A Centrality Performance Index for Assessing Vulnerability

T. E. Ernster, A. K. Srivastava and C. B. Vellaithurai

Goals

- Attempt to validate graph-theory-based approaches to power system contingency ranking using limited system information (due to the difficulty inherent to acquiring complete system information, a coordinated system attack is more likely to be planned from limited information).
- Develop an approach to identify higher-order contingency scenarios that have a statistically significant likelihood of resulting in a maximally adverse impact given incomplete system information.
- Assist with the development of a test-bed from which attack scenarios can be simulated in real-time, and the resulting data utilized by a vulnerability-related application tool.

Fundamental Questions/Challenges

- We seek to answer the question of whether or not high-impact contingencies can be identified without extensive operational knowledge of a power system. Challenge: conventional contingency screening methods utilize power-flow-based screening techniques requiring knowledge of system branch and shunt impedances, bus MVA injection, and bus voltage magnitudes to check for contingencies that would result in a voltage or branch flow violation.
- We wish to pursue a solution to the question of how to utilize graph theory in the development of an N-X contingency ranking scheme. Challenge: graph-theory-based centrality techniques have not been developed to assess the collective importance of a given group of buses or branches.

Research Results

- A closeness and edge betweenness based centrality performance index (PI) was developed for assessing vulnerability to N-X contingencies.

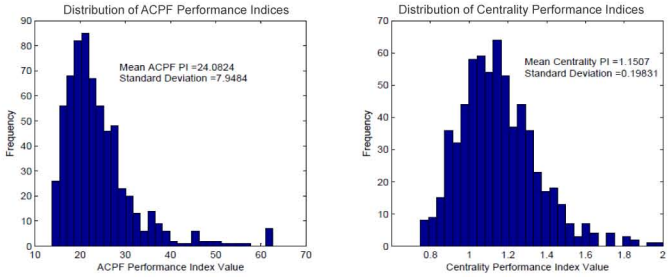

Figure 1: Distribution of ACPF (left) and Developed Centrality (right) Performance Indices for a Modified IEEE-14 System

- Simulations on a modified IEEE-14 bus system indicated N-3 contingencies selected amongst the top 5% of contingencies ranked by the centrality performance index had an expected 27% increase in adverse reliability impact, as defined by an ACPF performance index.

Table 1: Statistical Comparison of Highly Ranked Centrality PI Contingencies with the ACPF PI

	Sample Size	Sample Mean	Standard Deviation	Standard Error on Mean
ACPF Performance Index for All Cases	652	24.08	7.95	0.31
ACPF Performance Index for the Top 5% of Contingencies Ranked by the Centrality Performance Index	33	30.60	13.0	2.3
Estimate for Difference Between Means	6.52			
95% Confidence Interval for Difference Between Means	1.88 to 11.16			
T-Test for Equal Means vs. Different Means	T-Value	2.86		
	P-Value	0.007		

Research Plan

- Student working on this project completed his thesis and will receive a Master of Science in Electrical Engineering in August 2012.
- Currently deliberating whether to continue this project or pursue an alternate research direction with a new student.

Broader Impact

- Research would result in significant findings for power grid vulnerability analysis using incomplete system information. If graph theory can be reliably utilized to select targets for a coordinated attack on the power system, an attacker can assess the vulnerability of a power system without obtaining confidential power system operational data.
- This topology based vulnerability analysis method was generated from a principles of warfare (objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity) framework that can be utilized to generate credible attack/defense models for adversarial operations.
- The developed test-bed can be utilized by multiple institutions for further research studies.

Interaction with Other Projects

- Work is inspired by the publication "Electrical Centrality Measures for Electric Power Grid Vulnerability Analysis" from Wang (UI Urbana-Champaign), Scaglione (UC Davis), and Thomas (Cornell).
- Results will serve as an application tool for coordinating cyber attack scenarios simulated with the test-bed being developed using funding from NSF, DOE, and industry partners.

Future Efforts

- Continue validation efforts for the developed centrality performance index. Perform N-X contingency ranking comparisons with the conventional AC power flow performance index for additional test systems under various operating states.
- Explore alternative topology based approaches to power system vulnerability analysis.
- Create a centrality application to analyze topology processor data for physical attack signatures indicating a coordinated cyber attack.

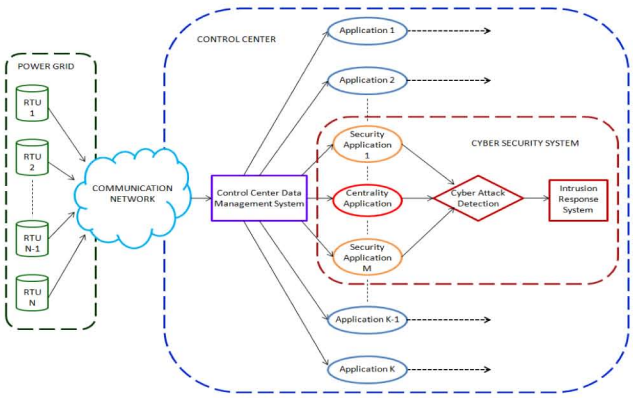

Figure 2: Role of a Centrality Application in Electric Grid Operations