Wireless Networks

Series editor
Xuemin Sherman Shen
University of Waterloo, Waterloo, ON, Canada

The purpose of Springer's Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.

** Indexing: Wireless Networks is indexed in EBSCO databases and DPLB **

More information about this series at http://www.springer.com/series/14180

Beibei Li • Rongxing Lu • Gaoxi Xiao

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

Springer

Beibei Li
College of Cybersecurity
Sichuan University
Chengdu, Sichuan, China

Rongxing Lu
Faculty of Computer Science
University of New Brunswick
Fredericton, NB, Canada

Gaoxi Xiao
School of Electrical and Electronic Engineering
Nanyang Technological University
Singapore, Singapore

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-030-58671-3 ISBN 978-3-030-58672-0 (eBook)
https://doi.org/10.1007/978-3-030-58672-0

© Springer Nature Switzerland AG 2020
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

This book is wholeheartedly dedicated to my respectable supervisors, as well as our group members, with whom we have worked over the years and have made it possible to reach this moment.

To my beloved families.

Preface

Building an automated, green, and efficient smart grid cyber-physical system (CPS) while ensuring high reliability and security is an extraordinarily 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 attackers attempt to inject either fabricated measurement data to mislead power grid state estimation and bad data detection or tampered command data to misguide power management and control. Accordingly, FDI attacks can be subdivided into false measurement data injection (FmDI) attacks and false command data injection (FcDI) attacks.

Detection techniques for FDI attacks have been a significant research focus for 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 monograph 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, particularly against topology attacks under system countermeasures (such as intrusion detection systems and malfunction recovery techniques) in place. Evolved from FmDI attacks, topology attacks inject false data 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 chapter that phasor measurement units (PMUs), deployed to measure the operating status of power grids, can be compromised by FmDI attackers. Trusted host monitors (HMs) are assigned to each PMU 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 designed to evaluate the overall operating status of PMUs, by which FmDI attacks, as well as the attackers, can be distinctly observed.

Third, a Dirichlet-based detection scheme for FcDI attacks in hierarchical smart grid CPSs is proposed. In the future hierarchical paradigm of a smart grid CPS, it is considered that the decentralized LAs responsible for local management and control can be compromised by FcDI attackers. By issuing fake or biased commands, the attackers anticipate manipulating 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. This probabilistic model, used in conjunction with a designed adaptive reputation incentive mechanism, enables quick and efficient detection of FcDI attacks as well as the attackers.

Lastly, 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 chapter, the feasibility of employing PFDD approach to detect FmDI attacks is investigated under single-bus, uncoordinated multiple-bus, and coordinated multiple-bus FmDI attacks. It is proved that the PFDD approach is capable of detecting all these three types of FmDI attacks targeted on buses or super-buses with degrees larger than 1, as long as the deployment of D-FACTS devices covers branches forming at least a spanning tree of the power grid graph. Then, the minimum efforts demanded for activating D-FACTS devices to detect the considered three types of FmDI attacks are evaluated. In addition, the limitations of PFDD are also discussed, and it is strictly proven that this approach is not able to identify FmDI attacks on smart grid CPSs that are targeted on buses or super-buses with degrees equaling 1.

Chengdu, Sichuan, China — Beibei Li
Fredericton, NB, Canada — Rongxing Lu
Singapore, Singapore — Gaoxi Xiao
June 2020

Acknowledgements

There have been many people who have walked alongside me during my Ph.D. journey. They have guided, supported, and accompanied me. I would like to, hereby, thank each and every one of them sincerely.

First and foremost, I would like to express my deepest gratitude to my respectable supervisors—Dr. Xiao Gaoxi at Nanyang Technological University (NTU), Singapore, and Dr. Lu Rongxing at the University of New Brunswick (UNB), Canada—for their unwavering support and constructive guidance throughout this thesis. They, upon whose shoulders I stand, explored and paved the path before me. Without them, this thesis would simply not have been possible. Such academic rigor as may be found in this thesis is largely due to Dr. Xiao's refusal to let me get away with things, while his unerring sense of when and how to intervene has taught me not only as a good researcher but also a potential good tutor. He is always willing to take time to listen and usually provide insightful questions and comments, as well as clear instructions as feedback. Dr. Lu is a renowned expert in cybersecurity domain, whose passion for doing research and teaching has set a new standard for everyone involved. His unstinting support and encouragement have driven me to strive for excellence. Having also a friend figure, Dr. Lu is really a nice guy who cares about his students not only on their research career but also on daily lives. Many thanks are also due to Dr. Wang Licheng at Beijing University of Posts and Telecommunications (BUPT), China, who started me down this road with selfless support, encouragement, and guidance.

I would especially acknowledge my Thesis Advisory Committee (TAC) members—Dr. Zhang Jie and Dr. Ma Maode at NTU. Thanks for their faith in my ability and continuous support ever since I joined NTU. I hope this research opens up opportunities for us to do research together in the future.

I would extend my heartfelt gratitude to Dr. Ali A. Ghorbani, Dr. Kim-Kwang Raymond Choo, Dr. Bao Haiyong, Dr. Deng Ruilong, Dr. Wang Wei, and Dr. Luo Sheng, who contributed to the making of this monograph. Thanks for their constructive criticism, which enabled me to improve my research and writing skills. Particular thanks must also be recorded to Dr. Xu Chang, Dr. Liu Yali, Dr. Kong Qinglei, Dr. Zhao Ming, Dr. Meng Min, Dr. Lin Changlu, Dr. Liu Ximeng, Dr. Li

Chen, Dr. Li Lichun, Dr. Hu Hao, Dr. Zhai Chao, Mr. Huang Cheng, Mr. Wang Guoming, Mr. Katuwal Rakesh, Mr. Cheng Shuo, Mr. Hao Changyu, Mr. Zhang Hehong, and Mr. Li Xiang who offered collegial guidance and support over the years.

There are many of my friends to name individually; however, special thanks are given to Dr. Yang Rong, Dr. Li Dan, Dr. Yang Ming, Dr. Bi Hui, Dr. Ma Lijia, Dr. Zhang Heng, Dr. Wang Zeng, Dr. Chen Chunyang, Ms. Sun Meng, Ms. Gao Yumeng, Ms. Gong Bo, Ms. Huang Yi, Ms. Wang Zhenzhen, Ms. Huang Rui, Ms. Xin Jian, Ms. Chen Qian, Ms. Wang Yongheng, Ms. Li Yanan, Ms. Chen Shi, Ms. Chen Qiyin, Ms. Zhang Lili, Ms. Ouyang Qingling, Ms. Zhang Ran, Mr. Cheng Yanyu, Mr. Liu Yunxiang, Mr. Pan Zihan, Mr. Wang Yang, Mr. Shao Hongxin, Mr. Li Xiaochen, Mr. Zhang Yunlong, Mr. Guo Zhihong, Mr. Zhang Songze, and Mr. Gao Li at NTU and Dr. Yang Haomiao, Dr. Huang Junlin, Ms. Yang Xue, Ms. Zheng Yandong, Ms. Li Huixia, Ms. Deepigha S. V. Babu, Mr. Guo Wei, Mr. Xu Chenghao, Mr. Hassan Mahdikhani, Mr. Saeed Shafeiee Hasanabadi, Mr. Tao Xi, Mr. Zhang Xichen, Mr. Xiao Hongtao, and Mr. Zhang Yongcan at UNB. Thanks for giving me a wonderful and memorable life at both NTU and UNB. In addition, my wholehearted thanks are given to Mrs. Han Yuhong, Ms. Xie Wanlun, Ms. Yu Pan, Mr. Du Wuhang, and Mr. Chen Dawen at BUPT for their generous support, understanding, and encouragement given in many moments of crisis over the years. I cannot list all the names here, but you guys hold a special place in my heart.

Finally, and most importantly, my most heartfelt and forever gratitude goes to my family and girlfriend, who have always been a constant source of support and encouragement. Thanks to my parents and elder sister for putting me through the best education possible and giving me the strength to reach for the stars and chase my dreams. I appreciate their sacrifices and unending support, and I would not have been able to get to this stage without them.

Contents

1 Introduction 1
1.1 Background 1
1.1.1 Cybersecurity Events Relating to Electric Grids 1
1.1.2 Recent Actions and Investments in Security and Reliability of Electric Grids 4
1.2 Brief Introduction of a Smart Grid CPS 5
1.2.1 Cyber-Physical System 5
1.2.2 Smart Grid CPS 6
1.2.3 The Architecture of SCADA 8
1.2.4 The Architecture of WAMS 9
1.3 Security Requirements, Challenges, and Research Motivations 11
1.3.1 Security Requirements 11
1.3.2 Security Challenges 13
1.3.3 Research Motivations 19
1.4 Research Contributions 20
1.5 Monograph Outline 21
References 22

2 Fundamentals and Related Literature 23
2.1 State Estimation and Bad Data Detection 23
2.1.1 AC Power Flow Model State Estimation Formulation 23
2.1.2 DC Power Flow Model State Estimation Formulation 24
2.1.3 General Structure of H matrix 25
2.1.4 Bad Data Detection 30
2.2 FmDI Attacks Against AC State Estimation 31
2.3 FmDI Attacks Against DC State Estimation 33
2.4 State-of-the-Art Literature 34
2.4.1 A Taxonomy of IDSs 34
2.4.2 FDI Attacks Detection 37
2.4.3 Insider Threats Detection 37
References 38

3 SPNTA: Reliability Analysis Under Topology Attacks—A Stochastic Petri Net Approach 41
3.1 Introduction 41
3.2 Preliminaries 43
3.2.1 Petri Net Modeling 43
3.2.2 Coordinated Attacks 44
3.3 Models and Design Goals 45
3.3.1 System Model 45
3.3.2 Adversary Model 47
3.3.3 Design Goals 49
3.4 Proposed Analytical Model 49
3.4.1 Construction of the Proposed SPN Model 50
3.4.2 Maximum Spanning Tree Based Unreliability Enabling Scheme 54
3.5 Performance Evaluation 59
3.5.1 Performance Metrics 59
3.5.2 Numerical Results 62
3.6 Summary 72
References 72

4 DHCD: Distributed Host-Based Collaborative Detection for FmDI Attacks 75
4.1 Introduction 75
4.2 Models and Design Goals 77
4.2.1 System Model 77
4.2.2 Threat Model 77
4.2.3 Design Goals 78
4.3 Proposed DHCD Method 79
4.3.1 Collaborative FDD 79
4.3.2 Determination of Compromised PMU 83
4.4 Performance Evaluation 88
4.4.1 Efficacy of FDD Algorithm 89
4.4.2 Identification of Compromised PMUs with Our Reputation System 91
4.5 Summary 95
References 96

5 DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks 99
5.1 Introduction 99
5.2 Models and Design Goals 102
5.2.1 System Model 102
5.2.2 Threat Model 103
5.2.3 Design Goals 105
5.3 Preliminaries 105
5.3.1 State Estimation 106

5.3.2 Real-Time LMPs 106
5.3.3 Dirichlet Distribution 107
5.4 The Proposed DDOA Scheme 108
5.4.1 Behavior Rule Specifications 108
5.4.2 Dirichlet-Based Reputation Model 109
5.4.3 Description of DDOA 111
5.5 Performance Evaluation 114
5.5.1 Data Collection in PowerWorld 114
5.5.2 Data Analytics in MATLAB 115
5.6 Summary 120
References 120

6 PFDD: On Feasibility and Limitations of Detecting FmDI Attacks Using D-FACTS 123
6.1 Introduction 123
6.2 Overview and Models 125
6.2.1 Overview of D-FACTS Devices 125
6.2.2 System Model 125
6.2.3 Adversary Model 127
6.3 The Feasibility of PFDD 128
6.3.1 The Framework for PFDD Approach 128
6.3.2 Evaluation of the Minimum Efforts Demanded for D-FACTS Devices to Identify Effective FmDI Attacks 130
6.3.3 The Minimum Requirement of D-FACTS Devices Implementation to Detect FmDI Attacks 137
6.4 Discussions on the Limitations of PFDD Approach 139
6.4.1 Limitations of Identifying Effective FmDI Attacks by Using the PFDD Approach 140
6.4.2 Case Studies 144
6.5 Summary 147
References 147

7 Epilogue 149
7.1 Summary of Contributions 149
7.2 Future Work 150

Index 153

Acronyms

AC	Alternating current
CC	Control center
CPS	Cyber-physical system
DC	Direct current
DDoS	Distributed denial-of-service
DoS	Denial-of-service
D-FACTS	Distributed flexible AC transmission system
FcDI	False command data injection
FDD	False data detection
FDI	False data injection
FmDI	False measurement data injection
GPS	Global positioning system
HM	Host monitor
HMI	Human–machine interface
ICS	Industrial control system
ICT	Information and communications technology
IDS	Intrusion detection system
IED	Intelligent electronic device
IoT	Internet-of-things
IPS	Intrusion prevention system
LA	Local agent
LAN	Local area network
LMP	Locational marginal price
MLE	Maximum likelihood estimation
MTTD	Mean time to disturbance
MTTF	Mean time to failure
MTTM	Mean time to malfunction
MxST	Maximum spanning tree
PDC	Phasor data concentrator
PLC	Programmable logic controller
PMU	Phasor measurement unit

RF	Radio frequency
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SDH	Synchronous digital hierarchy
SONET	Synchronous optical networking
SPN	Stochastic Petri net
WAMS	Wide area measurement system
WAN	Wide area network