Strategic Protection Against Data Injection Attacks on Power Grids

Authors: Tung T. Kim and Vincent Poor, Princeton University

Presenter: Hung D. Ly

Submitted in Partial Fulfillment of the Course Requirements for
ECEN 689: Cyber Security of the Smart Grid
Instructor: Dr. Deepa Kundur

Outline

- This talk is to understand
  - false data injection attacks on state estimation in power grids
  - some protection strategies against these attacks

Power System State Estimation

- Monitor the power flow in the power system
- Consider a linearized measurement model

$$\mathbf{z} = \mathbf{H}\theta + \mathbf{n}$$

  - $\mathbf{z} \in \mathbb{R}^M$ is the vector of measurements
  - $\theta \in \mathbb{R}^N$ is the state vector
  - $\mathbf{H} \in \mathbb{R}^{M \times N}$ is the measurement Jacobian matrix
  - $\mathbf{n}$ is the vector of measurement noise

- The estimated state vector

$$\hat{\theta} = (\mathbf{H}^T\mathbf{H})^{-1}\mathbf{H}\mathbf{z}$$

Bad Measurement Detection

- Bad measurement can exist due to meter failures, malicious attacks, etc.
- The common approach to detect the bad measurement is to use the statistical testing on $||\mathbf{z} - \mathbf{H}\hat{\theta}||_2$
  - if $||\mathbf{z} - \mathbf{H}\hat{\theta}||_2 > \mu$, the bad measurement is present
- Let $\mathbf{z}_b = \mathbf{z} + \mathbf{x}$ and $\hat{\theta}_b = \hat{\theta} + \mathbf{c}$
  - $\mathbf{x}$ is the false data injected by the attacker
  - if $\mathbf{x} = \mathbf{Hc}$,
  $$||\mathbf{z}_b - \mathbf{H}\hat{\theta}_b||_2 = ||\mathbf{z} - \mathbf{H}\hat{\theta}||_2$$
  - No bad measurements can be detected !

Main Results

- From the attack modeling viewpoint
  - How to construct $\mathbf{c}$ s.t. $\mathbf{x} = \mathbf{Hc}$?
- From the grid designer's viewpoint
  - How to choose a subset of measurements to protect s.t. the false data injection attacks can be detected ?
  - How to place secure PMUs to protect the state estimation under false injection attacks ?

Attack Modeling

- Let $\mathcal{S}$ be a set of indices of N_S protected measurements
- and $\mathbf{H}^{\mathcal{S}}$ be a submatrix of $\mathbf{H}$ whose rows are indicated by the indices in $\mathcal{S}$
- The measurement constraint for the attacker

$$\mathbf{H}^{\mathcal{S}}\mathbf{c} = \mathbf{0}$$

  - if either $\text{rank}(\mathbf{H}^{\mathcal{S}}) = N$ or there exists N linearly independent measurements, $\mathbf{c} = \mathbf{0}$
  - **assumptions**
    - $\text{rank}(\mathbf{H}^{\mathcal{S}}) < N$
    - $||\mathbf{c}||_\infty \geq \tau$ (small shifts have very small impact on the state estimation). Note $||\mathbf{c}||_\infty = \max\{|c_1|, \ldots, |c_N|\}$

Attack Modeling

- Attacker can find the smallest number of meters to tamper with and their associated indices

$$\min_{\mathbf{c}} ||\mathbf{H}^{\overline{\mathcal{S}}}\mathbf{c}||_0$$
$$\text{s.t.} \quad \mathbf{H}^{\mathcal{S}}\mathbf{c} = 0$$
$$||\mathbf{c}||_\infty \geq \tau$$

  - That is, it looks for the sparsest attack vector **c**
  - $||\mathbf{y}||_0$ is the number of nonzero elements in **y**

- Equivalently,

$$\min_{i=1,\ldots,N} \min_{\mathbf{c}} ||\mathbf{H}^{\overline{\mathcal{S}}}\mathbf{c}||_0$$
$$\text{s.t.} \quad \mathbf{H}^{\mathcal{S}}\mathbf{c} = 0$$
$$|c_i| \geq \tau$$

Attack Modeling

- The inner minimization problem was shown to be

$$\min_{\mathbf{c_i} \in \mathbb{R}^{\mathbf{N-1}}} ||\mathbf{H}_i^{\overline{\mathcal{S}}} \mathbf{c}_i + \mathbf{h}_i^{\overline{\mathcal{S}}}||_0$$

$$\text{s.t.} \quad \mathbf{H}_i^{\mathcal{S}} \mathbf{c}_i + \mathbf{h}_i^{\mathcal{S}} = 0$$

  - Here $\mathbf{H}_i^{\mathcal{S}}$ is $\mathbf{H}^{\mathcal{S}}$ after deleting the ith column $\mathbf{h}_i^{\mathcal{S}}$
  - NP-hard in general !

Attack Modeling

- Approach 1:

$$\min_{\mathbf{c_i}\in\mathbb{R}^{\mathbf{N-1}}} ||\text{diag}(\mathbf{w}_i)(\mathbf{H}_i^{\overline{\mathcal{S}}}\mathbf{c}_i + \mathbf{h}_i^{\overline{\mathcal{S}}})||_1 \quad (1)$$
$$\text{s.t.} \quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i + \mathbf{h}_i^{\mathcal{S}} = 0$$

where $\mathbf{w}_i \in \mathbb{R}^{M-N_S}$ and attacker can choose $w_{ik} = \frac{1}{|x_{ik}|+\epsilon}$ for $\epsilon > 0$, $k = 1, \ldots, M - N_S$. Remember N_S is the number of protected measurements

- Approach 2:

$$\min_{\mathbf{c_i}\in\mathbb{R}^{\mathbf{N-1}}} ||\mathbf{c}_i||_1 \quad (2)$$
$$\text{s.t.} \quad \mathbf{H}_i^{\mathcal{S}}\mathbf{c}_i + \mathbf{h}_i^{\mathcal{S}} = 0$$

Attacker's Strategies

- Combination of both Approach 1 and Approach 2
- In particular, for state i
  - Solve (2) to find an initial $\mathbf{c}_i$
  - for a fixed number of iterations
    - Compute $\mathbf{x}_i = \mathbf{H}_i^{\overline{\mathcal{S}}}\mathbf{c}_i + \mathbf{h}_i^{\overline{\mathcal{S}}}$
    - Find $w_{ik} = \frac{1}{|x_{ik}|+\epsilon}$
    - Then solve (1) to obtain new $\mathbf{c}_i$

Protection Strategies

- Under the above attack strategy, the grid designer can
  - Choose a subset of measurements to protect
    - Which subset should be chosen?
  - Place some secure PMUs into the grid
    - Where should secure PMUs be placed?

Measurement Subset Selection

- Let N_A be the minimum number of measurements that the attacker needs to modify to evade the bad data detection
- The injected data to the ith state

$$\mathbf{x}_i = \mathbf{H}_i^{\overline{\mathcal{S}}} \mathbf{c}_i^* + \mathbf{h}_i^{\overline{\mathcal{S}}}$$

where $\mathbf{c}_i^*$ is the best possible attack vector modifying at least the ith state

- The goal

$$\min_{\mathcal{S}} |\mathcal{S}| \quad (3)$$

$$\text{s.t.} \quad \min_{i} ||\mathbf{x}_i||_0 \geq N_A$$

Subset Selection Algorithm

- Initialize $\mathcal{S} = \emptyset$
- While $||\mathbf{x}_i||_0 < N_A$ for all $i = 1, \ldots, N$
  - generate an array $\mathbf{\Gamma}$ of M elements that count the number of times each measurement is modified under the attack ($\mathbf{\Gamma} = \mathbf{0}$ initially)
  - for each state
    - solve (3) to find $\mathcal{S}_i$ and $||\mathbf{x}_i||_0$
    - update $\mathbf{\Gamma}$ by adding one unit to the elements of $\mathbf{\Gamma}$ with indices in $\mathcal{S}_i$ if $||\mathbf{x}_i||_0 < N_A$
  - find the measurement that is modified the most and add it into $\mathcal{S}$

Secure PMU placement

- Adding additional PMUs into the grid modifies the measurement Jacobian matrix $\mathbf{H}$ in the original model
- Let $\overline{\mathbf{H}}_k$ be Jacobian matrix associated with adding a secure PMU to bus k, $k = 1, \ldots, N$
- For the attacker

$$\begin{pmatrix} \mathbf{H}^{\mathcal{S}} \\ \overline{\mathbf{H}}_k \end{pmatrix} \mathbf{c} = 0$$

- Given $\mathbf{c}_i^*$, the goal is to find a bus to place an EPU s.t.

$$\overline{\mathbf{H}}_k \mathbf{c}_i^* \neq 0$$

  - adding an PMU must force the attacker to find another solution $\mathbf{c}$

Secure PMU placement Algorithm

- While $||\mathbf{x}_i||_0 < N_A$ for all $i = 1, \ldots, N$
  - Initialize a count array $\boldsymbol{\Delta}$ of N elements that counts the number of times that adding new secure PMUs can help ($\boldsymbol{\Delta} = 0$)
  - For each state
    - find $\mathbf{c}_i^*$ and $||\mathbf{x}_i||_0$
    - if $||\mathbf{x}_i||_0 < N_A$,

$$\boldsymbol{\Delta}(k) = \boldsymbol{\Delta}(k) + \mathbb{I}(\overline{\mathbf{H}}_k \mathbf{c}_i^* = 0)$$

  - Find $k^* = \arg\max_k \boldsymbol{\Delta}(k)$
  - Update $\mathbf{H}^{\mathcal{S}}$ to $\begin{pmatrix} \mathbf{H}^{\mathcal{S}} \\ \overline{\mathbf{H}}_{k^*} \end{pmatrix}$

Simulations

- Consider the **H** matrices for standard IEEE test systems (IEEE 30-bus, 57-bus, 118-bus, and 300-bus)
- Evaluation metrics
  - The min number of measurements attacker needs to manipulate to pass the detection v.s. the fraction of measurements being protected
  - The min number of meters attacker needs to manipulate to pass the detection v.s. the fraction of buses having secure PMUs placed
- Refer to the paper for the numerical simulation results for both algorithms

Discussion

- One attack at a time. The attack model can be modified to deal with the attacks to multiple states
  - However, the optimization problem may be infeasible
  - Hence, an alternative attack modeling needs investigating
- In the measurement subset selection algorithm, only one measurement is chosen to protect at one time. Is there any approach to choose multiple measurements to protect at one time?
- Grid topology changes such as line outages, meter failures, meter adding, etc.
  - The new algorithms are worthy investigating to incorporate the dynamics of the power grid