TCIPG

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

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

Goals

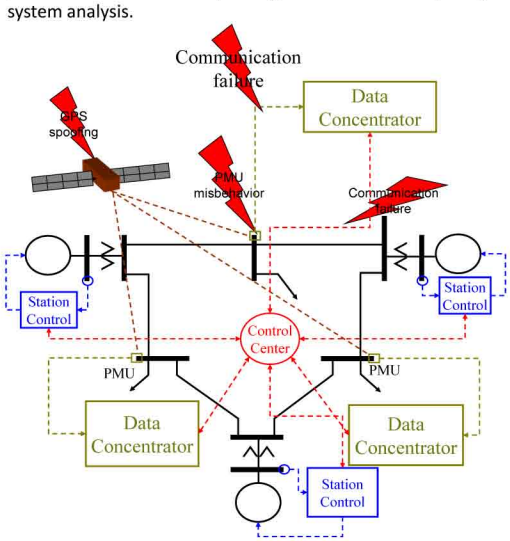
- Develop an exhaustive taxonomy of the potential faults in cyber components.
- Construct appropriate models to quantify the impacts of faults on the physical system's stability and reliability.
- Build an overall framework combining cyber and physical information to monitor, control, and protect power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

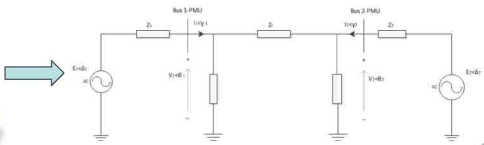
Fundamental Questions/Challenges

- The operation of most modern electrical energy systems is dependent on a cyber infrastructure of sensing, communication, and control devices (cyber components); 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.
- Without adequate emphasis on the impact of integrating new technologies, ad hoc system designs will likely lead to the deployment of poorly understood, unreliable, and unsafe systems, which could have catastrophic consequences.

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.



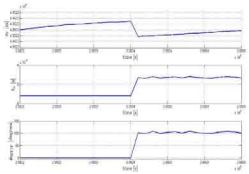


$P = \frac{E_1 E_2 \sin(\delta_1 - \delta_2)}{X_{total}}$, $\delta_1 - \delta_2$: system metric

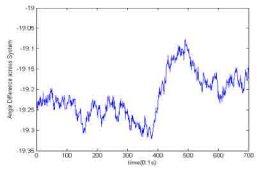
An example of the impact of GPS spoofing on system behavior

Research Results

- Different methods of attack on PMU synchronization are being developed and simulated.
- Demonstration of the feasibility of these attacks is allowing for better preparedness against security threats.
- Potential PMU misbehaviors are being identified and characterized: hardware faults, filtering algorithm implementation errors, data communication failures, and GPS signal spoofing.
- Simulation of GPS spoofing has been carried out in MatLab.
- Applications of PMU data are being investigated; a Thevenin equivalent model to qualify the impact of PMU misbehaviors is 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 half cycle!



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

Broader Impact

- The research will help accomplish 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.

Interaction with Other Projects

- An alternative method to reduce faults' impact would be to detect inconsistent data in data concentrators based on physical constraints in a power system; this will be shown in a security demonstration.

Future Efforts

- Construct models to analyze the impact of PMU misbehavior mechanisms:
  - Develop GPS spoofing code and implement it in a hardware setup.
  - 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.