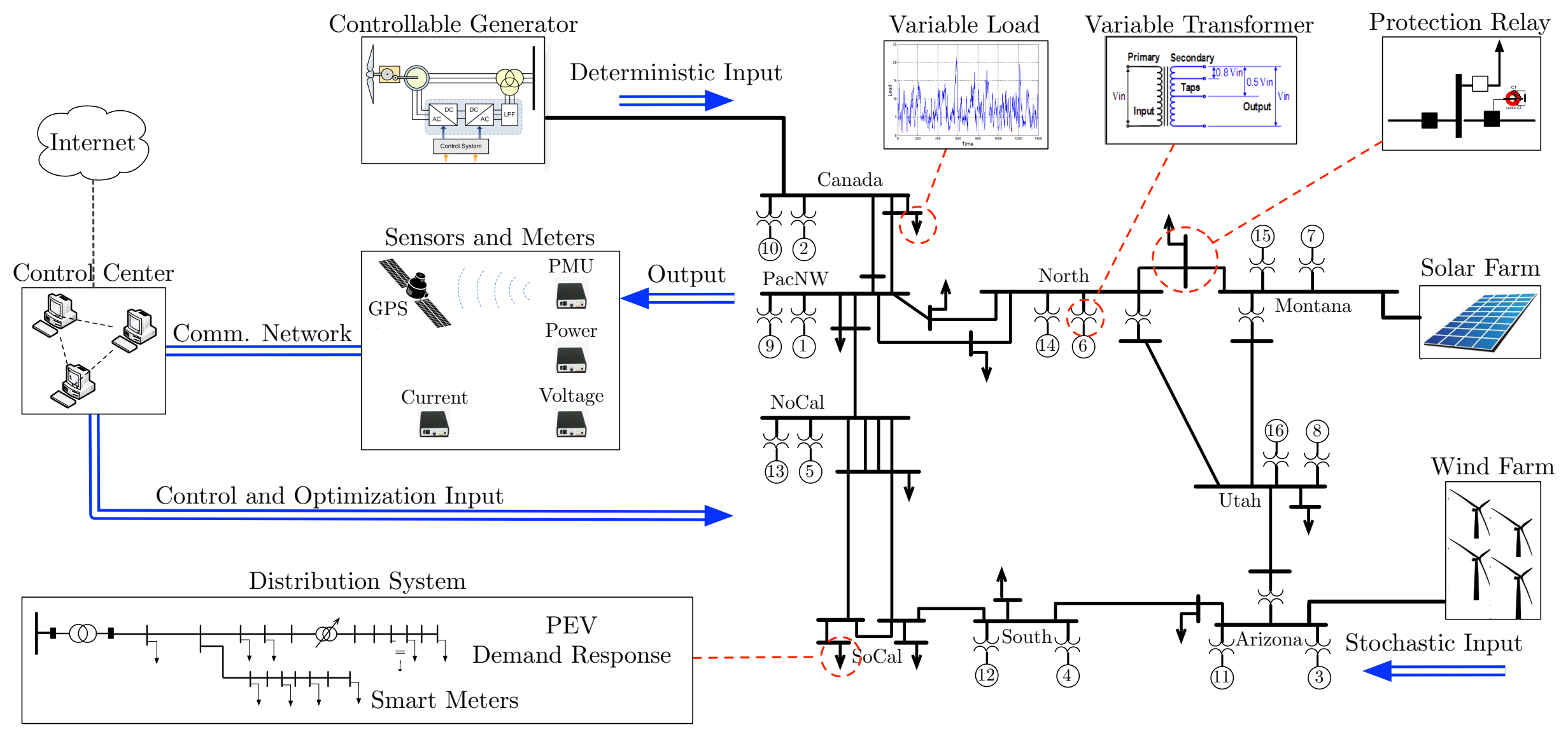
Control-Theoretic Defense Strategies for Cyber-Physical Systems

Fabio Pasqualetti and Amir-Hamed Mohsenian-Rad

Departments of Mechanical Engineering and Electrical Engineering
University of California, Riverside

Cyber-physical power grid



Dynamical model:

$$\begin{bmatrix} I & 0 & 0\\ 0 & M_g & 0\\ 0 & 0 & 0\end{bmatrix}\begin{bmatrix}\dot\delta\\ \dot\omega\\ \dot\theta\end{bmatrix} = \begin{bmatrix}0 & I & 0\\ \mathcal{L}_{gg}(\gamma) & D_g & \mathcal{L}_{gl}(\gamma)\\ \mathcal{L}_{lg}(\gamma) & 0 & \mathcal{L}_{ll}(\gamma)\end{bmatrix}\begin{bmatrix}\delta\\ \omega\\ \theta\end{bmatrix} + \begin{bmatrix}0\\ P_\omega\\ P_\theta\end{bmatrix}$$

$$y = \begin{bmatrix} C_\delta(\gamma) & C_\omega(\gamma) & C_\theta(\gamma)\end{bmatrix}\begin{bmatrix}\delta\\ \omega\\ \theta\end{bmatrix} + \eta$$

Research objectives and methodologies

Control-theoretic modeling of attack/defense:

- modeling and implementation of attacks
- centralized and localized attack/defense

Detection and classification monitors:

- detectability/identifiability in stochastic systems
- distributed vs centralized detection

Adaptive defense mechanisms:

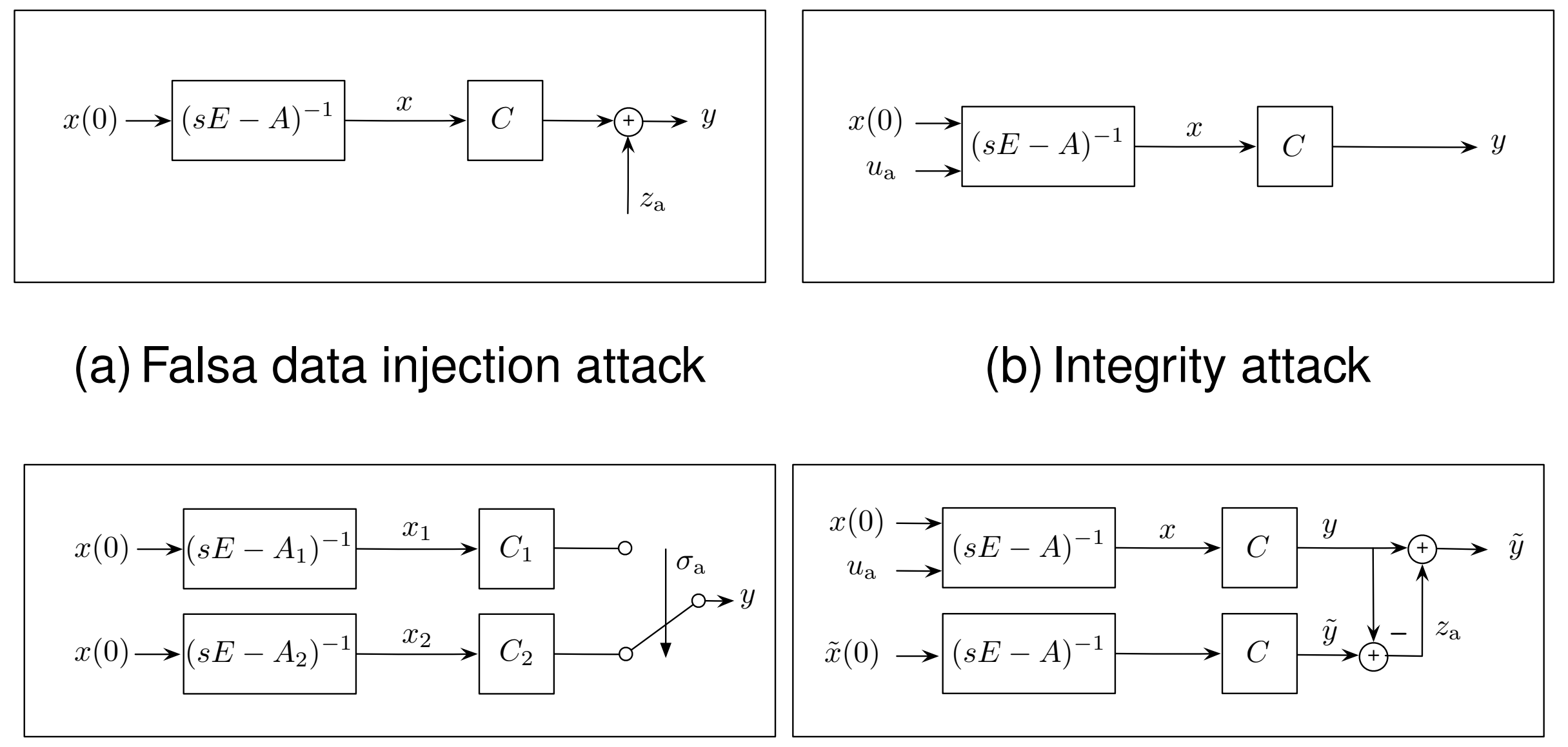
- online topology modification to limit attack
- system redesign based on available resources

Experimental validation:

- Synthesis of attacks/monitors via RTDS/PSCAD

These results are based upon work supported by NSF award ECCS-1405330.

Year 0: attacks in deterministic systems



(a) Falsa data injection attack

(b) Integrity attack

(c) Topology change attack

(d) Replay attack

Attack detectability $\Leftrightarrow \boldsymbol{y(x_1, 0, t) \not\equiv y(x_2, u, t)}$

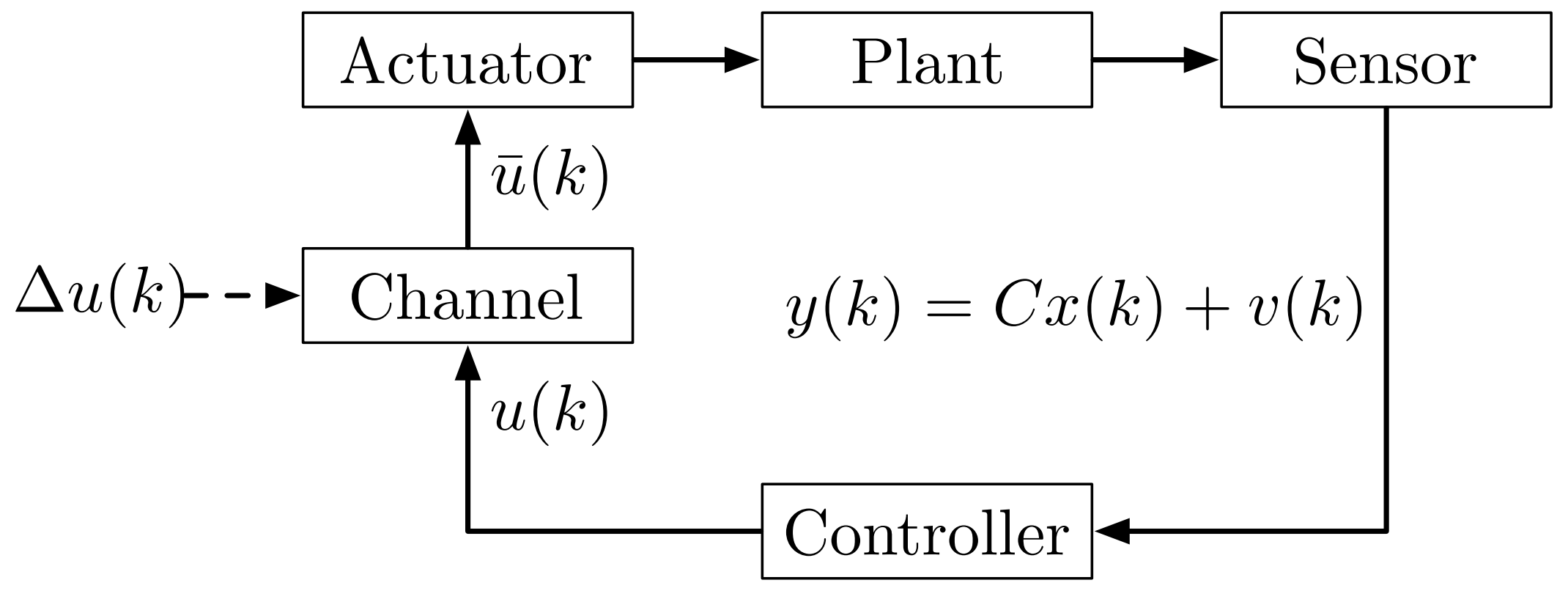
Attack identifiability $\Leftrightarrow \boldsymbol{y(x_1, u_1, t) \not\equiv y(x_2, u_2, t)}$

Fundamental detectability/identifiability limitations

Attacks remain undetected/unidentified iff they excite only the zero dynamics of the attacked system.

Years 1-2: security in stochastic systems

$$x(k+1) = Ax(k) + Bu(k) + w(k)$$



$$u(k) = F\hat x(k)$$
$$\hat x(k+1) = A\hat x(k) + Bu(k) + K(k)z(k)$$

- if attack undetected, controller implements Kalman filter with wrong data → performance degradation
- perf. degradation as induced error covariance
- ε-stealthiness via performance of *any* detector

Conditions for ε-stealthiness

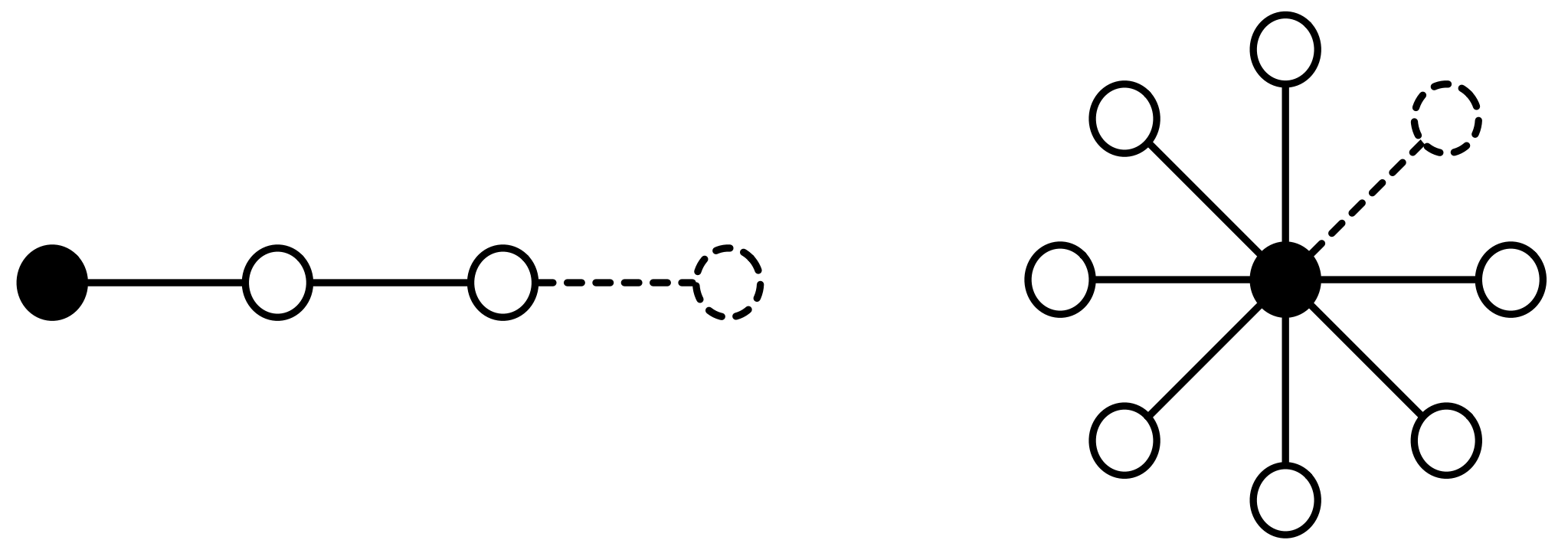
An attack is ε-stealthy only if

$$\limsup_{k\to\infty} \mathrm{KLD}(\tilde{y}_1^k \| y_1^k) \le \varepsilon,$$

- y_1^k measurements expected if no attack
- $\tilde{y}_1^k$ received measurements

Years 1-2: network observability radius

Modify network edges to prevent observability:



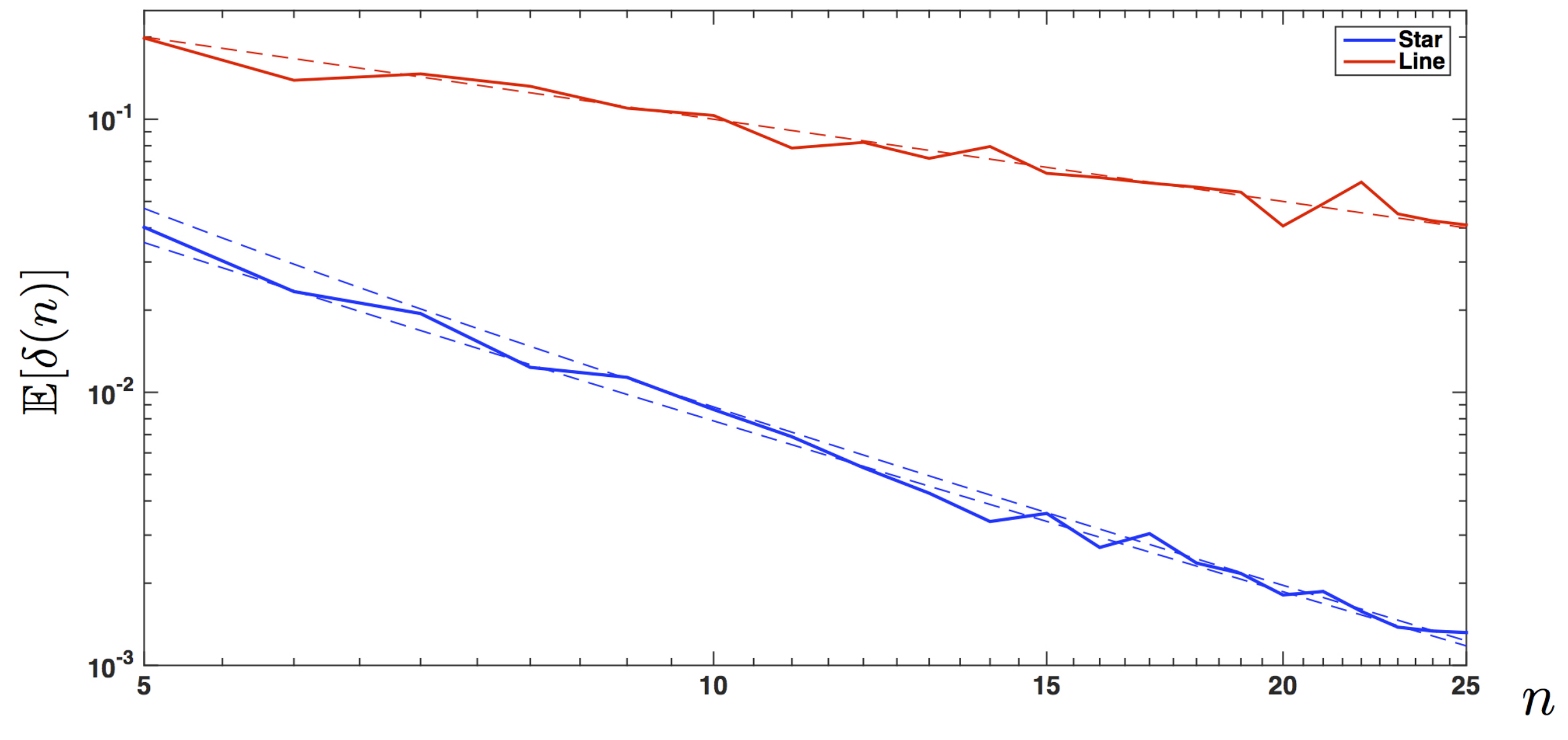
$$\min \|\boldsymbol{\Delta}\|_F$$

s.t. $(\boldsymbol{A} + \boldsymbol{\Delta})\boldsymbol{x} = \lambda \boldsymbol{x}$ (eigenvalue constraint)

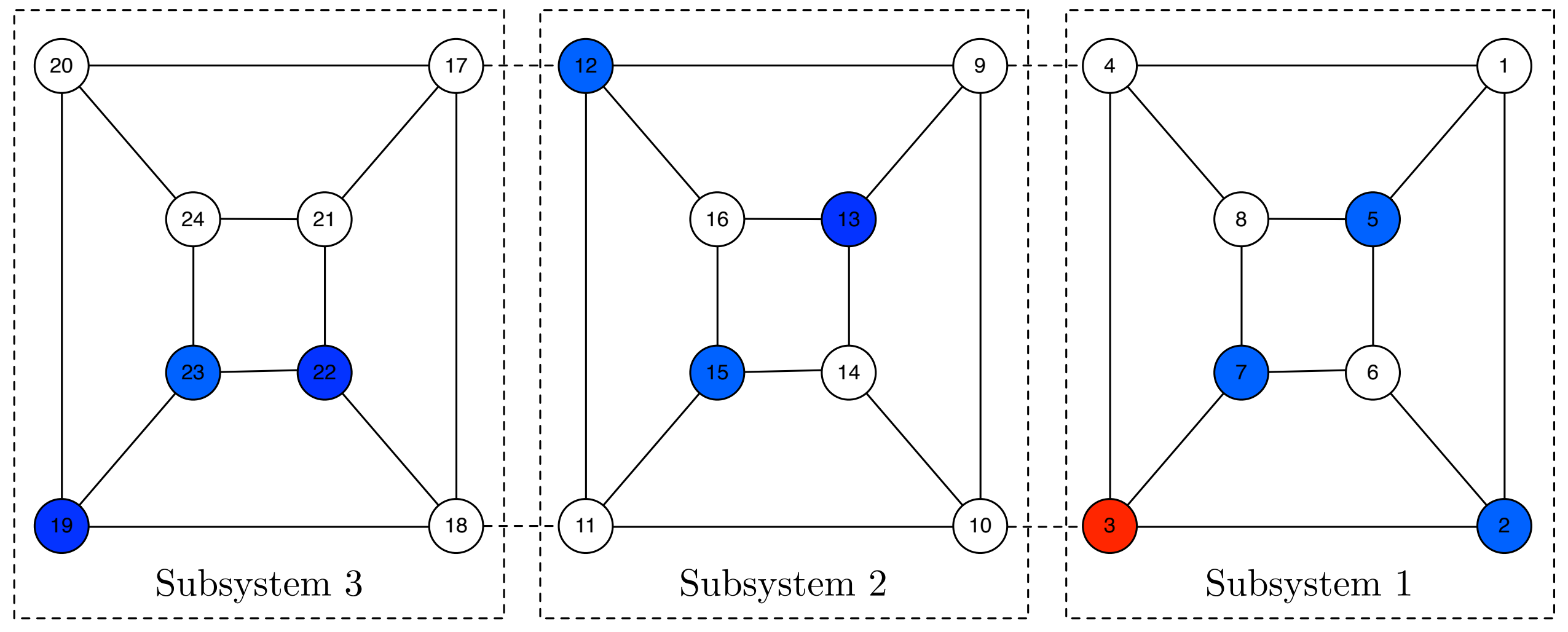
$C_{\mathcal{O}}\boldsymbol{x} = 0$ (unobservability)

$\boldsymbol{\Delta} \in \mathcal{A}_{\mathcal{H}}$ (structural constraint)

- analytic bounds/algorithms *(total least squares)*
- resilience of networks with random weights

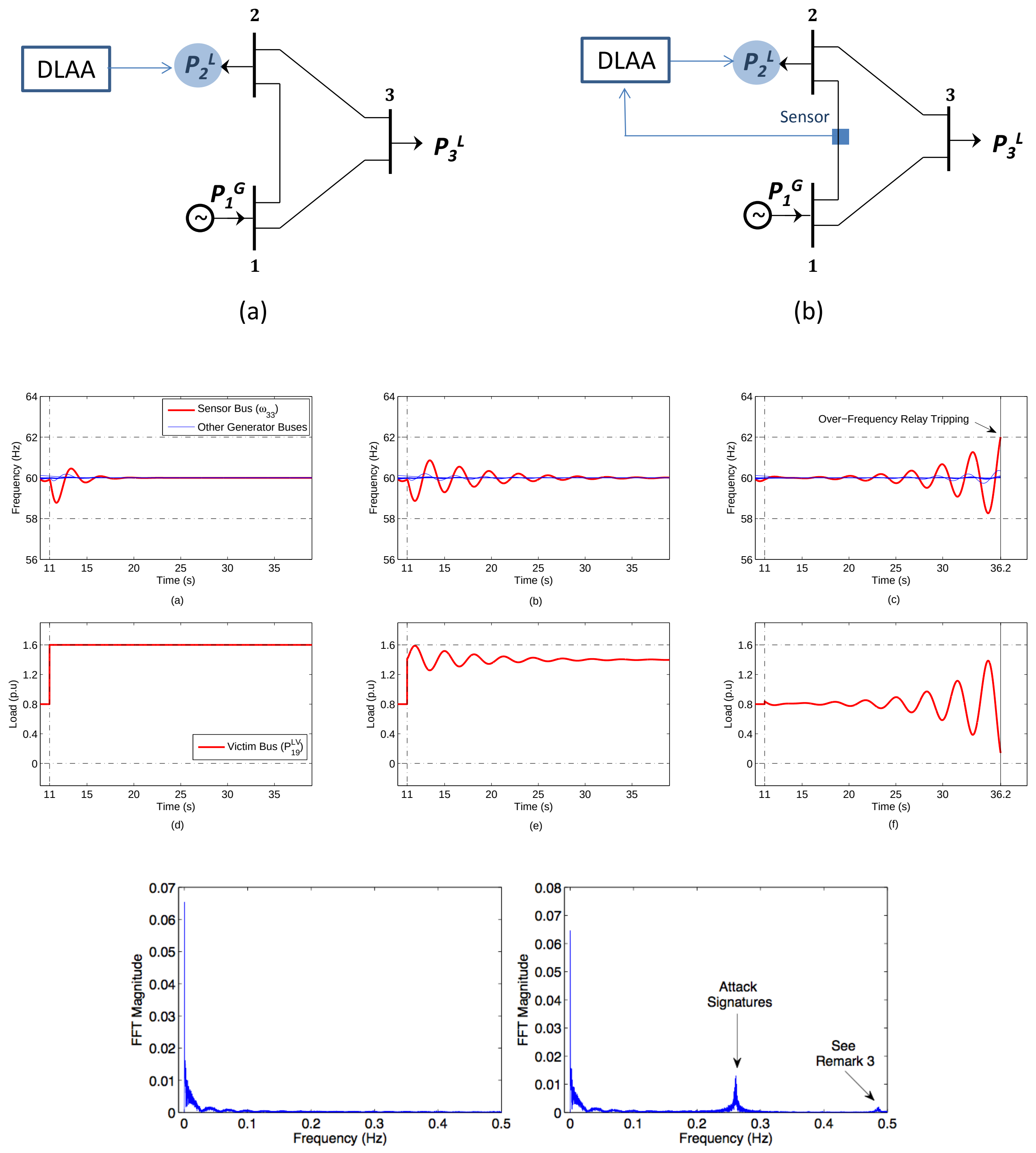


Years 1-2: distributed attack identification



- cooperation + unknown input observers
- complexity vs identification accuracy
- limitations of convexity reduction methods

Years 1-2: dynamic load altering attacks



- tamper with a group of loads (positive feedback)
- demand response and demand management
- time-frequency detection analysis

Selected products

- G. Bianchin, P. Frasca, A. Gasparri, and F. Pasqualetti. "The Observability Radius of Networks," *IEEE Transactions on Automatic Control*, To appear, 2016.
- S. Amini, H. Mohsenian-Rad, and F. Pasqualetti. "Dynamic load altering attacks against power system stability: Attack models and protection designs," *IEEE Transactions on Smart Grid*, To appear, 2016.
- C. Bai, F. Pasqualetti, and V. Gupta. "Data-Injection Attacks in Stochastic Control Systems: Detectability and Performance Tradeoffs," *Automatica*, Submitted, 2016.
- S. Zhao and F. Pasqualetti. "Network Design with Guaranteed Controllability and Robustness Performance," *IEEE Transactions on Control of Network Systems*, Submitted, 2016.
- C. Bai, F. Pasqualetti, and V. Gupta. "Security in Stochastic Control Systems: Fundamental Limitations and Performance Bounds," *American Control Conference*, pag. 195 – 200, Chicago, Il, July 2015 (best paper award finalist).
- S. Amini, F. Pasqualetti, and H. Mohsenian-Rad. "Detecting Dynamic Load Altering Attacks: A Data-Driven Time-Frequency Analysis," *Conference on Innovative Smart Grid Technologies*, To appear, 2015.
- F. Pasqualetti, F . Dörfler, and F. Bullo "A Divide-and-Conquer Approach to Distributed Attack Identification," *Conference on Decision and Control*, To appear, 2015.
- S. Amini, H. Mohsenian-Rad, and F. Pasqualetti. "Dynamic Load Altering Attacks in Smart Grid," *Conference on Innovative Smart Grid Technologies*, To appear, 2015.

Department of Mechanical Engineering - Bourns College of Engineering - University of California, Riverside fabiopas@engr.ucr.edu http://www.fabiopas.it