# Security for
# Wireless Sensor Networks

# Advances in Information Security

**Sushil Jajodia**
*Consulting Editor*
*Center for Secure Information Systems*
*George Mason University*
*Fairfax, VA 22030-4444*
*email: jajodia@gmu.edu*

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

## *Additional titles in the series:*

***MALWARE DETECTION*** edited by Somesh Jha, Cliff Wang, Mihai Christodorescu, Dawn Song, and Douglas Maughan; ISBN: 978-0-387-32720-4
***ELECTRONIC POSTAGE SYSTEMS: Technology, Security, Economics*** by Gerrit Bleumer; ISBN: 978-0-387-29313-2
***MULTIVARIATE PUBLIC KEY CRYPTOSYSTEMS*** by Jintai Ding, Jason E. Gower and Dieter Schmidt; ISBN-13: 978-0-378-32229-2
***UNDERSTANDING INTRUSION DETECTION THROUGH VISUALIZATION*** by Stefan Axelsson; ISBN-10: 0-387-27634-3
***QUALITY OF PROTECTION: Security Measurements and Metrics*** by Dieter Gollmann, Fabio Massacci and Artsiom Yautsiukhin; ISBN-10: 0-387-29016-8
***COMPUTER VIRUSES AND MALWARE*** by John Aycock; ISBN-10: 0-387-30236-0
***HOP INTEGRITY IN THE INTERNET*** by Chin-Tser Huang and Mohamed G. Gouda; ISBN-10: 0-387-22426-3
***CRYPTOGRAPHICS: Exploiting Graphics Cards For Security*** by Debra Cook and Angelos Keromytis; ISBN: 0-387-34189-7
***PRIVACY PRESERVING DATA MINING*** by Jaideep Vaidya, Chris Clifton and Michael Zhu; ISBN-10: 0-387- 25886-8
***BIOMETRIC USER AUTHENTICATION FOR IT SECURITY: From Fundamentals to Handwriting*** by Claus Vielhauer; ISBN-10: 0-387-26194-X
***IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY:Enabled Information Small-Medium Enterprises (TEISMES)*** by Charles A. Shoniregun; ISBN-10: 0-387-24343-7

*Additional information about this series can be obtained from*
http://www.springer.com

# Security for Wireless Sensor Networks

*by*

**Donggang Liu**
*The University of Texas at Arlington, TX*
*USA*

**Peng Ning**
*North Carolina State University, Raleigh, NC*
*USA*

Springer

Donggang Liu
Dept. Computer Science & Engineering
Univ. of Texas, Arlington
Arlington TX 76019-0015

Peng Ning
North Carolina State University
Dept. of Computer Science
Raleigh NC 27695-8206

Library of Congress Control Number:

Security for Wireless Sensor Networks by Donggang Liu and Peng Ning

ISBN-10: 0-387-32723-1
ISBN-13: 978-0-387-32723-5
e-ISBN-10: 0-387-46781-5
e-ISBN-13: 978-0-387-46781-8

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

To my wife Rongfang.
—DL

To my wife Li and my son Daniel.
—PN

# Preface

The recent technological advances have made it possible to deploy small, low-power, low-bandwidth, and multi-functional wireless sensor nodes to monitor and report the conditions and events in their local environments. A large collection of these sensor nodes can thus form a wireless sensor network in an ad hoc manner, creating a new type of information systems. Such sensor networks have recently emerged as an important means to study and interact with the physical world and have received a lot of attention due to their wide applications in military and civilian operations such as target tracking and data acquisition. However, in many of these applications, wireless sensor networks could be deployed in hostile environments where there are malicious attacks against the network.

Providing security services in sensor networks, however, turns out to be a very challenging task. First, sensor nodes usually have limited resources such as storage, bandwidth, computation and energy. It is often undesirable to implement expensive algorithms (e.g., frequent public key operations) on sensor nodes. Second, sensor nodes are usually deployed unattended and built without compromise prevention in mind. An attacker can easily capture and compromise a few sensor nodes without being noticed. When sensor nodes are compromised, the attacker can learn all the secrets stored on them and launch a variety of attacks. Thus, any security mechanism for sensor networks has to be resilient to compromised sensor nodes. Third, most sensor applications are based on local computation and communication, while adversaries are usually much more powerful and resourceful than sensor nodes. In many cases, one has to use resource-constrained sensor nodes to deal with very powerful attacks.

This book discusses fundamental security issues in wireless sensor network and presents techniques for the protection of such networks. The purpose of this book is to help both students and professionals to understand fundamental security issues and techniques for wireless sensor network security and prepare them for doing research in this domain. This book could be used as a supplemental textbook covering wireless sensor networks for undergraduate/graduate level security courses with prior knowledge of compute networks, operating systems, probability and statistics, and information security.

This text includes results from recent advances in wireless sensor network security. However, many of these techniques are transitory due to the rapid technological advances in wireless sensor networks. This book is written and organized with special emphasis on basic design principals that may survive current rapid changes in wireless sensor network security.

*Donggang Liu*
The University of Texas at Arlington
*Peng Ning*
North Carolina State University

# Contents