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 cybersecurity mechanisms to design effective and cost-efficient security schemes.

Approach I: Power-System-Aware Measurement Protection

Application: DC State Estimation

System of linear equations

\[ \mathbf{z} = \mathbf{Hx} + \mathbf{e} \]

\[ \mathbf{x} = (\mathbf{H}^\top \mathbf{W}_m \mathbf{H})^{-1} \mathbf{H}^\top \mathbf{W}_m \mathbf{z} \]

- \( \mathbf{x} \) is \( n \times 1 \) vector of state variables;
- \( \mathbf{z} \) is \( m \times 1 \) vector of measurements;
- \( \mathbf{H} \) is \( m \times n \) Jacobian matrix representing topology;
- \( \mathbf{W}_m \) is diagonal weight matrix.

Traditional Bad Data Detection: if \( ||z - Hx|| \leq t \) then \( \Rightarrow no\ bad\ measurements; \)

\( t \) is a predetermined threshold, \( || \cdot || \) stands for \( L_2 \) norm.

False Data Injection Attacks [Lu et al., ACM CCS 2009]:

If \( a = Hc \) and \( ||z - Hx|| \leq t \) then \( ||\text{bad} - Hc|| \leq t \)

- \( a \) is \( m \times 1 \) attack vector;
- \( \text{bad} = z + a \)
- \( c \) is \( n \times 1 \) vector of induced error; \( \text{bad} - Hc = t + c \)

Results:

- To ensure \( a \neq Hc \), that is, to detect false data injection attacks:
  - It is necessary but not sufficient to protect \( n > q (\approx no.\ of\ state\ variables) \) 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