Towards Secured and Efficient Energy-Based Cyber-Physical Systems

Wei Yu
Assistant Professor
Director of Cyber-Physical Networking System and Security Research Laboratory
Department of Computer and Information Sciences, Towson University, Towson, MD
Email: wyu@towson.edu

1. Introduction

Smart grid is a highly distributed and complicated system and inherently operates under the presence of various uncertainties in both energy supply and demand. On the supply side, uncertainties can be raised by distributed renewable energy resources such as solar irradiance, wind speed and others. On the demand side, natural disasters, plug-in vehicles, personal habits of using energy, weather, and many others can make predicting energy usage difficult. Uncertainties can be raised by malicious attacks against communication network and physical grid as well. Hence, a systematical investigation of attack impacts on smart grid and the development of effective countermeasures to mitigate such attacks are critical.

To address these challenges, we consider that it is necessary to establish a strong theoretical and empirical foundation for secured and efficient energy resource management in smart grid. For this purpose, we will present in the workshop a modeling framework, which allows effective investigation of the interaction between communication networks and physical power grid. Based on the established theoretical framework, we will demonstrate how to utilize this model to systematically investigate the space of attacks in smart grid and develop countermeasures. Our established framework is generic and can be extended to investigate the security of other cyber-physical systems such as manufacture, weapon, and transportation systems.

The remainder of this position paper is organized as follows: In Section 2, we first present a modeling framework on secured and efficient energy resource management. In Section 3, we explore the space of attacks against system operation of smart grid and present countermeasures. We conclude the position paper in Section 4.

2. A Modeling Framework

The effective energy resources management in smart grid largely depends on the following orthogonal problems: (i) *How can we develop a modeling framework that considers and quantifies different uncertainties?* Uncertainties are mixtures of two dimensions: X: {cyber, physical} and Y: {failure, attack, others (e.g., user behavior)}. It is critical to quantify natural uncertainties from physical components (e.g., solar irradiance, weather such as wind speed, temperature, and others), failures, and malicious adversaries (e.g., injecting false information to the power grid). (ii) *How can we develop effective mechanisms to reduce impact from those uncertainties*? It is necessary to develop techniques that can effectively manage energy resources (e.g., transmission, distribution and storage) and adapt to those uncertainties, making the system efficient and resilient. As an example, it is critical to develop mechanisms to accurately model and predict diversified energy generation resources and demands from users and develop effective energy distribution schemes to balance energy demand and response.

To categorize the characteristics of failures and attacks, we consider developing the taxonomy of failures and threats in both power grid and communication network and develop modeling techniques to quantify the risk of different uncertainties, including <cyber network, failure>, <cyber network, attack>, <cyber network, other>, <physical grid, failure>, <physical grid, attack>, and <physical grid, other>. While attacks and failure are two different things, they could be tightly correlated as well. The impact of different failures and attacks on system performance shall be studied through real-world natural disasters, system failures, and/or attack scenarios to validate modeling results. The random noise that does not correlate with system parameters to quantify random failures in physical grid and communication networks needs be considered. In addition, the noise that is non-random and correlates with a system model, parameters, and configuration needs to be seriously considered because such noise can be used by cyber adversaries against both power grid and communication network components.

To effectively manage energy management, effective mechanisms to accurately model and predict energy generation and demands from users are needed. With accurate prediction for both generation and demand, effective energy distribution can balance supply and demand and can be formalized as an optimization problem. DER (Distributed Energy Resources) shall be integrated into the smart grid, which can be used to replace traditional fossil fuel resources [1]. With the development of electronic storage technology, integrating

the storage devices can reduce disturbances caused by peak and non-peak power usage [2]. Because the power grid has similarities to communication networks, the application of network traffic engineering techniques that have been traditionally used in communication networks can be beneficial. Storage devices can reduce the effects of short duration of outage, support more reliable services, and also be a defense scheme to counter cyber threats that tend to disrupt power grid operation.

3. Cyber Attacks in Smart Grid and Countermeasures

Smart grid may operate in hostile environments and smart meters in Advanced Metering Infrastructure (AMI) and sensor nodes in SCADA (Supervisory Control and Data Acquisition) lacking tamper-resistant hardware that increases the possibility to be compromised by the adversary [3-5]. The adversary can inject false measurement reports to the controller through compromised nodes (meters or sensors) and disrupt system operation and end users (e.g., consumer price, user privacy etc.). As the real time measurement data collected from AMI and SCADA for monitoring and control of energy resources provides the wide area situational awareness of power grid status, one of the most dangerous attacks are denoted as false data injection threats that can pose dangerous threats to smart grid [3, 6, 7, 8, 9]. However, the impact of cyber threats against monitoring and control of energy resources in the smart grid have not been systematically studied.

To address this issue, we shall systematically explore the space of attacks against the system operation from key functional modules, including static and dynamic state estimation, integration of DER and storage, optimal power flow control, contingency analysis, economic dispatch, and others. The first dimension X represents modules being attacked (e.g., *X_1: dynamic state estimation, X_2: static state estimation, X_3: optimal flow control, X_4: DER/storage integration*). The second dimension Y represents attack avenue *<Y_1: integrity of data, Y_2: timing accuracy>*, where Y_1 refers to ones that compromise the integrity of data such as the false data injection [3, 6, 7, 8, 9] and Y_2 refers to ones that disrupt the timing accuracy of data such as the attack against IEEE 1588 time synchronization protocol [10, 11]. The third dimension Z represents attack strength - either *<Z_{11}: strong, Z_{12}: stealthy>* or *<Z_{21}: full system knowledge, Z_{22}: partial system knowledge, Z_{23}: zero system knowledge>***.** In our preliminary result, we studied cyber-attacks against Kalman filtering on dynamic state estimation in smart grid, which can be generally categorized into *<X_1: dynamic state estimation (Kalman filtering), Y_1: integrity of data, Z_{12}: stealthy & Z_{12} stealthy/ $Z_{21/22}$: partial/full system knowledge>* [9].

In dimension X, attacks targeting different modules need to be systematically investigated and the attack avenue in dimension Y should be systematically explored, including data integrity attacks and timing-based attacks. Using the time synchronization as an example [11], time synchronization is a core component of reliable automation, fault analysis and recording in smart grid and other critical infrastructure applications. Both protocol-based and network-based attacks against time synchronization need to be investigated time synchronization protocols (e.g., IEEE 1588). Combined with attack dimensions X and Y, attack dimension Z shall be considered, including stealthy/strong attacks and attacks with full system/semi/zero system knowledge.

To defend against those attacks, we shall consider protection mechanisms to increase attack cost such as efficient mechanisms to filter out false data [12]. Using the power grid structure as an example, to make power grid resilient to attacks, some critical sensors shall be made resilient to increase the attack cost based on the power grid structure model. A resilient system, including both power grid and network structure needs to be carefully designed. As an example of enhancing the resilience of a component, the resilience of the Kalman filter - UKF technique [13] can be used to deal with attacks and make the component adapt to noise dynamically.

In addition to prevention, threat detection and attrition need to be seriously considered. For anomaly detection, we shall consider detection using both spatial and temporal correlation. For spatial-based detection, a hypothesis test can be leveraged to cause the damage to smart grid, manipulated measurements deviate more from their means than regular measurements with random noise. For temporal-based detection, consider that the adversary may slowly and stealthily launch attacks, nonparametric cumulative sum schemes can be used to deal with such attacks as it is capable of accumulating the small deviation of the observed measurement until value approaches a given threshold. To attack smart meters, the adversary needs to send malicious code propagation traffic over the network and inject the malicious code to devices in smart grid. With the awareness of power grid configuration and key characteristics, the correlation and integration of software behavior and network traffic should be considered to improve detection accuracy. Once an attack is detected, the compromised devices shall be identified and isolated. One possible technique is to use a watermarking technique to trace back malicious meters or sensors [14].

4. Conclusion

In this position paper, we considered that it is necessary to establish a theoretical and empirical foundation for secured and efficient energy resource management in smart grid. In the workshop, we present a modeling framework to investigate the interaction between communication network and power grid. Based on the developed framework, we will demonstrate how to utilize this model to systematically investigate the space of attacks in smart grid and develop countermeasures.

References

[1] MIT Energy Initiative, "The Future of the Electric Grid," 2011. Available at: *http://mitei.mit.edu/publications/reports-studies/future-electric-grid*.

[2] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang, "Smart Grid – the New and Improved Power Grid: A Survey," *IEEE Communications Surveys and Tutorials*, 2011.

[3] Yao Liu, Peng Ning, and Michael Reiter "Generalized False Data Injection Attacks against State Estimation in Electric Power Grids," *ACM Transactions on Information and System Security (TISSEC), vol. 14, no. 1*, May 2011.

[4] Alvaro A. Cárdenas, Saurabh Amin, and Shankar Sastry, "Research Challenges for The Security of Control Systems," in *Proceedings of 3rd USENIX Workshop on Hot Topics in Security (HotSec)*, 2008.

[5] Jaikumar Vijayan, "BStuxnet Renews Power Grid Security Concerns," in *Proceedings of Computerworld*, 2010.

[6] Jie Lin, Wei Yu, Xinyu Yang, Guobin Xu, and Wei Zhao, "On False Data Injection Attacks against Distributed Energy Routing in Smart Grid," in *Proceedings of ACM/IEEE Third International Conference on Cyber-Physical Systems (ICCPS)*, 2012.

[7] Wei Yu, "False Data Injection Attacks in Smart Grid: Challenges and Solutions," in *Proceeding of NIST Cyber Security for Cyber-Physical System (CPS) Workshop*, 2012.

[8] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, "On False Data Injection Attacks against Power System State Estimation: Modeling and Countermeasures," to appear in *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 2013.

[9] Qingyu Yang, Liguo Chang, and Wei Yu, "On False Data Injection Attacks against Kalman Filtering in Power System Dynamic State Estimation," in *International Journal of Security and Communication Networks (SCN)*, Wiley, 2013.

[10] Qingyu Yang, Dou An, and Wei Yu, "On Time Desychronization Attack against IEEE 1588 Protocol," in *Proceedings of IEEE EnergyTech*, 2013.

[11] IEEE, "IEEE 1588TM Standard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," Available at: *http://grouper.ieee.org/groups/1588/*

[12] Xinyu Yang, Jie Lin, Wei Yu, Paul Moulema, Xinwen Fu, and Wei Zhao, "A Novel En-route Filtering Scheme against False Data Injection Attacks in Cyber-Physical Networked Systems," to appear in IEEE Transactions on Computers (TC), 2013.

[13] Gustavo Valverde and Vladimir Terzija, "Unscented Kalman Filter for Power System Dynamic State Estimation," in *Generation, Transmission and Distribution - IET, vol. 5, no. 1*, pp.29–37, 2011.

[14] Sulabh Bhattarai, Linqiang Ge, and Wei Yu, "A Novel Architecture against False Data Injection Attacks in Smart Grid", in *Proceeding of IEEE ICC 2012 – Communication and Information Systems Security Symposium*, June 2012.