Cyber-Physical Security Testbed Federation for Large-Scale, High fidelity, Closed loop Attack/Defense Experimentation

Aditya Ashok – PhD student, Iowa State University
Advisors – Dr. Manimaran Govindarasu, Dr. Venkataramana Ajjarapu

Cyber security of the smart grid -- encompassing attack prevention, detection, mitigation, resilience, and deterrence -- is among the top R&D priorities today. With growing concerns for the cyber security of power grid and other critical infrastructures, it is not possible to do cyber attack-defense experimental studies on real systems. Moreover, it becomes prohibitively expensive to replicate real systems for security and performance evaluations. In this respect, testbeds provide an optimal balance between the cost and the ability to accurately capture real system characteristics. Testbeds also adequately capture the complex cyber-physical interactions in the power system, which cannot be accurately modeled using traditional modeling and simulation tools.

Testbed design will typically balance the integration of physical, emulation and simulation-based components. While a physical environment with industry standard hardware, software and power system components is ideal, the high cost will typically outweigh practicality. Therefore, in order to create realistic CPS testbeds of reasonable scale without compromising on the key testbed design principles, there is a strong need for developing federated CPS testbeds leveraging testbed infrastructures across several educational organizations and national laboratories.

There are significant challenges in creating a federated testbed infrastructure that can facilitate large-scale, high fidelity, real-time, closed-loop experimentation for critical infrastructures like the power grid. The proposed poster would describe potential testbed federation architectures that enable large-scale, high-fidelity, real-time, closed-loop cyber security experimentation for critical infrastructures like the power grid, and potentially other interdependent critical infrastructures like water, natural gas, etc.

Also, the poster will describe proof of concept implementation of CPS security testbed federation across the testbeds at Iowa State University (ISU) and University of Southern California, Information Sciences Institute (USC/ISI). This implementation was used to demonstrate a high-fidelity, highly-scalable, remotely accessible CPS security testbed environment for Smart Grid cyber security and resiliency experimentations and was showcased as part of the *Smart America Challenge*, organized by the National Institute for Standards and Technology (NIST) and the White House Office of Science and Technology Policy (OSTP), held at Washington, D.C., in June 2014.