Modeling Security Risk to and Resiliency of EDS Using Software-Defined Networks and Robust Networked Control Systems

Sachin Shetty, L.H. Keel, Hellen Maziku and Esther Amullen

RESEARCH GOALS

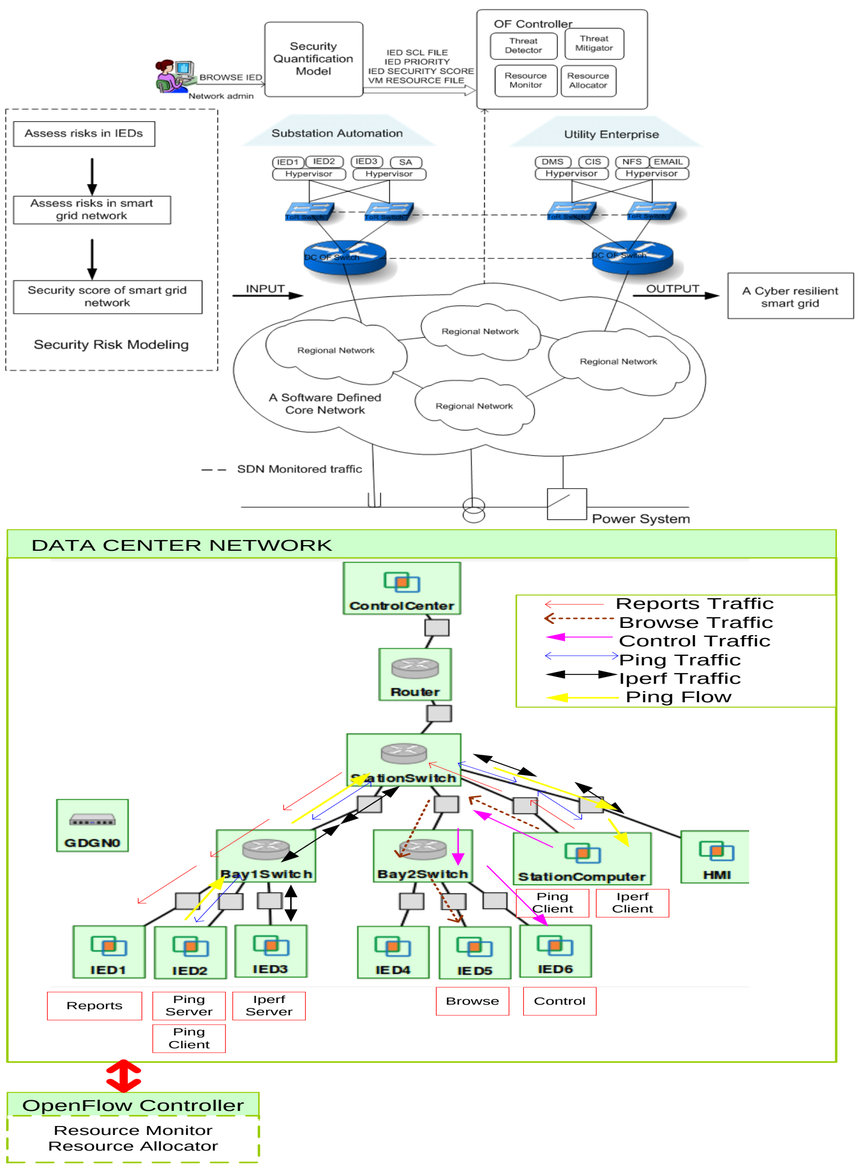
- Risk Assessment models to quantify impact of threats in EDS.
- Diversity modeling using multiple SDN controllers to improve the resilience of EDS against zero day attacks.
- Cost model to select countermeasures which balance tradeoff between security risk and quality of service.
- Develop security scores for robust controller configuration in EDS.
- Design robust controllers to ensure system operation resilience in the presence of attacks.

RESEARCH APPROACH

- Systematic characterization of attack paths exploited by zero-day vulnerabilities in EDS.
- Network diversity modeling to evaluate resiliency of EDS in the presence of zero-day vulnerabilities.
- Assessing the impact of attacks on cyber-physical systems and mitigation of zero-day attacks.
- Designing controller algorithms to protect against specific attack categories.
- Realize security diversity metrics for multiple controllers using a probabilistic approach.
- Develop a robust controller whose control action can be done while meeting reliability and security requirements of EDS.
- Model the cost of network configurations which mitigate risk of cyber threats.

RESEARCH ACCOMPLISHMENTS

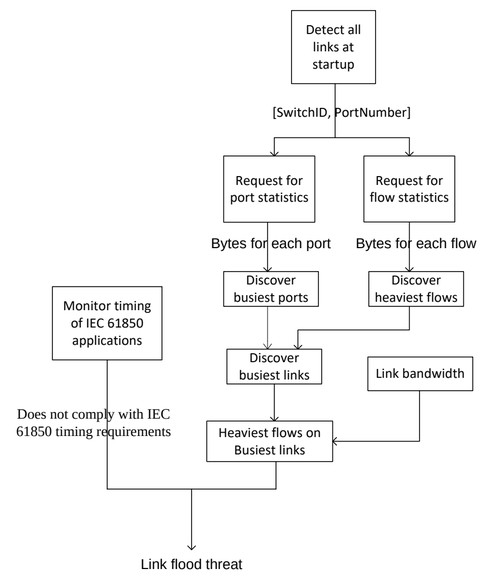
- Developed a risk assessment model to assess security risks within an SDN-enabled EDS communication network.
- Quantified the impact of low-intensity legitimate-traffic DoS attacks in a simulated SDN environment.
- Deployed and evaluated performance of the model in an Openflow controller within a Global Environment for Networking Innovation (GENI) testbed.
- Conducted experimental evaluation of resilience of IEC 61850-based Substation Communication Systems in a Software Defined Network.

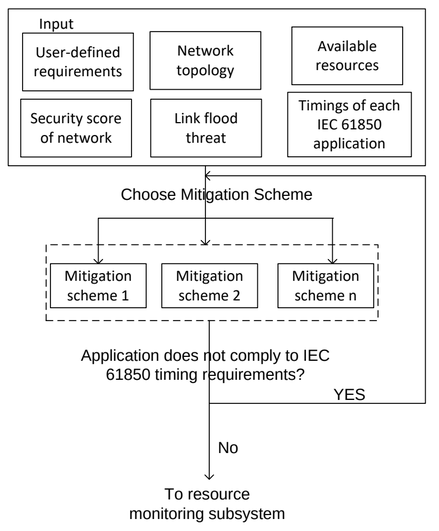


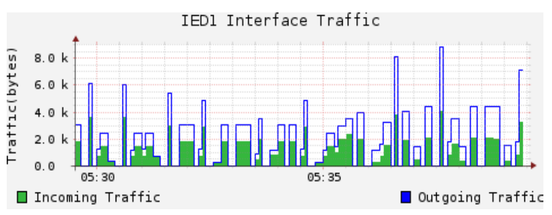
SDN Enabled Resilient Smart Grid

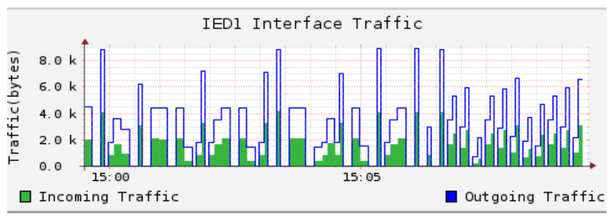
Experimental Validation in GENI testbed

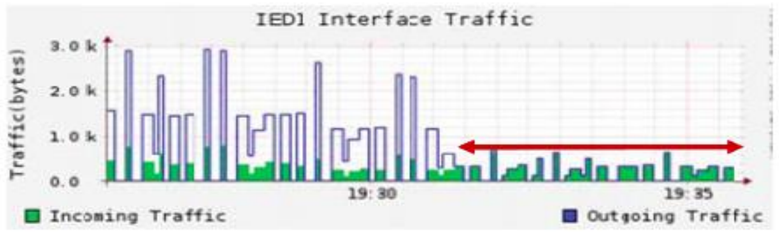
RESEARCH RESULTS



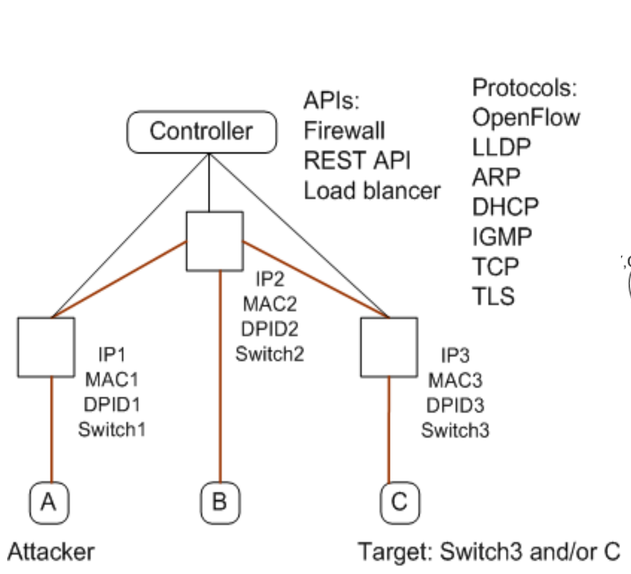




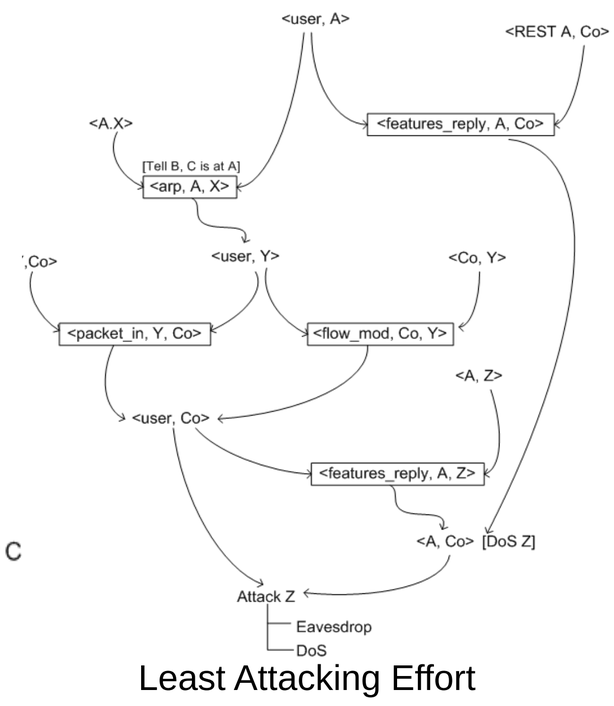




DIVERSITY MODELING



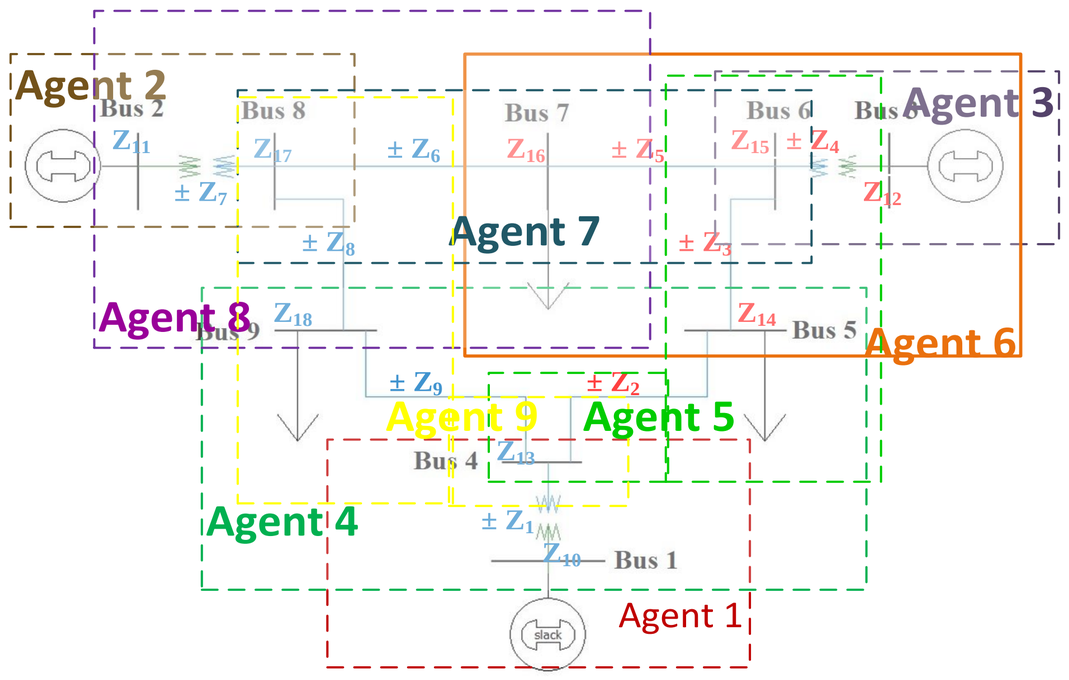
Example Network Topology for Diversity Modeling



Least Attacking Effort

MULTI-AGENT SYSTEM FOR INTRUSION DETECTION

- Addressed false data injection attacks by exploiting the topology of the power grid.
- Software based agents that facilitate communication among adjacent substations share measurement data.
- Agents partition the power grid into virtual sub-grids such that a successful false data injection attacks would have to be in the null. space of the main grid topology matrix and also the null space of the topology matrix for each of the virtual sub-grids.



FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY