TCIPG

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

A. D. Domínguez-García, L. DeVille, P. W. Sauer, D. Apostolopoulou, X. Jiang, and J. Zhang

GOALS

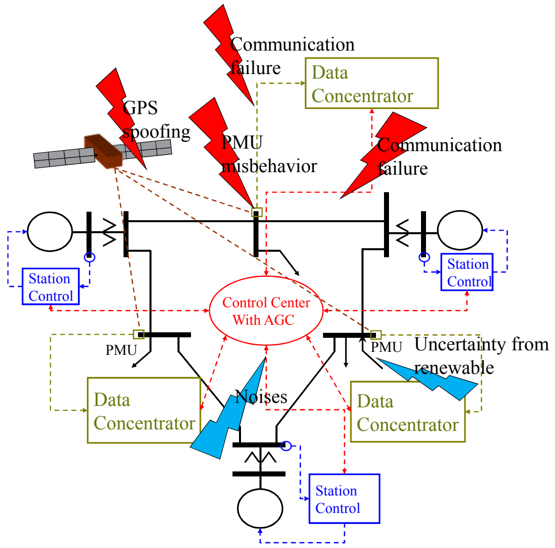
- Develop an exhaustive taxonomy of uncertainty factors in both cyber and physical components in a power grid:
  - Physical-related uncertainty factors: potential faults in physical infrastructure for generation and transmission, and uncertainties from renewable energies;
  - Cyber-related uncertainty factors: potential faults, attacks, and noises in cyber infrastructure for measuring, communication, and control.
- Construct appropriate models to quantify the impacts of uncertainties defined on the taxonomy on system dynamic performance and reliability.

FUNDAMENTAL QUESTIONS/CHALLENGES

- The extensive interaction of cyber components and physical components adds higher levels of uncertainty, vulnerability, and complexity to the power grid.
- Conventional analysis methods are mainly focused on impact of faults in physical components, but are not well-equipped to evaluate the impact of:
  - Deep penetration of renewable energy sources, whose generation is highly variable;
  - Faults and noises in cyber infrastructure that is closely coupled with physical components.
- Without adequate tools to address the impact of integrating new technologies, ad hoc system designs will likely result, leading to the deployment of poorly understood, unreliable, and unsafe systems, which could have catastrophic consequences.

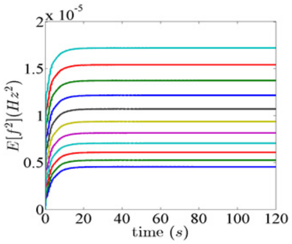
RESEARCH PLAN

- Identify faults and misbehaviors of cyber components commonly used for communication and control in the power grid.
- Characterize the effect of those faults on system monitoring.
  - Develop analysis tools to monitor system stability and reliability by utilizing information from advanced cyber components, e.g., phasor measurement units (PMU);
  - Identify the impact of misbehavior of cyber components on system awareness performance.
- Assess the impact on overall system dynamic performance and reliability of the uncertainties affecting system operations and control, through tools from switched/hybrid system analysis.

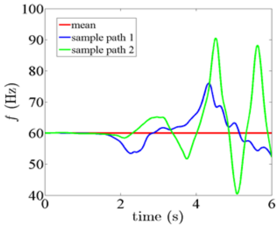


RESEARCH RESULTS

- Different methods of attack on PMU synchronization have been developed and simulated. The impact on system awareness performance has been evaluated.
- Uncertain renewable-based generation, noises, and potential continuous attacks on communication networks are properly modeled as stochastic processes.
- A framework to evaluate the impact of various uncertainty factors has been set up:
  - A comprehensive power system model with automatic generation control has been formulated as a stochastic hybrid system;
  - The statistics of system performance metrics (e.g., system frequency) are being evaluated through tools from hybrid system analysis; and
  - the impact of uncertainty factors on performance metrics is being provided through sensitivity analysis.
- We have proposed a variety of system communication network attack scenarios that would adversely affect power system performance metrics.
  - System frequency may vary drastically from the nominal value under properly designed continuous random attacks (e.g., imposing random noises onto the measurements).



Frequency variation with different penetration levels of renewable energies



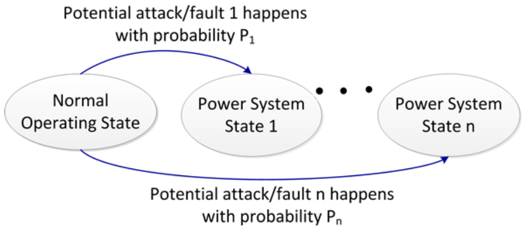
Frequency under a deliberately designed attack

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.
- The algorithms developed will contribute to tackling a “closure problem” of stochastic hybrid systems mathematically.

FUTURE EFFORTS

- Identify the critical location and level of the uncertainty sources in terms of their impact on system performance.
- Construct general effective attack models based on the proposed framework.
  - Construct optimal continuous attack models that will significantly influence the system performance with subtle changes to the measurements.
  - Investigate discrete faults and attacks in communication networks (such as package loss) that will cause system state to change.


Potential attack/fault 1 happens with probability P_1
Normal Operating State
Power System State 1
• • •
Power System State n
Potential attack/fault n happens with probability P_n

Stochastic Hybrid System-based Reliability Model

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T