

Smart Grid Communications and Networking

The smart grid will transform the way power is delivered, consumed and accounted for. Adding intelligence through the newly networked grid will increase reliability and power quality, improve responsiveness, increase efficiency and provide a platform for new applications. This one-stop reference covers the state-of-the-art theory, key strategies, protocols, applications, deployment aspects and experimental studies of communication and networking technologies for the smart grid. Throughout the book's 20 chapters, a team of expert authors cover topics ranging from architectures and models through to integration of plug-in hybrid vehicles and security. Essential information is provided for researchers to make progress in the field and to allow power systems engineers to optimize communication systems for the smart grid.

Ekram Hossain is a Professor in the Department of Electrical and Computer Engineering at the University of Manitoba, Canada, where his current research interests lie in the design, analysis and optimization of wireless/mobile communications networks, smart grid communications, and cognitive and green radio systems. He has received several awards including the University of Manitoba Merit Award in 2010 (for Research and Scholarly Activities) and the 2011 IEEE Communications Society Fred W. Ellersick Prize Paper Award.

Zhu Han is an Assistant Professor in the Electrical and Computer Engineering Department at the University of Houston, Texas. He received his Ph.D. in electrical engineering from the University of Maryland, College Park, in 2003 and worked for 2 years in industry as an R&D Engineer for JDSU. He is a recipient of the NSF CAREER Award (2010) and the IEEE Communications Society Fred W. Ellersick Prize Paper Award.

H. Vincent Poor is the Michael Henry Strater University Professor at Princeton University, New Jersey, where he is also Dean of the School of Engineering and Applied Science. He is a Fellow of the IEEE, and is a member of the US National Academy of Engineering and of the US National Academy of Sciences. He is also a Fellow of the American Academy of Arts and Sciences, an International Fellow of the Royal Academy of Engineering, and a former Guggenheim Fellow. Recent recognition of his work includes the 2009 Edwin Howard Armstrong Award of the IEEE Communications Society, the 2010 IET Ambrose Fleming Medal, the 2011 IEEE Eric E. Sumner Award, and an honorary doctorate from the University of Edinburgh.

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

“... an invaluable resource to engineers involved in the design of smart grid... this book will become an essential reference in the literature of smart grids and smart infrastructures.”

Alberto Leon-Garcia, Univeristy of Toronto

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

Smart Grid Communications and Networking

EKRAM HOSSAIN

University of Manitoba, Canada

ZHU HAN

University of Houston, Texas

H. VINCENT POOR

Princeton University, New Jersey



CAMBRIDGE
UNIVERSITY PRESS

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9781107014138

© Cambridge University Press 2012

This publication is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without the written
permission of Cambridge University Press.

First published 2012

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Smart grid communications and networking / [edited by] Ekram Hossain, Zhu Han, H. Vincent Poor.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-107-01413-8 (hardback)

1. Smart power grids. I. Hossain, Ekram, 1971– II. Han, Zhu, 1974– III. Poor, H. Vincent.

TK3105.S488 2012

621.310285'46–dc23 2012008157

ISBN 978-1-107-01413-8 Hardback

Cambridge University Press has no responsibility for the persistence or
accuracy of URLs for external or third-party internet websites referred to in
this publication, and does not guarantee that any content on such websites is,
or will remain, accurate or appropriate.

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

**For
our families**

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

Contents

<i>List of contributors</i>	<i>page</i> xvii
<i>Preface</i>	xxi
Part I Communication architectures and models for smart grid	1
1 Communication networks in smart grid: an architectural view	3
1.1 Introduction	3
1.2 Smart grid conceptual model	5
1.3 Smart grid communication infrastructures	6
1.3.1 Home-area networks (HANs)	8
1.3.2 Neighbourhood-area networks (NANs)	8
1.3.3 Wide-area networks (WANs)	8
1.3.4 Enterprise	9
1.3.5 External	9
1.4 Interoperability issues	9
1.5 Role of communication infrastructures in smart grid	12
1.5.1 Customer premises	12
1.5.2 Core communication network	15
1.5.3 Last-mile connection	18
1.5.4 Control centre	20
1.5.5 Sensor and actuator networks (SANETs)	21
1.6 Security and privacy in the communications infrastructure for smart grid	23
1.6.1 Component-wise security	23
1.6.2 Protocol security	24
1.6.3 Network-wise security	25
1.7 Open issues and future research directions	26
1.7.1 Cost-aware communication and networking infrastructure	26
1.7.2 Quality-of-service (QoS) framework	26
1.7.3 Optimal network design	27
1.8 Conclusion	27

2	New models for networked control in smart grid	34
2.1	Introduction	34
2.2	Information in today's power system management operations	35
2.2.1	The management operations in today's power systems	35
2.2.2	Supervisory control and data acquisition (SCADA)	37
2.2.3	Basic models for power system controls	38
2.2.4	Existing power grid controls	41
2.2.5	The intrinsic difficulties of networked control	42
2.3	Enhanced smart grid measuring functionalities	43
2.3.1	State estimation	44
2.3.2	Wide-area measurement system (WAMS) and GridStat	46
2.4	Demand-side management and demand response: the key to distribute cheap and green electrons	50
2.4.1	The central electricity market	51
2.4.2	Real-time pricing	55
2.4.3	Direct load control	59
2.4.4	Possibilities and challenges at the edge of the network	60
2.5	Conclusion	61
3	Demand-side management for smart grid: opportunities and challenges	69
3.1	Introduction	69
3.2	System model	70
3.3	Energy-consumption scheduling model	71
3.3.1	Residential load-scheduling model	71
3.3.2	Energy-consumption scheduling problem formulation	72
3.3.3	Energy-consumption scheduling algorithm	75
3.3.4	Performance evaluation	76
3.4	Energy-consumption control model using utility functions	77
3.4.1	User preference and utility function	77
3.4.2	Energy consumption-control problem formulation	79
3.4.3	Equilibrium among users	81
3.4.4	The Vickrey–Clarke–Groves (VCG) approach	84
3.4.5	Performance evaluation of power-level selection algorithms	86
3.5	Conclusion	88
4	Vehicle-to-grid systems: ancillary services and communications	91
4.1	Introduction	91
4.2	Ancillary services in V2G systems	92
4.3	V2G system architectures	95
4.3.1	Aggregation scenarios	97
4.3.2	Charging scenarios	98
4.4	V2G systems communications	99

4.4.1	Power-line communications and HomePlug	99
4.4.2	Wireless personal-area networking and ZigBee	99
4.4.3	Z-Wave	100
4.4.4	Cellular networks	100
4.4.5	Interference management and cognitive radio	101
4.5	Challenges and open research problems	101
4.5.1	Fulfilling communications needs	101
4.5.2	Coordinating charging and discharging	103
4.6	Conclusion	103
Part II Physical data communications, access, detection, and estimation techniques for smart grid		109
5	Communications and access technologies for smart grid	111
5.1	Introduction	111
5.1.1	Legacy grid communications	112
5.1.2	Smart grid objectives	112
5.1.3	Data classification	116
5.2	Communications media	117
5.2.1	Wired solutions	118
5.2.2	Wireless solutions	121
5.3	Power-line communication standards	125
5.3.1	Broadband power-line communications	126
5.3.2	Narrowband power-line communications	128
5.3.3	PLC coexistence	130
5.4	Wireless standards	131
5.4.1	Short-range solutions	131
5.4.2	Long-range solutions	133
5.5	Networking solutions	136
5.5.1	Hybrid solutions	136
5.5.2	Public vs. private networks	137
5.5.3	Internet and IP-based networking	137
5.5.4	Wireless sensor networks	139
5.5.5	Machine-to-machine communications	140
5.6	Conclusion	142
6	Machine-to-machine communications in smart grid	147
6.1	Introduction	147
6.2	M2M communications technologies	150
6.2.1	Wired vs. wireless	150
6.2.2	Capillary M2M	152
6.2.3	Cellular M2M	154
6.3	M2M applications	156

6.4	M2M architectural standards bodies	157
6.4.1	ETSI M2M	158
6.4.2	3GPP MTC	160
6.5	M2M application in smart grid	163
6.5.1	M2M architecture	163
6.5.2	Transmission and distribution networks	165
6.5.3	End-user appliances	168
6.6	Conclusion	171
7	Bad-data detection in smart grid: a distributed approach	175
7.1	Introduction	175
7.2	Distributed state estimation and bad-data processing: state-of-the-art	176
7.2.1	Wide-area state-estimation model	176
7.2.2	Bad-data processing in state estimation	177
7.2.3	Related work	178
7.3	Fully distributed bad-data detection	180
7.3.1	Preliminaries	180
7.3.2	Proposed algorithm for distributed bad-data detection	181
7.4	Case study	183
7.4.1	Case 1	184
7.4.2	Case 2	187
7.5	Conclusion	189
8	Distributed state estimation: a learning-based framework	191
8.1	Introduction	191
8.2	Background	192
8.3	State estimation model	193
8.4	Learning-based state estimation	195
8.4.1	Geographical diversity	195
8.4.2	Side information	195
8.4.3	Weighted average estimation	195
8.4.4	Estimation performance	198
8.5	Conclusion	198
	Part III Smart grid and wide-area networks	203
9	Networking technologies for wide-area measurement applications	205
9.1	Introduction	205
9.2	Components of a wide-area measurement system	206
9.2.1	PMU and PDC	206
9.2.2	Hardware architecture	207

		9.2.3 Software infrastructure	209
	9.3	Communication networks for WAMS	210
		9.3.1 Communication needs	211
		9.3.2 Transmission medium	212
		9.3.3 Communication protocols	213
	9.4	WAMS applications	214
		9.4.1 Power-system monitoring	214
		9.4.2 Power-system protection	217
		9.4.3 Power-system control	221
	9.5	WAMS modelling and network simulations	223
		9.5.1 Software introduction	223
		9.5.2 System infrastructure modelling	223
		9.5.3 Application classification	226
		9.5.4 Monitoring simulation	226
		9.5.5 Protection simulation	228
		9.5.6 Control simulation	229
		9.5.7 Hybrid simulation	230
	9.6	Conclusion	231
10		Wireless networks for smart grid applications	234
	10.1	Introduction	234
	10.2	Smart grid application requirements	234
		10.2.1 Application types	235
		10.2.2 Quality-of-service (QoS) requirements	235
		10.2.3 Classifying applications by QoS requirements	236
		10.2.4 Traffic requirements	240
	10.3	Network topologies	243
		10.3.1 Communication actors	244
		10.3.2 Connectivity	245
	10.4	Deployment factors	248
		10.4.1 Spectrum	248
		10.4.2 Path-loss	248
		10.4.3 Coverage	249
		10.4.4 Capacity	251
		10.4.5 Resilience	252
		10.4.6 Security	253
		10.4.7 Resource sharing	253
	10.5	Performance metrics and tradeoffs	253
		10.5.1 Coverage area	254
		10.5.2 Capacity	256
		10.5.3 Reliability	258
		10.5.4 Latency	260
	10.6	Conclusion	261

Part IV	Sensor and actuator networks for smart grid	263
11	Wireless sensor networks for smart grid: research challenges and potential applications	265
11.1	Introduction	265
11.2	WSN-based smart grid applications	266
11.2.1	Consumer side	267
11.2.2	Transmission and distribution side	268
11.2.3	Generation side	271
11.3	Research challenges for WSN-based smart grid applications	272
11.4	Conclusion	274
12	Sensor techniques and network protocols for smart grid	279
12.1	Introduction	279
12.2	Sensors and sensing principles	280
12.2.1	Metering and power-quality sensors	281
12.2.2	Power system status and health monitoring sensors	284
12.3	Communication protocols for smart grid	285
12.3.1	MAC protocols	287
12.3.2	Routing protocols	290
12.3.3	Transport protocols	295
12.4	Challenges for WSN protocol design in smart grid	297
12.5	Conclusion	299
13	Potential methods for sensor and actuator networks for smart grid	303
13.1	Introduction	303
13.2	Energy and information flow in smart grid	305
13.3	SANET in smart grid	306
13.3.1	Applications of SANET in SG	307
13.3.2	Actors of SANET in smart grid	310
13.3.3	Challenges for SANET in smart grid	313
13.4	Proposed mechanisms	314
13.4.1	Pervasive service-oriented network (PERSON)	314
13.4.2	Context-aware intelligent control	316
13.4.3	Compressive sensing (CS)	316
13.4.4	Device technologies	317
13.5	Home energy-management system – case study of SANET in SG	318
13.5.1	Energy-management system	318
13.5.2	EMS design and implementation	320
13.6	Conclusion	321

14	Implementation and performance evaluation of wireless sensor networks for smart grid	324
14.1	Introduction	324
14.2	Constrained protocol stack for smart grid	325
14.2.1	IEEE 802.15.4	326
14.2.2	IPv6 over low-power WPANs	327
14.2.3	Routing protocol for low-power and lossy networks	328
14.2.4	Constrained application protocol	331
14.2.5	W3C efficient XML interchange	332
14.3	Implementation	332
14.3.1	802.15.4	333
14.3.2	6LoWPAN	333
14.3.3	RPL	335
14.3.4	CoAP	336
14.3.5	EXI	339
14.4	Performance evaluation	339
14.4.1	Link performance using IEEE 802.15.4	340
14.4.2	Network throughput with 6LoWPAN	341
14.4.3	Network throughput with RPL in multihop scenarios	343
14.4.4	CoAP performance	345
14.4.5	CoAP multihop performance	347
14.5	Conclusion	348
Part V Security in smart grid communications and networking		351
15	Cyber-attack impact analysis of smart grid	353
15.1	Introduction	353
15.2	Background	354
15.2.1	Risk management	354
15.2.2	Prior art	356
15.3	Cyber-attack impact analysis framework	356
15.3.1	Graphs and dynamical systems	357
15.3.2	Graph-based dynamical systems model synthesis	358
15.4	Case study	359
15.4.1	13-node distribution test system	359
15.4.2	Model synthesis	362
15.4.3	Attack scenario 1	363
15.4.4	Attack scenario 2	365
15.4.5	Attack scenario 3	367
15.5	Conclusion	368

16	Jamming for manipulating the power market in smart grid	373
16.1	Introduction	373
16.2	Model of power market	375
16.3	Attack scheme	376
16.3.1	Attack mechanism	376
16.3.2	Analysis of the damage	379
16.4	Defence countermeasures	383
16.5	Conclusion	384
17	Power-system state-estimation security: attacks and protection schemes	388
17.1	Introduction	388
17.2	Power-system state estimation and stealth attacks	389
17.2.1	Power network and measurement models	389
17.2.2	State estimation and bad-data detection	391
17.2.3	BDD and stealth attacks	392
17.3	Stealth attacks over a point-to-point SCADA network	393
17.3.1	Minimum-cost stealth attacks: problem formulation	394
17.3.2	Exact computation of minimum-cost stealth attacks	395
17.3.3	Upper bound on the minimum cost	396
17.3.4	Numerical results	398
17.4	Protection against attacks in a point-to-point SCADA network	400
17.4.1	Perfect protection	400
17.4.2	Non-perfect protection	401
17.4.3	Numerical results	401
17.5	Stealth attacks over a routed SCADA network	403
17.5.1	Measurement attack cost	404
17.5.2	Substation attack impact	405
17.5.3	Numerical results	406
17.6	Protection against stealth attacks for a routed SCADA network	407
17.6.1	Single-path and multi-path routing	408
17.6.2	Data authentication and protection	410
17.7	Conclusion	410
18	A hierarchical security architecture for smart grid	413
18.1	Introduction	413
18.2	Hierarchical architecture	415
18.2.1	Physical layer	418
18.2.2	Control layer	418
18.2.3	Communication layer	419
18.2.4	Network layer	419
18.2.5	Supervisory layer	419
18.2.6	Management layer	420
18.3	Robust and resilient control	420

	18.4 Secure network routing	425
	18.4.1 Hierarchical routing	425
	18.4.2 Centralized vs. decentralized architectures	427
	18.5 Management of information security	429
	18.5.1 Vulnerability management	429
	18.5.2 User patching	430
	18.6 Conclusion	434
19	Application-driven design for a secured smart grid	439
	19.1 Introduction	439
	19.2 Intrusion detection for advanced metering infrastructures	441
	19.2.1 Smart meters and security issues	442
	19.2.2 Architecture for situational awareness and monitoring solution	443
	19.2.3 Enforcing security policies with specification-based IDS	445
	19.3 Converged networks for SCADA systems	448
	19.3.1 Requirements and challenges for convergence	449
	19.3.2 Architecture with time-critical constraints	450
	19.4 Design principles for authentication	453
	19.4.1 Requirements and challenges in designing secure authentication protocols for smart grid	454
	19.4.2 Design principles for authentication protocols	454
	19.4.3 Use case: secure authentication supplement to DNP3	455
	19.5 Conclusion	458
	Part VI Field trials and deployments	463
20	Case studies and lessons learned from recent smart grid field trials	465
	20.1 Introduction	465
	20.2 Smart power grids	465
	20.2.1 The Jeju smart grid testbed	465
	20.2.2 ADS program for Hydro One	467
	20.2.3 The SmartHouse project	469
	20.3 Smart electricity systems	470
	20.4 Smart consumers	471
	20.4.1 PEPCO	472
	20.4.2 Commonwealth Edison	473
	20.4.3 Connecticut light and power	474
	20.4.4 California statewide pricing pilot	474
	20.5 Lessons learned	475
	20.6 Conclusion	476
	<i>Index</i>	478

Cambridge University Press
978-1-107-01413-8 - Smart Grid Communications and Networking
Ekram Hossain, Zhu Han and H. Vincent Poor
Frontmatter
[More information](#)

Contributors

Mahnoosh Alizadeh

University of California Davis, USA

Jesus Alonso-Zarate

CTTC, Barcelona, Spain

Tamer Başar

University of Illinois at Urbana-Champaign, USA

Sara Bavarian

The University of British Columbia, Canada

Robin Berthier

University of Illinois at Urbana-Champaign, USA

Rakesh B. Bobba

University of Illinois at Urbana-Champaign, USA

Nicola Bui

University of Padova, Italy

Karen Butler-Purry

Texas A&M University, USA

Paolo Casari

University of Padova, Italy

Angelo P. Castellani

University of Padova, Italy

Dae-Hyun Choi

Texas A&M University, USA

György Dán

KTH Royal Institute of Technology, Sweden

Yi Deng

Virginia Polytechnic Institute and State University, USA

Mischa Dohler

CTTC, Barcelona, Spain

Nada Golmie

NIST, USA

David Gregoratti

CTTC, Barcelona, Spain

David Griffith

NIST, USA

Vehbi Cagri Gungor

Bahcesehir University, Turkey

Gerhard P. Hancke Jr

Royal Holloway University of London, UK

Gerhard P. Hancke

University of Pretoria, South Africa

Erich Heine

University of Illinois at Urbana-Champaign, USA

Ekram Hossain

University of Manitoba, Canada

Rose Qingyang Hu

Utah State University, USA

Cunqing Hua

Zhejiang University, P. R. China

Jianwei Huang

The Chinese University of Hong Kong, Hong Kong, China

Soumya Kar

Carnegie Mellon University, USA

Nipendra Kayastha

Nanyang Technological University, Singapore

Himanshu Khurana

Honeywell Research Labs, USA

Deepa Kundur

Texas A&M University, USA

Lutz Lampe

The University of British Columbia, Canada

Husheng Li

University of Tennessee, USA

Victor O. K. Li

University of Hong Kong, Hong Kong, China

Hua Lin

Virginia Polytechnic Institute and State University, USA

Salman Mashayekh

Texas A&M University, USA

Javier Matamoros

CTTC, Barcelona, Spain

Amir-Hamed Mohsenian-Rad

Texas Tech University, USA

Dusit Niyato

Nanyang Technological University, Singapore

Arun G. Phadke

Virginia Polytechnic Institute and State University, USA

H. Vincent Poor

Princeton University, USA

Michele Rossi

University of Padova, Italy

Dilan Sahin

Bahcesehir University, Turkey

Pedram Samadi

The University of British Columbia, Canada

Henrik Sandberg

KTH Royal Institute of Technology, Sweden

William H. Sanders

University of Illinois at Urbana-Champaign, USA

Anna Scaglione

University of California Davis, USA

Robert Schober

The University of British Columbia, Canada

Sandeep Shukla

Virginia Polytechnic Institute and State University, USA

Kin Cheong Sou

KTH Royal Institute of Technology, Sweden

Michael Souryal

NIST, USA

Ali Tajer

Princeton University, USA

James S. Thorp

Virginia Polytechnic Institute and State University, USA

Yi Qian

University of Nebraska-Lincoln, USA

Lorenzo Vangelista

University of Padova, Italy

Ping Wang

Nanyang Technological University, Singapore

Zhifang Wang

University of California Davis, USA

Vincent W. S. Wong

The University of British Columbia, Canada

Chenye Wu

Tsinghua University, China

Le Xie

Texas A&M University, USA

Guang-Hua Yang

University of Hong Kong, Hong Kong, China

Tim Yardley

University of Illinois at Urbana-Champaign, USA

Rong Zheng

The University of Houston, USA

Quanyan Zhu

University of Illinois at Urbana-Champaign, USA

Michele Zorzi

University of Padova, Italy

Takis Zourntos

Texas A&M University, USA

Preface

A brief journey through 'Smart Grid Communications and Networking'

A power grid consists of two major parts: the transmission and distribution systems. The transmission system refers to the high-voltage network infrastructure that connects the power generation facilities with the various distribution points. At the distribution points, the electrical carrier is converted to medium and low-voltage signals for the distribution systems that connect the customers. The smart power grid (or *smart grid* in short) refers to the next-generation electrical power grid that aims to provide reliable, efficient, secure, and quality energy generation/distribution/consumption using modern information, communications, and electronics technology. The smart grid will introduce a distributed and user-centric system that will incorporate end-consumers into its decision processes to provide a cost-effective and reliable energy supply. The modern communication infrastructure will play a vital role in managing, controlling, and optimizing different devices and systems in smart grids. Information and communication technologies are at the core of the smart grid vision as they will provide the power grid with the capability to support two-way energy and information flow, isolate and restore power outages more quickly, facilitate the integration of renewable energy sources into the grid and empower the consumer with tools for optimizing their energy consumption.

From an architectural perspective, a smart grid is comprised of three high-level layers: the physical power layer (transmission and distribution), the data transport and control layer (communication and control), and the application layer (applications and services). Each of these high-level layers breaks down further into sub-layers and more detailed market segments. Unlike its predecessor (i.e., the existing electrical power grid), smart grid will use two-way data communication technologies to integrate the utility control system with end-users and consumers, so that intelligent power generation, control, and consumption can be achieved. Moreover, smart grid will allow active participation of users by providing user information related to demand and fault reporting. Many standard bodies and organizations throughout the world are working towards this vision of smart grid. Among many, the Electrical Power Research Institute (EPRI), the National Institute of Standards and Technology (NIST), and European Commission Research (ECR) are working towards developing the most comprehensive frameworks, communication specifications, standards, and roadmaps for the smart grid. However, many issues such as cost, interoperability, cyber and physical security, lack of communication and architectural standards, etc., need to be addressed. Developing the smart grid has become an urgent

global priority as its economic, environmental, and societal benefits will be enjoyed by future generations.

The objective of this book is to provide a useful background on advanced data communication and networking mechanisms, models for networked control, and security mechanisms for the smart grid. This book consists of chapters covering different aspects of data communications and networking in the smart grid that include the following: communications architectures and models for smart grid for advanced metering infrastructure (AMI), networked control, demand-side management (DSM), distributed energy resource (DER) management; physical communications, detection, estimation, and access design for smart grid; smart grid and area networks such as home-area networks (HANs), neighbourhood-area networks (NANs), wide-area networks (WANs), wide-area measurement systems (WAMSs); sensor and actuator networks (SANETs) for the smart grid and the related protocol design issues; security in communications infrastructure for the smart grid; and the ongoing projects and field-trials on the smart grid.

This book contains 20 chapters which are organized into six parts. A brief account of each chapter in each of these parts is given next.

Part I: Communication architectures and models for smart grid

A smart grid is a visionary user-centric system that will elevate the conventional power grid system to one that functions more cooperatively, responsively, and economically. In addition to the incumbent function of delivering electricity from suppliers to consumers, smart grids will also provide information and intelligence to the power grid to enable grid automation, active operation, and efficient demand response. A reliable and efficient communication and networking infrastructure will connect the functional elements within the smart grid.

In *Chapter 1*, Kayastha *et al.* describe the conceptual model for a smart grid adopted by NIST, and describe the interactions among its different domains (e.g., generation, transmission, distribution, customer, service provider, operations, market). In this context, the authors highlight the role and importance of smart grid communications and networking infrastructures, and present an overview of a hierarchical communication infrastructure which spans across the different domains in a smart grid. Such an infrastructure, which is also termed an AMI, comprises many systems and subsystems such as HANs, SANETs, NANs, and WANs. The authors also briefly describe the GridWise Architecture Council (GWAC) framework for interoperability in the integrated smart grid communications infrastructure. In addition, security and privacy issues related to the communications infrastructures in the smart grid are also reviewed.

In *Chapter 2*, Scaglione, Wang, and Alizadeh provide a brief overview of the classical issues of network control and how they relate to the challenges of creating a new architectural model for managing energy distribution in a smart grid that relies on real-time, dependable information gathering and decisions. The authors discuss the important questions that exist in tightening the networked control at the core of the network and at its edges and why these are important parts to unleash innovations in the smart grid.

They discuss how wide-area measurement systems connecting phasor measurement units (PMUs) through novel sensor networking paradigms can help increase the situation awareness in the smart grid. The authors also review the supervisory control and data acquisition (SCADA) model which is currently used for grid monitoring and control. At the edge, the emerging smart metering infrastructure today offers only a glimpse of the possible advantages of having broad consumer participation. The opportunity is to tighten the control of the demand via real-time load scheduling. The authors discuss what are reasonable models for demand and response systems, also referred to as DSM systems, that proactively control smart loads, focusing on the specific example of an electric vehicle, as a compelling case to target for the study of load scheduling.

In *Chapter 3*, Samadi *et al.* present a number of methods for DSM based on smart pricing to improve the efficiency of traditional power grids. Two different objectives for such algorithms are: reducing power consumption and shifting (or scheduling) power consumption. Energy-consumption scheduling can reduce the peak-to-average ratio (PAR) of power consumption as well as minimize the total energy cost in the system. For users, another objective could be to minimize jointly the energy cost and waiting time. The authors consider these design objectives for DSM and present optimization and game-theoretic models to solve the DSM problem. The concept of utility functions is used to model different objectives of users.

In *Chapter 4*, Wu, Mohsenian-Rad, and Huang provide an introduction to vehicle-to-grid (V2G) systems and highlight the role of a reliable and secure communication and networking infrastructure for such systems in the future smart grid. A V2G system can inject power into the grid when required through discharging the batteries of plug-in electric vehicles (PHEVs). Such a system can improve the PAR in the system through a coordinated charging and discharging mechanism for the PHEVs. Also, the V2G power storage mechanism can facilitate integration of renewable energy (RE) sources into the smart grid. In addition, a V2G system can help to regulate frequency and voltage in a power grid. All of these services, which are referred to as ancillary services, can be offered to the power grid efficiently through an advanced communication and networking infrastructure. The authors briefly describe several technologies for V2G system communications which include broadband power-line communication (PLC), ZigBee, Z-Wave, cognitive radio, and cellular wireless technologies. The details of these technologies are discussed in Part II of the book.

Part II: Physical data communications, access, detection, and estimation techniques for smart grid

Different physical data communication technologies for the smart grid will empower the legacy power grid with the capability to support two-way energy and information flow. These technologies will facilitate integration of renewable energy sources into the grid, and empower the consumers with tools to optimize energy consumption. The smart grid will rely on several existing and future wired and wireless communications

technologies (e.g., PLC, cellular network, IP networks, ZigBee, Wi-Fi, WiMAX, etc.). Also, advanced techniques for power-system state estimation and data processing (e.g., bad-data detection) will be required for smart grids.

In *Chapter 5*, Bavarian and Lampe provide an exposition on the different communications and access technologies and their applications in smart grid communications. Different wired communications technologies including power-line and optical-fibre technologies, and wireless technologies including cellular, satellite, wireless mesh, and wireless personal-area networking technologies are reviewed. Broadband and narrow-band power-line communications technologies and the related standards (e.g., IEEE 1901, ITU-T G.9960/61, HomePlug) are discussed. Among the wireless technologies, the authors discuss the ZigBee, Wi-Fi, WiMAX, 3GPP LTE, and IEEE 802.22 standards. To this end, the authors also review networking solutions such as Internet and IP-based networks, private networks, wireless sensor and machine-to-machine (M2M) communication networks for smart grids.

In *Chapter 6*, Alonso-Zarate *et al.* review the emerging paradigm of M2M communications, including its definition, historical developments, design drivers, and the status-quo of its standardization efforts. The authors discuss in detail the applicability of the M2M communications to the smart grid and identify open challenges for a symbiotic development of both M2M and smart grid technologies. Different M2M communications technologies including cabled technologies (e.g., PLC, Ethernet), low-power wireless technologies such as ZigBee, Wi-Fi, 6LoWPAN (which are referred to as capillary M2M technologies), and hybrid M2M technologies are discussed. The authors argue that the cellular M2M communications technologies are suitable for smart grid applications such as wide-area situational awareness, interconnection of distributed energy resources, and distribution automation in the transmission and distribution networks. Also, cellular M2M is a technology enabler to build the AMI, and to realize the concept of direct load control (DLC) where intelligent devices can automatically schedule their power loads.

In *Chapter 7*, Xie *et al.* focus on the problem of fast and robust state-estimation techniques for wide-area monitoring, control, and protection in the smart grid. One essential functionality in state estimation is to detect, identify, and eliminate measurement errors, which arise due to the existence of large measurement bias, drifts, or wrong connections. This functionality is referred to as ‘bad-data processing’, which consists of two steps: bad-data detection and identification. Generally, a chi-square test is used for bad-data detection, and then a normalized residual test is used for bad-data identification. The authors review the state-of-the-art of bad-data processing techniques and present a distributed approach for bad-data detection. The performance of the proposed approach is observed by simulations using the IEEE 14-bus system. The information exchange and communication requirements for the proposed approach are also discussed.

In *Chapter 8*, Tajer, Kar, and Poor also deal with the problem of distributed power-system state estimation taking into account the uncertainties in the underlying physical and sensing models as well as the rapidly varying dynamics of the system. The authors define a learning-based framework for adaptive and distributed power-state estimation. They model the smart grid as a collection of multiple overlapping distributed subnetworks (or clusters) covering the entire network. The subnetworks share their estimates of

network state with a central decision-maker entity (central estimator) through a backbone communication network. Then the central estimator combines the local state estimates to obtain the global state of the network. The estimation performance at the central estimator, as well as the estimation quality in each cluster, are modelled analytically using cost functions.

Part III: Smart grid and wide-area networks

Advanced data communication and networking techniques will play a key role in the successful development of the emerging smart grid system. The communication network in the smart grid must be able to support all aspects of generation, transmission, distribution, as well as the requirements of users and utility service providers. The data communication network in the smart grid will be responsible for sensing (i.e., gathering real-time measurements from various locations of the power grid through a WAMS), communication (i.e., bidirectional data exchange between smart meters and control centres), and control (i.e., delivery of control messages to ensure optimal, reliable, and resilient operation of the grid and its subsystems).

In *Chapter 9*, Deng *et al.* focus on the performance evaluation of network architectures and protocols for WAMS applications in the smart grid. The authors review the WAMS architecture (software and hardware) and the different components of WAMS, namely, the PMUs, regional phasor data concentrators (PDCs), centralized super-phasor data concentrator (SPDC), and hierarchically organized communication networks. A WAMS uses a multi-level hierarchical communication network with reliability, real-time responsiveness, scalability, and reliability, to integrate all these components together. The applications of WAMS for power-system monitoring, protection, and control are discussed in detail. A simulation platform based on the OPNET Modeler is designed for a realistic communication system of WAMS and simulation results are obtained for various control, monitoring, and hybrid WAMS applications.

In *Chapter 10*, Griffith, Souryal, and Golmie focus on the use of wireless networks to support the communications quality-of-service (QoS) and traffic requirements of different smart grid applications. These applications include firmware/program update (FPU), field distribution automation maintenance-centralized control (FDAMC) for communications between the distribution management system and various field devices, PHEV messaging, customer information/messaging (CMMSG), and meter reading. The QoS requirements (e.g., latency and reliability) and the traffic characteristics of these applications, and also the message flows among the various actors for these applications and the resulting network topologies are discussed. The key factors such as the choice of radio spectrum, wireless channel propagation characteristics, wireless link coverage, and network capacity, resilience and security, which need to be considered for the deployment of wireless networks, are described. In this context, performance metrics such as coverage, capacity, reliability, and latency, which can be used to evaluate different wireless network alternatives, are also discussed.

Part IV: Sensor and actuator networks for smart grid

In a smart grid, wireless SANETs will be deployed in generation systems, transmission and distribution systems, and consumers' premises to monitor and control the functioning of the grid. The existing and potential applications of SANETs in the smart grid include advanced metering, fault diagnosis, demand response and dynamic pricing, energy management, etc. SANETs will be an integral component in future generation smart grids. However, the existing communication protocols for SANETs may need to be modified/optimized taking into consideration the smart grid application requirements.

In *Chapter 11*, Sahin *et al.* present the potential applications of wireless sensor networks (WSNs) in the smart grid and the related technical challenges. In particular, WSN-based applications have been described for power generation systems, transmission and distribution networks, and consumer facilities. For WSN-based smart grid applications, a number of research challenges exist which involve power, data, and resource management in sensors, interoperability among WSN protocols, QoS provisioning in the network, and system integration.

In *Chapter 12*, Zheng and Hua focus on the sensor technologies and communication protocols for sensor networks in the smart grid. The authors review major types of sensors which are categorized into metering and power-quality sensors and power-system status and health-monitoring sensors. In this context, different sensing principles, which are used to convert the physical parameters into electronic signals, are reviewed. The authors discuss the issues related to designing medium access control (MAC), routing, and transport protocols for WSNs in the smart grid. A brief survey on the existing protocols for general WSNs, along with a qualitative comparison among the different protocols, are also provided. The authors point out that designing sensor networking protocols for the smart grid is challenging due to the unique features of such systems; for example, the complex and heterogeneous nature of the environment, dynamic nature of the system, reliability, availability, and diverse QoS requirements, energy and cost-efficiency, and scalability and security issues.

In *Chapter 13*, Li and Yang focus on addressing the major design challenges of SANETs in smart grids as mentioned before. The authors propose mechanisms such as pervasive service-oriented networking, context-aware intelligent control, compressive sensing, and advanced device technologies (e.g., with low-power, modular, and compact design and power-harvesting mechanisms) to address the challenges. To this end, the effectiveness of the proposed mechanisms is demonstrated with a case study of a home energy-management system (HEMS).

In *Chapter 14*, Bui *et al.* focus on the implementation and performance evaluation of WSN protocols for smart grid applications in a test-bed built from off-the-shelf wireless sensors. In particular, the authors consider the protocol stack of the 'Internet of things' with IEEE 802.15.4 protocols at the physical (PHY) and MAC layers, 6LoWPAN (IPv6 over low-power wireless personal-area networks) at the routing layer, and CoAP (Constrained Application Protocol) at the application/session layer. The implementation of the test-bed is discussed along with the different optimization techniques used for the network and software implementations. The experimental results for the different layers

of the protocol stack are presented. The authors conclude that WSN solutions based on the ‘Internet of things’ protocol stack are feasible to be integrated with the smart grid.

Part V: Security in smart grid communications and networking

Although the communication infrastructure can considerably improve the efficiency of the power system, it brings significant vulnerability since malicious users can attack the communication system and thus cause various damages to the smart grid, or even result in a large-area blackout. Hence, security is of high priority in the study of smart grids and has attracted substantial attention in industry and academia. We have five chapters which discuss the security issues in the smart grid from different perspectives.

In *Chapter 15*, Kundur *et al.* present a framework for cyber-attack impact analysis in the smart grid. First, background is provided to motivate and introduce fundamental research and development questions on cyber-attack impact analysis. Second, a graph-theoretic dynamical system approach is employed to model the interactions between the cyber and electricity networks in the model synthesis stage. Finally, a test case study is presented to demonstrate the potential for modelling.

In *Chapter 16*, Li proposes a jamming-based attack scheme for manipulating the power market in the smart grid. By intelligently blocking and releasing the information in the power market via jamming the wireless communications, malicious jammers/attackers can manipulate the power price, thus making profit for themselves and causing damage to the power grid. To combat this attack, random frequency hopping can be employed for communication, and a random backoff method is proposed for load adjustment in order to avoid the impulsive impact on the market price and power load due to jamming.

In *Chapter 17*, Dán, Sou, and Sandberg study bad-data injection attacks on state estimation in the smart grid using SCADA systems. State estimation is used to estimate the complete physical state of the power system, and bad-data detection is used to identify faulty equipment and corrupted measurement data. A stealth attack against bad-data detection is investigated, and several algorithms are used to protect the power system against this attack. A realistic model is added for communication of the supervisory control and data acquisition systems. Some new protection mechanisms are also presented.

In *Chapter 18*, Zhu and Başar describe a cross-layer architecture to address security issues in the smart grid. The tradeoff between information assurance and the physical layer system performance is investigated by three security issues at different layers: the resilient control design problem at the physical power plant, the data-routing problem at the network and communication layer, and the information security management at the application layers. The proposed hierarchical model extends the open system interconnection (OSI) and Purdue Reference models for their integration into smart grids.

In *Chapter 19*, Berthier *et al.* discuss an application-driven design approach that builds the large cyber security toolset. A key element is careful enumeration of the control-system-specific aspects of each system and an integrated study of these aspects, cyber security properties, and solutions. Specifically, the following topics are discussed

in detail: intrusion detection for advanced metering infrastructure, converged networks for supervisory control and data acquisition, and design principles for authentication of SCADA protocols.

Part VI: Field trials and deployments

The relevance of smart grid is reflected by the increasing number of national and international projects on this topic as well as new initiatives by standardization bodies and organizations such as NIST, EPRI, ECR, and the IEEE. There have been several smart grid field trials in the last few years.

In *Chapter 20*, Hu and Qian provide an overview of several smart grid field trials which are divided into three categories: smart power grids, smart electricity systems, and smart customers. The first category includes the Jeju smart grid testbed in Korea, the advanced distribution system (ADS) programme in Ontario, Canada, and the SmartHouse project in Europe. The second category includes an intelligent protection relay system for smart grids. The third category includes several dynamic pricing schemes. The authors summarize the lessons learned from these pilot projects.