Detection of False Data Injection Attacks in Smart Grid Cyber-Physical Systems

LI BEIBEI, G1402613K

Abstract

Building an efficient, green, and multifunctional smart grid cyber-physical system (CPS) while maintaining high reliability and security is an extremely challenging task, particularly in the ever-evolving cyber threat landscape. This challenge is also compounded by the increasing pervasiveness of information and communications technologies across the power infrastructure, as well as the growing availability of advanced hacking tools in the hacker community. One of the most critical security threats in smart grid CPSs lies in the high-profile false data injection (FDI) attacks, where the attackers attempt to inject either fabricated measurement data to mislead power grid state estimation & bad data detection or tampered command data to misguide power management & control. Accordingly, FDI attacks can be subdivided into false measurement data injection (FMDI) attacks and false command data injection (FCDI) attacks, respectively.

Detection techniques for FDI attacks have been a significant research focus in smart grid CPSs to withstand these security threats and further protect the power infrastructure. However, conventional state estimation based bad data detection approaches have been proved vulnerable to the evolving FDI attacks. To meet this gap, this thesis introduces four creative research works to analyze and detect FDI attacks in smart grid CPSs.

First, a stochastic Petri net based analytical model is developed to evaluate and analyze the system reliability of smart grid CPSs, specifically against topology attacks under system countermeasures (i.e., intrusion detection systems and malfunction recovery techniques). Topology attacks are evolved from FDI attacks, where attackers initialize FDI attacks by tempering with both measurement data and grid topology information. This analytical model is featured by bolstering both transient and steady-state analysis of system reliability.

Second, a distributed host-based collaborative detection scheme is proposed to detect FMDI attacks in smart grid CPSs. It is considered in this work that the phasor measurement units (PMUs), deployed to measure the operating states of power grids, can be compromised by FMDI attackers, and the trusted host monitors (HMs) assigned to each PMU are employed to monitor and assess PMUs' behaviors. Neighboring HMs make use of the majority voting algorithm based on a set of predefined normal behavior rules to identify the existence of abnormal measurement data collected by PMUs. In addition, an innovative reputation system with an adaptive reputation updating algorithm is also designed to evaluate the overall operating status of PMUs, by which FMDI attacks can be distinctly observed.

Third, a Dirichlet-based detection scheme for FCDI attacks in hierarchical smart grid CPSs are proposed. In the future hierarchical paradigm of a smart grid CPS, it is considered that the decentralized local agents (LAs) responsible for local management and control can be compromised by FCDI attackers. By issuing fake or biased commands, the attackers anticipate to manipulate the regional electricity prices with the purpose of illicit financial gains. The proposed scheme builds a Dirichlet-based probabilistic model to assess the reputation levels of LAs. Integrated with a newly designed adaptive reputation incentive mechanism, this model enables quick and efficient detection of FCDI attacks as well as the attackers.

Last, we systematically explore the feasibility and limitations of detecting FMDI attacks in smart grid CPSs using distributed flexible AC transmission system (D-FACTS) devices. Recent studies have investigated the possibilities of proactively detecting FMDI attacks on smart grid CPSs by using D-FACTS devices. We term this approach as proactive false data detection (PFDD). In this work, the feasibility of using PFDD to detect FMDI attacks are investigated by considering single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FMDI attacks, respectively. It is proved that PFDD can detect all these three types of FMDI attacks as long as the deployment of D-FACTS devices covers branches at least containing a spanning tree of the grid graph. In addition, the limitations of using PFDD to localize the FMDI targeted bus(es) are also discussed. It is noted that, although PFDD is almost perfect in detecting FMDI attacks, imperfect localization accuracies arise in certain cases due to limited information provided by using PFDD.

Publication List

- **Book Chapters:**

B1. **Beibei Li**, Rongxing Lu, and Haiyong Bao. “Behavior Rule Specification-based False Data Injection Detection Technique for Smart Grid”. In *Cyber Security for Industrial Control Systems: From the Viewpoint of Close-Loop,* pp. 119-150, Apr. 2016, CRC Press.

- **Journal Papers:**

J1. **Beibei Li**, Gaoxi Xiao, Rongxing Lu, Ruilong Deng, Haiyong Bao. “On Feasibility and Limitations of Detecting False Data Injection Attacks on Smart Grids Using D-FACTS Devices”. Submitted to *IEEE Internet of Things Journal,* 2018.

J2. **Beibei Li**, Rongxing Lu, Kim-Kwang Raymond Choo, Wei Wang, Sheng Luo. “On Reliability Analysis of Smart Grids under Topology Attacks: A Stochastic Petri Net Approach”. *ACM Transactions on Cyber-Physical Systems*, to appear, 2018.

J3. **Beibei Li**, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo. “Distributed Host-based Collaborative Detection for False Data Injection Attacks in Smart Grid Cyber-Physical System”. *Journal of Parallel and Distributed Computing,* vol. 103, pp. 32-41, May 2017.

J4. **Beibei Li**, Rongxing Lu, Wei Wang, Kim-Kwang Raymond Choo. “DDOA: A Dirichlet-based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System”. *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415 - 2425, Nov. 2016.

J5. Haiyong Bao, Rongxing Lu, **Beibei Li**, Ruilong Deng. “BLITHE: Behavior Rule Based Insider Threat Detection for Smart Grid”. *IEEE Internet of Things Journal*, vol. 3, no. 2, pp. 190-205, Apr. 2016.

- **Conference Papers:**

C1. **Beibei Li**, Rongxing Lu, Gaoxi Xiao, Zhou Su, Ali Ghorbani. “PAMA: A Proactive Approach to Mitigate False Data Injection Attacks in Smart Grids”. Submitted to *IEEE GLOBECOM 2018*.

C2. Mi Wen, Donghuan Yao, **Beibei Li**, Rongxing Lu. “State Estimation Based Energy Theft Detection Scheme with Privacy Preservation in Smart Grid”. *IEEE International Conference on Communications (ICC) 2018*, to appear.

C3. **Beibei Li**, Rongxing Lu, Gaoxi Xiao. “HMM-Based Fast Detection of False Data Injections in Advanced Metering Infrastructure”. *IEEE GLOBECOM*, Singapore, Dec. 2017.