

A Hierarchical Approach to Dynamic Big Data Analysis in Power Infrastructure Security

(NSF/AFOSR DDS EAGER Project 1462530)

PIs: Hamed Mohsenian-Rad (EE), Christian Shelton (CS), Fabio Pasqualetti (ME)

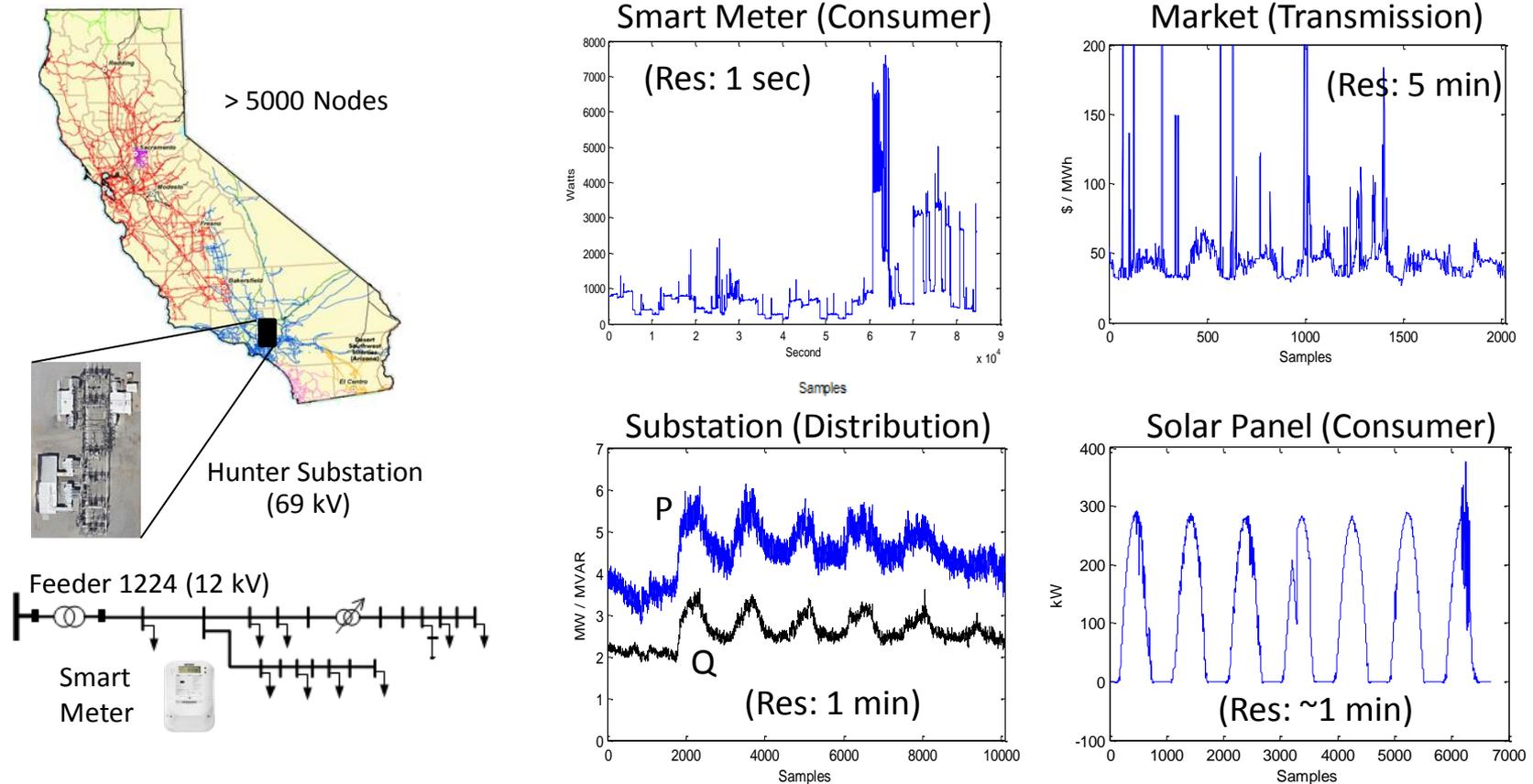
University of California at Riverside



PI Meeting – Arlington, VA, January 2016

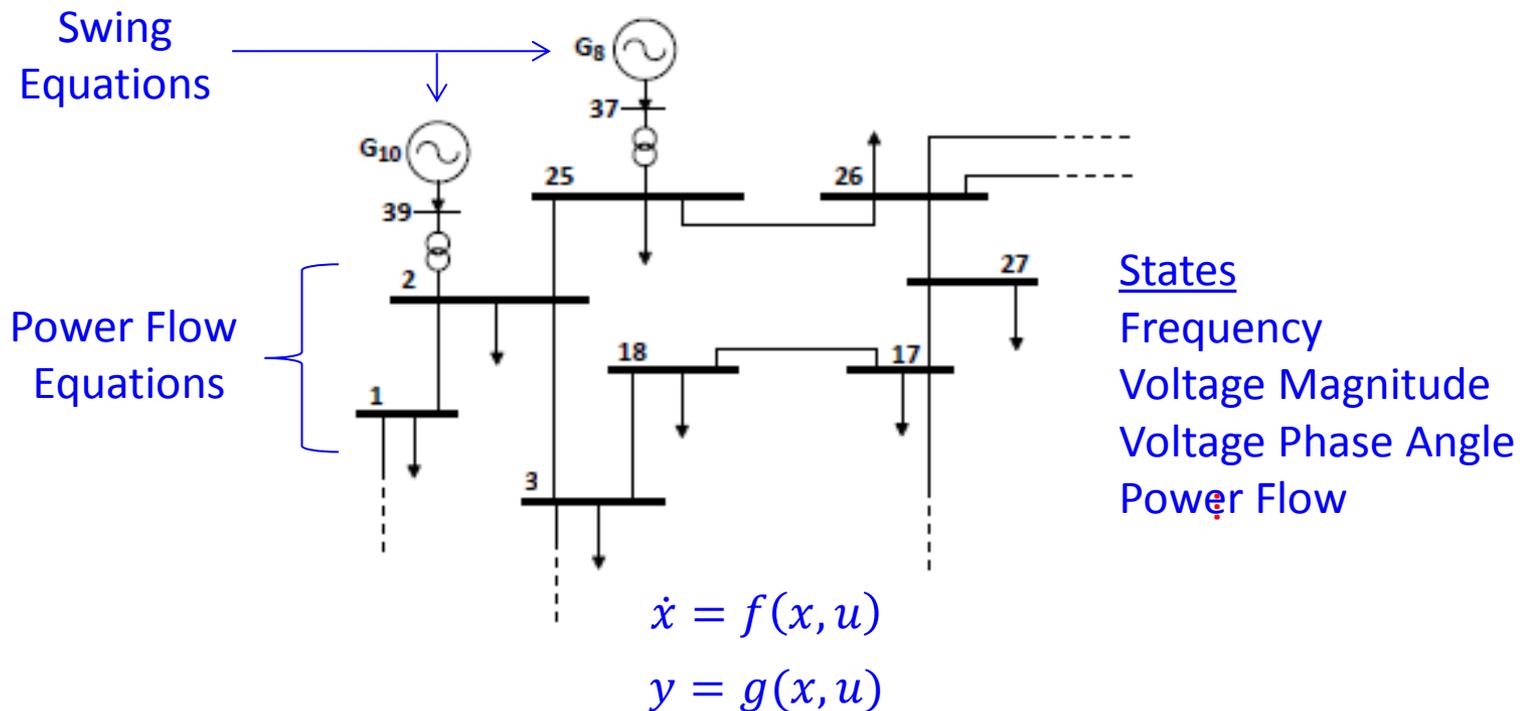
Problem Statement

- **Goal:** Detect and identify faults and attacks from diverse multi-resolution dynamic data in a power infrastructure.



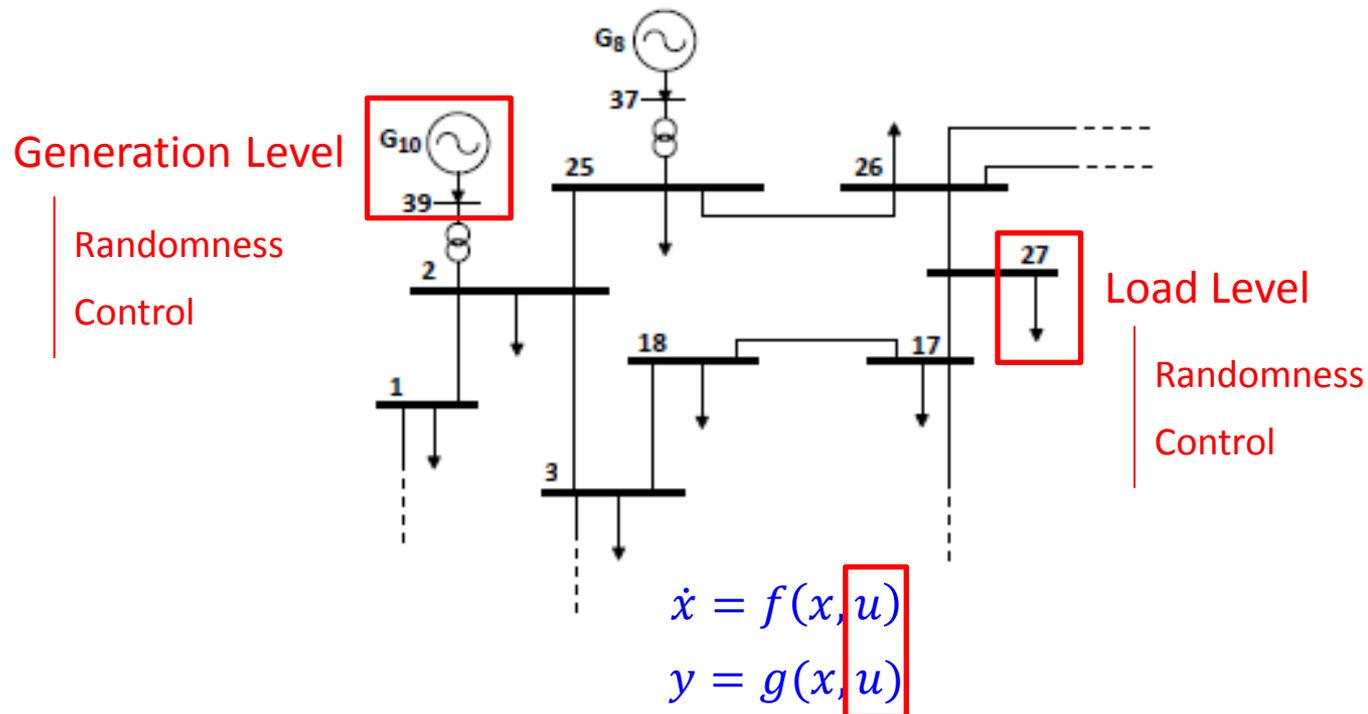
Problem Statement

- **Goal:** Detect and identify faults and attacks from diverse multi-resolution dynamic data in a power infrastructure.



Problem Statement

- **Goal:** Detect and identify faults and attacks from diverse multi-resolution dynamic data in a power infrastructure.

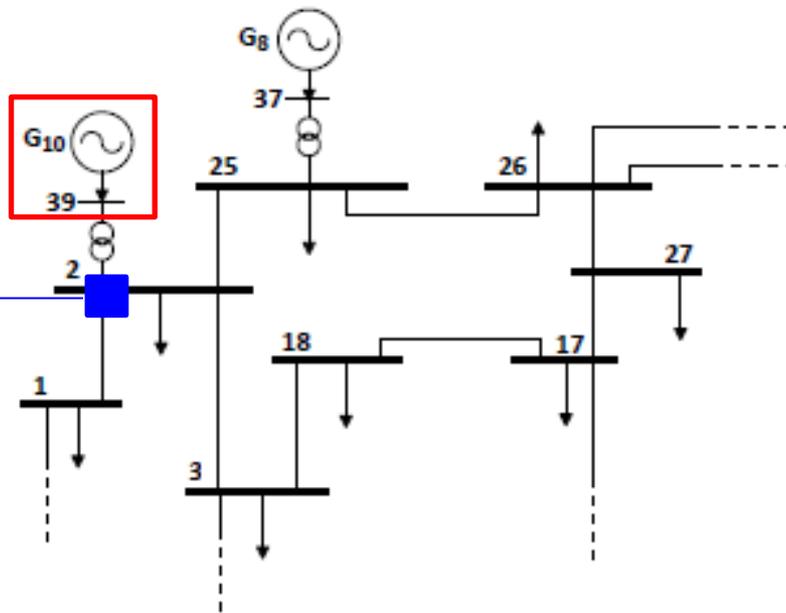


Problem Statement

- **Goal:** Detect and identify faults and attacks from diverse multi-resolution dynamic data in a power infrastructure.

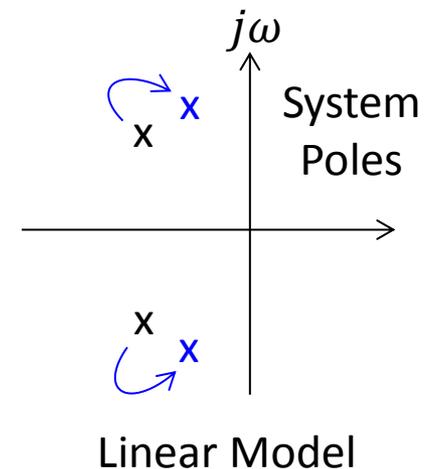
Positive Feedback

Generation Level



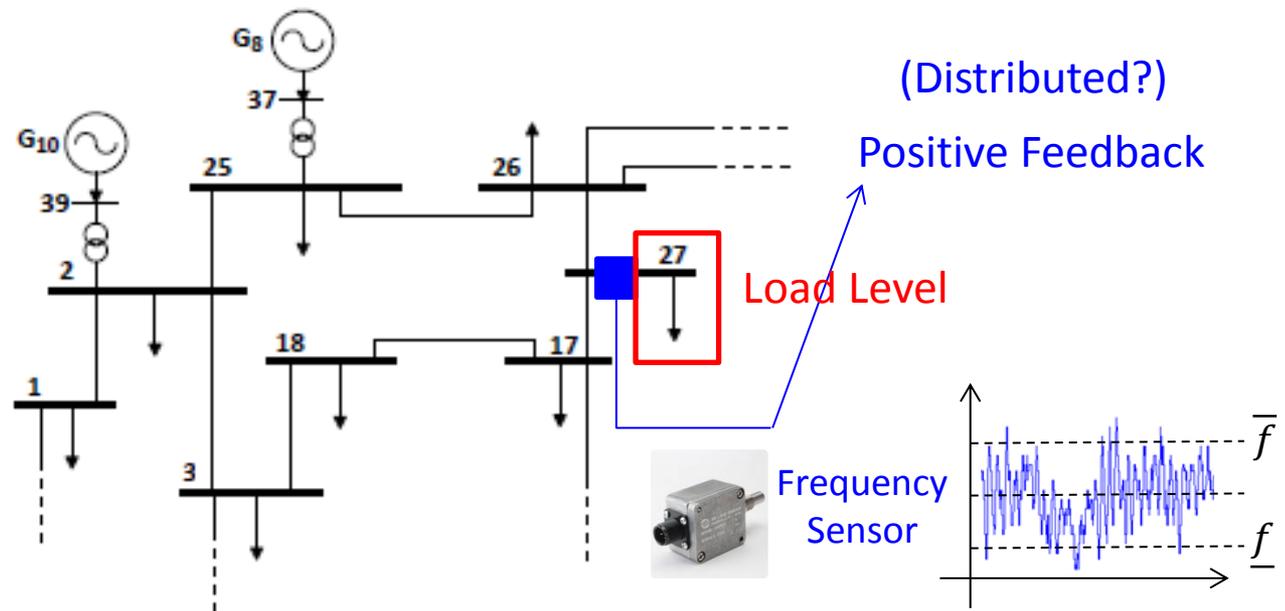
Fault

Attack [DeMarco 1996, Pasqualetti 2012, etc.]



Problem Statement

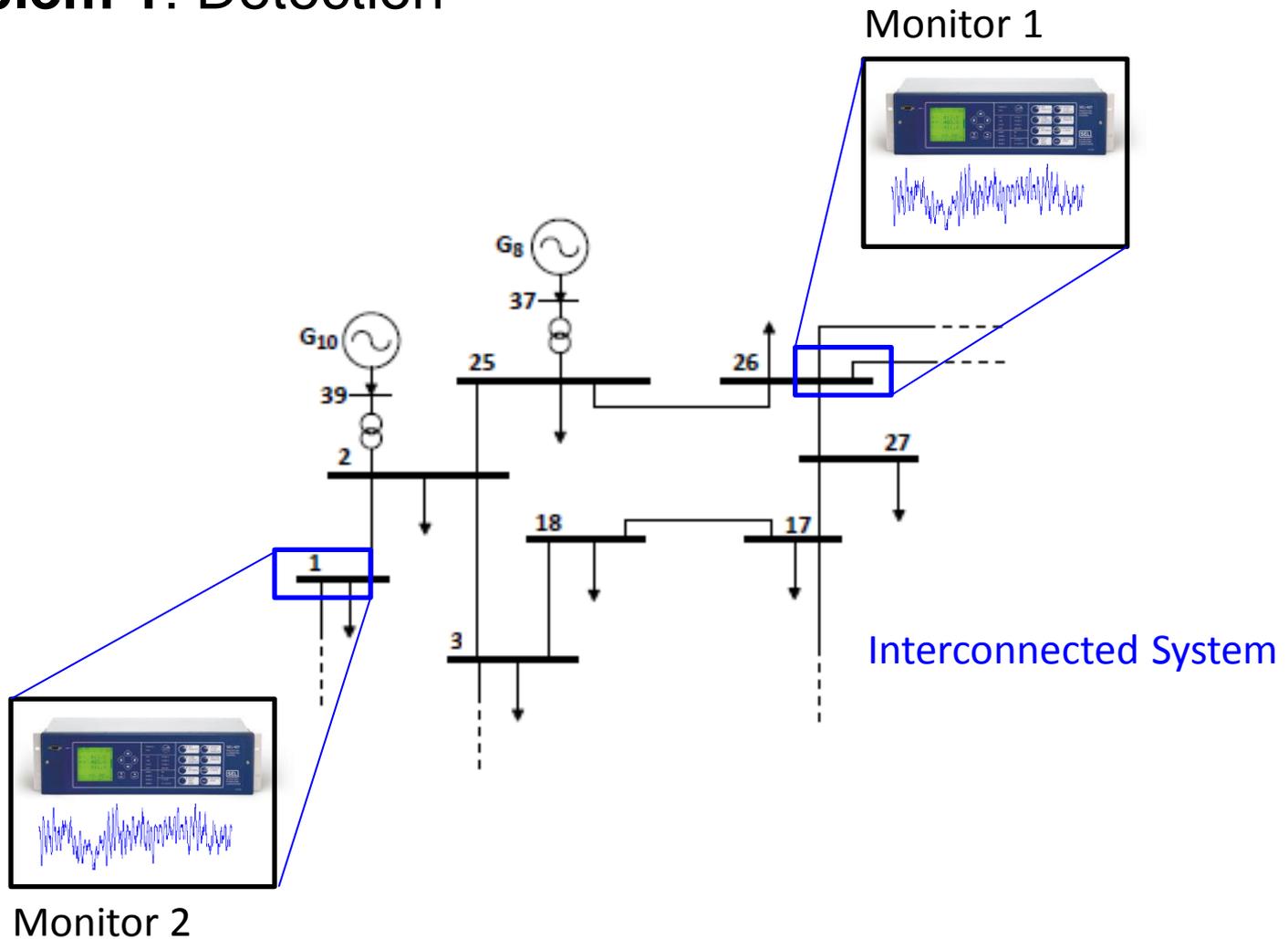
- **Goal:** Detect and identify faults and attacks from diverse multi-resolution dynamic data in a power infrastructure.



Fault

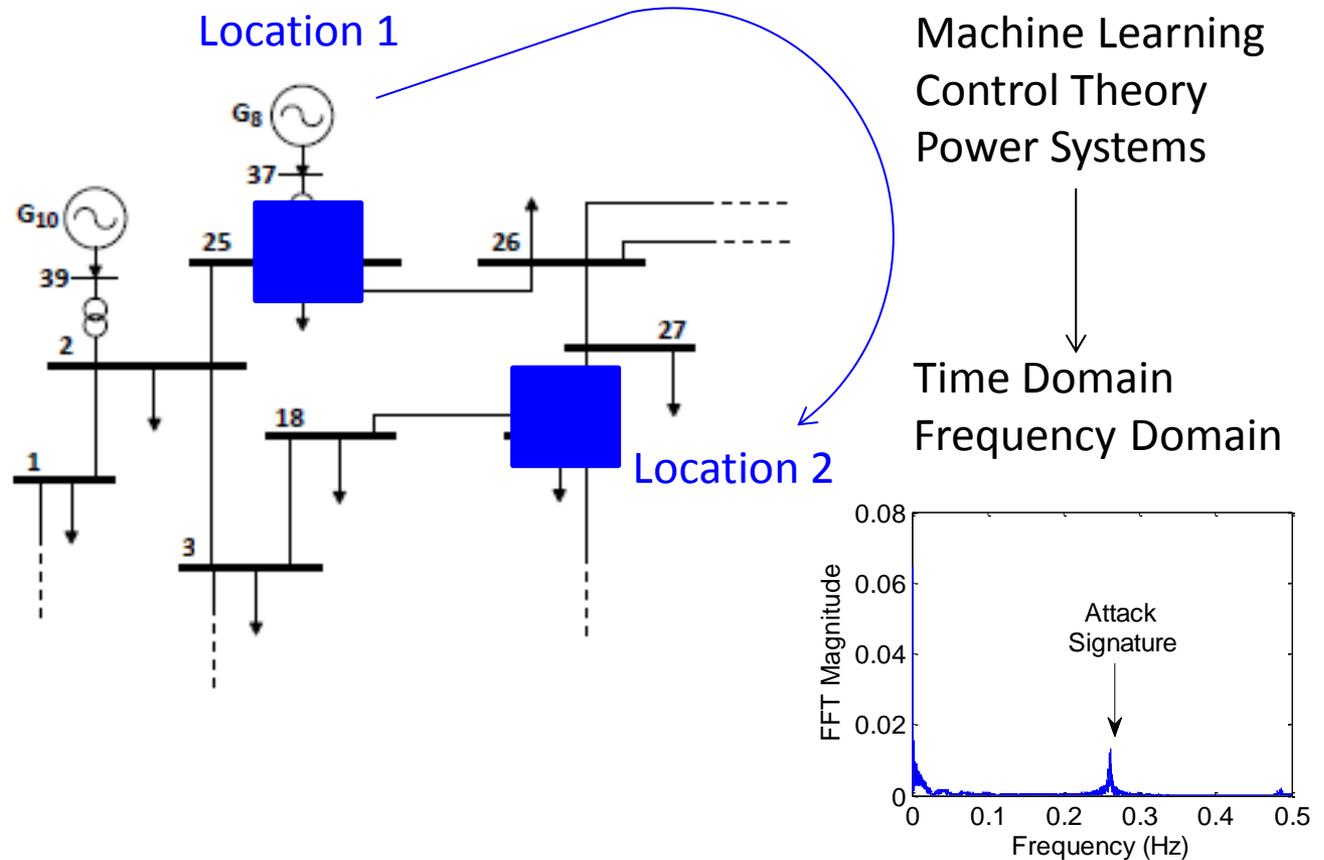
Attack [Mohsenian-Rad 2010, Marnerides 2014, Amini 2015, etc.]

- **Problem 1: Detection**



Research Challenges

- **Problem 2: Identification (Recall > 5000 nodes, etc.)**



- Parallel Research Efforts:
 - **Task 1:** Problem Formulation
 - **Task 2:** Designing Detection / Monitoring Tools
 - **Task 3:** Designing Identification Tools
 - **Additional Task:**
 - Developing Proper [Hierarchical] Simulation and Testing Tools

Thank You!

E-mail: hamed@ece.ucr.edu

Web: www.ece.ucr.edu/~hamed

- [1] C. L. DeMarco, J. V. Sariashkar, and F. Alvarado, "The potential for malicious control in a competitive power systems environment," in *Proc. of the IEEE International Conference on Control Applications*, Dearborn, MI, 1996.
- [2] F. Pasqualetti and F. Dörfler and F. Bullo "Cyber-Physical Security via Geometric Control: Distributed Monitoring and Malicious Attacks" in *Proc. of the IEEE Conference on Decision and Control*, Maui, Hi, USA, 2012.
- [3] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed Internet-based load altering attacks against smart power grids", *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp.667-674, December 2011.
- [4] A. K. Marnierides, P. Smith, P. A. Schaeffer-Filho, and A. Mauthe, "Power Consumption Profiling Using Energy Time-Frequency Distributions in Smart Grids", *IEEE Communications Letters*, vol. 19, no. 1, pp. 46-49, January 2015.
- [5] S. Amini and F. Pasqualetti and H. Mohsenian-Rad, "Detecting Dynamic Load Altering Attacks: A Data-Driven Time-Frequency Analysis" in *Proc. of the IEEE International Conference on Smart Grid Communications*, Miami, FL, 2015.
- [6] S. Amini and H. Mohsenian-Rad and F. Pasqualetti, "Dynamic Load Altering Attacks in Smart Grid", in *Proc. of the IEEE PES Conference on Innovative Smart Grid Technologies*, Washington, DC, 2015.