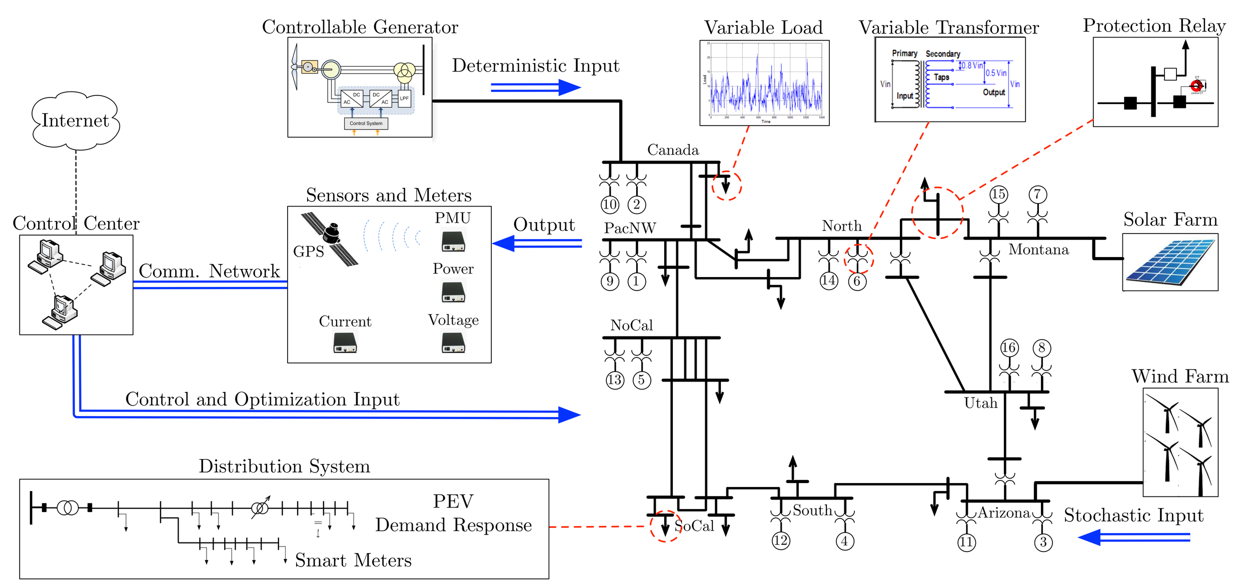
# Control-Theoretic Defense Strategies for Cyber-Physical Systems

**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 implementability of attacks
- centralized and localized attack/defense

*Detection and classification monitors:*

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

*Adaptive defense mechanisms:*

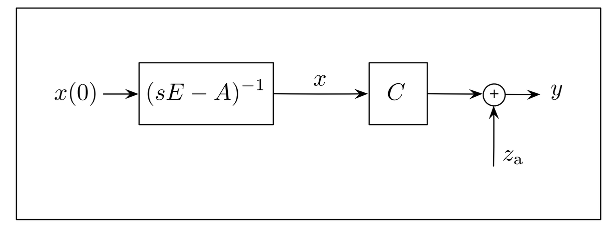
- online topology modification to limit attack
- system redesign based on available resources

*Experimental validation:*

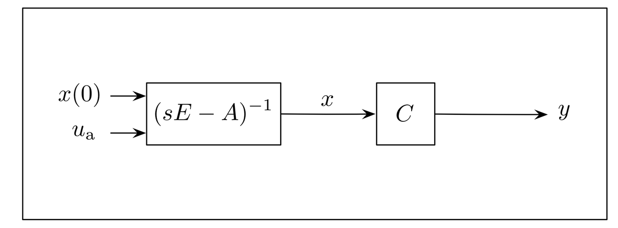
- Synthesis of attacks/monitors via RTDS/PSCAD

*This material is based upon work supported by NSF Award ECCS-1405330.*

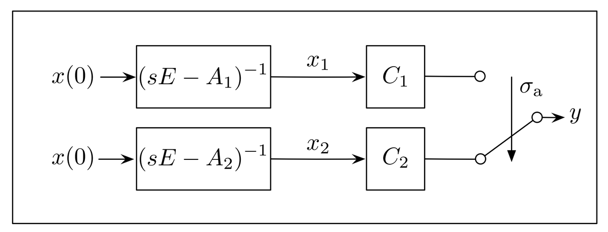
## Year 0: attacks in deterministic models



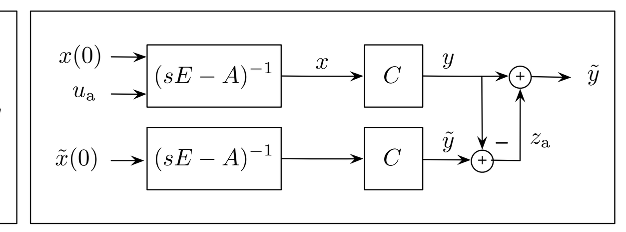
(a) Falsa data injection attack



(b) Integrity attack



(c) Topology change attack



(d) Replay attack

Attack detectability ⇔ distinguishable from measurements from a normal operating condition:

$$y(x_1, 0, t) \not\equiv y(x_2, u, t)$$

Attack detectability ⇔ distinguishable from measurements from other attacks:

$$y(x_1, u_1, t) \not\equiv y(x_2, u_2, t)$$

**Fundamental detectability/identifiability limitations**

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

**Existence of undetectable attacks**

$$\begin{bmatrix} sE - A & -B_K \\ C & D_K \end{bmatrix} \begin{bmatrix} x \\ g \end{bmatrix} = 0$$

**Existence of unidentifiable attacks**

$$\begin{bmatrix} sE - A & -B_K & -B_R \\ C & D_K & D_R \end{bmatrix} \begin{bmatrix} x \\ g_K \\ g_R \end{bmatrix} = 0$$

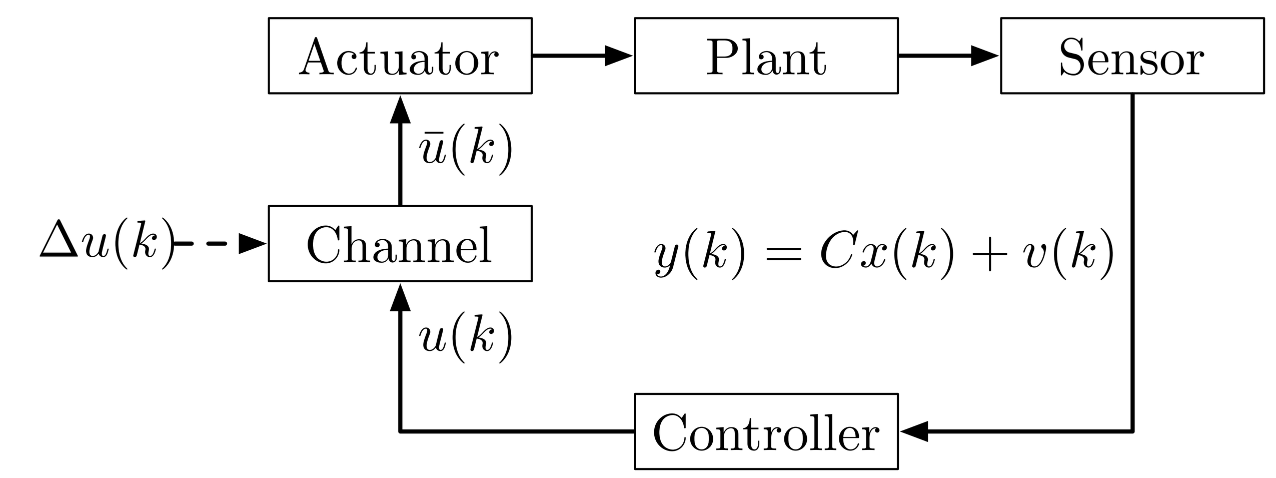
- centralized/distributed detection algorithms
- geometric design of optimal attacks

## Products

- 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).
- G. Bianchin, P. Frasca, A. Gasparri, and F. Pasqualetti. "The Observability Radius of Network Systems: Algorithms and Estimates for Random Networks," *IEEE Transactions on Automatic Control*, Submitted, 2015.

## Year 1: security in stochastic control 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
- $\varepsilon$-stealthiness via performance of *any* detector

**Conditions for $\varepsilon$-stealthiness**

An attack is $\varepsilon$-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.

- sufficiency under ergodicity assumption
- performance bounds and limitations

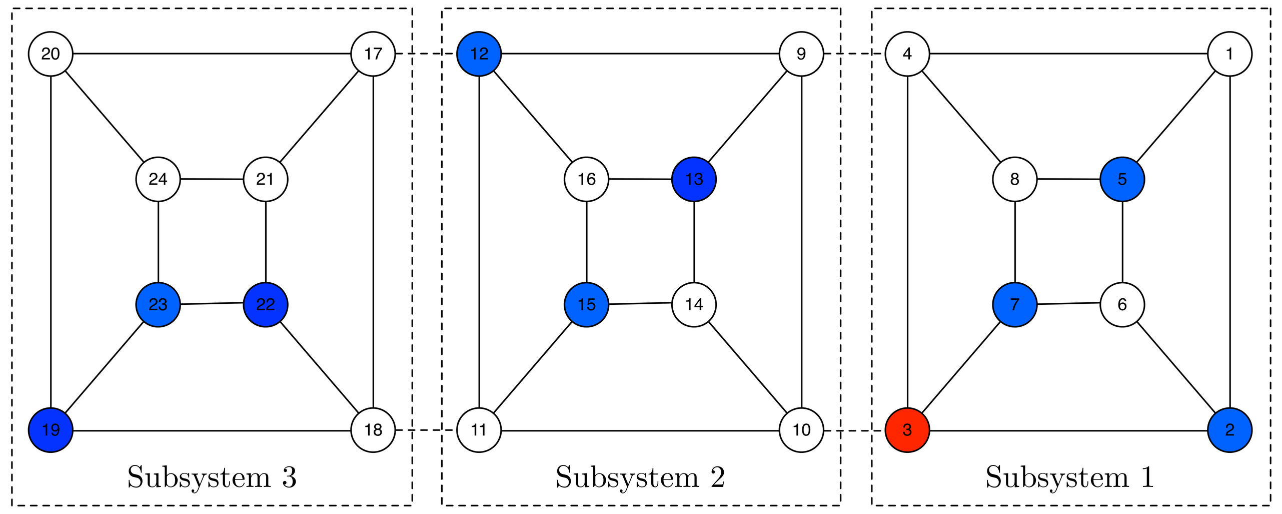
## Year 1: network observability radius

Modify network edges to prevent observability:

$$\begin{aligned} \min\ & \|\Delta\|_F \\ \text{s.t.}\ & (A + \Delta)x = \lambda x && \text{(eigenvalue constraint)} \\ & \|x\|_2 = 1 && \text{(eigenvector constraint)} \\ & C_{\mathcal{O}} x = 0 && \text{(unobservability)} \\ & \Delta \in \mathcal{A}_{\mathcal{H}} && \text{(structural constraint)} \end{aligned}$$

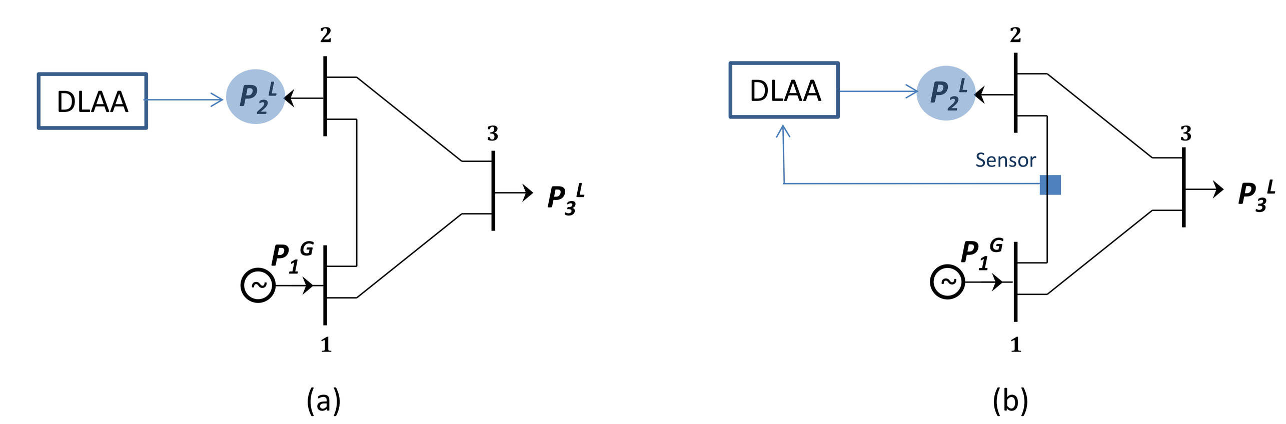
- optimality conditions via *total least squares*
- analytic bounds and algorithms
- resilience of networks with random weights
- topology vulnerabilities of IEEE14

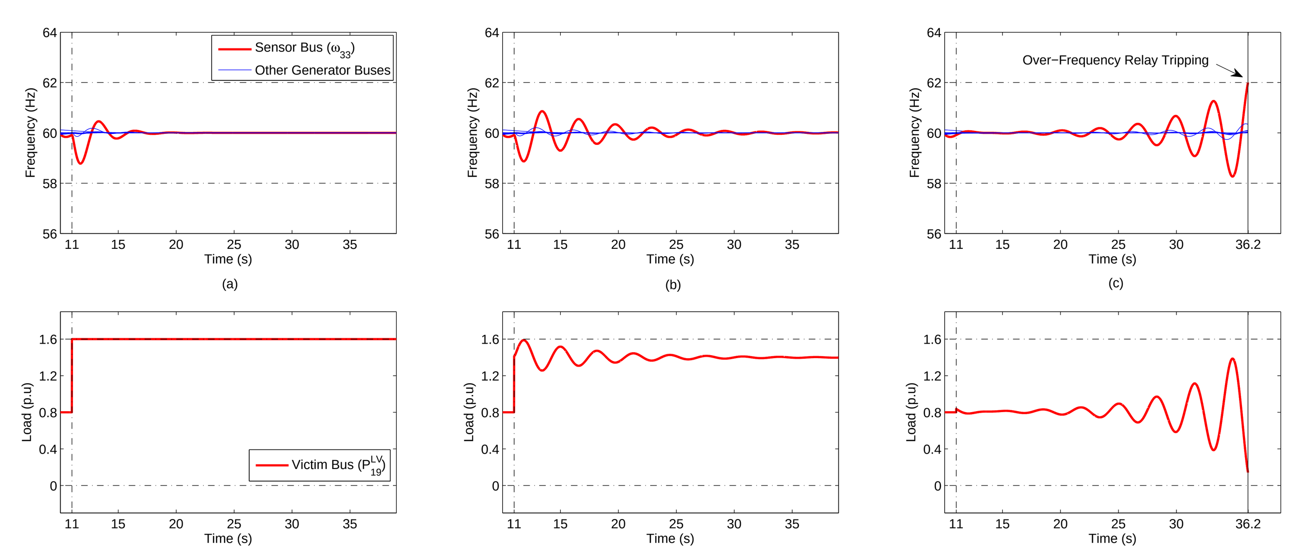
## Year 1: distributed identification




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

## Year 1: dynamic load altering attacks




- tamper with a group of loads (positive feedback)
- demand response and demand management
- open/closed loop, dynamic, single/coordinated

## Products

- 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.
- 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*, Submitted, 2015.

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