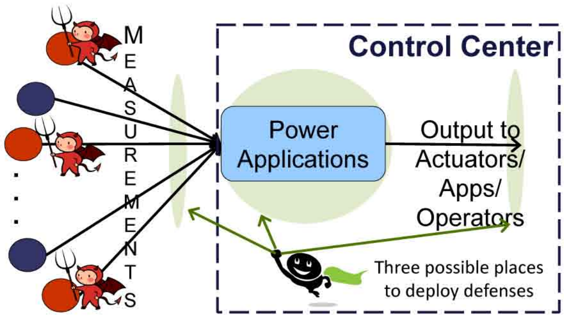
TCIPG

Defending Against False Data Injection Attacks in the Power Grid

R. B. Bobba, E. Heine, H. Khurana, K. L. Morrow, K. Nahrstedt, T. J. Overbye, K. M. Rogers, and Q. Wang

Goals

- Study the security and robustness of power applications in the face of malicious sensor data manipulation attacks.
- Develop effective and cost-efficient defenses against malicious sensor data manipulation attacks.
- Evolve a process to include security and robustness considerations during the power system application design phase.



Fundamental Questions/Challenges

- When do the results of a given power system application become compromised/invalid?
- How many sensors have to go bad or be compromised?
- By how much should each sensor value deviate from the original?
- Is it possible to design robust power applications that can tolerate malicious data modification to a given extent at a reasonable cost?
- Is it possible to detect malicious data modifications and recover from them?

Research Plan

- Understand the behavior of power system applications and analyze their robustness in the presence of malicious data modification.
- Leverage the physical properties (e.g., topology) of the underlying electrical network along with cryptographic and other cyber security mechanisms to design effective and cost-efficient security schemes.

Approach I: Power-System-Aware Measurement Protection

Application: DC State Estimation

System of linear equations

$$z = Hx + e$$
$$\underline{x} = (H^T W H)^{-1} H^T W z$$

x is n x 1 vector of state variables; **z** is m x 1 vector of measurements
H is m x n Jacobian matrix representing topology
w is diagonal weight matrix **e** m x 1 vector of errors

Traditional Bad Data Detection: *if* $||z - H\underline{x}|| \leq \tau$ *=> no bad measurements;*
τ is a predetermined threshold, $||\,.\,||$ stands for L_2 norm

False Data Injection Attacks [Liu et al., *ACM CCS 2009*]:
If $a = Hc$ *and* $||z - H\underline{x}|| \leq \tau$ *then* $||z_{bad} - H\underline{x}_{bad}|| \leq \tau$
a is m x 1 attack vector; $z_{bad} = z + a$
c is n x 1 vector of induced error; $\underline{x}_{bad} = \underline{x} + c$

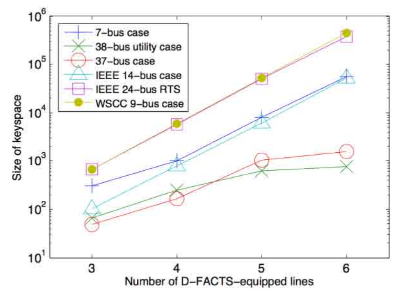
Results:

- *To ensure* $a \neq Hc$, *that is, to detect false data injection attacks:*
  - *It is necessary but not sufficient to protect ≥ n (= no. of state variables) measurements.*
  - *It is necessary and sufficient to protect a set of **basic measurements (BM)***, that is those needed for observability.
- *Having q verifiable state variables (e.g., through PMUs) doesn't reduce the number of measurements that need to be protected by more than q.*

Approach II: Topology Perturbation

- Probe: Apply known perturbations to system topology and look for expected changes.
- Difference in expected vs. measured sensor values after a probe indicates presence of malicious activity.
- Choice of "probe" is randomized and is picked from a large set of available probes.
- Perturbation achieved through D-FACTS devices and limited to those with minimum operational impact: in our case, minimum power loss impact.
- Viable perturbations further limited by "observability" and "linearity" constraints.

Results:



Broader Impact

- Provide guidance on where to focus an organization's security budget to secure applications.
- Provide input to operators and incident response engines as to when an application can be considered compromised.
- Help develop a process to include security and robustness considerations during application design phase.

Interaction with Other Projects

- The security and robustness boundary analysis can feed into the Response and Recovery Engine (RRE) project.
- Analysis of PMU application security and robustness can feed into design of secure communication framework for PMU data sharing.

Future Efforts

- Study cost-based frameworks for use when protecting n measurements is not feasible.
- Further study topology perturbation approach to detecting bad data.
- Study the robustness of topology processor both individually and together with state estimator.
- Study the robustness of distributed state estimation and compare it with traditional state estimation.

Publications and Related Work

- K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye. "Topology Perturbation for Detecting Malicious Data Injection." In the *Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS '12)*, Maui, Hawaii, January 2012.
- R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T. J. Overbye. "Detecting False Data Injection Attacks on DC State Estimation." In *Preprints of 1st Workshop on Secure Control Systems (SCS '10)*, Stockholm, Sweden, April 2010.
- Y. Liu, P. Ning, and M. K. Reiter. "False Data Injection Attacks Against State Estimation in Electric Power Grids." In the Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), Chicago, Illinois, Nov. 9-13, 2009, pp. 21-32.