Enabling a Secure and Resilient Energy System with AI-Assisted Programmable Networks

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

Executive Summary

Providing secure and resilient energy delivery systems is strategically and tactically critical to our national security. In this proposal, we aim to integrate the advancement of programmable networks into energy system cyberinfrastructure, and explore innovative applications across attack detection, mitigation, and prevention empowered by data plane programmability and artificial intelligence (AI) technologies.

Our first funded CITES project explored control plane programmability using software-defined networking (SDN) for energy system security and resilience, which laid a good foundation for this proposed project. While SDN reduces network complexity and enables control plane innovation at the speed of software development, it is restricted to the fixed-function data plane. Consequently, attack detection and mitigation are mainly offloaded to the control plane, which operates at significantly lower speeds than the data plane. In this proposal, we aim to improve the existing work by enabling real-time and in-network attack detection and mitigation at data plane as well as automating the decision-making process using AI techniques to minimize the slow and vulnerable human decisions.

To achieve these objectives, we will develop multiple AI-assisted applications using P4. P4 stands for Programming Protocol-independent Packet Processors and is the de facto data plane programming language permitting network owners to run customized packet processing functions. The unique advantages brought by P4-based solutions include (i) packet-level analysis with extremely high speed to achieve real-time performance, (ii) information extraction from both network protocols and power system applications to expand the type of anomalies that one can detect and auto-correct, and (iii) the solution will require very minimal change to the existing utility network and its operations, and thus enables smooth tech transfer. Our three proposed research tasks include (1) a real-time in-network intrusion detection system (detection), (2) a formal-method-assisted network auto correction (mitigation), and (3) AI-based planning for operation automation (prevention). In addition to conducting performance analysis, we will leverage the formal nature of our system to prove (via automated mechanisms) the key safety and security properties our system will provide.

The proposed project would enable cross-site research collaboration. The PIs have a rich history of collaboration, which has 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 AI-assisted models, algorithms, and tools for cyber-attack and cyber-mistake detection, prevention, and mitigation that incorporates both cyber and physical system properties.