Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective

Presenter: Yihai Zhu

Authors: Yihai Zhu, Jun Yan Yan Sun, Haibo He

Dept. of Electrical, Computer & Biomedical Engineering

University of Rhode Island

THINK BIG WE DO

THE UNIVERSITY OF RHODE ISLAND

NEST

Overview

- Background
- Problem Statement
- Model and Attack
- Experiments
- Questions

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective

By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

THINK BIG WE DO

NEST

Background

- The largest blackouts around the world
  - 2003 Italy, 2003 Northest, 2005 Java-Bali, 2009 Brazil and Parguay, and 2012 India (670 millions)
    - Rare to happen
    - Cause disasters to modern society
- What is the ***cascading failure*** of power grid?
  - One of major reasons of large blackous
  - A cascading failure is an initial failure of certain parts, such as transmission lines, which triggers the successive failure of other parts, and finally disable the whole power grid.
  - To understand cascading failure is an important step to solve the problem of blackouts.

Problem Statement

- To find stronger attack strategies, aiming to cause severe cascading failures.
- Comparisons schemes
  - Load-based approach
  - Optimal search approach
- Contribution
  - Understanding vulnerability of power grid systems
  - Provide insights for future defense solutions

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

Model and Attack

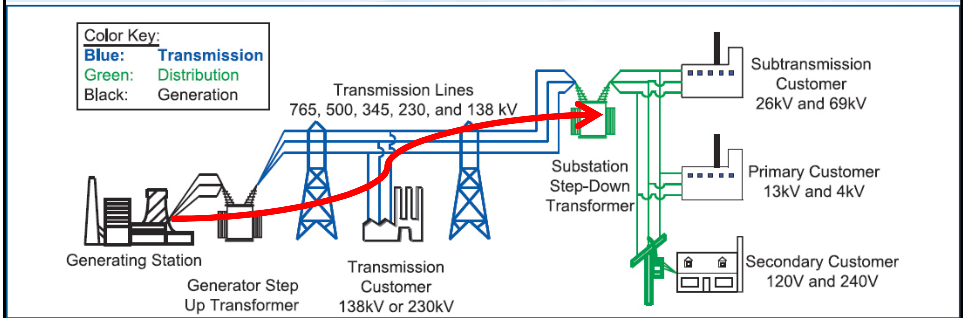


Fig. 1 Basic structure of power grid

Extended Model

- Basic concepts
  - Directed graph (***A***): current direction on a link
  - Nodes: Generators, load substations, and transmission substations.
  - Adopt **Power Transfer Distribution Factors** (PTDFs) to reflect the power distribution in transmission lines.
  - **Extended Betweenness** (EB) of a node
    - Summation of the power in all links connecting to this node.
- Cascading simulator
  - **Load**: extende betweenness
  - **Capacity**: proportional to the initial load, e.g. node *i*

    $$C_i = T * L_i(0)$$
  - **System tolerance**: *T*
  - **Overloadeing**: removed from power grid network
  - **Load rebalance**
    - Recalculate EB
  - **Assessment**: percent of failure (PoF)

    $$PoF = 1 - \frac{M}{N}$$

N and *M* the number of surviving nodes before and after an attack

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)
THINK BIG WE DO
NEST

Sub-optimal Search Attack

- Motivation
  - Exisiting malicious attacks do not stand for the strongest attacks.
  - Optimal search is computationally infeasible.
    - Five-node attack on IEEE 118 bus system needs to search more than a hundred million node combinations
- Sub-optimal Search Attack
  - Goals: (1) sharply reduce the computation task, (2) obtain good attack performance
  - Primary idea: limit the number of candidate combinations during the each round search.

The sub-optimal search attack

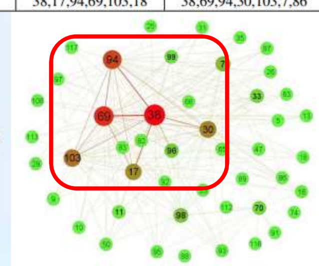
- Procedure
  - Step 1: Set the number of target nodes, ***M***, and system tolerance, ***T***.
  - Step 2: Run one-node attacks, and select the top ***P*** strongest nodes as first round chosen combinations.
  - Step 3: Cascading simulator runs ***M*** – 1 rounds. In each round
    - Combine each candidate node with each chosen combination from the previous round to get new combinations.
    - Run attacks for all new combinations.
    - Top ***P*** strongest attacks as this round chosen combinations.

- A realization of the sub-optimal search
  - IEEE 118 bus system
  - M = 8, T = 1.2, P = 16, all nodes as candidate node

70	17,38	38,17,94	38,17,94,69	38,17,94,69,103	38,69,94,30,103,7	38,69,94,30,103,7,98	38,69,94,30,103,7,98,99
23	70,98	38,17,96	38,17,96,69	38,17,96,69,103	38,17,94,69,103,98	38,69,94,30,103,7,33	38,69,94,30,103,11,98,99
38	38,69	38,69,94	38,69,94,30	38,69,94,30,103	38,17,94,69,103,99	38,17,94,69,103,98,99	38,69,94,30,103,11,98,33
65	38,94	38,17,69	38,69,30,96	38,17,94,69,98	38,17,94,69,103,33	38,17,94,69,103,98,33	38,69,94,30,103,11,99,33
24	23,98	38,94,30	38,17,69,82	38,17,94,30,7	38,69,94,30,103,11	38,17,94,69,103,99,33	38,69,94,30,103,7,98,50
19	38,96	38,17,82	38,17,69,103	38,69,30,96,103	38,69,30,96,103,7	38,69,94,30,103,11,98	38,69,94,30,103,7,98,47
34	70,89	38,69,30	38,17,94,103	38,17,94,69,106	38,17,94,69,103,96	38,69,94,30,103,11,99	38,69,94,30,103,7,98,99
68	70,86	38,69,96	38,17,94,66	38,17,94,69,33	38,17,94,69,103,29	38,69,94,30,103,11,33	38,69,94,30,103,7,98,87
30	70,112	38,96,30	38,17,96,103	38,17,94,69,117	38,17,94,69,103,31	38,69,94,30,103,7,96	38,69,94,30,103,7,98,93
17	70,116	70,98,88	38,69,94,26	38,17,94,69,98	38,17,94,69,103,50	38,69,94,30,103,7,50	38,69,94,30,103,7,98,95
31	30,38	38,17,83	38,69,94,5	38,69,94,30,11	38,17,94,69,103,16	38,69,94,30,103,7,63	38,69,94,30,103,7,98,97
80	30,65	38,69,82	38,17,69,83	38,69,30,96,7	38,17,94,69,103,47	38,69,94,30,103,7,47	38,69,94,30,103,7,33,96
64	70,16	65,30,94	38,17,69,92	38,17,94,69,29	38,17,94,69,103,113	38,69,94,30,103,7,99	38,69,94,30,103,7,33,50
61	70,74	65,30,96	38,69,30,82	38,17,94,69,16	38,17,94,69,103,9	38,69,94,30,103,7,13	38,69,94,30,103,7,33,99
37	70,91	70,98,93	38,17,96,66	38,17,94,69,47	38,17,94,69,103,10	38,69,94,30,103,7,35	38,69,94,30,103,7,33,86
69	38,82	70,98,95	38,69,94,25	38,17,94,69,9	38,17,94,69,103,18	38,69,94,30,103,7,86	38,69,94,30,103,7,33,87

Risk-Graph based Attack

70	17,38	38,17,94	38,17,94,69	38,17,94,69,103	38,69,94,30,103,7	38,69,94,30,103,7,98	38,69,94,30,103,7,98,99
23	70,98	38,17,96	38,17,96,69	38,17,96,69,103	38,17,94,69,103,98	38,69,94,30,103,7,33	38,69,94,30,103,11,98,99
38	38,69	38,69,94	38,69,94,30	38,69,94,30,103	38,17,94,69,103,99	38,17,94,69,103,98,99	38,69,94,30,103,11,98,33
65	38,94	38,17,69	38,69,30,96	38,17,94,69,98	38,17,94,69,103,33	38,17,94,69,103,98,33	38,69,94,30,103,11,99,33
24	23,98	38,94,30	38,17,69,82	38,17,94,30,7	38,69,94,30,103,11	38,17,94,69,103,99,33	38,69,94,30,103,7,98,50
19	38,96	38,17,82	38,17,69,103	38,69,30,96,103	38,69,30,96,103,7	38,69,94,30,103,11,98	38,69,94,30,103,7,98,47
34	70,89	38,69,30	38,17,94,103	38,17,94,69,106	38,17,94,69,103,96	38,69,94,30,103,11,99	38,69,94,30,103,7,98,99
68	70,86	38,69,96	38,17,94,66	38,17,94,69,33	38,17,94,69,103,29	38,69,94,30,103,11,33	38,69,94,30,103,7,98,87
30	70,112	38,96,30	38,17,96,103	38,17,94,69,117	38,17,94,69,103,31	38,69,94,30,103,7,96	38,69,94,30,103,7,98,93
17	70,116	70,98,88	38,69,94,26	38,17,94,69,98	38,17,94,69,103,50	38,69,94,30,103,7,50	38,69,94,30,103,7,98,95
31	30,38	38,17,83	38,69,94,5	38,69,94,30,11	38,17,94,69,103,16	38,69,94,30,103,7,63	38,69,94,30,103,7,98,97
80	30,65	38,69,82	38,17,69,83	38,69,30,96,7	38,17,94,69,103,47	38,69,94,30,103,7,47	38,69,94,30,103,7,33,96
64	70,16	65,30,94	38,17,69,92	38,17,94,69,29	38,17,94,69,103,113	38,69,94,30,103,7,99	38,69,94,30,103,7,33,50
61	70,74	65,30,96	38,69,30,82	38,17,94,69,16	38,17,94,69,103,9	38,69,94,30,103,7,13	38,69,94,30,103,7,33,99
37	70,91	70,98,93	38,17,96,66	38,17,94,69,47	38,17,94,69,103,10	38,69,94,30,103,7,35	38,69,94,30,103,7,33,86
69	38,82	70,98,95	38,69,94,25	38,17,94,69,9	38,17,94,69,103,18	38,69,94,30,103,7,86	38,69,94,30,103,7,33,87



Construction of Risk Graph

- Procedure
  - Step 1: all the nodes in the table are vertexes in the risk graph.
  - Step 2: deal with the combinations one by one.
    - A node appears in a combination, its frequency +1.
    - A combination contains more than one node, e.g. ***K*** nodes.
      - Add ***K***(***K-1***)/2 edges into the risk graph.
      - Add the weight of each edge with 2/[***K***(***K-1***)].

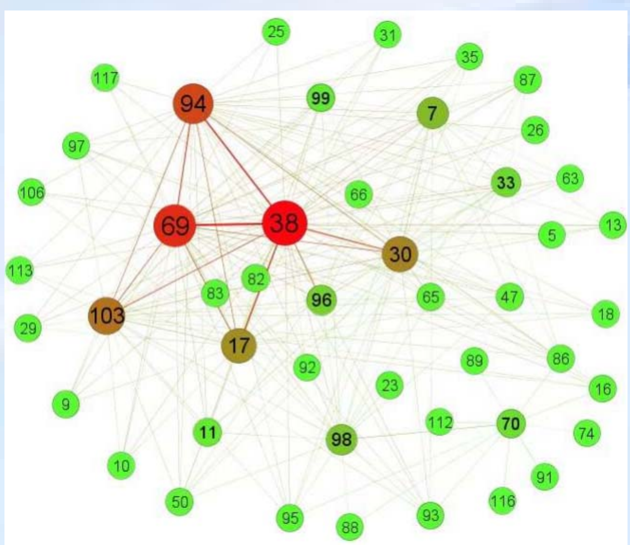


Fig. 2 An single risk graph of IEEE 118 bus system

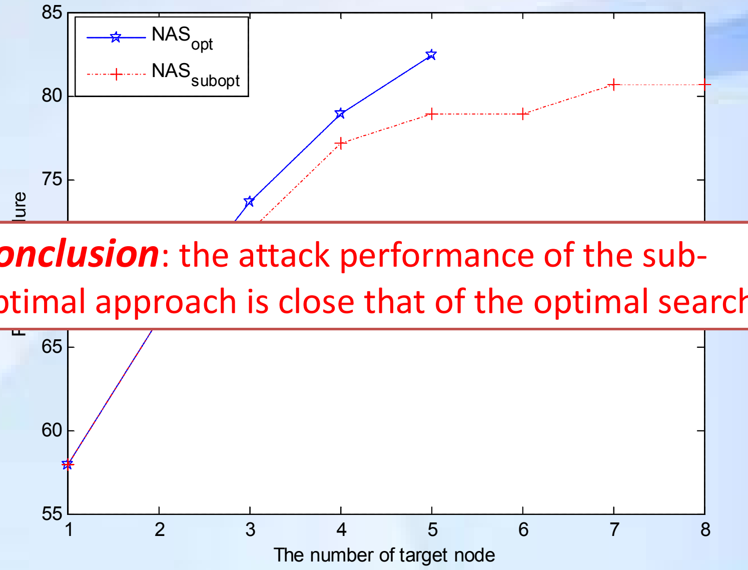
Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

Risk-graph Based Attack

- Integrated Risk Graph (IRG)
  - Set ***T*** from 1.05 to 2 with an interval 0.05, and obtain 20 single risk graphs.
  - Add those 20 single risk graphs as a IRG.
- Risk-graph based attack based IRG
  - ***M*** == 1, choose the node with largest frequency.
  - ***M*** >=2, choose the ***M*** nodes. First, there must exist an edge between each pair of vertexes. Second, the summation of the weight on all those edges is maximum.

Experiments

- Test benchmarks
  - IEEE 57 bus system and IEEE 118 bus system
- Comparisons
  - Sub-optimal vs optimal
  - Load-based, riskgraph-based, sub-optimal



Conclusion: the attack performance of the sub-optimal approach is close that of the optimal search.

Fig. 3 Comparison between sub-optimal and optimal methods on IEEE 57 bus system

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective

By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

NEST

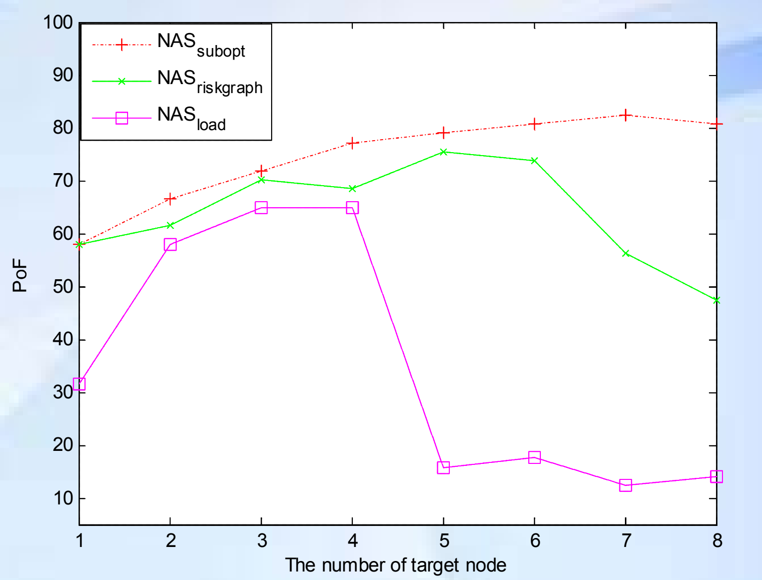
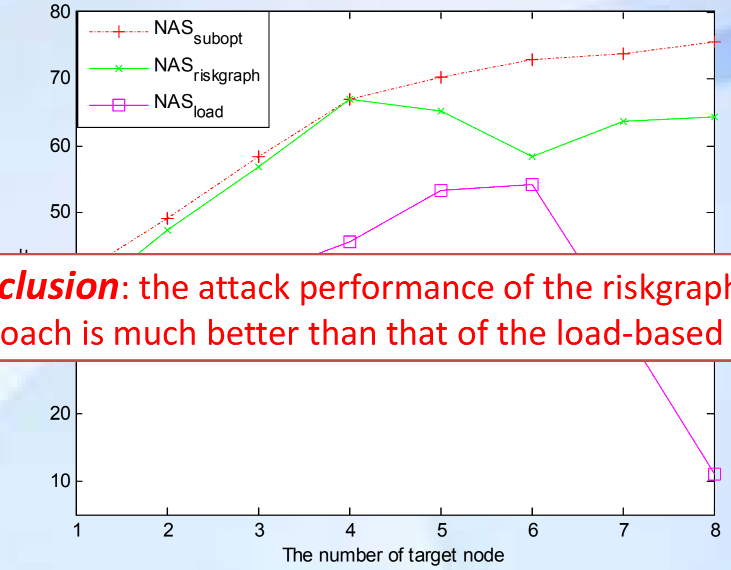


Fig. 4 Comparison among load-based, riskgraph-based and sub-optimal methods on IEEE 57 bus system

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective

By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

NEST



Conclusion: the attack performance of the riskgraph-based approach is much better than that of the load-based one.

Fig. 5 Comparison among load-based, riskgraph-based and sub-optimal methods on IEEE 118 bus system

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

NEST

Summary of Different Attacks

THE SUMMARY OF DIFFERENT ATTACK STRATEGIES

Attack Strategy	NAS^M_{load}	$NAS^M_{riskgraph}$	NAS^M_{subopt}	NAS^M_{opt}
Complexity	$O(1)$	$O(1)$	$O(M(N_B)^2)$	$O((N_B)^M)$
Effectiveness	Low	High	High	High
Need system tolerance	No	No	Yes	Yes

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)

NEST

Acknowledgement

- We gratefully acknowledge the support from National Science Foundation (NSF) under Grant # CNS 1117314
- For more information, please contact **Prof. Haibo He** at **he@ele.uri.edu**

References

- U.S.-Canada Power System Outage Task Force, "Final report on theaugust 14, 2003 blackout in the united states and canada: Causes and recommendations," April 2004.
- M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines,M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges,"IEEE Transactions on Power Systems, vol. 27, no. 2, 2012.
- 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, 2011, pp. 1–6.
- S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Powergrid vulnerabil-ity: a complex network approach," EChaos: An Interdisciplinary Journal of Nonlinear Science, vol. 19, 2009.
- E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," IET Generation, Transmission and Distribution, vol. 4, pp. 716–724, 2010.

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)
THINK BIG WE DO
NEST

- Comments & Questions?

Thanks!

Risk-Aware Vulnerability Analysis of Electric Grids from Attacker's Perspective
By Yihai Zhu, Ph.D. Candidate, URI (Kingston, RI)