Robustness Analysis of Power Grid under False Data Attacks Against AC State Estimation

Presenter: Ming Jin

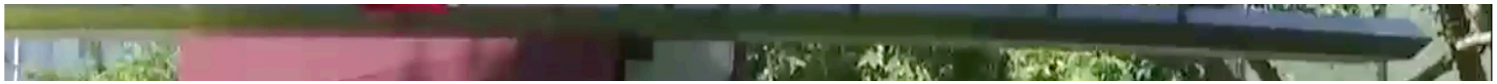
INFORMS 2017

Ming Jin, Prof Javad Lavaei, and Prof Karl Johansson

Power system resilience against cyber attack has become a critical issue

BRIEF

NERC proposal targets cybersecurity risks in electric system supply chains

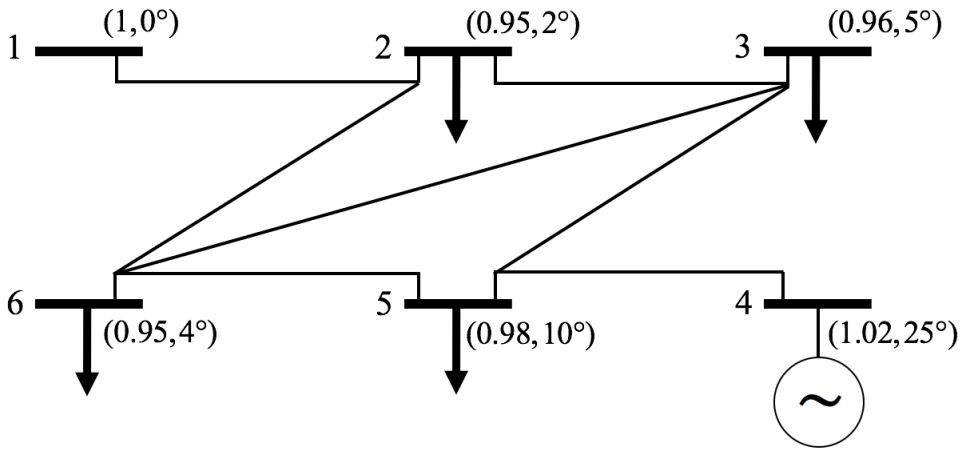


Outline

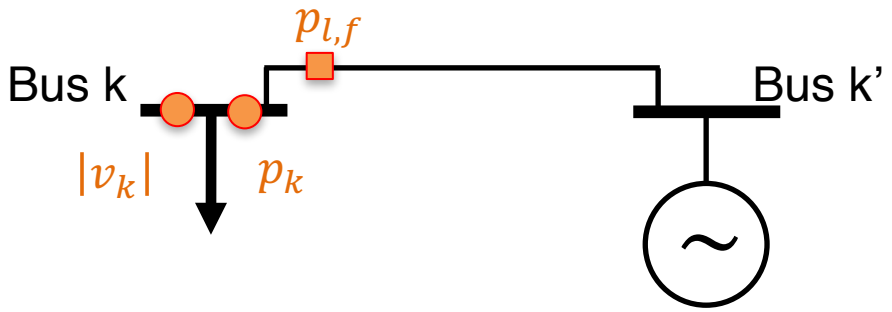
- Power system modeling and state estimation
- False data injection attack (FDIA) framework
- Semidefinite programming relaxation
- Experiments
- Conclusion

Power system modeled as a graph

- A power system $\mathcal{G} = (\mathcal{N}, \mathcal{L})$
  - Transmission lines, buses, and transformers
- Complex voltage: $\boldsymbol{v} = [v_1, v_2, \ldots, v_n]^T \in \mathbb{C}^n$
- Nodal current injection: $\boldsymbol{i} = \boldsymbol{Y}\boldsymbol{v}$
- Injected complex power: $\boldsymbol{p} + \boldsymbol{q}j = \mathrm{diag}(\boldsymbol{v}\boldsymbol{i}^*)$



Nodal and line measurements



- Voltage magnitude and nodal power injections:

$$|v_k|^2 = \mathrm{Tr}(\boldsymbol{E}_k \boldsymbol{v}\boldsymbol{v}^*),\ p_k = \mathrm{Tr}(\boldsymbol{Y}_{k,p} \boldsymbol{v}\boldsymbol{v}^*),\ q_k = \mathrm{Tr}(\boldsymbol{Y}_{k,p} \boldsymbol{v}\boldsymbol{v}^*)$$

where $\boldsymbol{E}_k = \boldsymbol{e}_k \boldsymbol{e}_k^T$, $\boldsymbol{Y}_{k,p} = \frac{1}{2}(\boldsymbol{Y}^* \boldsymbol{E}_k + \boldsymbol{E}_k \boldsymbol{Y})$, $\boldsymbol{Y}_{k,q} = \frac{j}{2}(\boldsymbol{E}_k \boldsymbol{Y} - \boldsymbol{Y}^* \boldsymbol{E}_k)$

- Branch active and reactive power flows:

$$p_{l,f} = \mathrm{Tr}(\boldsymbol{Y}_{l,p_f} \boldsymbol{v}\boldsymbol{v}^*),\ p_{l,t} = \mathrm{Tr}(\boldsymbol{Y}_{l,p_t} \boldsymbol{v}\boldsymbol{v}^*)$$
$$q_{l,f} = \mathrm{Tr}(\boldsymbol{Y}_{l,q_f} \boldsymbol{v}\boldsymbol{v}^*),\ q_{l,t} = \mathrm{Tr}(\boldsymbol{Y}_{l,q_t} \boldsymbol{v}\boldsymbol{v}^*)$$

- All quantities are quadratic functions of complex voltage, which is the state of the system

Power system state estimation

Problem statement:

- Given noisy measurements

$$m_r = \langle \boldsymbol{v}\boldsymbol{v}^*, \boldsymbol{M}_r \rangle + w_r + b_r$$

measurement unknown state noise bad data

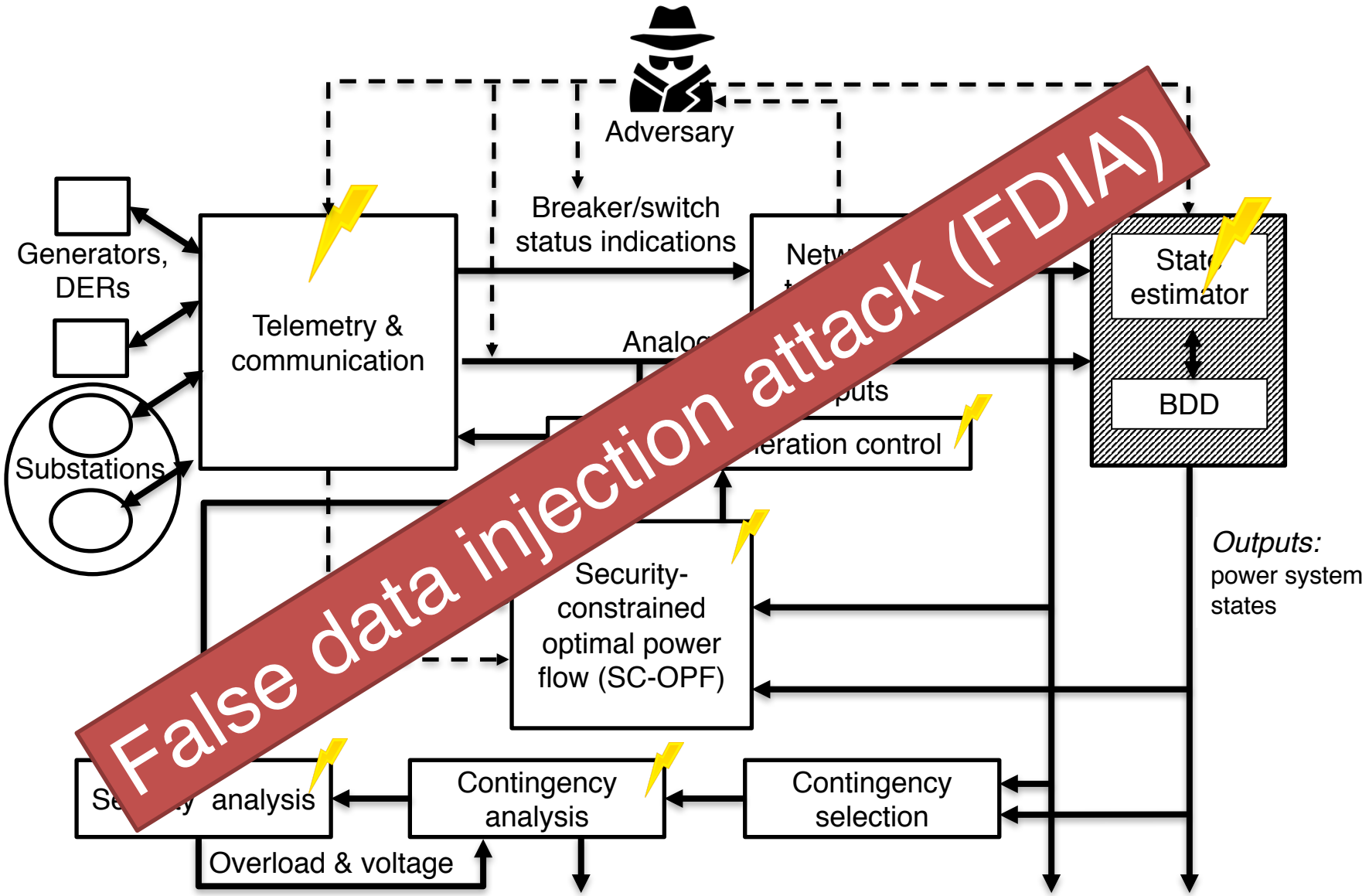
estimate the unknown state $\boldsymbol{v}$.

Why state estimation?

- Provides real-time power system conditions
- Constitutes the core of online security analysis
- Provides diagnostics for modeling and maintenance

(Zhang, Madani, Lavaei, 2017)

Cyber attack vs.resilience



FDIA is stealthy if the spurious data correspond to a valid state

- **State estimation:** Quadratic measurements subject to noise and bad data

$$m_r = \langle \boldsymbol{v}\boldsymbol{v}^*, \boldsymbol{M}_r \rangle + w_r + b_r$$

measurement unknown state noise adversarial data

Can be solved by Gauss-Newton or SDP

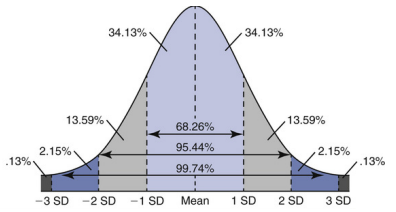
- **Stealth attack:**

$$b_r = m_r - \langle \tilde{\boldsymbol{v}}\tilde{\boldsymbol{v}}^*, \boldsymbol{M}_r \rangle$$

Bad data detection

Residuals:

$$m_r - \langle \hat{\boldsymbol{v}}\hat{\boldsymbol{v}}^*, \boldsymbol{M}_r \rangle$$



FDIA causes spurious state estimation by tampering sensor data

- DC-based: (Liu et al., 2010) (Kosut et al., 2010) (Sandberg et al., 2010) (Dan and Sandberg, 2010) (Yuan et al., 2011) (Sou et al., 2013) (Hendrickx et al., 2014)
- Negative impact: Electricity market (Xie et al., 2010), Load redistribution (Yuan et al., 2011)

- AC-based

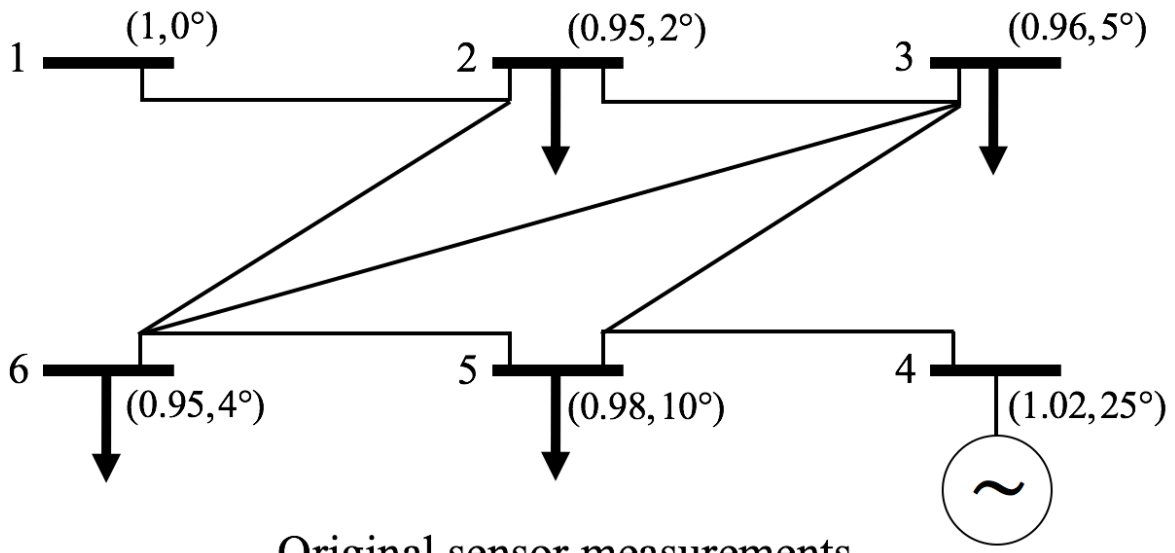
(Rahman and Mohsenian-Rad, 2013)

(Hug and Giampapa, 2012)

Stealth vs. sparsity

State estimation can be falsified..

True system state



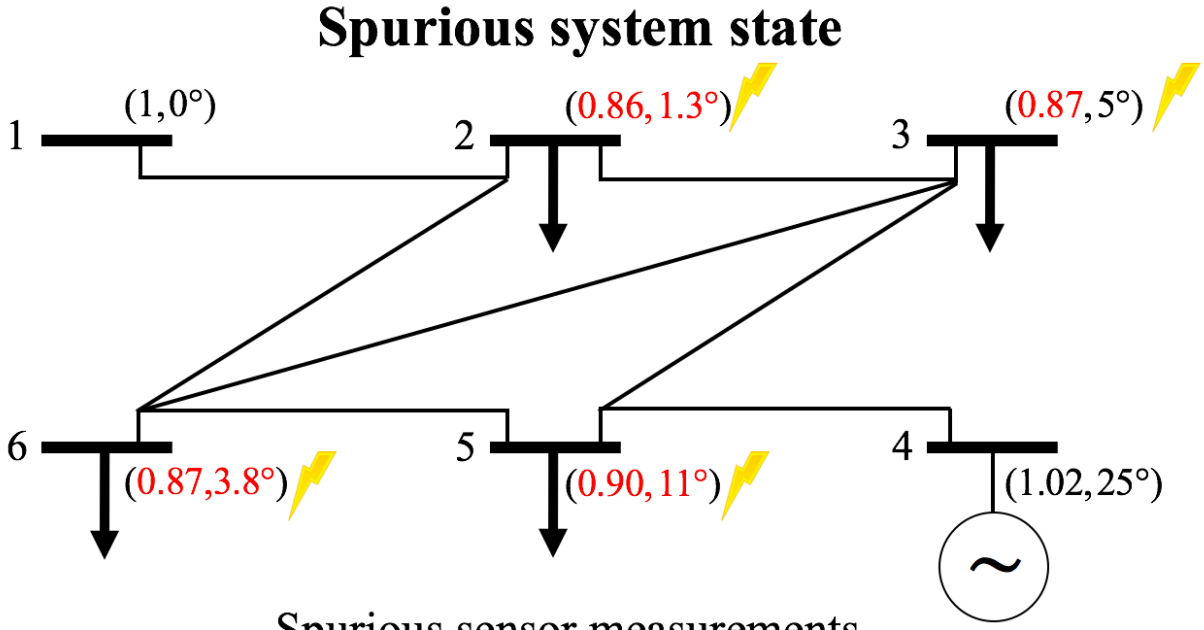
Original sensor measurements

P_1	v_1	P_2	Q_2	P_3	Q_3	P_4	v_4	P_5	Q_5	P_6	Q_6
.087	1	-.504	-.110	-.067	.048	1.668	1.02	-.134	.588	-.570	.180

p_{12}	p_{21}	p_{23}	p_{32}	p_{45}	p_{54}	p_{56}	p_{65}	p_{26}	p_{62}	p_{35}	p_{53}	p_{36}	p_{63}
.087	-.069	-.280	.293	1.668	-1.319	.659	-.604	-.155	.160	-.488	.526	.128	-.126

q_{12}	q_{21}	q_{23}	q_{32}	q_{45}	q_{54}	q_{56}	q_{65}	q_{26}	q_{62}	q_{35}	q_{53}	q_{36}	q_{63}
.394	-.423	.175	-.207	-.945	1.244	-.338	.347	.138	-.177	.309	-.318	-.054	.010

..with sparse sensor data attack



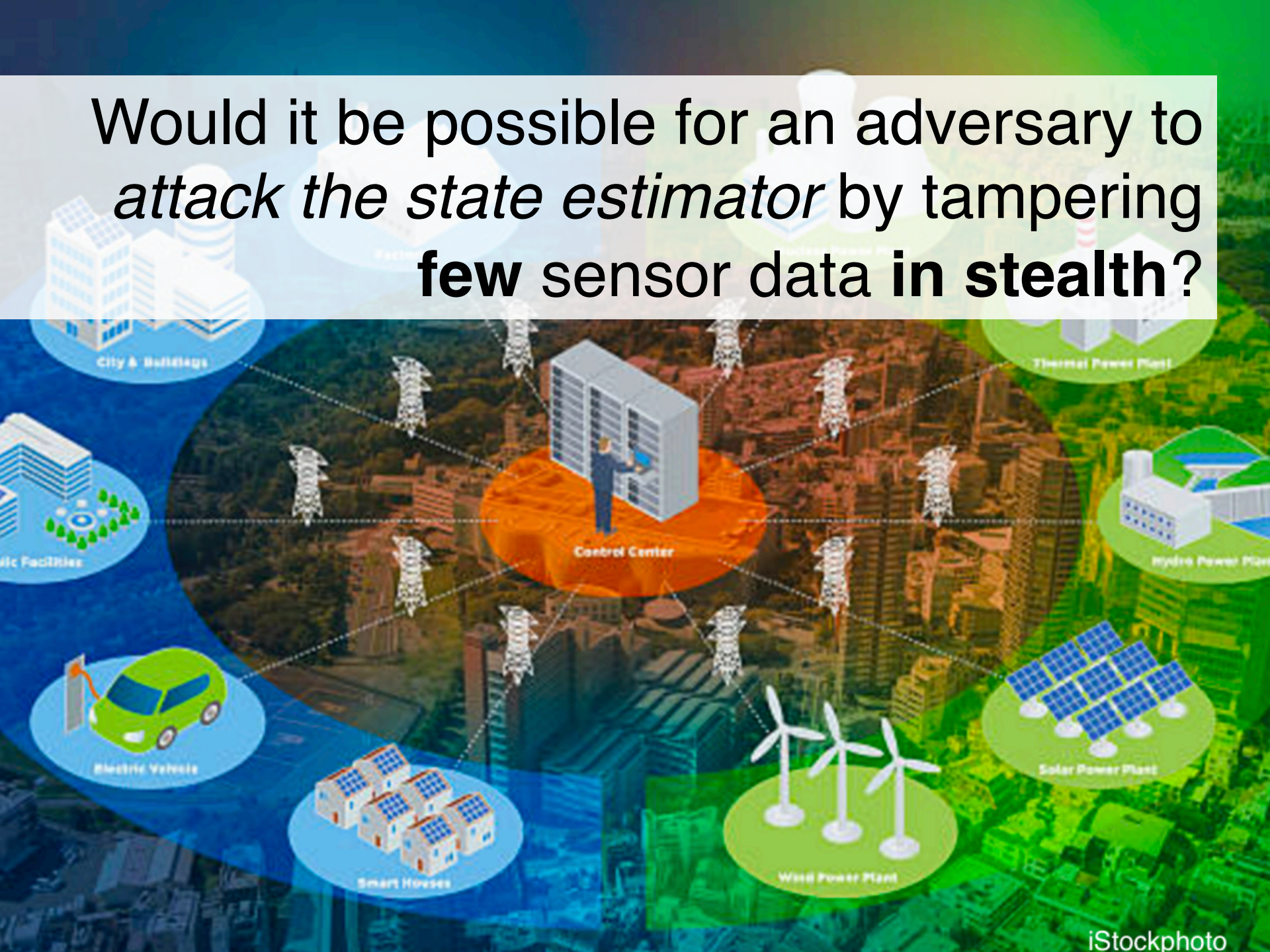
Spurious sensor measurements

P_1	v_1	P_2	Q_2	P_3	Q_3	P_4	v_4	P_5	Q_5	P_6	Q_6
.580	1	**-.914**	**-.365**	-.067	.048	**1.870**	1.02	**-.319**	**.053**	-.570	.180

p_{12}	p_{21}	p_{23}	p_{32}	p_{45}	p_{54}	p_{56}	p_{65}	p_{26}	p_{62}	p_{35}	p_{53}	p_{36}	p_{63}
.580	**-.485**	-.280	.293	**1.870**	**-1.522**	.659	-.604	-.155	.160	-.488	.526	.128	-.126

q_{12}	q_{21}	q_{23}	q_{32}	q_{45}	q_{54}	q_{56}	q_{65}	q_{26}	q_{62}	q_{35}	q_{53}	q_{36}	q_{63}
.757	**-.705**	**.189**	-.207	**-.372**	**.674**	**-.319**	.347	**.151**	-.177	.309	**-.302**	-.054	.010

Would it be possible for an adversary to *attack the state estimator* by tampering **few** sensor data **in stealth**?



General FDIA framework with cardinality / stealth constraints

$$\min_{\tilde{\boldsymbol{v}} \in \mathbb{C}^{n_b}, \boldsymbol{b} \in \mathbb{R}^{n_m}} \quad h(\tilde{\boldsymbol{v}})$$

$$\text{s.t.} \quad b_r = m_r - \langle \tilde{\boldsymbol{v}} \tilde{\boldsymbol{v}}^*, \boldsymbol{M}_r \rangle$$

$$\|\boldsymbol{b}\|_0 \leq k$$

- Objective function $h(\tilde{\boldsymbol{v}})$
  - Target state attack: $h(\tilde{\boldsymbol{v}}) = \left\|\tilde{\boldsymbol{v}} - \boldsymbol{v}_{tg}\right\|_2^2$
  - Voltage collapse attack: $h(\tilde{\boldsymbol{v}}) = \|\tilde{\boldsymbol{v}}\|_2^2$
  - State deviation attack: $h(\tilde{\boldsymbol{v}}) = -\|\tilde{\boldsymbol{v}} - \boldsymbol{v}_{true}\|_2^2$

Semidefinite programming (SDP)

SDP standard form:

$$\min \langle \boldsymbol{C}, \boldsymbol{W} \rangle$$

$$\text{s.t.} \quad x_i = \langle \boldsymbol{W}, \boldsymbol{M}_r \rangle$$

$$\boldsymbol{W} \succcurlyeq \boldsymbol{0}$$

Definition: a Hermitian matrix $\boldsymbol{W} \in \mathbb{H}^n$ is positive semidefinite (PSD), $\boldsymbol{W} \succcurlyeq \boldsymbol{0}$ iff:

- All eigenvalues of $\boldsymbol{W}$ are non-negative
- $\boldsymbol{x}^* \boldsymbol{W} \boldsymbol{x} \geq \boldsymbol{0}$ for all $\boldsymbol{x} \in \mathbb{C}^n$

Wide applications in systems and control theory, robust optimization, nonconvex optimization

Convexification procedure

$$\min \langle \tilde{\boldsymbol{v}}\tilde{\boldsymbol{v}}^*, \boldsymbol{M}_{tg} \rangle + 2Re\{\boldsymbol{v}_{tg}^* \tilde{\boldsymbol{v}}\}$$
$$\text{s.t.} \quad b_r = m_r - \langle \tilde{\boldsymbol{v}}\tilde{\boldsymbol{v}}^*, \boldsymbol{M}_r \rangle$$
$$\|\boldsymbol{b}\|_0 \leq k$$

- **Transformation:** Replace $\tilde{\boldsymbol{v}}\tilde{\boldsymbol{v}}^*$ with $\boldsymbol{W}$
- The augmented matrix $\mathbf{Z} = \begin{bmatrix} 1 & \tilde{\boldsymbol{v}}^* \\ \tilde{\boldsymbol{v}} & \boldsymbol{W} \end{bmatrix}$ is positive semidefinite and rank 1

$$\min \langle \boldsymbol{W}, \boldsymbol{M}_{tg} \rangle + 2Re\{\boldsymbol{v}_{tg}^* \tilde{\boldsymbol{v}}\}$$
$$\text{s.t.} \quad b_r = m_r - \langle \boldsymbol{W}, \boldsymbol{M}_r \rangle$$
$$\begin{bmatrix} 1 & \tilde{\boldsymbol{v}} \\ \tilde{\boldsymbol{v}} & \boldsymbol{W} \end{bmatrix} \succcurlyeq 0, \; rank{=}1$$
$$\|\boldsymbol{b}\|_0 \leq k$$

$$\min \langle \boldsymbol{W}, \boldsymbol{M}_{tg} \rangle + 2Re\{\boldsymbol{v}_{tg}^* \tilde{\boldsymbol{v}}\}$$
$$+ \alpha \|\boldsymbol{b}\|_1 + \langle \boldsymbol{W}, \boldsymbol{M}_{penalty} \rangle$$
$$\text{s.t.} \quad b_r = m_r - \langle \boldsymbol{W}, \boldsymbol{M}_r \rangle$$
$$\begin{bmatrix} 1 & \tilde{\boldsymbol{v}} \\ \tilde{\boldsymbol{v}} & \boldsymbol{W} \end{bmatrix} \succcurlyeq 0$$

- **Relaxation:** relax the rank 1 constraint
- **Penalty:** add penalty for the rank and cardinality constraint

If the rank-1 constraint is satisfied, then we can recover a near-global stealthy attack solution

Key result: rank penalty design and performance bounds

Theorem: For carefully designed $\boldsymbol{M}_{penalty}$ and α, if the measurements include real and reactive branch power flows, and nodal voltage magnitudes, we have

- The attack $\boldsymbol{b}$ is stealthy, and sparse for large α
- The performance difference compared to an oracle by solving the original nonconvex problem is bounded

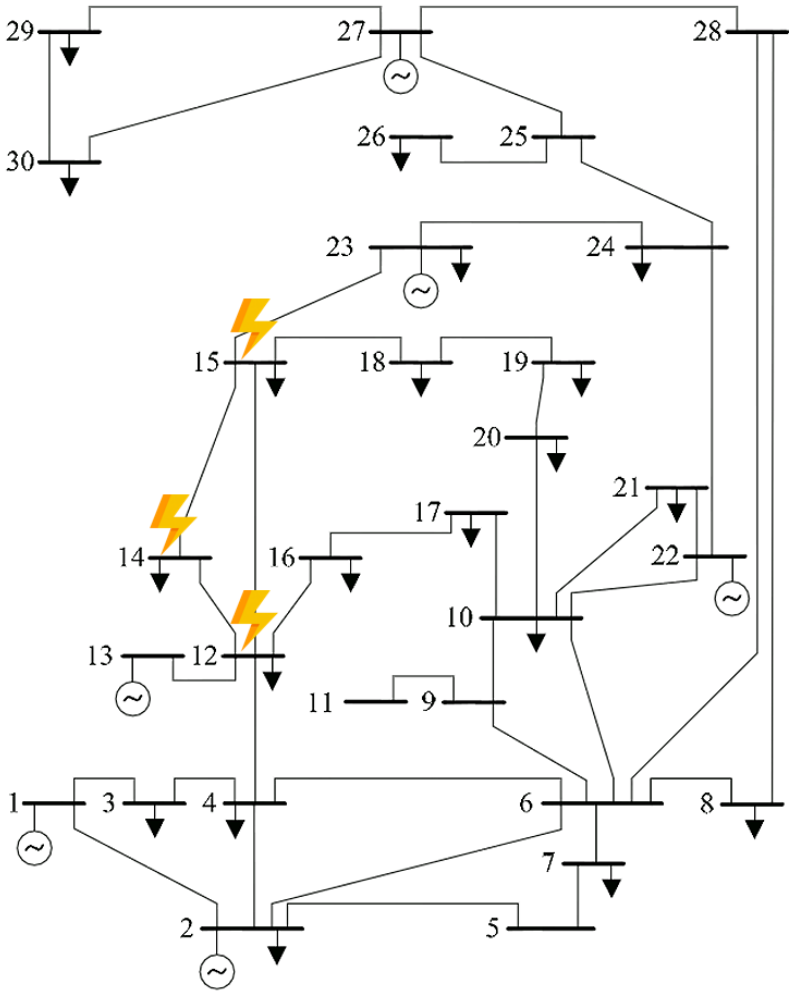
- Relation to compressed sensing: the trace penalty is equivalent to choosing $\boldsymbol{M}_{penalty}$ as the identity matrix
- Extends the low-rank optimization method to deal with the augmented matrix $\operatorname{rank}\left(\begin{bmatrix} 1 & \tilde{\boldsymbol{v}} \\ \tilde{\boldsymbol{v}} & \boldsymbol{W} \end{bmatrix}\right) = 1$, needed in a wide range of problems

Experiment on IEEE 30-bus

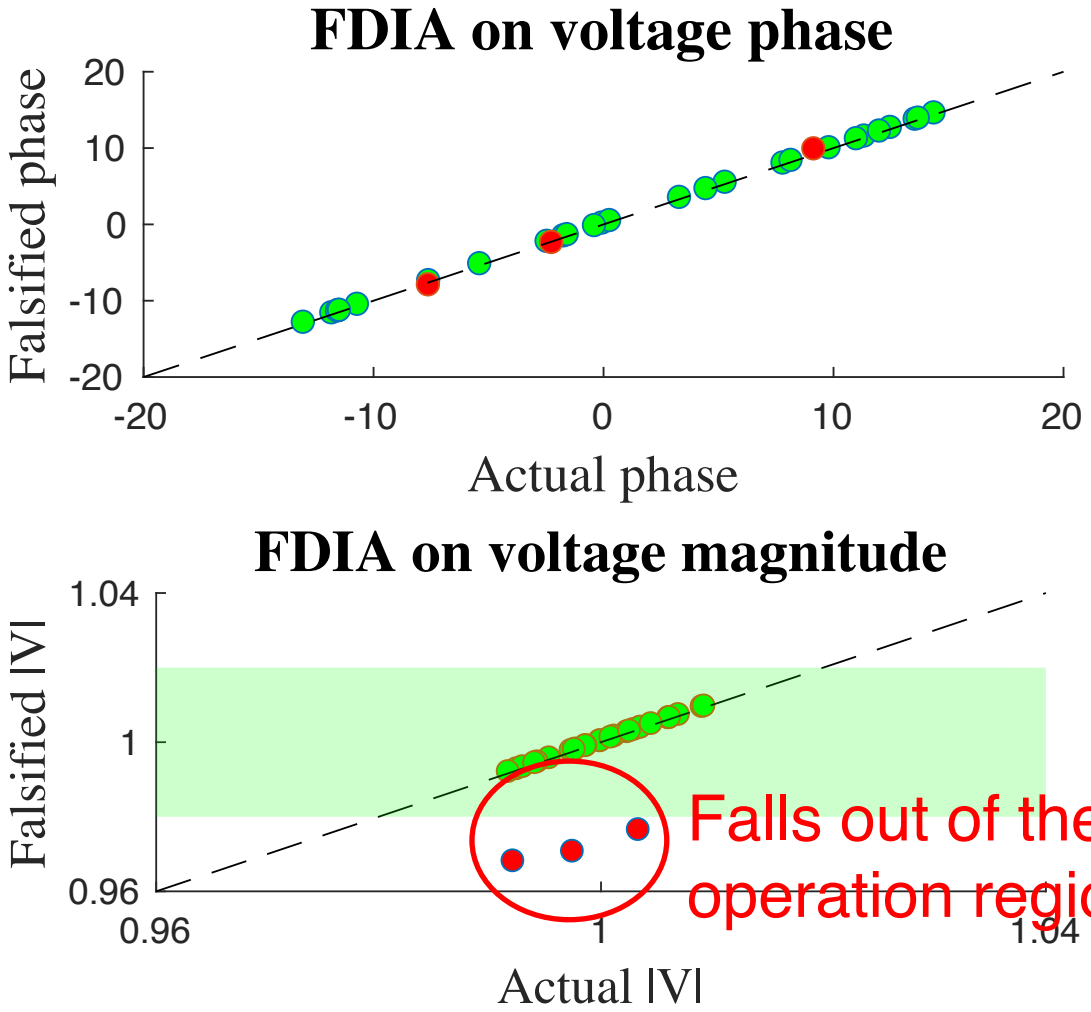
- Target attack:

$$h(\tilde{\boldsymbol{v}}) = \left\| \tilde{\boldsymbol{v}} - \boldsymbol{v}_{tg} \right\|_2^2$$

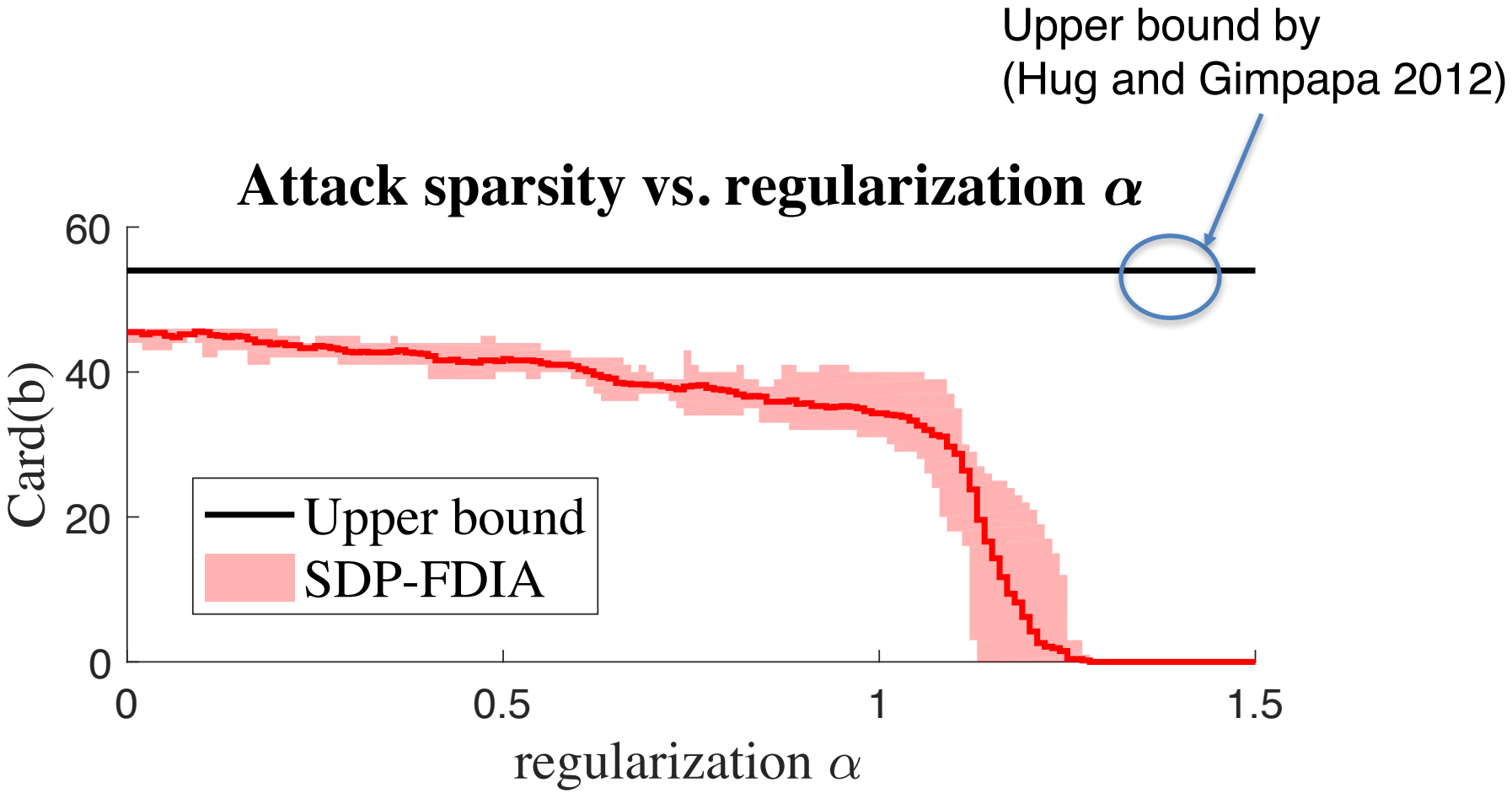
- Solve for the stealth attack $\boldsymbol{b}$ using SDP relaxation
- Estimate the spurious state using Gauss-Newton in MATPOWER
- Check for BDD



FDIA "tricks" the operator to believe a potential "voltage sag"



The sparsity is controlled by the l1 penalty weight α



FDIA is triggered by tampering a small set of sensors

system	α	Rank(Z)	Card(b)	Upper bound	Pass BDD
6-bus	.4	1	18	40	Yes
14-bus	.2	1	16	46	Yes
30-bus	1.16	1	21	54	Yes
39-bus	1.82	1	18	36	Yes
57-bus	.5	1	30	92	Yes

Our results analyze the *potential threat of cyber attack* on power grid *AC-based* state estimation.

It should be used to inform new designs of Bad Data Detection.

Theoretical contributions

- Formulation of the nonconvex FDIA problem for AC grid
- Convex relaxation of the problem with cardinality constraint using Semidefinite programming
  - design proper penalty matrix to induce rank 1 solution
  - Prove performance bounds of the near-optimal solution compared to the original problem