SpringerBriefs in Electrical and Computer Engineering

More information about this series at http://www.springer.com/series/10059

Asmaa Abdallah • Xuemin Shen

Security and Privacy in Smart Grid

Springer

Asmaa Abdallah
Faculty of Engineering
Port Said University
Port Fouad, Egypt

Xuemin Shen
Electrical and Computer
Engineering Department
University of Waterloo
Waterloo, ON, Canada

ISSN 2191-8112 ISSN 2191-8120 (electronic)
SpringerBriefs in Electrical and Computer Engineering
ISBN 978-3-319-93676-5 ISBN 978-3-319-93677-2 (eBook)
https://doi.org/10.1007/978-3-319-93677-2

Library of Congress Control Number: 2018946557

Printed on acid-free paper

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

To my mother, Samia, and my father, Refaat—A.A.

To my sons, Alan and Alvin—X.S.

Preface

Smart grid is a promising upgrade of the traditional power grid. It provides advanced cooperation among the involved parties in the grid, such as electricity consumers, utility companies, electric vehicles (EVs), and distributed generators (DGs). Although smart grid can improve the electricity generation and distribution, and customers' services by utilizing various types of wired/wireless communication networks to exchange information among different parties in the power grid, it will be vulnerable to cyber-attacks from communication networks. Therefore, security and privacy concerns are significant challenges in smart grid.

In this brief, we first present the smart grid technology and its main communication networks: the customer-side networks, which communicate electricity customers and utility companies via various networks, i.e., home area networks (HANs), neighbor area networks (NANs), and wide area networks (WANs). The second network is the communication between EVs and grid to charge/discharge the vehicles' batteries via vehicle-to-grid (V2G) connection. The last network is the grid's connection with measurements units that spread all over the grid to monitor its status and send periodic reports to the main control center (CC) for state estimation and bad data detection purposes. We then discuss the major security threats for smart grid and propose the corresponding security and privacy-preserving schemes. For customer-side networks, two lightweight lattice-based security and privacy-preserving schemes are introduced: the first scheme is based on forecasting the future electricity demands for a cluster of residential units, while the second solution utilizes homomorphic aggregation to aggregate household appliances' readings. For the V2G connection, a lightweight secure and privacy-preserving scheme is presented, in which the power grid guarantees its financial profits and at the same time prevents EVs from acting maliciously. Finally, a protection technique is presented to resist the severe false data injection (FDI) attacks, which insert fake grid status measurements among the correct readings to mislead the CC to make wrong decisions and consequently threaten the smart grid's efficiency and reliability.

Toronto, ON, Canada — Asmaa Abdallah
Waterloo, ON, Canada — Xuemin Shen
April 2018

Acknowledgements

The authors gratefully acknowledge the Egyptian Cultural Affairs and Missions Sector, Higher Education Ministry, Egypt, for funding this research work.

We would also like to thank all the colleagues in the Broadband Communications Research (BBCR) Lab at the University of Waterloo for the useful discussions and continuous exchange of knowledge.

Contents

Acronyms

ABE	Attribute-based Encryption Scheme
AP	Access Point
APs	Smart Household Appliances
BANs	Building Area Networks
BEVs	Battery Electric Vehicles
BSs	Base Stations
CA	Central Authority
CC	Control Center
CS	Cramer-Shoup Cryptosystem
CSs	Charging Stations
CUSUM	Cumulative Sum Control Chart Test
DGs	Distributed Generators
DoS	Denial-of-Service Attacks
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EPPDR	Efficient Privacy-Preserving Demand Response Scheme
EVs	Electric Vehicles
FDI	False Data Injection Attacks
GLRT	Generalized Likelihood Ratio Test
HANs	Home Area Networks
HMI	Human Machine Interface
IANs	Industrial Area Networks
IBC	Identity-based Cryptography Scheme
ICS	Industrial Control System
KP-ABE	Key-Policy Attribute-based Encryption
LAs	Local Aggregators
LMP	Locational Marginal Price
LR	Load Redistribution Attack
LRT	Likelihood Ratio Test
LS	Local Substation

LWE	Learning with Error Problem
MMSE	Minimum Mean Squared Error
MUs	Measurement Units
NANs	Neighborhood Area Networks
NSS	NTRU Signature Scheme
PHEVs	Plug-in Hybrid Vehicles
PIDs	Pseudonym IDs
PKI	Public Key Infrastructure
PLC	Power Line Carrier
PMUs	Phasor Measurement Units
QoS	Quality of Service
RTUs	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition Systems
SE	State Estimator
SMs	Smart Meters
SSS	Shamir Secret Sharing Scheme
SVP	Shortest Vector Problem
TA	Trusted Authority
TPM	Trusted Platform Module
UBAPV2G	Unique Batch Authentication Protocol for V2G Communications
V2G	Vehicle-to-Grid Networks
WAMS	Wide-Area Measurement System
WAN	Wide Area Network