SpringerBriefs in Computer Science

Series Editors
Stan Zdonik
Peng Ning
Shashi Shekhar
Jonathan Katz
Xindong Wu
Lakhmi C. Jain
David Padua
Xuemin (Sherman) Shen
Borko Furht
V.S. Subrahmanian
Martial Hebert
Katsushi Ikeuchi
Bruno Siciliano

For further volumes:
http://www.springer.com/series/10028

Hongwei Li

Enabling Secure and Privacy Preserving Communications in Smart Grids

Springer

Hongwei Li
University of Electronic Science
and Technology of China
Chengdu, Sichuan
People's Republic of China

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-3-319-04944-1 ISBN 978-3-319-04945-8 (eBook)
DOI 10.1007/978-3-319-04945-8
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014933524

© The Author(s) 2014
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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.
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.
While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

A smart grid has emerged as a promising solution to the next generation power grid system. It utilizes information and communications technology to gather and act on information, such as the behavior of suppliers and consumers, in an automated fashion to improve the reliability, efficiency, economics, and sustainability of the generation and distribution of electricity. However, security and privacy issues still present practical concerns to the deployment of smart grids. In this book, we investigate three schemes for secure and privacy-preserving smart grid communications.

In Chap. 2, we present an efficient privacy-preserving demand response scheme which employs a homomorphic encryption to achieve privacy-preserving demand aggregation and efficient response. In addition, an adaptive key evolution technique is further investigated to ensure the users' session keys to be forward secure. In Chap. 3, we introduce an efficient authentication scheme which utilizes the Merkle hash tree technique to secure smart grid communication. Specifically, the proposed authentication scheme considers the smart meters with computation-constrained resources and puts the minimum computation overhead on them. In Chap. 4, an efficient fine-grained keywords comparison scheme is proposed. Based on the homomorphic Pailier cryptosystem, we use two super-increasing sequences to aggregate multidimensional keywords. As a result, the comparison between the keywords of all sellers and those of one buyer can be achieved with only one calculation.

This book presents an overview of the state-of-the-art solutions to secure and privacy-preserving communications in smart grids. It not only reveals unique security and privacy characteristics but also offers effective solutions. Security analysis and performance evaluation demonstrate effectiveness and efficiency of three schemes. Last but not least, this book highlights promising future research directions to guide interested readers.

Sichuan, China

Hongwei Li

Acknowledgments

This book is supported by the National Natural Science Foundation of China under Grants 61350110238, 61103207, U1233108, 61272525, 61073106, and 61003232; the Fundamental Research Funds for Chinese Central Universities under Grant ZYGX2011J059; and the 2011 Korea-China Young Scientist Exchange Program.

Contents

1 Introduction to Smart Grids 1
1.1 Smart Grids 1
1.1.1 Communication Network Architecture 1
1.1.2 Characteristics of Smart Grids 2
1.2 Research Topics in Smart Grids 4
1.3 Security Primitives 6
1.3.1 Homomorphic Encryption 6
1.3.2 Bilinear Pairing 7
1.3.3 Identity-Based Signature 7
1.3.4 Merkle Hash Tree 7
1.4 Summary 8
References 9

2 Privacy-Preserving Demand Response in Smart Grids 11
2.1 Introduction 11
2.2 Models and Design Goal 12
2.2.1 Network Model 12
2.2.2 Security Model 13
2.2.3 Design Goal 14
2.3 Methodologies 14
2.3.1 System Initialization 14
2.3.2 Demand Aggregation 15
2.3.3 Demand Processing and Response 17
2.3.4 Key Evolution 18
2.4 Security Analysis 20
2.4.1 Authenticity, Data Integrity and Confidentiality 20
2.4.2 Privacy Preservation of Electricity Demand 21
2.4.3 Forward Secrecy of Users' Session Keys 22
2.4.4 Evolution of Users' Private Keys 24

2.5 Performance Evaluation 25
2.5.1 Communication Overhead 25
2.5.2 Computation Overhead 26
2.6 Related Works 27
2.7 Summary 29
References 29

3 An Efficient Authentication Scheme in Smart Grids 31
3.1 Introduction 31
3.2 Models and Design Goal 33
3.2.1 Network Model 33
3.2.2 Threat Model 33
3.2.3 Design Goal 34
3.3 Methodologies 35
3.3.1 System Initialization 35
3.3.2 Reports Generation 37
3.3.3 Neighborhood Gateway Authentication 37
3.4 Security Analysis 39
3.4.1 Resist the Message Analysis Attack 39
3.4.2 Resist the Message Modification Attack 39
3.4.3 Resist the Replay Attack 40
3.4.4 Resist the Message Injection Attack 40
3.5 Performance Evaluation 41
3.5.1 Communication Overhead 41
3.5.2 Computation Complexity 42
3.6 Related Works 43
3.7 Summary 44
References 45

4 An Efficient Fine-Grained Keywords Comparison Scheme in the Smart Grid Auction Market 47
4.1 Introduction 47
4.2 System Model, Security Requirements, and Design Goals 48
4.2.1 System Model 48
4.2.2 Security Requirements 49
4.2.3 Design Goals 49
4.3 Methodologies 50
4.3.1 System Initialization 50
4.3.2 Auction Message Creating 51
4.3.3 Filtering 52
4.4 Security Analysis 54
4.4.1 Secure Fine-Grained Keywords Comparison Between Tag and Trapdoor 55
4.4.2 Privacy Preservation of Auction Messages 55
4.4.3 Encrypted Messages' Authentication and Data Integrity 55

4.4.4 Private Messages' Authentication, Data Integrity and Confidentiality 56
4.5 Performance Evaluation 56
4.5.1 Computation Overhead 56
4.5.2 Communication Overhead 58
4.6 Related Works 59
4.7 Summary 59
References 59

5 Conclusions and Future Directions 61
5.1 Research Conclusions 61
5.2 Future Extensions 62