Cyberphysical Challenges of Transient Stability and Security in Power Grids

Ian Dobson
Francesco Bullo
Bruno Sinopoli

Iowa State University
UCSB
Carnegie Mellon

Objective

Detect, avoid and control instabilities and cyber attacks of power grids to avoid blackouts

CPS challenge

Power grids are already huge, complicated cyber- physical systems; and new measurements, communications, and computing are tightly coupled to grid physics and together drive the emerging smart grid. We need to transform power grid measurements into actionable information to keep the grid stable and secure.

Education

- New cyberphysical grad course on synchrophasor measurements

Maintain Synchrony

- Synchronization in power grids keeps all at 60 Hz and lights on
- want: Stable synchronization with line angle differences < γ degrees
- Networks of generators (oscillators) synchronize if couplings strong and natural frequencies close enough
- Nearly exact condition for synchronization:

$$\|L^{\dagger}\omega\| < \sin\gamma$$

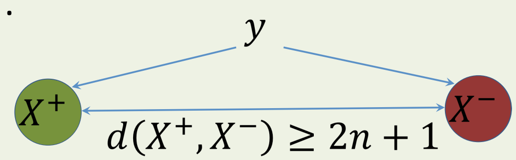
L = Laplacian (network coupling)

ω = natural frequencies, proportional to generator power injections in grid

PNAS paper in 2013

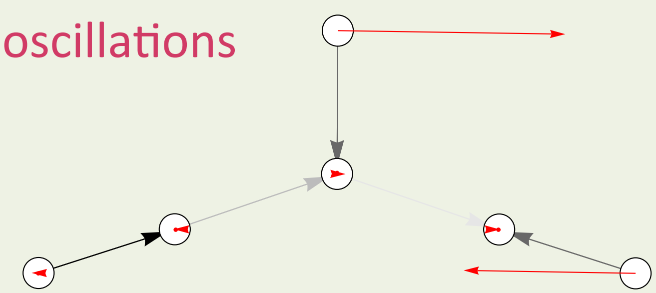
Robustness to cyber attack

- Grid operation relies on voluminous sensor data and is somewhat robust to errors but not to attacks
- Our goal: robust anomaly detection algorithm against worst case attacks on *n* sensors
- The optimal algorithm triggers an alarm if the Hamming distance between measurements *y* and X^+ is smaller than the one between y and X^-.



Suppress oscillations

- Electromechanical grid oscillations example: voltages in Arizona swing at ~1 Hz relative to voltages in Canada.
- We published a formula for generator dispatch to suppress harmful oscillations based on measurements of the patterns of oscillations and power flows.



red arrows = pattern of oscillation
gray arrows = power flows on lines
(blacker = higher flow)