Coordinated Attacks against Substations and Transmission Lines in Power Grids

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

Presenter: Yihai Zhu, Ph.D.

University of Rhode Island

Email: yhzhu@ele.uri.edu

THE UNIVERSITY OF RHODE ISLAND

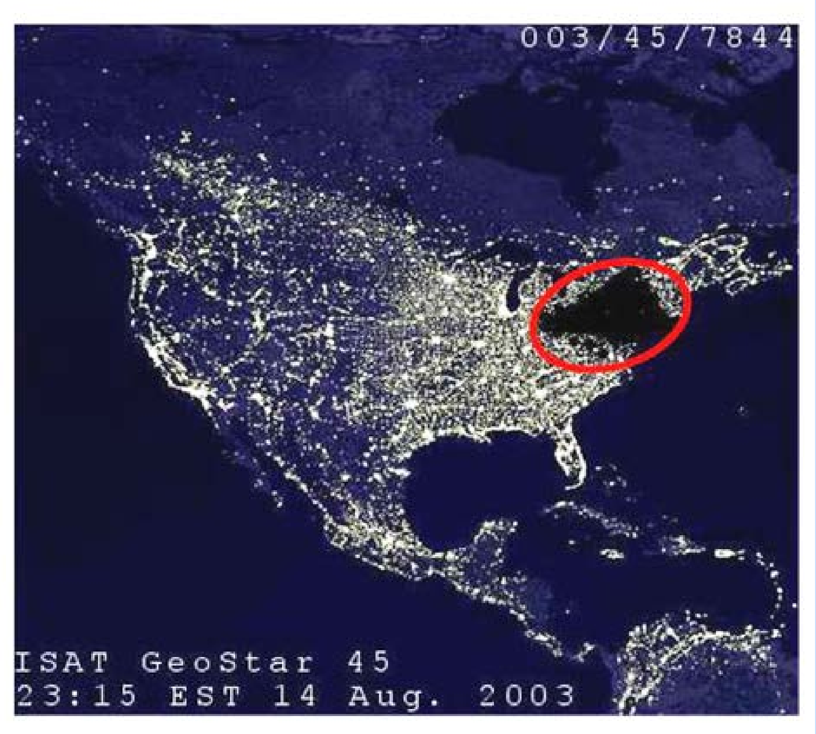
NEST

IEEE GLOBECOM 2014 GLOBAL COMMUNICATIONS CONFERENCE EXHIBITION & INDUSTRY FORUM

AUSTIN, TX USA
★ 8-12 DECEMBER 2014 ★
THE GREAT STATE OF COMMUNICATIONS

Massive Blackouts

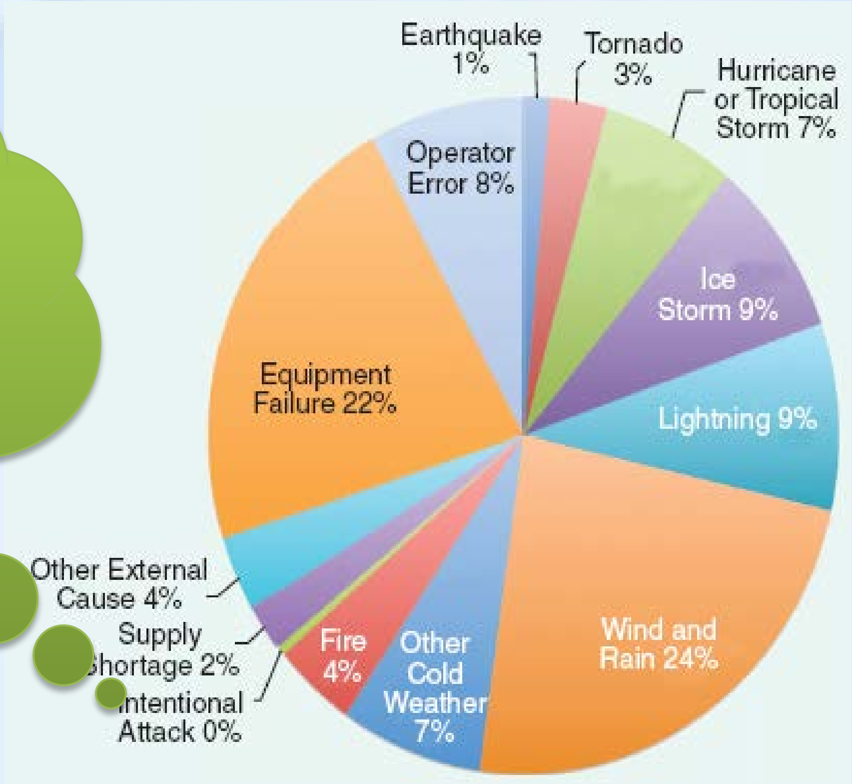
- **Power Grids**
  - Critical infrastructures
  - Experiences of power outages
- **Massive Blackouts**
  - Large-scale power outage
  - Affecting millions of people
  - Tremendous economic loss
- **Northeast Blackout in 2003** [1]
  - 50 million people
  - 10 billion U.S. dollar



The 2003 Northeast Blackout as a seen from space (NASA provided)

Reasons of Power Outages

Attacks



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) [3]

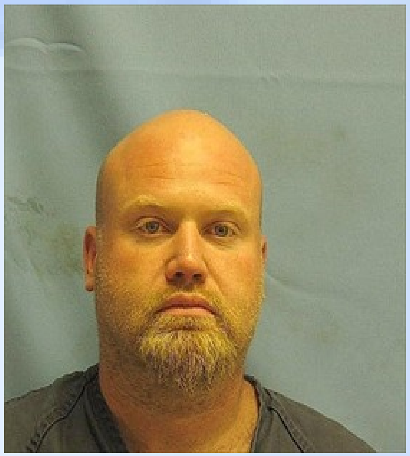
  "The former DHS chief Janet Napolitano says: Cyber Attack Will Bring Down Power Grid: 'When Not If' "

- **The Wall Street Journal** (February 5, 2014) [4]

  "Assault on California Power Station Raises Alarm on Potential for Terrorism"

Two Real-life Cases

- **Case I: The attack from an individual** [5]
  - On Oct. 6, 2013, a man attacked a high-voltage transmission line near Cabot, Arkansas, USA.
  - 10,000 customers lost power.



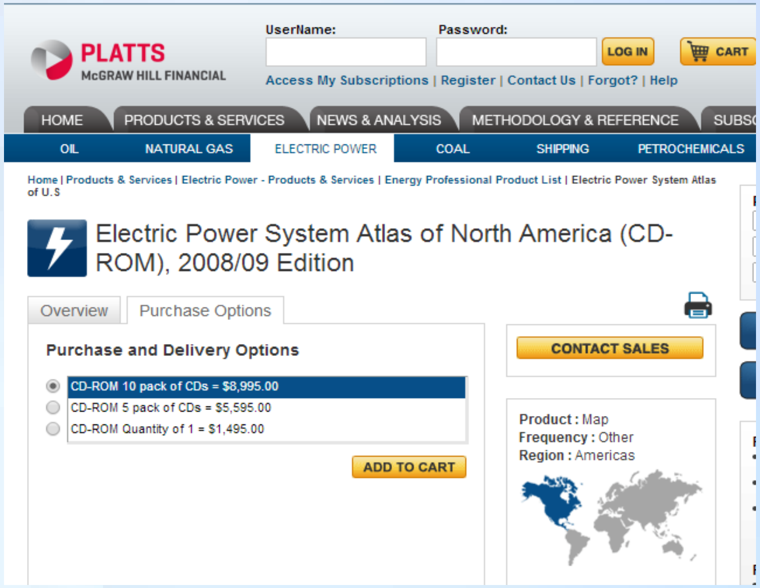
Jason Woodring

- **Case II: The attack from a team** [6]
  - On Apr. 16, 2013, a team of armed people shot on a substation near San Jose, California, USA.
  - 17 giant transformers were knocked out, and this substation was closed for a month.
- **Case III: Simulated Cyber attacks** [7]
  - Aurora Generator Test in 2007: A diesel-electric generator is destroyed.

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



Platts.com

Outline

- Background
- Related Work
- Joint substation-transmission line Attack
  - Motivation & Challenge
  - Cascading Failure Simulator
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work

Outline

- Background
- Related Work
- Joint substation-transmission line Attack
  - Motivation & Challenge
  - Cascading Failure Simulator
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work

Related Work

Vulnerability Analysis of Power Grids

Cascading Failure Models[10,11,12]

Contingency Analysis[12]

Cyber Vulnerability Analysis[16]

Defense Analysis[17]

Attack Analysis:

- Substation-only attack [13,14]
- Transmission-line only attack [15]
- Joint substation-transmission line attack

Outline

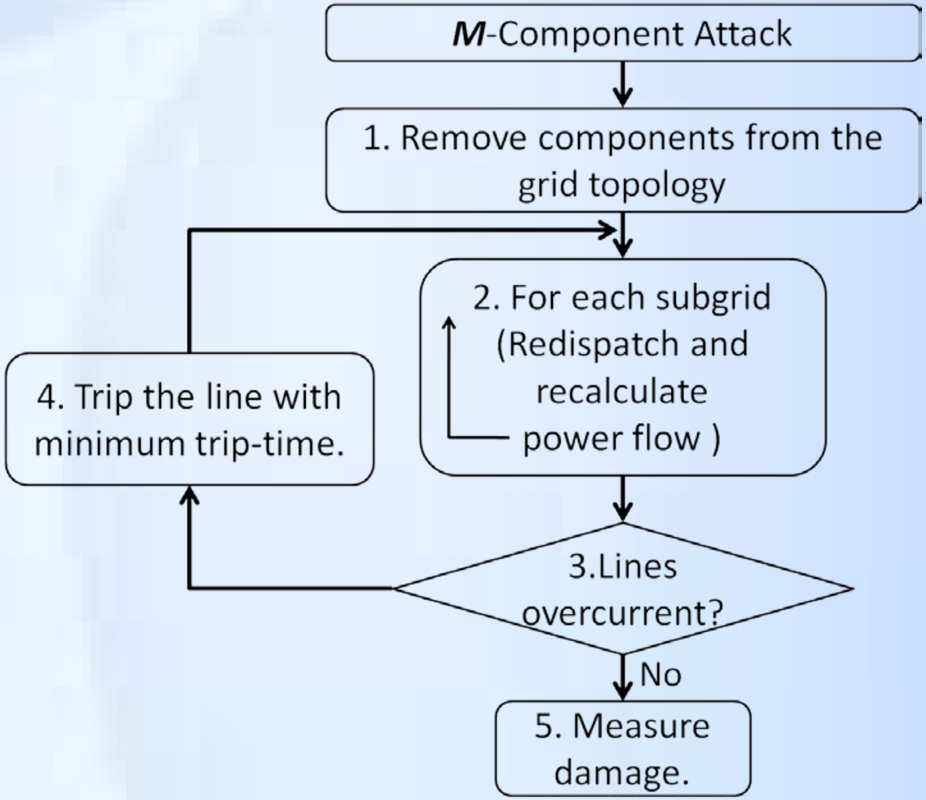
- Background
- Related Work
- Joint substation-transmission line Attack
  - Motivation & Challenge
  - Cascading Failure Simulator
  - Vulnerability Analysis
  - Metric Study
- Summary & Future Work

Joint substation-transmission line Attack

- **Motivation**
  - The attackers are able to launch multiple-target attacks against both substations and lines.
  - Provide a new angle to conduct the vulnerability analysis of power transmission systems.
- **Challenges**
  - Model development
  - Conducting vulnerability analysis
  - Studying metrics to find strong joint substation-transmission line attacks

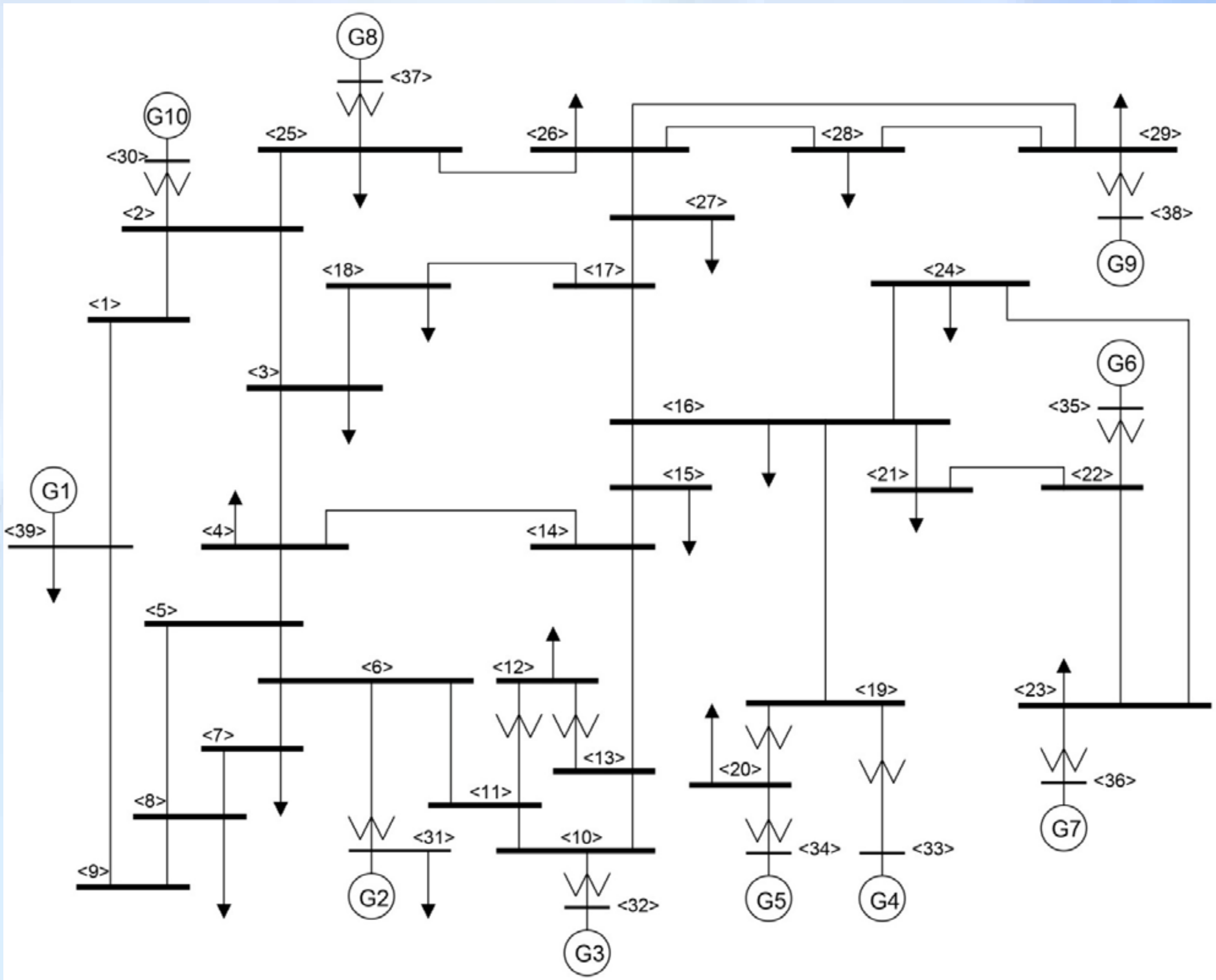
Cascading Failure Simulator

- **DC power-flow model** [14]
- **Five steps**
  - Step 1: Conduct *M*-component attacks.
  - Step 2: Build subgrids, and redispatch power and recalculate power flows.
  - Step 3: Check overloading lines. If NO, goes to Step 5.
  - Step 4: Trip the line with minimum trip-time, and goes to Step 2.
  - Step 5: Evaluate the damage.
- **Assessment measure**
  - Blackout size (***B***): total power loss, normalized to 0 ~ 100% .



Flowchart of cascading failure simulator (CFS)

Test benchmark: IEEE 39 Bus System



< #>: Substation Index (G#): Generator Index ↓ : Demand Substation

39 substations (10 generators and 21 demand substations), and 46 transmission lines

Vulnerability Analysis

❖ Concepts

- Power grid → Network (Substation → node; line → link)
- A *M-component combination* consists of *M* network components (nodes, links, or both).
  - Node-only combination: *M* nodes
  - Link-only combination: *M* links
  - Joint-node-link combination: *M* components, but at least one node and one link
- For one *M-component combination* → Blackout size (***B***).

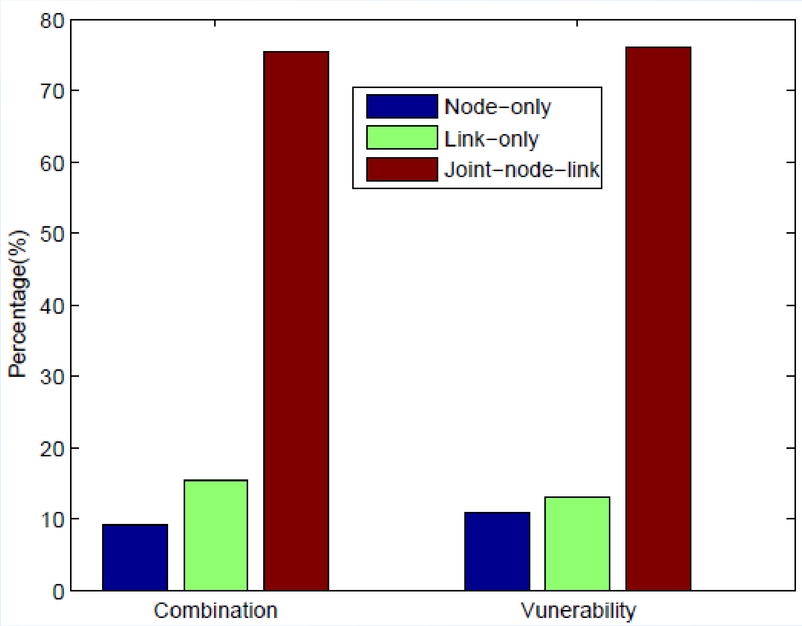
  B value is called the strength of this combination attack.
- Vulnerability: the combination that can yield large attack strength. In particular, $B \geq \eta$ (eta is the threshold.)
- Three types of vulnerability: Node-only vulnerabilities, Link-only vulnerabilities, Joint-node-link vulnerabilities

❖ Demonstration of Vulnerabilities

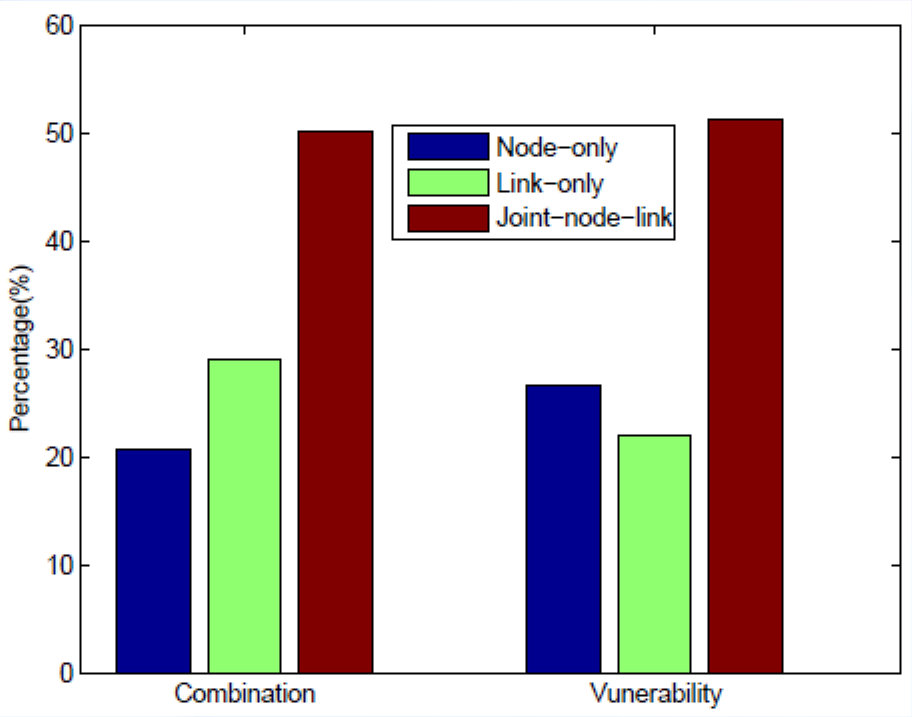
- IEEE 39 bus system(39 nodes & 46 links→ 85 components)
- Let *M = 3,*
  - Node-only combinations: $\binom{39}{3} = 9{,}139$
  - Link-only combinations: $\binom{46}{3} = 15{,}180$
  - Joint-node-link combinations:

$$\binom{85}{3} - \binom{39}{3} - \binom{46}{3} = 74{,}451$$

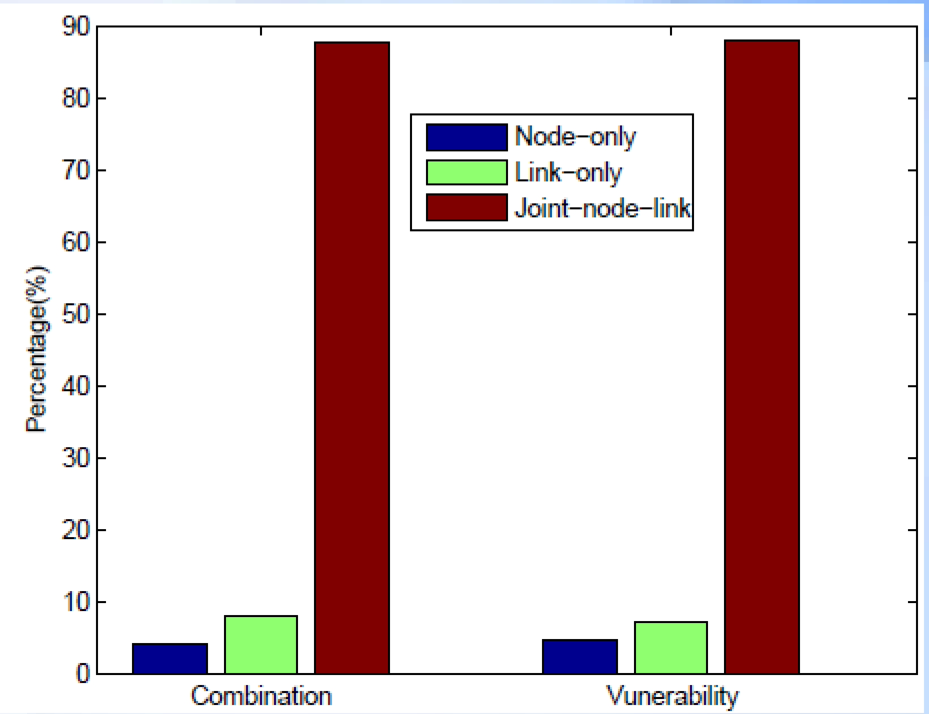
- Use CFS to obtain attack strength (***B***) for each combination and set eta to be 0.2 (20% of power loss)
  - Node-only vulnerabilities: 7,406 (10.96%)
  - Link-only vulnerabilities: 8,780 (12.98%)
  - Joint-node-link vulnerabilities : 51,416 (76.06%)



Percentage comparison regarding *three-component* combinations and vulnerabilities



Percentage comparison regarding *two-component* combinations and vulnerabilities



Percentage comparison regarding *four-component* combinations and vulnerabilities

❖ Observation

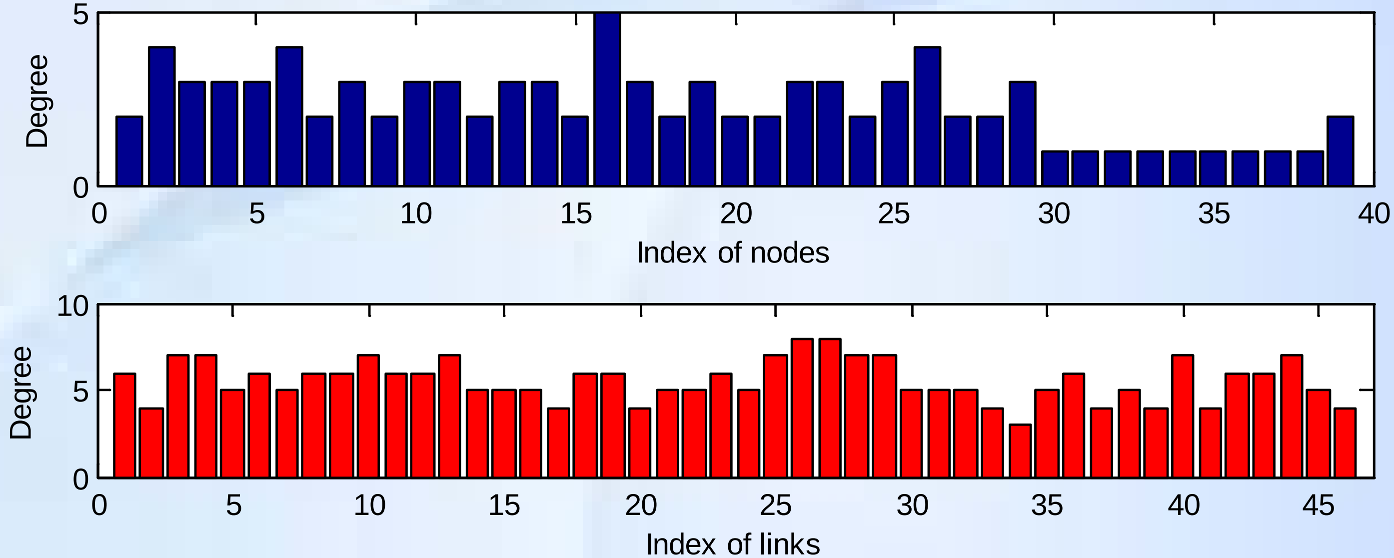
- Joint-node-link vulnerabilities take the largest portion of all vulnerabilities and are critical to the power grid.
- As M increases, Joint-node-link vulnerabilities increase sharply and provide more chances to find strong attacks.

Metric Study

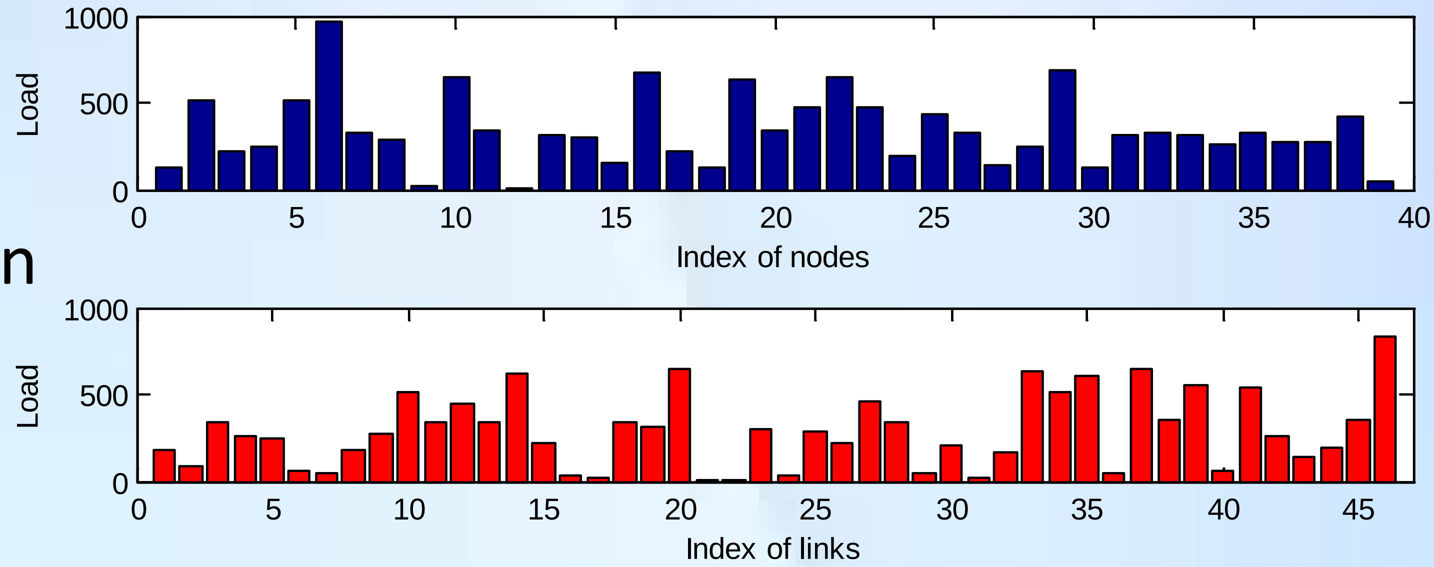
- **Goal**
  - Study existing metrics to identify strong Joint-node-link targeted attack strategies.
- **Two existing metrics**
  - ***Metric 1***: Degree
    - *Degree of a node*: the number of links connecting to this node
    - *Degree of a link* : the summation of two nodes' degree. These two nodes are connected by this link.
  - ***Metric 2***: Load:
    - *Load of a link*: the power flow goes through this link.
    - *Load of a node*: the summation of all power flows going through the links connecting to this node.

Distribution of Degree and Load on IEEE 39 Bus System

Degree distribution



Load distribution



Metric Study

❖ Degree-based Attack Strategies

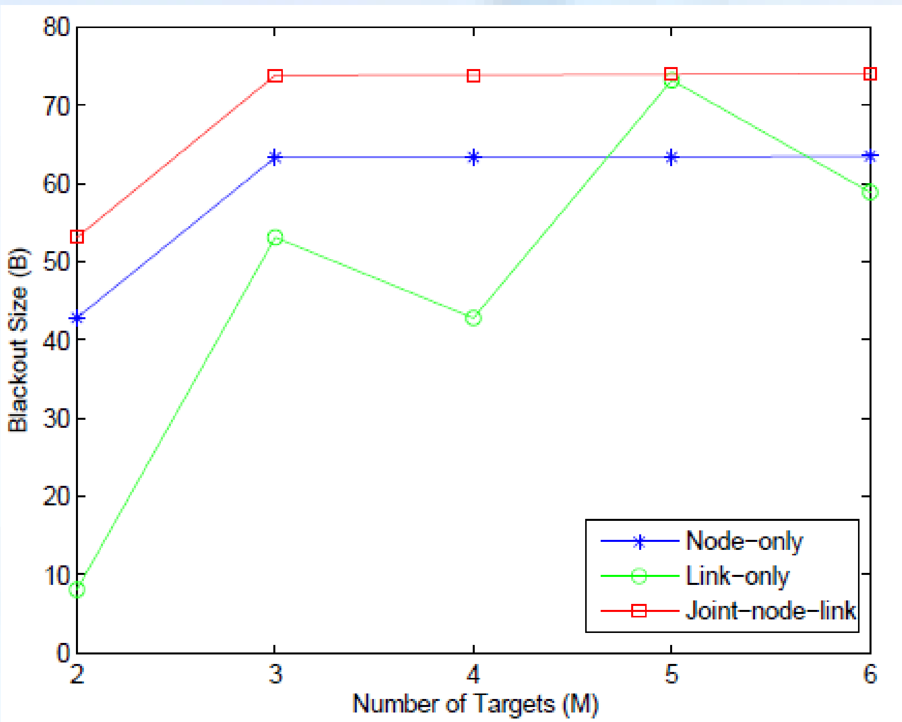
- ***Degree-based node-only attack strategy***: Sort all nodes descendingly according to *nodes' degrees*, and select first *M* nodes as targets.
- ***Degree-based link-only attack strategy***: Sort all links descendingly according to *links' degrees*, and select first *M* links as targets.
- ***Degree-based Joint-node-link attack strategy***:
  - Select *M* nodes and *M* links together as candidate targets based on *degree* values.
  - Among these *2M* candidate targets, generate all *M*-target combinations, which are in total $\binom{2M}{M}$. There are $\binom{2M}{M}-2$ joint-node-link combinations.
  - Conduct simulations for these joint-node-link combinations and find the combination with the largest ***B*** value (attack strength). The components in this combination are the chosen targets for this attack strategy.

❖ Load-based Attack Strategies

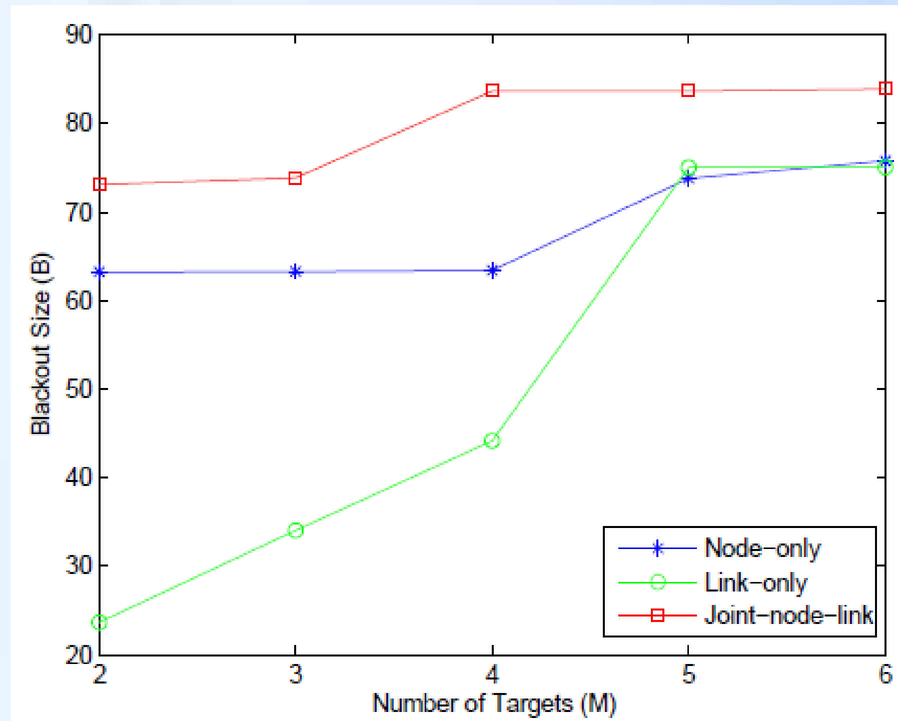
- Three attack strategies are conducted similarly, except replacing *degree* by *load*.

Simulation Results

- Set up
  - Test benchmark : IEEE 39 bus system
  - *M* is set to be 2, 3, 4, 5 and 6.



Comparison among *degree*-based attack strategies



Comparison among *load*-based attack strategies

Comparison between two joint-node-link attack strategies

Metric	Measured by B				
	$M=2$	$M=3$	$M=4$	$M=5$	$M=6$
Degree	53.15	**73.86**	73.89	73.98	74.1
Load	**73.08**	**73.86**	**83.64**	**83.64**	**83.87**

Comparison of the search space between different schemes

Attack Strategy	$M=2$	$M=3$	$M=4$	$M=5$	$M=6$
Node-only	0	0	0	0	0
Link-only	0	0	0	0	0
Joint-node-link $\binom{2M}{M}-2$	4	18	68	250	922

❖ Observation

- Joint-node-link attack strategy can obtain better performances.
- Metric *load* is more insightful than metric *degree*.
- As M increases, the complexity of the joint-node-link attack strategy will sharply increase.

Summary & Future Work

❖Summary

- Propose the joint-substation-transmission-line perspective to study power grid vulnerability.
- Discover many joint-node-link vulnerabilities.
- Adopt two existing metrics, degree and load, to study joint-node-link attack strategies.

❖Future Work

- Design new metrics to study joint- joint-node-link attack strategies → low complexity

  Yihai Zhu, Jun Yan, Yufei Tang, Yan Sun, Haibo He, "*Joint Substation-Transmission line Vulnerability Assessment against the Smart Grid*", IEEE Transactions on Information Forensics and Security (T-IFS), 2014, Accept with minor revision.

- Defense of targeted attacks against power girds.

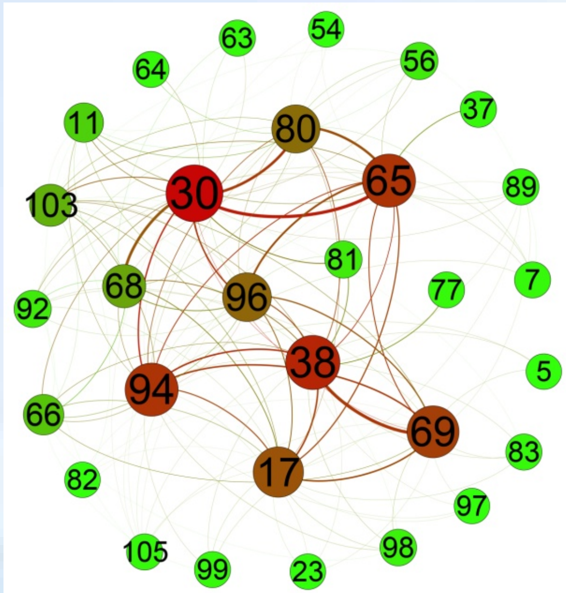
Reference

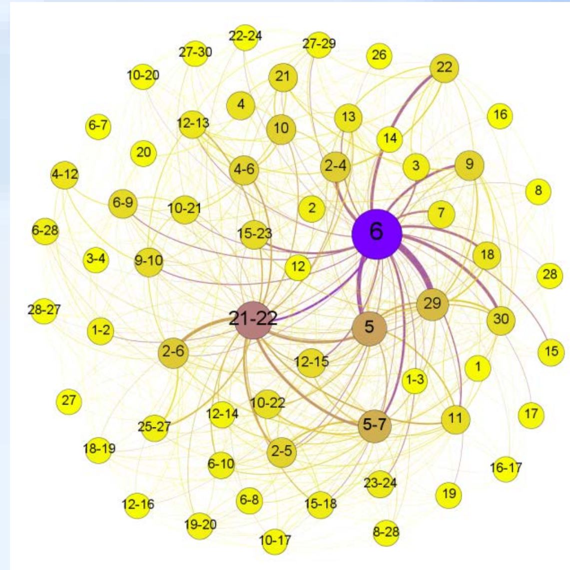
1. U.S.-Canada Power System Outage Task Force, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," Apr. 2004.
2. Paul Hines, “Cascading failures in power grids”, IEEE Potentials, vol. 28, no. 5, pp. 24–30, 2009
3. M. Levine, “Outgoing dhs secretary janet napolitano warns of serious cyber attack, unprecedented natural disaster," Aug.27 2013. [Online]. Available: http://abcnews.go.com/.
4. “Small-scale power grid attack could cause nationwide blackout, study says,” Mar.13 2014. [Online]. Available: FoxNews.com
5. “FBI, joint terrorism task force arrest suspect in arkansas power grid attacks," 2013. [Online]. Available: http://www.forbes.com/
6. R. Smith, "Assault on california power station raises alarm on potential for terrorism," Feb.18 2014. [Online]. Available: http://online.wsj.com/
7. “Aurora Generator Test," [Online]. Available: http://en.wikipedia.org/wiki/Aurora_Generator_Test
8. 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.
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. Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, “The sequential attack against power grid networks,” in Proceeding of IEEE International Conference on Communications, Sydney, Australia, Jun.10-14 2014.
16. 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
17. 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.

Advertising Time

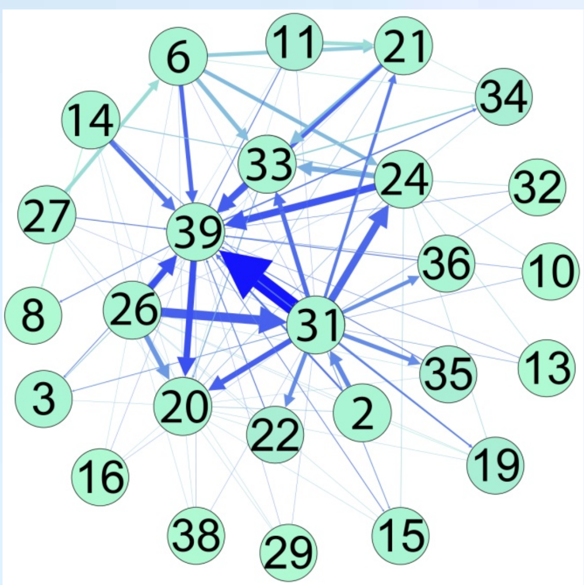
Risk Graph

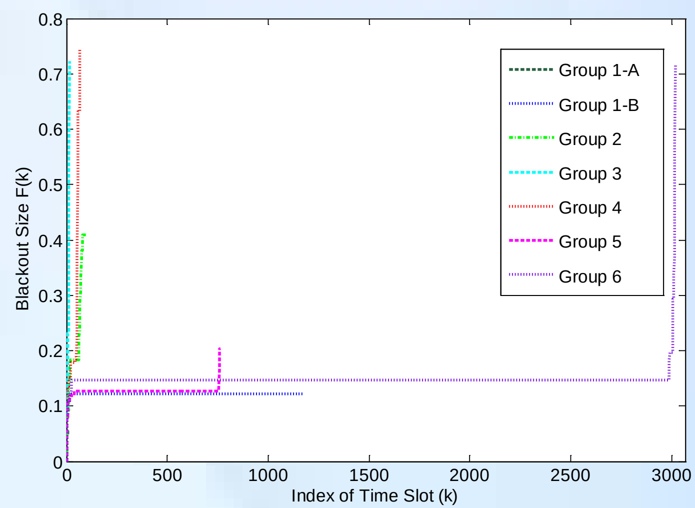




Component Interdependency Graph

Sequential Attack Graph





Diversity of Cascading Processes

Thanks
Any Questions?

Take my business card

or

Email: yhzhu@ele.uri.edu
Web: www.ele.uri.edu/~yhzhu

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

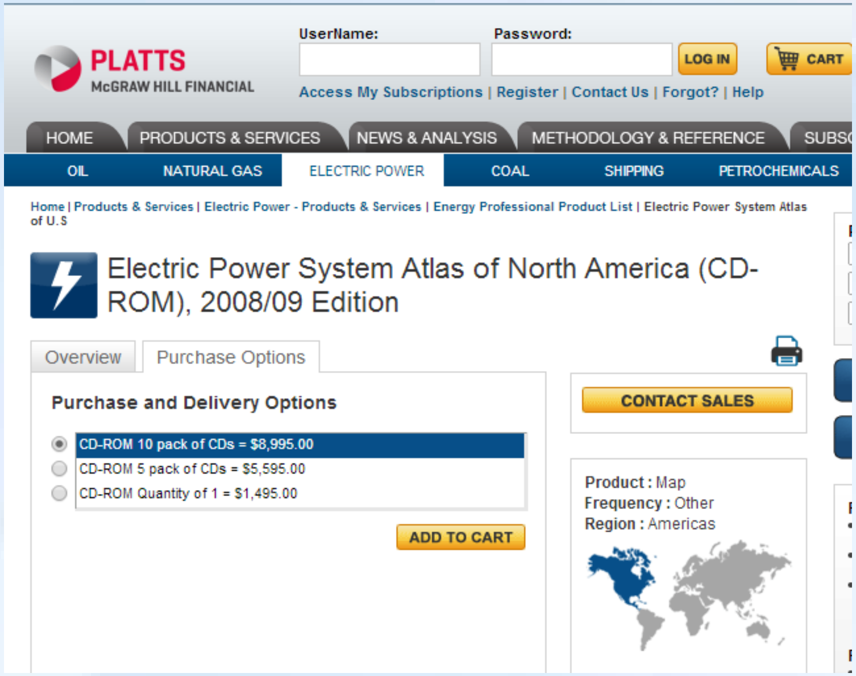
- **Attackers**
  - Disgruntled individuals
  - Terrorist teams
  - Computer hackers
  - Energy companies
  - Hostile Countries
- **Attacker can be from inside and outside.**
- **Attackers can well organize the attacks, aiming to cause large damage.**

- **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 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



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