Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc 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:

PRESERVING PRIVACY IN ON-LINE ANALYTICAL PROCESSING (OLAP) by Lingyu Wang, Sushil Jajodia and Duminda Wijesekera; ISBN: 978-0-387-46273-8
SECURITY FOR WIRELESS SENSOR NETWORKS by Donggang Liu and Peng Ning; ISBN: 978-0-387-32723-5
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

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

Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks

Edited by

Radha Poovendran
University of Washington, USA

Cliff Wang
Army Research Office, USA

Sumit Roy
University of Washington, USA

Springer

Radha Poovendran
University of Washington
Dept. Computer Science & Engineering
P.O.Box 352350
Seattle WA 98195
radha@ee.washington.edu

Cliff Wang
Computing and Information Science Div.
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211
cliff.wang@us.army.mil

Sumit Roy
University of Washington
Dept. Computer Science & Engineering
P.O.Box 352350
Seattle WA 98195
roy@ee.washington.edu

Library of Congress Control Number: 2006934200

Secure Localization and Time Synchronization for Wireless Sensor and
Ad Hoc Networks edited by Radha Poovendran, Cliff Wang, Roy Sumit

ISBN-13: 978-0-387-32721-1
ISBN-10: 0-387-32721-5
e-ISBN-13: 978-0-387-46276-9
e-ISBN-10: 0-387-46276-7

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

Foreword

During the past three decades, every major advance in computing introduced new and largely unanticipated security challenges. Wireless sensor networks are only the latest technology that confirms this observation. These networks, which represent a basic tenet of what we call ubiquitous computing, are now or will soon be deployed in physical environments that are vulnerable not only to the vicissitudes of nature but also to acts that could be easily viewed as hostile attacks by potent adversaries. Indeed, unattended operation of sensor-network nodes in hostile environments requires that we rethink the definition of our adversary, its capabilities and modes of attack.

There are few problems of wireless sensor network design and analysis that are as challenging as localization and time synchronization. Yet both are fundamental building blocks not just for new applications and but also security services themselves. Localization complexity is, to a significant degree, the result of deployment and operation in environments that lack of unobstructed line-of-site connectivity, reference points, and communications. Further, time synchronization gains added complexity due to the limited computing resources sensor nodes possess. As a consequence, the natural interplay between space and time measurements and bounds, which are basic to both localization and time synchronization, produces a largely uncharted research territory. And, of course, the new capabilities and attack modes of the new adversary complicates the landscape in unanticipated ways.

This book represents a snapshot of our understanding in solving problems of robust, resilient and secure localization and time synchronization at the inception of the sensor network technology development. It offers a clear view of the essential challenges posed by localization and time synchronization in sensor networks, subtleties of potential solutions, and extensive discussion of specific protocols and mechanisms required by these solutions. In short, the book is an indispensable reference to both researchers and developers, and an invaluable aid to students.

I am pleased and honored to have been asked to write the foreword for this book. The authors, all active researchers in the area of sensor network security, should be congratulated for providing this valuable reference book for the research community.

September 2006, College Park, Maryland *Virgil D. Gligor*

Preface

This book is an outcome of a special workshop on Localization in Wireless Sensor Networks, held between June 13-14 of 2005, at the University of Washington, Seattle.

During several technical discussions, Dr. Radha Poovendran of University of Washington and ARO Information Assurance (IA) program director Dr. Cliff Wang felt that robust and resilient localization for wireless sensor networks is an important research area and a special workshop was needed to address the research challenges and to promote innovative ideas for solutions. Dr. Sumit Roy from the University of Washington later joined the organizing committee. The workshop was organized and held successfully. Over 30 researchers participated in the workshop and a total of 18 presentations were made, covering various aspects of the localization problem.

This book is a direct outcome of this special workshop. We have also expanded the scope of this book to include secure time synchronization since the techniques used for localization distance bounding protocols are dependent on correct time synchronization of wireless sensor networks. A total of sixteen contributed papers are received from both workshop participants and researchers active in wireless sensor network research. The collection of these high quality papers makes this edited volume a valuable resource for both researchers and engineers in related fields. We believe that this book will serve as a reference as well as the starting point of research in the exciting areas of secure location estimation, secure time synchronization, verification of sensor security protocols, and location privacy.

The book is organized into three parts. The chapters in Part I present approaches for sensor location estimation under a benign environment and technical discussions focus on the quality of location estimation. The chapters in the Part II of the book contain the latest work on resilient sensor location estimation in the presence of an adversary that may inject Byzantine errors into the localization process. Also in Part II of the book, there is one chapter dedicated to distance bounding protocol verification and there is another chapter that focuses specifically on privacy protection against location tracking. The Part III of the book contains chapters addressing the problem of secure time synchronization in wireless sensor networks.

We would like to express our thanks to Professor Sushil Jajodia for including this book in his series. We thank Susan Lagerstrom-Fife and Sharon Palleschi of Springer, and Krishna Sampigethaya of University of Washington for working closely with us during the production of this book. We also thank Krishna Sampigethaya, Loukas Lazos, Mingyan Li, Patrick Tague, and Javier Salido for their help and support during the workshop.

September 2006, University of Washington	*Radha Poovendran*
September 2006, ARO/NCSU	*Cliff Wang*
September 2006, University of Washington	*Sumit Roy*

Contents

Part I Localization Techniques

Part II Secure Localization

Part III Secure Time Synchronization

List of Contributors

Prathima Agrawal
200, Broun Hall
Auburn University
Auburn, Alabama 36830
agrawpr@auburn.edu

Farooq Anjum
Telcordia Technologies
One Telcordia Drive
Piscataway, NJ 08854
fanjum@telcordia.com

Nirupama Bulusu
Department of Computer Science
Portland State University
Portland, OR 97207-0751
nbulusu@cs.pdx.edu

Srdjan Čapkun
Informatics and Mathematical Modelling Department,
Technical University of Denmark
DK-2800 Lyngby, Denmark
sca@imm.dtu.dk

LiWu Chang
U.S. Naval Research Laboratory,
Code 5543
Washington, DC 20375
lchang@itd.nrl.navy.mil

Jose A. Costa
Center for the Mathematics of Information
California Institute of Technology
1200 E. California Blvd.
Pasadena, CA 91106
jcosta@caltech.edu

Thanh X Dang
Department of Computer Science
Portland State University
Portland, OR 97207-0751
dangtx@cs.pdx.edu

Wenliang Du
Department of Electrical Engineering
and Computer Science
Syracuse University
3-114 Sci-Tech Building
Syracuse, NY 13244
wedu@ecs.syr.edu

Lei Fang
Department of Electrical Engineering
and Computer Science
Syracuse University
3-114 Sci-Tech Building
Syracuse, NY 13244
lefang@ecs.syr.edu

Saurabh Ganeriwal
Networked and Embedded Systems Lab
University of California
Los Angeles, CA 90095-1594
saurabh@ee.ucla.edu

Simon Han
Networked and Embedded Systems Lab
University of California
Los Angeles, CA 90095-1594
simonhan@ee.ucla.edu

Tian He
Department of Computer Science and Engineering
University of Minnesota
200 Union Street SE
Minneapolis, MN 55455
tianhe@cs.umn.edu

Alfred O. Hero III
Department of Electrical Engineering and Computer Science
University of Michigan
1301 Beal Avenue
Ann Arbor, MI 48109-2122
hero@umich.edu

Leping Huang
Nokia Research Center/University of Tokyo
1-8-1, Shimomeguro, Meguro-ku
Tokyo, Japan
leping.huang@nokia.com

Sanjay Jha
School of Computer Science and Engineering,
University of New South Wales
Sydney 2052, Australia
sjha@cse.unsw.edu.au

Manali Joglekar
WINLAB
Rutgers University
671 Route 1 South
North Brunswick, N.J. 08902-3390
manali@winlab.rutgers.edu

Bhaskar Krishnamachari
Department of Electrical Engineering-Systems
University of Southern California
3740 McClintock Avenue
Los Angeles, CA 90089
bkrishna@usc.edu

Loukas Lazos
Network Security Lab
Department of Electrical Engineering
Box 352500
University of Washington
Seattle, WA 98195-2500
llazos@u.washington.edu

Zang Li
WINLAB
Rutgers University
671 Route 1 South
North Brunswick, N.J. 08902-3390
zang@winlab.rutgers.edu

Donggang Liu
Department of Computer Science and Engineering
University of Texas at Arlington
330 Nedderman Hall
Arlington, Texas 76019-0015
dliu@cse.uta.edu

Dimitrios Lymberopoulos
Department of Electrical Engineering
Yale University
51 Prospect St.
New Haven, CT 06511
dimitrios.lymberopoulos
@yale.edu

Michael Manzo
Department of Electrical Engineering
and Computer Sciences
University of California at Berkeley
333 Cory Hall
Berkeley, CA 94720
mike@manzo.org

Kanta Matsuura
University of Tokyo
4-6-1 Komaba, Meguro-ku
Tokyo, Japan
kanta@iis.u-tokyo.ac.jp

Catherine Meadows
U.S. Naval Research Laboratory,
Code 5543
Washington, DC 20375
meadows@itd.nrl.navy.mil

Badri Nath
Computer Science Department
Rutgers University
110 Frelinghuysen Road
Piscataway, NJ 08854
badri@cs.rutgers.edu

Peng Ning
Department of Computer Science
North Carolina State University
890 Oval Dr.
Raleigh, NC 27695-8206
pning@ncsu.edu

Santosh Pandey
200, Broun Hall
Auburn University
Auburn, Alabama 36830
pandesg@auburn.edu

Pubudu N Pathirana
School of Engineering and Technology
Deakin University
Geelong 3217, Australia
pubudu@deakin.edu.au

Neal Patwari
Department of Electrical Engineering
and Computer Science
University of Michigan
1301 Beal Avenue
Ann Arbor, MI 48109-2122
npatwari@umich.edu

Dusko Pavlovic
Kestrel Institute,
3260 Hillview Avenue
Palo Alto, CA 94304
dusko@kestrel.edu

Radha Poovendran
Network Security Lab
Department of Electrical Engineering
Box 352500
University of Washington
Seattle, WA 98195-2500
rp3@u.washington.edu

Tanya Roosta
Department of Electrical Engineering
and Computer Sciences
University of California at Berkeley
333 Cory Hall
Berkeley, CA 94720
roosta@eecs.berkeley.edu

Shankar Sastry
Department of Electrical Engineering
and Computer Sciences
University of California at Berkeley
514 Cory Hall
Berkeley, CA 94720
sastry@eecs.berkeley.edu

Andrey V Savkin
School of Electrical Engineering and
Telecommunications
University of New South Wales
Sydney 2052, Australia
a.savkin@unsw.edu.au

Andreas Savvides
Department of Electrical Engineering
Yale University
51 Prospect St.
New Haven, CT 06511
andreas.savvides@yale.edu

Kaoru Sezaki
University of Tokyo
4-6-1 Komaba, Meguro-ku
Tokyo, Japan
sezaki@iis.u-tokyo.ac.jp

Mani Srivastava
Networked and Embedded Systems Lab
University of California
Los Angeles, CA 90095-1594
mbs@ee.ucla.edu

John A. Stankovic
Department of Computer Science
University of Virginia
151 Engineer's Way, P.O. Box 400740
Charlottesville, VA 22904-4740
stankovic@cs.virginia.edu

Radu Stoleru
Department of Computer Science
University of Virginia
151 Engineer's Way, P.O. Box 400740
Charlottesville, VA 22904-4740
stoleru@cs.virginia.edu

Kun Sun
Department of Computer Science
North Carolina State University
890 Oval Drive
Raleigh, NC 27695-8206
ksun3@ncsu.edu

Paul Syverson
U.S. Naval Research Laboratory,
Code 5543
Washington, DC 20375
syverson@itd.nrl.navy.mil

Wade Trappe
WINLAB
Rutgers University
671 Route 1 South
North Brunswick, N.J. 08902-3390
trappe@winlab.rutgers.edu

Cliff Wang
Army Research Office
4300 S Miami Blvd.
RTP, NC 27709
cliff.wang@us.army.mil

Hiroshi Yamane
University of Tokyo
4-6-1 Komaba, Meguro-ku
Tokyo, Japan
yamane@mcl.iis.u-tokyo.ac.jp

Kiran Yedavalli
Department of Electrical Engineering-Systems
University of Southern California
3740 McClintock Avenue
Los Angeles, CA 90089
kyedaval@usc.edu

Yanyong Zhang
WINLAB
Rutgers University
671 Route 1 South
North Brunswick, N.J. 08902-3390
yyzhang@winlab.rutgers.edu