TCIPG

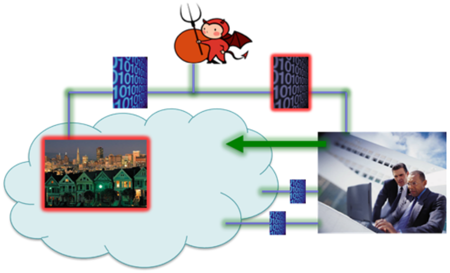
Security and Robustness Evaluation and Enhancement of Power System Applications:

Malicious Data Detection in State Estimation Leveraging System Losses & Estimation of Perturbed Parameters

William Niemira, Rakesh B. Bobba, Peter Sauer, William H. Sanders, and Miao Lu

GOALS

- Reliable detection of bad data injection attacks that are potentially undetectable by conventional methods.



- Improved understanding of full taxonomy of attacks that are presently potentially undetectable by conventional methods.

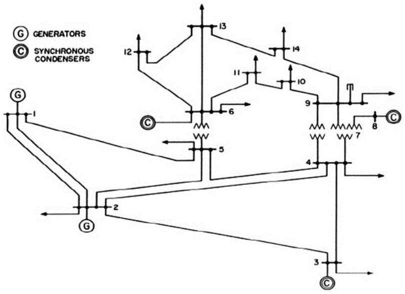
FUNDAMENTAL QUESTIONS/CHALLENGES

- For attacks using DC model, can the approximations made by the attacker be leveraged for detection?
- Can topology perturbation in combination with parameter estimation enhance the detectability of malicious data injection attacks?

RESEARCH PLAN

- Analyze the sensitivities of specific power system quantities to attacks and study their potential as indicators of attacks.
- Study the viability of parameter estimation along with topology (parameter) estimation as a means of detecting data injection attacks.

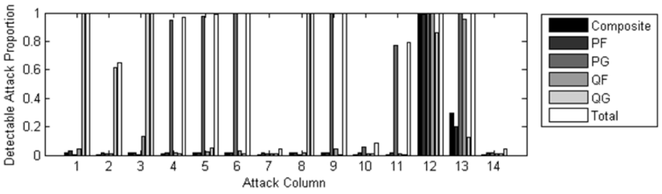
RESEARCH RESULTS



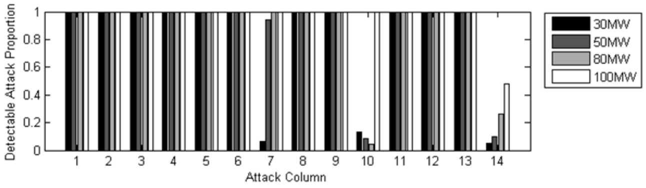
- Tested 140 linear data injection attacks against IEEE 14-bus system and observed residuals for different measurement types.

Residual Type	Attacks Detected
Weighted Composite	2
Real Power Flows	8
Real Power Injections	60
Reactive Power Flows	17
Reactive Power Injections	53

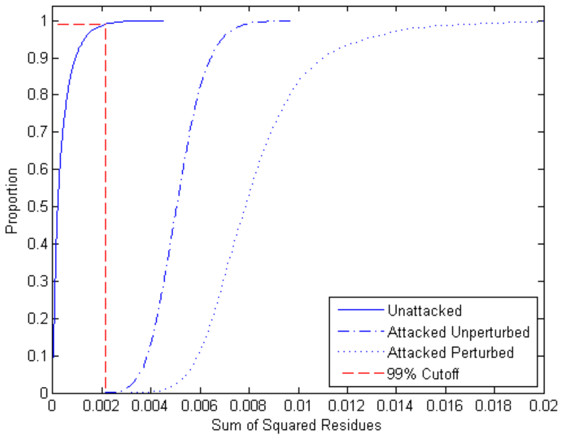
- A combined total of 113 out of 140 attacks (~81% of attacks) were detected by the residual of the real and reactive power injections.



RESEARCH RESULTS (CONTINUED)



- The grouped bars indicate the total proportion of each attack column type detected at 10MW, 30MW, 50MW, 80MW, and 100MW attack levels for IEEE 14-bus system.
- At 30MW level, 11 out of 14 injection attacks were detected.
- Residual of estimated parameters (line reactance) alone turned out to be a decent indicator of attacks, especially at higher attack energy levels.
- Perturbation of parameters shifted the CDF further to the right, improving detectability.



BROADER IMPACT AND PROJECT INTERACTION

- This work indicates that conventional bad-data detection methods in EMS can be augmented to detect DC model-based false data injection attacks.
- In discussion with researchers at PNNL to integrate bad-data detection into EMS.

FUTURE EFFORTS

- Further investigate the attacks that are difficult to detect even at high energy levels. We intend to study such attacks in the future for different bus systems and identify ways to detect them.
- Compare residual distributions to ordinary bad data to distinguish between bad and malicious data.
- Locate the specific measurements that are being attacked if malicious data appear.

RELATED PUBLICATIONS

- W. Niemira, R. B. Bobba, P. Sauer, and W. H. Sanders. “Malicious Data Detection in State Estimation Leveraging System Losses & Estimation of Perturbed Parameters.” *IEEE SmartGridComm 2013.*
- K. R. Davis, K. L. Morrow, R. Bobba, E. Heine. “Power Flow Cyber Attacks and Perturbation-Based Defense.” *IEEE SmartGridComm 2012.*

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG
UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T