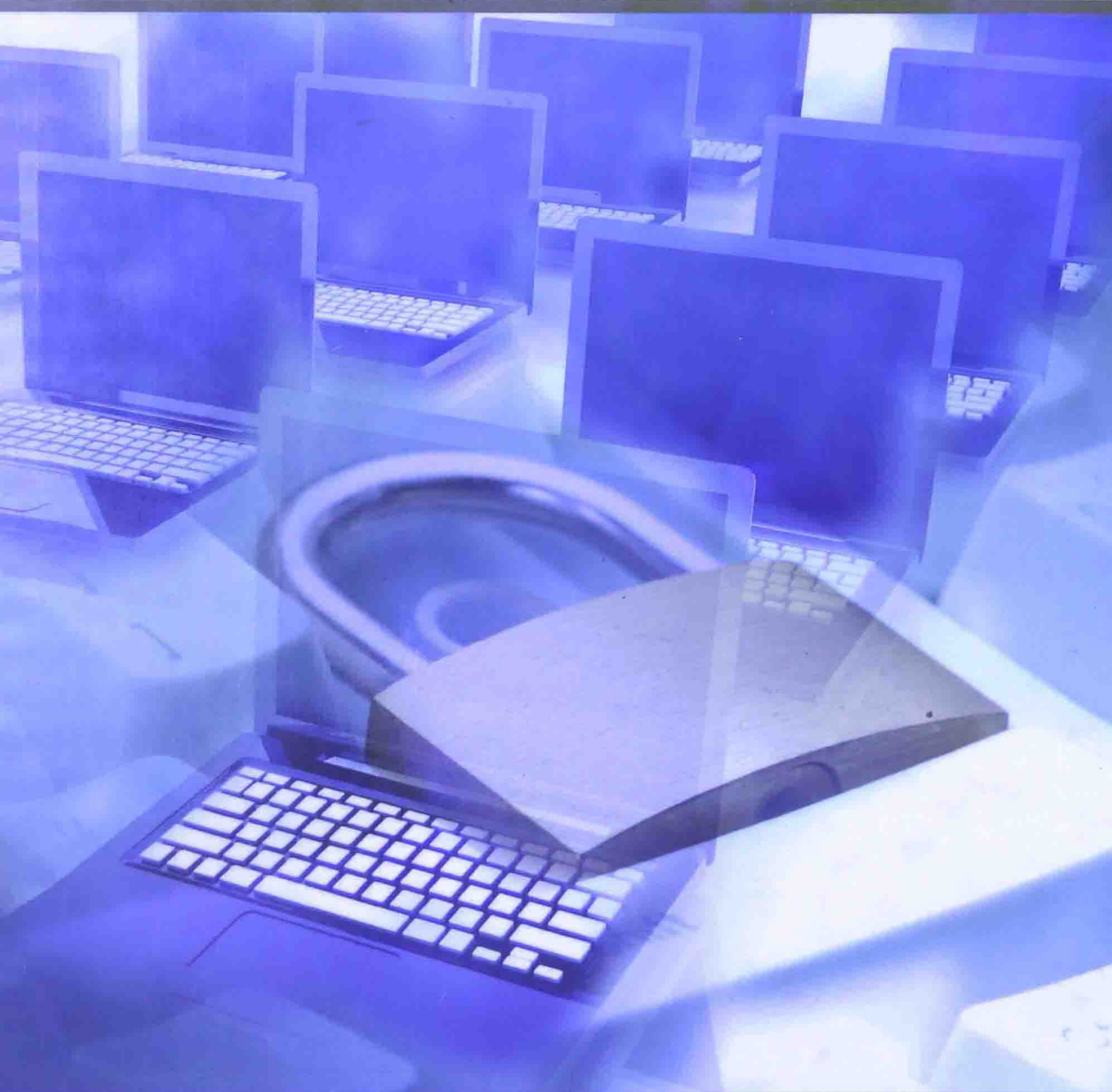


Security of Self-Organizing Networks

MANET, WSN, WMN, VANET



Edited by Al-Sakib Khan Pathan

Security of Self-Organizing Networks

MANET, WSN, WMN, VANET

Edited by Al-Sakib Khan Pathan



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **Informa** business
AN AUERBACH BOOK

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2011 by Taylor and Francis Group, LLC
Auerbach Publications is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number: 978-1-4398-1919-7 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Library of Congress Cataloging-in-Publication Data

Security of self-organizing networks : MANET, WSN, WMN, VANET / editor, Al-Sakib Khan Pathan.
p. cm.

Includes bibliographical references and index.

ISBN 978-1-4398-1919-7 (hardcover : alk. paper)

1. Ad hoc networks (Computer networks)--Security measures. 2. Self organizing systems--Security measures. I. Pathan, Al-Sakib Khan.

TK5105.77.S43 2011
005.8--dc22

2010028807

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the Auerbach Web site at
<http://www.auerbach-publications.com>

Preface

Various types of wireless networks and their applications can be seen in many places nowadays. With the increase in the number of Internet users, with the aid of wireless communications and demand of flexible anytime, anywhere networking, self-organizing wireless networks have already gained huge popularity among users. For wider support of wireless connectivity and developing easy-to-use technologies, substantial efforts are underway to reduce human intervention in the configuration, formation, and maintenance processes of these networks. This book is an attempt to address the security issues of four types of self-organizing networks (SONs): the Wireless Mobile *Ad hoc* Network (MANET), Wireless Sensor Network (WSN), Wireless Mesh Network (WMN), and Vehicular *Ad hoc* Network (VANET). Although various issues of these networks have been addressed extensively in different literature and numerous researchers around the globe are working on different aspects, here we have mainly focused on various facets of security in these networks.

As in an SON, hundreds and thousands of wireless devices can participate in a limited area with wireless communications but the information exchange among the devices needs appropriate privacy-, authenticity-, availability-, and nonrepudiation-ensuring mechanisms. Without proper security policy, any type of SON is exposed to a wide variety of security vulnerabilities and threats. Other than data security in such types of networks, there are also multiple factors that should be considered for ensuring overall security. For example, physical security of wireless devices is one of the important issues especially for WSNs and VANETs. Severe limitation of available device-resources (e.g., energy, radio, storage, processing, etc.) is a critical point for some networks. Again, security measures should be employed based on the special characteristics of a particular SON. All these issues related to security, problems, challenges, hopes, and solutions are discussed in various chapters of this book.

About the Contents of the Book

There are a total of 23 chapters in this book, which is divided into four parts. Different chapters in different parts address various security issues of SONs from different angles. The first part deals with general security topics. This part sets the base for the following chapters. Many terms are introduced in the chapters under Part I so that later they become easily accessible to readers. Part II deals with different security issues in MANETs and VANETs. For some of the chapters, the authors have proposed specific solutions to specific security problems. As VANET is a special class of MANET, we have included both of these networks under the same part. Part III discusses critical issues of

WSN security, and Part IV briefly touches on the security issues of WMNs. Most of these chapters are written in a tutorial manner. However, for some of the chapters, mathematical equations and detailed analysis are used for advanced readers. Hence, this book talks about relatively easier issues as well as analyzes some security-related issues in depth. Although in some cases, the contents of a chapter may overlap with some of the contents of another chapter, the repeated information might be helpful in clarifying specific points dealt with in that particular chapter. This is also useful in the sense that different people think of the same point from different perspectives. We hope that the book will really be helpful in giving a thorough and wide picture of the security aspects of MANETs, WSNs, WMNs, and VANETs.

What Not to Expect from the Book

This book is not a basic tutorial on the security issues of SONS. Hence, it does not have detailed introductory information about security. Although some chapters contain some elementary information, those should not be considered adequate for a beginner. Users/readers need to have at least some basic knowledge about security in networking. Again, this book should not be taken as a detailed research report. Some chapters simply present a specific problem and its solution that might be helpful for graduate students, some talk about elementary information that might be useful for general readers, some discuss in-depth security issues that might be helpful for advanced readers, and some chapters talk about the latest updates in a particular research area that might assist researchers in determining their future research objectives.

Target Audience

The book is very useful for Master's- or PhD-level students working on security issues in these networks, for researchers, for faculty members at the university level, and for some industry professionals. Questions and their sample answers have been provided with each chapter so that the readers' understanding from a chapter can be tested. Supplementary materials have been provided so that each chapter can be taught in a classroom environment with presentation slides. The book's chapters have been placed in such a sequence that it can be helpful to readers if they are read sequentially or to other readers who skip some of the chapters as they like. Overall, this book can guide readers to the latest trends, issues, and aspects of security of MANETs, WSNs, WMNs, and VANETs.

Dr. Al-Sakib Khan Pathan

Acknowledgments

I am very much thankful to the Almighty for giving me strength, keeping me fit, and giving me this time to accomplish this work. My sincere thanks to the authors of different chapters of this book without whose invaluable contributions, this project could not be completed. All the authors have been cooperative on different occasions during the submission, review, and editing process of the book. I am very thankful to Richard O'Hanley who helped me at each step of the publication process. I express my earnest gratitude to him for giving me this opportunity to edit such a book. Also thanks to him for his contribution to this book of choosing a timely, concise, and catchy title. Finally, I would like to thank my parents; Abdus Salam Khan Pathan, Delowara Khanom, my loving wife Labiba Mahmud, my younger brother Dr. Mukaddim Pathan, and my elder sister Tahmina A. Khanam for their continuous support and encouragement while preparing the book.

Dr. Al-Sakib Khan Pathan

Editor

Al-Sakib Khan Pathan is an assistant professor at the Computer Science and Engineering Department of Bangladesh Rural Advancement Committee (BRAC) University, Bangladesh. He worked as a researcher at the Networking Lab, Department of Computer Engineering in Kyung Hee University, South Korea, where he received his PhD in 2009. He received his BSc degree in computer science and information technology from the Islamic University of Technology (IUT), Bangladesh, in 2003. He has served as a chair, organizing committee member, and technical program committee member in several international conferences/workshops such as HPCS 2010, ICA3PP 2010, WiMob'09 and 08, HPCC'09, IDCS'09 and 08. He is currently serving as an area editor of *IJCNIS*, associate editor of IASTED/ACTA Press *IJCA*, guest editor of several international journals, including Elsevier's *Mathematical and Computer Modelling*, and editor of a book. He also serves as a referee of a few renowned journals such as the *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*; the *IEEE Transactions on Vehicular Technology (IEEE TVT)*; the *IEEE Communications Letters*; Elsevier's *Computer Communications*, *Computer Standards and Interfaces*; the *Computers & Electrical Engineering* journal; the *Journal of High Speed Networks (JHSN, IOS Press)*; the *EURASIP Journal on Wireless Communications and Networking (EURASIP JWCN)*; and the *International Journal of Communication Systems (IJCS, Wiley)*. He is a member of IEEE and several other international organizations. His research interest includes wireless sensor networks, network security, and e-services technologies.

Contributors

Mozaffar Afaq
Department of Computer Science
and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, India

Johnson I. Agbinya
Centre for Real-Time Information Networks
University of Technology
Sydney, Australia

Syed Ishtiaque Ahmed
Department of Computer Science
and Engineering
Bangladesh University of Engineering
and Technology
Dhaka, Bangladesh

Tarem Ahmed
Department of Electrical and
Electronic Engineering
BRAC University
Dhaka, Bangladesh

Nancy Alrajai
Department of Computer Science
and Engineering
Oakland University
Rochester, Michigan

Hani Alzaid
Information Security Institute
Queensland University of Technology
Queensland, Australia

Sharifah Hafizah Syed Ariffin
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia

Michel Barbeau
School of Computer Science
Carleton University
Ontario, Canada

Dan Chalmers
School of Informatics
University of Sussex
Brighton, United Kingdom

Gihwan Cho
Division of Electronics and
Information Engineering
Chonbuk National University
Chonju, South Korea

John A. Clark
Department of Computer Science
University of York
York, United Kingdom

Zubair Muhammad Fadlullah
Graduate School of Information Sciences
Tohoku University
Sendai, Japan

Norsheila Fisal
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia

Joaquin Garcia-Alfaro

School of Computer Science
Carleton University
Ontario, Canada

and

Computer Science and Multimedia
Studies
Open University of Catalonia
Catalonia, Spain

M.S. Gaur

Department of Computer Engineering
Malaviya National Institute
of Technology
Jaipur, India

Swapna Ghanekar

Department of Computer Science
and Engineering
Oakland University
Rochester, Michigan

S.K. Ghosh

School of Information Technology
Indian Institute of Technology
Kharagpur
Kharagpur, India

Stephen Glass

School of Information and Communication
Technology
Griffith University

and

National Information and
Communications Technology
Australia (NICTA)
Queensland Research Laboratory
Queensland, Australia

Vikrant Gokhale

School of Information Technology
Indian Institute of Technology
Kharagpur
Kharagpur, India

Sumit Goswami

DESIDOC, Defence Research
& Development Organization
Delhi, India

Jyoti Grover

Department of Computer Engineering
Malaviya National Institute of Technology
Jaipur, India

Arobinda Gupta

Department of Computer Science
and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, India

Md. Abdul Hamid

Department of Information and
Communications Engineering
Hankuk University of Foreign Studies
Kyonggi-do, South Korea

James Harbin

Department of Electronics
University of York
York, United Kingdom

Bing He

Department of Computer Science
University of Cincinnati
Cincinnati, Ohio

Md. Shariful Islam

Department of Computer Engineering
Kyung Hee University
Gyeonggi-do, South Korea

Evangelos Kranakis

School of Computer Science
Carleton University
Ontario, Canada

V. Laxmi

Department of Computer Engineering
Malaviya National Institute of Technology
Jaipur, India

Sungyoung Lee

Department of Computer Engineering
Kyung Hee University (Global Campus)
Gyeonggi-do, South Korea

Effie Makri

Department of Mathematics
University of the Aegean
Karlovassi, Greece

Yasir Arfat Malkani

School of Informatics
University of Sussex
Brighton, United Kingdom

Fatma Mili

Department of Computer Science
and Engineering
Oakland University
Rochester, Michigan

Sudip Misra

School of Information Technology
Indian Institute of Technology Kharagpur
Kharagpur, India

Paul Mitchell

Department of Electronics
University of York
York, United Kingdom

Vallipuram Muthukkumarasamy

School of Information and
Communications Technology
Griffith University
and

National Information and Communications
Technology Australia (NICTA)
Queensland Research Laboratory
Queensland, Australia

Al-Sakib Khan Pathan

Department of Computer Science
and Engineering
BRAC University
Dhaka, Bangladesh

and

Department of Computer Engineering
Kyung Hee University
Gyeonggi-do, South Korea

David Pearce

Department of Electronics
University of York
York, United Kingdom

Zeeshan Pervez

Department of Computer Engineering
Kyung Hee University (Global Campus)
Gyeonggi-do, South Korea

Marius Portmann

School of Information Technology
and Electrical Engineering
University of Queensland

and

National Information and Communications
Technology Australia (NICTA)
Queensland Research Laboratory
Queensland, Australia

Syed Muhammad Khaliq-ur-Rahman Raazi

Department of Computer Engineering
Kyung Hee University (Global Campus)
Gyeonggi-do, South Korea

Rumana Rahman

Department of Electrical and Electronic
Engineering
BRAC University
Dhaka, Bangladesh

Rozeha A. Rashid

Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia

Ranga Reddy

U.S. Army—Communications Electronics
Research, Development, and Engineering
Center (CERDEC)
Fort Monmouth, New Jersey

Une Thoing Rosi
Department of Computer Science
and Engineering
United International University
Dhaka, Bangladesh

Kashif Saleem
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia

Marcus Schöller
NEC Europe Ltd
Heidelberg, Germany

Jaydip Sen
Innovation Lab
Tata Consultancy Services
Kolkata, India

Sevil Şen
Department of Computer
Science
University of York
York, United Kingdom

Yannis C. Stamatiou
Department of Mathematics
University of Ioannina
Ioannina, Greece

and
Research Academic
Computer Technology
Institute
University of Patras
Patras, Greece

Tarik Taleb
NEC Europe Ltd
Heidelberg, Germany

Juan E. Tapiador
Department of Computer Science
University of York
York, United Kingdom

Thanh Dai Tran
Centre for Real-Time Information Networks
University of Technology
Sydney, Australia

Ian Wakeman
School of Informatics
University of Sussex
Brighton, United Kingdom

Gicheol Wang
Department of Computing and
Networking Resources
Supercomputing Center, KISTI
Daejeon, South Korea

Bin Xie
InfoBeyond Technology LLC
Louisville, Kentucky

Vikas Singh Yadav
Department of Computer
Science and Engineering
Indian Institute of Technology
Kharagpur
Kharagpur, India

Sharifah Kamilah Syed Yusof
Faculty of Electrical Engineering
Universiti Teknologi Malaysia
Skudai, Malaysia

David Zhao
U.S. Army—Communications Electronics
Research, Development, and Engineering
Center (CERDEC)
Fort Monmouth, New Jersey

Contents

Prefaceix

Acknowledgmentsxi

Editorxiii

Contributors xv

**PART I GENERAL TOPICS: SECURITY OF WIRELESS AND
SELF-ORGANIZING NETWORKS**

1 Secure Device Association: Trends and Issues 3
YASIR ARFAT MALKANI, DAN CHALMERS, and IAN WAKEMAN

2 Securing Route and Path Integrity in Multihop Wireless Networks 25
STEPHEN GLASS, MARIUS PORTMANN, and VALLIPURAM MUTHUKUMARASAMY

3 Handling Security Threats to the RFID System of EPC Networks 45
JOAQUIN GARCIA-ALFARO, MICHEL BARBEAU, and EVANGELOS KRANAKIS

4 Survey of Anomaly Detection Algorithms: Toward Self-Learning Networks..... 65
TAREM AHMED and RUMANA RAHMAN

5 Reputation- and Trust-Based Systems for Wireless Self-Organizing Networks..... 91
JAYDIP SEN

**PART II MOBILE *AD HOC* NETWORK AND VEHICULAR *AD HOC*
NETWORK SECURITY**

6 Security Threats in Mobile *Ad Hoc* Networks 127
SEVIL ŞEN, JOHN A. CLARK, and JUAN E. TAPIADOR

7 Key Management in Mobile *Ad Hoc* Networks..... 147
SUDIP MISRA and SUMIT GOSWAMI

8	Combating against Security Attacks against Mobile <i>Ad Hoc</i> Networks (MANETs)	173
	ZUBAIR MUHAMMAD FADLULLAH, TARIK TALEB, and MARCUS SCHÖLLER	
9	Classification of Attacks on Wireless Mobile <i>Ad Hoc</i> Networks and Vehicular <i>Ad Hoc</i> Networks: A Survey	195
	VIKRANT GOKHALE, S.K. GHOSH, and AROBINDA GUPTA	
10	Security in Vehicular <i>Ad Hoc</i> Networks	227
	VIKAS SINGH YADAV, SUDIP MISRA, and MOZAFFAR AFAQUE	
11	Toward a Robust Trust Model for Ensuring Security and Privacy in VANETs	251
	UNE THOING ROSI and SYED ISHTIAQUE AHMED	
12	Sybil Attack in VANETs: Detection and Prevention	269
	JYOTI GROVER, M.S. GAUR, and V. LAXMI	

PART III WIRELESS SENSOR NETWORK SECURITY

13	Key Management Schemes of Wireless Sensor Networks: A Survey	297
	SYED MUHAMMAD KHALIQ-UR-RAHMAN RAAZI, ZEESHAN PERVEZ, and SUNGYOUNG LEE	
14	Key Management Techniques for Wireless Sensor Networks: Practical and Theoretical Considerations	317
	EFFIE MAKRI and YANNIS C. STAMATIOU	
15	Bio-Inspired Intrusion Detection for Wireless Sensor Networks	347
	SWAPNA GHANEKAR, NANCY ALRAJEL, and FATMA MILI	
16	Biological Inspired Autonomously Secure Mechanism for Wireless Sensor Networks	375
	KASHIF SALEEM, NORSHEILA FISAL, SHARIFAH HAFIZAH SYED ARIFFIN, SHARIFAH KAMILAH SYED YUSOF, and ROZEHA A. RASHID	
17	Controlled Link Establishment Attack on Key Pre-Distribution Schemes for Distributed Sensor Networks and Countermeasures	409
	THANH DAI TRAN and JOHNSON I. AGBINYA	
18	Proactive Key Variation Owing to Dynamic Clustering (PERIODIC) in Sensor Networks	437
	GICHEOL WANG and GIHWAN CHO	
19	Secure Routing Architectures Using Cross-Layer Information for Attack Avoidance (with Case Study on Wormhole Attacks)	465
	JAMES HARBIN, PAUL MITCHELL, and DAVID PEARCE	
20	Reputation-Based Trust Systems in Wireless Sensor Networks	493
	HANI ALZAID	

21	Major Works on the Necessity and Implementations of PKC in WSNs:	
	A Beginner's Note.....	525
	AL-SAKIB KHAN PATHAN	

PART IV WIRELESS MESH NETWORK SECURITY

22	Secure Access Control and Authentication in Wireless Mesh Networks.....	545
	BING HE, BIN XIE, DAVID ZHAO, and RANGA REDDY	
23	Misbehavior Detection in Wireless Mesh Networks.....	571
	MD. ABDUL HAMID and MD. SHARIFUL ISLAM	
	Index	595

**GENERAL
TOPICS—SECURITY
OF WIRELESS AND
SELF-ORGANIZING
NETWORKS**

Chapter 1

Secure Device Association *Trends and Issues*

Yasir Arfat Malkani, Dan Chalmers, and Ian Wakeman

Contents

- 1.1 Introduction..... 4
- 1.2 Background..... 5
 - 1.2.1 Attack Types in Device Association Model 5
 - 1.2.1.1 Eavesdropping..... 5
 - 1.2.1.2 MiTM Attack..... 5
 - 1.2.1.3 DoS Attack 6
 - 1.2.1.4 Bidding-Down Attack 6
 - 1.2.1.5 Compromised Devices..... 7
 - 1.2.2 Device Association in *Ad Hoc* Environments..... 7
 - 1.2.2.1 Resurrecting Duckling Security Model..... 7
 - 1.2.2.2 Talking to Strangers..... 7
 - 1.2.2.3 Device Association Using Visual Out-of-Band Channels..... 8
 - 1.2.2.4 Device Association Using Audio Out-of-Band Channels..... 8
 - 1.2.2.5 Device Association Using Accelerometers..... 9
 - 1.2.2.6 Device Association Using Radio Signals 10
 - 1.2.2.7 Device Association Using Biometric Data 10
 - 1.2.2.8 Button-Enabled Device Association (BEDA) 10
 - 1.2.2.9 Bluetooth Pairing..... 11
 - 1.2.2.10 Device Association Using Near-Field Communication Technology 12
 - 1.2.2.11 Wireless Universal Serial Bus (WUSB) Association, WPS, and Windows Connect now-Net..... 13
 - 1.2.3 Comparative Analysis of Device Association Methods 13
- 1.3 Future Directions for Research..... 15
- 1.4 Conclusions 16
- Acknowledgments 19