

# **Securing Emerging Wireless Systems**

## **Lower-Layer Approaches**

Yingying Chen • Wenyuan Xu • Wade Trappe •  
YanYong Zhang

# Securing Emerging Wireless Systems

Lower-Layer Approaches

Yingying Chen  
Stevens Institute of Technology  
Hoboken, NJ  
USA

Wenyuan Xu  
University of South Carolina  
Columbia, SC  
USA

Wade Trappe  
Rutgers University  
North Brunswick, NJ  
USA

Yanyong Zhang  
Rutgers University  
North Brunswick, NJ  
USA

ISBN 978-0-387-88490-5

e-ISBN 978-0-387-88491-2

Library of Congress Control Number: 2008936474

© 2009 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of going to press, 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.com

*To Our Families*

# Preface

We live in an increasingly wireless world and, even though the benefits of tetherless communication are sure to attract a plethora of new applications and help bring communication to those who were never before connected to the broader world, these very same benefits can also serve as the means to cause damage upon individuals, enterprises and governments. Unlike traditional wired communication, where physically protecting the medium is, to a large part, possible by running cables underground and wires in walls, wireless communication is not able to physically protect in the conventional sense. Sure, wireless access points are placed in buildings that may be locked, or cellular basestations are protected by fences and security cameras, but the medium itself is trivially open to a broad array of threats and thus securing wireless communication necessitates a collection of tools that can suitably protect the wireless medium.

This book is about security for wireless networks. However, whereas most conventional approaches to security focus on *cryptographic* solutions that are applied in building families of interconnected network security protocols, this book instead focuses on complementary techniques that aim to invoke unique properties of wireless communications in order to add security to wireless systems.

In order to place this book in an appropriate context, it is perhaps best to think of a simple analogy. Consider a cocktail party where two people, Alice and Bob in the usual parlance of the security community, are trying to have a conversation. Their vocal chords create an audio waveform that travels through the air and which can be heard by others who are close enough to Alice and Bob. Their voices correspond to wireless communication signals,

which propagate in all directions. If Alice and Bob want to make certain that there are no eavesdroppers, they must communicate in a way to make certain that others won't be able to hear or decipher their conversation. Another concern that they might have is that there may be an imposter in the room, seeking to imitate Alice, when starting a conversation with Bob. For such masquerading or spoofing attacks, Bob must use some information specific to Alice, such as her previous location or even some unique aspect of her voice, in order to discern between legitimate and illegitimate conversations. Or, yet another concern that Alice and Bob may have is that there may be unsociable people present at the party who constantly interrupt their conversation. In such cases, Alice and Bob must find a way to excuse themselves and resume their conversation at a different place.

In this book, we deal with these sort of challenges as they apply to wireless communication networks. When considering the standard protocol stack, the aspects that are unique to wireless communications exist at the lower layers of the network stack. Signals and their properties are representative of the physical layer, and take on special characteristics based on their location relative to other wireless devices and to the background environment. It is at the lowest layer of the protocol stack where transmitter location has its greatest impact. The link layer, or medium access control (MAC) layer, must cope with the fact that multiple communications (or conversations) might be carried on at the same time and, just as we have *social protocols* that govern our interactions with each other in a party, wireless networks must also employ suitable MAC protocols to allow for sharing of the wireless medium. Although all communications systems involve localized communications as the basic building block to communicating long distances, many different wireless systems, ranging from sensor networks to ad hoc networks, are characterized by their multi-hop routing protocols. It is at the routing layer where we may direct communication towards or away from certain areas in hopes of achieving improved security or privacy.

Throughout this book we will explore a variety of different *lower layer* strategies for securing wireless networks. Our solutions build largely upon non-cryptographic methods, though occasionally we will employ cryptography in our solutions to make them more robust and resilient to attacks. Applications of cryptography to securing wireless protocols is a necessary component to securing wireless systems, and we thus feel it is important to iterate up front that the methods presented in this book should not be considered a replacement to a well-designed network security protocol. The methods presented in this book will never replace the role of TLS or HTTPS. Instead, it is our viewpoint and belief that wireless systems can only be secured when the full spectrum of tools available to the wireless engineer are brought to bear on the problem. A toolbox that leaves out either cryptography or lower layer characteristics would correspond to an incomplete set of tools that might require more effort in order to achieve

a comparable level of security when cryptography and lower layer security methods are combined.

The approaches to securing wireless systems that exploit lower layer phenomena is an emerging area of research in the wireless security community, and the material presented in this book is, in large part, a compilation of research that was conducted by the authors. However, there are many people who should be acknowledged for their efforts in conducting research that led to some of the material presented in the book. Notably, the authors would like to acknowledge their colleagues Qing Li, Pandurang Kamat, Shu Chen, and Zang Li, who conducted research on forge-resistant relationships, privacy-enhanced routing, and physical layer security as part of their thesis research. Additionally, the authors would like to acknowledge several other collaborators who have helped in different ways to make this research lively: Konstantinos Kleisouris, Eiman Elnahrawy, John-Austin Francisco, Rob Miller, Ke Ma, Richard Martin, Rich Howard, and Ivan Seskar. Each, in their own way, has helped make the material presented in this book possible.

# Contents

<b>Preface</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Book Overview . . . . .	3
<b>I Secure Localization</b>	<b>9</b>
<b>2 Overview of Wireless Localization</b>	<b>11</b>
2.1 Introduction . . . . .	11
2.2 Wireless Localization . . . . .	13
2.3 Secure Localization . . . . .	15
2.4 Location-based Access Control . . . . .	18
2.5 Coping with Identity Fraud . . . . .	19
2.6 Conclusion . . . . .	20
<b>3 On the Robustness of Localization Algorithms to Signal Strength Attacks</b>	<b>23</b>
3.1 Introduction . . . . .	23
3.2 Localization Algorithms . . . . .	26
3.2.1 Point-based Algorithms . . . . .	26
3.2.2 Area-based Algorithms . . . . .	27
3.3 Conducting Signal Strength Attacks . . . . .	29
3.3.1 Signal Strength Attacks . . . . .	29
3.3.2 Experimental Results of Attacks . . . . .	30

3.3.3	Attack Model . . . . .	31
3.4	Measuring Attack Susceptibility . . . . .	32
3.4.1	A Generalized Localization Model . . . . .	32
3.4.2	Attack Susceptibility Metrics . . . . .	34
3.5	Experimental Results . . . . .	36
3.5.1	Experimental Setup . . . . .	36
3.5.2	Localization Angle Bias . . . . .	37
3.5.3	Localization Error Analysis . . . . .	39
3.5.4	Linear Response . . . . .	45
3.5.5	Precision Study . . . . .	51
3.5.6	Robust Multi-device Localization . . . . .	53
3.6	Discussion about Hölder Metrics . . . . .	55
3.7	Conclusion . . . . .	56
<b>4</b>	<b>Attack Detection in Wireless Localization</b>	<b>59</b>
4.1	Introduction . . . . .	59
4.2	Feasibility of Attacks . . . . .	60
4.2.1	Localization Attacks . . . . .	60
4.2.2	Signal Strength Attacks . . . . .	61
4.2.3	Experimental Methodology . . . . .	61
4.3	Generalized Attack Detection Model . . . . .	63
4.3.1	Localization Attack Detection . . . . .	63
4.3.2	Effectiveness . . . . .	63
4.4	Using Least Squares . . . . .	64
4.4.1	Localization . . . . .	64
4.4.2	The Residuals . . . . .	65
4.4.3	The Detection Scheme . . . . .	65
4.4.4	Experimental Evaluation . . . . .	67
4.5	Distance In Signal Space . . . . .	69
4.5.1	Overview . . . . .	70
4.5.2	Finding Thresholds . . . . .	71
4.5.3	Experimental Evaluation . . . . .	71
4.6	Other Test Statistics . . . . .	74
4.6.1	Nonlinear Least Squares (NLS) . . . . .	74
4.6.2	Area Based Probability (ABP) . . . . .	74
4.6.3	Bayesian Networks (BN) . . . . .	75
4.7	Discussion . . . . .	77
4.8	Conclusion . . . . .	78
<b>5</b>	<b>Robust Statistical Methods for Attack-tolerant Localization</b>	<b>81</b>
5.1	Introduction . . . . .	81
5.2	Robust Localization: Living with Bad Guys . . . . .	82
5.3	Robust Methods for Triangulation . . . . .	83
5.3.1	Robust Fitting: Least Median of Squares . . . . .	84

5.3.2	Robust Localization with LMS . . . . .	85
5.3.3	Simulation . . . . .	89
5.3.4	An Efficient Switched LS-LMS Localization Scheme . . . . .	92
5.4	Robust Methods for RF-Based Fingerprinting . . . . .	92
5.5	Conclusion . . . . .	95
<b>6</b>	<b>Spatio-Temporal Access Control by Dual-using Sensor Networks</b>	<b>97</b>
6.1	Introduction . . . . .	97
6.2	Overview of Inverted Sensor Networks . . . . .	98
6.3	Spatio-Temporal Access Control Model . . . . .	100
6.3.1	STAC Components . . . . .	101
6.3.2	Access policies and their representations . . . . .	103
6.4	Centralized Mechanisms for STAC . . . . .	107
6.5	Decentralized Approach for STAC through Inverted Sensor Networks . . . . .	110
6.5.1	Inverted sensor network infrastructure . . . . .	110
6.5.2	Improving the coverage . . . . .	111
6.5.3	Dynamic Encryption and Key Updating . . . . .	115
6.6	Discussion on the operation of inverted sensor networks . . . . .	117
6.6.1	Reduced Contextual Privacy Risk . . . . .	117
6.6.2	Resistant to Positioning Spoofing . . . . .	118
6.6.3	Support of Applications with Little Effort . . . . .	119
6.7	Conclusion . . . . .	120

## II Defending Against Wireless Spoofing Attacks 121

<b>7</b>	<b>Relationship-based Detection of Spoofing-related Anomalous Traffic</b>	<b>123</b>
7.1	Introduction . . . . .	123
7.2	Strategy Overview . . . . .	124
7.3	Forge-resistant Relationships via Auxiliary Fields . . . . .	126
7.3.1	Anomaly Detection via Sequence Number Monotonicity . . . . .	126
7.3.2	One-Way Chain of Temporary Identifiers . . . . .	132
7.4	Forge-resistant Relationships via Intrinsic Properties . . . . .	135
7.4.1	Traffic Arrival Consistency Checks . . . . .	135
7.4.2	Joint Traffic Load and Interarrival Time Detector . . . . .	137
7.5	Enhanced Detectors using Multi-Level Classification . . . . .	138
7.6	Experimental Validation on the ORBIT Wireless Testbed . . . . .	140
7.6.1	Validation of Detection using Sequence Numbers . . . . .	141
7.6.2	Validation of Detection using Traffic Statistics . . . . .	145
7.6.3	Validation of the Joint Traffic Arrival and Traffic Load Detector . . . . .	147
7.7	Conclusion . . . . .	152

<b>8</b>	<b>Detecting and Localizing Wireless Spoofing Attacks</b>	<b>155</b>
8.1	Introduction . . . . .	155
8.2	Feasibility of Attacks . . . . .	156
8.2.1	Spoofing Attacks . . . . .	156
8.2.2	Experimental Methodology . . . . .	157
8.3	Attack Detector . . . . .	159
8.3.1	Formulation of Spoofing Attack Detection . . . . .	159
8.3.2	Test Statistic for Spoofing Detection . . . . .	159
8.3.3	Determining Thresholds . . . . .	161
8.3.4	Performance Metrics . . . . .	161
8.3.5	Experimental Evaluation . . . . .	161
8.4	Localizing Adversaries . . . . .	163
8.4.1	Localization System . . . . .	163
8.5	Architecture Design . . . . .	163
8.5.1	Attack Localizer . . . . .	166
8.5.2	Experimental Evaluation . . . . .	167
8.6	Discussion . . . . .	169
8.7	Conclusion . . . . .	171

### III Defending Against Radio Interference 173

<b>9</b>	<b>A Brief Survey of Jamming and Defense Strategies</b>	<b>175</b>
9.1	Introduction . . . . .	175
9.2	Interference Case Studies . . . . .	176
9.2.1	Non-MAC-compliant Interferer Case Study . . . . .	177
9.2.2	Cross-channel Interference Case Study . . . . .	179
9.2.3	Congestion Case Study . . . . .	182
9.3	Defense: Detection and Evasion . . . . .	187
9.4	Channel Surfing Overview . . . . .	189
9.4.1	Two-Party Radio Communication . . . . .	189
9.4.2	Infrastructured Network . . . . .	191
9.4.3	Ad Hoc Network . . . . .	193
9.5	Spatial Retreats . . . . .	195
9.5.1	Two-Party Radio Communication . . . . .	195
9.5.2	Infrastructured Network . . . . .	198
9.5.3	Ad Hoc Network . . . . .	199
9.6	Conclusion . . . . .	200
<b>10</b>	<b>Jamming Attacks and Radio Interference</b>	<b>201</b>
10.1	Introduction . . . . .	201
10.2	Theoretical Analysis on the Effectiveness of Jamming . . . . .	202
10.2.1	Jamming Impact on Channel Capacity . . . . .	202
10.2.2	Non-isotropic Model for Jamming . . . . .	204

10.3	System Study on Jamming/Interference Models and their Effectiveness . . . . .	206
10.3.1	Jamming Characteristics and Metrics . . . . .	207
10.3.2	Jamming Attack/Radio Interference Models . . . . .	208
10.3.3	Experimental Results . . . . .	210
10.4	Conclusion . . . . .	212
<b>11</b>	<b>Detecting Jamming Attacks and Radio Interference</b>	<b>215</b>
11.1	Introduction . . . . .	215
11.2	Basic Statistics for Detecting Jamming Attacks and Radio Interference . . . . .	216
11.2.1	Signal Strength . . . . .	216
11.2.2	Carrier Sensing Time . . . . .	220
11.2.3	Packet Delivery Ratio . . . . .	223
11.3	Jamming Detection with Consistency Checks . . . . .	224
11.3.1	Signal Strength Consistency Checks . . . . .	225
11.3.2	Location Consistency Checks . . . . .	228
11.4	Conclusion . . . . .	231
<b>12</b>	<b>Channel Surfing: Defending Wireless Networks against Radio Interference:</b>	<b>233</b>
12.1	Introduction . . . . .	233
12.2	System Models . . . . .	234
12.2.1	Our Sensor Communication Paradigm . . . . .	234
12.2.2	Our Interference Model . . . . .	235
12.3	Channel Surfing Overview . . . . .	236
12.4	Channel Surfing Strategies . . . . .	239
12.4.1	Coordinated Channel Switching . . . . .	239
12.4.2	Spectral Multiplexing . . . . .	243
12.5	Sensor Testbed and Metrics . . . . .	249
12.5.1	Testbed Configuration . . . . .	249
12.5.2	Implementation of a Sensor Network . . . . .	250
12.5.3	Building a Jamming-Resistant Network . . . . .	252
12.5.4	Performance Metrics for Channel Surfing . . . . .	252
12.6	Experimental Results . . . . .	254
12.6.1	The Impact of Jamming/Interference . . . . .	254
12.6.2	Coordinated Channel Switching Results . . . . .	256
12.6.3	Spectral Multiplexing Results . . . . .	259
12.6.4	Channel Surfing Discussion . . . . .	262
12.6.5	Channel Following Jammers . . . . .	262
12.7	Conclusion . . . . .	264

## IV Preserving Privacy in Wireless Networks 265

<b>13 Enhancing Source-Location Privacy in Sensor Network Routing</b>	<b>267</b>
13.1 Introduction . . . . .	267
13.2 Asset Monitoring Sensor Networks . . . . .	269
13.2.1 The Panda-Hunter Game . . . . .	269
13.2.2 A Formal Model . . . . .	270
13.2.3 Simulation Model . . . . .	272
13.3 Privacy Protection for a Stationary Source . . . . .	273
13.3.1 Baseline Routing Techniques . . . . .	273
13.3.2 Routing with Fake Sources . . . . .	278
13.3.3 Phantom Routing Techniques . . . . .	281
13.4 Privacy Protection for a Mobile Source . . . . .	286
13.5 Conclusion . . . . .	289
<b>14 Temporal Privacy in Wireless Networks</b>	<b>291</b>
14.1 Introduction . . . . .	291
14.2 Overview of Temporal Privacy in Sensor Networks . . . . .	292
14.2.1 The Baseline Adversary Model . . . . .	294
14.3 Temporal Privacy Formulation . . . . .	295
14.3.1 Temporal Privacy: Two-Party Single-Packet Network	295
14.3.2 Temporal Privacy: Two-Party Multiple-Packet Network	297
14.3.3 Temporal Privacy: Multihop Networks . . . . .	299
14.4 Queuing Analysis of Privacy-Enhancing Buffering . . . . .	299
14.5 RCAD: Rate-Controlled Adaptive Delaying . . . . .	303
14.6 Evaluating RCAD Using Simulations . . . . .	304
14.6.1 Privacy and Performance Metrics . . . . .	304
14.6.2 Simulation Setup . . . . .	305
14.6.3 Simulation Results . . . . .	306
14.6.4 The Adaptive Adversary Model . . . . .	310
14.7 Conclusion . . . . .	312
<b>15 Securing Wireless Systems via Lower Layer Enforcements</b>	<b>313</b>
15.1 Introduction . . . . .	313
15.2 Alice, Bob and Eve Get Physical . . . . .	314
15.3 PHY-Enhanced Authentication . . . . .	316
15.3.1 Channel-based Authentication . . . . .	317
15.3.2 Maintenance of the channel authenticator . . . . .	319
15.4 PHY-Enhanced Confidentiality . . . . .	321
15.4.1 Key Extraction from Channel Estimates . . . . .	321
15.4.2 Key Dissemination via Channel State Masking . . . . .	322
15.4.3 Key Dissemination via Probabilistic Encoding . . . . .	323
15.5 Experimental Validation . . . . .	326
15.5.1 Fundamental Measurements . . . . .	327

15.5.2 Evaluation of PHY Authentication . . . . .	329
15.5.3 Evaluation of PHY Confidentiality . . . . .	330
15.6 Conclusion . . . . .	331
<b>16 Concluding Remarks</b>	<b>333</b>
<b>References</b>	<b>337</b>
<b>Index</b>	<b>357</b>