641, 2012.
13. W. Wang, Q. Cai, Y. Sun, and H. He, “Risk-aware attacks and catastrophic cascading failures in U.S. power grid,” in IEEE Global Telecommunications Conference, Houston, TX, USA, Dec.5-9 2011.
14. P. Hines, E. Cotilla-Sanchez, and S. Blumsack, “Do topological models provide good information about electricity infrastructure vulnerability?” Chaos, vol. 20, no. 3, 2010.
15. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M., "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *Smart Grid, IEEE Transactions on* , vol.4, no.2, pp.847,855, June 2013
16. M X. Liu, K. Ren, Y. Yuan, Z. Li, and Q. Wang, “Optimal budget deployment strategy against power grid interdiction,” in INFOCOM, 2013 Proceedings IEEE, Turin, Italy, Apr.14-19 2013.

The simultaneous attack versus the sequential attack

- **The simultaneous attack**
  - Conduct multiple removals simultaneously.
- **The sequential attack**
  - Conduct multiple removals in the predefined sequence.



Comparison between the simultaneous attack and the sequential attack

Summary of typical works in studying the attacks against power systems

Attack Strategy		Single-node Synchronous	Multiple-node Synchronous	Multiple-node Sequential
Random removal [25]		✓	✓	
Search-based approaches [4]		✓	✓	
Attack metrics	Degree [25]	✓	✓	
	Load [21]	✓	✓	
	RIF [9]	✓	✓	
	LDV [10]		✓	
	Geographic information [12]		✓	
	RG [11]	✓	✓	
	Proposed work			✓

Models of Cascading Failures

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

Attackers and Means of Attacks

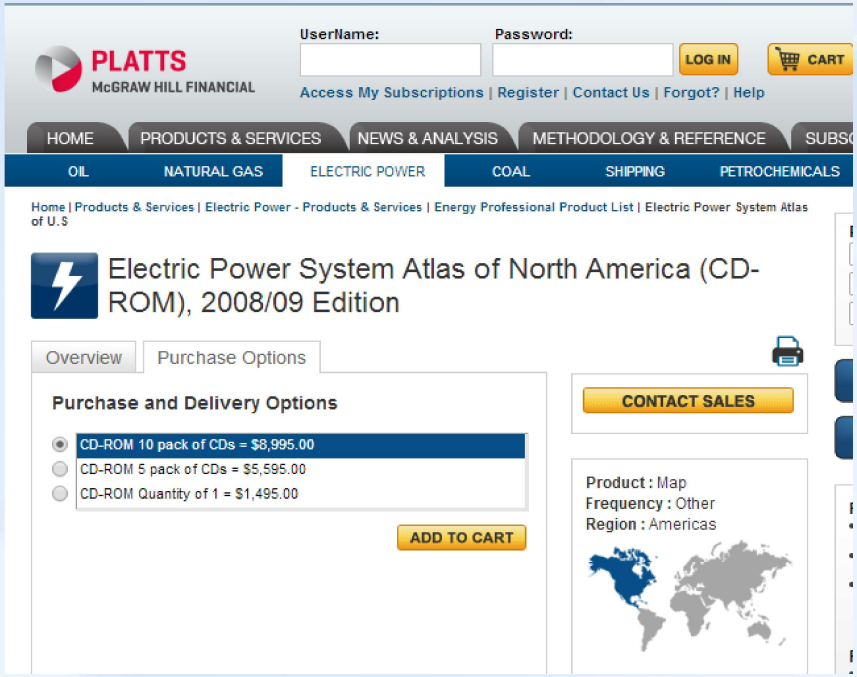
- **Attackers**
  - Disgruntled individuals
  - Terrorist teams
  - Computer hackers
  - Energy companies
  - Hostile Countries
- **Attacker can be from inside and outside.**
- **Attackers can well organize the attacks, aiming to cause large damage.**

- **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 sentmalicious commands to force the generator overheat and shut down.
  - Results: the generator was completely destroyed.
  - Effects: Cyber vulnerabilities of many generators that are currely in use in USA.

Commercially Available



Platts.com

FID	Shape	CHARID	NAME	COMPANY	COMPID	MAXKV	CIRCUITS	POS_REL	SUBID	ASTATUS
0	Point	3337420229	Pajaro Valley	Unknown	-99	0	0	Not verified to be within 1 mile	3337420229	-1
1	Point	3337432042	Watsonville	Pacific Gas and Electric Co.	100540	69	3	Within 40 feet	3337432042	9
2	Point	3337432043	Watsonville Cogeneration Partn	Unknown	-99	69	0	Not verified to be within 1 mile	3337432043	-1
3	Point	3337408226	Buena Vista Landfill	Unknown	-99	0	0	Not verified to be within 1 mile	3337408226	-1
4	Point	3365669834	Buena Vista Landfill		-99	0	0	Not verified to be within 1 mile	3365669834	-1
5	Point	3341135614	Tap	Pacific Gas and Electric Co.	100540	69	3	Within 1 mile	3341135614	8
6	Point	3341135615	Erta	Pacific Gas and Electric Co.	100540	69	1	Within 1 mile	3341135615	8
7	Point	3337413924	Green Valley	Pacific Gas and Electric Co.	100540	115	7	Within 40 feet	3337413924	8
8	Point	3337426023	Tap	Pacific Gas and Electric Co.	100540	115	3	Within 40 feet	3337426023	8
9	Point	3337422061	Rob Roy	Pacific Gas and Electric Co.	100540	115	1	Within 40 feet	3337422061	8
10	Point	3337420437	Paul Sweet	Pacific Gas and Electric Co.	100540	115	2	Within 165 feet	3337420437	8
11	Point	3337429483	UC Santa Cruz Cogeneration	Unknown	-99	0	0	Not verified to be within 1 mile	3337429483	-1
12	Point	3360294987	Unknown		-99	-99	1	Within 40 feet	3360294987	7
13	Point	3337413473	Gilroy (CPN)	Pacific Gas and Electric Co.	100540	115	3	Within 40 feet	3337413473	9
14	Point	3337413474	Gilroy Energy Co.	Pacific Gas and Electric Co.	100540	10	1	Within 40 feet	3337413474	-1
15	Point	3337416916	Llagas	Pacific Gas and Electric Co.	100540	115	3	Within 1 mile	3337416916	8
16	Point	3337426018	Tap	Pacific Gas and Electric Co.	100540	115	3	Within 40 feet	3337426018	8
17	Point	3337426019	Tap	Pacific Gas and Electric Co.	100540	115	3	Within 165 feet	3337426019	8
18	Point	3341135624	Lone Star		-99	69	1	Within 40 feet	3341135624	8
19	Point	3341135625	Tap	Pacific Gas and Electric Co.	100540	69	3	Within 40 feet	3341135625	8
20	Point	3337408555	Camp Evers	Pacific Gas and Electric Co.	100540	115	2	Within 1 mile	3337408555	8
21	Point	3341135626	Crusher	Pacific Gas and Electric Co.	100540	69	1	Within 1 mile	3341135626	8
22	Point	3341135627	Pt. Moretti	Pacific Gas and Electric Co.	100540	69	1	Within 1 mile	3341135627	8

GIS raw data

Bay Area power grid