

# SpringerBriefs in Computer Science

## *Series Editors*

Stan Zdonik  
Peng Ning  
Shashi Shekhar  
Jonathan Katz  
Xindong Wu  
Lakhmi C. Jain  
David Padua  
Xuemin Shen  
Borko Furht  
V. S. Subrahmanian  
Martial Hebert  
Katsushi Ikeuchi  
Bruno Siciliano

For further volumes:  
<http://www.springer.com/series/10028>

Hong Wen

# Physical Layer Approaches for Securing Wireless Communication Systems

 Springer

Hong Wen  
University of Electronic Science  
and Technology of China  
Chengdu  
Sichuan  
People's Republic of China

ISSN 2191-5768                      ISSN 2191-5776 (electronic)  
ISBN 978-1-4614-6509-6            ISBN 978-1-4614-6510-2 (eBook)  
DOI 10.1007/978-1-4614-6510-2  
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2013930686

© The Author(s) 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law. The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, 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 is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Preface

Along with the rapid development of wideband wireless communication networks, wireless security has become a critical concern. Traditionally, in current wired or wireless communication networks, the issue of security is viewed as a whole independent feature addressed above the physical layer and cryptographic protocols are widely used to guarantee the security of the network. And the cryptographic protocols are designed assuming the physical layer has already been established and is error free. However, this assumption is usually impractical in the case of wireless communication. Compared with wireline networks, wireless networks lack a physical boundary due to the broadcasting nature of wireless transmissions. Any receivers nearby can hear the transmissions, and can potentially listen/analyze the transmitted signals, or conduct jamming. This unique physical-layer (PHY) weakness has motivated innovative PHY security designs in addition to, and integrated with, the traditional data encryption approaches.

One of the fundamental issues for PHY security is defined as information theoretic security, i.e., the adversary's received signal gives no more information for eavesdropping than legitimate receiver. The information-theoretic secrecy was first introduced by Shannon. "Perfect Secrecy" is defined by requiring of a system that after a cryptogram is intercepted by the enemy the a posteriori probabilities of this cryptogram representing various messages be identically the same as the a priori probabilities of the same messages before the interception. It is shown that perfect secrecy is possible by two approaches. First, perfect secrecy is possible but requires, if the number of messages is finite, the same number of possible keys. Second, perfect information theoretic secrecy requires that the signal  $Z$  received by the eavesdropper does not provide any additional information about the transmitted message  $W$ . Therefore, the build-in security of PHY security is also defined as: no secret keys are required before transmission.

In information-theoretic secrecy, channel noise plays a role of randomness resource. This book gives a review of the previous outstanding works of PHY security, and then provides the recent achievements on the confidentiality and authentication for wireless communications systems by channel identification. The first chapter introduces the PHY confidentiality and authentication concept. [Chapter 2](#) introduces a practical approach to build unconditional confidentiality for

wireless communication security by feedback and error correcting code. In wireless channels, multiple antennas can increase system robustness against fading, and also transmission rates, as well as providing valid ways to realize information-theoretic secrecy. A framework of PHY security based on space time block code (STBC) MIMO system is introduced in [Chap. 3](#). Innovative cross-layer security designs with both PHY security and upper-layer traditional security techniques are desirable for wireless networks. In this chapter, we also present a scheme that combines cryptographic techniques implemented in higher layers with the physical layer security approach using redundant antennas of MIMO systems to provide stronger security for wireless networks. The channel responses between communication peers have been explored as a form of fingerprint with spatial and temporal uniqueness. [Chapters 4](#) and [5](#) fulfill this idea and develop a new lightweight method of channel identification for Sybil attack and node clone detection in wireless sensor networks (WSNs).

# Acknowledgments

The author wishes to acknowledge the partial support of the NSFC (Project No. 61032003, 61071100 and 61271172), NCET (Project No. NCET-09-0266), and the National Important Special Fund Project of China (Project No. 2011ZX03002-005-03). The author is thankful to Master candidates: Mr. Guo Chao Liu and Ms. Xiao Cheng for their contribution to editing work and figure reproduction. The author would also like to thank Prof. Bin Wu for his careful proof reading.

Very special thanks to Prof. Sherman Shen who made this book possible.

# Contents

<b>1</b>	<b>Introduction for PHY Security</b> . . . . .	1
1.1	Introduction . . . . .	1
1.2	Outline . . . . .	3
<b>2</b>	<b>Unconditional Security Wireless Communication</b> . . . . .	5
2.1	Perfect Security Model . . . . .	6
2.2	Powerful Multi-round Feedback for Build Wiretap Channel Model . . . . .	7
2.2.1	Two Way Communication for Build-in Wiretap Channel . . . . .	7
2.2.2	Multi-round Feedback for Build Wiretap Channel Model . . . . .	9
2.3	Performance with LDPC Codes . . . . .	11
2.3.1	The Threshold Property of LDPC Codes . . . . .	12
2.3.2	Some Performance Results . . . . .	14
2.4	Security Code . . . . .	14
2.4.1	Coset Security Code . . . . .	14
2.4.2	Unconditional Security Communication Model . . . . .	18
2.4.3	Some Performance Results . . . . .	19
2.5	Summary . . . . .	22
<b>3</b>	<b>MIMO Based Enhancement for Wireless Communication Security</b> . . . . .	23
3.1	MIMO Cross-Layer Secure Communication Based on STBC . . . . .	24
3.1.1	Overview of Alamouti Code . . . . .	24
3.1.2	Distort Signal Set Design for Security Purpose . . . . .	25
3.1.3	The Action of the Legitimate Receiver . . . . .	27

3.2	Security Performance Analysis . . . . .	29
3.2.1	Attackers Action with Multiple Receive Antennas . . . . .	29
3.2.2	Comparing the Proposed New Models with the Traditional Stream Cipher Encryption System . . . . .	30
3.3	The Simulation Performance of the Proposed Method . . . . .	32
3.3.1	The Performance Properties . . . . .	32
3.3.2	The Secret Capacity . . . . .	34
3.4	Summary . . . . .	35
<b>4</b>	<b>Physical Layer Assisted Authentication for Wireless Sensor Networks . . . . .</b>	<b>37</b>
4.1	System Model . . . . .	37
4.2	Physical Channel Identification . . . . .	39
4.2.1	Physical Layer Channel Response Extraction . . . . .	39
4.2.2	Physical Layer Authentication Based on LRT . . . . .	40
4.2.3	Physical Layer Authentication Based on SPRT . . . . .	41
4.3	Physical Layer Assisted Authentication Based on PKI . . . . .	42
4.3.1	Physical Layer Assisted Authentication Principle . . . . .	42
4.3.2	Application Examples . . . . .	43
4.4	Physical Layer Assisted Authentication Based on SCA . . . . .	51
4.4.1	Physical Layer Assisted Authentication Principle . . . . .	51
4.4.2	Application Examples . . . . .	54
4.5	Summary . . . . .	57
<b>5</b>	<b>Detection of Node Clone and Sybil Attack Based on CI Approach . . . . .</b>	<b>59</b>
5.1	Detection Node Clone Based on Channel Identification . . . . .	60
5.1.1	Network Model and Security Goals . . . . .	60
5.1.2	Node Clone Detection Principle Based on CI . . . . .	61
5.1.3	Determinant of Suspect Nodes . . . . .	63
5.1.4	Performance Results . . . . .	67
5.2	Detection Sybil Nodes Based on Channel Identification . . . . .	70
5.2.1	Sybil Nodes Detection Principle Based on CI . . . . .	72
5.2.2	Determinant of Suspect Nodes . . . . .	73
5.2.3	Performance Results . . . . .	74
5.3	Summary . . . . .	78
	<b>References . . . . .</b>	<b>79</b>