SPRINGER BRIEFS IN ELECTRICAL AND
COMPUTER ENGINEERING · SIGNAL PROCESSING

Y.-W. Peter Hong · Pang-Chang Lan
C.-C. Jay Kuo

Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems

Springer

SpringerBriefs in Electrical and Computer Engineering

Signal Processing

Series Editors

Woon-Seng Gan, Singapore
C.-C. Jay Kuo, Los Angeles, USA

For further volumes:
http://www.springer.com/series/11560

Y.-W. Peter Hong · Pang-Chang Lan
C.-C. Jay Kuo

Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems

Springer

Y.-W. Peter Hong
Department of Electrical Engineering
National Tsing Hua University
Hsinchu
Taiwan, R.O.C.

C.-C. Jay Kuo
Department of Electrical Engineering
University of Southern California
Los Angeles, CA
USA

Pang-Chang Lan
Department of Electrical Engineering
University of Southern California
Los Angeles, CA
USA

ISSN 2196-4076 ISSN 2196-4084 (electronic)
ISBN 978-981-4560-13-9 ISBN 978-981-4560-14-6 (eBook)
DOI 10.1007/978-981-4560-14-6
Springer Singapore Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013944087

© The Author(s) 2014
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)

To my beloved family

—Peter

Dedicated to my parents

—Pang-Chang

In memory of my beloved father

—Jay

Preface

Physical layer secrecy has received much attention in recent years, especially in wireless communications, due to the rapidly increasing data traffic and high demand for ubiquitous connectivity. Different from conventional cryptographic approaches used to address wireless security issues, physical layer secrecy utilizes channel coding and signal processing techniques to communicate secret messages between the source and the destination while maintaining confidentiality against the eavesdropper. These studies originate from the information theory literature, where the focus is often to determine the existence of channel codes that can achieve this task or to derive the fundamental limit on the maximum code rate that can be applied reliably under the secrecy constraint (i.e., the secrecy capacity). In particular, information-theoretic results have shown that the secrecy capacity increases with the difference between the reception quality at the destination and that at the eavesdropper. Motivated by this result, signal processing approaches have been developed in both the data transmission and channel estimation phases to maximize the signal quality difference between the destination and the eavesdropper. In general, both coding and signal processing aspects of the problem must be taken into consideration in order to achieve the secrecy capacity. However, when the optimal joint design is unknown, signal processing techniques can also be used to help increase the achievable secrecy rate or reduce the complexity of the channel coding operations. These approaches are especially interesting in multi-antenna wireless systems, where the spatial degrees of freedom can be exploited to further enhance secrecy.

This book provides an overview of signal processing approaches that can be used to enhance physical layer secrecy in multi-antenna wireless systems. Specifically, in the data transmission phase, we review secrecy beamforming and precoding techniques that can be used to not only strengthen the signal at the destination, but also reduce the information leakage to the eavesdropper. We also consider the use of artificial noise along with the transmission of the information signal to further degrade the reception quality at the eavesdropper. Moreover, we further extend the use of these techniques to distributed antenna or relay systems where the multiple antennas may not be located at a single terminal. The additional spatial degrees of freedom provide more design flexibility and performance gains, but may also increase the security threats due to additional transmission required for coordination among the distributed terminals and also due to the trustworthiness of system members. In terms of channel estimation, we review the so-called discriminatory channel estimation scheme which utilizes the design of artificial noise aided training signals to increase the difference between the effective signal quality at the destination and that at the eavesdropper. In this case, the desired signal quality discrepancy is enhanced even before the transmission of the confidential message and need only be done once every coherence interval (instead of every symbol period).

This book is divided into 6 chapters. Chapter 1 introduces the importance and challenge of achieving secrecy in wireless systems, and provides a brief mention of the background on different notions of physical lay secrecy. Chapter 2 briefly summarizes the basic results in information-theoretic secrecy. In Chapter 3, secrecy beamforming and precoding designs along with the use of artificial noise are described as ways to effectively enhance the desired signal quality discrepancy in the data transmission phase. In Chapter 4, these techniques are extended to distributed antenna or relay systems. In Chapter 5, discriminatory channel estimation schemes are described as methods to achieve signal quality discrepancy in the channel estimation phase. Finally, in Chapter 6, several applications of physical layer secrecy and their respective research directions are further introduced.

The purpose of this book is to highlight the role of signal processing in achieving secrecy in the physical layer, and to provide researchers and graduate students, who are interested in pursuing research in this area, an overview of the standard techniques known today and a basic understanding of the challenges that may arise in this area. We would like to remark that, due to the vast literature in this area, it is not possible to give a comprehensive treatment of the material in the literature. However, we hope that the materials included in this book provide a logical treatment of the basic results and allow researchers and graduate students to gain sufficient knowledge to pursue research in this area.

Hsinchu, Taiwan, May 2013
Los Angeles, USA, May 2013

Y.-W. Peter Hong
Pang-Chang Lan
C.-C. Jay Kuo

Acknowledgments

This work was supported in part by the National Science Council, Taiwan, under grant NSC 100-2628-E-007-025-MY3. The authors would also like to thank Ta-Yuan Liu, Yu-Ching Chen, Li-Ren Chen, and Lin-Ming Huang for extensive proof-reading of the manuscript.

Contents

Chapter 1
Introduction

Abstract This chapter provides a brief introduction of security issues that may arise in wireless communication systems and describe physical layer techniques that can be used to address these issues. Different notions of physical layer secrecy are introduced, including keyless transmission of confidential messages (which is the focus of this book), channel-based secret key generation, and signal transmissions with low probability of interception and detection. Backgrounds on these techniques as well as an overview of the book content are provided.

Keywords Security · Cryptography · Physical layer secrecy · Secret key generation · Low probability of interception (LPI) · Low probability of detection (LPD).

1.1 Security in Wireless Communication Systems

With the increasing demand for mobility and ubiquitous connectivity, wireless communications is playing an integral part in our daily lives and is having a significant impact on society. Confidential and private information, such as e-banking, e-commerce, and medical information, is part of the mass data being transmitted over the wireless medium. However, due to the broadcast nature of wireless transmissions, communication over the wireless medium is often vulnerable to signal interception or eavesdropping by unauthorized receivers, as depicted in Fig. 1.1. Security and privacy issues have thus drawn much attention from both industry and academia, but many problems remain to be open and challenging.

In general, security in wireless networks may involve many tasks, including confidentiality, authentication, integrity, access control, and availability, etc. [1, 2]. Confidentiality refers to the prevention of unauthorized disclosure of information; authentication refers to the confirmation of the identity of different terminals; integrity ensures that the transmitted information is not illegally modified; access control and availability prevent denial-of-service (DoS) attacks. Conventionally, these

Y.-W. P. Hong et al., *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*, SpringerBriefs in Signal Processing, DOI: 10.1007/978-981-4560-14-6_1, © The Author(s) 2014

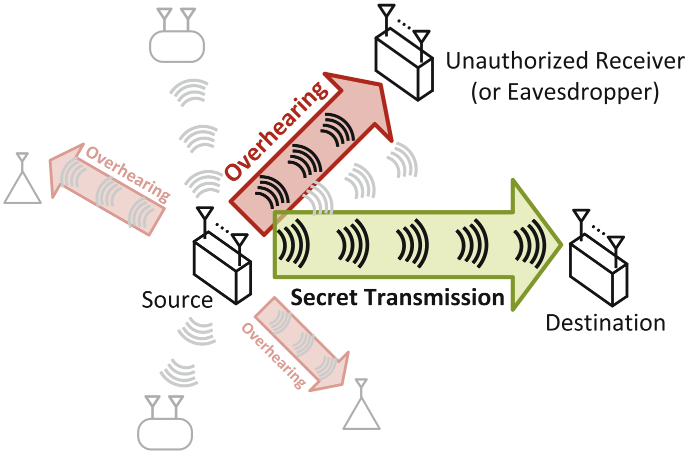

Fig. 1.1 The risk of overhearing in secret communications over the wireless medium

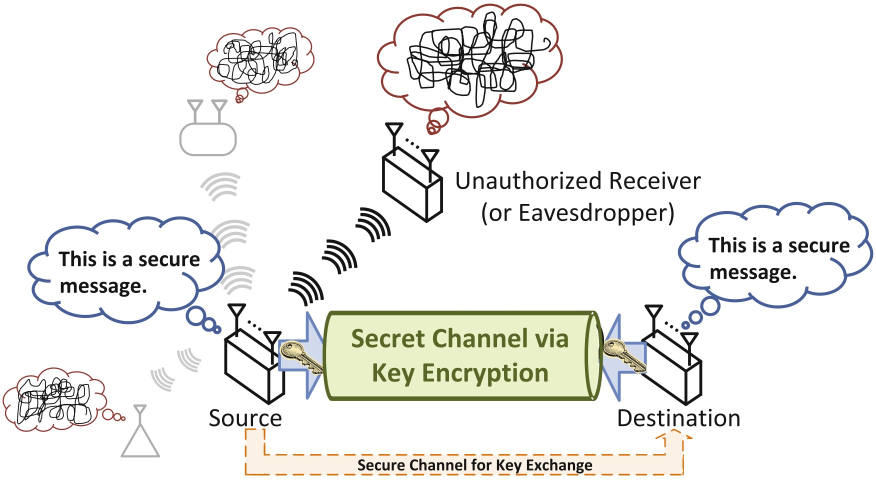
Unauthorized Receiver
(or Eavesdropper)
This is a secure message.
This is a secure message.
Secret Channel via Key Encryption
Source
Destination
Secure Channel for Key Exchange

Fig. 1.2 Illustration of symmetric-key cryptography, which is used to construct a secrecy channel between the source and the destination for transmission of a confidential message, but requires a secure channel or protocol for the exchange of secret keys

issues have been addressed mostly in the upper layers of the network protocol stack using cryptographic encryption and decryption methods, e.g., data encryption standard (DES) [3] and advanced encryption standard (AES) [4]. When symmetric-key cryptosystems are employed, as illustrated in Fig. 1.2, a common private key is to be shared by two users and is used to encrypt and decrypt the confidential message. However, this requires a secure channel or protocol, such as the Diffie-Hellman [5] key exchange protocol, for the exchange of shared secret keys. The difficulties in secret key distribution and management [6] lead to security vulnerabilities in wireless systems. Alternatively, public-key cryptosystems, such as RSA [7], allow the use of a public key for encryption and a separate private key for decryption. The public key is available to all users whereas the private key is known only to the receiver. However, the security achieved by the cryptographic methods mentioned above relies on the computational hardness of decrypting the message when the secret key is not available. As the computational power increases, e.g., with the development of quantum computers, the computational hardness of certain mathematical problems, for which the encryption and decryption are based on, may no longer hold, causing many current cryptosystems to break down.

In recent years, many coding and signal processing techniques in the physical layer have been developed to support and to further enhance security in wireless systems. These techniques include, e.g., keyless physical layer secrecy transmission schemes [8–10], channel-based secret key generation schemes [11], and signal designs with low probability of interception and detection [12]. Different from conventional cryptographic methods, where the fast channel variations and the broadcast nature of the wireless medium may cause additional challenges to their design, these physical layer techniques exploit (rather than avoid) properties of wireless transmissions to better secure the communication channel. In particular, spatial variations of the channel are utilized to ensure that signals received at different locations are not the same; temporal variations of the channel are essential for destinations (that, on average, experience worse channel conditions than the eavesdropper) to temporarily experience better channel conditions at certain time instants; and the broadcast nature of wireless transmissions makes possible the emission of jamming signals to degrade the eavesdropper's reception. These physical layer techniques are used to support and complement security protocols in the upper layers of the network protocol stack, but are not meant as replacements for conventional cryptographic approaches. These physical layer techniques are mentioned in more detail in the following section.

It is worthwhile to note that, while many of the security issues mentioned above (e.g., authentication, integrity, and availability) are equally important, this book focuses on the issue of maintaining confidentiality of information transfer. Moreover, we consider only the case of passive adversaries, that only aim to intercept the confidential message or to detect the transmission activities but do not actively transmit signals. In cases with active adversaries, different attacks, such as jamming, impersonation, and message modification, can also be performed to limit the achievable secrecy. However, these topics are beyond the scope of this book. Readers are referred to [1, 2] for further discussions on these topics.

1.2 Background on Physical Layer Secrecy

In this section, we discuss briefly the three physical layer secrecy techniques mentioned in the previous section, namely, keyless physical layer secrecy transmission, channel-based secret key generation, and signal designs with low probability of interception and detection. Special emphasis is given to keyless physical layer secrecy transmissions as it is the focus of this book.

1.2.1 Keyless Physical Layer Secrecy Transmissions

Keyless physical layer secrecy transmission schemes were first studied in the context of wiretap channels by Wyner in [8], and was later extended to Gaussian channels in [9] and to broadcast channels with confidential messages in [10]. Here, confidential messages are transmitted using channel coding schemes (with random binning and channel prefixing techniques) to allow for reliable decoding at the destination while achieving substantial confusion at the eavesdropper. Early works in this field appeared mostly in the information theory literature and were mostly concerned with the so-called secrecy capacity, which is defined as the maximum achievable rate between the source and the destination while ensuring that no information can be inferred by the eavesdropper. It was shown that a non-zero secrecy capacity can be achieved between the source and the destination if the channel to the destination is better than that to the eavesdropper. These studies demonstrated the possibility of using properties of physical channels (without the use of secret keys) to ensure confidentiality of the transmitted messages against the eavesdropper. This avoids the inherent vulnerabilities caused by key distribution and management in conventional cryptographic systems.

Motivated by the emergence of wireless applications, keyless physical layer transmission schemes were also examined in wireless systems, where the dynamic nature of fading channels must also be taken into consideration [13, 14]. Specifically, it was shown in [13, 14] that, by exploiting the temporal variations of the channel, a positive secrecy rate can be achieved even when the average channel to the destination is of lower average quality than that to the eavesdropper. Extensions to multiple-input multiple-output (MIMO) wiretap channels, where the source, the destination, and the eavesdropper are all equipped with multiple antennas, were also examined recently in, e.g., [15–18]. The additional degrees of freedom provided by the multiple antennas in this case can be exploited to further enhance secrecy in the physical layer. In particular, as shown in [16, 18], this can be done by first employing secrecy precoding techniques to decompose the channel into multiple parallel sub-channels and by using wiretap codes over sub-channels that yield better quality to the destination than to the eavesdropper. However, this scheme requires perfect knowledge of the main and eavesdropper channels at the source, which may not be achievable in practice. When the eavesdropper's channel is unknown, artificial noise (AN) can also be emitted on top of the information-bearing signal to disrupt the reception at the eavesdropper, as illustrated in Fig. 1.3. With multiple antennas at the source, AN can be placed in dimensions that cause least interference at the destination. By doing so, the difference between the signal qualities at the destination and the eavesdropper (and, thus, the achievable secrecy rate) can be effectively increased. The desired spatial degrees of freedom can also be provided by relays or distributed antenna systems, and secrecy precoding and AN techniques can be applied accordingly.

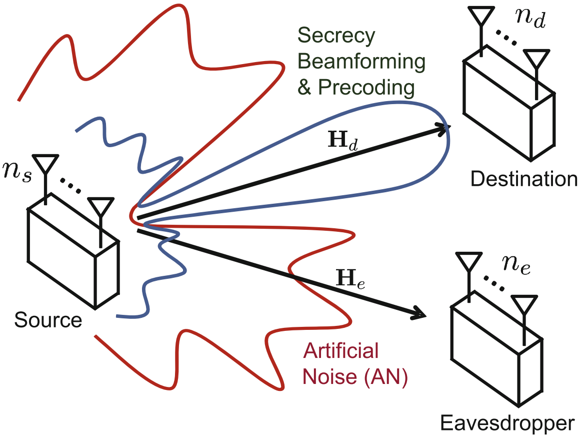

Fig. 1.3 Illustration of secrecy beamforming/precoding and artificial noise usage in a wireless multi-antenna system in the presence of an eavesdropper

1.2.2 Channel-Based Secret Key Generation

Channel-based secret key generation schemes [11] utilize unique characteristics of the channel between two users (i.e., the source and the destination) as the common randomness to generate symmetric keys locally at the two terminals. Here, channel knowledge is typically obtained by having the two terminals transmit training sequences to each other and by having the terminals perform channel estimation locally based on their received training signals. By assuming that the channel between the two terminals is reciprocal, the channel estimate at both ends will be approximately the same and can be utilized as the common random seed for secret key generation. However, these channel estimates are often subject to discrepancies caused by noise and may lead to key disagreement. Hence, key reconciliation and privacy amplification methods are necessary for error detection and correction. Since an eavesdropper located more than half a wavelength away will experience independent fading, it will not be able to infer the common secret key generated by the source and the destination.

The use of common randomness to generate secret keys at different terminals was first examined in [19, 20]. The use of channel characteristics as the common randomness was examined more recently, e.g., in [21–24]. These schemes utilize quantization of the amplitude and/or phase of the channel to mitigate the effect of noise and to determine the common index of the secret key at the two terminals. Similar concepts were also utilized to generate group keys in [25]. The performance of channel-based secret key generation schemes is often measured by the key generation rate, the key entropy, and the key disagreement probability. These three measures are often limited by properties of the physical channel, such as the channel coherence time and the channel quality. Techniques that can achieve the best tradeoff between