



Al-Sakib Khan Pathan

Securing WSN with Lightweight Resource- Efficient Schemes

Security From the Bootstrapping Phase



LAMBERT
Academic Publishing

Al-Sakib Khan Pathan

**Securing WSN with Lightweight
Resource-Efficient Schemes**

Security From the Bootstrapping Phase

LAP LAMBERT Academic Publishing

Impressum/Imprint (nur für Deutschland/only for Germany)

Bibliografische Information der Deutschen Nationalbibliothek Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie, detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar
Alle in diesem Buch genannten Marken und Produktnamen unterliegen Warenzeichen-, marken- oder patentrechtlichem Schutz bzw. sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber Die Wiedergabe von Marken, Produktnamen, Gebrauchsnamen, Handelsnamen, Warenbezeichnungen u s w in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutzgesetzgebung als frei zu betrachten waren und daher von jedermann benutzt werden durften

Coverbild www.ingimage.com

Verlag LAP LAMBERT Academic Publishing GmbH & Co KG
Dudweiler Landstr. 99, 66123 Saarbrücken, Deutschland
Telefon +49 681 3720-310, Telefax +49 681 3720-3109
Email. info@lap-publishing.com

Approved by Seoul, Kyung Hee University, Diss., 2009

Herstellung in Deutschland
Schaltungsdienst Lange o H G , Berlin
Books on Demand GmbH, Norderstedt
Reha GmbH, Saarbrücken
Amazon Distribution GmbH, Leipzig
ISBN: 978-3-8465-1681-2

Imprint (only for USA, GB)

Bibliographic information published by the Deutsche Nationalbibliothek The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie, detailed bibliographic data are available in the Internet at <http://dnb.d-nb.de>
Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc even without a particular marking in this works is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone

Cover image www.ingimage.com

Publisher LAP LAMBERT Academic Publishing GmbH & Co KG
Dudweiler Landstr. 99, 66123 Saarbrücken, Germany
Phone +49 681 3720-310, Fax +49 681 3720-3109
Email info@lap-publishing.com

Printed in the U S A
Printed in the U.K by (see last page)
ISBN: 978-3-8465-1681-2

Copyright © 2011 by the author and LAP LAMBERT Academic Publishing GmbH & Co KG and licensors
All rights reserved Saarbrücken 2011

Table of Contents

CHAPTER 1	INTRODUCTION	1
1.1	BACKGROUND	2
1.1.1	<i>Key Aspects to Consider for WSN Security</i>	4
1.1.2	<i>Feasibility of Different Security Approaches in WSN</i>	6
1.2	MOTIVATION AND BOOK CONTRIBUTION	8
1.2.1	<i>Motivation and Problem Description</i>	8
1.2.2	<i>Goals and Contributions</i>	8
1.3	OUTLINE OF THIS BOOK	10
CHAPTER 2	LITERATURE REVIEW: SECURITY ISSUES IN WIRELESS SENSOR NETWORK	11
2.1	DENIAL OF SERVICE (DOS) ATTACK	12
2.2	ATTACKS ON INFORMATION IN TRANSIT	17
2.3	SYBIL ATTACK	18
2.4	BLACKHOLE/SINKHOLE ATTACK	20
2.5	HELLO FLOOD ATTACK	21
2.6	WORMHOLE ATTACK	22
2.7	KEY MANAGEMENT ISSUES IN WSN	25
2.8	SECURE ROUTING AND PHYSICAL SECURITY ISSUES	28
2.9	RESEARCH CHALLENGES	31
2.9.1	<i>Holistic Approach to Security in WSN</i>	31
2.9.2	<i>Achievements and Goals</i>	33
CHAPTER 3	PHASE I: SECURE CLUSTERING AND OPERATION IN DISTRIBUTED SENSOR NETWORKS	36
3.1	OVERVIEW	37
3.2	RELATED WORKS	39
3.3	NETWORK MODEL, ASSUMPTIONS, AND PRELIMINARIES	41
3.4	PROPOSED APPROACH OF SECURE CLUSTERING	45

3.4.1	<i>Offline Rank Assignment with Key Pre-Distribution</i>	46
3.4.2	<i>Post Deployment Cluster Formation</i>	48
3.4.3	<i>Authenticated Message Delivery</i>	50
3.4.4	<i>Optional Re-keying Mechanism</i>	51
3.5	PERFORMANCE EVALUATION AND COMPARISON	53
3.5.1	<i>Simulation, Analysis, and Results</i>	53
3.5.2	<i>Limitations of our Approach</i>	59
3.6	SUMMARY	60
CHAPTER 4 PHASE II: SERP: SECURE ENERGY-EFFICIENT ROUTING PROTOCOL		
	61
4.1	INTRODUCTION.....	62
4.2	RELATED WORKS	63
4.3	ASSUMPTIONS AND PRELIMINARIES	66
4.3.1	<i>Sensor Deployment and Network Model</i>	66
4.3.2	<i>Energy Model and Observations</i>	66
4.3.3	<i>Basic Terms and Definitions</i>	68
4.3.4	<i>Security Assumptions and Threat Model</i>	69
4.3.5	<i>Design Goals</i>	70
4.4	SECURE ENERGY-EFFICIENT ROUTING PROTOCOL (SERP).....	70
4.4.1	<i>Tree Construction and OHC Initialization Phase</i>	71
4.4.2	<i>Network Operation and Secure Data Transmission Phase</i>	74
4.4.3	<i>Optional Key Refreshment</i>	77
4.4.4	<i>Repairing a Broken Path and OHC Re-Initialization</i>	78
4.5	SIMULATION RESULTS AND PERFORMANCE ANALYSIS	80
4.5.1	<i>Simulation</i>	80
4.5.2	<i>Storage Requirement for One-way Hash Chain</i>	84
4.5.3	<i>Security Analysis</i>	85
4.5.3.1	<i>Base Station Detection</i>	86
4.5.3.2	<i>Detection by the Intermediate Nodes</i>	86
4.6	SUMMARY	89
CHAPTER 5 CONCLUSIONS AND FUTURE WORKS		90

BIBLIOGRAPHY.....	93
--------------------------	-----------