TCIPG

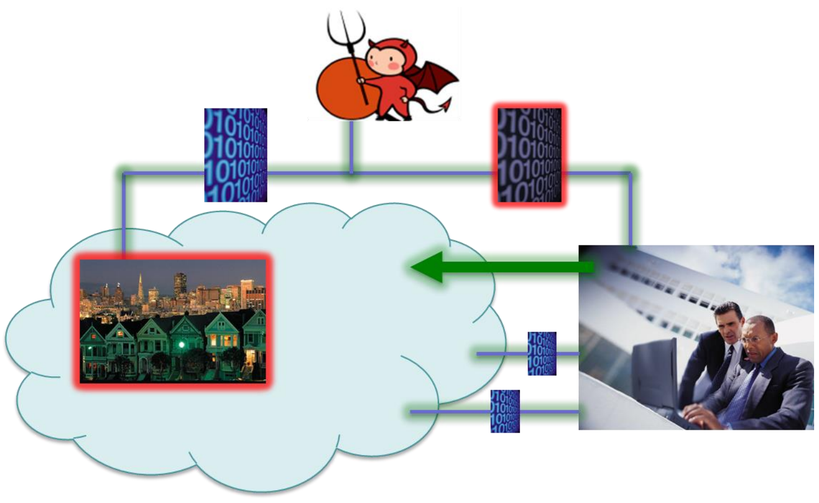
Security and Robustness Evaluation and Enhancement of Power System Applications:

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

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

GOALS

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



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

FUNDAMENTAL QUESTIONS/CHALLENGES

- For attacks using a 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?
- How can one further enhance the detection and localization of malicious data injection attacks?

RESEARCH PLAN

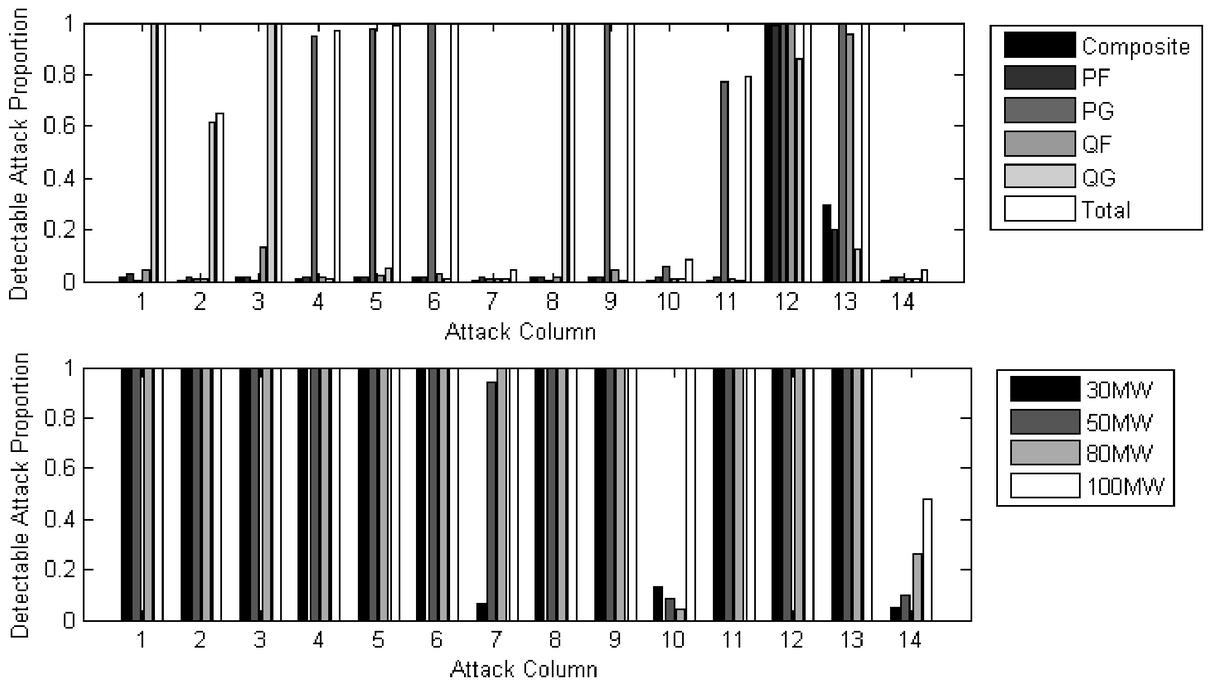
- Analyze the sensitivities of specific power system quantities to attacks and study their potential as indicators of attacks.
- Study the viability of parameter estimation along with topology (parameter) estimation as a means of detecting data injection attacks.
- Incorporate PMUs to further improve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

RESEARCH RESULTS

- Tested 140 linear data injection attacks against the 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

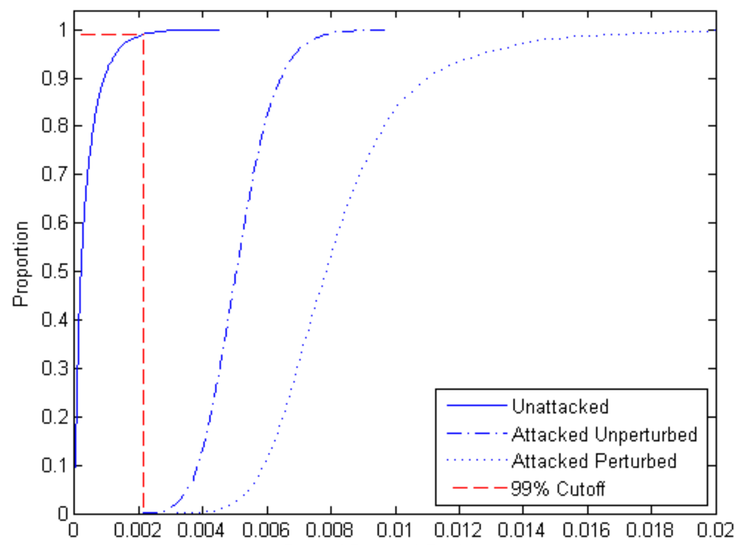
- A combined total of 113 out of 140 attacks (~81% of attacks) were detected by the residual of the real and reactive power injections.



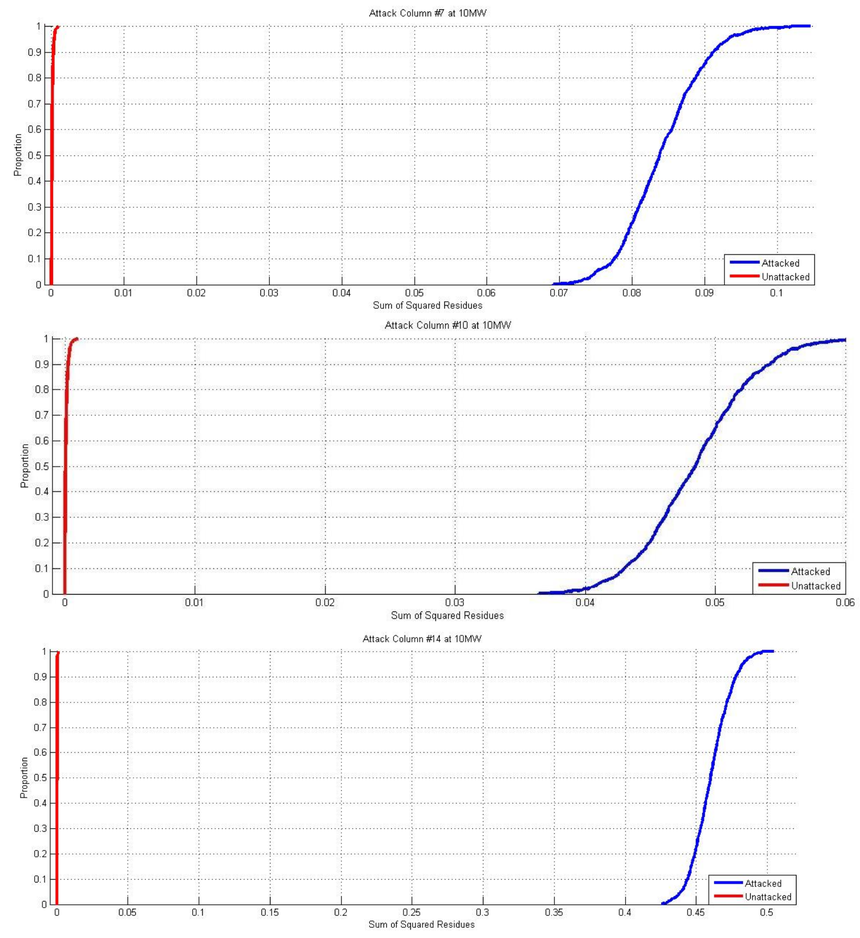
- The grouped bars indicate the total proportion of each attack column type detected at 30MW, 50MW, 80MW, and 100MW attack levels for the IEEE 14-bus system.
- At the 10MW level, 11 out of 14 injection attacks were detected.

RESEARCH RESULTS (CONTINUED)

- 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.



- Through incorporation of PMU measurements, attack detectability has been further enhanced through use of residues of phase angle differences.
- At the 10MW attack level, attacks in columns 7, 10, and 14 were detected.
- Attacks can be localized at locations where PMUs have been installed.

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.
- The work also provides another meaningful application of PMUs.

FUTURE EFFORTS

- Further investigate the attacks that are difficult to detect for larger bus systems, and identify ways to detect them.
- Locate the specific measurements that are being attacked if malicious data appear.
- Provide optimum location for PMU placements to further improve the detection of malicious data injection attacks.

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.*
- Andre Teixeira, Gyorgy Dan, Henrik Sandberg, Robin Berthier, Rakesh Bobba, and Alfonso Valdes. “Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures.” *American Control Conference 2014*.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T