Towards a Secure and Resilient Energy System Cyberinfrastructure Using Software-Defined Networking

Dong (Kevin) Jin, University of Arkansas
Matthew Caesar, University of Illinois at Urbana-Champaign

Executive Summary

Today's energy systems are increasingly adopting advanced information technology to boost control efficiency, which unfortunately opens up a new front for a potential "cyber Pearl Harbor." This proposed collaborative research project aims to develop a software-defined networking (SDN) enabled cyberinfrastructure with the objective of building a secure and resilient power system cyberenvironment. Specifically, we will develop numerous SDN-aware applications for energy system protection including intrusion detection (cyber-attack detection), network verification (cyber-attack prevention), and traffic management for network self-healing (cyber-attack mitigation) with a strong and sound evaluation.

SDN is a network architecture approach that enables the network to be intelligently managed and directly programmed using software applications. SDN enables (1) situational awareness of the entire grid with global visibility, (2) timely response to cyber-attacks through network direct programmability and traffic management, and (3) fine-grained analysis with rich information from both the communication network and the power system applications.

The proposed project will address the *Zero-Trust Networking* Needs Assessment. The integration of SDN to energy systems will enhance the effective deployment of zero-trust networking including network segmentation, continuous monitoring and verification, self-healing network architecture to enable resilient traffic delivery. We will also address the *Energy System Protection* Needs Assessment by exploring multiple SDN-aware applications. In particular, we will perform attack detection and network verification against the customizable security policies. Violations will indicate vulnerabilities and faults caused by cyber-attacks and system faults. We will also dynamically construct the network to isolate compromised devices and optimally reroute traffic to mitigate the attacks.

The proposed project would enable cross-site research collaboration. The PIs have a rich history of collaboration, which have resulted in multiple academic publications and collaborative research grants. The proposed project, with its targeted mix of systems and algorithmic work, draws on the PIs' expertise. Jin brings experience in cyber security and resilience of smart grid systems and applications and development of co-simulation testbed. Caesar brings experience in designing and implementing networked systems, creating algorithmic solutions to networking problems, and modeling and characterization of network protocols.

The impact of the proposed research will lay a scientific foundation and a secure and resilient cyberinfrastructure through the development of innovative models, algorithms, and tools for cyber-attack detection, prevention, and mitigation for the electric power grid that incorporates both cyber and physical system properties. The overall deliverables include (1) a final report describing the research progress and results, (2) technical papers for security/networking/power system journals/conferences, (3) software codebase of the prototyping system with documentation, and (4) technical presentations in the IUCRC meetings.