

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

Contents

List of contributors
Preface

page xvii
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
--------------	-----