Worst-case Robust False Data Injection Attacks on Electricity Market

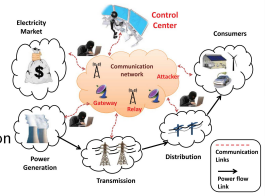
Mengheng Xue and Ali Tajer
Rensselaer Polytechnic Institute

False Data Injection Attacks

definition: cyber attack against state estimation

impacts

- state estimation error
- system black-out
- power delivery disruption
- financial misconduct



Monitoring Model

From operator's respective

- measurement model: $\boldsymbol{z} = \boldsymbol{H}_s + \boldsymbol{w}$
- ML state estimate model: $\hat{\boldsymbol{x}} = \boldsymbol{K}\boldsymbol{z}$,
- residue-based bad data detection: $\|(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}\|_2 \le \tau$

Network Uncertainty Model

Uncertainty model:

- partial information about $\boldsymbol{Q}$ is in the set $\mathcal{A}(\beta) = \{\boldsymbol{Q} \mid \boldsymbol{Q} = \tilde{\boldsymbol{Q}} + \Delta\boldsymbol{Q}, \|\boldsymbol{Q}\|_2 \le \beta\}$
- $\boldsymbol{p}^*$, $\boldsymbol{\ell}^*$ and $\boldsymbol{f}^*$ reported by RTOs in the day-ahead market

Attack Model

From attacker's respective:

- attacked measurement: $\boldsymbol{z}' = \boldsymbol{z} + \boldsymbol{z}_a$
- compromised state estimate: $\hat{\boldsymbol{x}}' = \hat{\boldsymbol{x}} + \boldsymbol{K}\boldsymbol{z}_a$,
- residue for bad data detection: $\boldsymbol{r}' = \boldsymbol{r} + \boldsymbol{r}_a$, where $\boldsymbol{r}_a = (\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a$
- undetectable attack: $\|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\| \le \varepsilon,\ \forall k \in \{1,\dots,\nu\}$

ε-robust attack constraint

$\|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \le \varepsilon,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall k \in \{1,\dots,\nu\}$

Electricity Market

- **Day-Ahead Market**:

$$\begin{aligned} \underset{\boldsymbol{p}}{\text{minimize}} \quad & \mathbf{1}_M \cdot \boldsymbol{C}(\boldsymbol{p}) \\ \text{subject to} \quad & \mathbf{1}_M \cdot \boldsymbol{p} = \mathbf{1}_J \cdot \boldsymbol{\ell} \\ & p_m^{\min} \le p_m \le p_m^{\max}, \quad \forall m \in \{1,\dots,M\} \\ & f_l^{\min} \le f_l \le f_l^{\max}, \quad \forall l \in \{1,\dots,L\} \end{aligned}$$

- **Real-Time Market**:

$$\begin{aligned} \underset{\Delta\boldsymbol{p}}{\text{minimize}} \quad & \mathbf{1}_M \cdot \boldsymbol{C}(\hat{\boldsymbol{p}} + \Delta\boldsymbol{p}) \\ \text{subject to} \quad & \mathbf{1}_M \cdot \Delta\boldsymbol{p} = 0 \\ & \Delta p_m^{\min} \le \Delta p_m \le \Delta p_m^{\max}, \quad \forall m \in \{1,\dots,M\} \\ & \Delta f_l \le 0, \quad \forall l \in \Omega_+ \\ & \Delta f_l \ge 0, \quad \forall l \in \Omega_- \end{aligned}$$

Profit Model

- LMPs at each load buses: $\lambda_l = \lambda_{\text{ref}} + \boldsymbol{H}_l^T \cdot \pi$
- virtual bidding profit: $g(\boldsymbol{z}') = \lambda_{l_1}^{\text{RT}} - \lambda_{l_2}^{\text{RT}} + \lambda_{l_2}^{\text{DA}} - \lambda_{l_1}^{\text{DA}}$

positive $g(\boldsymbol{z}')$ conditions:

- $\lambda_{l_2}^{\text{DA}} - \lambda_{l_1}^{\text{DA}} \ge 0$
- $\forall l \in \mathcal{L}_+$ we have $\hat{f}_l' \ge f_l^{\min}$
- $\forall l \in \mathcal{L}_-$ we have $\hat{f}_l' \le f_l^{\max}$

δ-profitable constraints

$$\begin{aligned} f_l^* + \boldsymbol{Q}_l\boldsymbol{z}_a &\le f_l^{\max} - \delta,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall l \in \mathcal{L}_- \\ f_l^* + \boldsymbol{Q}_l\boldsymbol{z}_a &\ge f_l^{\min} + \delta,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall l \in \mathcal{L}_+ \end{aligned}$$

Attack strategy

Goal: maximizing the attacker's probability of making profitable trades.

- **stage** 1: in the day-ahead market
  - buy and sell equal amount of energy at location j_2 and j_1 respectively
- **stage** 2: in the real-time market
  - construct and inject attack vector $\boldsymbol{z}_a$
  - sell and buy the same amount energy at location j_2 and j_1 respectively

Robust Attack

Goal: find an ε-robust attack vector $\boldsymbol{z}_a$ such that the profit confidence δ is maximized.

robust attack strategy

$$\begin{aligned} \underset{\boldsymbol{z}_a \in \mathcal{S}}{\text{maximize}} \quad & \delta \\ \text{subject to} \quad & \|\boldsymbol{e}_k(\boldsymbol{I}-\boldsymbol{Q})\boldsymbol{z}_a\|_2 \le \varepsilon,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall k \in \{1,\dots,\nu\} \\ & f_l^* + \boldsymbol{Q}_l\boldsymbol{z}_a \le f_l^{\max} - \delta,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall l \in \mathcal{L}_- \\ & f_l^* + \boldsymbol{Q}_l\boldsymbol{z}_a \ge f_l^{\min} + \delta,\ \forall \boldsymbol{Q} \in \mathcal{A}(\beta),\ \forall l \in \mathcal{L}_+ \\ & \delta > 0 \end{aligned}$$

- it is semi-infinite nonconvex quadratic program

Worst-case Robust Attack

Goal: using worst-case approach to convert robust attack formulation into a convex SDP problem.

- in worst-case sense, ε-robust attack is equivalent to

worst-case δ-profitable attack

$$\begin{aligned} f_l^* + \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{Q}}_l\boldsymbol{z}_a &\le f_l^{\max} - \delta,\ \forall l \in L_- \\ f_l^* - \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{Q}}_l\boldsymbol{z}_a &\ge f_l^{\min} + \delta,\ \forall l \in L_+ \end{aligned}$$

- in worst-case sense, δ-profitable attack is equivalent to

worst-case ε-robust attack constraint

there exists a $\gamma \ge 0$ such that for $\forall k \in \{1,\dots,\nu\}$,

$$\boldsymbol{T}_k \triangleq \begin{bmatrix} \varepsilon^2 & \boldsymbol{z}_a^T(\boldsymbol{I}-\tilde{\boldsymbol{Q}})^T\boldsymbol{e}_k^T & -\beta\boldsymbol{z}_a^T \\ \boldsymbol{e}_k(\boldsymbol{I}-\tilde{\boldsymbol{Q}})\boldsymbol{z}_a & 1-\gamma & \boldsymbol{0} \\ -\beta\boldsymbol{z}_a & \boldsymbol{0} & \gamma\boldsymbol{I} \end{bmatrix} \succeq 0$$

- in worst-case sense, robust attack strategy is

worst-case robust attack strategy

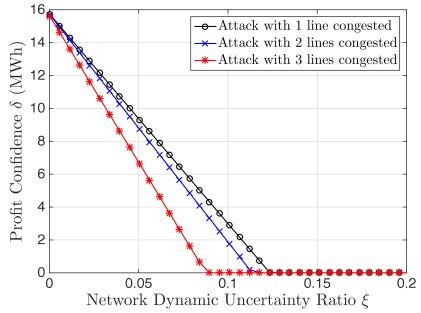
$$\begin{aligned} \underset{\boldsymbol{z}_a \in \mathcal{S}, \gamma \ge 0}{\text{maximize}} \quad & \delta \\ \text{subject to} \quad & \boldsymbol{T}_k \succeq 0,\ \forall k \in \{1,\dots,\nu\} \\ & f_l^* + \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{Q}}_l\boldsymbol{z}_a \le f_l^{\max} - \delta,\ \forall l \in L_- \\ & f_l^* - \beta\|\boldsymbol{z}_a\|_2 + \tilde{\boldsymbol{Q}}_l\boldsymbol{z}_a \ge f_l^{\min} + \delta,\ \forall l \in L_+ \\ & \delta > 0 \end{aligned}$$

- it is a convex SDP problem.

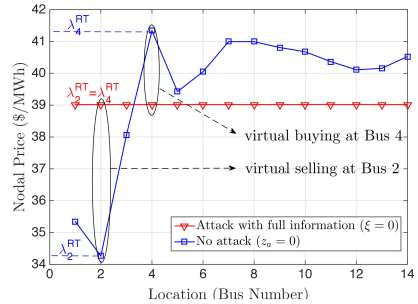
simulation

IEEE 14-bus system

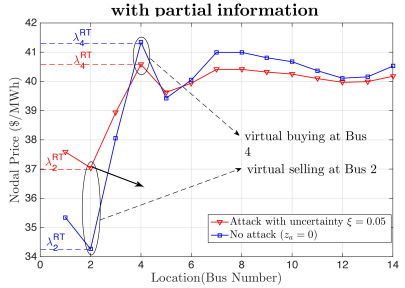
$\xi = \beta/\|\boldsymbol{Q}\|_2$



with full information



with partial information



conclusions

- consider limited adversary with partial information
- propose worst-case robust attack strategy
- test profit confidence decreasing with uncertainty