s_i

MODELING A CYBER RESILIENT SMART GRID
USING SOFTWARE DEFINED NETWORKS

Hellen Maziku and David M. Nicol

SCIENCE OF SECURITY
VIRTUAL ORGANIZATION

The Science of Security Initiative is funded by the National Security Agency.

IP-BASED COMMUNICATIONS IN THE SMART GRID

- Digital intelligence to the power system network.
- Intelligent Electronic Devices (IEDs) used to monitor the state of the power system
- IP-based communications also increase the likelihood of successful IP-based network attacks
- *Challenge*: Enabling the smart grid communication network become cyber resilient
- **DOE Vision:** *By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions*

SECURITY QUANTIFICATION MODEL

- The cyber resilient model depends on the security score of IEDs in the smart grid network
- The score for a particular threat based upon its susceptibility s_i and countermeasure factor c_i is given by:

$$t_i = s_i \left(1 - c_i\right)$$

- The score for the *jth* IED with m_j threats becomes:

$$E_j = \sum_{i=1}^{m_j} t_i * S_R \qquad (1)$$

  - Where S_R is security requirement of an IED
  - If this IED were to be compromised, how much impact would it have on the smart grid?

- Overall security score of the network with *n* IEDs:

$$R = 10 - \min\left(10, \sum_{j=1}^{n} E_j\right) \qquad (2)$$

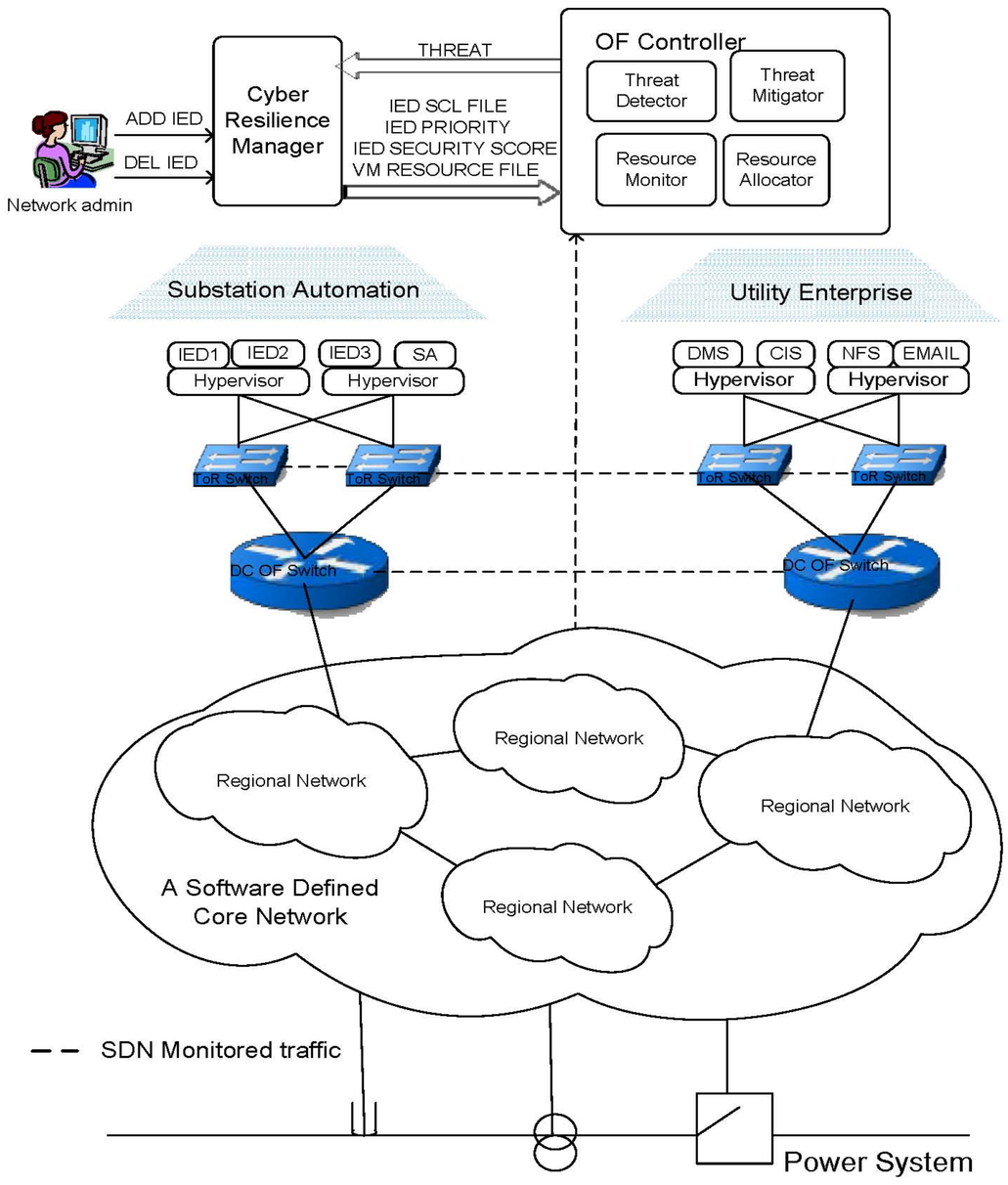
SDN FRAMEWORK FOR CYBER RESILIENCE

- Develop an OpenFlow controller that constantly monitors network utilization
- When an attack is detected, the controller calculates the security score of the network using (1) and (2)
- The controller then takes into account:
  - The current security posture
  - Cyber resilience requirements (tradeoffs)
  - Network topology and network traffic
  - Previous similar attacks
  - Available network resources
- The controller makes an informed decision on the SDN mitigation method to use:
  - Reroute, rate limit, or drop flows
  - Migrate virtualized IED
  - Prioritize flows, etc.

ACKNOWLEDGMENT

- This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141

A CYBER RESILIENT SOFTWARE DEFINED SMART GRID



PRELIMINARY IMPLEMENTATION

- Consider a windmill collector substation with:
  - 2 Current Differential and Overcurrent IEDs
    - ✓ Transmission domain (medium critical)
  - 1 Distribution Substation Transformer Monitoring IED
    - ✓ Substation domain (most critical)
  - 3 Distribution Feeder protection and control IEDs
    - ✓ Distribution domain (Least Critical)
  - 6 OpenFlow switches, 3 end hosts and 3 servers
- Mininet used to simulate the OpenFlow switches
- Triangle Microworks IEC61850 suite to simulate IEDs
- Ryu for implementing the OpenFlow controller

TABLE 1: SECURITY SCORE FOR THE SUBSTATION IED

DoS Attack	Si	Ci	Ti
Energy based DoS over LAN	0.2	1	0
Bulky messages over LAN	0.2	0	0.2
Low rate link foods over LAN/WAN	0.2, 1	0, 0	1.2
Protocol based DoS over LAN/WAN	0.2, 1	0, 0	1.2
Software based DoS over LAN/WAN	0.2, 1	0, 0	1.2
Ej			5.74

CONCLUSION

- Classified criticality of IEDs and developed a model for security posture of smart grid networks
- Modeled SDN framework for cyber resilient smart grid
- *Next Phase:* Implement the OF controller in the SDN framework

CSL: COORDINAT SCIENCE L