Software Defined Networking for Smart Grid Resilience

Hui Lin¹, Xinshu Dong², Rui Tan²,³, Ravishankar K. Iyer²,³, Zbigniew Kalbarczyk¹,²
¹ Coordinated Science Laboratory, University of Illinois at Urbana Champaign, IL, USA;
² Advanced Digital Sciences Center, Illinois at Singapore;
³ School of Computer Science and Engineering, Nanyang Technological University, Singapore

Software Defined Networking

- **SDN for the Grid: Opportunities & Risks**
  - SDN for greater resilience in smart grid [1]
    - Example 1: detecting malicious command forwarding behaviors
    - Example 2: filtering out flooded responses from control and field devices caused by spoofed requests

- **Cyber-Physical Simulation & Testbed**
  - Applying SDN to strengthen smart grid operations
    - Smart grid: critical infrastructure leveraging information and communications technology
    - Initial industrial effort towards SDN-enabled smart grid
    - SEL-2740S switch

- **Fault Injection on SDN-Enabled Grid**
  - Example 1: "darknets" created by SDN rootkits
  - Example 2: denial-of-service attacks from weakness with the SDN controller

- **SDN with Synchronized Clock**
  - Ongoing work: Investigating the practical benefits of having time-synchronized network updates
  - Preventing varying degrees of packet loss
  - Eliminating ambiguous states when access control policy is integrated into SDN switches
  - Requiring less changes compared to packet versioning

References


This work was supported by the research grant for the Human-Centered Cyber-Physical Systems Programme at the Advanced Digital Sciences Center from Singapore’s Agency for Science, Technology and Research (A*STAR). Zbigniew Kalbarczyk and Ravishankar Iyer are supported in part by the grant Cyber-Resilient Power Grid Security (Contract number 2015-01-053-000) from the US Department of Energy, USA, and another grant from Siemens Security Monitoring for Industrial Control Systems, awarded to USEPA, and another grant from ACCE, Washington DC, USA.