

False Data Injection Attacks in Smart Grid: Challenges and Solutions

Wei Yu

Department of Computer and Information Sciences
Towson University, Towson, MD 21252.
Email: wyu@towson.edu

Abstract—Smart Grid, as an energy-based Cyber-Physical System (CPS), is a new type of power grid that will provide reliable, secure, and efficient energy transmission and distribution. As the quality of assurance of monitoring data is essential to smart grid, in this talk we will first present two dangerous false data injection attacks, which target the state estimation and energy distribution in smart grid, respectively. We then present several defensive strategies against such attacks.

I. INTRODUCTION

The design of Cyber-Physical System (CPS) tends to integrate computing and communication capabilities with monitoring and control of entities in the physical world. Unlike traditional embedded systems, CPS is natural and engineered physical systems, which are integrated, monitored and controlled by an intelligent computational core [6]. A host of CPS, including the smart grid, process control systems, and transportation systems, are expected to be developed using advanced computing and communication technologies [4]. A smart grid is a typical energy-based CPS [1], which integrates a physical power transmission system with the cyber process of network computing and communication.

The quality of assurance of monitoring data is essential to smart grid. While most existing techniques for protecting power grids were designed to ensure system reliability (e.g., against random failures), recently there is a growing concern in smart grid initiatives on the protection against malicious cyber attacks. It was found that an adversary may launch attacks by compromising meters, hacking communication networks between meters and SCADA systems, breaking into the SCADA system through a control center office LAN, and breaking home area network and neighboring area network to compromise meters. Smart grid may operate in hostile environments and the sensor nodes lacking tamper-resistance hardware increases the possibility to be compromised by the adversary. Hence, the adversary can inject false measurement reports to disrupt the smart grid operation through the compromised meters and sensors. Those attacks are denoted as false data injection attacks and raise dangerous threats to the grid. In this following, we will first present two representative types of false data injection attacks and then discuss possible countermeasures.

II. FALSE DATA INJECTION ATTACKS

We now present two representative false data injection attacks, which target the state estimation and energy trans-

mission in smart grid.

(i) *False Data Injection Attacks against State Estimation*: It is critical for a smart grid to estimate its operating state based on meter measurements in the field and the configuration of grid. Recently, Liu *et al.* [3] developed a novel false data injection attack, which bypasses all the existing detection schemes and is therefore capable of arbitrarily manipulating power system states, posing dangerous threats to the control of power system. Differently, we considered the issue of how an adversary can choose the meters to compromise in order to cause the most significant deviation of the system state estimation [5]. We developed the least-effort attack model, which efficiently identifies the optimal set of meters to launch false data injection attacks for a fixed number of state variables. We also developed a heuristic algorithm to derive the results efficiently. The basic idea is listed below: the large power grid network is divided into a number of overlapping areas; the brute-force search method is used to identify the optimal set of meters for individual small areas and derive the optimal set of meters for the whole network. This heuristic algorithm was implemented on power system state manipulation using various IEEE standards buses (e.g., 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus). Our data validated the feasibility and effectiveness of the developed scheme.

(ii) *False Data Injection Attacks against Distributed Energy Distribution*: Smart grid shall integrate the distributed energy resources and intelligently transmit energy to meet the requests from users. Hence, how to secure the distributed energy transmission and distribution process that utilizes the distributed energy resources and minimizes the energy transmission overhead is critical in smart grid. In our preliminary study, we studied the vulnerability of distributed energy transmission and distribution process and investigate novel false data injection attacks against distributed energy transmission and distribution process [2]. We considered several types of representative attacks, in which the adversary may manipulate the quantity of energy supply, the quantity of energy response, and link state of energy transmission. The forged data injected by those attacks will cause imbalanced demand and supply, increase the cost for energy distribution, disrupt the energy distribution causing some nodes energy outage in smart grid, and even manipulating energy price. Using graph and optimization theory, we formally modeled the attacks and quantitatively analyze their impact on energy distribution in smart grid. Our simulation data validated the effectiveness of those attacks

disrupting the effectiveness of energy distribution process, which may pose significant supplied energy loss, the increase of energy transmission cost, the number of outage users, and manipulation of energy price.

III. COUNTERMEASURES

To address those issues, we shall design the defensive countermeasures from the following perspectives: attack prevention, detection and response.

(i) *Prevention*: We shall enhance the network configuration to improve the resilience of grid to attacks. One way is to fully protect some of critical sensors and make them hard to be attacked. From the both attacks describe above, we can see that the false data injection attacks will become more difficult when we hide more system topology information. However, protecting all the sensors are impossible to realize in real-world practice because of deployment cost. Hence, we shall investigate the problem: given the limited number of sensors to be protected due to the cost constraint, how we can find the set of sensors to protect and make false data injection attacks difficult to deploy? We shall investigate the effectiveness of this countermeasure against the attacks when critical and redundant measurements are provided.

(ii) *Detection*: We shall develop robust intrusion detection techniques. Recall that in order to cause damage (e.g., manipulating the state estimation and energy transmission), the adversary needs to manipulate the sensor measurements. Obviously, if the adversary changes the true measurement value by a larger margin, he can manipulate smaller number of sensors, given a number of states to manipulate. In order to avoid from being detected by the standard anomaly detection, the adversary may become stealthy and tend to marginally change the sensor measurements, but still be able to manipulate the states to some extent. To address this problem, we shall analyze the properties of the false data injection attacks and find that the features with attacks always deviate much more from their means than measurements with random noises.

(iii) *Response*: Once an attack is detected, we shall develop schemes to localize the compromised devices and isolate the compromised devices from the grid. For example, to achieve this goal, one of schemes we shall consider is to adopt efficient watermarking-based forensic traceback scheme, which embeds secret signal (bits of 1 and 0) into the meter data stream. If the meter data stream is manipulated by any device during the transmission path, the receiver can correlate the received data stream with the secret signal and detect whether the data stream has been manipulated. By repeating the process over the transmission path, we can trace the origin which manipulates the data.

IV. CONCLUSION

In this talk, we first present two types of false data injection attacks against smart grid operation. One is to disrupt the state estimation of smart grid and the other is to disrupt the energy distribution of smart grid. We then present several possible countermeasures, including attack prevention, detection and response.

REFERENCES

- [1] Nsf workshop on new research directions for future cyber-physical energy systems. Technical report, <http://www.ece.cmu.edu/nsf-cps/>, Baltimore, MD, 2009.
- [2] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao. On false data injection attacks against distributed energy routing in smart grid. In *Proc. of ACM/IEEE Third International Conference on Cyber-Physical Systems (ICCPs) (part of CPS Week 2012)*, April 2012.
- [3] Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, November 2009.
- [4] J. Wang, D. Li, Y. Tu, P. Zhang, and F. Li. A survey of cyber physical systems. In *Proc. of IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, March 2011.
- [5] Q. Yang, J. Yang, W. Yu, N. Zhang, and W. Zhao. On a hierarchical false data injection attack of power system state estimation. In *Proc. of IEEE Globe Communication (GlobeCom)*, December 2011.
- [6] T. Znati. Security for emerging cyber-physical systems research challenges and directions. In *Proc. of First International Workshop on Data Security and Privacy in wireless Networks Panel*, July 2010.