Wireless Networks

Yulong Zou
Jia Zhu

# Physical-Layer Security for Cooperative Relay Networks

Springer

# Wireless Networks

*Series Editor:*
Xuemin (Sherman) Shen
*University of Waterloo, Waterloo, Ontario, Canada*

More information about this series at http://www.springer.com/series/14180

Yulong Zou • Jia Zhu

# Physical-Layer Security for Cooperative Relay Networks

Springer

Yulong Zou
Nanjing University of Posts
and Telecommunications
Nanjing, Jiangsu, China

Jia Zhu
Nanjing University of Posts
and Telecommunications
Nanjing, Jiangsu, China

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-319-31173-9 ISBN 978-3-319-31174-6 (eBook)
DOI 10.1007/978-3-319-31174-6

Library of Congress Control Number: 2016936582

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

# Preface

Recently, cybercriminal activities in wireless communications systems are growing due to the fact that more and more emerging malware programs (also known as computer viruses) are targeted on the mobile terminals. Accordingly, an increasing attention has been paid to the research of wireless security against various malicious attacks. The radio propagation inherits the broadcast nature, leading to any receivers within the coverage area of a radio transmitter being capable of overhearing the wireless transmission. This makes the wireless communication systems extremely vulnerable to the eavesdropping attack. Typically, cryptographic techniques relying on secret keys are employed for preventing an eavesdropper from interpreting the wireless transmissions.

However, classic cryptographic techniques including both public-key cryptography and symmetric-key cryptography are only computationally secure and rely upon the hardness of their underlying mathematical problems. Cryptography security would be significantly compromised if an efficient method of solving its underlying mathematical problem was to be discovered. Moreover, conventional secret key exchange relies on a trusted key management center, which may not be always applicable in wireless networks. To this end, physical-layer security is emerging as a promising paradigm to secure wireless communications by exploiting the physical-layer characteristics of wireless channels. It is proved from an information-theoretic perspective that perfect secrecy can be achieved if the wiretap channel from a source to an eavesdropper is a degraded version of the main channel from the source to its intended destination. However, due to the time-varying fading effect of wireless channels, the main channel may experience a deep fade, which makes the perfect secrecy become impossible in some cases.

This book presents the concept and practical challenges of physical-layer security as well as examines recent advances in cooperative relaying for the wireless physical-layer security. In Chap. 1, we first review a range of physical-layer security techniques, namely, information-theoretic security, artificial-noise-aided security, security-oriented beamforming, and diversity-assisted security, along with an in-depth discussion of cooperative relaying techniques for wireless networks. Next, Chap. 2 investigates the physical-layer security for a wireless network consisting of a source and a destination with the aid of multiple relays, where only the single "best" relay is selected among the multiple relays to assist the source-destination transmission against eavesdropping. In Chap. 3, we then examine joint relay and jammer selection for enhancing the wireless physical-layer security of the source-destination transmission with the help of multiple intermediate nodes in the presence of an eavesdropper. In the joint relay and jammer selection, an intermediate node is selected to act as the relay for assisting the source-destination transmission and another intermediate node is chosen to act as the jammer for interfering with the eavesdropper.

Additionally, Chap. 4 explores the security-reliability tradeoff (SRT) for a wireless network, where security and reliability are measured by using the intercept probability experienced by the eavesdropper and outage probability encountered at the legitimate destination, respectively. We present two relay selection schemes for the SRT improvement, namely, single-relay selection (SRS) and multi-relay selection (MRS). To be specific, in the SRS scheme, only the single "best" relay is selected to assist the source-destination transmission, whereas in the MRS scheme, multiple relays are invoked to participate in forwarding the source signal to the destination. Finally, Chap. 5 re-examines the joint relay and jammer selection from the SRT perspective, where a relay is used to help the source transmission enhance wireless reliability and a friendly jammer is adopted to improve wireless security through the emission of the artificial noise for confusing the eavesdropper. It is shown that with an increasing number of relays and jammers, the security and reliability of wireless communications relying on the joint relay and jammer selection can be significantly enhanced concurrently.

Nanjing, China
January 2016

Yulong Zou
Jia Zhu

# Contents

# Acronyms

| | |
|---|---|
| 3G | Third generation |
| AF | Amplify-and-forward |
| AP | Access point |
| AWGN | Additive white Gaussian noise |
| BS | Base station |
| CDF | Cumulative distribution function |
| CF | Compress-and-forward |
| CRC | Cyclic redundancy check |
| CSI | Channel state information |
| DF | Decode-and-forward |
| DoS | Denial-of-service |
| GSVD | Generalized singular value decomposition |
| I.I.D | Independent identically distributed |
| LoS | Line-of-sight |
| LTE | Long-term evolution |
| LTE-A | Long-term evolution advanced |
| MAC | Medium access control |
| MER | Main-to-eavesdropper ratio |
| MIMO | Multiple-input multiple-output |
| MISOME | Multiple-input single-output multiple-eavesdropper |
| MRS | Multi-relay selection |
| OFDMA | Orthogonal frequency-division multiple access |
| PDF | Probability density function |
| SNR | Signal-to-noise ratio |
| SRS | Single-relay selection |
| SRT | Security-reliability tradeoff |
| TDMA | Time-division multiple access |

# Chapter 1
# Introduction

**Abstract** Due to the broadcast nature of radio propagation, wireless transmissions are accessible to any eavesdroppers and thus become extremely vulnerable to the eavesdropping attack. Physical-layer security is emerging as a promising paradigm to achieve the information-theoretic secrecy for wireless networks. This chapter introduces the current research on physical-layer security for wireless networks. We first discuss a range of physical-layer security techniques, including the information-theoretic security, artificial noise aided security, security-oriented beamforming, and diversity assisted security approaches. Then, we present an overview on the cooperative relaying methods for wireless networks, namely the orthogonal relaying, non-orthogonal relaying and relay selection. Additionally, the application of cooperative relaying to wireless physical-layer security is also discussed for protecting the wireless communications against eavesdropping.

## 1.1 Wireless Physical-Layer Security

Recent years have witnessed the widespread use of smartphones for accessing various wireless networks, such as the third-generation (3G), long-term evolution (LTE) and LET-advanced (LTE-A) mobile communications systems as well as the Wi-Fi [1]. Meanwhile, it has been reported that an increasing number of wireless terminals are compromised by the adversary for carrying out cybercriminal activities, including malicious hacking, data forging, financial information theft, and so on. Moreover, as discussed in [2] and [3], the broadcast nature of radio propagation makes the wireless communication systems extremely vulnerable to the eavesdropping attack. As shown in Fig. 1.1, an access point (AP) is considered to transmit data packets to its associated legitimate users, which can be readily overheard by an eavesdropper as long as it lies in the coverage area of AP.

Traditionally, cryptographic techniques relying on secret keys were adopted for preventing an eavesdropper from interpreting the wireless data transmissions. There are two main types of cryptographic techniques, namely the public-key cryptography and symmetric-key cryptography, which are however only computationally secure and rely upon the hardness of their underlying mathematical problems [4, 5]. The security of a cryptographic approach would be significantly compromised, if an efficient method of solving its underlying hard mathematical problem was to be

Y. Zou, J. Zhu, *Physical-Layer Security for Cooperative Relay Networks*,
Wireless Networks, DOI 10.1007/978-3-319-31174-6_1