

# Smart Grids: Security and Privacy Issues

Kianoosh G. Boroojeni • M. Hadi Amini  
S.S. Iyengar

# Smart Grids: Security and Privacy Issues

 Springer

Kianoosh G. Boroojeni  
School of Computing and Information  
Sciences  
Florida International University  
Miami, FL, USA

S.S. Iyengar  
School of Computing and Information  
Sciences  
Florida International University  
Miami, FL, USA

M. Hadi Amini  
SYSU-CMU Joint Institute of Engineering  
School of Electronics and Information  
Technology  
Sun Yat-sen University  
Guangzhou, Guangdong, China

Department of Electrical and Computer  
Engineering  
Carnegie Mellon University  
Pittsburgh, PA, USA

ISBN 978-3-319-45049-0

ISBN 978-3-319-45050-6 (eBook)

DOI 10.1007/978-3-319-45050-6

Library of Congress Control Number: 2016951722

© Springer International Publishing Switzerland 2017

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, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

There has been a growing trend in the power systems from a centralized producer-driven grid to a smarter interactive customer network. This requirement compels a new way of designing smart grids for a more reliable and secure power system performance. Involving the demand side in the power system management requires large-scale utilization of distributed communication networks. In this context, there is a considerably increasing concern regarding the security and privacy of both physical and communication layers of the network. This book utilizes an advanced interdisciplinary approach to address the existing security and privacy issues and propose legitimate countermeasures for each of them in the standpoint of both computing and electrical engineering. The proposed methods are theoretically proved by mathematical tools and illustrated by real-world examples.

This book paves the way for researchers working on privacy and security issues spread throughout computer science and smart grids. Furthermore, it provides the readers with a comprehensive insight to understand an in-depth big picture of privacy and security challenges in both physical and information aspects of smart grids. This book can be used as textbook for graduate-level courses in computer engineering, computer science, electrical engineering, and other related areas.

## Features

Here are the unique aspects of our book which address the oblivious network routing problems:

- (1) Preserving of the location privacy of mobile users of future smart grids.
- (2) The security of smart grids attracts researchers' attentions.
- (3) Information privacy for smart meters and mobile users plays a key role in future smart grids.
- (4) Maintaining the reliability of the smart grids.

- (5) Providing security countermeasures for false data injection into the communication networks of smart grids.
- (6) Evaluating the privacy and security of both physical and information infrastructures.

Proposing a novel congestion-based economic dispatch framework based on oblivious routing network concept.

## **Intended Audience**

This monograph is suitable for senior undergraduate students, graduate students, and the researchers working in the related areas.

Miami, FL, USA  
Pittsburgh, PA, USA  
Miami, FL, USA

Kianoosh G. Boroojeni  
M. Hadi Amini  
S.S. Iyengar

# Acknowledgments

This work has evolved from our research on security and privacy in smart grids. Kianoosh G. Boroojeni and S.S. Iyengar would like to thank NSF, NIH, and other research funding institutes for funding their research works.

M. Hadi Amini would like to thank his parents, Alireza and Parvin, for their unconditional support and encouragement throughout his life. He also would like to appreciate the kindly support of his artist sister, his uncle, and his brother-in-law. He also would like to express his gratitude towards his beloved niece.

Kianoosh G. Boroojeni would like to express his sincere gratitude to his family for their continuous inspiration and support.

# Contents

<b>1</b>	<b>Overview of the Security and Privacy Issues in Smart Grids</b>	<b>1</b>
1.1	Security Issues in Smart Grid	1
1.2	Physical Network Security	3
1.3	Information Network Security	6
1.3.1	Detection Mechanisms	7
1.3.2	Mitigation Mechanisms	7
1.4	Privacy Issues in Smart Grids	8
1.4.1	$k$ -Anonymity Cloaking	9
1.4.2	Location Obfuscation	9
1.4.3	Location Privacy Quantification and Formalization	10
1.5	Book Structure and Outlook	10
	References	11

## Part I Physical Network Security

<b>2</b>	<b>Reliability in Smart Grids</b>	<b>19</b>
2.1	Introduction	19
2.2	Preliminaries on Reliability Quantification	22
2.3	System Adequacy Quantification	23
2.4	Congestion Prevention: An Economic Dispatch Algorithm	24
2.5	Summary and Conclusion	25
	References	28
<b>3</b>	<b>Error Detection of DC Power Flow Using State Estimation</b>	<b>31</b>
3.1	Introduction	31
3.2	Preliminaries of the DC Power Flow and State Estimation	33
3.2.1	Introduction to State Estimation	35
3.3	Minimum-Variance Unbiased Estimator (MVUE)	36
3.3.1	Measurement Error Representation in the Linear DC Power Flow Equation	37
3.3.2	Linear Model	37
3.3.3	Generalized Linear Model for State Estimation	38

3.4	Bayesian-Based LMMSE Estimator for DC Power Flow Estimation	39
3.4.1	Linear Model	39
3.4.2	Bayesian Linear Model	40
3.4.3	Maximum Likelihood Estimator for DC Power Flow Estimation	40
3.4.4	Bayesian-Based Linear Estimator for DC Power Flow	40
3.4.5	Recursive Bayesian-Based DC Power Flow Estimation Approach for DC Power Flow Estimation	41
3.5	Error Detection Using Sparse Vector Recovery	42
3.5.1	Sparse Vector Recovery	43
3.5.2	Proposed Sparsity-Based DC Power Flow Estimation	44
3.5.3	Case Study and Discussion	46
	References	48
<b>4</b>	<b>Bad Data Detection</b>	<b>53</b>
4.1	Preliminaries on Falsification Detection Algorithms	53
4.1.1	Autocorrelation Function (ACF)	54
4.2	Time Series Modeling of Load Power	54
4.2.1	Outline of the Proposed Methodology	54
4.2.2	Seasonality	56
4.2.3	Fitting the AR and MA Models	59
4.3	Case Study	59
4.3.1	Stabilizing the Variance	60
4.3.2	Fitting the Stationary Signal to a Model with Autoregressive and Moving-Average Elements	61
4.3.3	Model Fine-Tuning and Evaluation	64
4.4	Summary and Conclusion	68
	References	68
<b>Part II Information Network Security</b>		
<b>5</b>	<b>Cloud Network Data Security</b>	<b>71</b>
5.1	Introduction	71
5.2	Data Security Protection in Cloud-Connected Smart Grids	73
5.2.1	Simulation Scheme	78
5.2.2	Simulation Results	79
5.3	Summary and Outlook	80
	References	81
<b>Part III Privacy Preservation</b>		
<b>6</b>	<b>End-User Data Privacy</b>	<b>85</b>
6.1	Introduction	85
6.2	Preliminaries to Privacy Preservation Methods	87
6.2.1	$k$ -Anonymity Cloaking	87
6.2.2	Location Obfuscation	88
6.2.3	Preliminary Definitions	89



- 6.3 Privacy Preservation: Location Obfuscation Methods ..... 90
- 6.4 Summary and Conclusion ..... 91
- References ..... 91
- 7 Mobile User Data Privacy ..... 93**
  - 7.1 Introduction ..... 94
  - 7.2 Preliminaries on Mobile Nodes Trajectory Privacy ..... 95
    - 7.2.1 Location-Based Service ..... 96
    - 7.2.2 Location Privacy-Preserving Mechanism ..... 96
    - 7.2.3 Adversary ..... 97
  - 7.3 Privacy Preservation Quantification: Probabilistic Model ..... 97
  - 7.4 A Vernoï-Based Location Obfuscation Method ..... 100
    - 7.4.1 A Stochastic Model of the Node Movement ..... 102
    - 7.4.2 Proposed Scheme for a Mobile Node ..... 103
    - 7.4.3 Computing the Instantaneous Privacy Level ..... 104
    - 7.4.4 Concealing the Movement Path ..... 107
  - 7.5 Summary and Conclusion ..... 108
  - References ..... 109
- Index ..... 111**

# Biography

## **Kianoosh G. Boroojeni**

Kianoosh Gholami Boroojeni is a Ph.D. candidate of computer science at FIU. He received his B.Sc. in computer science in the University of Tehran, Iran (2012). His research interests include smart grids and algorithms.

During Kianoosh's graduate years, he has authored a book at MIT Press, a book at Springer Publishers, and several journal and conference papers. Currently, Kianoosh is collaborating with Dr. S.S. Iyengar on some cybersecurity issues in the context of smart grids and cloud computing.

## **M. Hadi Amini**

Mohammad Hadi Amini received the B.Sc. degree from Sharif University of Technology, Tehran, Iran, in 2011, and the M.Sc. degree from Tarbiat Modares University, Tehran, in 2013, both in electrical engineering. He also received the M.Sc. degree in electrical and computer engineering from Carnegie Mellon University in 2015. He is currently pursuing the dual-degree Ph.D. in electrical and computer engineering with the Department of Electrical and Computer Engineering, Carnegie Mellon University (CMU), Pittsburgh, PA, USA, and Sun Yat-sen University-CMU Joint Institute of Engineering, Guangzhou, China. He is also with the School of Electronics and Information Technology, SYSU, Guangzhou, China, and SYSU-CMU Shunde International Joint Research Institute, Shunde, Guangdong, China. Hadi serves as reviewer for several high-impact journals and international conferences and symposiums in the field of smart grid. He has published more than 30 refereed journals and conference papers in the smart grid-related areas and served as a session chair in INFORMS Annual Meeting 2015. He has been awarded the 5-year scholarship from the SYSU-CMU Joint Institute of Engineering in 2014, sustainable mobility summer fellowship from Massachusetts Institute

of Technology (MIT) Office of Sustainability in 2015, and the dean's honorary award from the president of Sharif University of Technology in 2007. His current research interests include smart grid, electric vehicles, optimization methods in interdependent power and transportation networks, and distributed optimization.

## **S.S. Iyengar**

S.S. Iyengar is a leading researcher in the fields of distributed sensor networks, computational robotics, and oceanographic applications and is perhaps best known for introducing novel data structures and algorithmic techniques for large-scale computations in sensor technologies and image processing applications. He has published more than 500 research papers and has authored or coauthored 12 textbooks and edited 10 others. Iyengar is a member of the European Academy of Sciences, a fellow of the Institute of Electrical and Electronics Engineers (IEEE), a fellow of National Academy of Inventors (NAI), a fellow of the Association for Computing Machinery (ACM), a fellow of the American Association for the Advancement of Science (AAAS), and fellow of the Society for Design and Process Science (SDPS). He has received the Distinguished Alumnus Award of the Indian Institute of Science. In 1998, he was awarded the IEEE Computer Society's Technical Achievement Award and is an IEEE Golden Core Member. Professor Iyengar is an IEEE Distinguished Visitor, SIAM Distinguished Lecturer, and ACM National Lecturer. In 2006, his paper entitled "A Fast Parallel Thinning Algorithm for the Binary Image Skeletonization", was the most frequently read article in the month of January in the *International Journal of High Performance Computing Applications*. His innovative work called the Brooks-Iyengar algorithm along with Prof. Richard Brooks from Clemson University is applied in industries and some real-world applications.