Quantifying the Impacts on Reliability of Coupling Between Power System Cyber and Physical Components

A. D. Domínguez-García, X. Jiang, B. Harding, J. J. Makela, and J. Zhang

Goals

- Develop a taxonomy of the potential faults in cyber components.
- Construct appropriate models to quantify the impacts of faults on the physical system's stability and reliability.
- Build an overall framework combining cyber and physical information to monitor, control, and protect power systems.

Fundamental Questions/Challenges

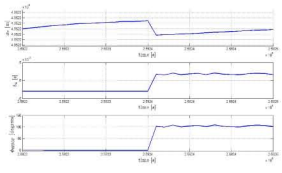
- The operation of most modern electrical energy systems is dependent on a cyber infrastructure of sensing, communication, and control devices; however, conventional analysis methods are:
  - Focused on impact of faults in the physical infrastructure for generation and transmission.
  - Not well-equipped to describe the impact of faults in the cyber infrastructure that controls the physical infrastructure.
- A thorough understanding of the impact of integrating new technologies is needed to prevent catastrophic system failures.

Research Plan

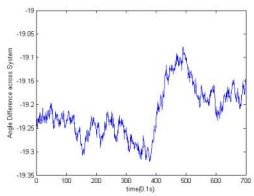
- Identify faults and misbehaviors of cyber components commonly used for communication and control in the power grid.
- Develop analysis tools to improve system stability and reliability by exploiting information from advanced cyber components.
- Characterize the effect of these faults on overall system dynamic performance and reliability through tools from developed hybrid system analysis.

GPS Spoofing Simulation Results

- Feasibility of GPS spoofing is being demonstrated in simulation using MatLab.
- Problem has been formulated as an optimization program in which the difference between the receiver clock offsets before and after the attack is maximized.
- Spoofing methods for an arbitrary number of visible satellites are being developed.



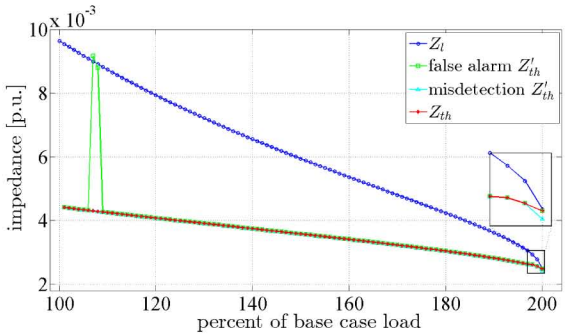
Navigation solution with 4 satellites: clock bias can be spoofed up to 8ms from the nominal value. PMU measurement phase information shifted by a half cycle!



Normal angle difference across system: critical angle difference is 45° with 30% margin

Impact on Voltage Stability Algorithm

- Potential PMU misbehaviors resulting from GPS spoofing are being identified and characterized.
- Effects of GPS receiver clock spoofing is being demonstrated on a voltage stability monitoring algorithm that uses Thévenin equivalent parameters computed from the PMUs' data.
- Simulations show the possibilities of false alarm and misdetections due to the attack.



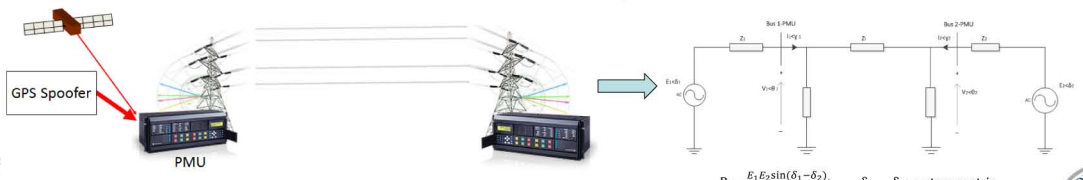
Deleterious effects of GPS spoofing on voltage-stability algorithm using Thévenin equivalent parameters. A possible false alarm and misdetection of voltage stability are shown.

Broader Impact

- The research supports the Smart Grid vision by providing powerful tools for engineering more reliable and more responsive electrical energy systems.
- The methods and tools developed will also help to broaden the understanding of cyber-physical systems.

Future Efforts

- Construct models to analyze the impact of PMU misbehavior mechanisms:
  - Implement GPS spoofing in a hardware setup.
  - Develop detection schemes for GPS spoofing attacks.
  - Investigate the specific effects of filtering algorithm implementation, data transmission limitations, and communication failures.
- Identify the impact of PMU misbehavior on overall system performance when phasor measurements are used in real-time control applications.
- Generalize potential misbehavior mechanisms of cyber-based control strategies that are likely to become pervasive in distribution systems.



$P = \frac{E_1 E_2 \sin(\delta_1 - \delta_2)}{X_{total}}$, $\delta_1 - \delta_2$: system metric

An example of the impact of GPS spoofing on system behavior