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

Website: http://cred-c.org/researchactivity/riskmodels

Researchers (ODU/TSU): Sachin Shetty (ODU), L.H. Keel (TSU), Esther Amullen (TSU), Kamrul Hasan (ODU), Marco Gamarra (ODU), Md Sharif Ullah (ODU)

Industry Collaboration:

- Accenture Technology Labs
- MidAmerican Energy

Description of research activity: We will formally model risk assessment and network diversity to assess the resiliency of EDS against zero-day attacks. The risk assessment model will quantify the impact of the various attack paths on EDS. We will also propose an EDS network-diversity metric based on the configurations and policies of various resources. The security metric will be computed for different network configurations and policies and will consider the similarity and dissimilarity of network resources and account for minimum impact to maximum impact attacks. The metric will be useful for evaluating the impact of different classes of cyber attacks**.** The risk assessment and network diversity model will be implemented within an OpenFlow controller. The OpenFlow controller will monitor networking resources in EDS networks. In case of an attack, the architecture will rely heavily on the risk assessment model to select a resilient mitigation approach, taking into account resiliency requirements of the cyber physical system. The risk assessment model will classify attacks in terms of how severely they will impact the cyber physical system's operation. The model will also quantify the security posture of the cyber physical network at any given time.

We propose to address FDI detection problem in SDN-enabled EDS based on a multi-agent system and develop a quarantine service with SDN technology to achieve autonomous attack containment during such an attack. We will logically partition the SDN-enabled EDS into multiple sub-systems, each comprising a substation and other substations directly connected to it through network of SDN switches. Software-based agents in each substation will communicate with each other. The agents facilitate exchange of meter measurements among substations that are included in each subsystem. Each agent can perform local state estimation for its sub-system. In the absence of FDI attacks, state estimation results at each sub-system are identical to state estimation results for the whole grid. However, in the presence of FDI attacks, compromised measurements can evade bad data detectiontechniques during state estimation for the whole grid. State estimation performed at each sub-system is used to analyze the compromised measurements and identify disparities. Risk scores will be computed to quantify the impact of a FDI attack. We will develop the quarantine service that will take into account the risk scores and network configurations to isolate the impacted portions of the power grid and ensure operational of the power grid with minimal impact.

How does this research activity address the Roadmap to Achieve Energy Delivery Systems Cybersecurity?
This activity falls under "Assess and Monitor Risk" and "Develop and Implement New Protective Measures to Reduce Risk". There is a need to understand and quantify cybersecurity risk EDS. In our activity, we develop risk assessment models to quantify cyber threats in smart grid. The deployment of the risk assessment models in SDN switches will facilitate continuous monitoring of risk and selection of network configurations to mitigate risk. The ability to detect and quarantine false data injection attacks provides mechanisms to reduce the risk from threats which compromise the integrity of measurements in the smart grid.

Summary of EDS gap analysis: We will develop security risk assessment capability within a SDN controller to compute risk scores for both known and zero day attacks in EDS. The availability of risk scores will result in the SDN controller choosing mitigation policies, in response to attack or failure, which balance between security risk and operation cost. We will also develop diversity modeling using distributed SDN controllers to mitigate against attacks on the SDN control

plane. We will develop a quarantine service with SDN technology to achieve autonomous attack containment during FDI attack.

Full EDS gap analysis: Software defined networking (SDN) is a networking paradigm to provide automated network management at run time through network orchestration and virtualization. SDN has been used primarily for quality of service (QoS) and automated response to network failures. A central controller realizes the automatic network configuration in SDN at run time by conforming to a control plane protocol (e.g., OpenFlow) and switches act as simple forwarding devices. However, in the context of EDS, SDN can enhance system resilience through recovery from failures and maintaining critical operations during cyber attacks. In addition, SDN must also be defended against attack due to potential vulnerabilities in the control plane. Our proposed research will extend the capabilities of SDN devices in OT, such as those offered by SEL, so that the controller can dynamically manage risk by the choice of countermeasures. We will develop the security risk scoring model to characterize risks for both known and zero-day attacks. The risk model will also incorporate the criticality of the nodes in the OT environment. We will also develop a quarantine service using SDN technology to conduct autonomous attack containment during a False Data Injection (FDI) attack. The quarantine service will isolate portions of the network impacted by FDI, thereby mitigating the risk and ensuring minimal impact to the operation of the power grid. In order to defend against attacks on SDN controller, we will develop a distributed SDN controller framework based on diversity modeling for EDS. The success of our research will enhance potential of SDN in EDS OT beyond the current QoS benefits to permit dynamic response and operation through failure or attack.

Security Risk Assessment for SDN-enabled EDS – According to the Energy Sector Cybersecurity Capability Maturity Model [1], there is a need to develop techniques to manage cyber security risk in EDS. A SDN controller that can modify network configurations based on risk scores enables better cyber security risk management in EDS. At the same time, efforts to develop risk scores based on model based security assessment have focused on known attacks [2]. However, with ever evolving nature of cyber-threats, there is a need to develop risk scores for zero day attacks to ensure that SDN controller's risk assessment capability is not limited to known attacks. In addition, the controller also needs to be equipped with the capability to compare the countermeasures with the aim to reduce risk, ensure operational resilience, and minimize cost to the operator. Currently SDN controllers are only equipped with the ability to ensure QoS and are not adequately capable of managing risk.

The static, non-adaptive design of current grid communication networks makes it nearly impossible or unacceptably time-consuming to reconfigure a network to react to zero-day attacks [3]. Software Defined Networking (SDN) allows decoupling of the control and data plane, enabling logically centralized network controllers to manage whole networks. SDN enables real-time flow management, which can be modified based on the QoS needs [4-5]. Schweitzer Engineering Lab (SEL) is using SDN to enhance the performance, configuration, and proactive management of OT networks. Specifically, the SEL-2740S SDN Switch provides user path- and packet-level control of communications flows, and maximizes application performance under all conditions by pre-engineering primary and failover communications flows that fail over in less than 100 µs [6]. The SEL-5056 SDN switch simplifies the design, test, and implementation of critical power utility and industrial OT networks [6].

However, the SEL-2740S and SEL-5056 SDN switches currently do not have the capability to modify network configurations/topologies based on risk assessment of known or zero-day attacks. The controller currently is focused on automated network management and traffic engineering to meet QoS requirements. The controllers within the SEL-2740S and SEL-5056 SDN switches will benefit from risk assessment models to achieve a balance between managing security risk and traffic engineering. There are several risk assessment models reported in literature which can be considered for these switches [7-14]. Modeling formalisms such as, UML [11], petri nets [12], attack graphs [13] and hybrid approaches [14] provide quantitative security assessment based on metrics. However, these formalisms only focus on known attacks and do not take into account impact of zero-day attacks. We will map security requirements of a smart grid network to corresponding networking requirements, leading to a better informed security risk assessment modeling and attack mitigation. We address the limitations in the security score model of IEDs [15] to reflect the criticality of each IED and its impact on the overall smart grid network. We will demonstrate that the knowledge of the security score of the smart grid network helps the SDN controller choose an effective mitigation policy in the presence of

attacks. In addition, the SDN controller can choose optimal mitigation policies by balancing security risk and operational cost. We also show SDN principles for enforcing quality of service (QoS) policies, such as bandwidth reservation, mitigate DoS-based flood attacks on network links and help IEC 61850 applications meet their time transfer limits.

Diversity-based security mechanisms have traditionally operated on the system level by deploying multiple diverse software replicas. However, in EDS, it will be important to model network diversity as computer networks play a key role in transmission of control and data information throughout the critical infrastructure. Network diversity modeling for risk assessment in SDN-enabled EDS has not received much attention. A centralized SDN controller is vulnerable to attacks directed at the control plane. The concept of a SDN controller cluster has been proposed as a solution to improve system resilience, reliability, security and efficient topology management. Opendaylight [16] and ONOS [17] are examples of distributed SDN controller platforms, which overcome the issues with scalability and vulnerability plaguing single-controllers. We will develop network diversity models with distributed SDN controllers and address research challenges such as the optimal number of controllers, cost model to determine distributed SDN controller configuration, and delegating responsibilities among the controllers.

Resilient Networked Control Systems for Energy Delivery Systems – EDS rely on state estimation to obtain information about their operating conditions. State estimation is carried out based on the topology of the power network and data readings taken from measurement units deployed locally at substations. Based on state estimates obtained from the state estimator, control decisions and subsequent actions that directly impact the operation of the power grid are made. Attackers with access to the power grid's topology information can carry out false data injection (FDI) attacks which can lead to incorrect control actions that adversely impact the resilience of the power grid. A SDN controller equipped with risk score for a FDI attack can autonomously contain the attack based on available countermeasures which balance between security risk and operational resilience. The SDN controller needs to be equipped with a quarantine service which can create a quarantine zone and isolate portions of the power grid that are affected by the FDI attack from other parts of the network. The ability to deploy this autonomous attack containment will rely on accurate detection of FDI, computation of risk scores, and modeling the cost of countermeasures for quarantine

Researchers have proposed several approaches to address the problem of FDI attacks that target measurement data used in DC state estimation [23-32]. These efforts include, a detection framework employing a security manager, a managed switch and security agents running alongside critical nodes (controllers and edge nodes), detection tests based on excess deviations in the state estimation as measured by norms of residuas, and a strategy based on formation control to identify corrupted measurements from phasor measurement units (PMUs). Liu et al. proposed an adaptive partitioning state estimation (APSE) technique to detect bad data injections in the smart grid [30]. Specifically, the APSE partitions the power network into several subsystems, and the Chi-square test for bad data detection is used to detect bad data for each subsystem. Upon detection of bad-data, the subsystems are re-partitioned over several iterations until the bad data is located. The multi-agent system for FDI attack detection proposed is practical to deploy because it leverages on the existing communication channels among substations stipulated in the IEEE standard [31]. Our proposed technique addresses several limitations with the APSE techniques to enhance the accuracy of detecting FDI attack. First, we will address the scalability challenge of adopting APSE technique by ensuring that the node degree does not increase with the scale of the EDS. Second, our technique will also address the limitation of APSE's ability to detect bad data within a single transmission line. We will address the computational cost with the iterative execution of APSE. We will leverage the security score model to compute the risk of FDI attack for a given power grid topology. The security score will be utilized by the quarantine service in the SDN controller to determine the autonomous attack containment procedure. The goal for the service is to isolate the portion of the network impacted by FDI and ensure that the impact on operation of the power grid is minimal.

Bibliography:

1. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
2. Sumeet Jauhar, Binbin Chen, William G. Temple, Xinshu Dong, Zbigniew Kalbarczyk, William H. Sanders, and David M. Nicol. 2015. Model-Based Cybersecurity Assessment with NESCOR Smart Grid Failure Scenarios.

In *Proceedings of the 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC)* (PRDC '15). IEEE Computer Society, Washington, DC, USA.

3. Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K Iyer, and Zbigniew Kalbarczyk. Software-defined networking for smart grid resilience: Opportunities and challenges, Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, 2015.
4. Nick McKeown. Software-defined networking. INFOCOM keynote talk, 2009
5. SEL-2740 and SEL-5056 Software-Defined Network (SDN) Flow Controller, https://selinc.com/solutions/p/software-defined-network/
6. Dimitrios Gkounis. Cross-domain DoS link-flooding attack detection and mitigation using SDN principles. PhD thesis, MS thesis. Institute of Technology Zurich, 2014.
7. Upeka Premaratne, Jagath Samarabandu, Tarlochan Sidhu, Robert Beresh, and Jian-Cheng Tan. Security analysis and auditing of iec61850-based automated substations. Power Delivery, IEEE Transactions on, 25(4):2346-2355, 2010.
8. Deepa Kundur, Xianyong Feng, S Mashayekh, Shan Liu, Takis Zourntos, and Karen L Butler-Purry. Towards modelling the impact of cyber attacks on a smart grid. International Journal of Security and Networks, 6(1):2-13, 2011.
9. Thomas M Chen, Juan Carlos Sanchez-Aarnoutse, and John Buford. Petri net modeling of cyber physical attacks on smart grid. Smart Grid, IEEE Transactions on, 2(4):741-749, 2011.
10. Jinsub Kim and Lang Tong. Against data attacks on smart grid operations: Attack mechanisms and security measures. In Cyber Physical Systems Approach to Smart Electric Power Grid, pages 359-383. Springer, 2015.
11. T. Sommestad, M. Ekstedt, and H. Holm, The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures, Systems Journal, IEEE, vol. 7, no. 3, Sep. 2013.
12. E. LeMay, M. Ford, K. Keefe, W. Sanders, and C. Muehrke, Model based security metrics using ADversary VIew Security Evaluation (ADVISE), in QEST, Sep. 2011.
13. B. Kordy, L. Pietre-Cambacedes, and P. Schweitzer, DAG-based attack and defense modeling: Don't miss the forest for the attack trees, CoRR, vol. abs/1303.7397, 2013.
14. A. H. Vu, N. O. Tippenhauer, B. Chen, D. M. Nicol, and Z. Kalbarczyk, CyberSAGE: A tool for automatic security assessment of cyberphysical systems, in QEST, Sep. 2014.
15. Upeka Premaratne, Jagath Samarabandu, Tarlochan Sidhu, Robert Beresh, and Jian-Cheng Tan. Security analysis and auditing of iec61850-based automated substations. Power Delivery, IEEE Transactions on, 25(4):2346-2355, 2010.
16. OpenDaylight. http://www.opendaylight.org/.
17. ONOS, http://onosproject.org/
18. E. Handschin, F. C. Schweppe, J. Kohlas and A. Fiechter, Bad data analysis for power system state estimation, in IEEE Transactions on Power Apparatus and Systems, vol. 94, no. 2, pp. 329-337, Mar 1975.
19. Liu, Yao, Peng Ning, and Michael K. Reiter, False data injection attacks against state estimation in electric power grids, ACM Transactions on Information and System Security, 2011.
20. G. Hug and J. A. Giampapa, Vulnerability Assessment of AC State Estimation With Respect to False Data Injection CyberAttacks, Smart Grid, IEEE Transactions on, vol. 3, pp. 1362-1370,2012
21. O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, Malicious Data Attacks on the Smart Grid, Smart Grid, IEEE Transactions on, vol. 2, pp. 645-658, 2011.
22. Le Xie, M. Yilin and B. Sinopoli, False Data Injection Attacks in Electricity Markets, in Smart Grid Communications (SmartGridComm), 2010 First IEEE international Conference on, pp. 226-231, 2010.
23. Bobba, Rakesh B., et al. Detecting false data injection attacks on dc state estimation. Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010
24. G. Dan and H. Sandberg, Stealth Attacks and Protection Schemes for State Estimators in Power Systems, Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, Gaithersburg, MD, 2010, pp. 214-219.
25. S. Bi and Y. J. Zhang, Defending mechanisms against false-data injection attacks in the power system state

estimation,"2011 IEEE GLOBECOM Workshops (GC Workshops), Houston, TX, 2011, pp. 1162-1167.
26. D. Wei, M. Jafari and Y. Lu, On Protecting Industrial Automation and Control Systems against Electronic Attacks, 2007 IEEE International Conference on Automation Science and Engineering, Scottsdale, AZ, 2007, pp. 176-181.
27. Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 717-729, March 2014.
28. O. Kosut, Liyan Jia, R. J. Thomas and Lang Tong, Limiting false data attacks on power system state estimation, Information Sciences and Systems (CISS), 2010 44th Annual Conference on, Princeton, NJ, 2010, pp. 1-6.
29. J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, Probing the telltale physics: Towards a cyber-physical protocol to mitigate information corruption in smart grid systems, Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm), 2012, pp. 372-377.
30. T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, A novel method to detect bad data injection attack in smart grid, in Proc. IEEE INFOCOM, 2013, pp. 3423-3428
31. IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation," in IEEE Std 1646-2004, 2005
32. Z. Wang, A. Scaglione and R. J. Thomas, Generating Statistically Correct Random Topologies for Testing Smart Grid Communication and Control Networks, in IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 28-39, June 2010.