

Securing Wireless Communications at the Physical Layer

Ruoheng Liu · Wade Trappe
Editors

Securing Wireless Communications at the Physical Layer



Springer

Editors

Ruoheng Liu
Princeton University
Department of Electrical Engineering
Olden Street
Princeton, NJ 08544
USA
rliu@princeton.edu

Dr. Wade Trappe
Rutgers University
Technology Centre of New Jersey
Wireless Information
671 Route 1 South
North Brunswick, NJ 08902
USA
trappe@winlab.rutgers.edu

ISBN 978-1-4419-1384-5 e-ISBN 978-1-4419-1385-2

DOI 10.1007/978-1-4419-1385-2

Springer New York Dordrecht Heidelberg London

Library of Congress Control Number:

© Springer Science+Business Media, LLC 2010

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.

Cover design:

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

To Our Families

Preface

Securing communications is a challenging task. A first attempt at security involves learning basic cryptography, and applying encryption algorithms to make messages unintelligible to adversaries. However, rarely is the task of securing a message exchange so simple. When one steps back and contemplates how to secure the exchange of communications, one realizes that the challenge is fundamentally one of building a *complete* solution. For example, one must ensure that all entities involved have proper and authenticated cryptographic material, or one must ensure that one verifiably knows to whom one is communicating, or one must understand how the communication process takes place so as to make certain there are no vulnerabilities introduced by the communication process itself.

This last issue, namely that security methods are often built without consideration to how communication takes place, represents a fundamental gap where much of modern security research has fallen short. The security literature is filled with a mass of articles on cryptographic primitives and, although there are still many theoretical hurdles to be overcome by the cryptographic community, most of these short comings are academic and there are now numerous textbooks on cryptography that can provide the basic introduction needed to employ cryptographic primitives. On the other side of the coin, the security literature is also filled with a mass of articles devoted to building secure protocols and, similarly, there are now numerous textbooks on computer security that provide the instruction needed to design secure protocols. Unfortunately, the issue of how communication takes place or, more specifically, whether there are any specific issues that might arise or be circumvented because message exchanges are taking place on one medium versus another (e.g., wireless communication versus wired communication), is generally neglected.

In fact, although the layered approach to communication system design, as corresponds to the general Open Systems Interconnection (OSI) reference model, is often referred to in the design of network security protocols, the resulting protocols tend to be layer-specific and ignore the most fundamental of communication layers—the physical layer, whereby devices communicate through the encoding and modulation of information into waveforms. This is truly a sad situation, as it means that the approaches taken to secure modern communication systems are incomplete and, as

is often chanted as a mantra in the security circles, we should be concerned because “a system is only as strong as the weakest link.”

In response to this apparent shortcoming, this anthology presents a collection of chapters devoted to recent research results examining security issues at the physical layer. In particular, all of the authors amassed in this collection take the viewpoint that the physical layer of wireless communications should be considered as unique and different from the physical layer of other communication systems, and thus the challenges of securing the physical layer should take into account the special properties of the wireless medium. Throughout this book, a common theme that frequently emerges is that, in the rich multipath environment typical of wireless scenarios, the channel response of the medium along any transmit-receive path is frequency-selective (or in the time domain, dispersive) in a way that is location-specific (implying that channel responses decorrelate rapidly from one transmit-receive path to another if the paths are separated by the order of an RF wavelength). These unique space, time, and frequency characteristics of the wireless physical layer serve as a powerful basis for building new security services at the physical layer.

The chapters that we have assembled are contributions from a broad variety of research groups examining security issues at the physical layer of wireless systems. In selecting the contributions, we have sought to cover a spectrum of security issues (ranging from confidentiality to authentication to trustworthiness), as well as both theoretical and practical aspects of securing the physical layer. As such, the chapters in this book have been loosely organized thematically. We start by examining the issue of confidentiality at the physical layer. Confidentiality typically involves algorithms, like ciphers, and is concerned with the guarantee that information exchange is only able decipherable by legitimate entities. In the context of physical layer security, we are more concerned with mechanisms that use the wireless medium to support the confidential exchange of messages. **Typically, though, the resulting mechanisms operate at communication rates that are much lower than their conventional *non-secret* counterparts, and thus physical layer confidentiality mechanisms should be used in support of conventional confidentiality mechanisms. For example, one might use physical layer confidentiality mechanisms to secretly exchange or establish conventional cryptographic keys.**

Confidentiality mechanisms at the physical layer may be further decomposed into methods that secretly *disseminate* information using the properties of the wireless medium and methods that *extract* secret information from the wireless medium. We have arranged the confidentiality chapters by first examining the issue of disseminating information secretly. Most of these chapters explore the fundamental theoretical aspects related to secrecy dissemination, and several fundamental observations emerge. First, the fading process experienced in typical wireless communication scenarios is very special and can serve to enhance the ability to secretly communicate when compared to less harsh communication scenarios. Second, the broadcast nature of the wireless medium allows for one to introduce interference into the medium that can harm an adversary’s ability to eavesdrop while strengthening the ability for two legitimate entities to communicate. In all cases, knowledge of the channel state is important to the ability to communicate, and thus understanding the

properties of secret communication when there is incomplete or inaccurate channel information is important. Moving away from the foundational information-theoretic aspects of secrecy dissemination, are two chapters that are devoted to examining the design of specific coding schemes and which serve as the first step towards realistic implementations of secrecy dissemination methods.

The second set of confidentiality chapters seek to use the unique space, time and frequency properties of the wireless channel as the source of shared, secret information between a transmitter and receiver. If this shared, secret information can be mined from the wireless channel, then it can serve as the basis for establishing secret keys. Secrecy extraction techniques are a particularly promising direction for using the physical layer to enhance security as the basic step needed to support secrecy extraction, namely the probing of the wireless medium in order to obtain a channel estimate, is also a fundamental step to general communication, i.e., channel estimation is already performed in the physical layer of most wireless systems. Although the chapters devoted to secrecy extraction involve significant theoretical aspects, they also represent some of the most solid evidence in support of real-world deployment of physical layer security techniques. Many of the chapters include experimental evidence and, in one case, a real-time implementation, of the validity of physical layer security mechanisms.

Next we turn to the problem of authentication. Authentication typically involves providing assurance that entities are who they claim to be, or that messages come from where they claim to originate. At the physical layer, the notion of identity is different. In this context, we are not as worried with *who* someone is, but rather with being able to distinguish between different transmitters. In the general wireless authentication problem, we are concerned with an active adversary injecting communications into the medium and claiming that these transmissions come from a legitimate wireless device. Interestingly, there are many situations where cryptographic techniques for authentication are not easy to employ, and thus it is desirable for an entity to differentiate between signals coming from a legitimate entity and those coming from an illegitimate entity. Physical layer authentication methods are a natural complement to secrecy extraction techniques as, in both cases, the characterization of the wireless channel serves as the fundamental building block. Whereas for secrecy extraction the channel estimate serves as the secret information that is used to establish a key, for physical layer authentication the channel estimate serves as the authenticator to distinguish between transmitters and receivers. An interesting challenge that arises in physical layer authentication is the need to maintain the authenticator when the environment is dynamic and entities are moving around. Our two chapters on physical layer authentication include discussion on the theoretical limits of authentication, as well as provide a thorough survey of physical layer authentication, with special attention devoted to addressing the time-varying nature of the wireless channel.

Lastly, we look at two other aspects related to security and physical layer communication. Cooperative communications is an emerging technique to improve the channel capacity of wireless communication systems, and involves multiple entities assisting each other in the transmission and decoding of messages by relaying

replicas of transmitted messages. Unfortunately, traditional cooperative communication schemes assume that all entities are trustworthy and follow protocols precisely, and thus these promising communication schemes are particularly sensitive to scenarios where entities falsely or maliciously cooperate. We have included a chapter that examines the security issues that arise in cooperative communications, and proposes an improved design for strengthening the security of cooperative transmission schemes by carefully integrating the notion of trust into cooperative communication protocols. Our final chapter discusses the issue of modulation forensics, which involves identifying the type of modulation that is being employed when there is no prior information about the transmitter. This is particularly important for emerging wireless systems, such as cognitive radio systems, where there may not be any prior relationship between a transmitter and a receiver, and it is necessary to identify the communication methods being employed before commencing with communication. Further, such analysis is also important in conducting attacks against the physical layer as knowing what modulation methods are being employed allows one to best adapt their attacks, whether attempting to spoof an entity or interfere with that entity.

We note that the physical layer for wireless systems provides an exciting collection of tools to enhance security that is not available to one who strictly employs a cryptographic toolkit. Traditional higher-layer security methods must play an important role in securing communications and certainly physical layer security techniques should not be considered a replacement for well-tested cryptography algorithms and security protocols. However, the properties of the wireless medium are a powerful source of domain-specific information that can be used to complement and enhance traditional security mechanisms that has remained, to date, an untapped resource and thus should be considered as expanding the tools available to engineers seeking to secure wireless systems. The methods described in this book will serve as the basis for removing a potential weak link in the design of future wireless systems and, as wireless systems become increasingly pervasive, we expect that physical layer security methods will be very useful in thwarting attacks that cannot be dealt with using conventional network security mechanisms.

Contributors

Babak Azimi-Sadjadi Intelligent Automation Inc., 15400 Calhoun Drive, Suite 400, Rockville, MD 20855, USA, e-mail: babak@i-a-i.com

Ersen Ekrem Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, e-mail: ersen@umd.edu

Hesham El Gamal Department of Electrical and Computer Engineering, Ohio State University, Columbus, OH 43210, USA, e-mail: helgamal@ece.osu.edu

Elza Erkip Department of Electrical and Computer Engineering, Polytechnic University, Brooklyn, NY 11201, USA, e-mail: elza@poly.edu

Satashu Goel Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA, USA, e-mail: satashu@cmu.edu

Larry Greenstein Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: ljjg@winlab.rutgers.edu

Deniz Gündüz Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA and Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA, e-mail: dgunduz@princeton.edu

Zhu Han ECE Department, University of Houston, Houston, TX 77004, USA, e-mail: hanzhu22@gmail.com

Xiang He Department of Electrical and Computer Engineering, Penn State University, University Park, PA 16802, USA, e-mail: xxh119@psu.edu

Hisato Iwai Department of Electronics, Doshisha University, Kyoto, Japan, e-mail: iwai@mail.doshisha.ac.jp

Aggelos Kiayias Department of Computer and Electrical Engineering, University of Connecticut, Storrs, CT, USA, e-mail: akiayias@engr.uconn.edu

Deepa Kundur Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA, e-mail: deepa@ece.tamu.edu

Lifeng Lai Department of Systems Engineering, University of Arkansas at Little Rock, Little Rock, AR 72204, USA, e-mail: lxlai@ular.edu

Zang Li Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: zang@winlab.rutgers.edu

Yingbin Liang Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822, USA, e-mail: yingbinl@hawaii.edu

W. Sabrina Lin ECE Department, University of Maryland, College Park, MD 20742, USA, e-mail: wylin@umd.edu

K. J. Ray Liu ECE Department, University of Maryland, College Park, MD 20742, USA, e-mail: kjrliu@umd.edu

Ruoheng Liu Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA, e-mail: rliu@princeton.edu

William Luh Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA, e-mail: luh@ece.tamu.edu

Narayan Mandayam Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: narayan@winlab.rutgers.edu

Suhas Mathur Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: suhas@winlab.rutgers.edu

Alejandra Mercado ADG, Hughes Network Systems, Germantown, MD, USA, e-mail: alejandra.mercado@hughes.com

Rohit Negi Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA, USA, e-mail: negi@ece.cmu.edu

H. Vincent Poor Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA, e-mail: poor@princeton.edu

Alex Reznik InterDigital, 781 Third Avenue King of Prussia, PA, USA, e-mail: Alex.Reznik@interdigital.com

Hideichi Sasaoka Department of Electronics, Doshisha University, Kyoto, Japan, e-mail: hsasaoka@mail.doshisha.ac.jp

Shlomo Shamai (Shitz) Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel, e-mail: sshlomo@ee.technion.ac.il

Predrag Spasojevic Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: spasojev@winlab.rutgers.edu

Yan Lindsay Sun University of Rhode Island, 4 East Alumni Ave., Kingston, RI 02881, USA, e-mail: yansun@ele.uri.edu

Xiaojun Tang Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: xtang@winlab.rutgers.edu

Wade Trappe Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: trappe@winlab.rutgers.edu

Sennur Ulukus Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA, e-mail: ulukus@umd.edu

Liang Xiao Department of Communication Engineering, Xiamen University, Fujian 361005, China, e-mail: lxiao@winlab.rutgers.edu

Roy Yates Wireless Information Network Laboratory (WINLAB), Rutgers University, 671 Rt. 1 South, North Brunswick, NJ 08902, USA, e-mail: ryates@winlab.rutgers.edu

Chunxuan Ye InterDigital, 781 Third Avenue King of Prussia, PA 19406, USA, e-mail: Chunxuan.Ye@interdigital.com

Aylin Yener Department of Electrical Engineering, Penn State University, University Park, PA 16802, USA, e-mail: yener@ee.psu.edu

Bülent Yener Department of Computer Science, Rensselaer Polytechnic Institute, Troy, NY, USA, e-mail: yener@cs.rpi.edu

Contents

1 Secrecy Capacity of Independent Parallel Channels	1
Zang Li, Roy Yates and Wade Trappe	
2 Obtaining Secrecy Through Intentional Uncertainty	19
Satashu Goel and Rohit Negi	
3 Distributed Secret Sharing over the Gaussian Interference Wiretap Channel	39
William Luh and Deepa Kundur	
4 Cooperative Jamming: The Tale of Friendly Interference for Secrecy	65
Xiang He and Aylin Yener	
5 Hybrid-ARQ Schemes for Reliable and Secret Wireless Communications	89
Xiaojun Tang, Ruoheng Liu, Predrag Spasojević and H. Vincent Poor	
6 Secret Communication Under Channel Uncertainty	113
Yingbin Liang, H. Vincent Poor and Shlomo Shamai (Shitz)	
7 Cooperative Secrecy in Wireless Communications	143
Erşen Ekrem and Sennur Ulukus	
8 Source Coding Under Secrecy Constraints	173
Deniz Gündüz, Elza Erkip and H. Vincent Poor	
9 Secret Key Extraction from Level Crossings over Unauthenticated Wireless Channels	201
Suhas Mathur, Wade Trappe, Narayan Mandayam, Chunxuan Ye and Alex Reznik	

10 Secret Key Generation Among Multiple Terminals with Applications to Wireless Systems	231
Chunxuan Ye and Alex Reznik	
11 Secret Key Agreement Techniques Based on Multipath Propagation Characteristics	261
Hideichi Sasaoka and Hisato Iwai	
12 Secret Communication over Fading Channels	281
B. Azimi-Sadjadi, A. Kiayias, A. Mercado and B. Yener	
13 Fingerprints in the Ether: Channel-Based Authentication	311
Liang Xiao, Larry Greenstein, Narayan Mandayam and Wade Trappe	
14 Message Authentication: Information Theoretic Bounds	335
Lifeng Lai, Hesham El Gamal and H. Vincent Poor	
15 Trusted Cooperative Transmissions: Turning a Security Weakness into a Security Enhancement	355
Yan Lindsay Sun and Zhu Han	
16 Modulation Forensics for Wireless Digital Communications in Frequency-Selective Fading Channels	379
W. Sabrina Lin and K. J. Ray Liu	

Chapter 1

Secrecy Capacity of Independent Parallel Channels*

Zang Li, Roy Yates and Wade Trappe

1.1 Introduction

Ensuring the confidentiality of communications is fundamental to securing any network. This requirement becomes particularly important for wireless systems, where eavesdropping is facilitated by the broadcast nature of the wireless medium. Rather than physically guard the communication medium to provide confidentiality, the traditional approach is to employ cryptographic algorithms to ensure that only legitimate users can correctly interpret the messages, while all other entities fail to glean any useful information.

The question of how much information is too much to leak to an eavesdropping adversary is at the heart of modern cryptography, and two important schools of thought have emerged: information-theoretic and complexity-based security. Information-theoretic encryption was first formulated by Shannon in 1949 [1], where the adversary is assumed to have unlimited computational resources and the cipher objective is to ensure that absolutely no information is released to the adversary. Thus, should the adversary observe an encrypted message (the ciphertext), the adversary is no better off than just randomly guessing the original message (the plaintext). Complexity-based cryptography, on the other hand, discards the notion that the adversary has infinite computing capabilities, and instead assumes the adversary has limitations on how much computation can be performed. Now, when an adversary witnesses a ciphertext, the necessary computations render it practically infeasible for the adversary to deduce the corresponding plaintext.

Common to both approaches, encryption algorithms are characterized by the existence of some form of information shared between the legitimate entities. This

Z. Li (✉)
Wireless Information Network Laboratory (WINLAB)
Rutgers University, 671 Rt. 1 South
North Brunswick, NJ 08902, USA
e-mail: zang@winlab.rutgers.edu

*Portions of the material have appeared previously in “Secrecy Capacity of Independent Parallel Channels,” Proceedings of the Forty-Fourth Annual Allerton Conference, 2006.

information, which is often colloquially referred to as a key, parameterizes specific realizations of the encryption service and must be kept private. Conventionally, the formation of these keys requires third parties, such as certificate authorities or key distributors, to administer these secrets. Unfortunately, for many wireless scenarios, it is difficult to ensure the availability of these third parties, thereby making the reliance on external key administration impractical. Ideally, rather than require the assistance of trusted third parties, what we would like is for each communicating pair to take advantage of some physical resource that can facilitate the sharing of a key. In fact, there is a fundamental viewpoint that underlies throughout this chapter and, more generally most of the contributions of this book. Notably, the information-theoretic approach to confidential communications offers advantages in wireless scenarios when compared with conventional complexity-based cryptography. In particular, due to the complexity of the wireless propagation environment, different users will get different noisy copies of the transmitted signals, and this difference can enable confidential transmission of information (including keys) among users.

Information-theoretic secret communication was first studied by Wyner [2] for the classical wiretap channel. Wyner found that there is a tradeoff between the transmission rate of the main system and the equivocation at the wire-tapper. He further derived the capacity region characterized by these two quantities, and showed that a positive rate of perfectly secret communication in the presence of a passive wiretapper is achievable. Later in 1978, Csiszár and Körner [3] extended Wyner's work to general broadcast scenarios. Their results proved that secret transmission is possible in a broadcast scenario as well as long as the channel satisfies certain conditions. The largest rate at which perfectly secret communication is possible was derived in both papers.

The purpose of this chapter is to extend the prior secrecy results to a system consisting of multiple independent parallel channels. We show that the secrecy capacity of the composite system is simply the summation of the secrecy capacities of the individual channels. We further derive the optimal power allocation strategy for a system with parallel AWGN channels subject to a total power constraint. The results can be extended to random fading channels with additive Gaussian noise. Secrecy capacity under various channel conditions and the benefit of the optimal power allocation strategy are evaluated numerically for an *Orthogonal Frequency-Division Multiplexing* (OFDM) system as an example. The rest of this chapter is organized as follows: the necessary theoretical background is described in Sect. 1.2, followed by a summary of our main results in Sect. 1.3. The proofs for the main results are provided in the Appendix of this chapter. Numerical evaluation for a typical OFDM system is presented in Sect. 1.4. We conclude the chapter in Sect. 1.5.

1.2 Background

In an information-theoretic secret communication system, a sender (Alice) wishes to reliably communicate a secret S to an intended receiver (Bob) in the presence of an eavesdropper (Eve). The secret S , a random integer from the set $\{1, 2, \dots, 2^{nR}\}$,

is transmitted in n channel uses. In this case, the secret has entropy $H(S) = nR$ bits and the secrecy communication rate is $R = H(S)/n$ bits per channel use. In these n channel uses, Alice transmits the coded signal $X^n = X_1, \dots, X_n$; Bob receives the channel output $Y^n = Y_1, \dots, Y_n$ and decodes \hat{S} with error probability $P_e = \Pr[S \neq \hat{S}]$. After Eve overhears the output $Z^n = Z_1, \dots, Z_n$, her residual uncertainty regarding the secret message S is given by the conditional entropy $H(S|Z^n)$. This conditional entropy is generally expressed as a normalized equivocation rate $\Delta = H(S|Z^n)/H(S)$. From the perspective of confidential and reliable communication, the system performance depends on both the communication rate R and the equivocation rate Δ . In particular, the rate tuple (R_0, Δ_0) is achievable if for any $\epsilon > 0$ there exists a rate R encoder and decoder with equivocation rate Δ such that for some n ,

$$P_e \leq \epsilon, \quad R \geq R_0 - \epsilon, \quad \Delta \geq \Delta_0 - \epsilon. \quad (1.1)$$

In this chapter, we focus on the case $\Delta_0 = 1$, corresponding to the case where Eve's information per secret information bit regarding the secret S gained by the observation Z^n is given by

$$\begin{aligned} I(S; Z^n) &= H(S) - H(S|Z^n) \\ &= (1 - \Delta)H(S) \leq \epsilon H(S). \end{aligned} \quad (1.2)$$

That is, Eve learns arbitrarily little information regarding the secret S .

This model of information-theoretic secret communication started with Wyner's analysis of the discrete memoryless wiretap channel [2]. In Wyner's system, Eve hears a degraded version of Bob's received signal in that the channels are defined by a Markov chain $X \rightarrow Y \rightarrow Z$. This was generalized by Csiszár and Körner [3] to a system in which Alice transmits confidential messages to Bob at rate R as well as common messages to both Bob and Eve at rate R_0 . When the rate of common messages is $R_0 = 0$, [3] defined the secrecy capacity \mathcal{C} as the maximum rate R , such that the tuple $(R, \Delta = 1)$ is achievable and showed that

$$\mathcal{C} = \max_{V \rightarrow X \rightarrow YZ} I(V; Y) - I(V; Z). \quad (1.3)$$

In this case, given the discrete memoryless channel (DMC) $P_{YZ|X}$, secrecy capacity is achieved by maximizing over all joint distributions $P_{V,X}(v, x)$ such that the Markov chain $V \rightarrow X \rightarrow YZ$ holds.¹ In subsequent work, Maurer and Wolf [4] showed that the secrecy condition Eq. (1.2) employed by Wyner and by Csiszár and Körner could be strengthened considerably through a technique called *privacy amplification* without reducing the secret capacity \mathcal{C} . In this work, we follow the traditional information-theoretic definitions of security with a focus on the optimization of \mathcal{C} while keeping in mind that an actual system would likely employ privacy amplification [5].

¹The notation \max_X where X is a random variable is a shorthand for maximization over the choice of PMF $P_X(x)$ when X is discrete or PDF $f_X(x)$ when X is continuous.

In theory, Eq. (1.3) is a complete characterization of the secrecy capacity \mathcal{C} ; however, many questions remain unanswered. For example, there are no systematic methods to optimize over the auxiliary input V and the $P_{X|V}$ channel. Yet the auxiliary is often essential, and how to choose it optimally remains elusive for general cases. However, for fixed channels, some results are known when the channels of Bob and Eve satisfy certain conditions. In [6], the DMC $P_{Y|X}$ is defined to be *more capable* than $P_{Z|X}$ if $I(X; Y) - I(X; Z) \geq 0$ for all inputs X . In addition, the DMC $P_{Y|X}$ is defined to be *less noisy* than $P_{Z|X}$ if $I(U; Y) - I(U; Z) \geq 0$ for all inputs U and DMCs $P_{X|U}$. It is known that less noisy implies more capable. In [3], it is shown that if Bob's channel is *more capable* than Eve's channel then the secrecy rate \mathcal{C} is achieved when $V = X$. Thus, when Bob has a more capable channel,

$$\mathcal{C} = \max_X I(X; Y) - I(X; Z). \quad (1.4)$$

Nevertheless, it remains to find the optimal input X that achieves \mathcal{C} for common channels. A fundamental difficulty is that $I(X; Y)$ and $I(X; Z)$ are both concave functions in the input distribution P_X . Thus the difference $I(X; Y) - I(X; Z)$ is, in general, neither concave nor convex in P_X and may have multiple local maxima. In this case, convex optimization procedures are not guaranteed to find the optimal input distribution [7]. We do note that the case that Bob's channel is less noisy than Eve's is an exception since van Dijk [8] has shown that $P_{Y|X}$ is less noisy than $P_{Z|X}$ if and only if $I(X; Y) - I(X; Z)$ is a concave function of P_X .

The memoryless discrete-time AWGN channel is an important example for which the secrecy capacity is known. At time t , Alice's transmitted signal is X_t and the received signals of Bob and Eve are

$$Y_t = \sqrt{b}X_t + W_{1,t}, \quad Z_t = \sqrt{g}X_t + W_{2,t}. \quad (1.5)$$

The independent additive noises $W_{i,t}$ are assumed to have unit variance and b and g represent link gains normalized by the power spectral density of the additive noise. When $b < g$, we can construct an equivalent system in which Y_t and Z_t have the same conditional marginal distributions but Bob's signal Y_t is a degraded version of Z_t . It follows that $I(X; Y) - I(X; Z) \leq 0$ for all inputs X . In this case, the secrecy capacity is zero, which is achieved by any input X with entropy $H(X) = 0$. When $b > g$, Bob's channel is more capable, and the secrecy capacity is given by Eq. (1.4). Here the complication is that while $I(X; Y)$ is maximized under an average power constraint by a Gaussian input X so too is $I(X; Z)$ maximized. Nevertheless, Leung-Yan-Cheong and Hellman [9] verified that a Gaussian input X also maximizes the secret capacity \mathcal{C} . In this case, $I(X; Y)$ and $I(X; Z)$ are given by AWGN Shannon capacity. Thus, an average power P for the input X yields a secrecy capacity of

$$\mathcal{C}_{\text{AWGN}}(b, g, P) = \frac{1}{2}(\log(1 + bP) - \log(1 + gP))^+, \quad (1.6)$$

where $(x)^+ = \max(x, 0)$. This result is subject to a quite negative interpretation. First, $b \leq g$ yields zero secrecy capacity. Second, even if Bob's channel is more

capable, the capacity is power limited; for arbitrarily large power P , the capacity is upper bounded by $(1/2) \log(b/g)$, which may be quite small.

The assumptions underlying this pessimism, however, do not reflect the design of modern communications systems, and in particular do not exploit the large number of degrees of freedom available to a modern wireless system. For example, it is possible to use multiple subcarriers in order to provide a large number of parallel subchannels, as is utilized in OFDM transceivers, and the underlying frequency selectivity induced by multipath may provide a diversity advantage [10]. The questions we aim to answer in this chapter are the following: what is the secrecy capacity for a system consisting of M independent parallel channels? What is the optimal power allocation strategy if all the channels are AWGN channels but the system has to satisfy a total power constraint? Our main results are summarized in the next section.

1.3 Main Results

Consider a system with M independent parallel subchannels. Alice's channel input is $X^M = X_1, \dots, X_M$. Bob and Eve receive $Y^M = Y_1, \dots, Y_M$ and $Z^M = Z_1, \dots, Z_M$, respectively. The channel is characterized by

$$P(Y^M Z^M | X^M) = \prod_{m=1}^M P(Y_m Z_m | X_m). \quad (1.7)$$

From Eq. (1.3), the secrecy capacity is

$$\mathcal{C}_M = \max_{V \rightarrow X^M \rightarrow Y^M Z^M} I(V; Y^M) - I(V; Z^M). \quad (1.8)$$

Note that Bob's channel $P_{Y^M|X^M}$ is, in general, not more capable than Eve's channel $P_{Z^M|X^M}$. When there exists a subchannel \hat{m} satisfying $I(X_{\hat{m}}; Y_{\hat{m}}) < I(X_{\hat{m}}; Z_{\hat{m}})$ for some input $X_{\hat{m}}$, the *more capable* condition is violated. A natural question raised here is whether we can decouple the composite system. This is answered by the following theorem.

Theorem 1 *The secrecy capacity Eq. (1.8) of the system with M independent parallel subchannels is given by*

$$\mathcal{C}_M = \sum_{m=1}^M \max_{V_m \rightarrow X_m \rightarrow Y_m Z_m} I(V_m; Y_m) - I(V_m; Z_m), \quad (1.9)$$

where V_m is an auxiliary variable designed just for subchannel m .

The proof follows. The method of the proof is essentially the same as that used in [3] to derive a single letter characterization of the secrecy capacity.

Proof We follow the method used in [3] to derive a single-letter characterization in the secrecy capacity converse. Denote $Y^m = Y_1, \dots, Y_m$, and $Z_m^M = Z_m, \dots, Z_M$.

From the chain rule, we can write

$$\begin{aligned} & I(V; Y^M) - I(V; Z^M) \\ &= \sum_{m=1}^M I(V; Y_m | Y^{m-1}) - \sum_{m=1}^M I(V; Z_m | Z_{m+1}^M). \end{aligned} \quad (1.10)$$

Moreover, we can obtain

$$\begin{aligned} & I(V; Y_m | Y^{m-1}) \\ &= H(Y_m | Y^{m-1}) - H(Y_m | VY^{m-1}) \end{aligned} \quad (1.11)$$

$$\begin{aligned} &= H(Y_m | Y^{m-1}) - H(Y_m | VY^{m-1} Z_{m+1}^M) \\ &\quad + H(Y_m | VY^{m-1} Z_{m+1}^M) - H(Y_m | VY^{m-1}) \end{aligned} \quad (1.12)$$

$$= I(VZ_{m+1}^M; Y_m | Y^{m-1}) - I(Z_{m+1}^M; Y_m | VY^{m-1}) \quad (1.13)$$

$$\begin{aligned} &= I(Z_{m+1}^M; Y_m | Y^{m-1}) + I(V; Y_m | Y^{m-1} Z_{m+1}^M) \\ &\quad - I(Z_{m+1}^M; Y_m | VY^{m-1}) \end{aligned} \quad (1.14)$$

$$\begin{aligned} &= \sum_{j=m+1}^M I(Z_j; Y_m | Y^{m-1} Z_{j+1}^M) + I(V; Y_m | Y^{m-1} Z_{m+1}^M) \\ &\quad - \sum_{j=m+1}^M I(Z_j; Y_m | VY^{m-1} Z_{j+1}^M). \end{aligned} \quad (1.15)$$

Similarly,

$$\begin{aligned} & I(V; Z_m | Z_{m+1}^M) \\ &= H(Z_m | Z_{m+1}^M) - H(Z_m | VZ_{m+1}^M) \end{aligned} \quad (1.16)$$

$$\begin{aligned} &= H(Z_m | Z_{m+1}^M) - H(Z_m | VY^{m-1} Z_{m+1}^M) \\ &\quad + H(Z_m | VY^{m-1} Z_{m+1}^M) - H(Z_m | VZ_{m+1}^M) \end{aligned} \quad (1.17)$$

$$= I(VY^{m-1}; Z_m | Z_{m+1}^M) - I(Y^{m-1}; Z_m | VZ_{m+1}^M) \quad (1.18)$$

$$\begin{aligned} &= I(Y^{m-1}; Z_m | Z_{m+1}^M) + I(V; Z_m | Y^{m-1} Z_{m+1}^M) \\ &\quad - I(Y^{m-1}; Z_m | VZ_{m+1}^M) \end{aligned} \quad (1.19)$$

$$\begin{aligned} &= \sum_{j=1}^{m-1} I(Y_j; Z_m | Z_{m+1}^M Y^{j-1}) + I(V; Z_m | Y^{m-1} Z_{m+1}^M) \\ &\quad - \sum_{j=1}^{m-1} I(Y_j; Z_m | VZ_{m+1}^M Y^{j-1}). \end{aligned} \quad (1.20)$$

Note that

$$\begin{aligned} & \sum_{m=1}^M \sum_{j=m+1}^M I(Z_j; Y_m | Y^{m-1} Z_{j+1}^M) \\ &= \sum_{m=1}^M \sum_{j=1}^{m-1} I(Y_j; Z_m | Z_{m+1}^M Y^{j-1}) \end{aligned} \quad (1.21)$$

and

$$\begin{aligned} & \sum_{m=1}^M \sum_{j=m+1}^M I(Z_j; Y_m | VY^{m-1} Z_{j+1}^M) \\ &= \sum_{m=1}^M \sum_{j=1}^{m-1} I(Y_j; Z_m | VZ_{m+1}^M Y^{j-1}). \end{aligned} \quad (1.22)$$

Combining Eq. (1.10) to Eq. (1.22), we get

$$\begin{aligned} & I(V; Y^M) - I(V; Z^M) \\ &= \sum_{m=1}^M I(V; Y_m | Y^{m-1}) - \sum_{m=1}^M I(V; Z_m | Z_{m+1}^M) \end{aligned} \quad (1.23)$$

$$= \sum_{m=1}^M [I(V; Y_m | Y^{m-1} Z_{m+1}^M) - I(V; Z_m | Y^{m-1} Z_{m+1}^M)]. \quad (1.24)$$

Denote $U_m = Y^{m-1} Z_{m+1}^M$, $\hat{V}_m = VU_m$, then

$$\begin{aligned} & I(V; Y^M) - I(V; Z^M) \\ &= \sum_{m=1}^M [I(V; Y_m | U_m) - I(V; Z_m | U_m)] \end{aligned} \quad (1.25)$$

$$= \sum_{m=1}^M [I(VU_m; Y_m | U_m) - I(VU_m; Z_m | U_m)] \quad (1.26)$$

$$= \sum_{m=1}^M [I(\hat{V}_m; Y_m | U_m) - I(\hat{V}_m; Z_m | U_m)] \quad (1.27)$$

$$\leq \sum_{m=1}^M \max_{\hat{V}_m \rightarrow X_m \rightarrow Y_m Z_m} [I(\hat{V}_m; Y_m) - I(\hat{V}_m; Z_m)]. \quad (1.28)$$

Note that the term inside the sum is just the secrecy capacity of each parallel independent channel, thus is achievable. The equality holds if and only if each channel achieves its individual secrecy capacity. \square

This theorem shows that we can choose the optimal V_m for each subchannel independently. The secrecy capacity of the system is simply the summation of the secrecy capacities of the individual subchannels. Note that Eq. (1.9) holds for any collection of M independent parallel subchannels, regardless of the model for each subchannel. If all subchannels are AWGN channels of the form of Eq. (1.5), we can represent the normalized link gains for the Alice-Bob and Alice-Eve subchannels by the vectors $\mathbf{v} = [b_1, \dots, b_M]^T$ and $\mathbf{g} = [g_1, \dots, g_M]^T$. For the AWGN case, $b_m \leq g_m$ implies subchannel m has zero secrecy capacity while $b_m > g_m$ implies Bob has a more capable subchannel. Therefore, the secrecy capacity of a system of M orthogonal AWGN channels is

$$\mathcal{C}_M = \sum_{m=1}^M \max_{X_m \rightarrow Y_m Z_m} I(X_m; Y_m) - I(X_m; Z_m), \quad (1.29)$$

since when $b_m \leq g_m$, the maximization in Eq. (1.29) for subchannel m will yield zero secrecy capacity for subchannel m . Moreover, because each subchannel is just an AWGN channel, capacity is achieved using Gaussian input on each subchannel. Thus, a subchannel m with transmit power P_m contributes $\mathcal{C}_{\text{AWGN}}(b_m, g_m, P_m)$ to the secrecy capacity

$$\mathcal{C}_M(\mathbf{v}, \mathbf{g}, \mathbf{P}) = \sum_{m=1}^M \mathcal{C}_{\text{AWGN}}(b_m, g_m, P_m). \quad (1.30)$$

A fundamental question is how $\mathcal{C}_M(\mathbf{v}, \mathbf{g}, \mathbf{P})$ depends on the power allocation \mathbf{P} , particularly when we are subject to the total power constraint $\sum_{m=1}^M P_m \leq P_{\text{tot}}$. Our second result gives the optimal power allocation \mathbf{P} that maximizes the secrecy capacity under this situation.

Theorem 2 *The secrecy capacity of a system of M orthogonal AWGN subchannels, with normalized link gain \mathbf{v}, \mathbf{g} , under the total power constraint $\sum_{m=1}^M P_m \leq P_{\text{tot}}$ is*

$$\mathcal{C}_M(\mathbf{v}, \mathbf{g}, P_{\text{tot}}) = \sum_{m=1}^M \mathcal{C}_{\text{AWGN}}(b_m, g_m, P_{\text{AWGN}}(b_m, g_m, \lambda)). \quad (1.31)$$

If $b_m \leq g_m$ for every m , the secrecy capacity is zero regardless of the power allocation strategy. Otherwise, $P_{\text{AWGN}}(b_m, g_m, \lambda)$ is given by

$$P_{\text{AWGN}}(b, g, \lambda) = \frac{1}{2} \left(f(b, g, \lambda) - \left(\frac{1}{b} + \frac{1}{g} \right) \right)^+, \quad (1.32)$$

where

$$f(b, g, \lambda) = \sqrt{\left(\frac{1}{b} + \frac{1}{g}\right)^2 + 4\left[\frac{1}{\lambda} \left(\frac{1}{g} - \frac{1}{b}\right) - \frac{1}{gb}\right]}, \quad (1.33)$$

and $\lambda > 0$ is chosen such that we satisfy the total power constraint

$$\sum_{m=1}^M P_{AWGN}(b_m, g_m, \lambda) = P_{\text{tot}}. \quad (1.34)$$

The proof follows. The proof uses the well-known Lagrangian method, which gives the solution due to the convexity of the AWGN channel secrecy capacity.

Proof To prove Theorem 2, we need to resort to the secrecy capacity results for AWGN channels, as characterized by Eq. (1.6). We observe that if $b_m \leq g_m$, channel m will go unused since its secrecy capacity is zero, and no power will be allocated to this channel. Thus we can simplify the subsequent proof by assuming that channels $1, \dots, \bar{M}$ satisfy $b_m > g_m$, and only consider the power allocation to these channels. In this case, it is easily verified that $b_m > g_m$ implies $C_{AWGN}(b_m, g_m, P_m)$ is concave in P_m . In terms of the vector $\mathbf{P} = [P_1, \dots, P_{\bar{M}}]^T$, we use Eq. (1.6) and form the Lagrangian

$$\begin{aligned} \mathcal{L}(\lambda, \mathbf{P}) \\ = \sum_{m=1}^{\bar{M}} [\log(1 + b_m P_m) - \log(1 + g_m P_m) - \lambda P_m], \end{aligned} \quad (1.35)$$

where $\lambda > 0$. Maximization of the Lagrangian requires that $\partial \mathcal{L} / \partial P_m = 0$ if $P_m > 0$ or $\partial \mathcal{L} / \partial P_m \leq 0$ if $P_m = 0$. This implies that the nonzero P_m satisfy the quadratic equation

$$\left(P_m + \frac{1}{g_m}\right)\left(P_m + \frac{1}{b_m}\right) - \frac{1}{\lambda} \left(\frac{1}{g_m} - \frac{1}{b_m}\right) = 0. \quad (1.36)$$

We can then solve for non-negative P_m and express the general solution as $P_m = P_{AWGN}(b_m, g_m, \lambda)$ described by Eq. (1.32). It follows that $P_m > 0$ if and only if $b_m - g_m > \lambda$. The Lagrange multiplier λ is chosen so that the power constraint is met. Since Eq. (1.32) already implies that $P_{AWGN}(b, g, \lambda) = 0$ for $b \leq g$, we have proved Theorem 2 for a general system with M independent parallel AWGN channels. \square

We note that in the optimal power allocation Eq. (1.32), $P_m > 0$ if and only if $b_m - g_m > \lambda$. Since λ is positive, subchannel m will go unused if $b_m \leq g_m$. This is expected as $C_{AWGN}(b_m, g_m, P_m) = 0$ no matter what power is used when $b_m \leq g_m$. For the subchannels with $b_m > g_m$, they are ranked according to the differences

$b_m - g_m$. For very small P_{tot} , only the subchannel with the largest difference is used. As P_{tot} is increased, λ decreases and additional subchannels are employed in the order given by $b_m - g_m$. This solution is conceptually similar to the familiar capacity-achieving waterfilling solution in that the power level P_m is determined by the channel parameters and the Lagrange multiplier λ that is used to meet the power constraint. The difference in the secrecy capacity power allocation Eq. (1.32) is that subchannels are ranked not by the gain b_m but rather by the gain differences $b_m - g_m$.

The result above can be extended to the fading channel scenario when the channel realizations are known to all parties. Consider a discrete-time memoryless channel with normalized stationary and ergodic time-varying gains $\sqrt{b_i}$ and $\sqrt{g_i}$ at the i th time unit for Bob and Eve, respectively. For convenience, we use $\gamma_i = (b_i, g_i)$ to denote the joint channel state. The noise is assumed to be AWGN, with unit power spectral density. Let $S(\gamma)$ denote the transmit signal power, and \bar{S} denote the average transmit signal power. Let W denote the received signal bandwidth, which is assumed to be the same for both Bob and Eve. The instantaneous received signal-to-noise ratio (SNR) is then $S(\gamma_i)b_i/W$ and $S(\gamma_i)g_i/W$. Given the knowledge of the channel states, the sequence of fading channels is just a special case of a system of independent parallel channels. With similar methods, we can show the following theorem.

Theorem 3 *When the channel side information $\gamma = (b, g)$ is known to all parties, the secrecy capacity of a discrete-time memoryless fading channel with additive unit Gaussian noise subject to an average power constraint \bar{S} is*

$$\mathcal{C} = \max_{S(\gamma): E_\gamma[S(\gamma)] = \bar{S}} E_\gamma[\mathcal{C}(\gamma, S(\gamma))], \quad (1.37)$$

where

$$\mathcal{C}(\gamma, S(\gamma)) = W \left(\log \left(1 + \frac{S(\gamma)b}{W} \right) - \log \left(1 + \frac{S(\gamma)g}{W} \right) \right). \quad (1.38)$$

The optimal power allocation to achieve the secrecy capacity Eq. (1.37) is

$$S^*(\gamma) = \frac{W}{2} \left(f(b, g, \lambda) - \left(\frac{1}{b} + \frac{1}{g} \right) \right)^+, \quad (1.39)$$

where $f(b, g, \lambda)$ is given by Eq. (1.33), and λ is chosen such that the average transmit signal power satisfies the constraint

$$E_\gamma[S^*(\gamma)] = \bar{S}. \quad (1.40)$$

Moreover, a single codebook with the dynamic power adaptation Eq. (1.39) is sufficient to achieve the secrecy capacity.

Proof We will prove the converse of the theorem first, and show the achievability afterwards.

Denote $W \in \{1, \dots, 2^{nR}\}$ as the secret message index. To prove the converse, we note that

$$nR = H(W|\gamma^n) \quad (1.41)$$

$$\leq H(W|Z^n, \gamma^n) + \epsilon \quad (1.42)$$

$$= H(W|Y^n, \gamma^n) + I(W; Y^n|\gamma^n) - I(W; Z^n|\gamma^n) + \epsilon \quad (1.43)$$

$$\leq I(W; Y^n|\gamma^n) - I(W; Z^n|\gamma^n) + \eta + \epsilon, \quad (1.44)$$

where Eq. (1.42) is due to the perfect secrecy requirement and Eq. (1.44) is due to the capacity requirement.

Using the same method as in proof for Theorem 1, we can show that

$$I(W; Y^n|\gamma^n) - I(W; Z^n|\gamma^n) \quad (1.45)$$

$$= \sum_{i=1}^n (I(W; Y_i|U_i, \gamma^n) - I(W; Z_i|U_i, \gamma^n)) \quad (1.46)$$

$$= \sum_{i=1}^n (I(V_i; Y_i|U_i, \gamma^n) - I(V_i; Z_i|U_i, \gamma^n)) \quad (1.47)$$

$$\leq \sum_{i=1}^n \max_{V_i \rightarrow X_i \rightarrow Y_i Z_i} (I(V_i; Y_i|\gamma_i) - I(V_i; Z_i|\gamma_i)) \quad (1.48)$$

Since the channel at time i is an AWGN channel with unit noise for a given γ_i , we can write

$$\max_{V_i \rightarrow X_i \rightarrow Y_i Z_i} I(V_i; Y_i|\gamma_i) - I(V_i; Z_i|\gamma_i) = \mathcal{C}(\gamma_i, S(\gamma_i)), \quad (1.49)$$

where $\mathcal{C}(\gamma, S(\gamma))$ is the secrecy capacity for channel with gain γ and power $S(\gamma)$, and is given by Eq. (1.38).

Assume that the channel state is a discrete random variable, perhaps derived from quantization of a continuous channel state, and takes values from $\{\gamma_1, \dots, \gamma_M\}$. Denote N_m to be the number of appearance that $\gamma = \gamma_m$ during the n transmissions, we then have

$$\begin{aligned} & I(W; Y^n|\gamma^n) - I(W; Z^n|\gamma^n) \\ & \leq \sum_{i=1}^n \mathcal{C}(\gamma_i, S(\gamma_i)) \end{aligned} \quad (1.50)$$

$$= \sum_{m=1}^M \mathcal{C}(\gamma_m, S(\gamma_m)) N_m. \quad (1.51)$$

Combining all above, we see that

$$R \leq \frac{1}{n} (I(W; Y^n | \gamma^n) - I(W; Z^n | \gamma^n) + \eta + \epsilon), \quad (1.52)$$

$$\leq \sum_{m=1}^M C(\gamma_m, S(\gamma_m)) \frac{N_m}{n} + \frac{\eta}{n} + \frac{\epsilon}{n}. \quad (1.53)$$

As n increases, N_m/n approaches $p(\gamma_m)$, implying

$$R \leq E_\gamma [C(\gamma, S(\gamma))] + \frac{\eta}{n} + \frac{\epsilon}{n}. \quad (1.54)$$

Maximizing the right hand side over $S(\gamma)$ subject to the average power constraint using the method in the proof of Theorem 2, we get the optimal power allocation Eq. (1.39). This completes the converse for Theorem 3.

As for the achievability, we note that a multiplexing codebook scheme similar to that proposed in [11] can achieve the secrecy rate $E_\gamma [C(\gamma, S(\gamma))]$. Combining with Eq. (1.54), this ends the proof of Eq. (1.37). On the other hand, using similar arguments as in [12], we can show that a multiplexing codebook is actually not necessary, as detailed below.

Suppose Alice chooses $X = \tilde{S}(\gamma)V$, where $\tilde{S}(\gamma)$ is a power function adapted to the channel state γ , and V is a unit power Gaussian random variable independent of γ . In this case, Bob receives

$$Y = \sqrt{b}\tilde{S}(\gamma)V + W_1, \quad (1.55)$$

and Eve receives

$$Z = \sqrt{g}\tilde{S}(\gamma)V + W_2. \quad (1.56)$$

Since all parties know γ and in turn $\tilde{S}(\gamma)$, we can consider the random channel state Γ as an output of the channel. Thus, with the coding procedure in [3], a single codebook can be used to achieve the secrecy rate of

$$I(V; Y\Gamma) - I(V; Z\Gamma) = I(V; Y|\Gamma) - I(V; Z|\Gamma) \quad (1.57)$$

$$= E_\gamma [C(\gamma, \tilde{S}(\gamma))]. \quad (1.58)$$

When $\tilde{S}(\gamma) = S^*(\gamma)$, the optimum power allocation strategy, we achieve the secrecy capacity Eq. (1.37). \square

Although a multiplexing codebook scheme similar to that proposed in [11] can be deployed to achieve the secrecy capacity Eq. (1.37), we have shown that it is not necessary. Just as in the case of ordinary capacity, a single codebook with optimal power adaptation is sufficient to achieve the capacity [12], it is also enough to achieve the secrecy capacity. The transmitter transmits only when Bob's channel gain is greater than Eve's channel by at least λ , and the transmitted power is adapted to the variation of channel gains.

1.4 Numerical Evaluation

Our results can be easily applied to an OFDM system with independent Rayleigh fading AWGN subchannels. We start by noting that the secrecy capacity Eq. (1.31) is determined by M , the total number of channels, Bob and Eve's channel gain vectors \mathbf{v} and \mathbf{g} , and the power constraint P_{tot} . In an OFDM system with fixed frequency spacing of subchannels, M will be proportional to the transmission bandwidth. For Rayleigh fading, Bob and Eve's channel gain vectors \mathbf{v} and \mathbf{g} can be modeled as independent random vectors (assuming Bob and Eve are separated by a distance of more than a wavelength) with i.i.d. exponentially distributed components, and is characterized by their mean $E[b]$ and $E[g]$. Therefore, an interesting question is how the secrecy capacity varies with M , $E[b]$, $E[g]$ and P_{tot} . In this section, we will study the effect of these factors on the secrecy capacity through numerical evaluations.

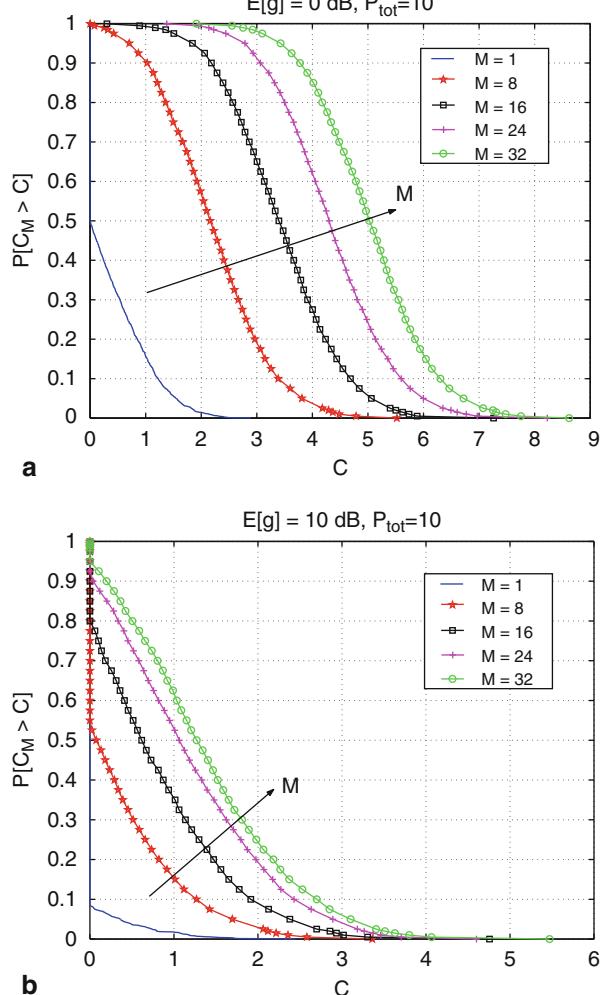
The secrecy capacity depends on the exact channel realizations. For a setting of $\{M, E[b], E[g], P_{\text{tot}}\}$, since channel gains are randomly drawn from their distributions, C_M is a random variable. To characterize the distribution of C_M under each setting, we choose to show its *Complementary Cumulative Distribution Function* (CCDF), i.e. $\Pr[C_M > C]$ for increasing C , estimated from numerical methods. For simplicity, we fix $E[b] = 1$ for all settings. Let us first look at how the secrecy capacity changes with M . Intuitively, due to the randomness of the channel gains, the larger M is, the more good subchannels Bob may have relative to Eve's subchannels. As a result, the secrecy capacity increases with M . This is illustrated in Fig. 1.1 under two levels of $E[g]$. The improvement from single channel to multiple channels is significant. The intersection of the curve to the vertical axis represents the probability that Bob has at least one subchannel better than Eve, given by

$$1 - \Pr[b \leq g]^M = 1 - (E[g]/(E[b] + E[g]))^M, \quad (1.59)$$

which increases rapidly with M . The improvement gets smaller as M gets larger because the total power is fixed. Even though more good channels are available as M increases, only the best a few are used due to the power limitation.

The change in secrecy capacity with the average Alice-Eve channel gain is plotted in Fig. 1.2a. As Eve's channel gets better on average, the secrecy capacity becomes smaller. For comparison purposes, the ordinary non-secure capacity is also plotted in the same figure. Obviously, this is an upper bound to the secrecy capacity. We note that if Eve's channel is significantly worse than Bob's channel on average, the capacity reduction due to the secrecy requirement is quite small. This is as expected, since as $E[g] \rightarrow 0$, we should approach the ordinary capacity. Moreover, even when Eve's channel is much better on average, we can still obtain positive secrecy capacity because of the availability of multiple independent random channels. We also plot the change in secrecy capacity versus the total power in Fig. 1.2b. Larger power budget improves the secrecy capacity, but will not cause an unbounded increase because the secrecy capacity of each subchannel is upper bounded by $1/2 \log(b_m/g_m)$ no matter how large the power is.

Fig. 1.1 Change in the secrecy capacity CCDF versus the number of channels M for **a** $E[g] = 0$ dB, and **b** $E[g] = 10$ dB. We fix $P_{\text{tot}} = 10$ and $E[b] = 1$

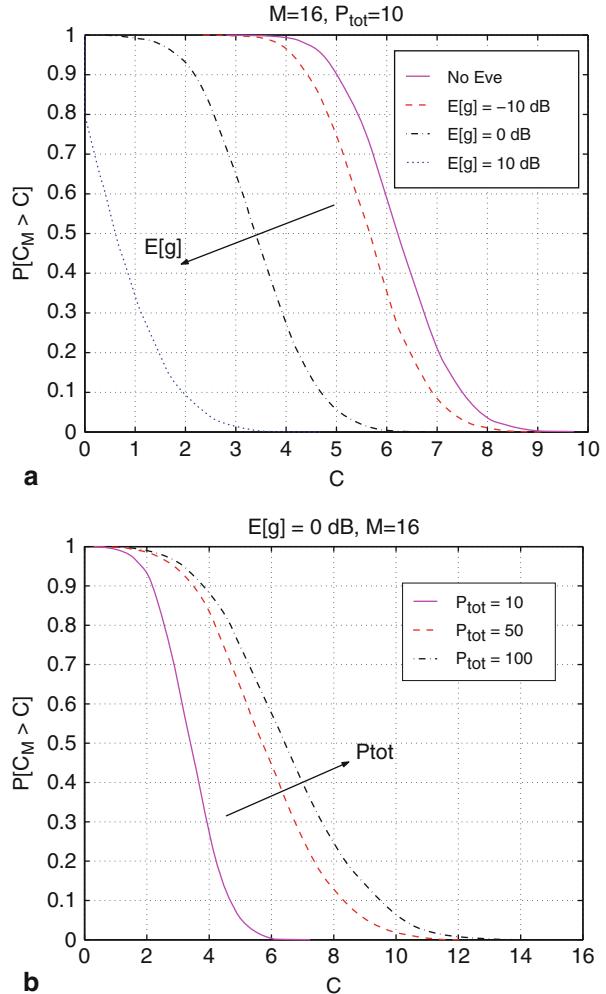


To assess the benefits of the optimal power allocation, we can compare against the non-adaptive uniform power allocation $\mathbf{P} = \bar{\mathbf{P}} = (P_{\text{tot}}/M)[1, \dots, 1]$. This uniform allocation yields the secrecy rate

$$\mathcal{C}_M(\mathbf{v}, \mathbf{g}, \bar{\mathbf{P}}) = \sum_{m=1}^M \mathcal{C}_{\text{AWGN}}(b_m, g_m, P_{\text{tot}}/M). \quad (1.60)$$

The uniform power allocation forfeits power when a subchannel is bad; however, it does take advantage of good (for secrecy capacity) subchannels. In addition, the uniform power allocation is easy to analyze since it is a sum of M independent

Fig. 1.2 Change in the secrecy capacity CCDF versus **a** $E[g]$ for $P_{\text{tot}} = 10$, and **b** P_{tot} for $E[g] = 0 \text{ dB}$. We fix $M = 16$ and $E[b] = 1$



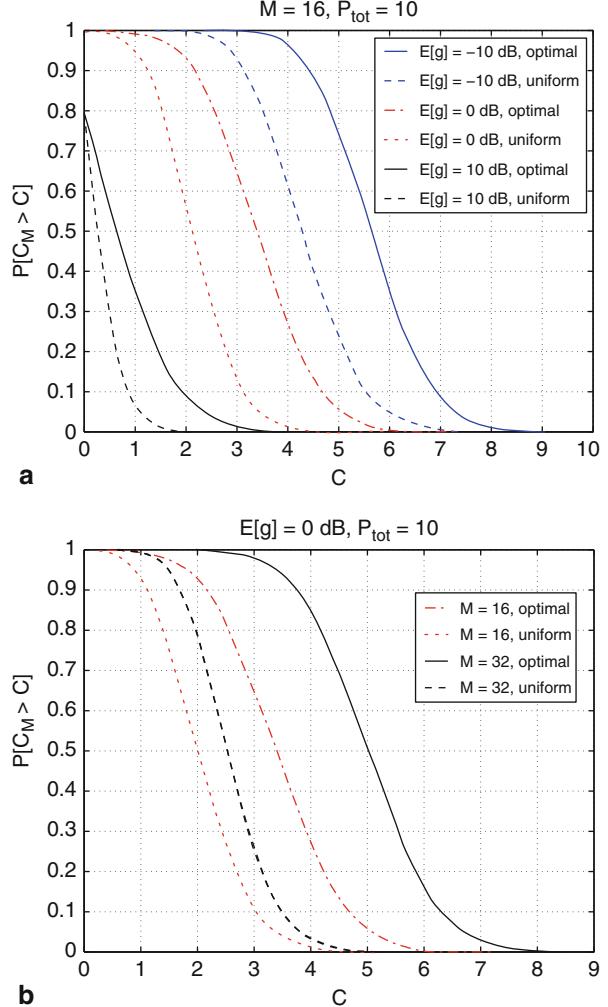
random variables. With the approximation of $\log(1 + x) \approx x / \ln 2$ for small x , we can derive from Eqs. (1.60) and (1.6) that

$$\lim_{M \rightarrow \infty} \mathcal{C}_M(\mathbf{v}, \mathbf{g}, \bar{\mathbf{P}}) = \frac{P_{\text{tot}}}{2 \ln 2} E[(b - g)^+] \quad (1.61)$$

$$= \frac{P_{\text{tot}}}{2 \ln 2} \frac{E[b]^2}{(E[b] + E[g])} \quad (1.62)$$

for the uniform power allocation. The secrecy capacity with the optimal power allocation and the non-adaptive uniform power allocation are compared in Fig. 1.3. The result shows that there is a significant capacity loss due to the non-optimal

Fig. 1.3 Comparison between optimal power allocation and uniform power allocation for **a** varying $E[g]$ with $M = 16$, and **b** varying M with $E[g] = 0$ dB. We fix $P_{\text{tot}} = 10$, and $E[b] = 1$



power allocation. The penalty becomes increasingly severe as M increases. Thus, optimal power allocation is crucial for fully exploiting the advantage brought by multiple random channels when the power budget is tight. On the other hand, the benefits of the simpler power allocation may be overstated. The fundamental binning code method of Csiszár and Körner [3] demands knowledge of the channel states. If this requirement is unavoidable, then the residual complexity of channel-dependent codebooks will likely outweigh any complexity reduction associated with uniform power allocation. Moreover, OFDM channels become increasingly difficult to estimate as the average power per subchannel P_{tot}/M goes to zero. For traditional data communication, these same issues are addressed in [13–16].

1.5 Conclusions

Modern wireless communication systems are being built to exploit the advantages of multiple independent parallel subchannels. It is well known that the advantages of such multi-carrier systems becomes increasingly pronounced as these wireless systems are deployed in environments involving complex channel conditions. However, although these advantages have been framed in the context of conventional communication and information theory, similar benefits also exist for the case of secret communication, where two parties (Alice and Bob) wish to communicate with an assurance that an eavesdropping third party (Eve) is not able to infer the communications between Alice and Bob. In this chapter, we have studied the secrecy capacity of a system consisting of multiple independent parallel subchannels. Multi-carrier systems are becoming increasingly common in modern communication system, as is evidenced by the use of OFDM in WiMax and WiFi systems, to cope with frequency-selective fading. We have shown that the extra dimensionality provided in such systems facilitates secret communication and improves the secrecy capacity. In particular, the secrecy capacity of the system is achieved when each subchannel achieves its own secrecy capacity. Therefore, we can choose the secrecy capacity achieving codebook for each subchannel independently. We further derived the optimal power allocation strategy when the subchannels are AWGN channels and the system operates under a total power constraint. The resulting optimal power allocation strategy is similar to the well-known waterfilling strategy except that the subchannels are ranked according to the difference of channels gains. With the optimal power allocation strategy, we can utilize the multiple random channels most efficiently and increase the secrecy capacity significantly under the same total power constraint.

References

- [1] C. Shannon. Communication theory of secrecy systems. *Bell. Syst. Tech. J.*, 28:657–715, 1949.
- [2] A. Wyner. The wire-tap channel. *Bell. Syst. Tech. J.*, 54(8):1355–1387, Jan. 1975.
- [3] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.
- [4] U. M. Maurer and S. Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. *Adv. Cryptol. EUROCRYPT*, 351–368, 2000.
- [5] C. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41:1915–1923, 1995.
- [6] J. Körner and K. Marton. Comparison of two noisy channels. In I. Csiszár and P. Elias, editors, *Topics In Information Theory*, 411–423. Colloquia Mathematica Societatis Janos Bolyai, Amsterdam, The Netherlands: North Holland, 1977.
- [7] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.
- [8] M. Van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 43(2):712–714, Mar. 1997.
- [9] S. K. Leung-Yan-Cheong and M. Hellman. The gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.

- [10] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.
- [11] A. J. Goldsmith and P. P. Varaiya. Capacity of fading channels with channel side information. *IEEE Trans. Inf. Theory*, 43(6):1986–1992, Nov. 1997.
- [12] G. Caire and S. Shamai. On the capacity of some channels with channel state information. *IEEE Trans. Inf. Theory*, 45(6):2007–2019, Sept. 1999.
- [13] S. Verdú. Spectral efficiency in the wideband regime. *IEEE Trans. Inf. Theory*, 48(6):1319–1343, Jun. 2002.
- [14] E. Telatar and D. N. C. Tse. Capacity and mutual information of wideband multipath fading channels. *IEEE Trans. Inf. Theory*, 46(4):1384–1400, Jul. 2000.
- [15] M. Medard and R.G. Gallager. Bandwidth scaling for fading multipath channels. *IEEE Trans. Inf. Theory*, 48(6):840–852, Apr. 2002.
- [16] S. Verdu. Recent results on the capacity of wideband channels in the low-power regime. *IEEE Wireless Commun.*, 40–45, Aug. 2002.

Chapter 2

Obtaining Secrecy Through Intentional Uncertainty*

Satashu Goel and Rohit Negi

2.1 Introduction

The tremendous popularity of wireless medium for communications is mainly because of the broadcast nature, which allows access to multimedia and information without restriction on the user's location. However, guaranteeing secure communication in a wireless medium is made difficult by the same broadcast nature, which makes it easy to eavesdrop on an ongoing communication, while making it nearly impossible to detect eavesdropping. The time-varying and unreliable nature of the wireless channels poses further difficulties. However, the same physical properties, which have a detrimental effect on reliability in communication, provide an opportunity to enhance the secrecy of communication, if used carefully.

The foundation for the theory of secrecy systems was laid by Claude Shannon in [1]. He showed that perfect secrecy can be obtained only if the size of the secret key is at least as large as the size of the message. Perfect secrecy means that the intended receiver can decode the secret message without any error, while the eavesdrop cannot decode the secret message. The underlying assumptions in this analysis were,

- the eavesdropper can utilize infinite computational power and time,
- both the receiver and the eavesdropper receive precisely the same signal.

The first assumption results in the worst case scenario in terms of the resources assumed at the eavesdropper, and therefore, leads to *provable* secrecy. The second assumption may only be valid in certain special cases, e.g., if the channels to both the receiver and the eavesdropper are noiseless. This would be a reasonable model if only the higher layers of networking are of interest, and an idealized (error-free bit

S. Goel (✉)
Carnegie Mellon University, 5000 Forbes Avenue
Pittsburgh, PA
e-mail: satashu@cmu.edu

*Portions of the material have appeared in "Guaranteeing Secrecy using Artificial Noise," IEEE Transactions on Wireless Communications, vol. 7, no. 6, June 2008, ©IEEE 2008.

pipe) model for the physical layer can be used. However, this restrictive assumption results in the pessimistic result mentioned above.

In cryptography, the effect of the physical layer is usually ignored, and secrecy is ensured through encoding and decoding at a higher layer. In particular, it is assumed that both the receiver and the eavesdropper receive exactly the same message, and the encoding and decoding process is known to both of them. The secret key is assumed known only to the receiver and the transmitter. The eavesdropper must determine the secret key (and hence, the secret message) from the received signal. However, the key must be at least as large as the secret message itself, based on Shannon's result mentioned above. The key assumption that allows the cryptographic algorithms to provide secrecy using a key much smaller than the message is that the eavesdropper has limited computing resources and time. The difficulty in decrypting the received signal is often based on a known difficult problem, e.g., prime factorization [2].

In many practical systems, the eavesdropper may have a worse channel than the receiver, e.g., if the eavesdropper *wire-taps* the receiver's channel, thus experiencing noise from both the receiver's channel and its own channel. This wire-tap channel model was analyzed in [3], which showed that in fact perfect secrecy can be guaranteed for a non-zero information rate, if the eavesdropper has a degraded channel compared to the eavesdropper. Perfect secrecy is possible for the wire-tap channel, because of the relaxed assumption on the signal received by the eavesdropper. The system was characterized by *secrecy capacity*, which is the maximum possible rate for which perfect secrecy can be achieved. In this analysis, the eavesdropper was assumed to have unlimited computing resources and time, unlike the assumption in cryptography, and therefore, the secrecy is provable. The secrecy results were obtained using information theoretic tools, and hence, this form of secrecy is called information theoretic secrecy. The secrecy guarantees, in this case, are closely related to the physical layer model, which is ignored in the cryptographic approach.

In a broadcast medium, the eavesdropper and the receiver will, in general, have different channels, and hence, the degraded (wire-tap) channel model may not hold. Communication of secret messages over broadcast channels was considered in [4], which showed that perfect secrecy can be guaranteed for a non-zero information rate, if the eavesdropper's channel is worse than the receiver's channel. In a wireless environment, there is no guarantee that the eavesdropper's channel will be worse than the receiver's channel. For example, the eavesdropper may have a larger channel gain if it is closer to the transmitter, compared to the receiver. Further, the effective channel gain may be increased using directional antennas [5]. If the eavesdropper channel turns out to be better than the receiver's channel, secrecy capacity is zero. It may appear that provable secrecy cannot be guaranteed in such a scenario. How can we design a communication system, which can overcome the eavesdropper's advantage of a better channel? In this chapter, we will show that it is in fact possible to utilize communication theoretic ideas to ensure secrecy of communication, even when the eavesdropper may have a better channel. In particular, we will show how multiple transmit antennas may be used to obtain non-zero secrecy capacity. The key idea in this chapter is that the transmitter can use the degrees of freedom, provided by multiple transmit antennas, to enhance the rate of secret communication, instead of

using them to increase the information rate. The method essentially involves creating intentional uncertainty or “artificial noise”.

The remainder of the chapter is organized as follows. Section 2.2 provides an overview of the key results on perfect secrecy that will be used in this chapter. Section 2.3 formally describes the system under consideration and the assumptions involved. Section 2.4 presents the scheme for introducing intentional uncertainty in the transmitted signal to obtain secrecy. The scheme is first described in a simple scenario in Sect. 2.4.1. The scheme is then generalized to the multiple input multiple output (MIMO) scenario in Sect. 2.4.3. Section 2.5 describes the related work on achieving perfect secrecy over wireless channels. Finally, Sect. 2.6 concludes this chapter.

2.2 Overview of Secrecy Capacity

In this section, we will provide a brief overview of relevant results on information theoretic secrecy. The notion of secrecy capacity was introduced in [3]. The paper considered a wire-tap model, where the eavesdropper’s channel is a degraded version of the receiver’s channel. Secrecy capacity for the *Gaussian* wire-tap channel was obtained in [6]. As a generalization of the wire-tap model, secrecy capacity for broadcast channels was obtained in [4]. We now present the assumptions and results used in the wiretap model, and the broadcast model. We denote the sequence $h^k \doteq (h_1, h_2, \dots, h_k)$.

2.2.1 Assumptions

We first present the assumptions common to the various models considered in information theoretic secrecy. Additional assumptions, specific to a given model, will be presented along with the description of the model. In contrast to the cryptographic approach, it is assumed that the transmitter and the intended receiver do not share a secret key. Thus, the information theoretic secrecy schemes discussed in this chapter enable secret communication without requiring a prior exchange of a secret key, although the guaranteed information rates may be smaller. The advantages of both these approaches can be utilized by using the provable information theoretic secrecy schemes to establish a shared secret key, and then use the traditional symmetric key encryption to achieve a higher information rate. Authentication, however, is assumed, meaning that the transmitter and the receiver can verify each others identity. Alternatively, a passive eavesdropper is assumed which only listens but does not transmit.

It is assumed that both, the receiver and the eavesdropper can estimate their own channels perfectly. The transmitter is assumed to know the receiver’s channel through (authenticated) feedback. However, it does not know the eavesdropper’s channel, since the eavesdropper is passive. Further, the transmitter may not know the location, or the presence, of the eavesdropper(s). Thus, this chapter considers secrecy of communication under the assumption that the eavesdropper’s channel gain is not known to the transmitter.

2.2.2 Wire-Tap Model

The wire-tap model was introduced in [3]. In contrast to Shannon's assumption of both the receiver and the eavesdropper receiving the same signal [1], the paper assumed that the eavesdropper puts a wire-tap on the receiver's channel, and hence, receives a degraded version of the signal at the receiver. The key property that enabled secret communication in this case, even in the absence of a shared secret key, was that the eavesdropper's channel is noisier than the receiver's channel. The wire-tap model is appropriate for wireline systems.

The transmitter encodes a block of K symbols of the secret message into a block of N coded symbols. That is, secret message m^K is encoded into symbols x^N , which is the input to the receiver's channel. The output of the receiver's channel is $z^N = f(x^N)$, where $f(\cdot)$ is a random mapping. The receiver estimates the secret message based on z^N . z^N is the input to the wire-tap channel, whose output $y^N = g(z^N)$ is observed by the eavesdropper, where $g(\cdot)$ is another random mapping. The eavesdropper tries to decode the secret message based on y^N . The rate of secret information is given by $R = H(m^K)/N$, which is the per symbol entropy of the secret message. The eavesdropper's uncertainty about the secret message, after it has observed y^N , is measured by *equivocation* per source letter $R_e \doteq H(m^K|y^N)/K$. For simplification in notation, we can normalize equivocation by the source entropy per source letter, resulting in *fractional equivocation* $\Delta \doteq H(m^K|y^N)/H(m^K)$ [6]. The achievable rate region in terms of (R, Δ) was obtained in [3]. The specific case where $\Delta = 1$ has special significance, since $\Delta = 1$ ensures that the eavesdropper is as ignorant of the secret message after observing y^N , as it was before observing y^N . That is, observing the output of the wire-tap channel does not increase eavesdropper's knowledge about the secret message. Thus, *perfect secrecy* is said to be achieved if $\Delta = 1$. Rate R is achievable with perfect secrecy if for every $\epsilon > 0$, there exists a (k, n) code such that $k/n > R - \epsilon$, $\Delta > 1 - \epsilon$, and $Pr\{\text{decoding error}\} < \epsilon$ at the receiver. Essentially, perfect secrecy means that the receiver can decode the secret message with negligible decoding error probability, while the eavesdropper cannot decode the secret message. Further, *secrecy capacity* C_s was defined as the maximum achievable rate R such that perfect secrecy is maintained (i.e., $\Delta = 1$). Wyner [3] showed that for most channels, a non-zero secrecy capacity is achievable, i.e., $C_s > 0$, assuming that the eavesdropper's channel is a degraded version of the receiver's channel.

Note that the secrecy condition $\Delta = 1$ restricts the rate at which the eavesdropper can obtain the secret information. A stricter secrecy condition can be used for discrete memoryless channels, which restricts the total amount of secret information obtained by the eavesdropper without any reduction in the secrecy capacity, as shown by [7]. However, it is not known if a similar result holds for the Gaussian case considered in this chapter. Therefore, we will use the secrecy condition presented above.

The secrecy capacity for the Gaussian wire-tap channel was obtained in an explicit form in [6]. Both the receiver's and eavesdropper's channels were assumed to be additive white Gaussian noise (AWGN) channels, with the channel outputs given by,

$$z_k = x_k + n_k, \quad (2.1)$$

$$y_k = z_k + e_k, \quad (2.2)$$

where n_k and e_k are i.i.d. additive white Gaussian noise (AWGN) samples with variances σ_n^2 and σ_e^2 , respectively, and they are independent of each other. Thus, the equivalent transmitter-eavesdropper channel is an AWGN channel with noise variance $\sigma_n^2 + \sigma_e^2$. An average power constraint (over a codeword of length N) of P_0 was assumed, so that

$$\frac{1}{N} \sum_{i=1}^N \mathbf{E}[X_i^2] \leq P_0. \quad (2.3)$$

It was shown that the secrecy capacity for the Gaussian wire-tap model is given by,

$$C_s = \frac{1}{2} \log(1 + P_0/\sigma_n^2) - \frac{1}{2} \log(1 + P_0/(\sigma_n^2 + \sigma_e^2)). \quad (2.4)$$

The secrecy capacity, in this case, is given by the difference in the capacity of the receiver's channel and that of the eavesdropper's channel. Further, note that the secrecy capacity is positive for any power P_0 as long as $\sigma_e > 0$, i.e., as long as the eavesdropper's channel is degraded. An important question was whether the existence of non-zero secrecy capacity is only possible for the wire-tap model (which is a good model for wireline systems, but not for wireless systems).

2.2.3 Broadcast Model

In [4], the more general broadcast channel model was considered, where the eavesdropper's channel need not be a degraded version of the receiver's channel. In this model, the receiver and the eavesdropper have separate channels, and x^N is the input to both the channels. The outputs of these channels z^N and y^N are observed by the receiver and the eavesdropper, respectively. This is a more appropriate model for communication over the wireless broadcast channel. Again, perfect secrecy was defined in terms of equivocation, and secrecy capacity C_s was defined as the maximum rate at which secret information can be sent to the receiver, under perfect secrecy. It was shown that the secrecy capacity is given by [4],

$$C_s = \max[I(U; Z) - I(U; Y)], \quad (2.5)$$

where the maximization is over the joint distributions of random variables U, X which satisfy the Markov chain $U \rightarrow X \rightarrow YZ$. Instead of attempting to find the optimal transmission strategy, we will consider a particular strategy for generating the codeword x^N . Therefore, we obtain an achievable lower bound to Eq. (2.5). Notice that the term to be maximized in Eq. (2.5) is the difference in the mutual information between the transmitter and the receiver versus the eavesdropper. This

is similar to the difference in channel capacities in Eq. (2.4) but this result holds for more general channels.

We will use the result in Eq. (2.5), since the focus of this chapter is on secure communication over wireless channels. However, the eavesdropper can use the physical properties of the wireless medium to ensure that its channel is not worse than the receiver's channel, forcing the secrecy capacity to zero. For example, the eavesdropper may move closer to the transmitter than the receiver, or it can use directional antennas to increase its overall channel gain. We take a concrete example to show how such a scheme may affect secrecy capacity.

2.2.4 A Motivating Example

Let us consider a simple example where all the nodes—transmitter, receiver, and eavesdropper, have a single antenna each. We assume a simple flat-fading channel model [8] for both the transmitter-receiver and transmitter-eavesdropper channels. x_k is the transmitted symbol at time k , whereas z_k and y_k are the output samples of the receiver and eavesdropper channels, respectively, at time k . The output samples z_k and y_k are related to the transmitted symbol as,

$$z_k = h_k x_k + n_k, \quad (2.6)$$

$$y_k = g_k x_k + e_k, \quad (2.7)$$

where h_k and g_k are the time-varying channel gains in the receiver and eavesdropper channel, respectively. n_k and e_k are i.i.d. additive white Gaussian noise samples with variance σ_n^2 and σ_e^2 , respectively. A block fading model is assumed for h_k and g_k , meaning that they remain constant for a block of large number of symbols, and are independent across blocks. The assumption of constant h_k and g_k over a large number of symbols allows us to apply information theoretic results Eq. (2.5) in each block. The variation of h_k and g_k from block to block allows us to model the time-varying nature of a wireless channel (assuming the variation is slow). Across blocks, h_k and g_k are assumed to be complex numbers, i.i.d. Gaussian distributed (assuming Rayleigh fading), and independent of each other. A power constraint of P_0 is assumed, similar to Eq. (2.3). The average SNR at the receiver is given by $SNR_r = \mathbf{E}[|h_k|^2]P_0/\sigma_n^2$. Similarly, the average SNR at the eavesdropper is given by $SNR_e = \mathbf{E}[|g_k|^2]P_0/\sigma_e^2$.

The capacity of the transmitter-receiver channel is given by,

$$C = \log(1 + |h_k|^2 P_0 / \sigma_n^2). \quad (2.8)$$

The secrecy capacity is given by [4],

$$C_s = \left(\log(1 + |h_k|^2 P_0 / \sigma_n^2) - \log(1 + |g_k|^2 P_0 / \sigma_e^2) \right)^+, \quad (2.9)$$

where $(x)^+ \doteq \max(0, x)$. Note that both capacity C and secrecy capacity C_s are random variables, since they depend on h_k and g_k , which are random. We will

evaluate the performance in terms of outage probability. An outage occurs if the capacity (or the secrecy capacity) is smaller than a certain fixed value, called *outage capacity*, i.e., probability that a certain outage capacity cannot be supported. The secrecy requirements may be specified in terms of a certain outage probability, say 10^{-3} , at a desired outage capacity. For capacity, the outage probability for a certain outage capacity C_{outage} is defined as $\Pr\{C < C_{\text{outage}}\}$. Outage probability for secrecy capacity is defined similarly. Another metric of interest may be expected capacity, which can be readily computed from the outage capacity versus outage probability curve.

Let us consider a specific scenario, to study the behavior of secrecy capacity. Assume that $SNR_e = SNR_r = 20$ dB (this can happen if they are at the same distance from the transmitter). The secrecy capacity will be zero whenever $|h_k| \leq |g_k|$ (assuming $\sigma_n^2 = \sigma_e^2$). It is easily seen using the symmetry of the problem, that the probability of this event is 1/2. Thus, $C_s = 0$ with probability 1/2. Clearly, the performance will be much worse when SNR_e is larger.

The outage probabilities for capacity C and secrecy capacity C_s , for various SNR_e , are shown in Fig. 2.1. The capacities are measured in nats/symbol (instead of bits/symbol), which means that we use $\log_e(\cdot)$ for calculating entropy. SNR_r is fixed at 20 dB, while SNR_e is varied from 10 to 30 dB. A higher SNR_e implies that the eavesdropper is closer to the transmitter, which results in a higher outage probability. For capacity, an outage probability of 10^{-2} can be achieved for $C_{\text{outage}} \sim 0.7$ nats/symbol. For secrecy capacity, however, even an outage probability of 10^{-1} can be barely achieved for an outage capacity of 0.1 nats/symbol, even when the eavesdropper's channel is 10 dB worse than the receiver's channel. In this chapter, the focus is on the worst case performance when the eavesdropper's SNR is much better than the receiver's SNR. However, the performance degrades rapidly as SNR_e increases. Clearly, the performance will not be good enough at large SNR_e , as evidenced from the plot for $SNR_e = 30$ dB. Note the rapid decay in performance with increasing SNR_e . Ideally, we would like to guarantee a low outage probability for secrecy capacity at a non-negligible outage capacity. The results in Fig. 2.1, however, suggest that providing such guarantees may be extremely difficult.

We will now present a secrecy scheme which uses the degrees of freedom provided by multiple transmit antennas, to add artificially generated noise to the secret message such that the eavesdropper is unable to decode the message. The receiver, on the other hand, can still decode the message, since the *artificial noise* is generated such that the receiver's channel is not affected. We will introduce the system model and notation in the next section.

2.3 System Description

In this section, we formally present the system model and notation. We begin by describing the scenario, and then discuss the assumptions of our model. We denote vectors and matrices with bold font, and the Hermitian operator by \dagger .

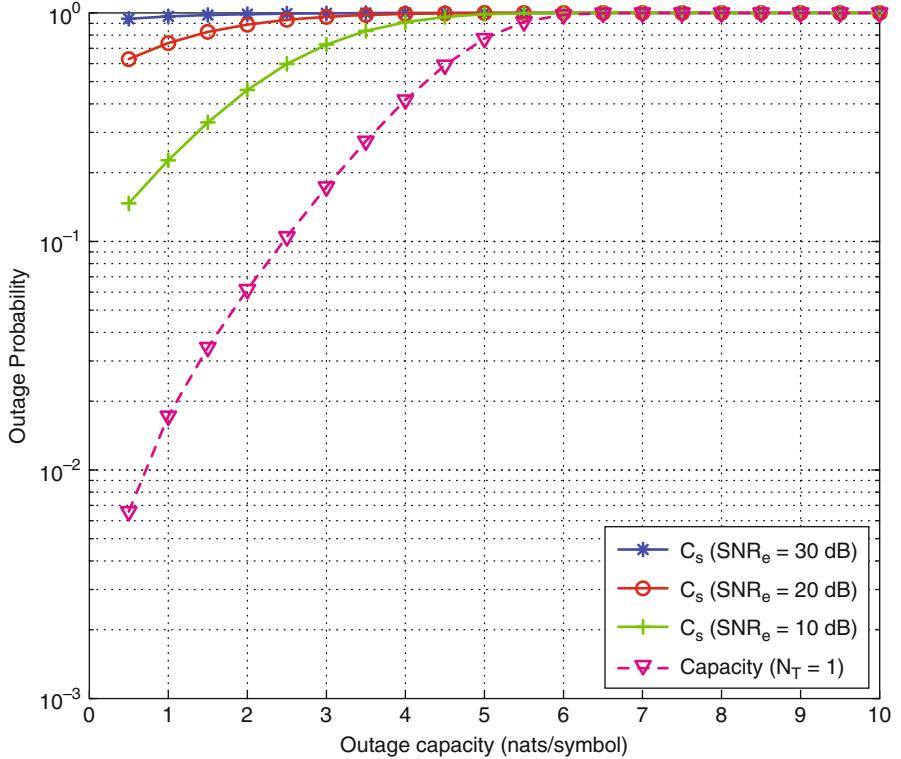


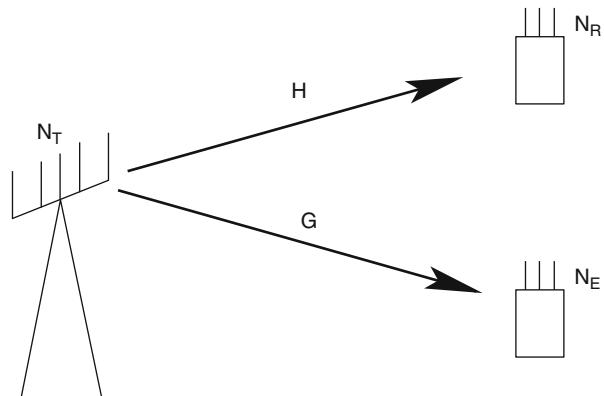
Fig. 2.1 Outage probability

2.3.1 Scenario

We consider the scenario where a transmitter wants to send information to the intended receiver secretly, over a wireless link, so that a passive eavesdropper cannot decode the secret information. This scenario is shown in Fig. 2.2. The transmitted signal propagates through the wireless medium and is received by both the receiver and the eavesdropper. The received signal suffers from both path loss and additive noise. The transmitter, receiver, and eavesdropper are assumed to have N_T , N_R , and N_E antennas respectively. The transmitter-receiver channel at time k is denoted by the $N_R \times N_T$ matrix \mathbf{H}_k . The j^{th} row of \mathbf{H}_k relates the received signal at the j^{th} receive antenna to the transmitted signal. In particular, the element of \mathbf{H}_k denoted by $h_{i,j}$, is the channel gains from transmit antenna i to receive antenna j . If \mathbf{x}_k is the transmitted signal, and \mathbf{z}_k is the received signal, both at time k , then the received signal is given by,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \quad (2.10)$$

Fig. 2.2 Framework for secrecy capacity



where the components of \mathbf{n}_k are i.i.d. Additive White Gaussian Noise (AWGN) samples with variance σ_n^2 . Similarly, the transmitter-eavesdropper channel is denoted by the $N_E \times N_T$ matrix \mathbf{G}_k , and signal received by the eavesdropper (\mathbf{y}_k) is given by,

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k, \quad (2.11)$$

where the components of \mathbf{e}_k are i.i.d. Additive White Gaussian Noise (AWGN) samples with variance σ_e^2 .

The multiple antennas at the eavesdropper can also be used as a model for multiple eavesdroppers, each with a single antenna, colluding to decode the secret information. A single eavesdropper with multiple antennas (equal to the number of eavesdroppers each with a single antenna) will model the case where the received signal from all the eavesdroppers can be processed by a central node, and thus, represents the worst case scenario in terms of maintaining secrecy.

The secrecy condition is defined in terms of fractional equivocation, defined as $\Delta \doteq H(m^K|\mathbf{y}^N)/H(m^K)$. Perfect secrecy is achieved if $\Delta = 1$. Secrecy capacity C_s is defined as the maximum rate at which secret information may be sent to the receiver, under perfect secrecy.

2.3.2 Assumptions

We assume that both, the receiver and the eavesdropper can estimate their own channels perfectly. The transmitter is assumed to know the receiver's channel \mathbf{H}_k through (authenticated) feedback over the wireless channel. However, it does not know the eavesdropper's channel \mathbf{G}_k , since the eavesdropper is passive. The eavesdropper, on the other hand, is assumed to know both the receiver's channel (since the receiver broadcasts its channel \mathbf{H}_k) as well as its own channel. This represents the best possible scenario for the eavesdropper.

Both the receiver's and the eavesdropper's channels are assumed to be slowly varying. A block fading model is assumed, meaning that the channel gain matrices \mathbf{H}_k and \mathbf{G}_k remain constant over a *block* of large number of symbols, and the gains are independent across blocks. The block fading model allows the application of information theoretic results in each block separately, where the channel gains are fixed. In each block, one codeword is transmitted, spanning the length of the block. The codeword is generated using an encoder chosen for the particular block based on the channel gains in the current block.

The transmitter is assumed to have a power constraint of P_0 , i.e., $\mathbf{E}[\mathbf{x}_k^\dagger \mathbf{x}_k] \leq P_0$.

2.4 Intentional Uncertainty Using Multiple Antennas

In Sect. 2.2.4, we saw that the secrecy capacity is close to zero with a high probability when the eavesdropper has a better channel than the intended receiver. This situation may easily occur in the broadcast wireless medium if, either the eavesdropper is closer to the transmitter, or the eavesdropper uses a directional antenna for reception (resulting in higher overall gain). Thus, at the first glance, it seems that guaranteeing information theoretic secrecy in a wireless environment may not be possible. Ideally, we would like to design a secrecy scheme which can guarantee non-zero secrecy capacity, even when the eavesdropper has a better channel than the receiver. However, this must be achieved without assuming the secrecy of channel gain information, and without the knowledge of the eavesdropper's location or its channel gain information. This section will present a secrecy scheme which shows that it is indeed possible to achieve non-zero secrecy capacity under the above stated conditions.

As shown in the previous section, the lower bound on secrecy capacity is the difference of two terms. The first term is the mutual information between the transmitter and the receiver $I(X; Z)$. An upper bound on this term is the capacity of the transmitter-receiver link. From the first term, we must subtract the mutual information between the transmitter and the eavesdropper $I(X; Y)$. For fixed channels \mathbf{H}_k , \mathbf{G}_k and given the statistics for \mathbf{x}_k , mutual information $I(X; Y)$ is fixed. Ideally, we would like to minimize the mutual information term $I(X; Y)$, while at the same time, maximize $I(X; Z)$. How can this be done, if the eavesdropper's channel \mathbf{G}_k is not known (since $I(X; Z)$ depends on \mathbf{G}_k)? One way to achieve this would be to somehow degrade the eavesdropper's channel, perhaps by introducing some intentional uncertainty in the transmitted signal. However, the uncertainty must be introduced such that the receiver's channel is unaffected. Further, the uncertainty must degrade the eavesdropper's channel substantially, regardless of the position of the eavesdropper. It may seem unlikely that designing such a scheme is at all possible. We now present a method for obtaining secrecy by introducing intentional uncertainty in the form of *artificial noise*. For simplicity in presentation, we will first present the case where the receiver and the eavesdropper each have a single antenna only, while the transmitter has multiple antennas.

2.4.1 Artificial Noise Generation Using Multiple Transmit Antennas

We now describe an approach that can selectively degrade the eavesdropper's channel. This is achieved by transmitting artificially generated noise along with the information signal. Formally, the transmitter chooses the transmitted signal \mathbf{x}_k as the *sum* of the information bearing signal \mathbf{s}_k and the *artificial noise* signal \mathbf{w}_k ,

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k. \quad (2.12)$$

The artificial noise is transmitted so that the intended receiver does not receive additional noise. This is achieved by generating the artificial noise such that it lies in the null space of the receiver's channel \mathbf{H}_k , i.e., $\mathbf{H}_k \mathbf{w}_k = \mathbf{0}$. Then, the received signal at the receiver is,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k. \quad (2.13)$$

Note how the artificial noise is nulled by the receiver's channel. Thus, the receiver only receives the information bearing signal, corrupted by AWGN. The transmit power dedicated to the information bearing signal, given by $P_{info} = \mathbf{E}[\mathbf{s}_k^\dagger \mathbf{s}_k]$, is smaller than the total transmit power P_0 , since some of the transmit power is used for artificial noise. This limits the information rate for secret information. The eavesdropper's channel \mathbf{G}_k is, in general, different from the receiver's channel \mathbf{H}_k . Hence, the artificial noise will not be nulled out in the eavesdropper's case. Indeed, the received signal for the eavesdropper is given by,

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k. \quad (2.14)$$

Note that the artificial noise is present in Eq. (2.14), as opposed to Eq. (2.13). The artificial noise \mathbf{w}_k is generated as complex Gaussian random vector in the null space of \mathbf{H}_k . In particular, if \mathbf{Z}_k is an orthonormal basis for the null space, meaning that $\mathbf{Z}_k^\dagger \mathbf{Z}_k = I$, then $\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$, where the elements of \mathbf{v}_k are i.i.d. complex Gaussian random variables, independent of each other, each with mean zero and variance σ_v^2 . The components of \mathbf{w}_k are Gaussian distributed as well but are not independent of each other. For the eavesdropper, both \mathbf{e}_k and $\mathbf{G}_k \mathbf{w}_k$ act as noise. Therefore, the eavesdropper's channel has an effective noise power of $\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2$. Using Eq. (2.5), the secrecy capacity lower bound, in this case, is given by,

$$C_s \geq C_{sec} = \left(I(Z; U) - I(Y; U) \right)^+ \quad (2.15)$$

$$= \left(\log \left(1 + \frac{|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2} \right) - \log \left(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{\mathbf{E}|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2} \right) \right)^+. \quad (2.16)$$

We have obtained a lower bound here, since we are using a specific scheme for introducing artificial noise, which may not be optimal.

Since the eavesdropper is passive, the transmitter is unaware of the eavesdropper's channel \mathbf{G}_k , and hence, it chooses the transmitted signal vector \mathbf{s}_k to maximize the

first term in Eq. (2.15). This is achieved by matching the signal vector \mathbf{s}_k to its channel \mathbf{H}_k , so that $\mathbf{s}_k = \mathbf{p}_k u_k$, where $\mathbf{p}_k = \mathbf{H}_k^\dagger / \|\mathbf{H}_k\|$, and u_k is the information signal. Thus, the secret message is transmitted in the range space of \mathbf{H}_k , while the artificial noise is transmitted in its null space. Hence, the two kind of signals are transmitted in orthogonal sub-spaces.

Intuitively, the outage probability of secrecy capacity should improve substantially as the number of transmit antennas increase. The secret message is always transmitted in the range space of \mathbf{H}_k , which is one dimensional here. The artificial noise, on the other hand, is transmitted in all the remaining dimensions ($N_T - 1$). As N_T increases, the probability that \mathbf{G}_k has a large component along \mathbf{H}_k reduces rapidly, since \mathbf{H}_k spans only 1 out of N_T dimensions. On the other hand, the probability of \mathbf{G}_k having a large component in the null space of \mathbf{H}_k increases rapidly, since the null space spans $N_T - 1$ out of N_T dimensions. Thus, with a high probability, $\mathbf{G}_k \mathbf{p}_k$ is small, while $\mathbf{G}_k \mathbf{w}_k$ is large, leading to a small $I(Y; U)$ based on Eq. (2.16).

Note the differences between Eq. (2.16) and Eq. (2.9). In Eq. (2.16), the first term involves σ_u^2 instead of P_0 , since only part of the available transmit power is used to transmit the information bearing signal. The rest of the power is transmitted as artificial noise, which only affects the eavesdropper's channel, as shown by the second term in Eq. (2.16).

The secrecy capacity lower bound C_{sec} obtained in Eq. (2.16) is a random variable because it depends on random channel gains \mathbf{H}_k and \mathbf{G}_k . In this scenario, the metrics of interest are the average of secrecy capacity and its outage probability. Even though \mathbf{G}_k is unknown at the transmitter, its statistics may be known. The average is taken over the random channel gains \mathbf{H}_k and \mathbf{G}_k to yield,

$$\overline{C_{sec}} \doteq \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathbf{E}_{\mathbf{H}_k, \mathbf{G}_k} [C_{sec}]. \quad (2.17)$$

The outage probability for a given outage capacity C_{outage} is the probability that the secrecy capacity lower bound is smaller than the outage capacity, i.e., $\Pr\{C_{sec} < C_{outage}\}$.

We will now show how the artificial noise is different from AWGN, even though both of them affect the eavesdropper in the same manner. Equation (2.16) holds for specific values of noise powers σ_n^2 and σ_e^2 . In practice, the thermal noise power depends on temperature and bandwidth, while the channel gains are dependent on the transmitter-receiver distance. For convenience, let us normalize Eq. (2.16) by a factor of $\|\mathbf{G}_k\|$, so that the distance between the transmitter and the eavesdropper is modeled not by the channel gains $\|\mathbf{G}_k\|$, but by the noise power σ_e^2 . Thus, we can study the effect of eavesdropper's position on the secrecy capacity lower bound.

The key problem that we noticed in Sect. 2.2.4 was that the eavesdropper may have a better channel than the receiver, if it is closer to the transmitter, or if it uses a directed antenna for reception. This would imply a smaller σ_e^2 . In terms of maintaining secrecy, the worst case scenario would occur if $\sigma_e^2 \rightarrow 0$, i.e., if the eavesdropper's channel is noiseless. This is the *minimum* secrecy capacity that can be guaranteed regardless of the eavesdropper's position. Hence, it is called minimum

guaranteed secrecy capacity and is given by [9],

$$C_{sec,mg} = \left(\log \left(1 + \frac{\|\mathbf{H}_k\|^2 \sigma_u^2}{\sigma_n^2} \right) - \log \left(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{(\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2} \right) \right)^+. \quad (2.18)$$

Notice that in the absence of artificial noise ($\sigma_v^2 = 0$), the second term in Eq. (2.18) will be infinite, leading to minimum guaranteed secrecy capacity lower bound being identically zero, i.e., $C_{sec,mg} \doteq 0$. The presence of artificial noise limits the second term in Eq. (2.18) (mutual information between the transmitter and the eavesdropper), allowing for non-zero minimum guaranteed secrecy capacity. Further, the choice of σ_v^2 lies with the transmitter, and it can be increased up to the total available power P_0 to ensure secrecy in communication, unlike thermal noise power which is fixed.

Again, $C_{sec,mg}$ in Eq. (2.18) is a random variable, since it depends on the random channel gains \mathbf{H}_k and \mathbf{G}_k . Appropriate values for σ_u^2 and σ_v^2 are chosen based on the statistics of \mathbf{H}_k and \mathbf{G}_k . The average minimum guaranteed secrecy capacity is defined by taking expectation of $C_{sec,mg}$ over \mathbf{H}_k and \mathbf{G}_k , and by choosing the optimum σ_u^2 and σ_v^2 . Formally,

$$\overline{C_{sec,mg}} \doteq \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathbf{E}_{\mathbf{H}_k, \mathbf{G}_k} [C_{sec,mg}]. \quad (2.19)$$

The outage probability for a given outage capacity C_{outage} is given by $Pr\{C_{sec,mg} < C_{outage}\}$.

2.4.2 Example

We now present an example to show the efficacy of the artificial noise technique, in providing secrecy. We compare the outage probability obtained, when using the artificial noise technique, with that obtained without the artificial noise. The artificial noise is generated using five transmit antennas. The receiver and the eavesdropper are assumed to have one antenna each. 70% power was used for the information signal (i.e., $\sigma_u^2/P_0 = 0.7$), while rest of the power was used for generating artificial noise.

In Fig. 2.3, we have superimposed the results obtained using artificial noise ($N_T = 5$), with the results in Fig. 2.1. The figure shows that the outage curve for capacity has improved. Instead of ~ 0.7 nats/symbol, now ~ 5 nats/symbol can be guaranteed at an outage probability of 10^{-2} . However, the improvement in the outage curve for secrecy capacity is far more dramatic. In contrast to not being able to provide any rate guarantees at outage probability of even 10^{-1} (assuming $SNR_e \geq 20$ dB), we can now guarantee a secrecy rate of ~ 3 nats/symbol at outage probability of 10^{-2} for the worst case scenario ($SNR_e \rightarrow \infty$). Note that the outage capacities for secrecy capacity and capacity are of the same order.

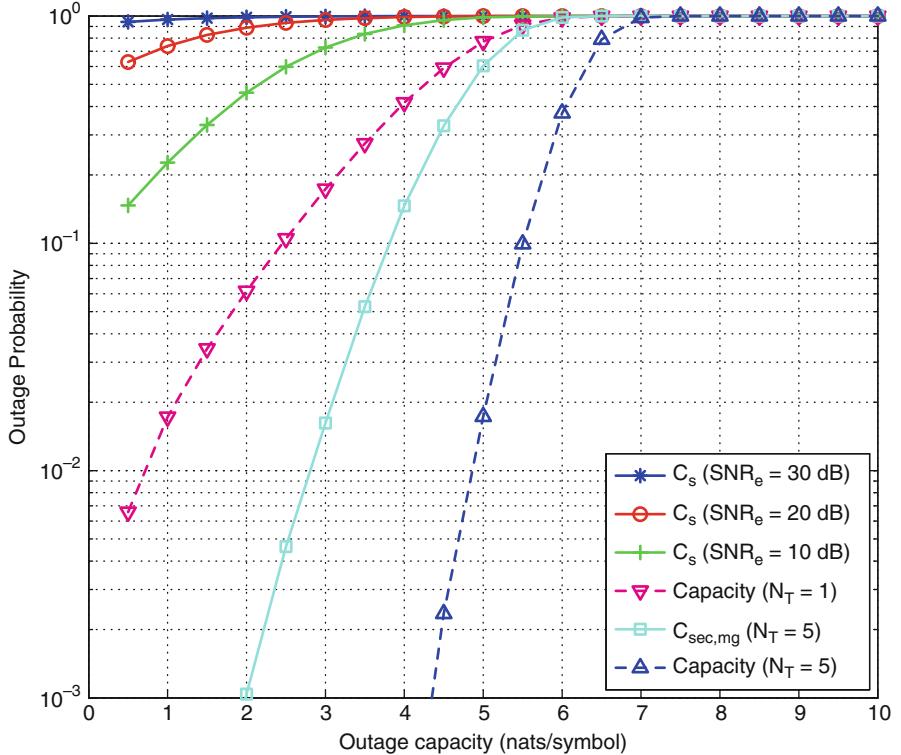


Fig. 2.3 Outage probability using artificial noise

2.4.3 Artificial Noise Generation in MIMO Scenario

Section 2.4.1 showed how artificial noise can be used to attain low outage probability for secrecy capacity, when both the receiver and the eavesdropper have a single antenna each. The scheme presented there can be extended to a more general scenario, where all the nodes—transmitter, receiver and eavesdropper may have multiple antennas. However, the artificial noise must be generated more carefully in this case. In particular, it is important to determine the number of dimensions to use for the artificial noise versus the information bearing signal, to ensure that minimum guaranteed secrecy capacity is non-zero.

Since we now have a matrix channel in Eq. (2.13), we will need to use results on multiple input multiple output (MIMO) capacity. For the receiver's channel given by Eq. (2.13), the capacity is given by $\log |\mathbf{I} + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger / \sigma_n^2|$ (see [10] for details), where $\mathbf{Q}_s = \mathbf{E}[\mathbf{s}_k \mathbf{s}_k^\dagger]$ is the covariance matrix for the information signal \mathbf{s}_k , which is Gaussian distributed. Notice that this capacity expression reduces to $\log(1 + |\mathbf{H}_k|^2 \sigma_u^2 / \sigma_n^2)$ (in Eq. (2.16)), when $N_R = 1$.

The eavesdropper has a matrix channel as well, and the noise $\mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k$ is characterized by the covariance matrix given by ([9]),

$$\mathbf{K} = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2 + \mathbf{I} \sigma_e^2. \quad (2.20)$$

As discussed in Sect. 2.4.1, the worst-case situation occurs when the eavesdropper has a noiseless channel, i.e., $\sigma_e^2 \rightarrow 0$. Then, the only noise received by the eavesdropper is the artificial noise, and hence, the noise covariance matrix is given by,

$$\mathbf{K}' = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2. \quad (2.21)$$

The capacity of the eavesdropper's channel is $\log(|\mathbf{K}' + \mathbf{G}_k \mathbf{Q}_s \mathbf{G}_k^\dagger|/|\mathbf{K}'|)$ [10].

Therefore, the minimum guaranteed secrecy capacity in this case is given by [9],

$$C_{sec,mg} = \log|\mathbf{I}\sigma_n^2 + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger| - \log(|\mathbf{K}' + \mathbf{G}_k \mathbf{Q}_s \mathbf{G}_k^\dagger|/|\mathbf{K}'|), \quad (2.22)$$

where $\mathbf{Q}_s = \mathbf{E}[\mathbf{s}_k \mathbf{s}_k^\dagger]$ and \mathbf{s}_k is complex Gaussian distributed. Further, $\mathbf{K}' = (\mathbf{G}_k \mathbf{Z}_k \mathbf{Z}_k^\dagger \mathbf{G}_k^\dagger) \sigma_v^2$. We immediately note that in order to avoid the case $|\mathbf{K}'| = 0$, the rank of \mathbf{Z}_k (which lies in the null-space of \mathbf{H}_k), must be at least N_E . Therefore, the transmitter must use at least N_E dimensions to transmit artificial noise, say N_{ND} dimensions. The remaining dimensions ($N_T - N_{ND}$) can be used to transmit the information bearing signal. On the other hand, at most N_R dimensions can be used to transmit the information bearing signal, since the receiver has only N_R antennas. Since both these conditions must be satisfied, the information bearing signal is transmitted in $N_S = \min(N_T - N_{ND}, N_R)$ dimensions. Further details on artificial noise generation may be found in [9]. A key observation in [9] was that the minimum guaranteed MIMO secrecy capacity does not behave like the usual MIMO capacity. In particular, it was shown that the minimum guaranteed MIMO secrecy capacity does not increase monotonically with the minimum of transmitter and receive antennas. This was confirmed both by analytical results in the case of large number of antennas, and simulation results for small number of antennas.

Goel and Negi [9] showed that analytical results can be obtained for secrecy capacity, in the regime of large number of antennas. The paper obtained a lower bound on the average minimum guaranteed secrecy capacity $\overline{C}_{sec,mg}(LB)$ using results from the theory of random matrices [12]. In particular, $\overline{C}_{sec,mg}(LB)$ was obtained in terms of eigenvalues of a Wishart matrix $\tilde{\mathbf{G}}_2 \tilde{\mathbf{G}}_2^\dagger$, where $\tilde{\mathbf{G}}_2$ represents the equivalent channel from the artificial noise signal \mathbf{v}_k to the eavesdropper [9]. The elements of $\tilde{\mathbf{G}}_2$ are i.i.d. complex Gaussian random variables. The eigenvalues are given by [11, 12],

$$p(\lambda) = \begin{cases} \frac{1}{\pi} \sqrt{\frac{\beta}{\lambda} - \frac{1}{4} \left(1 + \frac{\beta-1}{\lambda}\right)^2}, & \text{if } (\sqrt{\beta} - 1)^2 \leq \lambda \leq (\sqrt{\beta} + 1)^2 \\ 0, & \text{otherwise,} \end{cases} \quad (2.23)$$

where β depends on the dimensions of $\tilde{\mathbf{G}}_2$ as $\beta = N_{ND}/N_E$. Then, the lower bound $\overline{C}_{sec,mg}(LB)$ can be obtained as [9],

$$\begin{aligned} \overline{C}_{sec,mg} &\geq \overline{C}_{sec,mg}(LB) = \max_{tr(\mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger) + N_{ND}\sigma_v^2 \leq P_0} \\ &E[\log |\mathbf{I}\sigma_n^2 + \mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger| - \sum_i \log \left(\frac{P_{info} + \lambda_i \sigma_v^2}{\lambda_i \sigma_v^2} \right)], \end{aligned} \quad (2.24)$$

where $P_{info} = tr(\mathbf{H}_k \mathbf{Q}_s \mathbf{H}_k^\dagger)$ is the transmit power of the information signal. $\overline{C}_{sec,mg}(LB)$ was computed numerically in [9] for various values of N_T , N_R , and N_E , and the results were compared with average capacity. The results showed that fairly large average secrecy capacity can be achieved using the artificial noise technique.

2.5 Related Work

In the last decade, several researchers have studied the problem of secret communication over the wireless medium, in presence of a passive eavesdropper.

Koorapaty, Hassan and Chennakeshu [13] presented a scheme for achieving secrecy by using the channel state information (CSI) as the secret key. In particular, the phase of the channel gain was used as the secret key, and was assumed known only to the transmitter and the receiver. The secret information was encoded into the phase of the transmitted signal. The transmitter compensated for the phase of the receiver's channel, so that the receiver could decode the secret message. The phase of the eavesdropper's channel, being different from that of the receiver's channel, in general, prevented the eavesdropper from decoding the message. However, the paper did not analyze the secrecy capacity achieved by this scheme. Hero [14] presented a more general scheme for the MIMO scenario, where perfect secrecy could be achieved under the assumption that the eavesdropper is unaware of its own channel. Essentially, the training sequence was used as the secret key in this case; assumed known only to the transmitter and the receiver. It was shown that the eavesdropper could be kept ignorant of the secret message, by choosing the space-time modulation such that the *spatial inner product* of the transmitted matrix remains constant. Note that while [13, 14] obtained secrecy by using CSI or training sequence as the secret key, the secrecy results presented in this chapter do not assume a shared secret key between the transmitter and the receiver. Li, Chen and Ratazzi [15] considered a MIMO scenario with $N_R = 1$, and an arbitrary number of antennas at the eavesdropper. The paper presented a scheme for introducing intentional ambiguity using multiple transmit antennas. A random beamforming direction was chosen such that the component along the receiver's channel is constant. The key assumption that ensured secrecy was that the eavesdropper is unaware of the receiver's channel, and hence, could not extract the signal component from the ambiguous received signal. The paper did not analyze the secrecy capacity of this scheme. Secrecy capacity for slow fading wireless channels was analyzed in [16], using the results in [4]. The

paper did not use a scheme to degrade the eavesdropper's channel by introducing ambiguity in the transmitted signal. Therefore, a non-zero secrecy capacity is possible only if the eavesdropper has a worse channel than the receiver. A fast fading channel model was considered in [17], under the assumption that the transmitter knows the channels gains of the eavesdropper's channel.

Recently, several researchers have studied the problem of secret communication over MIMO broadcast channels. Computing MIMO secrecy capacity when the eavesdropper's channel is not known at the transmitter is still an open problem. The secrecy problem in the MIMO scenario is made tractable by considering specific achievable schemes, which are not optimal. The problem is simplified by either assuming that no intentional ambiguity is introduced, or by assuming a specific encoding scheme for introducing ambiguity. Note that in the absence of intentional ambiguity (e.g., artificial noise), the secrecy capacity is zero when the eavesdropper's channel is noiseless, as opposed to the results in [9] which uses a stochastic encoder [4] to add artificial noise to the transmitted signal. References [18–21] have considered the MIMO scenario under the assumption that the eavesdropper's channel is known to the transmitter. [18] obtained the secrecy capacity for the MIMO scenario with $N_R = N_E = 1$, analytically. Shafiee, Liu and Ulukus [20] considered the MIMO case with $N_T = N_R = 2$ and $N_E = 1$, and showed that beamforming is the optimal transmission strategy in this case. The MIMO secrecy capacity for any N_T, N_R, N_E was computed in [19, 21]. Shafiee and Ulukus[22] considered the MIMO scenario under the assumption that only the eavesdropper knows its own channel. The paper considered the MIMO case with $N_R = N_E = 1$. It showed that the average secrecy capacity is maximized by beamforming in the direction of the receiver's channel.

Khisti and Wornell [23] considered the MIMO scenario with $N_R = 1$, where the eavesdropper's channel is not known at the transmitter. Instead of trying to find the optimal transmission strategy, the paper analyzed the artificial noise technique presented in [9, 25]. The paper obtained both an upper and a lower bound on the secrecy capacity in the regime of large number of antennas. Further, the paper presents upper and lower bounds on secrecy capacity for the fast fading scenario. The bounds were shown to be tight in the regime of large SNR. However, the paper used a (fixed) sub-optimal power allocation for information bearing signal and the artificial noise signal. In [24], the MIMO scenario with $N_R = N_E = 1$ was analyzed, where the transmitter sends independent confidential messages to two users with perfect secrecy. The paper presented an inner and outer bound for the capacity region.

2.6 Conclusions

The ease of passive eavesdropping in wireless networks poses a difficult challenge in providing secrecy guarantees. In this chapter, we reviewed results on information theoretic secrecy, and demonstrated using an example, that the traditional approaches are not sufficient in providing secrecy guarantees. We then presented a method of introducing intentional ambiguity (artificial noise) in the transmitted signal such that the

eavesdropper's channel is selectively degraded, thus enabling provably secure communication, based on the previous results. This chapter presented a specific scheme for introducing ambiguity in the transmitted signal, which may be sub-optimal. However, with this scheme, non-zero secrecy capacity can be guaranteed even when the eavesdropper has a noiseless channel, since the artificial noise power can be made proportional to the signal power. This is the key attribute of the artificial noise scheme presented in this chapter. Simulation results for a fading channel showed that fairly low outage probabilities can be achieved at non-negligible secrecy rates. We finally note that the problem of determining the optimal transmission strategy for perfect secrecy in a MIMO scenario is still an open problem.

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.
- [2] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [4] I. Csiszar, J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, pp. 339–348, May 1978.
- [5] D. Welch, S. Lathrop, "Wireless security threat taxonomy," *Proc. IEEE Inf. Assurance Workshop 2003* pp. 76–83, Nov. 2006.
- [6] S. Leung-Yan-Cheong, M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [7] U. Maurer, S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *LNCS*, Springer-Verlag, vol. 1807, pp. 352–368, 2000.
- [8] J. Proakis, "Digital Communications," McGraw-Hill, 1989.
- [9] S. Goel, R. Negi, "Guaranteeing secrecy using artificial noise," to appear in *IEEE Trans. Wireless Commun.*, Jun. 2008.
- [10] E. Telatar, "Capacity of multi-antenna Gaussian channels," *Eur. Trans. Telecomm. ETT*, vol. 10, no. 6, pp. 585–596, Nov. 1999.
- [11] B. M. Hochwald, T. L. Marzetta, V. Tarokh, "Multiple-antenna channel hardening and its implications for rate feedback and scheduling," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 1893–1909, Sep. 2004.
- [12] J. W. Silverstein, Z. D. Bai, "On the empirical distribution of eigenvalues of a class of large dimensional random matrices," *J. Mult. Anal.*, vol. 54, pp. 175–192, 1995.
- [13] H. Koropaty, A. A. Hassan, S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Trans. Wireless Commun.*, pp. 52–55, Jul. 2003.
- [14] A. E. Hero, "Secure space-time communication," *IEEE Trans. Inf. Theory*, pp. 3235–3249, Dec. 2003.
- [15] X. Li, M. Chen, E. P. Ratazzi, "Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy," *Proc. IEEE SPAWC 2005*, pp. 811–815, June 2005.
- [16] J. Barros, M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2006*, Jul. 2006.
- [17] Y. Liang, H. V. Poor, S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
- [18] Z. Li, W. Trappe, R. Yates, "Secret communication via multi-antenna transmission," *Proc. CISS '07*, Baltimore, MD, pp. 905–910, Mar. 2007.

- [19] F. Oggier, B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1920v1.pdf
- [20] S. Shafiee, N. Liu, S. Ulukus, “Towards the Secrecy Capacity of the Gaussian MIMO Wire-tap Channel: The 2-2-1 Channel,” *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0709/0709.3541v1.pdf
- [21] A. Khisti, G. W. Wornell, “The MIMOME Channel,” *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.1325v1.pdf
- [22] S. Shafiee, S. Ulukus, “Achievable rates in Gaussian MISO channels with Secrecy constraints,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2007*, Jun. 2007.
- [23] A. Khisti, G. W. Wornell, “Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel,” *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.4219v1.pdf.
- [24] R. Liu, V. Poor, “Multiple Antenna Secure Broadcast over Wireless Networks,” *Preprint*, available at http://arxiv.org/PS_cache/arxiv/pdf/0705/0705.1183v1.pdf.
- [25] S. Goel, R. Negi, “Secret communication in presence of colluding eavesdroppers,” *Proc. MILCOM*, vol. 3, pp. 1501–1506, Nov. 2005.
- [26] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [27] R. Negi, S. Goel, “Secret communication using artificial noise,” *Proc. VTC Fall 2005*, vol. 3, pp. 1906–1910, Sep. 2005.
- [28] G. J. Foschini, M. J. Gans, “On limits of wireless communications in a fading environment when using multiple antennas,” *Wireless Pers. Commun.* Kluwer Academic Press, no. 6, pp. 311–335, 1998.
- [29] U. M. Maurer, S. Wolf, “Unconditionally secure key agreement and the intrinsic conditional information,” *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, Mar. 1999.
- [30] D. Chizhik, J. Ling, P. W. Wolniansky, R. A. Valenzuela, N. E. Costa, K. Huber, “Multiple-input-multiple-output measurements and modeling in Manhattan,” *IEEE J. Select. Areas Commun.*, vol. 21, no. 3, pp. 321–331, Apr. 2003.
- [31] G. J. Foschini, D. Chizhik, M. J. Gans, C. Papadias, R. A. Valenzuela, “Analysis and performance of some basic spacetime architectures,” *IEEE J. Select. Areas Commun., Special Issue on MIMO Systems*, pt. I, vol. 21, pp. 303–320, Apr. 2003.
- [32] J. N. Laneman, D. N. C. Tse, G. W. Wornell, “Cooperative diversity in wireless networks: Efficient protocols and outage behavior,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

Chapter 3

Distributed Secret Sharing over the Gaussian Interference Wiretap Channel

William Luh and Deepa Kundur

3.1 Introduction and Motivation

In the process of secret sharing, a single secret is encoded into multiple entities called shares. These shares possess the special properties that they jointly contain no information about the original secret unless a sufficient quantity of them are available for decoding [1]. There has been a recent trend in applying secret sharing to mobile ad hoc networks [2] because the process of encoding and decoding does not require the use of keying and key management. Furthermore, secret sharing is inherently robust to limited degrees of insider attacks, in which partial knowledge of shares become available to an attacker. However, in many other network scenarios, secret sharing is deemed unsuitable for two reasons. First, each user is required to create multiple shares leading to excessive overhead and unnecessary bandwidth expansion in the network. Second, the routing of the shares to the destination(s) must remain as *separated* as possible so that enough of them do not easily fall into the hands of a restricted enemy who may then successfully decode the original secret. Spatially-restricted enemies can be thwarted somewhat through the use of mobility of intermediate network nodes that provide avenues for different shares to be sent along non-overlapping routes [2].

In this chapter we consider extending secret sharing to another networking framework. Suppose multiple users, each with independent secret messages, must independently and securely transmit their messages to multiple collaborating base stations that jointly decode the secret messages. This may, for example, model cellular uplink and soft handoff [3]. However some of these base stations may experience eavesdropping prior to joint decoding through insider attacks on one or more critical network entities. This is analogous to a distributed storage with secrecy constraint problem. Given the similarity of the proposed threat model to that considered in traditional secret sharing, we propose a “network-friendly” secret sharing solution instead

W. Luh (✉)

Department of Electrical & Computer Engineering
Texas A&M University, College Station, TX 77843, USA
e-mail: luh@ece.tamu.edu

of relying on conventional cryptographic techniques that require key establishment and update phases between users and base stations. An interesting characteristic of our problem is that the received message at each base station contains interference from all the users, which may be conveniently leveraged to enhance secrecy.

Thus we model this problem using an interference channel with additive Gaussian noise, such that the associated broadcast links may have different gains, and a legitimate joint decoder obtains the received signals from all the base stations to successfully decode all the secret messages. The attack is modeled as a wiretapper who acquires signals received from a proper subset of the set of base stations. A distinguishing characteristic of the attack is that users do not know which proper subset of the base stations will be compromised, and thus must protect against any possible combination of corrupted base stations. For this problem, our goal is to find the set of all communication rates such that secrecy is unconditional (i.e., no matter how much time and resources the wiretapper has, the amount of information that can be revealed by the wiretapper's proper subset of shares is negligible), which we call the *secrecy capacity region*. Since the secrecy capacity region is difficult to directly characterize, our analysis instead derives inner and outer regions, representing a subset and a superset of the secrecy capacity region.

3.1.1 Outline of Chapter

In Sect. 3.2 we formally define the above problem. In Sect. 3.3 we will outline the main results, i.e., the inner and outer regions, and provide discussions and interpretations. Specifically we give a numerical example that highlights the construction of the inner region. This example is the basis for an important part of the proof of the inner region. Since our inner region is not general (i.e., it is for the case when all channels have the same “SNR”), we also derive the inner region for a similar problem in which only one of the base stations experiences interference; this is the so called Z-channel. In Sect. 3.4 we will extend our system model such that the links experience slow and flat Rayleigh fading. Finally in Sect. 3.5 we provide the proofs of the results from Sect. 3.3 and in Sect. 3.6 we provide the proof for the fading result from Sect. 3.4.

3.2 System Model

For simplicity we formulate the problem for two nodes. Figure 3.1 models the wireless channel with interference at each of the two base stations. The noise vectors Z_1^n, Z_2^n are independent, and each component in the vector is an independent and identically distributed (i.i.d.) Gaussian random variable (RV), i.e., $Z_i^n = (Z_{i,1}, Z_{i,2}, \dots, Z_{i,n})$ with each $Z_{i,j}$ independent and normally distributed, $\mathcal{N}(0, \sigma_i^2)$, for $i = 1, 2$. The outputs at each of the two base stations are given by

$$Y_1^n = h_1 X_1^n + h_{21} X_2^n + Z_1^n \quad (3.1)$$

$$Y_2^n = h_{12} X_1^n + h_2 X_2^n + Z_2^n, \quad (3.2)$$

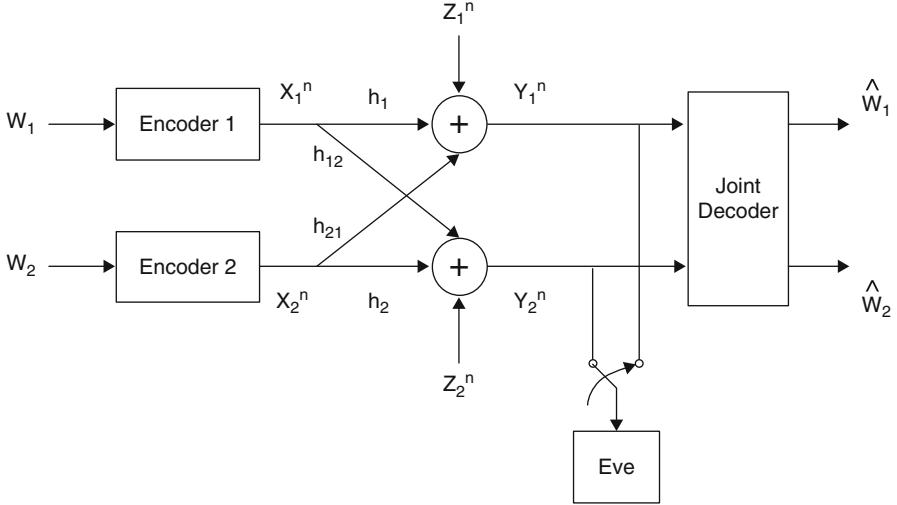


Fig. 3.1 Distributed secret sharing over the Gaussian interference channel with joint decoder and insider attack

respectively. The multiplicative terms h_1, h_2, h_{12}, h_{21} model the gains on the channels. For the first part of our results, we will assume that these are constants, and for the second part (Sect. 3.4) we will study the case when they are random. The channels corresponding to h_{12}, h_{21} model the interference and we also call these *cross-links*. Thus the channel transition probability is factored as $p(y_1, y_2|x_1, x_2) = p(y_1|x_1, x_2)p(y_2|x_1, x_2)$. Furthermore we impose a power constraint on the transmitters

$$\frac{1}{n} \mathbb{E} \|X_i^n\|^2 \leq P_i^{\max} \quad (3.3)$$

for $i = 1, 2$, where each transmitter has its own maximum allowable power given by P_1^{\max}, P_2^{\max} .

Note that our overall setup is different from [4, 5] in that there are no fixed wiretap channels, i.e., the wiretapper can choose either Y_1^n or Y_2^n (but not both), where Y_1^n and Y_2^n are also used by the legitimate joint decoder.

Definition 1 A $(2^{nR_1}, 2^{nR_2}, n)$ code for the wireless distributed secret sharing network depicted in Fig. 3.1 consists of two message sets $\mathcal{W}_i = \{1, \dots, 2^{nR_i}\}$ for $i = 1, 2$ such that W_i is uniformly selected from the set \mathcal{W}_i , two (stochastic) encoding functions $f_i : \mathcal{W}_i \rightarrow \mathcal{X}_i^n$ for $i = 1, 2$, and one decoding function $g : \mathcal{Y}_1^n \times \mathcal{Y}_2^n \rightarrow \mathcal{W}_1 \times \mathcal{W}_2$. Thus the encoding distribution is factored as $p(x_1, x_2|w_1, w_2) = p(x_1|w_1)p(x_2|w_2)$.

Let the average probability of error for the $(2^{nR_1}, 2^{nR_2}, n)$ be defined by

$$P_e^{(n)} = \frac{1}{2^{n(R_1+R_2)}} \cdot \sum_{\substack{(w_1, w_2) \in \\ \mathcal{W}_1 \times \mathcal{W}_2}} \Pr\{(\hat{W}_1, \hat{W}_2) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\}. \quad (3.4)$$

Let secrecy (or confidentiality) be measured by the mutual information, $I(W_1, W_2; Y_i^n)$ for either $i = 1$ or $i = 2$ depending on which Y_i^n the wiretapper selects. This measures the amount of information about the secret messages leaked to the wiretapper via his Y_i^n . Note that the wiretapper is only permitted to select *one* out of the two channel outputs.

Definition 2 A rate pair (R_1, R_2) is *achievable with unconditional secrecy* for the wireless distributed secret sharing network if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that for all $\epsilon > 0$

$$\begin{aligned} P_e^{(n)} &< \epsilon & (3.5) \\ \frac{1}{n} I(W_1, W_2; Y_i^n) &< \epsilon \\ \frac{1}{n} I(W_1; Y_i^n) &< \epsilon \\ \frac{1}{n} I(W_2; Y_i^n) &< \epsilon & (3.6) \end{aligned}$$

for $i = 1, 2$, for n sufficiently large.

The secrecy capacity region, denoted by \mathcal{C} , is defined as the closure of the set of all (R_1, R_2) achievable with unconditional secrecy. We will derive outer and inner regions, $\mathcal{C}^{\text{outer}}$ and $\mathcal{C}^{\text{inner}}$, respectively, such that

$$\mathcal{C}^{\text{inner}} \subseteq \mathcal{C} \subseteq \mathcal{C}^{\text{outer}}.$$

Essentially this means that there exists a coding scheme that achieves any rate pair in $\mathcal{C}^{\text{inner}}$. On the other hand, no coding scheme exists for any rate pair not in $\mathcal{C}^{\text{outer}}$.

3.3 Results on the Secrecy Capacity Region

In this section we first outline the main results, namely the outer and inner regions of the secrecy capacity region. We then discuss and give some insights on these results. The last part in this section looks at an important case of our problem, i.e., the case when only one base station experiences interference; this is modeled by the Z-channel.

3.3.1 General Outer Region

We now state the general outer region. Let $C(x) = \frac{1}{2} \log_2(1 + x)$.

Theorem 1 (Outer Region) *Let $\mathcal{C}^{\text{outer}}(P_1, P_2)$ be the set of (R_1, R_2) such that*

$$R_1 + R_2 \leq \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right) - \max \{ C(SNR_1), C(SNR_2) \} \quad (3.7)$$

where

$$K_{12} = \det \begin{pmatrix} h_1^2 P_1 + h_{21}^2 P_2 + \sigma_1^2 & h_1 h_{12} P_1 + h_2 h_{21} P_2 \\ h_1 h_{12} P_1 + h_2 h_{21} P_2 & h_{12}^2 P_1 + h_2^2 P_2 + \sigma_2^2 \end{pmatrix} \quad (3.8)$$

$$SNR_1 = \frac{h_1^2 P_1 + h_{21}^2 P_2}{\sigma_1^2} \quad (3.9)$$

$$SNR_2 = \frac{h_{12}^2 P_1 + h_2^2 P_2}{\sigma_2^2}. \quad (3.10)$$

Then

$$\mathcal{C}^{outer} = \mathcal{C}^{outer}(P_1^{\max}, P_2^{\max})$$

is an outer region.

3.3.2 Equal SNR Inner Region

We now state an inner region that is based on Gaussian codebooks and the equal SNR property:

$$SNR_1 = SNR_2 \triangleq SNR_{Eq}, \quad (3.11)$$

where SNR_1, SNR_2 is given in Eqs. (3.9) and (3.10). Thus this inner region is not the most generalized region possible. We will further show that our inner region restricts the users' powers to lie on a line segment (purple (vertical) line segment in Fig. 3.2) determined by the channel parameters, i.e.,

$$\alpha = \frac{h_2^2 \sigma_1^2 - h_{21}^2 \sigma_2^2}{h_1^2 \sigma_2^2 - h_{12}^2 \sigma_1^2} \quad (3.12)$$

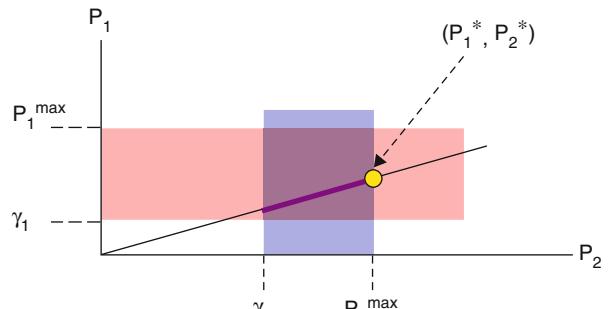


Fig. 3.2 Admissible users' powers

$$\gamma_1 = \begin{cases} \frac{\sigma_2^2 h_{21}^2}{h_1^2 h_2^2} - \frac{\sigma_1^2}{h_1^2} & \text{if } \frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}, \\ \frac{\sigma_1^2 h_2^2}{h_{12}^2 h_{21}^2} - \frac{\sigma_2^2}{h_2^2} & \text{if } \frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2}, \\ \infty & \text{otherwise.} \end{cases} \quad (3.13)$$

$$\gamma_2 = \begin{cases} \frac{\sigma_1^2 h_{12}^2}{h_1^2 h_2^2} - \frac{\sigma_2^2}{h_2^2} & \text{if } \frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}, \\ \frac{\sigma_2^2 h_1^2}{h_{12}^2 h_{21}^2} - \frac{\sigma_1^2}{h_2^2} & \text{if } \frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \text{ and } \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2}, \\ \infty & \text{otherwise.} \end{cases} \quad (3.14)$$

$$\mathcal{A} = \{(P_1, P_2) : \gamma_1 \leq P_1 \leq P_1^{\max}, \gamma_2 \leq P_2 \leq P_2^{\max}, \quad P_1 = \alpha P_2, \alpha > 0\}, \quad (3.15)$$

where \mathcal{A} is the set of admissible users' powers. Let the "largest" power pair in \mathcal{A} be denoted by (P_1^*, P_2^*) . In this case, if $\mathcal{A} \neq \emptyset$ then (P_1^*, P_2^*) is in fact the right-most yellow point on the purple (vertical) line segment shown in Fig. 3.2.

Let $|x|^+ = \max\{x, 0\}$. Let the notation $x \doteq a$ denote $a - \epsilon \leq x \leq a$ for $\epsilon > 0$ arbitrarily small. Recall that we only consider constructing achievable codes for the equal SNR case, i.e., $SNR_1 = SNR_2$, under Gaussian codebooks.

Theorem 2 *Let $\mathcal{C}^{inner}(P_1, P_2)$ be the set of (R_1, R_2) such that*

$$SNR_1 = SNR_2 \triangleq SNR_{Eq} \quad (3.16)$$

$$R_1 = |\bar{R}_1 - U_1|^+ \quad (3.17)$$

$$R_2 = |\bar{R}_2 - U_2|^+ \quad (3.18)$$

where

$$U_1 \leq \min \left\{ C \left(\frac{h_1^2 P_1}{\sigma_1^2} \right), \quad C \left(\frac{h_{12}^2 P_1}{\sigma_2^2} \right) \right\} \quad (3.19)$$

$$U_2 \leq \min \left\{ C \left(\frac{h_2^2 P_2}{\sigma_2^2} \right), \quad C \left(\frac{h_{21}^2 P_2}{\sigma_1^2} \right) \right\} \quad (3.20)$$

$$U_1 + U_2 \doteq C(SNR_{Eq}) \quad (3.21)$$

$$\bar{R}_1 \leq C \left(\frac{h_{12}^2 P_1}{\sigma_2^2} + \frac{h_1^2 P_1}{\sigma_1^2} \right) \quad (3.22)$$

$$\bar{R}_2 \leq C \left(\frac{h_{21}^2 P_2}{\sigma_1^2} + \frac{h_2^2 P_2}{\sigma_2^2} \right) \quad (3.23)$$

$$\bar{R}_1 + \bar{R}_2 \leq \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right). \quad (3.24)$$

Then

$$\mathcal{C}^{inner} = \mathcal{C}^{inner}(P_1^*, P_2^*)$$

is an inner region.

Remark Notice that when $SNR_1 = SNR_2$ and $(P_1^{\max}, P_2^{\max}) \in \mathcal{A}$ the sum rate bounds for both inner and outer regions match. This point will be illustrated in an example in Sect. 3.3.4.

3.3.3 Interpretation for Outer Region

Consider $p(y|x)$ with $y = (y_1, y_2)$, $x = (x_1, x_2)$ as the main (legitimate) “single-user” channel. The wiretap channel can be viewed as $p'(\tilde{y}|y)$, where \tilde{y} is either y_1 or y_2 . In this way, the wiretap channel is degraded, and by the Gaussian wiretap channel theorem [6], the secrecy capacity for this “single-user” channel is given by

$$\begin{aligned} C_S &= I(X; Y) - I(X; \tilde{Y}) \\ &= I(X_1, X_2; Y_1, Y_2) - I(X_1, X_2, Y_i), \quad i = 1 \text{ or } 2 \end{aligned}$$

which is similar to the upper bound in Theorem 1 when X_1, X_2 are independent.

3.3.4 Numerical Example for Inner Region

Next we give a numerical example to demonstrate the ideas behind the construction of the inner region. Let $h_1^2 = 1$, $h_{12}^2 = 1/0.91$, $h_{21}^2 = 0.6$, $h_2^2 = 1$, $\sigma_1^2 = 0.9$, $\sigma_2^2 = 1$, $P_1^{\max} = 13.65$, $P_2^{\max} = 0.5$ for our example. We have chosen the maximum powers such that $(P_1^{\max}, P_2^{\max}) \in \mathcal{A}$ as the reader may verify. Let $\bar{\mathcal{R}}$ be the region corresponding to Eqs. (3.22–3.24) for $P_1 = P_1^{\max}$, $P_2 = P_2^{\max}$. Thus $\bar{\mathcal{R}}$ is the multiple access channel (MAC) capacity region without considering secrecy. Let \mathcal{U} be the line segment corresponding to Eqs. (3.19–3.21). Here \mathcal{U} is *not* a MAC capacity region nor is it the boundary of a MAC capacity region due to the minima on the right hand sides of Eqs. (3.19) and (3.20). In Fig. 3.3a the $\bar{\mathcal{R}}$ region is *bounded by* the blue lines, while the \mathcal{U} region is *given by* the thicker (red) line.¹

¹Technically \mathcal{U} is not a line segment, but rather a set of points around the line segment due to the “ $\stackrel{\circ}{=}$ ” used in Eq. (3.21).

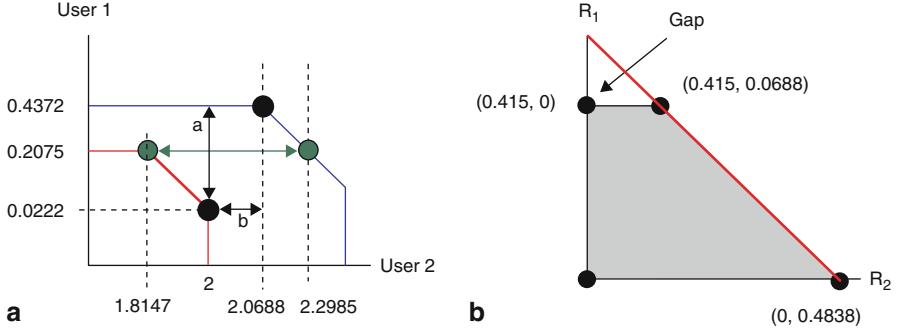


Fig. 3.3 **a** Example illustrating inner region calculations **b** Inner region of example

The maximum rate for User 1 can be acquired by choosing one black circle on the boundary of $\bar{\mathcal{R}}$ (blue line) and one black circle on \mathcal{U} (thick (red) line) such that the vertical distance between these two black circles (marked a in Fig. 3.3a) is as large as possible. The corresponding User 2 rate is then given by the largest horizontal distance marked b while maintaining the distance a . Thus the rate pair calculated in this manner is $(0.415, 0.0688)$, which corresponds to a point on the diagonal in Fig. 3.3b.

The maximum rate for User 2 can be acquired by choosing one green circle on the boundary of $\bar{\mathcal{R}}$ and one green circle on \mathcal{U} such that the horizontal distance between these green circles (as shown in Fig. 3.3a) is as large as possible. The corresponding User 1 rate is then given by the vertical distance between these two green circles, yielding the rate pair $(0, 0.4838)$, which lies on the lower end of the diagonal in Fig. 3.3b.

Given the points derived above, the inner region is then given in Fig. 3.3b as the shaded gray region. The thicker (red) diagonal line in Fig. 3.3b denotes the boundary of the outer region. It can be seen that the inner region partially matches the outer region on the diagonal, and this is because $(P_1^{\max}, P_2^{\max}) \in \mathcal{A}$. There is however a gap at the top. The reader can see that using $P_1 = P_1^{\max}, P_2 = P_2^{\max}$ is not at all obvious, since although using the maximum powers will enlarge $\bar{\mathcal{R}}$, it also affects \mathcal{U} . Thus it is not obvious that using the maximum powers will increase the differences/distances between the black and green circles illustrated in the example above. We note that such a geometric interpretation has also appeared in [7]. Part of the proof of our inner region will rely on this geometric interpretation.

3.3.5 Inner Region for the Z-Channel

Thus far we have seen the inner region for the case when $SNR_1 = SNR_2$. This does not imply that secrecy can only be achieved when $SNR_1 = SNR_2$. In this section we will give an example of an inner region when $SNR_1 \neq SNR_2$. In particular, consider the case when $h_{12} = 0$, i.e., interference is not present at the second base station; this is the Z-channel. Under this scenario, it is obvious that $SNR_1 \neq SNR_2$. It is

also obvious that User 2 cannot achieve any secrecy, since there is no interference from User 1 to protect User 2 at the second base station. This means that whatever User 2 transmits, should be used only to help protect User 1, and should not itself be a secret message. Such interference-assisted secrecy has been studied in [5, 7, 8] under a different wiretap channel model. This implies that from the eavesdropper's point of view, only the first base station contains secret messages from User 1, and thus wiretapping should only occur at the first base station. Let us first derive the inner region for this Z-channel and then discuss its implications.

The inner region for the Z-channel is an application of [9], which is based on [5]. In [9], a terminal wishes to send a secret message to a base station. A wiretapper nearby can also listen to the transmissions of the terminal. A second base station nearby produces artificial noise with the goal of jamming the wiretapper. This artificial noise also affects the first base station, however the first base station has a copy of this artificial noise, and hence can subtract it prior to decoding. The system model can be described by

$$Y_B^n = h_{TB} X_T^n + Z_B \quad (3.25)$$

$$Y_W^n = h_{TW} X_T^n + h_{BW} X_B^n + Z_W \quad (3.26)$$

where Y_B^n is the vector received at the first base station after subtracting the artificial noise, h_{TB} is the channel gain from the sending terminal to the first base station, X_T^n is the codeword sent by the terminal, $Z_B^n \sim \mathcal{N}(0, \sigma_B^2 I_n)$ is noise experienced on the channel from the terminal to the base station, Y_E^n is the vector received by the wiretapper, h_{TW} is the channel gain from the sending terminal to the wiretapper, h_{BW} is the channel gain from the second base station (the jammer) to the wiretapper, X_B^n is the artificial noise sent by the second base station, and $Z_W^n \sim \mathcal{N}(0, \sigma_W^2 I_n)$ accounts for the additive Gaussian noise experienced by the wiretapper. For simplicity, we have subtracted X_B^n from the first base station, which is why it is absent in Eq. (3.25), although in practice the first base station would perform this inside its decoder. This simplified system model is illustrated in Fig. 3.4. Let R_T be the rate of the sending

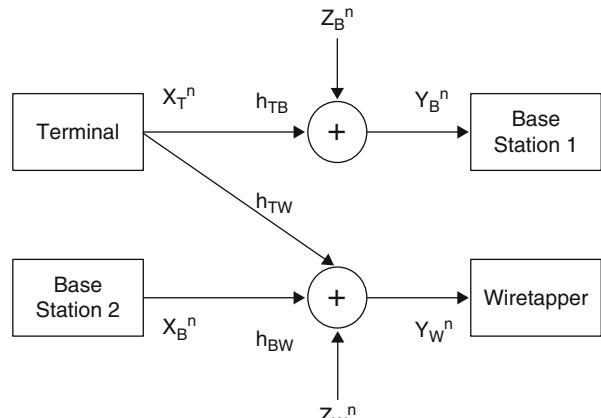


Fig. 3.4 Secure communications via cooperating base stations

terminal, and R_B be the rate of the second base station (the jammer). Let P_T be the power at the sending terminal, and P_B be the power at the second base station. In [9] the following rate R_T as a function of R_B is shown to be achievable with unconditional secrecy:

$$R_T(R_B) = \begin{cases} R_T^{(l)} & \text{if } R_B < C \left(\frac{h_{BW}^2 P_B}{\sigma_W^2 + h_{TW}^2 P_T} \right), \\ R_T^{(m)} & \text{if } C \left(\frac{h_{BW}^2 P_B}{\sigma_W^2 + h_{TW}^2 P_T} \right) < R_B \leq C \left(\frac{h_{BW}^2 P_B}{\sigma_W^2} \right), \\ R_T^{(u)} & \text{if } R_B > C \left(\frac{h_{BW}^2 P_B}{\sigma_W^2} \right). \end{cases} \quad (3.27)$$

where

$$R_T^{(l)} = \left| C \left(\frac{h_{TB}^2 P_T}{\sigma_B^2} \right) - C \left(\frac{h_{TW}^2 P_T}{\sigma_W^2} \right) \right|^+ \quad (3.28)$$

$$R_T^{(m)} = \left| C \left(\frac{h_{TB}^2 P_T}{\sigma_B^2} \right) - C \left(\frac{h_{TW}^2 P_T}{\sigma_W^2} + \frac{h_{BW}^2 P_B}{\sigma_W^2} \right) + R_B \right|^+ \quad (3.29)$$

$$R_T^{(u)} = \left| C \left(\frac{h_{TB}^2 P_T}{\sigma_B^2} \right) - C \left(\frac{h_{TW}^2 P_T}{\sigma_W^2 + h_{BW}^2 P_B} \right) \right|^+. \quad (3.30)$$

Although this does not appear to be related to our problem, since the wiretapper has his own channel, our Z-channel is in fact a special case of this problem. Consider our Z-channel in which $h_{12} = 0$ in Fig. 3.1. In this case User 2 clearly cannot achieve unconditional secrecy. Thus User 2 must play the role of the jammer to protect User 1's message from a wiretapper who intercepts Y_1^n in Fig. 3.1. Note that since the wiretapper can only choose either Y_1^n and Y_2^n , the wiretapper should always choose Y_1^n , which is the only one containing the secret message; Y_2^n only contains noise and User 2's jamming signal. On the other hand since the joint decoder receives both Y_1^n and Y_2^n , the joint decoder can subtract X_2^n from Y_1^n if and only if User 2's rate is less than or equal to its channel capacity $C(h_2^2 P_2 / \sigma_2^2)$. Since User 2 should maximize its rate in order to jam the wiretapper as much as possible, we set $R_2 = C(h_2^2 P_2 / \sigma_2^2)$.

If we let $h_{TB} = h_{TW} = h_1$, $Z_B^n = Z_W^n = Z_1^n$, $h_{BW} = h_{21}$, $Y_W^n = Y_1^n$, and Y_B^n is equal to Y_1^n minus User 2's jamming signal (available to the joint decoder through Y_2^n), then the relationship between our Z-channel and Fig. 3.4 is apparent. Then setting $P_1 = P_T$, $P_2 = P_B$, $R_1 = R_T$, $R_2 = R_B = C(h_2^2 P_2 / \sigma_2^2)$ and then applying

Eq. (3.27) yields the inner region for our Z-channel:

$$R_1^Z = \begin{cases} 0 & \text{if } \frac{h_2^2}{\sigma_2^2} < \frac{h_{21}^2}{\sigma_1^2 + h_1^2 P_1}, \\ \left| C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right) + C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right) - C(SNR_1) \right|^+ & \text{if } \frac{h_{21}^2}{\sigma_1^2 + h_1^2 P_1} < \frac{h_2^2}{\sigma_2^2} \leq \frac{h_{21}^2}{\sigma_1^2}, \\ C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right) - C\left(\frac{h_1^2 P_1}{\sigma_1^2 + h_{21}^2 P_2}\right) & \text{if } \frac{h_2^2}{\sigma_2^2} > \frac{h_{21}^2}{\sigma_1^2}. \end{cases} \quad (3.31)$$

where SNR_1, SNR_2 are given in Eqs. (3.9) and (3.10), respectively.

Interestingly, it can be shown that $R_1^Z \in \mathcal{C}^{inner}(P_1, P_2)$ where $\mathcal{C}^{inner}(P_1, P_2)$ is an equal SNR inner region when $h_{12} \neq 0$ is included and chosen appropriately. The implication of this result is that adding h_{12} does not lower the rate of User 1, but in fact usually increases the rate of User 1. The intuition is that adding the cross-link h_{12} gives the joint decoder more information about User 1's secret message. Of course at the same time the wiretapper may now try to access User 1's secret message through the second base station (in contrast to the Z-channel in which the second base station only receives User 2's jamming signal). However our equal SNR coding technique compensates for this, and usually out performs the Z-channel coding technique of [9] in terms of User 1's rate while still ensuring both channels are unconditionally secure.

3.4 Slow and Flat Rayleigh Fading

In this section we model the random fading as in [10–14]. This model is for narrow-band communications when the users are immobile, and must send their data as quickly as possible without incurring delays [3]. We assume that the encoders have the channel state information, i.e., have the fading realizations.

Consider the complex discrete-time base-band channel model, i.e., we assume that X_1, X_2 are complex-valued, that the additive noise variables are zero-mean circularly symmetric Gaussian, and the presence of a slow and flat fading channel such that $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_{12}, \mathbf{h}_{21}$ (where now bold font signifies that the variables are *random*, not vectors) are independent circularly symmetric Gaussian random variables. Their realizations are constant for an entire codeword block (slow fading) and known by all parties.² Then $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ are exponentially-distributed with means $\beta_1, \beta_2, \beta_{12}$, and β_{21} , respectively. We denote the powers of the noise for the two users by N_1 and N_2 . In the works of [10–12, 14], the outage probability, defined as the probability that a target rate is unachievable, is of interest. In our work, we are

²The capacity will be doubled to account for the real and imaginary parts.

interested in a simpler problem: the probability that it is impossible to achieve any non-zero rate given some power constraint. This is the same as $\Pr\{\mathcal{A} = \emptyset\}$. We will derive this probability, and plot it for varying parameters.

Define the following variables:

$$\begin{aligned} SNR_{11} &\triangleq \frac{\beta_1 P_1^{\max}}{N_1}, & SNR_{22} &\triangleq \frac{\beta_2 P_2^{\max}}{N_2}, \\ SNR_{12} &\triangleq \frac{\beta_{12} P_1^{\max}}{N_2}, & SNR_{21} &\triangleq \frac{\beta_{21} P_2^{\max}}{N_1}, \end{aligned} \quad (3.32)$$

which can be interpreted as the single-user expected signal-to-noise (SNR) ratio, and

$$DCR \triangleq \frac{\beta_1 \beta_2}{\beta_{12} \beta_{21}}, \quad CDR \triangleq \frac{\beta_{12} \beta_{21}}{\beta_1 \beta_2}, \quad (3.33)$$

which we define as the direct-to-cross-expected-fading-ratio (DCR) and the cross-to-direct-expected-fading-ratio (CDR), respectively; essentially these two ratios measure how different the expected fading is on the direct links and on the cross-links. Finally define

$$\xi = \frac{(\beta_{12} N_1 + \beta_1 N_2)(\beta_2 N_1 + \beta_{21} N_2)}{\beta_1 \beta_2 \beta_{12} \beta_{21} N_1 N_2}, \quad (3.34)$$

as a constant independent of P_1^{\max} , P_2^{\max} . Equipped with these definitions, the probability of not achieving a non-zero rate is given by

$$\begin{aligned} \Pr\{\mathcal{A} = \emptyset\} &= 1 - \Pr\{\mathcal{A} \neq \emptyset\} \\ &= 1 - \frac{(\beta_1 \beta_2 + \beta_{12} \beta_{21}) N_1 N_2}{(\beta_{12} N_1 + \beta_1 N_2)(\beta_2 N_1 + \beta_{21} N_2)} \\ &\quad + DCR \cdot SNR_{11}^{-1} \cdot E(\xi \cdot SNR_{11}^{-1}) \\ &\quad + DCR \cdot SNR_{22}^{-1} \cdot E(\xi \cdot SNR_{22}^{-1}) \\ &\quad + CDR \cdot SNR_{12}^{-1} \cdot E(\xi \cdot SNR_{12}^{-1}) \\ &\quad + CDR \cdot SNR_{21}^{-1} \cdot E(\xi \cdot SNR_{21}^{-1}) \\ &\quad - \frac{DCR}{SNR_{11} + SNR_{22}} \cdot E\left(\xi \frac{\beta_1 \beta_2}{SNR_{11} + SNR_{22}}\right) \\ &\quad - \frac{CDR}{SNR_{12} + SNR_{21}} \cdot E\left(\xi \frac{\beta_{12} \beta_{21}}{SNR_{12} + SNR_{21}}\right), \end{aligned} \quad (3.35)$$

where

$$E(x) = \exp(x) E_1(x), \quad E_1(x) = \int_x^\infty \frac{1}{t} \exp(-t) dt \quad (3.36)$$

and $E_1(x)$ is known as the exponential integral, which is common in the secrecy capacity of fading channels [12].

3.4.1 Discussion on Random Fading

We pointed out that some parameters may not satisfy the equal SNR requirement, and thus coding viz. the equal SNR inner region cannot be used. If these parameters are fixed, then there is nothing we can do, i.e., the users cannot send messages in secrecy viz. the equal SNR inner region. However, if the channel gains are random, this opens up the possibility that some realizations are amenable to the equal SNR coding technique. Thus random fading is a friend rather than a foe as we further detail.

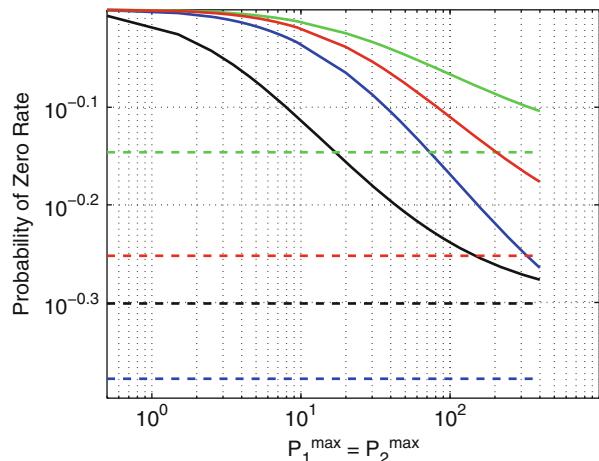
Figure 3.5 plots the derived $Pr\{\mathcal{A} = \emptyset\}$ for different channel parameters. There are three regions of interest that we will study: (1) $P_1^{\max}, P_2^{\max} \rightarrow 0$; (2) $P_1^{\max}, P_2^{\max} \rightarrow \infty$; (3) powers in between (1) and (2). The first two regions of interest are obvious and can be deduced simply from Eq. (3.57): when $P_1^{\max} = P_2^{\max} = 0$, the events never occur, and thus $Pr\{\mathcal{A} = \emptyset\} = 1 - Pr\{\mathcal{A} \neq \emptyset\} = 1$ as verified in Fig. 3.5; on the other hand when $P_1^{\max}, P_2^{\max} \rightarrow \infty$, it is easy to see that the only random event left would be $\{\alpha > 0\}$, which is independent of P_1^{\max}, P_2^{\max} , and thus

$$Pr\{\mathcal{A} = \emptyset\} \rightarrow 1 - \frac{(\beta_1\beta_2 + \beta_{12}\beta_{21})N_1N_2}{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}. \quad (3.37)$$

With sufficiently large maximum allowable power, the probability of not achieving a non-zero rate is bounded by Eq. (3.37), which is depicted by the dotted lines in Fig. 3.5.

The third case is the most interesting case, which is also of practical value. From Fig. 3.5 we see that when P_1^{\max}, P_2^{\max} is finite, the solid black curve performs better than the solid blue curve. However, in the infinite power regime, the reverse is true: the dotted blue line performs better than the dotted black curve. In fact from Fig. 3.5, one can see the solid blue and black curves may intercept and cross over at some point. Equation (3.35) is used informally for our interpretation of this third case.

Fig. 3.5 Solid lines: Probability that users cannot achieve a non-zero rate given maximal power constraints; Dotted lines: When $P_1^{\max}, P_2^{\max} \rightarrow \infty$
Black: $\beta_1 = \beta_2 = \beta_{12} = \beta_{21} = N_1 = N_2 = 1$,
Blue: $\beta_1 = 1, \beta_2 = 0.5, \beta_{12} = 0.9, \beta_{21} = 0.1, N_1 = 1, N_2 = 2$, **Green:** $\beta_1 = 1, \beta_2 = 0.5, \beta_{12} = 0.2, \beta_{21} = 0.8, N_1 = 1, N_2 = 2$, **Red:** $\beta_1 = 1, \beta_2 = 0.3, \beta_{12} = 0.7, \beta_{21} = 0.1, N_1 = 2, N_2 = 1$



First, it is desirable to decrease the positive terms in Eq. (3.35). The positive terms may be decreased by increasing SNR_{ij} , since $\frac{1}{x}E(x)$ is a decreasing function. For example, in the term

$$DCR \cdot SNR_{11}^{-1} \cdot E(\xi \cdot SNR_{11}^{-1})$$

if SNR_{11} is increased, this term decreases. If the maximum powers P_1^{\max} , and P_2^{\max} are held constant, SNR_{11} may be increased by increasing β_1 . The entire term may be further decreased if the denominator of DCR, $\beta_{12}\beta_{21}$, is increased. Thus we see that both β_1 (direct link) and $\beta_{12}\beta_{21}$ (cross-links) are increased together to decrease the above term. Similarly this argument can be applied to the other three positive terms in Eq. (3.35). This informally suggests that the expected fadings should approximately be equal to one another. Indeed, the black curve in Fig. 3.5 has the best performance in the finite power regime and it corresponds to the case when all parameters are equal.

3.5 Derivations of Secrecy Capacity Region Results

In this section we break down the results in Sect. 3.3, namely prove the outer region, followed by the inner region, which is more involved.

3.5.1 Proof of Theorem 1: Outer Region

The proof of the outer region consists of two parts. The first part is to prove an outer region for X_1^n, X_2^n . The second part is to show that choosing X_1^n, X_2^n as Gaussian vectors maximizes this outer region under a fixed power constraint. The first part uses standard information theory identities, while the second part is based on [15].

Therefore first we shall bound the sum rate as follows. Let entropy be the differential entropy.

$$\begin{aligned} n(R_1 + R_2) &= H(W_1, W_2) = H(W_1, W_2|Y_1^n, Y_2^n) + I(W_1, W_2; Y_1^n, Y_2^n) \\ &\stackrel{(a)}{\leq} n\epsilon_n + I(W_1, W_2; Y_1^n, Y_2^n) \\ &\stackrel{(b)}{=} I(W_1, W_2; Y_2^n) + I(W_1, W_2; Y_1^n|Y_2^n) + n\epsilon_n \\ &\stackrel{(c)}{\leq} n\epsilon + I(W_1, W_2; Y_1^n|Y_2^n) + n\epsilon_n \\ &\stackrel{(d)}{\leq} H(Y_1^n|Y_2^n) - H(Y_1^n|Y_2^n, W_1, W_2, X_1^n, X_2^n) + 2n\epsilon_n \\ &\stackrel{(e)}{\leq} H(Y_1^n|Y_2^n) - H(Y_1^n|Y_2^n, X_1^n, X_2^n) + 2n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_1^n|Y_2^n) + 2n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_1^n, Y_2^n) - I(X_1^n, X_2^n; Y_2^n) \end{aligned} \quad (3.38)$$

The explanations are: (a) Fano's inequality; (c) the unconditional secrecy requirement of Eq. (3.6); (d) conditioning reduces entropy; (e) the data processing inequality

on the Markov chain $(W_1, W_2) \leftrightarrow (X_1^n, X_2^n) \leftrightarrow (Y_1^n, Y_2^n)$. On the other hand, using the chain rule in (b) another way, gives another bound

$$n(R_1 + R_2) \leq I(W_1, W_2; Y_1^n) + I(W_1, W_2; Y_2^n | Y_1^n) + n\epsilon_n$$

and using Eq. (3.6), and then (c)–(e) again gives the other bound

$$\begin{aligned} n(R_1 + R_2) &\leq I(X_1^n, X_2^n; Y_2^n | Y_1^n) + 2n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_1^n, Y_2^n) - I(X_1^n, X_2^n; Y_1^n) \end{aligned} \quad (3.39)$$

To satisfy both bounds, we take the minimum of the two.

Next we bound the individual rates.

$$\begin{aligned} nR_1 &= H(W_1) = H(W_1 | Y_1^n Y_2^n) + I(W_1; Y_1^n, Y_2^n) \\ &\stackrel{(a)}{\leq} n\epsilon_n + I(W_1; Y_1^n, Y_2^n) \\ &\stackrel{(b)}{=} I(W_1; Y_2^n) + I(W_1; Y_1^n | Y_2^n) + n\epsilon_n \\ &\stackrel{(c)}{\leq} n\epsilon + I(W_1; Y_1^n | Y_2^n) + n\epsilon_n \\ &\stackrel{(d)}{\leq} H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, W_1, X_1^n, X_2^n) + 2n\epsilon_n \\ &\stackrel{(e)}{=} H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, X_1^n, X_2^n) + 2n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_1^n | Y_2^n) + 2n\epsilon_n \end{aligned} \quad (3.40)$$

The explanations are the same as before. The chain rule of (b) can also be written in another way. Thus the individual bounds are the same as the sum rate bound.

Finally we prove that X_1^n, X_2^n maximizes Eq. (3.38) when they are chosen as vectors of i.i.d. Gaussian RVs. The proof follows easily from the clever device used in [15], and we include it here for completeness.

$$\begin{aligned} I(X_1^n, X_2^n; Y_1^n | Y_2^n) &= H(Y_1^n | Y_2^n) - H(Y_1^n | Y_2^n, X_1^n, X_2^n) \\ &= H(Y_1^n | Y_2^n) - H(Z_1^n | Z_2^n) \end{aligned} \quad (3.41)$$

Thus maximizing $I(X_1^n, X_2^n; Y_1^n | Y_2^n)$ over X_1^n, X_2^n is equivalent to maximizing $H(Y_1^n | Y_2^n)$ over X_1^n, X_2^n , since Z_1^n, Z_2^n are independent of X_1^n, X_2^n . Let \mathbf{L} be a matrix such that $\mathbf{L}Y_2^n$ yields a vector in which each component in this vector is the best linear minimum mean square error (LMMSE) estimate of the corresponding component in vector Y_1^n . Formally, let

$$\mathbf{L} \triangleq \begin{pmatrix} L_1 \\ \vdots \\ L_n \end{pmatrix} \quad (3.42)$$

where L_i s are row vectors, and $L_i Y_2^n$ is the best LMMSE of $Y_{1,i}$. Then let the matrix \mathbf{M} be the diagonal matrix in which the diagonal entries are the corresponding mean square estimation errors. The following are information theoretic bounds.

$$\begin{aligned} H(Y_1^n | Y_2^n) &\stackrel{(a)}{=} H(Y_1^n - \mathbf{L}Y_2^n | Y_2^n) \\ &\stackrel{(b)}{\leq} H(Y_1^n - \mathbf{L}Y_2^n) \\ &\stackrel{(c)}{\leq} \frac{1}{2} \log(2\pi e)^n \det(\mathbf{M}). \end{aligned} \quad (3.43)$$

The explanations follow: (a) follows since conditioning on Y_2^n makes $\mathbf{L}Y_2^n$ a constant; (b) conditioning reduces entropy; (c) the maximum entropy of random vector $Y_1^n - \mathbf{L}Y_2^n$ given a covariance matrix $\det(\mathbf{M})$ is given by the expression of (c) [16]. To show that X_1^n, X_2^n achieves the maximum of Eq. (3.43), we show that the inequalities (b) and (c) are tight when X_1^n, X_2^n are the said Gaussian vectors.

From the orthogonality principle for the best LMMSE [17], $\mathbb{E}\{[(Y_1^n - \mathbf{L}Y_2^n)]_i Y_{2,j}\} = 0$ for each component i, j of the vectors. If X_1^n, X_2^n are Gaussian then the individual errors $[(Y_1^n - \mathbf{L}Y_2^n)]_i$ are also independent of $Y_{2,i}$, thus proving $Y_1^n - \mathbf{L}Y_2^n$ is independent of Y_2 . Finally (c) is also tight since $Y_1^n - \mathbf{L}Y_2^n$ is a Gaussian random vector when X_1^n, X_2^n are Gaussian, which maximizes entropy for a covariance constraint.

3.5.2 Proof of Theorem 2: Inner Region

The proof of Theorem 2 consists of three parts. The first part is an unsimplified inner region, which involves the infinite union of sub-regions. The second part is to prove that increasing power implies increasing inner sub-regions such that for $P_1 \leq Q_1$, $P_2 \leq Q_2$, $(P_1, P_2) \in \mathcal{A}$, $(Q_1, Q_2) \in \mathcal{A}$ implies $C^{\text{inner}}(P_1, P_2) \subseteq C^{\text{inner}}(Q_1, Q_2)$. This means that if we utilize the maximum admissible power, the resulting inner region is the largest inner region that is also a superset of all other inner sub-regions. Finally the last part is to show Eq. (3.15) is the admissible power set. Therefore Theorem 2 follows by using the largest powers in Eq. (3.15), which corresponds to the right-most point on the line segment.

3.5.2.1 Part 1: Proof of Inner Sub-Regions

In this first part of the proof, we will show that $C^{\text{inner}}(P_1, P_2)$ (as defined in Theorem 2) is achievable when $(P_1, P_2) \in \mathcal{A}$. This implies that the inner region can be written in unsimplified form as the closure of the convex hull of

$$\bigcup_{(P_1, P_2) \in \mathcal{A}} C^{\text{inner}}(P_1, P_2).$$

The achievability proof here is similar to that of the multiple access wiretap channels [18–21].

Codebook Generation

Randomly generate two tables. The first table will have $2^{n(\bar{R}_1-\epsilon)}$ vectors (codewords) whose components are randomly drawn from the normal distribution $\mathcal{N}(0, P_1^{\max} - \epsilon)$. Similarly, the second table will have $2^{n(\bar{R}_2-\epsilon)}$ vectors whose components are randomly drawn from the normal distribution $\mathcal{N}(0, P_2^{\max} - \epsilon)$. The first table has 2^{nR_1} rows and $2^{n(U_1-\epsilon')}$ columns, while the second table has 2^{nR_2} and $2^{n(U_2-\epsilon')}$ columns. The rates $\bar{R}_1, \bar{R}_2, U_1, U_2$ are chosen to satisfy Eqs. (3.19–3.24).

Encoding

If User 1 wishes to send index $i \in \{1, \dots, 2^{nR_1}\}$, randomly (uniformly) select a codeword from row i of the first table; call this X_1^n . If User 2 wishes to send index $j \in \{1, \dots, 2^{nR_2}\}$, randomly (uniformly) select a codeword from row j of the second table; call this X_2^n .

Decoding

Notice that the overall channel as seen by the joint decoder is a MAC with independent inputs X_1^n and X_2^n , and output (Y_1^n, Y_2^n) . It is known that the average probability of error tends to 0 as $n \rightarrow \infty$ if

$$\begin{aligned}\bar{R}_1 &< I(X_1; Y_1, Y_2 | X_2) \\ \bar{R}_2 &< I(X_2; Y_1, Y_2 | X_1) \\ \bar{R}_1 + \bar{R}_2 &< I(X_1, X_2; Y_1, Y_2)\end{aligned}$$

for some codebook generated randomly as above, which is precisely Eqs. (3.22–3.24) for the Gaussian MAC. Thus by the Gaussian MAC theorem, X_1^n and X_2^n are decodable by the joint decoder given (Y_1^n, Y_2^n) . In addition (X_1^n, X_2^n) are unique in the two tables resp. and thus the joint decoder can uniquely identify the rows (\hat{i}, \hat{j}) .

Secrecy Analysis

To show the above construction achieves unconditional secrecy, we write

$$\begin{aligned}H(W_1, W_2 | Y_i^n) &= H(W_1, W_2) - I(W_1, W_2; Y_i^n) \\ &= H(W_1, W_2) - H(Y_i^n) + H(Y_i^n | W_1, W_2) \\ &\stackrel{(a)}{=} H(W_1, W_2) - H(Y_i^n) + H(Y_i^n | X_1^n, X_2^n) \\ &\quad + H(Y_i^n | W_1, W_2) - H(Y_i^n | X_1^n, X_2^n, W_1, W_2) \\ &= H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) \\ &\quad + I(Y_i^n; X_1^n, X_2^n | W_1, W_2)\end{aligned}$$

$$\begin{aligned}
&= H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) \\
&\quad + H(X_1^n, X_2^n | W_1, W_2) - H(X_1^n, X_2^n | Y_i^n, W_1, W_2) \\
&\stackrel{(b)}{=} H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) + H(X_1^n | W_1) \\
&\quad + H(X_2^n | W_2) - H(X_1^n, X_2^n | Y_i^n, W_1, W_2) \\
&\stackrel{(c)}{=} H(W_1, W_2) - I(Y_i^n; X_1^n, X_2^n) + n(U_1 - \epsilon') \\
&\quad + n(U_2 - \epsilon') - H(X_1^n, X_2^n | Y_i^n, W_1, W_2) \\
&\stackrel{(d)}{=} H(W_1, W_2) - 2n\epsilon'' - H(X_1^n, X_2^n | Y_i^n, W_1, W_2). \tag{3.44}
\end{aligned}$$

The explanations are: (a) $(W_1, W_2) \leftrightarrow (X_1^n, X_2^n) \leftrightarrow Y_i^n$ forms a Markov chain; (b) from the factorization of the encoding distribution (cf. Definition 1); (c) from the codebook generation and encoding; (d) from Eq. (3.21). Finally note that the wiretapper also sees a MAC, either $(X_1^n, X_2^n) \rightarrow Y_1^n$ if he intercepts Y_1^n or $(X_1^n, X_2^n) \rightarrow Y_2^n$ if he intercepts Y_2^n . When the wiretapper is given the rows W_1, W_2 of the two tables, the wiretapper is looking at a MAC code with $2^{n(U_1 - \epsilon')}, 2^{n(U_2 - \epsilon')}$ codewords, which satisfy the MAC theorem (cf. Eqs. (3.19–3.21)), and thus he is able to decode X_1^n, X_2^n by the MAC theorem whether he wishes to or not! Thus the last term in Eq. (3.44) is bounded by Fano's inequality resulting in

$$H(W_1, W_2 | Y_i^n) \geq H(W_1, W_2) - n\epsilon. \tag{3.45}$$

To complete the secrecy proof for each individual message, we write

$$\begin{aligned}
H(W_1) + H(W_2 | Y_i^n) &\geq H(W_1 | Y_i^n) + H(W_2 | W_1, Y_i^n) \\
&= H(W_1, W_2 | Y_i^n) \\
&\geq H(W_1, W_2) - n\epsilon \\
&= H(W_1) + H(W_2) - n\epsilon \tag{3.46}
\end{aligned}$$

where the last equality follows since W_1, W_2 are independent. This proves

$$H(W_2 | Y_i^n) \geq H(W_2) - n\epsilon \tag{3.47}$$

and the secrecy for the other message can be proved in the same way.

Notice that in Eq. (3.44)d, we used the equal SNR assumption of Eqs. (3.16) and (3.21) to ensure unconditional secrecy is achieved whether the wiretapper intercepts Y_1^n or Y_2^n .

3.5.2.2 Part 2: Increasing Inner Sub-Regions

To prove that for $P_1 \leq Q_1, P_2 \leq Q_2, (P_1, P_2) \in \mathcal{A}, (Q_1, Q_2) \in \mathcal{A}$ implies $C^{\text{inner}}(P_1, P_2) \subseteq C^{\text{inner}}(Q_1, Q_2)$, we will show that each boundary segment of an inner sub-region (see Fig. 3.6a) increases when power is increased. Point C in

Fig. 3.6a corresponds to the distances between the black circles in the example in Sect. 3.3.4, while Point D corresponds to the distances between the green circles in the example in Sect. 3.3.4.

First we show that the diagonal (i.e., line segment between Points C and D) must necessarily expand when power is increased. The diagonal is simply the sum rate bound, which is given by Eq. (3.24) minus Eq. (3.21). This can be rewritten as

$$f(\mathbf{Q}) = \frac{1}{2} \log_2 \left(\frac{\det((\mathbf{Z} + \mathbf{HQH}^T))}{\det(\mathbf{Z})} \right) - \frac{1}{2} \log_2 \left(1 + \frac{\mathbf{H}_i \mathbf{Q} \mathbf{H}_i^T}{\sigma_i^2} \right)$$

where

$$\mathbf{H} = \begin{pmatrix} h_1 & h_{21} \\ h_{12} & h_2 \end{pmatrix}, \quad \mathbf{Q} = \begin{pmatrix} P_1 & 0 \\ 0 & P_2 \end{pmatrix}, \quad \mathbf{Z} = \begin{pmatrix} \sigma_1^2 & 0 \\ 0 & \sigma_2^2 \end{pmatrix} \quad (3.48)$$

and \mathbf{H}_i is row i of matrix \mathbf{H} . $f(\mathbf{Q})$ is increasing in P_1, P_2 as it has the form of the secrecy capacity of a degraded wiretap channel. Thus from this expression we know that the diagonal will increase when the powers are increased.

We now have to show the horizontal and vertical segments of Fig. 3.6a (if they exist), also increase with power. This is equivalent to showing that the maximum user rates increase with increasing power. Figure 3.6b illustrates a scenario in which we are trying to disprove, i.e., prove is impossible. Notice that the diagonal line increases as we proved above, but the horizontal and vertical parts decrease in this impossible scenario we set out to prove. Let us denote User i 's maximum rate by R_i^* . To show R_i^* increases with power, we must find the form(s) of R_i^* . It turns out that R_i^* can take on two forms, i.e., either

$$\text{Form A} = \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right) - C(SNR_{Eq}) \quad (3.49)$$

$$\text{Form B} = C_{R_i}^{\max} + C_{U_j}^{\max} - C(SNR_{Eq}), \quad i, j \in \{1, 2\}, i \neq j \quad (3.50)$$

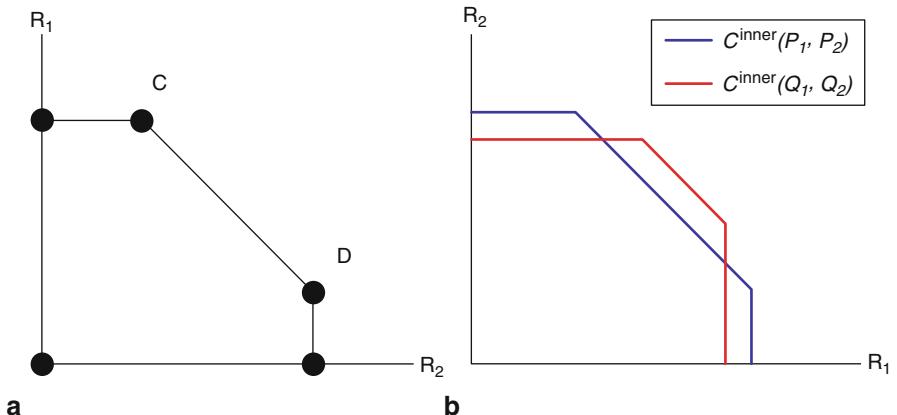


Fig. 3.6 **a** General inner sub-region **b** Impossible scenario when $(P_1, P_2) \leq (Q_1, Q_2)$

where $C_{\bar{R}_i}^{\max}$ is either the LHS of Eqs. (3.22) or (3.23) depending on i , and $C_{U_j}^{\max}$ is either the LHS of Eqs. (3.19) or (3.20) depending on j . Equations (3.49) and (3.50) can be observed by an exhaustive enumeration of all interactions between $\bar{\mathcal{R}}$ and \mathcal{U} as shown in Fig. 3.7. Without loss of generality we have only plotted the interactions between these two regions only for the vertical axes. Thus the maximum vertical distance between a blue line and the thick (red) line yields the maximum rate (either R_1^* or R_2^*). The reader can verify that this maximum vertical distance only takes on two forms, A and B as given by Eqs. (3.49) and (3.50). It is perhaps easiest to see this by first perusing the example in Sect. 3.3.4.

Equation (3.49) is nothing more than $f(\mathbf{Q})$, which we have already shown increases with power. Equation (3.50) can also be written as

$$\begin{aligned} \text{Form } B &= \frac{1}{2} \log_2 \left(1 + \frac{h_1^2 P_1 + h_{21}^2 P_2}{\sigma_1^2} + \frac{P_1 P_2 h_1^2 h_{21}^2}{\sigma_1^2} + \frac{P_2 h_2^2}{\sigma_2^2} + \frac{P_1 P_2 h_1^2 h_2^2}{\sigma_1^2 \sigma_2^2} \right) \\ &\quad - \frac{1}{2} \log_2 \left(1 + \frac{h_2^2 P_1 + h_{21}^2 P_2}{\sigma_1^2} \right) \\ &= \frac{1}{2} \log_2 \left(1 + \underbrace{\frac{P_2(h_2^2 \sigma_1^2 + h_1^2 P_1(h_2^2 + h_{21}^2 \sigma_2^2))}{\sigma_2^2(h_1^2 P_1 + h_{21}^2 P_2 + \sigma_1^2)}}_{\triangleq g(P_1, P_2)} \right). \end{aligned} \quad (3.51)$$

Now it is straightforward to show $g(P_1, P_2)$ is increasing in (P_1, P_2) by verifying that $\frac{\partial g(P_1, P_2)}{\partial P_1} > 0$ and $\frac{\partial g(P_1, P_2)}{\partial P_2} > 0$, and so Eq. (3.50) also increases with power.

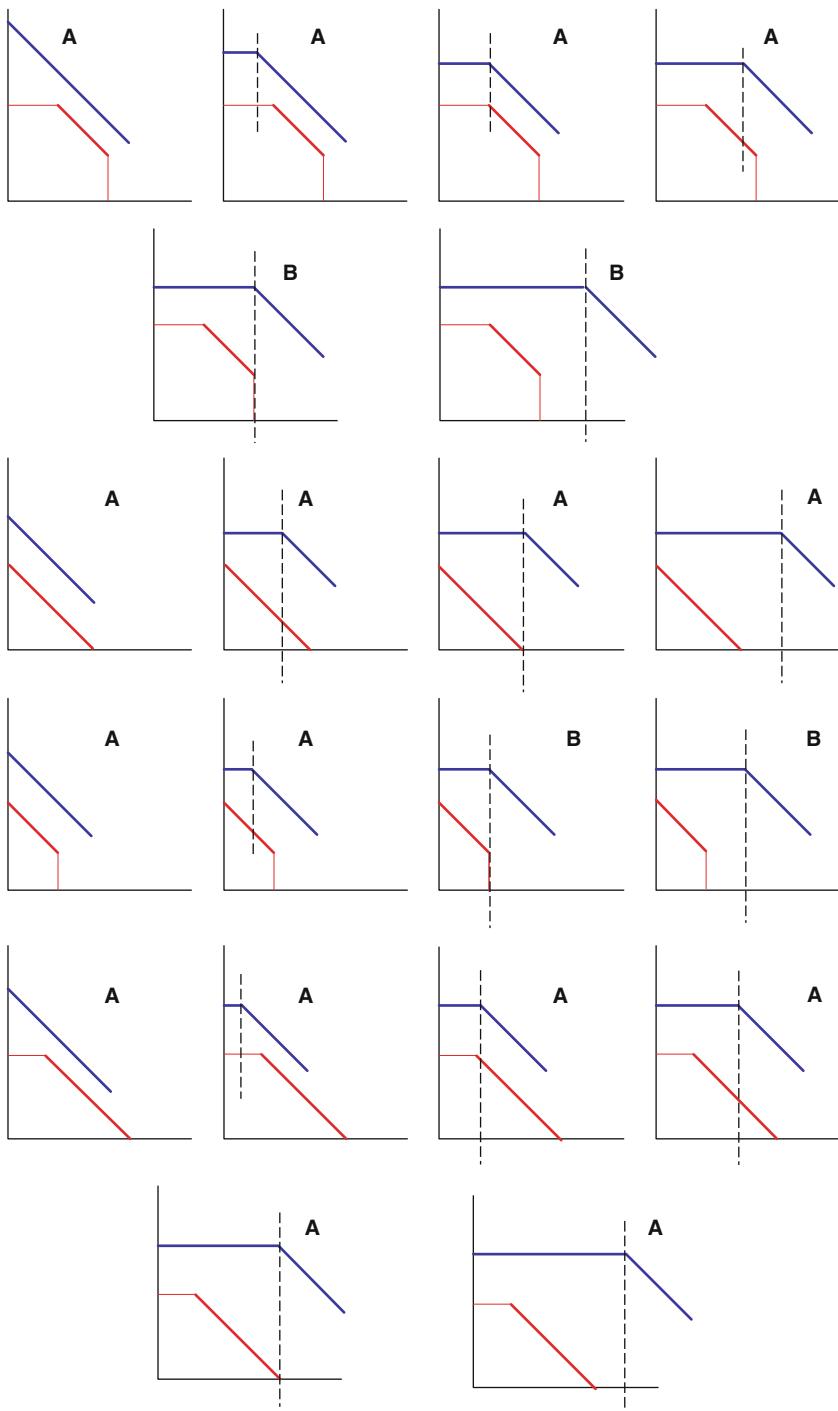
From this we have a partial conclusion. If $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate of Form A , and if $(Q_1, Q_2) \in \mathcal{A}$ (where $(Q_1, Q_2) \geq (P_1, P_2)$) also yields a maximum rate of Form A , then the maximum rate increases. Similarly if $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate of Form B , and if $(Q_1, Q_2) \in \mathcal{A}$ also yields a maximum rate of Form B , then the maximum rate increases.

For a complete conclusion we must also consider the scenario in which $(P_1, P_2) \in \mathcal{A}$ yields a maximum rate of Form A , but $(Q_1, Q_2) \in \mathcal{A}$ yields a maximum rate of Form B , and vice versa, i.e., the forms change. Notice (observed from Fig. 3.7) that Form B occurs when

$$C_{\bar{R}_i}^{\max} + C_{U_j}^{\max} \leq \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right), \quad i, j \in \{1, 2\}, i \neq j.$$

Thus when Form B occurs, Form A is larger than Form B . Therefore if we start with Form B , and applying (Q_1, Q_2) changes the maximum rate to Form A , then the maximum rate will have increased. Alternatively, consider starting with Form A , in which case we have

$$C_{\bar{R}_i}^{\max} + C_{U_j}^{\max} > \frac{1}{2} \log_2 \left(\frac{K_{12}}{\sigma_1^2 \sigma_2^2} \right), \quad i, j \in \{1, 2\}, i \neq j.$$

**Fig. 3.7** \bar{R}, \mathcal{U} region interactions for vertical axes

Thus when Form *A* occurs, Form *B* is larger than Form *A*. Therefore if we start from Form *A*, and applying (Q_1, Q_2) changes the maximum rate to Form *B*, then the maximum rate will have increased. This proves that increasing power always results in an inner region that is a superset.

As a concluding remark, we point out that Form *B* corresponds to the inner region having a horizontal or vertical part, while Form *A* corresponds to not having a horizontal or vertical part.

3.5.2.3 Part 3: Power Allocation

First we prove that the power assignments must be from \mathcal{A} (Eq. (3.15)) under the equal SNR assumption. The fact that (P_1, P_2) must lie on the line $P_1 = \alpha P_2$ (where α is from Eq. (3.12)) easily follows from solving the equation $SNR_1 = SNR_2$ as the reader may verify. The lower bounds γ_1, γ_2 (Eqs. (3.13) and (3.14)) are not as straightforward to see. First note that α must be positive, otherwise P_1 would be negative, which is impossible. α is positive under the following conditions:

$$\frac{h_{21}^2}{h_2^2} < \frac{\sigma_1^2}{\sigma_2^2} \quad \text{and} \quad \frac{h_{12}^2}{h_1^2} < \frac{\sigma_2^2}{\sigma_1^2} \quad \text{or} \quad (3.52)$$

$$\frac{h_{21}^2}{h_2^2} > \frac{\sigma_1^2}{\sigma_2^2} \quad \text{and} \quad \frac{h_{12}^2}{h_1^2} > \frac{\sigma_2^2}{\sigma_1^2}. \quad (3.53)$$

Next note that the \mathcal{U} region is not a multiple access channel (MAC) region even if the almost-equality in Eq. (3.21) is changed to an equality \leq . This is because U_1, U_2 in Eqs. (3.19) and (3.20) are bounded by the minima of capacities of different channels. Thus we must manually enforce the following, (which is always guaranteed for a MAC):

$$C_{U_1}^{\max} + C_{U_2}^{\max} \geq C(SNR_{Eq}), \quad (3.54)$$

where $C_{U_1}^{\max}$ and $C_{U_2}^{\max}$ are the left hand sides of Eqs. (3.19) and (3.20), respectively. This is required since if Eq. (3.54) is *not* satisfied, then the almost-equality in Eq. (3.21) cannot be satisfied either, and so Theorem 2 will yield an empty inner region. From Eqs. (3.52) and (3.53), we can make Eq. (3.54) explicit.

When Eq. (3.53) is true, the reader can verify that

$$C_{U_1}^{\max} = C\left(\frac{h_1^2 P_1}{\sigma_1^2}\right), \quad C_{U_2}^{\max} = C\left(\frac{h_2^2 P_2}{\sigma_2^2}\right), \quad (3.55)$$

which implies

$$P_1 \geq \frac{\sigma_2^2 h_{21}^2}{h_1^2 h_2^2} - \frac{\sigma_1^2}{h_1^2}, \quad P_2 \geq \frac{\sigma_1^2 h_{12}^2}{h_1^2 h_2^2} - \frac{\sigma_2^2}{h_2^2}, \quad (3.56)$$

matching the corresponding cases in γ_1 and γ_2 (Eqs. (3.13) and (3.14)), respectively. When Eq. (3.52) is true, the same technique may be applied. Thus this establishes the admissible power set \mathcal{A} .

3.6 Derivation of Random Fading Result

It is easier to derive the complement probability $\Pr\{\mathcal{A} \neq \emptyset\}$, and we do so towards this end. There are three main events that must occur: $\{\alpha > 0\}$, and $\{P_1^{\max} > \gamma_1\}, \{P_2^{\max} > \gamma_2\}$, of which $\alpha, \gamma_1, \gamma_2$ are functions of the random variables $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ described above. We simplify the derivation by separating the $\{\alpha > 0\}$ event into two disjoint events given by Eqs. (3.52) and (3.53), respectively. Since these two events are disjoint, the complement probability is the sum of two probabilities.

$$\begin{aligned} \Pr\{\mathcal{A} \neq \emptyset\} &= \Pr\left\{\frac{|\mathbf{h}_{21}|^2}{|\mathbf{h}_2|^2} > \frac{N_1}{N_2} \text{ and } \frac{|\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2} > \frac{N_2}{N_1}\right. \\ &\quad \text{and } P_1^{\max} \geq \frac{N_2 |\mathbf{h}_{21}|^2}{|\mathbf{h}_1|^2 |\mathbf{h}_2|^2} - \frac{N_1}{|\mathbf{h}_1|^2} \text{ and } P_2^{\max} \geq \frac{N_1 |\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2 |\mathbf{h}_2|^2} - \frac{N_2}{|\mathbf{h}_2|^2}\Big\} \\ &\quad + \Pr\left\{\frac{|\mathbf{h}_{21}|^2}{|\mathbf{h}_2|^2} < \frac{N_1}{N_2} \text{ and } \frac{|\mathbf{h}_{12}|^2}{|\mathbf{h}_1|^2} < \frac{N_2}{N_1}\right. \\ &\quad \text{and } P_1^{\max} \geq \frac{N_1 |\mathbf{h}_2|^2}{|\mathbf{h}_{12}|^2 |\mathbf{h}_{21}|^2} - \frac{N_2}{|\mathbf{h}_{12}|^2} \text{ and } P_2^{\max} \geq \frac{N_2 |\mathbf{h}_1|^2}{|\mathbf{h}_{12}|^2 |\mathbf{h}_{21}|^2} - \frac{N_1}{|\mathbf{h}_{21}|^2}\Big\} \end{aligned} \tag{3.57}$$

The above expression is still far too complex to obtain a closed form expression, thus we apply a few standard devices. The reader may verify that the above expression may be simplified to the following by combining conditions, using the total probability theorem, and noting that $|\mathbf{h}_1|^2, |\mathbf{h}_2|^2, |\mathbf{h}_{12}|^2, |\mathbf{h}_{21}|^2$ are independent:

$$\begin{aligned} \Pr\{\mathcal{A} \neq \emptyset\} &= \int_0^\infty \int_0^\infty \Pr\left\{|\mathbf{h}_2|^2 \frac{N_1}{N_2} < |\mathbf{h}_{21}|^2 \leq \frac{|\mathbf{h}_2|^2}{N_2} (P_1^{\max} |\mathbf{h}_1|^2 + N_1) \mid |\mathbf{h}_1|^2 = s, |\mathbf{h}_2|^2 = t\right\} \\ &\quad \Pr\left\{|\mathbf{h}_1|^2 \frac{N_2}{N_1} < |\mathbf{h}_{12}|^2 \leq \frac{|\mathbf{h}_1|^2}{N_1} (P_2^{\max} |\mathbf{h}_2|^2 + N_2) \mid |\mathbf{h}_1|^2 = s, |\mathbf{h}_2|^2 = t\right\} \\ &\quad \Pr\{|\mathbf{h}_1|^2 = s\} \Pr\{|\mathbf{h}_2|^2 = t\} ds dt \\ &\quad + \int_0^\infty \int_0^\infty \Pr\left\{|\mathbf{h}_{21}|^2 \frac{N_2}{N_1} < |\mathbf{h}_2|^2 \leq \frac{|\mathbf{h}_{21}|^2}{N_1} (|\mathbf{h}_{12}|^2 P_1^{\max} + N_2) \mid \right. \\ &\quad \quad \quad \left. |\mathbf{h}_{12}|^2 = u, |\mathbf{h}_{21}|^2 = v\right\} \\ &\quad \Pr\left\{|\mathbf{h}_{12}|^2 \frac{N_1}{N_2} < |\mathbf{h}_1|^2 \leq \frac{|\mathbf{h}_{12}|^2}{N_2} (|\mathbf{h}_{21}|^2 P_2^{\max} + N_1) \mid |\mathbf{h}_{12}|^2 = u, |\mathbf{h}_{21}|^2 = v\right\} \\ &\quad \Pr\{|\mathbf{h}_{12}|^2 = u\} \Pr\{|\mathbf{h}_{21}|^2 = v\} du dv. \end{aligned} \tag{3.58}$$

The simplified expression above allows us to use the cumulative distribution function (cdf) of the exponential distribution inside the integrals. Taking the integral then

yields

$$\begin{aligned}
& \Pr\{\mathcal{A} \neq \emptyset\} \\
&= \frac{(\beta_1\beta_2 + \beta_{12}\beta_{21})N_1N_2}{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)} \\
&\quad + \frac{\beta_1\beta_2N_1N_2}{\beta_{12}\beta_{21}(\beta_1N_2P_1^{\max} + \beta_2N_1P_2^{\max})} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_{12}\beta_{21}(\beta_1N_2P_1^{\max} + \beta_2N_1P_2^{\max})}\right) \\
&\quad + \frac{\beta_{12}\beta_{21}N_1N_2}{\beta_1\beta_2(\beta_{12}N_1P_1^{\max} + \beta_{21}N_2P_2^{\max})} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2(\beta_{12}N_1P_1^{\max} + \beta_{21}N_2P_2^{\max})}\right) \\
&\quad - \frac{\beta_{21}N_2}{\beta_1\beta_2P_1^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2\beta_{12}N_1P_1^{\max}}\right) \\
&\quad - \frac{\beta_1N_2}{\beta_{12}\beta_{21}P_2^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_2\beta_{12}\beta_{21}N_1P_2^{\max}}\right) \\
&\quad - \frac{\beta_2N_1}{\beta_{12}\beta_{21}P_1^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_{12}\beta_{21}N_2P_1^{\max}}\right) \\
&\quad - \frac{\beta_{12}N_1}{\beta_1\beta_2P_2^{\max}} \cdot E\left(\frac{(\beta_{12}N_1 + \beta_1N_2)(\beta_2N_1 + \beta_{21}N_2)}{\beta_1\beta_2\beta_{21}N_2P_2^{\max}}\right). \tag{3.59}
\end{aligned}$$

Then applying the definitions in Eqs. (3.32–3.34) to Eq. (3.59) yields Eq. (3.35).

3.7 Conclusions

In this chapter we studied a secret sharing problem in which each user with independent messages wishes to broadcast their encoded messages to multiple base stations. The reason why this is a secret sharing problem is because some (i.e., a proper subset) of these base stations may be eavesdropped upon in order to learn the users' messages. We derived an outer region and an inner region that requires an equal SNR property. With a given power constraint, we found the set of admissible power schemes that ensures equal SNR. An important technical property we derived is the fact that the inner region can be simplified as a single region (instead of an infinite union of regions), and that this region results from using the maximum power scheme from the set of admissible power schemes. When the power constraint lies in the admissible power set, the inner region and outer region partially coincide on the diagonal, which suggests that using Gaussian codebooks without pre-coding may be close to optimal in these cases. To further demonstrate that our inner region is significant, we showed that the inner region of a related Z-channel problem is a subset of our inner region. Lastly, we derived a kind of “outage” probability under the slow and flat Rayleigh fading scenario, which shows that if we are willing to pay a price in power, then the channel has a non-zero probability of being favorable for unconditional secret communications under the equal SNR regime.

References

- [1] Trappe, W., Washington, L.C.: *Introduction to Cryptography with Coding Theory*. Prentice-Hall, Inc., Upper Saddle River, New Jersey (2002)
- [2] Zheng, Q., Hong, X., Liu, J., Tang, L.: A secure data transmission scheme for mobile ad hoc networks. In: IEEE Globecom. Washington, DC (2007)
- [3] Tse, D., Viswanath, P.: *Fundamentals of Wireless Communication*. Cambridge University Press (2005)
- [4] Tekin, E., Yener, A.: The Gaussian multiple access wire-tap channel with collective secrecy constraints. In: IEEE International Symposium on Information Theory. Seattle, WA (2006)
- [5] Tekin, E., Yener, A.: The multiple access wire-tap channel: Wireless secrecy and cooperative jamming. In: Information Theory and Applications Workshop. San Deigo, CA (2007)
- [6] Leung-Yan-Cheong, S.K., Hellman, M.E.: The Gaussian wire-tap channel. *IEEE Transaction on Information Theory*. **24**(4), pp. 451–456 (1978)
- [7] Tang, X., Liu, R., Spasojevic, P., Poor, H.V.: Interference-assisted secret communication. In: Proceedings of IEEE Information Theory Workshop. Porto, Portugal (2008)
- [8] Tang, X., Liu, R., Spasojevic, P., Poor, H.V.: The Gaussian wiretap channel with a helping interferer. In: Proceedings of IEEE International Symposium on Information Theory. Toronto, Ontario, Canada (2008)
- [9] Simeone, O., Popovski, P.: Secure communications via cooperative base stations. *IEEE Communications Letters* **12**(3), pp. 188–190 (2008)
- [10] Barros, J., Rodrigues, M.R.D.: Secrecy capacity of wireless channels. In: IEEE International Symposium on Information Theory, pp. 356–360. Seattle, WA (2006)
- [11] Bloch, M., Barros, J., Rodrigues, M.R.D., McLaughlin, S.W.: Wireless information-theoretic security. *IEEE Transaction on Information Theory*. **54**(6), pp. 2515–2534, (2008)
- [12] Gopala, P.K., Lai, L., Gamal, H.E.: On the secrecy capacity of fading channels. *IEEE Transaction on Information Theory*. **54**(10), pp. 4687–4698, (Oct. 2008)
- [13] Liang, Y., Poor, H.V., Shamai (Shitz), S.: Secrecy capacity region of fading broadcast channels. In: IEEE International Symposium on Information Theory (2007)
- [14] Liang, Y., Poor, H.V., Shamai (Shitz), S.: Secure communication over fading channels. *IEEE Transaction on Information Theory*. **54**(6), pp. 2470–2492, (Jun. 2008)
- [15] Khisti, A., Wornell, G.W.: Secure transmission with multiple antennas: The MISOME wiretap channel. *IEEE Transaction on Information Theory* (2007). Submitted
- [16] Cover, T.M., Thomas, J.A.: *Elements of Information Theory*, 2nd edn. John Wiley & Sons, Inc. (2006)
- [17] Dougherty, E.R.: *Random Processes for Image and Signal Processing*. SPIE Optical Engineering Press and IEEE Press, Bellingham, Washington (1999)
- [18] Liang, Y., Poor, H.V.: Generalized multiple access channels with confidential messages. *IEEE Transaction on Information Theory* (2006). (Submitted)
- [19] Liang, Y., Poor, H.V.: Secrecy capacity region of binary and Gaussian multiple access channels. In: Proceedings of Allerton Conference on Communication, Control, and Computing. Urbana, IL (2006)
- [20] Liu, R., Maric, I., Yates, R.D., Spasojevic, P.: The discrete memoryless multiple access channel with confidential messages. In: IEEE International Symposium on Information Theory. Seattle, WA (2006)
- [21] Tekin, E., Serbetli, S., Yener, A.: On secure signaling for the Gaussian multiple access wire-tap channel. In: Asilomar Conference on Signals, Systems and Computers, pp. 1747–1751. Pacific Grove, CA (2005)

Chapter 4

Cooperative Jamming: The Tale of Friendly Interference for Secrecy*

Xiang He and Aylin Yener

4.1 Introduction

In wireless communications, interference is generally regarded as an undesired phenomenon. In multiuser systems, interference management and avoidance are essential for acceptable system performance [1, 2]. In systems including cognitive radios with secondary spectrum privileges, a system objective is detecting the channel occupancy in an intelligent way to limit interference to primary users [3].

In contrast with the conventional wisdom, in secure communications, interference can be a potentially beneficial phenomenon and hence a welcome addition, if injected to the system properly. This recently developed interesting form of cooperation enlists the help of nodes that are legitimate entities in the system and essentially asks them to jam the eavesdropper from whom the information flowing in the system is to be kept secret. The idea in essence is to put the eavesdropper at a disadvantage as compared to the legitimate parties. This chapter is devoted to exploring the technique based on this idea which we affectionately term “cooperative jamming” and its applications in different system models with Gaussian channels representing (wireless) communication scenarios of interest.

Before going into the details, a note on the naming conventions are in order. Though we will refer to this technique as “cooperative jamming”, as it was proposed in [4], the reader may encounter variants of this technique under names such as “artificial noise” [5], “noise forwarding” [6], or “interference assisted secret communication” [7]. All involve introducing interference into the system in one form or

X. He (✉)
Department of Electrical & Computer Engineering
Penn State University, University Park
PA 16802, USA
e-mail: xxh119@psu.edu

*Portions of the material have appeared previously in “The General Gaussian Multiple Access and Two-way Wire-tap Channels: Achievable Rates and Cooperative Jamming,” IEEE Transactions on Information Theory, vol. 54, no. 6, 2008 ©IEEE 2008; and “Two-hop Secure Communication Using and Untrusted Relay: A Case for Cooperative Jamming,” Proceedings of IEEE Global Telecommunication Conference, ©IEEE 2008.

another to increase secrecy rate. Indeed, cooperative jamming has become such an essential part of achievability proofs of multi-terminal channel models with secrecy constraints that the readers may encounter it in other chapters of this book. In this chapter, we focus on several interesting aspects of cooperative jamming and illustrate them with examples. In doing so, we must note that we will consider the three forms in which cooperative jamming can be accomplished by the friendly terminal(s):

- Cooperative Jamming with Noise
- Cooperative Jamming with a Random Code
- Cooperative Jamming with a Structured Code

The next three sections are devoted to exploiting the above methods to improve achievable secrecy rates in the basic Gaussian Wiretap channel that consists of a transmitter, the legitimate receiver and an external eavesdropper, with the addition of a friendly cooperative jammer. The model can also be thought of as a two-user multiple access channel where one user transmits data while the other does cooperative jamming. Section 4.5 changes the scenario and considers an example where no external eavesdropper is present, but one of the parties involved in communication, in this case the relay node between the two nodes, is not trustworthy. The impact of cooperative jamming by one of the end-nodes on the secrecy rate of the other is considered. Sections 4.6 and 4.7 consider the multiple access channel with an external eavesdropper, where cooperative jamming with noise is established as a method to improve the secrecy sum-rate of the channel. There we show, to maximize the secrecy sum rate, the users need to be divided into two groups: the transmitting nodes and the cooperative jammers, and no user does both, coming to a full circle with the original model we considered in Sect. 4.2.

4.2 Cooperative Jamming with Noise

A simple example is sufficient to explain the notion of cooperative jamming. Here, we start with the familiar Gaussian Wiretap channel shown in Fig. 4.1. Z_1 and Z_2 are zero mean Gaussian random variables with unit variance. It was proved in [8] that the secrecy capacity of this channel is the difference between the capacity of the

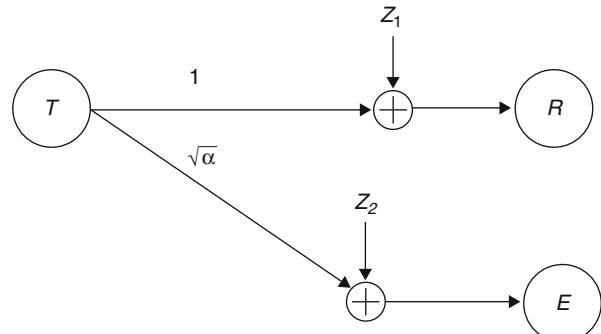
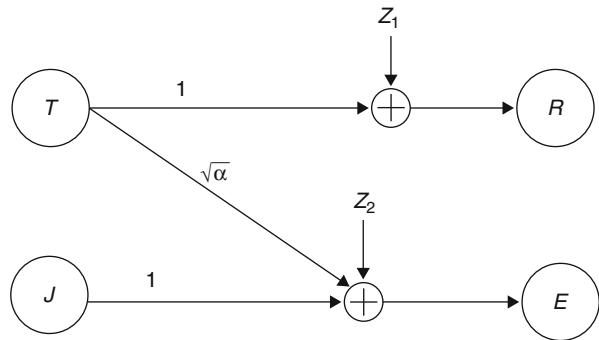


Fig. 4.1 Wiretap channel,
T: Transmitter, R: Receiver,
E: Eavesdropper

Fig. 4.2 Wiretap channel with a friendly cooperative jammer, J



main channel and the eavesdropper channel:

$$[C(P) - C(\alpha P)]^+ \quad (4.1)$$

where $C(x) = \frac{1}{2} \log_2 (1 + x)$, and P is the average power constraint of the transmitter. Equation (4.1) implies that, if $\alpha \geq 1$, meaning the channel to the eavesdropper (E) is better than to the legitimate receiver (R), the secrecy capacity of T is zero.

Now suppose that there is another transmitter in the system “close” to the eavesdropper. We denote this transmitter with J as shown in Fig. 4.2. This transmitter cannot have secure communication to R as it has a better channel to E . However, it may *choose* to transmit an i.i.d. Gaussian sequence to confuse the eavesdropper and help T . Let the variance of this sequence be P_J . Then with the help of node J , the secrecy rate of node T , which is the difference between the channel capacity of the main channel and the eavesdropper channel, becomes:

$$\left[C(P) - C\left(\frac{\alpha P}{1 + P_J}\right) \right]^+ \quad (4.2)$$

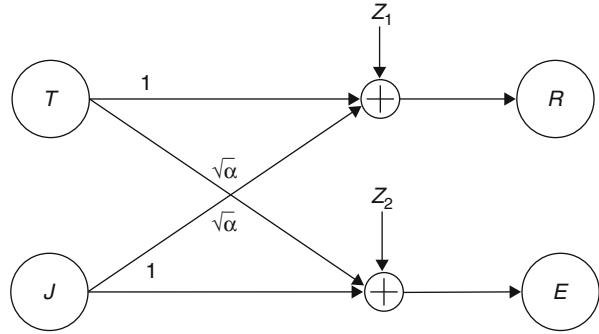
Comparing Eq. (4.2) with Eq. (4.1), we notice the secrecy rate of the transmitter T increases with the *cooperation* of the transmitter J , hence the name *cooperative jamming*.

4.3 Cooperative Jamming with a Random Codebook

The reader might fall under the impression that cooperative jamming should be used only if the friendly jammer can cause more interference to the eavesdropper than to the legitimate receiver. This feeling turns out to be overly pessimistic, as shown by the following example from [7].

Consider the channel in Fig. 4.3, where the cooperative jammer causes more interference to the legitimate receiver than it does to the eavesdropper when $\alpha > 1$. However, if the jamming signal is a codeword from a codebook, the legitimate

Fig. 4.3 Wiretap channel with a friendly cooperative jammer: the symmetric case



receiver can decode the jamming signal and remove this interference. Thus an advantage over the eavesdropper may still be attained. In fact, if $1 < \alpha < 1 + P$ and $P < P_J$, then a positive secrecy rate can be achieved as follows:

Let the cooperative jammer transmit with a codeword from a Gaussian code book. Its rate R_J is chosen such that the jamming signal can be decoded by the receiver. For example, R_J can be picked as

$$R_J = C\left(\frac{\alpha P_J}{P + 1}\right) \quad (4.3)$$

Under this choice, the receiver can decode and subtract the interference caused by the jammer by treating the rest part of the received signals as noise.

Let the set of the secret messages be $\{W\}$. To achieve a secrecy rate of R_s , the transmitter uses $2^{\lfloor nR_s \rfloor}$ independently generated Gaussian code books. Each code book corresponds to a secret message, and includes $2^{\lfloor nR_x \rfloor}$ code words. R_x, R_s are picked to meet the following condition:

$$R_x + R_s = C(P) \quad (4.4)$$

Therefore, the rate at which T is transmitting is below the channel capacity between T and the legitimate receiver node R . After subtracting the interference from the jammer, the receiver can always decode the codeword sent by the transmitter from the remaining part of its received signal.

R_x is chosen such that the pair (R_x, R_J) is in the capacity region of multiple access channel (MAC) between T, J and the eavesdropper node E . A simple choice would be making $R_x + R_J$ be the sum capacity:

$$R_x = C(\alpha P + P_J) - R_J \quad (4.5)$$

$$= C(\alpha P + P_J) - C\left(\frac{\alpha P_J}{P + 1}\right) \quad (4.6)$$

Also, the MAC capacity region requires $R_J < C(P_J)$. This means $\alpha < P + 1$.

With R_x given by Eq. (4.6), R_s can be computed according to Eq. (4.4).

$$R_s = C(P) - R_x \quad (4.7)$$

$$= C(P) - C(\alpha P + P_J) + C\left(\frac{\alpha P_J}{P+1}\right) \quad (4.8)$$

$$= \frac{1}{2} \log_2 \left(\frac{1 + P + \alpha P_J}{1 + \alpha P + P_J} \right) \quad (4.9)$$

Note that R_s is positive whenever $P_J > P$.

Let Y_e^n be the received signal by the eavesdropper. Let \mathcal{C} be the codebook used by the transmitter node T . The equivocation rate is lower bounded as follows:

$$H(W|Y_e^n \mathcal{C}) \quad (4.10)$$

$$= H(X^n W|Y_e^n \mathcal{C}) - H(X^n|WY_e^n \mathcal{C}) \quad (4.11)$$

$$\geq H(X^n W|Y_e^n \mathcal{C}) - n\varepsilon_n \quad (4.12)$$

$$= H(X^n|Y_e^n \mathcal{C}) + H(W|X^n Y_e^n \mathcal{C}) - n\varepsilon_n \quad (4.13)$$

$$= H(X^n|Y_e^n \mathcal{C}) - n\varepsilon_n \quad (4.14)$$

$$= H(X^n|Y_e^n \mathcal{C}) - H(X^n|\mathcal{C}) + H(X^n|\mathcal{C}) - n\varepsilon_n \quad (4.15)$$

$$= H(X^n|\mathcal{C}) - I(X^n; Y_e^n|\mathcal{C}) - n\varepsilon_n \quad (4.16)$$

$$= H(X^n|\mathcal{C}) - I(X^n J^n; Y_e^n|\mathcal{C}) + I(J^n; Y_e^n|X^n \mathcal{C}) - n\varepsilon_n \quad (4.17)$$

$$= H(X^n|\mathcal{C}) - I(X^n J^n; Y_e^n|\mathcal{C}) + H(J^n|X^n \mathcal{C}) - H(J^n|X^n Y_e^n \mathcal{C}) - n\varepsilon_n \quad (4.18)$$

$$\geq H(X^n|\mathcal{C}) - I(X^n J^n; Y_e^n|\mathcal{C}) + H(J^n|X^n \mathcal{C}) - n\varepsilon_n - n\nu_n \quad (4.19)$$

$$= H(X^n|\mathcal{C}) - I(X^n J^n; Y_e^n|\mathcal{C}) + H(J^n|\mathcal{C}) - n\varepsilon_n - n\nu_n \quad (4.20)$$

$$\geq H(X^n|\mathcal{C}) - I(X^n J^n; Y_e^n) + H(J^n|\mathcal{C}) - n\varepsilon_n - n\nu_n \quad (4.21)$$

$$\geq H(X^n|\mathcal{C}) + H(J^n|\mathcal{C}) - \sum_{i=1}^n I(X_i J_i; Y_{e,i}) - n\varepsilon_n - n\nu_n \quad (4.22)$$

$$= H(X^n|\mathcal{C}) + H(J^n|\mathcal{C}) - nI(XJ; Y_e) - n\varepsilon_n - n\nu_n \quad (4.23)$$

$$= H(X^n|\mathcal{C}) + H(J^n|\mathcal{C}) - nC(aP + P_J) - n\varepsilon_n - n\nu_n \quad (4.24)$$

The fact that (R_x, R_J) is in the capacity region of MAC channel between T, J and E is used along with Fano's inequality in Eqs. (4.12) and (4.19). ε_n and ν_n are two non-negative variables that go to 0 whenever n goes to ∞ .

From the coding scheme, we have

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(X^n|\mathcal{C}) = R_1 = C(P) \quad (4.25)$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(J^n|\mathcal{C}) = R_2 = C\left(\frac{\alpha P_J}{P+1}\right) \quad (4.26)$$

Substituting them into Eq. (4.24), we get

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W|Y_e^n \mathcal{C}) \quad (4.27)$$

$$= C(P) + C\left(\frac{\alpha P_J}{P+1}\right) - C(\alpha P + P_J) \quad (4.28)$$

$$= \frac{1}{2} \log_2 \left(\frac{1 + P + \alpha P_J}{1 + \alpha P + P_J} \right) \quad (4.29)$$

Comparing it with Eq. (4.9), we find that:

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W|Y_e^n \mathcal{C}) = \lim_{n \rightarrow \infty} \frac{1}{n} H(W) \quad (4.30)$$

Let $\Pr(E|\mathcal{C})$ be the probability of decoding error under the code book \mathcal{C} . Then

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(W; Y_e^n \mathcal{C}) + \Pr(E|\mathcal{C}) = 0 \quad (4.31)$$

Therefore, there must exist a codebook \mathcal{C}^* such that

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(W; Y_e^n \mathcal{C}^*) = 0 \quad (4.32)$$

$$\lim_{n \rightarrow \infty} \Pr(E|\mathcal{C}^*) = 0 \quad (4.33)$$

Hence we have shown that the secret rate of Eq. (4.9) is achievable when $1 < \alpha < P + 1$ and $P < P_J$.

4.4 Cooperative Jamming with a Structured Codebook

It was shown in [9] that a nested lattice codebook can be used to achieve the capacity of the AWGN channel. A lattice codebook is different from a random codebook in the sense that it has a structure in the high dimensional space. In this section, we discuss a lower bound to the secrecy rate from [10], when this structured codebook is used as the cooperative jamming signal. Once again, we focus on the channel model in Fig. 4.2, with $\alpha = 1$.

The codebook is constructed as follows: Let (Λ, Λ_1) be a properly designed nested lattice structure in \mathbb{R}^N as described in [9], where Λ_1 is the coarse sub-lattice of the fine lattice Λ . Let \mathcal{V}_1 and \mathcal{V} be their respective fundamental regions. The codebook is all the lattice points within the set $\Lambda \cap \mathcal{V}_1$.

Let t_A^N be the lattice point transmitted by node T . Let d_A^N be the dithering noise uniformly distributed over \mathcal{V}_1 . The transmitted signal is given by

$$t_A^N + d_A^N \mod \Lambda_1 \quad (4.34)$$

The receiver receives the above signal corrupted by Gaussian noise and tries to decode t_A^N . Let the decoding result be \hat{t}_A^N . Then as shown in [9, Theorem 5], for a sequence of properly designed (Λ, Λ_1) with increasing dimension, if

$$\lim_{N \rightarrow \infty} \frac{1}{N} \log_2 |\Lambda \cap \mathcal{V}_1| < C(P) \quad (4.35)$$

$$C(P) = \frac{1}{2} \log_2(1 + P) \quad (4.36)$$

then

$$\lim_{N \rightarrow \infty} \Pr(t_A^N \neq \hat{t}_A^N) = 0 \quad (4.37)$$

The cooperative jammer uses the same codebook as the node T . Let the lattice point transmitted by it be t_B^N and the dithering noise be d_B^N . The transmitted signal is given by

$$t_B^N + d_B^N \mod \Lambda_1 \quad (4.38)$$

As in [9], we assume that d_A^N is known by node T , the legitimate receiver node R and the eavesdropper node E . d_B^N is known by node T , and the eavesdropper node E . Hence, there is no common randomness between the legitimate communicating pairs that is not known by the eavesdropper.

Let $a \oplus b$ denote the operation $a + b \mod \Lambda_1$. Then the signal received by the eavesdropper can be represented as

$$t_A^N \oplus d_A^N + t_B^N \oplus d_B^N + n^N \quad (4.39)$$

where n^N is the Gaussian channel noise over N channel uses.

Since we have both \oplus and $+$ here, Eq. (4.39) is a nonlinear function of t_A^N . To work around this difficulty, we need the following representation theorem [10]: Let t_a^N, t_b^N be two points in \mathcal{V}_1 . In our case, t_a^N corresponds to $t_A^N \oplus d_A^N$. t_b^N corresponds to $t_B^N \oplus d_B^N$. Then we have:

Theorem 1 *There is a bijection between*

$$t_a^N + t_b^N \quad (4.40)$$

and the tuple

$$T, t_a^N \oplus t_b^N \quad (4.41)$$

where T is a discrete variable taking value from 1 to 2^N .

The proof can be found in [10]. Here we verify the theorem with a simple example: Consider a one-dimension lattice $N=1$: the set of integers \mathbb{Z} . The fundamental region in this case is $(-1/2, 1/2)$. We can recover $t_a + t_b$ from $t_a \oplus t_b$ according to the following rules:

1. If $T = 0$, then

$$t_a + t_b = t_a \oplus t_b \quad (4.42)$$

2. If $T = 1$, and $t_a \oplus t_b > 0$, then

$$t_a + t_b = t_a \oplus t_b - 1 \quad (4.43)$$

3. If $T = 1$, and $t_a \oplus t_b \leq 0$, then

$$t_a + t_b = t_a \oplus t_b + 1 \quad (4.44)$$

Therefore, 1 bit is enough to represent the difference between $t_a + t_b$ and $t_a \oplus t_b$.

With this result, we have:

$$\begin{aligned} H(t_A^N | t_A^N \oplus d_A^N + t_B^N \oplus d_B^N + n^N, d_A^N, d_B^N) \\ \geq H(t_A^N | t_A^N \oplus d_A^N + t_B^N \oplus d_B^N + n^N, d_A^N, d_B^N, n^N) \end{aligned} \quad (4.45)$$

$$= H(t_A^N | t_A^N \oplus d_A^N + t_B^N \oplus d_B^N, d_A^N, d_B^N) \quad (4.46)$$

$$= H(t_A^N | t_A^N \oplus d_A^N \oplus t_B^N \oplus d_B^N, d_A^N, d_B^N, T) \quad (4.47)$$

$$= H(t_A^N | t_A^N \oplus t_B^N, d_A^N, d_B^N, T) \quad (4.48)$$

$$= H(t_A^N | t_A^N \oplus t_B^N, T) \quad (4.49)$$

$$= H(T | t_A^N \oplus t_B^N, t_A^N) + H(t_A^N | t_A^N \oplus t_B^N) - H(T | t_A^N \oplus t_B^N) \quad (4.50)$$

$$\geq H(t_A^N | t_A^N \oplus t_B^N) - H(T | t_A^N \oplus t_B^N) \quad (4.51)$$

$$= H(t_A^N) - H(T | t_A^N \oplus t_B^N) \quad (4.52)$$

$$\geq H(t_A^N) - H(T) \quad (4.53)$$

In Eq. (4.52), we use the fact that t_A^N is independent from $t_A^N \oplus t_B^N$ [11, Lemma 4] because t_A^N and t_B^N are independent, and t_B^N is uniformly distributed over $\mathcal{V}_1 \cap \Lambda$.

Let

$$c = \frac{1}{N} I(t_A^N; t_A^N \oplus d_A^N + t_B^N \oplus d_B^N + n^N, d_A^N, d_B^N) \quad (4.54)$$

Then from Eq. (4.53), since $H(T) \leq N$, we have

$$c \leq 1 \quad (4.55)$$

Therefore, if the message is mapped one-to-one to t_A^N , then an equivocation rate of at least $C(P) - 1$ is achievable under a transmission rate of $C(P)$ bits per channel use.

To obtain perfect secrecy, we need to do a bit more work. First, we define a block of channel uses as the N channel uses required to transmit a N dimensional lattice point. A perfect secrecy rate of $C(P) - 1$ can then be achieved by coding across multiple blocks: A codeword in this case is composed of Q components, each

component is an N dimensional lattice point sampled from a uniform distribution over $\mathcal{V}_1 \cap \Delta$ in an i.i.d. fashion. The resulting codebook \mathcal{C} contains $2^{\lfloor NQR \rfloor}$ codewords with $R < C$. Like Wiretap codes, the codebook is then randomly binned into several bins, each bin contains $2^{\lfloor NQc \rfloor}$ codewords. The secret message W is mapped to the bins. The actual transmitted codeword is chosen from that bin according to a uniform distribution.

Let Y_e^{NQ} denote the signals available to the eavesdropper:

$$Y_e^{NQ} = \left\{ t_A^{NQ} \oplus d_A^{NQ} + t_B^{NQ} \oplus d_B^{NQ} + n^{NQ}, d_A^{NQ}, d_B^{NQ} \right\} \quad (4.56)$$

Then we have

$$H(W|Y_e^{NQ}, \mathcal{C}) \quad (4.57)$$

$$= H(W|t_A^{NQ}, Y_e^{NQ}, \mathcal{C}) + H(t_A^{NQ}|Y_e^{NQ}, \mathcal{C}) - H(t_A^{NQ}|W, Y_e^{NQ}, \mathcal{C}) \quad (4.58)$$

$$\geq H(t_A^{NQ}|Y_e^{NQ}, \mathcal{C}) - NQ\varepsilon \quad (4.59)$$

$$= H(t_A^{NQ}|Y_e^{NQ}, \mathcal{C}) - H(t_A^{NQ}|\mathcal{C}) + H(t_A^{NQ}|\mathcal{C}) - NQ\varepsilon \quad (4.60)$$

$$= H(t_A^{NQ}|\mathcal{C}) - I(t_A^{NQ}; Y_e^{NQ}|\mathcal{C}) - NQ\varepsilon \quad (4.61)$$

$$\geq H(t_A^{NQ}|\mathcal{C}) - \sum_{q=1}^Q I(t_A^N; Y_e^N|\mathcal{C}) - NQ\varepsilon \quad (4.62)$$

$$= H(t_A^{NQ}|\mathcal{C}) - QNc - NQ\varepsilon \quad (4.63)$$

$$= QN(R - c) - NQ\varepsilon \quad (4.64)$$

The fact that the size of each bin is smaller or equal to $2^{\lfloor NQc \rfloor}$ is used along with Fano's inequality in Eq. (4.59). Here $\varepsilon \geq 0$ and $\lim_{N, Q \rightarrow \infty} \varepsilon = 0$.

Similar arguments as in Eqs. (4.31–4.33) can then be used to show a secrecy rate of $C(P) - c$ is achievable. Since $c < 1$, this means a secrecy rate of at least $C(P) - 1$ bits per channel use is achievable.

It is interesting to compare the secrecy rate obtained here with that of cooperative jamming with noise. The latter is given by

$$C(P) - C\left(\frac{P}{P+1}\right) \quad (4.65)$$

$\lim_{P \rightarrow \infty} C\left(\frac{P}{P+1}\right) = 0.5$. Therefore there is at most 0.5 bit per channel use of loss in secrecy rate at high SNR by using a structured code book as the jamming signal.

At this point, the reader may ask why we would ever want to use a structured jamming signal. Although not advantageous in this system model, a structured cooperative jamming signal can be a powerful tool to provide secrecy and analyze the secrecy rate in larger networks. An example of this is the multi-hop half-duplex communication model considered in [10] in which a source wishes to communicate to a destination via relay nodes all of which have to be oblivious to the signal they

relay. Though, a natural choice of relaying scheme in this case is either compress-and-forward or amplify-and-forward [12, 13], we note that under neither scheme the relay node can remove the channel noise as it is not able to decode the messages. Instead, by using a structured codebook, both for data transmission and cooperative jamming, each relay node can decode the modulus sum of message and jamming signals, remain oblivious to the secret message and remove the channel noise at the same time. Hence, it becomes possible to achieve a secrecy rate that does not decrease with the number of hops. Details of this result can be found in [10].

4.5 Cooperative Jamming in Gaussian Two-Way Relay Channel

In the previous sections, we have assumed that the transmitter can communicate with the legitimate receiver directly. In this section, we consider a more complicated scenario: As shown in Fig. 4.4, the transmitter, node 1, can only communicate with the receiver, node 2, via a relay, node 3. To do that, a two-hop, two-phase communication protocol is used. During the first phase, node 1 transmits to node 3. During the second phase, node 3 relays what it received to node 2.

Consider now that node 3 is a unmalicious node which is willing to help relay node 1's signal, but is unauthenticated. Thus, we would like to treat node 3 as the eavesdropper. Conventional wisdom in this case would question the applicability of this communication protocol. After all, node 3 is the only transmitter from whom node 2 can receive any information. Is it then feasible to expect that node 1 can send information to node 2 that is secret from node 3? The answer again lies in cooperative jamming. Specifically, node 2 may jam node 3 while node 1 transmits its information to node 3. The resulting two-way relay channel model is shown in Fig. 4.5. Note that we still use a half duplex two-phase model. In the first phase, both node 1 and 2 transmit, node 3 listens. In the second phase, node 3 broadcasts to node 2 and node 1. The relationship between different signals can be expressed as:

$$Y_r = X_1 + X_2 + Z_3 \quad (4.66)$$

$$Y_1 = hX_r + Z_1 \quad (4.67)$$

$$Y_R = X_r + Z_2 \quad (4.68)$$

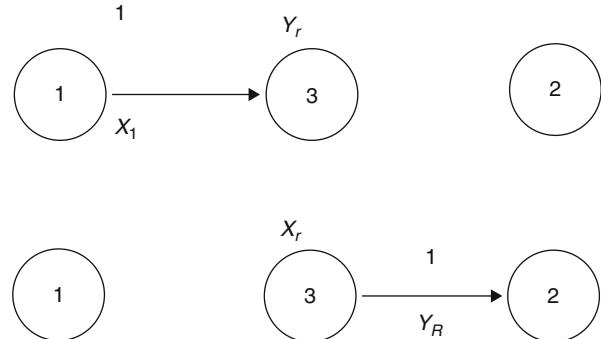
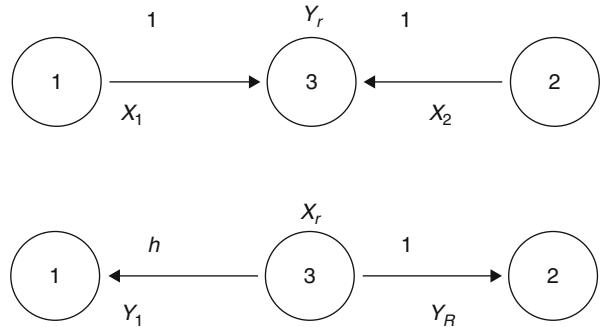


Fig. 4.4 Two hop communication

Fig. 4.5 Two way channel with un-trusted relay



where X_r, Y_r are the signal transmitted and received by node 3 respectively. X_1, Y_1 are the signal transmitted and received by node 1 respectively. X_2, Y_R are the signal transmitted and received by node 2 respectively.

A moment's thought reveals that in this model, node 2 essentially acts as a cooperative jammer and in effect also jams itself in addition to the eavesdropper node 2. However, since it knows its own jamming signal, it can remove its effect from its own received signal. Hence an advantage over the untrusted relay node is achieved. Reference [14] proves that the following rate is achievable:

$$0 \leq R_e \leq \max_{0 \leq P'_1 \leq P_1} \left[C \left(\frac{P'_1}{(1 + \sigma_c^2)} \right) - C \left(\frac{P'_1}{(1 + P_2)} \right) \right]^+ \quad (4.69)$$

where

$$\sigma_c^2 = \frac{P'_1 + 1}{P_r} \quad (4.70)$$

The expression is the difference of two rates. The first term is essentially the rate of the main channel, where σ_c^2 is the effective noise under the compress-and-forward scheme. The second term is the rate of the eavesdropper channel, where the effect of cooperative jamming is shown via the P_2 term on the denominator.

We note that the above coding scheme gives the secrecy rate where the past received signals at node 1 and 2 are not used to compute signals transmitted in the future. In other words, the encoders at node 1 and node 2 work independently. One wonders then how good this achievable secrecy rate is. Next we describe the upper bound derived in [14] to serve this purpose.

We begin by recognizing, if past signals are not used to compute signal transmitted in the future at either node 1 or 2, signal Y_1 is simply ignored. The channel model is equivalent to the model shown in Fig. 4.6.

The upper bound is then obtained via the following transformation steps:

- First, we add a second eavesdropper to the channel, as shown by Fig. 4.7. Its received signal Y_e is given by

$$Y_e = X_1 + X_2 + Z_e \quad (4.71)$$

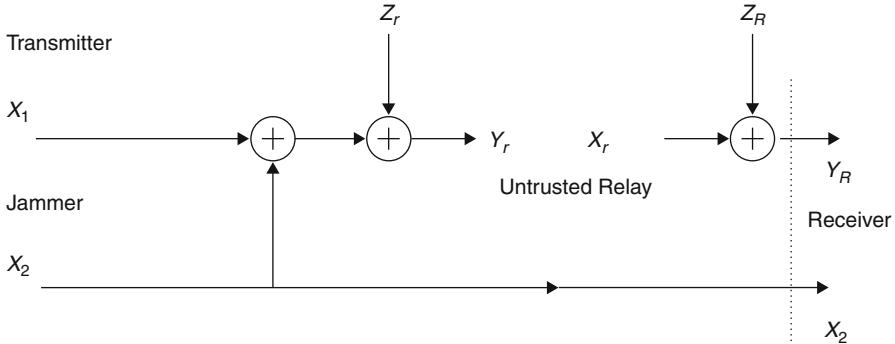


Fig. 4.6 Equivalent channel model (©IEEE 2008)

Here Z_e is a Gaussian noise with the same distribution as Z_r . However, it can be arbitrarily correlated with Z_r . It can be proved by following a slightly modified version of [15, Theorem 3] that doing so will not decrease the secrecy rate. In essence, this is because any coding scheme that works in the original system will still work in the new two-eavesdropper system.

2. Next, we remove the first eavesdropper at the relay. Doing so will not decrease the secrecy rate either, since we have one less secrecy constraint.

Remark 1 A key condition for the argument above to work is that the two eavesdroppers cannot hear each other [15]. This argument would not work if the jamming signal X_2 were allowed to depend on the signals received previously. In this case,

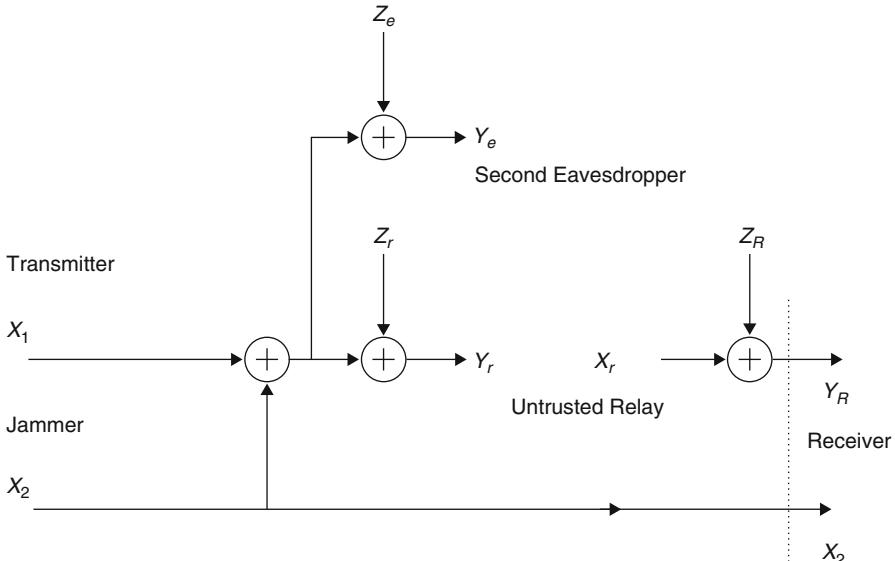


Fig. 4.7 Two eavesdropper channel (©IEEE 2008)

there would be a feedback link from Y_R to X_2 in Fig. 4.7. The eavesdroppers could hear each other via this feedback link and we would not be able to guarantee that the secrecy rate would not decrease.

Next, the signal X_r^n is provided to the destination by a genie. The signal X_2^n is revealed to the relay. The secrecy rate is then bounded by:

$$\begin{aligned} H(W_1|Y_e^n) &\leq H(W_1|Y_e^n) - H(W_1|X_r^n Y_R^n X_2^n) + n\varepsilon_n \end{aligned} \quad (4.72)$$

$$= H(W_1|Y_e^n) - H(W_1|X_r^n X_2^n) + n\varepsilon_n \quad (4.73)$$

$$\leq H(W_1|Y_e^n) - H(W_1|Y_r^n X_r^n X_2^n) + n\varepsilon_n \quad (4.74)$$

$$= H(W_1|Y_e^n) - H(W_1|Y_r^n X_2^n) + n\varepsilon_n \quad (4.75)$$

$$= H(W_1|Y_e^n) - H(W_1|X_1^n + Z_r^n) + n\varepsilon_n \quad (4.76)$$

$$\leq H(W_1|Y_e^n) - H(W_1|Y_e^n, X_1^n + Z_r^n) + n\varepsilon_n \quad (4.77)$$

Fano's inequality is used in Eq. (4.72). $\varepsilon_n > 0$ and $\lim_{n \rightarrow \infty} \varepsilon_n = 0$. The genie information X_r causes the signal Y_R to be useless to the destination, as shown by Eqs. (4.72–4.73). Revealing the genie information X_2 to the relay essentially removes the influence of the jamming signal from the relay link, as shown by Eqs. (4.74–4.77). These are essentially a consequence of the link noises being independent. The resulting channel is equivalent to the one shown in Fig. 4.8. It can be viewed as a special case of the channel in [7, 16], and similar techniques can be used here to bound its secrecy rate. Let $\tilde{Y}_r^n = X_1^n + Z_r^n$. Then, we have:

$$\begin{aligned} H(W_1|Y_e^n) - H(W_1|Y_e^n \tilde{Y}_r^n) + n\varepsilon_n &= I(W_1; \tilde{Y}_r^n | Y_e^n) + n\varepsilon_n \end{aligned} \quad (4.78)$$

$$\leq I(W_1 X_1^n; \tilde{Y}_r^n | Y_e^n) + n\varepsilon_n \quad (4.79)$$

$$= I(X_1^n; \tilde{Y}_r^n | Y_e^n) + n\varepsilon_n \quad (4.80)$$

$$= h(\tilde{Y}_r^n | Y_e^n) - h(Z_r^n | X_2^n + Z_e) + n\varepsilon_n \quad (4.81)$$

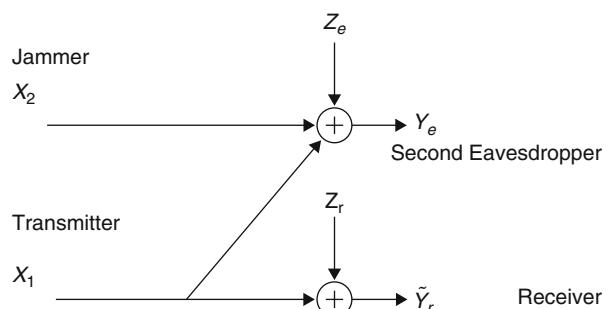


Fig. 4.8 Channel model after transformation
©IEEE 2008

$$\leq h(\tilde{Y}_r^n | Y_e^n) - h(Z_r^n | X_2^n + Z_e^n, X_2^n) + n\varepsilon_n \quad (4.82)$$

$$= h(\tilde{Y}_r^n | Y_e^n) - h(Z_r^n | Z_e^n) + n\varepsilon_n \quad (4.83)$$

The first term in Eq. (4.83) is maximized when X_1^n and X_2^n are i.i.d. Gaussian sequences. Let the variance of each component of X_i^n be P_i , $i = 1, 2$. Let ρ be the correlation factor between Z_r and Z_e . Then Eq. (4.83) is equal to

$$\frac{1}{2} \log_2 \frac{(P_1 + 1)(P_1 + P_2 + 1) - (P_1 + \rho)^2}{(P_1 + P_2 + 1)(1 - \rho^2)} \quad (4.84)$$

It can be verified that, for arbitrary ρ , Eq. (4.83) is an increasing function of P_1 and P_2 . Therefore, the upper bound is maximized with maximal average power. Equation (4.84) can then be tightened by minimizing it over ρ . The optimal ρ is given below:

$$\frac{2P_1 + P_1 P_2 + P_2 - \sqrt{4P_2 P_1^2 + 4P_2 P_1 + P_2^2 P_1^2 + 2P_2^2 P_1 + P_2^2}}{2P_1} \quad (4.85)$$

Theorem 2 *The secrecy rate of the channel in Fig. 4.6 is upper bounded by Eq. (4.84), where ρ is given by Eq. (4.85). P_1 and P_2 are the average power constraints of the transmitter and the jammer.*

Remark 2 The bound Eq. (4.84) is strictly smaller than the trivial bound $C(P_1)$ obtained by removing the secrecy constraints. To show that, simply let $\rho = 0$. Equation (4.84) becomes

$$C(P_1) + \frac{1}{2} \log_2 \frac{1 + \frac{P_1}{(P_1 + 1)(P_2 + 1)}}{1 + \frac{P_1}{(P_2 + 1)}} \quad (4.86)$$

The second term is always negative.

Remark 3 Fix P_2 , and increase P_1 . The bound (4.84) can be approximated by

$$\frac{1}{2} \log_2 \left(\frac{P_2 + 2(1 - \rho)}{1 - \rho^2} \right) \quad (4.87)$$

where

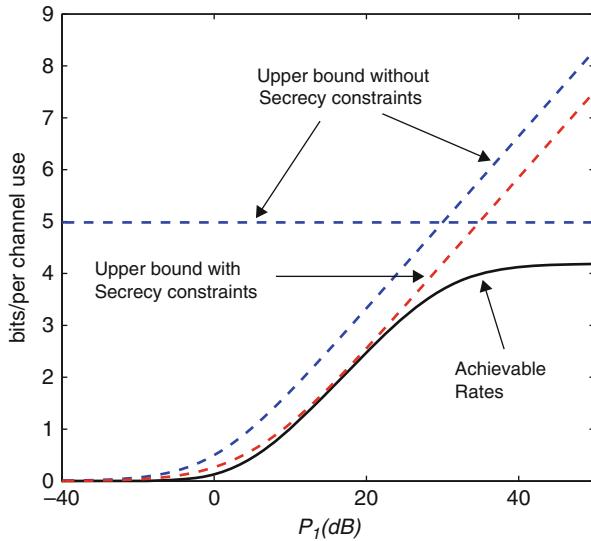
$$\rho = \frac{1 + P_2}{2 - \sqrt{P_2 + P_2^2/4}} \quad (4.88)$$

On the other hand, if we let $P_2 = cP_1$, and increase P_1 (and hence P_2), then the bound (4.84) can be approximated by

$$C(P_1) - C\left(\frac{1}{c}\right) \quad (4.89)$$

The approximation here means the difference between the bound and its approximation converges to 0 as $P_1 \rightarrow \infty$.

Fig. 4.9 Comparison of achievable rates and upper bounds when $P_r = 30$ dB $P_2 = 0.5P_1$ (©IEEE 2008)



Finally we compare the upper bound with the achievable rate. The numerical result is shown in Fig. 4.9, with the power of the relay node fixed at $P_r = 30$ dB. Also shown are cut-set bound computed by removing all the secrecy constraints. Fig. 4.9 shows the upper bound is tight when the source power P_1 is smaller than the relay power P_r .

4.6 Cooperative Jamming in Gaussian Multiple Access Wiretap Channel

In the previous sections, we have assumed that only one node wishes to transmit secret information. In this section, we consider the case where more than one users wish to send secret messages to a legitimate receiver [17, 18]. Specifically, we describe the solution given in [16, 19] of the secrecy sum rate maximization under superposition coding, which once again leads to cooperative jamming.

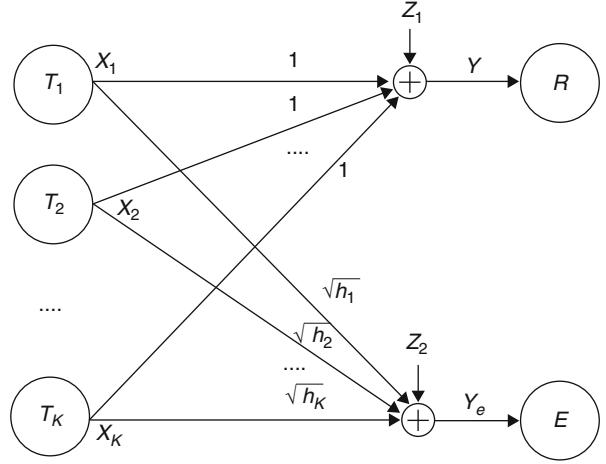
Consider K users communicating with an intended receiver in the presence of an eavesdropper who has the same capabilities. The channel model is depicted in Fig. 4.10. Node T_1, \dots, T_K are K transmitters. Node R is the legitimate receiver, and node E is the eavesdropper. The received signals at R and E are:

$$Y = \sum_{k=1}^K X_k + Z_1 \quad (4.90)$$

$$Y_e = \sum_{k=1}^K \sqrt{h_k} X_k + Z_2 \quad (4.91)$$

where Z_1 and Z_2 are Gaussian random variables with zero mean and unit variance, and $\sqrt{h_1}, \dots, \sqrt{h_K}$ denote the normalized channel gains to the eavesdropper.

Fig. 4.10 The Gaussian multiple access wiretap channel



The secrecy capacity region of this channel is currently an open problem. Achievable rates are presented in [16, 19]. Here, we will concentrate on the secrecy sum rate. Specifically, as is done in [16, 19], we will consider the secrecy sum rate maximizing power allocation under superposition coding and cooperative jamming. The optimization problem is stated as follows:

$$\max_{\substack{T \subseteq \{1, \dots, K\}, \\ 0 \leq P_k \leq \bar{P}_k}} C \left(\frac{\sum_{k \in T} P_k}{1 + \sum_{k \in T^c} P_k} \right) - C \left(\frac{\sum_{k \in T} h_k P_k}{1 + \sum_{k \in T^c} h_k P_k} \right) \quad (4.92)$$

where \bar{P}_k is the average power constraint of the k th user. $C(x) = \frac{1}{2} \log_2(1 + x)$.

In formulating Eq. (4.92), we consider that a user either transmits a valid codeword or Gaussian noise [19]. To see why a mixed strategy where a user splits its power between codeword transmission and jamming is unnecessary, we observe that Eq. (4.92) can be rewritten in the following form:

$$\min_{\substack{T \subseteq \{1, \dots, K\}, \\ 0 \leq P_k \leq \bar{P}_k}} \frac{\phi_K(P)}{\phi_{T^c}(P)} \quad (4.93)$$

$$\phi_K(P) = \frac{1 + \sum_{k \in \{1, \dots, K\}} h_k P_k}{1 + \sum_{k \in \{1, \dots, K\}} P_k} \quad (4.94)$$

$$\phi_{T^c}(P) = \frac{1 + \sum_{k \in T^c} h_k P_k}{1 + \sum_{k \in T^c} P_k} \quad (4.95)$$

$$P = \{P_k, k = 1, \dots, K\} \quad (4.96)$$

Note that we are not losing generality by letting a user split its power among jamming and transmitting, since, regardless to note that regardless of how a user splits its power, $\phi_K(P)$ will be the same, and the user only affects $\phi_{T^c}(P)$. Assume the

optimum solution P^* is such that user j splits its power, so $j \in T$ and $j \in T^c$. Then, it is easy to see that if $h_j < \phi_{T^c}(P)$, the sum-rate is increased when that user uses its jamming power to transmit, and when $h_j > \phi_{T^c}(P)$, the sum-rate is increased when the user uses its transmit power to jam. When $h_j = \phi_{T^c}(P)$, then regardless of how its power is split, the sum-rate is the same, and we can assume user j either transmits or jams.

Solving Eq. (4.92) requires careful examination of all possible choices of Lagrange multipliers and is involved. We refer the interested reader to [19, Sect. 3.5]. The solution, which we summarize below, has an interesting structure.

Theorem 3 Assume $h_1 \leq h_2 \leq \dots h_K$. The secrecy sum-rate using cooperative jamming is given by

$$R_{\text{sum}} = C \left(\frac{\sum_{k \in T} P_k^*}{1 + \sum_{k \in T^c} P_k^*} \right) - C \left(\frac{\sum_{k \in T} h_k P_k^*}{1 + \sum_{k \in T^c} h_k P_k^*} \right) \quad (4.97)$$

T is the set of users which should transmit codewords. The set T and the optimal power allocation has the following form

$$\underbrace{\{1, \dots, t, t+1, \dots, J-1\}}_{\substack{P^* = \bar{P} \\ \text{transmitting, i.e., } \in T}} \cup \underbrace{\{J, J+1, \dots, K\}}_{\substack{P_J^* \\ \text{jamming, i.e., } \in T^c}} \quad (4.98)$$

where P_J^* is a number between 0 and \bar{P}_J .

In essence, the theorem states that, under the optimal power allocation, users who transmit codewords either transmit with full power or shut down. Among those users who transmit Gaussian noise, i.e., cooperative jammers, at most one user may transmit at a power level less than its average power constraint. All others jam with full power.

We next demonstrate this property with a numerical example from [19]. We consider a 100×100 square, as shown in Fig. 4.11. Assume there are $K = 2$ users denoted by T_1 and T_2 . The legitimate receiver is at the origin, and is denoted by R . A simple path-loss model is used to compute the channel gains. For each position the eavesdropper might appear, the optimal power allocation is computed for each user and shown in Fig. 4.11 with different colors. By observing each row of Fig. 4.11, it is clear that a user never split its power between transmission and jamming. By observing the first column of Fig. 4.11, it is clear that if a user is not jamming, it either transmits with peak power or it remains silent. The last row of Fig. 4.11 plots the secrecy sum rate under different locations of the eavesdropper. It is seen that when the eavesdropper is in the vicinity of a transmitter, that transmitter cannot transmit in secrecy. However, in this case, the transmitter can jam the eavesdropper very effectively with low power, and allow the other transmitter to transmit and/or increase its secrecy rate with little jamming power.

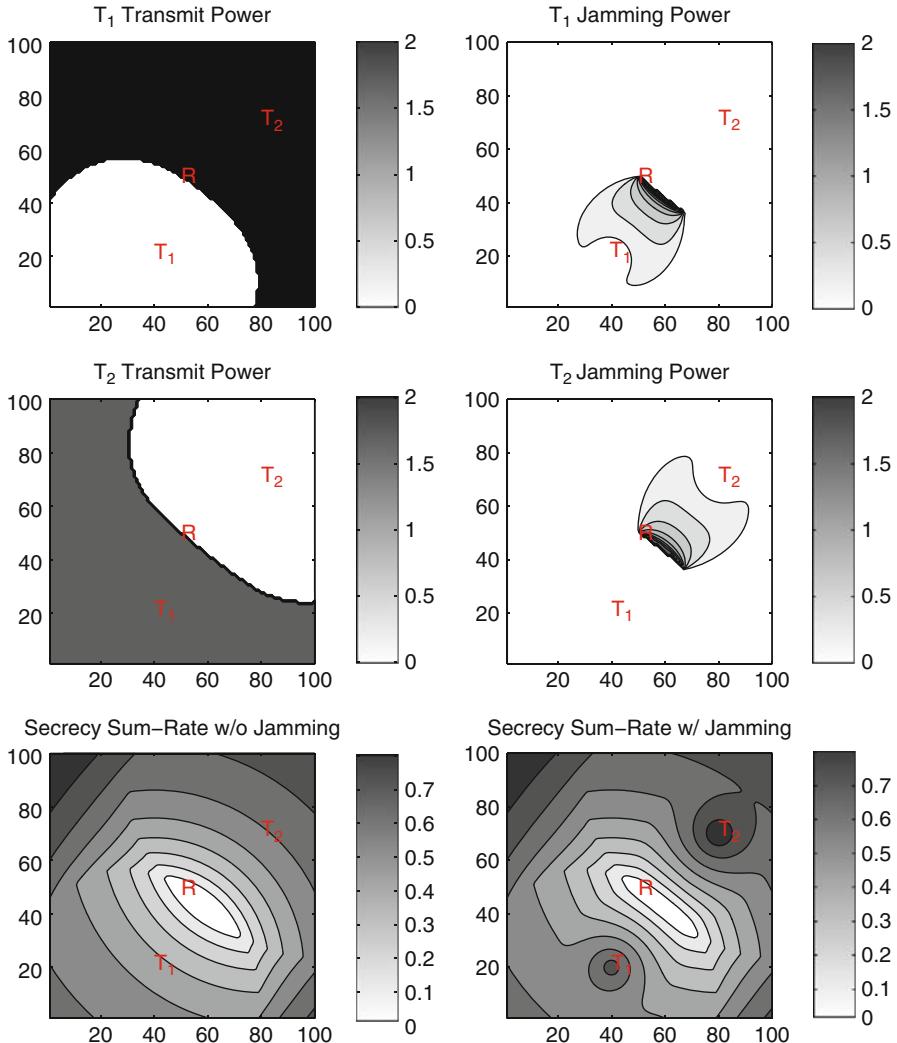


Fig. 4.11 Two user Gaussian MAC Wiretap channel: Numerical example—darker shades correspond to higher values (©IEEE 2008) [19]

4.7 Cooperative Jamming in Fading Gaussian Multiple Access Wiretap Channel

In wireless communication, fading is an unavoidable phenomena. In information theoretic security, it can potentially offer an advantage. Intuitively, legitimate parties should be able to communicate with higher rates when the eavesdropper happens to be in deep fading. The secrecy capacity of the single user Fading Wiretap channel has

been studied under different assumptions [20–22]. In this section, we focus on the same problem under the multi-user scenario, i.e., the fading multiple access channel with an external eavesdropper. Addressing the secrecy sum rate maximization problem under an ergodic block fading Gaussian multiple access Wiretap channel, references [19, 23] once again show that cooperative jamming can add to the secrecy benefits of opportunistic communication. We review this result next.

For simplicity, the discussion is restricted to the two user case. The instantaneous channel gain of user k 's main channel within one fading block is denoted by h_k^M , $k = 1, 2$. The instantaneous channel gain of the eavesdropper channel for user k within one fading block is denoted by h_k^W . The instantaneous transmission power of user k as P_k and jamming power of user k as Q_k . Then, the instantaneous achievable sum-rate is given by [23]:

$$\begin{aligned} & \frac{1}{2} \log \left(\frac{1 + h_1^M(P_1 + Q_1) + h_2^M(P_2 + Q_2)}{1 + h_1^M Q_1 + h_2^M Q_2} \right) \\ & - \frac{1}{2} \log \left(\frac{1 + h_1^W(P_1 + Q_1) + h_2^W(P_2 + Q_2)}{1 + h_1^W Q_1 + h_2^W Q_2} \right) \end{aligned} \quad (4.99)$$

The optimization problem can then be expressed as

$$\max_{P_1(\mathbf{h}), P_2(\mathbf{h})} \int_0^\infty \cdots \int \log \left(\frac{\Phi^M + \phi^M - 1}{\Phi^W + \phi^W - 1} \cdot \frac{\phi^W}{\phi^M} \right) p(\mathbf{h}) d\mathbf{h} \quad (4.100)$$

$$\text{s.t. } \int_0^\infty \cdots \int (P_k(\mathbf{h}) + Q_k(\mathbf{h})) p(\mathbf{h}) d\mathbf{h} \leq \bar{P}_k, \quad k = 1, 2 \quad (4.101)$$

$$P_k(\mathbf{h}) \geq 0, \quad k = 1, 2 \quad (4.102)$$

$$Q_k(\mathbf{h}) \geq 0, \quad k = 1, 2 \quad (4.103)$$

where

$$\phi^M = 1 + h_1^M Q_1 + h_2^M Q_2 \quad (4.104)$$

$$\phi^W = 1 + h_1^W Q_1 + h_2^W Q_2 \quad (4.105)$$

$$\Phi^M = 1 + h_1^M P_1(\mathbf{h}) + h_2^M P_2(\mathbf{h}) \quad (4.106)$$

$$\Phi^W = 1 + h_1^W P_1(\mathbf{h}) + h_2^W P_2(\mathbf{h}) \quad (4.107)$$

Note that P_1 , P_2 , Q_1 , Q_2 are functions of \mathbf{h} even though this is not explicitly shown.

We first show that dividing power is suboptimal, i.e., the optimum power allocation should not have P_k , $Q_k > 0$. We prove this using contradiction. Assume the optimum

power allocation is \mathbf{P}^* , \mathbf{Q}^* , and for user 1, $P_1^* > 0$. Note

$$\frac{\partial \frac{\phi^W}{\phi^M}}{\partial Q_1} = \frac{h_1^W \phi^M - h_1^M \phi^W}{\phi^{M2}} \quad (4.108)$$

$$= \frac{h_1^W - h_1^M - (h_1^M h_2^W - h_2^M h_1^W) Q_2}{\phi^{M2}} \quad (4.109)$$

the sign of which does not depend on Q_1 . Consider a power allocation such that $P_1 = P_1^* - \pi$, $Q_1 = Q_1^* + \pi$. Then, $P_1 + Q_1 = P_1^* + Q_1^*$ and $\frac{\Phi^M + \phi^M - 1}{\Phi^W + \phi^W - 1}$ does not change. If Eq. (4.109) is positive, any $\pi > 0$ causes an increase in the achievable sum-rate, and jamming with the same sum power is better. If Eq. (4.109) is negative, then any $\pi < 0$ increases the sum-rate, and transmitting with the same sum power gives a higher rate. If this quantity is zero, the sum-rate does not depend on Q_2 , and we can set it to 0. Thus, we see that the optimal allocation will have either $P_k > 0$ or $Q_k > 0$, but never both.

Another observation we can make is that, under the optimal solution, we must have $\frac{\phi^W}{\phi^M} \geq 1$. Otherwise, we can construct a power allocation that gives the same sum power, and hence the same $\frac{\Phi^M + \phi^M - 1}{\Phi^W + \phi^W - 1}$, but a larger $\frac{\phi^W}{\phi^M}$ which is equal or greater than 1. This would result in a higher transmission rate. The reason why $\frac{\phi^W}{\phi^M} \geq 1$ is seen from Eqs. (4.104) and (4.105). We can at least make $\frac{\phi^W}{\phi^M} = 1$ by picking $Q_1 = Q_2 = 0$ while maintaining the same sum power for each user $P_1 + Q_1$ and $P_2 + Q_2$. Therefore the optimal solution must have $\frac{\phi^W}{\phi^M} \geq 1$.

We can then write the derivative of the Lagrangian with respect to the transmit power of user k as

$$\frac{\partial \mathcal{L}}{\partial P_k} = \frac{h_k^M}{\Phi^M + \phi^M - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1} - \lambda_k + \mu_k = 0 \quad (4.110)$$

Noting that we must have

$$\frac{\Phi^M + \phi^M - 1}{\phi^M} \geq \frac{\Phi^W + \phi^W - 1}{\phi^W} \quad (4.111)$$

to have a non-negative secrecy rate, we can write

$$\lambda_k - \mu_k = \frac{h_k^M}{\Phi^M + \phi^M - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1} \quad (4.112)$$

$$\leq \frac{\frac{\phi^W}{\phi^M} h_k^M}{\Phi^W + \phi^W - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1} \quad (4.113)$$

$$\leq \frac{\phi^W h_k^M - \phi^M h_k^W}{\phi^M} \quad (4.114)$$

$$\leq \phi^W h_k^M - \phi^M h_k^W \quad (4.115)$$

and as a result, if $\phi^W h_k^M - \phi^M h_k^W < \lambda_k$, we must have $\mu_k > 0 \Rightarrow P_k = 0$. Now consider the jamming powers:

$$\frac{\partial \mathcal{L}}{\partial Q_k} = \frac{h_k^M}{\Phi^M + \phi^M - 1} - \frac{h_k^W}{\Phi^W + \phi^W - 1} - \frac{h_k^M}{\phi^M} + \frac{h_k^W}{\phi^W} - \lambda_k + \nu_k \quad (4.116)$$

Using Eq. (4.110) in (4.116), we get

$$-\frac{h_k^M}{\phi^M} + \frac{h_k^W}{\phi^W} + \nu_k = \mu_k \quad (4.117)$$

If a user is jamming, we must have $\nu_k = 0$, $\mu_k \geq 0$. Hence,

$$\frac{h_k^W}{\phi^W} \geq \frac{h_k^M}{\phi^M} \quad (4.118)$$

Since we should not have both users jamming at the same time (in which case the achievable rate is 0 and we should stop any transmission), this implies that for the jamming user,

$$\frac{h_k^W}{h_k^M} \geq \frac{1 + h_k^W Q_k}{1 + h_k^M Q_k} \Rightarrow h_k^W \geq h_k^M \quad (4.119)$$

Thus, if a user has $h_k^W > h_k^M$, since $\phi^W \geq \phi^M$, we necessarily have $\frac{h_k^W}{\phi^W} > \frac{h_k^M}{\phi^M}$ and as a result $\mu_k > 0$, indicating that user is not transmitting, as expected. If both users have $h_k^W \geq h_k^M$, no user transmits or jams. We see that

- A user will not be transmitting if $\phi^W h_k^M - \phi^M h_k^W < \lambda_k$.
- A user will not be jamming if $\phi^W h_k^M - \phi^M h_k^W > 0$ (or equivalently $h_k^M \geq h_k^W$).

Therefore, if for both users we have $h_k^M \geq h_k^W$, neither user will be jamming. The problems becomes the sum rate maximization without cooperative jamming, whose solution is given in [19, Sect. 5.4].

We are interested in the form of the solution if one user transmitting and the other jamming. Without loss of generality, assume $P_1 > 0$, $Q_2 > 0$, i.e. when user 1 is transmitting and user 2 is jamming. We can re-write Eq. (4.116) as:

$$\begin{aligned} h_2^W h_1^W P_1 \phi^M (\Phi^M + \phi^M - 1) - h_2^M h_1^M P_1 \phi^W (\Phi^W + \phi^W - 1) \\ = \lambda_2 \phi^M \phi^W (\Phi^M + \phi^M - 1)(\Phi^W + \phi^W - 1) \end{aligned} \quad (4.120)$$

We then need to have the following two equations simultaneously satisfied:

$$\frac{h_1^M}{\Phi^M + \phi^M - 1} - \frac{h_1^W}{\Phi^W + \phi^W - 1} = \lambda_1 \quad (4.121)$$

$$\frac{h_2^W h_1^W / \phi^W}{\Phi^W + \phi^W - 1} - \frac{h_2^M h_1^M / \phi^M}{\Phi^M + \phi^M - 1} = \frac{\lambda_2}{P_1} \quad (4.122)$$

The first equation Eq. (4.121) comes from Eq. (4.110).

No simple close-form expression exists for this case. However, we can still make the following two observations:

1. Cooperative jamming effectively reduces the transmission threshold for the active user. Since $\phi^W \geq \phi^M$, we see that the condition to transmit is relaxed from $h_k^M - h_k^W \geq \lambda_k$ to $\frac{\phi^W}{\phi^M} h_k^M - h_k^W \geq \lambda_k$.
2. A user only jams if its main channel gain is lower than that of its eavesdropper channel gain.

The optimal power allocation is solved numerically and shown in Fig. 4.12. Channel gains within each block follow independent Rayleigh fading. Letting the mean gain for the main channels to be unity, Fig. 4.12 plots the achievable ergodic secrecy sum-rate and upper bound in as a function of the mean eavesdropper channel gain. The dashed lines represent instantaneous power control, where we impose the same maximum power constraint on each fading block. The solid lines represent ergodic fading case, where we maintain a long-term average power constraint. The lines denoted by ∇ show achievable rates without cooperative jamming, the lines denoted by $*$ represent achievable rates with cooperative jamming. We see that the achievable rates for both instantaneous and ergodic power control are close when the eavesdropper channel is weak, but drift apart as the eavesdropper channel gets stronger. Cooperative jamming improves the achievable secrecy sum-rate most when the eavesdropper channel is strong, as it is possible to more effectively jam the eavesdropper. We note the increase in the achievable secrecy sum-rate when the transmitters have, on average, a high eavesdropper channel. In this case, when one of the transmitters has a good, and the other had a bad channel, cooperative jamming allows very high instantaneous rates.

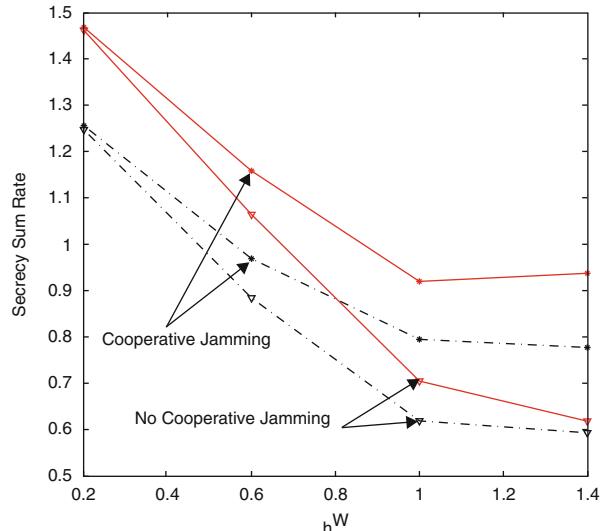


Fig. 4.12 Achievable secrecy sum-rate as a function of mean eavesdropper channel gain h^W . Dashed lines: no power control. Solid lines: Optimal power control

4.8 Conclusions

In this chapter, we demonstrated the positive impact of injecting judicious interference into a system with secrecy constraints, by friendly helpers called cooperative jammers. Cooperative jamming can be used even if the jammer caused more interference to the legitimate receiver than to the eavesdropper. Both random and lattice codebooks can be used as jamming signals. The latter proves particularly useful in large networks, and may turn out to be more amenable to analysis.

Cooperative jamming can also be used in systems where some of the nodes participating in the communication are untrusted, despite being non-malicious. We considered one such example where secret communication can be facilitated in a two-way relay network with an untrusted relay when the destination node cooperatively jams the relay node to aid the source node.

For the multi-user scenario, we considered two cases: the static Gaussian Multiple access Wiretap channel, and its ergodic block fading version. The power allocation solution to the secrecy sum rate maximization from [16, 19] was reviewed, under superposition coding scheme with cooperative jamming. For both cases, the solution had an interesting structure, in that a user either transmits data or transmits noise but not both. In the two user multiple access scenario, this model thus potentially reduces to the Gaussian Wiretap channel with a cooperative jammer, i.e., the model considered in Sect. 4.2.

In this chapter, we explained the basic idea of cooperative jamming and showed its usefulness by giving examples that represent the state-of-the-art in models that utilizing cooperative jamming in obtaining achievable secrecy rates. We aimed to point out the wide range of models for which cooperative jamming can be useful, and equip the reader with ability to introduce cooperative jamming into his/her model of choice to improve achievable secrecy rates. Finding upper bounds for multi-terminal problems, and consequently proofs that cooperative jamming may achieve secrecy capacity generally remain illusive. On the other hand, the growing interest in information theoretic secrecy in the research community is reassuring that more results are to come.

References

- [1] C. Rose, S. Ulukus, and R. D. Yates. Wireless Systems and Interference Avoidance. *IEEE Transactions on Wireless Communications*, 1(3):415–428, 2002.
- [2] R. D. Yates. A Framework for Uplink Power Control in Cellular Radio Systems. *IEEE Journal on Selected Areas in Communications*, 13(7):1341–1347, Sept. 1995.
- [3] L. Lai, H. El Gamal, H. Jiang, and H. V. Poor. Cognitive Medium Access: Exploration, Exploitation and Competition. *Submitted to IEEE Transactions on Networking*, 2007.
- [4] E. Tekin and A. Yener. Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy. *Allerton Conference on Communication, Control, and Computing*, 2006.
- [5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete Memoryless Interference and Broadcast Channels with Confidential Messages: Secrecy Rate Regions. *IEEE Transactions on*

- Information Theory, Special Issue on Information Theoretic Security*, 54(6):2493–2507, 2008.
- [6] L. Lai and H. El Gamal. The Relay-Eavesdropper Channel: Cooperation for Secrecy. *Submitted to IEEE Transactions on Information Theory*, 2006.
 - [7] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-Assisted Secret Communication. *IEEE Information Theory Workshop*, 2008.
 - [8] S. Leung-Yan-Cheong and M. Hellman. The Gaussian Wire-tap Channel. *IEEE Transactions on Information Theory*, 24(4):451–456, 1978.
 - [9] U. Erez and R. Zamir. Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN Channel with Lattice Encoding and Decoding. *IEEE Transactions on Information Theory*, 50(10):2293–2314, 2004.
 - [10] X. He and A. Yener. End-to-End Secure Multi-Hop Communication with Untrusted Relays is Possible. In *Proceedings of the 42nd Annual Asilomar Conference on Signals, Systems, and Computers, Asilomar'08*, 2008.
 - [11] L. Lai, H. El Gamal, and H. V. Poor. The Wiretap Channel with Feedback: Encryption over the Channel. *Submitted to IEEE Transaction on Information Theory*, 2007.
 - [12] X. He and A. Yener. On the Equivocation Region of Relay Channels with Orthogonal Components. In *Proceedings of the 41st Annual Asilomar Conference on Signals, Systems, and Computers*, 2007.
 - [13] E. Ekrem and S. Ulukus. Secrecy in Cooperative Relay Broadcast Channels. In *Proceedings of the IEEE International Symposium on Information Theory*, July 2008.
 - [14] X. He and A. Yener. Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming. In *Proceedings of the IEEE Global Telecommunication Conference*, Nov. 2008.
 - [15] X. He and A. Yener. The Role of an Untrusted Relay in Cooperation and Secret Communication. *Submitted to IEEE Transaction on Information Theory*, 2008.
 - [16] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory-Special Issue on Information Theoretic Security*, 54(6):2735–2751, 2008.
 - [17] E. Tekin and A. Yener. On Secure Signaling for the Gaussian Multiple Access Wire-Tap Channel. *Annual Asilomar Conference on Signals, Systems, and Computers*, 2005.
 - [18] E. Tekin and A. Yener. The Gaussian Multiple-Access Wire-Tap Channel. In *IEEE Transaction on Information Theory*, 54(12):5747–5755, 2008.
 - [19] E. Tekin. Information Theoretic Secrecy for Some Multiuser Wireless Communication Channels. *PhD Thesis*, 2008.
 - [20] Y. Liang, H. V. Poor, and S. Shamai. Secure Communication over Fading Channels. *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, 54(6):2470–2492, 2008.
 - [21] P. K. Gopala, L. Lai, and H. El Gamal. On the Secrecy Capacity of Fading Channels. *Submitted to IEEE Transaction on Information Theory*, 2006.
 - [22] Z. Li, R. Yates, and Trappe W. Secrecy Capacity of Independent Parallel Channels. *Allerton Conference on Communication, Control, and Computing*, 2006.
 - [23] E. Tekin and A. Yener. Secrecy Sum-Rates for the Multiple-Access Wire-Tap Channel with Ergodic Block Fading. *Allerton Conference on Communication, Control, and Computing*, 2007.

Chapter 5

Hybrid-ARQ Schemes for Reliable and Secret Wireless Communications*

Xiaojun Tang, Ruoheng Liu, Predrag Spasojević and H. Vincent Poor

5.1 Introduction

Retransmission is a widely adopted and effective approach for ensuring the reliability of communication links for applications of wireless packet-oriented data networks. In an *automatic retransmission request* (ARQ) scheme, frame errors are examined at the receiver by using error detecting codes, e.g., cyclic redundancy check (CRC). If a received packet passes the CRC, the receiver sends an acknowledgement (ACK) of successful transmission to the receiver. Otherwise, the receiver sends back a negative acknowledgement (NACK) to request retransmission. The user data and its CRC bits may be additionally protected by an error correcting code which increases the probability of successful transmission. These schemes, when combining powerful channel coding with retransmission protocols to enhance reliability, are called *hybrid ARQ* (HARQ).

Among currently available HARQ schemes, the most elementary form is the *repetition-coding-based* HARQ which combines several noisy observations of the same packet by using a suitable diversity technique at the receiver, such as maximum-ratio, equal-gain, or selection combining. A more powerful HARQ scheme is the so-called *incremental redundancy* HARQ, which achieves higher efficiency by adapting its error correcting code redundancy to fluctuating channel conditions. In an incremental redundancy scheme as depicted in Fig. 5.1, the message is encoded at the transmitter by a “mother” code. Initially, only a selected number of coded symbols are transmitted (transmission # 1 in the figure). The selected number of coded

X. Tang (✉)
Wireless Information Network Laboratory (WINLAB)
Department of Electrical and Computer Engineering
Rutgers University, 671 Rt. 1 South, North Brunswick
NJ 08902, USA
e-mail: xtang@winlab.rutgers.edu

*Portions of the material have appeared previously in “On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-Fading Channels”, IEEE Transactions on Information Theory, vol. 55, no. 4, 2009 ©IEEE 2009.

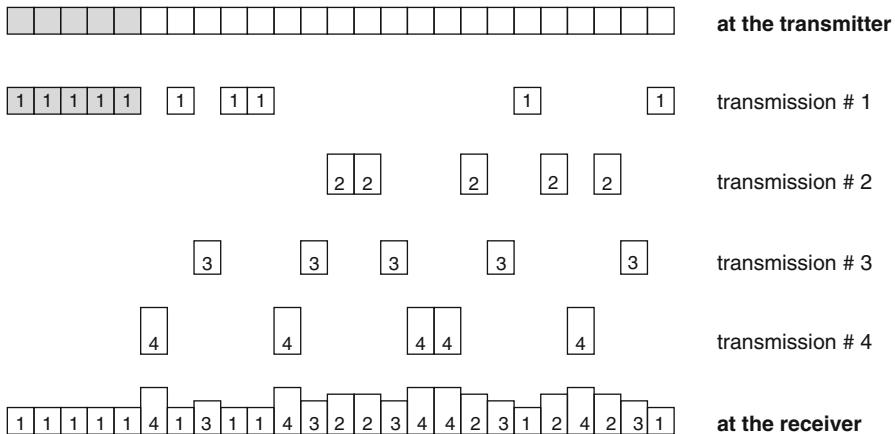


Fig. 5.1 An incremental redundancy HARQ scheme

symbols form a codeword of a punctured code. Decoding of this punctured code is attempted at the receiver. If a retransmission is requested, additional redundancy symbols are sent under possibly different channel conditions (depicted as taller boxes in transmission # 2 in the figure). Decoding is again attempted at the receiver, where the new parity bits are combined with the previously received bits. This procedure is repeated until either the receiver decodes successfully or all parity bits of the mother code are transmitted.

Confidentiality is a further basic requirement for secure communication over wireless networks. The broadcast nature of the wireless medium gives rise to a number of security issues. In particular, wireless transmission is very susceptible to eavesdropping since anyone within the communication range can listen to the traffic and possibly extract information. Traditionally, confidentiality has been provided by using cryptographic methods, which rely heavily on secret keys. However, the distribution and maintenance of secret keys are still open issues for large wireless networks. Fortunately, confidential communication is possible without sharing a secret key between legitimate users. This was shown by Wyner in his seminal paper [9]. In the discrete memoryless wire-tap channel model he proposed, the communication between two legitimate users is eavesdropped upon via a degraded channel (the eavesdropper channel). The level of ignorance of the eavesdropper with respect to the confidential message is measured by the equivocation rate. Perfect secrecy requires that the equivocation rate should be asymptotically equal to the message entropy rate. Wyner showed that perfect secrecy can be achieved via a stochastic code, referred to as the Wyner secrecy code in this work. A general review of the recent research advances in information theoretic security can be found in [32].

In this chapter, we investigate secure packet communication based on HARQ schemes. The challenge of this problem is twofold: first, the encoder at the transmitter needs to provide sufficient redundancy for the legitimate receiver to decode its message successfully; on the other hand, too much redundancy (or insufficient

randomness) may help adversarial eavesdropping. As an example, retransmission is an effective way to enhance reliability but, nevertheless, it may also compromise confidentiality. These considerations motivate the joint consideration of channel coding, secrecy coding and retransmission protocols.

5.1.1 Previous Work

An important performance metric of ARQ schemes is *throughput*, defined as the average number of user data bits accepted at the receiver correctly during the time required for transmission of a single bit. An information-theoretic analysis of the throughput of HARQ schemes over block-fading Gaussian collision channels is found in [1]. By assuming Gaussian random coding and typical-set decoding, the results of [1] are independent of the particular coding/decoding technique and can be regarded as providing a limiting performance in the information-theoretic sense, which is also the approach that we take in this work. Another line of recent research on HARQ focusing on the design of various mother codes and their puncturing can be found in [2–8].

Csiszár and Körner generalized Wyner's result [9] and determined the secrecy capacity region of the broadcast channel with confidential messages in [10]. The Gaussian wiretap channel was studied in [11]. Recently, Wyner secrecy coding has been considered in the study of other multi-user communication models with confidential messages. Those studies include multiple access channels with confidential messages [12, 13], multiple access wire-tap channels [14], and interference channels with confidential messages [15]. The effect of fading on secure communications has been studied in [16–19]. In those works, under the assumption that all communicating parties have perfect channel state information (CSI) prior to the message transmission, a slow fading channel can be modeled as a series of independent parallel wiretap channels. An optimal scheme suggests transmitting independent Wyner secrecy codes over each parallel channel. Within this context, [16] studies the delay limited secrecy capacity of wireless channels, while [17–19] study the secrecy capacity of ergodic fading channels and [19] also considers the ergodic scenario in which the transmitter has no CSI about the eavesdropper channel.

5.1.2 Proposed Work

We consider a frequency-flat block-fading Gaussian wire-tap channel. In this model, a transmitter sends confidential messages to a legitimate receiver via a block-fading channel in the presence of a passive eavesdropper who intercepts the transmission through an independent block-fading channel. We assume that the transmitter has no perfect CSI, but receives a 1-bit ACK/NACK feedback from the legitimate receiver via a reliable public channel. Under this setting, we study the secure HARQ schemes from an information theoretic point of view. In particular, the error and secrecy performance of *repetition time diversity* (RTD) and *incremental redundancy* (INR) schemes are investigated based on Wyner code sequences, which ensure that the confidential message is decoded successfully by the legitimate receiver and is kept

completely secret from the eavesdropper for a given set of channel realizations of the main and the eavesdropper channels. Next, we show that there exists a family of rate-compatible Wyner codes which suit the secure INR scheme.

Due to the absence of CSI, the transmitter cannot adapt its code and power level to channel conditions. Instead, for a given mother code, we consider the outage performance of secure HARQ schemes. Specifically, we define the *connection outage* and the *secrecy outage*. The outage probabilities (i.e., the probabilities of connection and secrecy outage) are used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. We evaluate the achievable throughput of RTD and INR HARQ schemes under the constraints on the two outage probabilities. Finally, we compare the secrecy throughput of two HARQ schemes through both numerical computations and an asymptotic analysis, and illustrate their benefit to information-theoretic secrecy.

5.1.3 Organization

The remainder of this chapter is organized as follows. We introduce the system model and preliminaries in Sect. 5.2. We prove the existence of good Wyner codes for parallel channel communication and define outage events in Sect. 5.3, while these results are applied to INR and RTD schemes in Sect. 5.4. We derive the secrecy throughput of two schemes over block fading channels in Sect. 5.5, and present an asymptotic analysis in Sect. 5.6. We illustrate and compare various results and schemes numerically in Sect. 5.7. Finally, we give conclusions and some interesting directions for future research in Sect. 5.8. Results will be stated without formal proof. The reader is referred to [20] for proofs and further discussions.

5.2 System Model and Preliminaries

5.2.1 System Model

As shown in Fig. 5.2, we consider a model in which a transmitter sends confidential messages to a destination via a source-destination channel (referred to as the main channel) in the presence of a passive eavesdropper which listens to the transmission through a source-eavesdropper channel (referred to as the eavesdropper channel). Both channels experience M -block fading, in which the channel gain is constant within a block while varying independently from block to block [21, 22]. We assume that each block is associated with a time slot of duration T and bandwidth W ; that is, the transmitter can send $N = \lfloor 2WT \rfloor$ real symbols in each slot. Additionally, we assume that the number of channel uses within each slot (i.e., N) is large enough to allow for the invocation of random coding arguments.¹

¹For example, in a 64 kb/s down-link reference data channel for universal mobile telecommunication system (UMTS) data-transmission modes, each slot can contain up to $N \approx 10000$ dimensions [23].

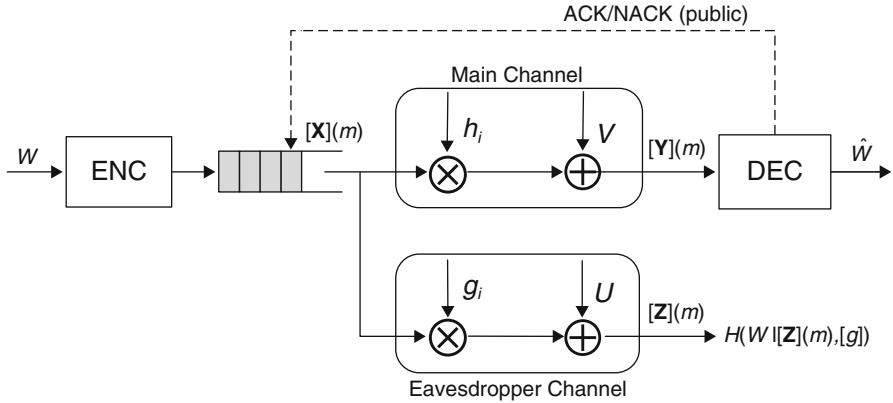


Fig. 5.2 System model: hybrid ARQ schemes for the block-fading channel in the presence of a passive eavesdropper (©IEEE 2009)

At the transmitter, a message $w \in \mathcal{W}$ is encoded into a codeword x^{MN} , which is then divided into M blocks $[x_1^N, x_2^N, \dots, x_M^N]$, each of length N . The codeword x^{MN} occupies M slots; that is, for $i = 1, \dots, M$, the i -th block x_i^N is sent in slot i and received by the legitimate receiver through the channel gain h_i and by the eavesdropper through the channel gain g_i . A discrete time baseband-equivalent block-fading wire-tap channel model can be expressed as follows:

$$y(t) = \sqrt{h_i}x(t) + v(t) \quad \text{and} \quad z(t) = \sqrt{g_i}x(t) + u(t) \quad \text{for } t = 1, \dots, MN, i = \lceil t/N \rceil, \quad (5.1)$$

where $x(t)$ denotes the input signal, $y(t)$ and $z(t)$ denote the output signals at the legitimate receiver and the eavesdropper, respectively, at time t , $\{v(t)\}$ and $\{u(t)\}$ are independent and identically distributed (i.i.d.) $\mathcal{N}(0, 1)$ random variable sequences, and h_i and g_i , for $i = 1, \dots, M$, denote the normalized (real) channel gains of the main channel and the eavesdropper channel, respectively. Furthermore, we assume that the average energy per symbol of the signal $x(t)$ has the constraint

$$E[|x(t)|^2] \leq \bar{P}. \quad (5.2)$$

Let $[h] = [h_1, \dots, h_M]$ and $[g] = [g_1, \dots, g_M]$ denote vectors whose elements are the main channel gains and the eavesdropper channel gains, respectively. We refer to $([h], [g])$ as a *channel pair* and assume that the legitimate receiver knows its channel $[h]$, while the eavesdropper knows its channel $[g]$.

5.2.2 “Good” Wyner Codes

In this subsection, we consider a single-block transmission, i.e., $M = 1$ and introduce Wyner codes [9], which form the basis of our secure HARQ protocols.

When there is no secrecy requirement, i.e., the eavesdropper is disregarded in Fig. 5.2, the stochastic encoder seldom brings any benefits. In this case, a deterministic code is used and can be denoted as $C \in \mathcal{C}(R_0, N)$, where 2^{NR_0} codewords in the codebook convey 2^{NR_0} messages by using a one-to-one mapping.

However, randomization can increase secrecy. In fact, the basic idea of Wyner codes is to use a stochastic encoder to increase the secrecy level [9, 10]. Let

$$C \in \mathcal{C}(R_0, R_s, N)$$

denote a Wyner code of size 2^{NR_0} to convey a confidential message set $\mathcal{W} = \{1, 2, \dots, 2^{NR_s}\}$, where $R_0 \geq R_s$ and N is the codeword length.² Hence, there are two rate parameters associated with the Wyner code: the main channel code rate R_0 and the secrecy information rate R_s . We refer to $R_0 - R_s$ as the secrecy gap, i.e., the rate sacrificed to ensure the secrecy requirement.

The Wyner code $C(R_0, R_s, N)$ is constructed based on random binning [9] as follows. We generate 2^{NR_0} codewords $x^N(w, v)$, where $w = 1, 2, \dots, 2^{NR_s}$, and $v = 1, 2, \dots, 2^{N(R_0 - R_s)}$, by choosing the $N2^{NR_0}$ symbols $x_i(w, v)$ independently at random according to the input distribution $p(x)$. A Wyner code ensemble $\mathcal{C}(R_0, R_s, N)$ is the set of all possible Wyner codes of length N , each corresponding to a specific generation and a specific labeling.

The stochastic encoder of $C(R_0, R_s, N)$ is described by a matrix of conditional probabilities so that, given $w \in \mathcal{W}$, we randomly and uniformly select v from $\{1, 2, \dots, 2^{N(R_0 - R_s)}\}$ and transmit $x^N = x^N(w, v)$. We assume that the legitimate receiver employs a typical-set decoder. Given the received signal y^N , the legitimate receiver tries to find a pair (\tilde{w}, \tilde{v}) so that $x^N(\tilde{w}, \tilde{v})$ and y^N are jointly typical [24], i.e.,

$$\{x^N(\tilde{w}, \tilde{v}), y^N\} \in T_\epsilon^N(p_{XY}),$$

where $T_\epsilon^N(p_{XY})$ denotes the set of (weakly) jointly typical sequences x^N and y^N with respect to $p_{XY}(x, y)$. If there is no such jointly typical pair, then the decoder claims failure.

Assume that signals y^N and z^N are received at the legitimate receiver and the eavesdropper, respectively, via a channel pair (h, g) . The average error probability is defined as

$$P_e(h) = \sum_{w \in \mathcal{W}} \Pr \{ \phi(Y^N) \neq w | h, w \text{ sent} \} \Pr(w), \quad (5.3)$$

where $\phi(Y^N)$ is the output of the decoder at the legitimate receiver and $\Pr(w)$ is the prior probability that message $w \in \mathcal{W}$ is sent.

²Without confusion, let $\mathcal{C}(R_0, N)$ represent non-secrecy deterministic codes and $\mathcal{C}(R_0, R_s, N)$ denote Wyner secrecy codes.

The secrecy level, i.e., the degree to which the eavesdropper is confused, is measured by the equivocation rate at the eavesdropper. We say that *perfect secrecy* is achieved if for all $\epsilon > 0$ the equivocation rate satisfies

$$\frac{1}{N} H(W|g, Z^N) \geq \frac{1}{N} H(W) - \epsilon. \quad (5.4)$$

For conciseness, we say that a code C of length N is *good* for a wire-tap channel with the channel pair (h, g) if $P_e(h) \leq \epsilon$ and the perfect secrecy requirement Eq. (5.4) can be achieved, for all $\epsilon > 0$ and sufficiently large N .

5.2.3 Non-Secure HARQ Schemes

We first describe a general non-secure HARQ scheme for a block-fading channel. The scheme ensures the reliable transmission over the main channel without regarding the presence of the eavesdropper in Fig. 5.2.

First, the transmitter encodes the information (and CRC bits) by using a mother code of length MN . The obtained codeword x^{MN} is partitioned into M blocks represented as $[x_1^N, x_2^N, \dots, x_M^N]$. The (re)transmission protocol is proceeded as follows. At the first transmission, the transmitter sends the block x_1^N under the channel gain pair h_1 . Decoding of this code is performed at the intended receiver. If no error is detected, the receiver sends back an acknowledgement (ACK) to stop the transmission; otherwise a negative acknowledgement (NACK) is sent to request retransmission, and the transmitter sends the block x_2^N under the channel gain pair h_2 . Now, decoding is again attempted at the receiver by combining the previous block x_1^N with the new block x_2^N . The procedure is repeated after each subsequent retransmission until all M blocks of the mother code are transmitted or an HARQ session completes due to the successful decoding at the intended receiver.

Now, we consider two classes of non-secure HARQ schemes, namely RTD and INR HARQs, based on the same basis code

$$C_1 \in \mathcal{C}(MR_0, N).$$

For the RTD scheme, the mother code is chosen as the M-repetition of the basis code C_1 , i.e., the same code is repeatedly used for each transmission; while for the INR scheme, the mother code can be viewed as $C \in \mathcal{C}(R_0, MN)$.

The above two schemes require different combining techniques at the receiver. In the case of the RTD scheme, the (re)transmitted blocks are combined based on the maximum ratio combining technique since the same block is repeated for all transmissions. In contrast, we require code combining in the INR scheme. More specifically, in the first transmission, the transmitted coded symbols $[x](1) = [x_1^N]$ form a codeword of a punctured code, $C_1 \in \mathcal{C}(MR_0, N)$, of length N . Similarly, after m transmissions, for $m \in \{1, \dots, M\}$, all the transmitted coded symbols $[x](m) = [x_1^N, \dots, x_m^N]$ form a codeword of a punctured code,

$$C_m \in \mathcal{C}\left(\frac{MR_0}{m}, mN\right).$$

The decoding at the receiver after m transmissions is attempted based on the punctured code C_m .

Note that the punctured codes $\{C_M, C_{M-1}, \dots, C_1\}$ in the INR scheme form a family of *rate-compatible* codes with the rate sequence

$$\left\{ R_0, \frac{M}{M-1}R_0, \dots, MR_0 \right\}.$$

In [1], Caire and Tuninetti proved that there exists a rate compatible code suitable for the INR scheme, and studied the throughput performance of the INR and RTD schemes. Here, the INR scheme effectively accumulates mutual information of the main channel with each transmission, while the RTD accumulates the signal to noise ratio (SNR) at the receiver. The RTD scheme is a strongly suboptimal scheme, and the INR scheme always outperform the RTD scheme.

The main questions to be answered are whether there exists a rate compatible secrecy code suitable for the secure HARQ schemes, and whether the INR scheme still outperforms the RTD scheme when both secrecy and reliability need to be ensured.

5.2.4 Secure HARQ Schemes

The retransmission protocol for secure HARQ schemes are similar to the non-secure schemes. One of the main differences is that for a secure HARQ scheme, the mother code is chosen to be a joint channel and secrecy code. That is, the transmitter encodes the confidential information (and CRC bits) by using a secrecy mother code of length MN . The obtained codeword x^{MN} is partitioned into M blocks represented as $[x_1^N, x_2^N, \dots, x_M^N]$, where the block x_i^N is sent over an independent channel with the channel gain pair (h_i, g_i) . During each transmission, decoding of this codeword is performed at the intended receiver, while the secrecy level is also measured at the eavesdropper.

5.2.4.1 Performance Measurement

Now, we focus on the error performance and the secrecy level after m transmissions for $m = 1, 2, \dots, M$. Let

$$[x](m) = [x_1^N, \dots, x_m^N], \quad [y](m) = [y_1^N, \dots, y_m^N], \quad \text{and} \quad [z](m) = [z_1^N, \dots, z_m^N]$$

denote the input, the output at the intended receiver, and the output at the eavesdropper after m transmissions, respectively. For a given channel pair $([h], [g])$, the average error probability after m transmissions is defined as

$$P_e(m|[h]) = \sum_{w \in \mathcal{W}} \Pr\{\phi([Y](m)) \neq w | w \text{ sent, } [h]\} \Pr(w), \quad (5.5)$$

where $\phi([Y](m))$ denotes the output of the decoder at the legitimate receiver when receiving $[Y](m)$ after m transmissions.

The secrecy level after m transmissions is given by

$$\frac{1}{mN} H(W|[Z](m), [g]).$$

We say that perfect secrecy is achieved after m transmissions if, for all $\epsilon > 0$, the equivocation rate satisfies

$$\frac{1}{mN} H(W|[Z](m), [g]) \geq \frac{1}{mN} H(W) - \epsilon. \quad (5.6)$$

We note that this definition implies that the perfect secrecy can also be achieved after j transmissions, for $j = 1, \dots, m-1$.

We say that a code C of length mN is *good* for the m -block transmission and a channel pair $([h], [g])$ if $P_e(m|[h]) \leq \epsilon$ and the perfect secrecy requirement Eq. (5.6) can be achieved, for all $\epsilon > 0$ and sufficiently large N .

Next, we consider the secure HARQ schemes based on time repetition diversity and incremental redundancy.

5.2.4.2 Repetition Time Diversity

We first consider a simple time-diversity secure HARQ scheme based on the repetition of a Wyner code. In this case, the mother code C is a concatenated code consisting of the Wyner code $C_1 \in \mathcal{C}(MR_0, MR_s, N)$ as the outer code and a simple repetition code of length M as the inner code, i.e.,

$$C = [\underbrace{C_1, C_1, \dots, C_1}_M]. \quad (5.7)$$

After each transmission, decoding and equivocation calculation are performed at the receiver and the eavesdropper, respectively, based on maximum-ratio combining.

5.2.4.3 Incremental Redundancy

In the INR secure HARQ protocol, the mother code is a Wyner code of length MN , i.e.,

$$C \in \mathcal{C}(R_0, R_s, MN).$$

In the first transmission, the transmitted coded symbols $[x](1) = [x_1^N]$ form a codeword of a punctured Wyner code of length N ,

$$C_1 \in \mathcal{C}(MR_0, MR_s, N).$$

Similarly, after m transmissions, for $m \in \{1, \dots, M\}$, all the transmitted coded symbols $[x](m) = [x_1^N, \dots, x_m^N]$ form a codeword of a punctured Wyner code of length mN ,

$$C_m \in \mathcal{C} \left(\frac{MR_0}{m}, \frac{MR_s}{m}, mN \right).$$

At the legitimate receiver and the eavesdropper, decoding and equivocation calculation are attempted, respectively, based on the punctured code C_m .

We note that the punctured codes $\{C_M, C_{M-1}, \dots, C_1\}$ form a family of *rate-compatible* Wyner codes with the secrecy rates

$$\left\{ R_s, \frac{M}{M-1}R_s, \dots, MR_s \right\}.$$

Hence, we refer to this scheme as the INR scheme based on rate-compatible Wyner codes.

5.3 Secure Channel Set and Outage Events

In this section, we study the error performance and the secrecy level when a mother Wyner code is transmitted over M parallel channels. Results given in this section form the basis for the performance analysis of secure HARQ schemes.

Note that in the system model described in Sect. 5.2, the transmitter does not have any channel state information; that is, one cannot choose the code rate pair based on a particular fading channel state. Instead, an in-advance fixed (Wyner) code rate pair is used for all channel conditions. An important practical question is: for a given pair of Wyner code rates, under what channel conditions will the communication be reliable and secure? In the following, we describe a *secure channel set* and demonstrate that there exists a Wyner code sequence good for all channel pairs in this set.

For a given pair of rates (R_0, R_s) and a fixed input distribution $p(x)$, the secure channel set \mathcal{P} is the union of all channel pairs $([h], [g])$ satisfying

$$\frac{1}{M} \sum_{i=1}^M I(X; Y|h_i) \geq R_0 \quad (5.8)$$

$$\text{and} \quad \frac{1}{M} \sum_{i=1}^M I(X; Z|g_i) \leq R_0 - R_s, \quad (5.9)$$

where $I(X; Y|h_i)$ and $I(X; Z|g_i)$ are single letter mutual information characterizations of the channel Eq. (5.1).

Theorem 1 *Let \mathcal{P} denote the secure channel set for the rate pair (R_0, R_s) and the input distribution $p(x)$. There exists a Wyner code $C \in \mathcal{C}(R_0, R_s, MN)$, generated based on $p(x)$, good for all channel pairs $([h], [g]) \in \mathcal{P}$.*

A proof of Theorem 1 can be found in [20]. To facilitate the formulation of outage-based throughput, we define the outage event as the one which occurs when the channel pair does not belong to the secure channel set, i.e., $([h], [g]) \notin \mathcal{P}$. Specifically, we distinguish two types of outage: *connection outage* and *secrecy outage*.³ In particular, we say that a connection outage occurs if

$$\frac{1}{M} \sum_{i=1}^M I(X; Y|h_i) < R_0, \quad (5.10)$$

while we say that a secrecy outage occurs if

$$\frac{1}{M} \sum_{i=1}^M I(X; Y|g_i) > R_0 - R_s. \quad (5.11)$$

Accordingly, we can evaluate both connection outage and secrecy outage probabilities, which are the probabilities of each of the outage events averaged over all possible fading states. In fact, the connection outage probability can be interpreted as the limiting error probability for large block length packets; the secrecy outage probability can be regarded as an upper bound on the probability of unsecured packets. Moreover, Theorem 1 implies that the connection outage probability and the secrecy outage probability are not just average probabilities over a code ensemble, but they can be achieved by a specific code sequence.

5.4 Wyner Codes Good for HARQ Schemes

In this section, we evaluate the error performance and measure the secrecy level of carefully designed Wyner codes employed in the secure HARQ session.

An important part of an ARQ scheme is that decoding errors should be detected, so that ACKs or NACKs can be generated accurately. A *complete decoding function* (e.g., maximum a posteriori probability decoding or maximum-likelihood decoding) requires the encoder to add extra redundancy to the information bits, which decreases the throughput slightly. The authors of [1] have shown that error detection can be accomplished by using the built-in error detection capability of suboptimal decoders.

Lemma 1 *For all $\epsilon > 0$ and channel $[h]$, any code C of length MN satisfies*

$$\Pr(\text{undetected error}|[h], C) < \epsilon,$$

for all sufficiently large N .

³The main channel is viewed as a communication link. The link is connected if a packet can be delivered to the intended receiver successfully within the delay constraint (within M transmissions), otherwise it is in the connection outage. The connection outage probability defined here is also referred to as *information outage probability* in [21].

5.4.1 Incremental Redundancy

To evaluate the performance of the INR scheme, we employ the following M -parallel channel model. Let us focus on the decoding after m transmissions, i.e., the coded blocks $[x](m) = [x_1^N, \dots, x_m^N]$ are transmitted, for $m \in \{1, \dots, M\}$. As shown in Fig. 5.3, the block x_i^N experiences the channel pair (h_i, g_i) , for $1 \leq i \leq m$. We assume that each of the punctured blocks $[x_{m+1}^N, \dots, x_M^N]$ is sent to a dummy memoryless component channel whose output is independent of the input.

In this case, the mother codeword is transmitted over M parallel channels. At the legitimate receiver, the decoder combines the real signal $[y](m) = [y_1^N, \dots, y_m^N]$ with $M - m$ dummy signal blocks $[b_1^N, \dots, b_{M-m}^N]$ to form

$$[y_1^N, \dots, y_m^N, b_1^N, \dots, b_{M-m}^N].$$

Similarly, the processed symbols at the eavesdropper are

$$[z_1^N, \dots, z_m^N, d_1^N, \dots, d_{M-m}^N],$$

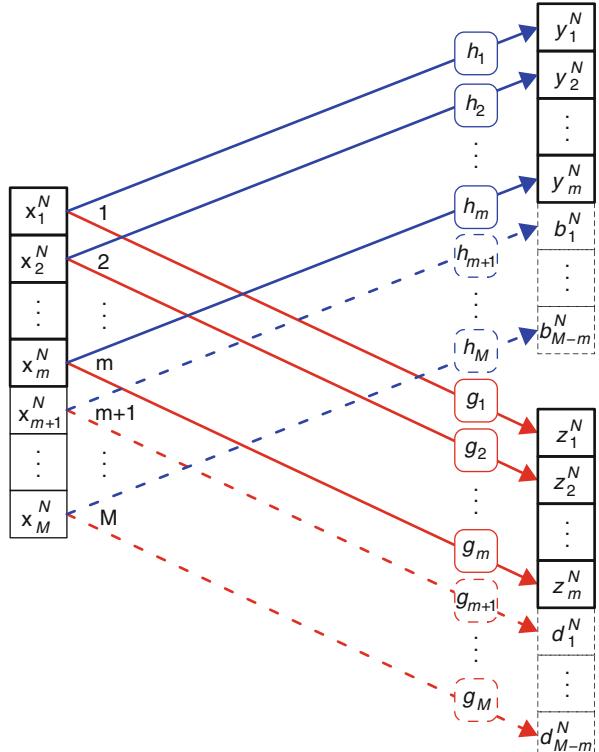


Fig. 5.3 M -parallel channel model for the INR scheme: the first m punctured blocks are actually transmitted (solid lines); the remaining $M - m$ punctured blocks are assumed to be sent via $M - m$ dummy memoryless channels whose outputs are independent of the inputs (dashed lines) (©IEEE 2009)

where $[d_1^N, \dots, d_{M-m}^N]$ are $M - m$ dummy signal blocks. We note that the added dummy blocks do not affect either the decoding at the legitimate receiver or the equivocation calculation at the eavesdropper since they are independent of the confidential message.

The codewords of the mother Wyner code C are transmitted in at most M transmissions during the secure HARQ session. By using the equivalent parallel channel model, we can describe this secure HARQ problem as the communication over M parallel wire-tap channels and, hence, establish the following theorem.

Theorem 2 Consider the secure INR scheme based on rate compatible Wyner codes

$$\{C_M, C_{M-1}, \dots, C_1\},$$

where

$$C_m \in \mathcal{C} \left(\frac{MR_0}{m}, \frac{MR_s}{m}, mN \right), \quad m = 1, \dots, M.$$

Let $\mathcal{P}(m)$ denote the union of all channel pairs $([h], [g])$ satisfying

$$\frac{1}{M} \sum_{i=1}^m I(X; Y|h_i) \geq R_0, \quad (5.12)$$

$$\text{and} \quad \frac{1}{M} \sum_{i=1}^m I(X; Z|g_i) \leq R_0 - R_s. \quad (5.13)$$

Then, there exists a family of rate compatible Wyner codes $\{C_M, C_{M-1}, \dots, C_1\}$ such that C_m is good for all channel pairs $([h], [g]) \in \mathcal{P}(m)$, for $m = 1, \dots, M$.

5.4.2 Repetition Time Diversity

In the secure RTD HARQ scheme, both the legitimate receiver and the eavesdropper combine several noisy observations of the same packet based on diversity techniques. The optimal receivers perform maximum ratio combining (MRC), which essentially transforms the vector channel pair $([h], [g])$ into a scalar channel pair $(\hat{h}(m), \hat{g}(m))$. Hence, after m transmissions, the equivalent channel model can be written as follows:

$$y(t) = \sqrt{\hat{h}(m)}x(t) + v(t) \quad \text{and} \quad z(t) = \sqrt{\hat{g}(m)}x(t) + u(t) \quad (5.14)$$

for $t = 1, \dots, N$, where $\hat{h}(m) = \sum_{i=1}^m h_i$ and $\hat{g}(m) = \sum_{i=1}^m g_i$.

For a given pair of rates (R_0, R_s) and a fixed input distribution $p(x)$, let $\mathcal{L}(m)$ denote the union of all channel pairs $([h], [g])$ satisfying

$$I(X; Y|\hat{h}(m)) \geq MR_0, \quad (5.15)$$

$$\text{and} \quad I(X; Z|\hat{g}(m)) \leq M(R_0 - R_s), \quad (5.16)$$

where $I(X; Y|\hat{h}(m))$ and $I(X; Z|\hat{g}(m))$ are single letter mutual information characterizations of the channel Eq. (5.14). For a given (finite) M , we have the following result for the secure RTD HARQ scheme.

Corollary 1 *There exists a Wyner code $C_1 \in \mathcal{C}(MR_0, MR_s, N)$ such that its m -repeating code*

$$C_m = [\underbrace{C_1, C_1, \dots, C_1}_m]$$

is good for all channel pairs $([h], [g]) \in \mathcal{L}(m)$, for $m = 1, \dots, M$.

5.5 Secrecy Throughput of HARQ schemes

In this section, we study the achievable secrecy throughput for HARQ schemes. We focus on Rayleigh independent block fading channels for illustration; other types of block fading channels can be studied in a similar way.

We note that the optimal input distribution of the channel Eq. (5.1) is not known in general when the transmitter has no CSI. For the sake of mathematical tractability, we consider Gaussian inputs. For INR, the mutual information $I_{XY}^{[\text{INR}]}(m)$ and $I_{XZ}^{[\text{INR}]}(m)$ can be written as

$$\begin{aligned} I_{XY}^{[\text{INR}]}(m) &= \frac{1}{2M} \sum_{i=1}^m \log_2 (1 + \lambda_i) \\ \text{and} \quad I_{XZ}^{[\text{INR}]}(m) &= \frac{1}{2M} \sum_{i=1}^m \log_2 (1 + v_i), \end{aligned} \tag{5.17}$$

where

$$\lambda_i = h_i \bar{P} \quad \text{and} \quad v_i = g_i \bar{P}, \quad i = 1, \dots, M, \tag{5.18}$$

are the signal-to-noise ratios (SNRs) at the legitimate receiver and the eavesdropper, respectively, during transmission i . For RTD, we can express the mutual information quantities $I_{XY}^{[\text{RTD}]}(m)$ and $I_{XZ}^{[\text{RTD}]}(m)$ as

$$\begin{aligned} I_{XY}^{[\text{RTD}]}(m) &= \frac{1}{2M} \log_2 \left(1 + \sum_{i=1}^m \lambda_i \right) \\ \text{and} \quad I_{XZ}^{[\text{RTD}]}(m) &= \frac{1}{2M} \log_2 \left(1 + \sum_{i=1}^m v_i \right). \end{aligned} \tag{5.19}$$

Although we consider only Gaussian signaling here, the results in Sect. 5.4 can be applied to other input distributions, for example, discrete signaling under modulation constraints.

Let \mathcal{M} denote the number of transmissions within a HARQ session. Given a distribution of the main channel SNR λ , for both INR and RTD schemes, the probability mass function of \mathcal{M} can be expressed as

$$\begin{aligned} \forall m \in [1, M-1] \quad p[\mathcal{M} = m] &= \Pr\{I_{XY}(m-1) < R_0 \text{ and } I_{XY}(m) \geq R_0\} \\ &= \Pr\{I_{XY}(m-1) < R_0\} - \Pr\{I_{XY}(m) < R_0\} \\ \text{and} \quad p[\mathcal{M} = M] &= \Pr\{I_{XY}(M-1) < R_0\}, \end{aligned} \quad (5.20)$$

where $I_{XY}(m)$ and $I_{XZ}(m)$ are chosen either from Eq. (5.19) or from Eq. (5.17) corresponding to a specific HARQ scheme. Let P_e denote the connection outage probability, and P_s denote the secrecy outage probability. The definition in Eq. (5.20) implies that P_e and P_s can be written as follows:

$$P_e = \Pr\{I_{XY}(M) < R_0\}, \quad (5.21)$$

$$\text{and} \quad P_s = \sum_{m=1}^M p[m] \Pr\{I_{XZ}(m) > R_0 - R_s\}. \quad (5.22)$$

5.5.1 Throughput with a Secrecy Requirement

Now, we study the secrecy throughput based on P_e and P_s as defined in the above. We first consider a target secrecy outage probability ξ_s ; that is, at least a fraction $1 - \xi_s$ of the confidential message bits sent by the transmitter are kept completely secret. Under this constraint, the secrecy throughput η , measured in bits per second per hertz, is defined to be the average number of bits decoded at the legitimate receiver,

$$\eta = \lim_{t \rightarrow \infty} \frac{a(t)}{tN}, \quad (5.23)$$

where again N is the number of symbols in each block and $a(t)$ is the number of information bits successfully decoded by the intended receiver up to time slot t (when a total of tN blocks are sent). The event that the transmitter stops sending the current codeword is recognized to be a *recurrent event* [25]. A random reward \mathcal{R} is associated with the occurrence of the recurrent event. In particular, $\mathcal{R} = MR_s$ bits/symbol if transmission stops because of successful decoding, and $\mathcal{R} = 0$ bits/symbol if it stops because successful decoding has not occurred after M transmissions. By applying the renewal-reward theorem [1, 25], we obtain the secrecy throughput as

$$\eta(R_0, R_s) = \frac{\mathbb{E}[\mathcal{R}]}{\mathbb{E}[\mathcal{M}]} = \frac{MR_s}{\mathbb{E}[\mathcal{M}]}(1 - P_e), \quad (5.24)$$

where $\mathbb{E}[\mathcal{M}]$ is the expected number of transmissions in order to complete a codeword transmission, i.e.,

$$\begin{aligned}\mathbb{E}[\mathcal{M}] &= \sum_{m=1}^M m p[\mathcal{M} = m] \\ &= 1 + \sum_{m=1}^M \Pr\{I_{XY}(m) < R_0\}. \end{aligned}\quad (5.25)$$

We can properly choose the mother code parameters (R_0 and R_s) to obtain the maximum throughput while satisfying ξ_s -secrecy requirement. Hence, we consider the following problem

$$\begin{aligned}\max_{R_0, R_s} \quad & \eta(R_0, R_s) \\ \text{s.t.} \quad & P_s \leq \xi_s. \end{aligned}\quad (5.26)$$

The optimization problem Eq. (5.26) imposes a probabilistic service requirement in terms of confidentiality; that is, the service quality is acceptable as long as the probability of the secrecy outage is less than ξ_s , a parameter indicating the outage tolerance of the application. Note that P_s is a decreasing function of R_s , and η is linearly proportional to R_s . Hence, we can solve the optimization problem Eq. (5.26) in the following two steps: first, for given M , R_0 , and ξ_s , we find the maximum value $R_s^*(R_0)$; next, we obtain the optimum R_0^* , which maximizes the secrecy throughput $\eta(R_0, R_s^*(R_0))$.

5.5.2 Throughput with Both Secrecy and Reliability Requirements

On the other hand, reliability is another important quality of service parameter. To achieve both the connection outage target ξ_e and the secrecy outage target ξ_s , we consider the following problem

$$\begin{aligned}\max_{R_0, R_s} \quad & \eta(R_0, R_s) \\ \text{s.t.} \quad & P_s \leq \xi_s, \quad P_e \leq \xi_e. \end{aligned}\quad (5.27)$$

In addition to the service requirement of confidentiality, problem Eq. (5.27) also imposes a probabilistic service requirement on the connection outage, i.e., at least a fraction $1 - \xi_s$ of HARQ sessions are successful. The connection outage constraint ensures that, at the expense of possibly lower average throughput, the delay constraint (that a packet can be delivered within M transmissions) is satisfied $1 - \xi_s$ of the time, hence enabling applications which trade average rate for decoding delay like voice communication systems, e.g., CDMA2000 [26]. A similar constraint has been considered in [27] in terms of *service outage* for parallel fading channels.

To evaluate $p[m]$, P_e , and P_s , we need the cumulative distribution functions (CDFs) of $I_{XY}(m)$ and $I_{XZ}(m)$. For the RTD scheme, we can use the fact that $\sum_{i=1}^m \lambda_i$ and $\sum_{i=1}^m v_i$ are Gamma distributed to express the CDFs of $I_{XY}^{[\text{RTD}]}(m)$ and $I_{XZ}^{[\text{RTD}]}(m)$ in terms of incomplete Gamma functions. In the case of the INR scheme, the distributions of $I_{XY}^{[\text{INR}]}(m)$ and $I_{XZ}^{[\text{INR}]}(m)$ cannot be written in a closed form. Hence, we resort to Monte-Carlo simulation in order to obtain empirical CDFs. Note that Monte Carlo simulation is needed only to estimate empirical CDFs, while (R_0^*, R_s^*) is found numerically by a (non-random) search.

5.6 Asymptotic Analysis

In general, the secrecy throughput of the INR scheme is difficult to calculate since there is no closed form available for $\Pr\{I_{XY}(m) < R_0\}$. In this section, we consider the asymptotic secrecy throughput, which does have a closed form.

We are interested in asymptotic results as M increases without bound. Note that this asymptote corresponds to a delay-unconstrained system. In this case, secure HARQ schemes yield zero packet loss probability, i.e., the transmission of a code-word ends only when it is correctly decoded. As a result, the problems Eq. (5.26) and Eq. (5.27) yield the same throughput, which can be obtained from Eq. (5.24) as follows:

$$\eta(R_0, R_s) = \frac{MR_s}{\mathbb{E}[\mathcal{M}]} = \frac{MR_s}{1 + \sum_{m=1}^M \Pr\{I_{XY}(m) < R_0\}}. \quad (5.28)$$

Let us consider how to choose a mother Wyner code for the INR scheme in order to meet reliability and confidentiality constraints when M is large. Let λ and v denote the instantaneous SNRs at the legitimate receiver and the eavesdropper, respectively.

Lemma 2 Consider an INR secure HARQ scheme with the mother Wyner code $C \in \mathcal{C}(R_0, R_s, MN)$. Then

$$\lim_{M \rightarrow \infty} P_e^{[\text{INR}]} = 0 \quad \text{and} \quad \lim_{M \rightarrow \infty} P_s^{[\text{INR}]} = 0, \quad (5.29)$$

if and only if

$$\begin{aligned} R_0 &\leq \frac{1}{2} \mathbb{E}[\log_2(1 + \lambda)] \\ \text{and} \quad R_0 - R_s &\geq R_0 \frac{\mathbb{E}[\log_2(1 + v)]}{\mathbb{E}[\log_2(1 + \lambda)]}, \end{aligned} \quad (5.30)$$

where the expectations are over λ and/or v . Furthermore, if Eq. (5.30) does not hold, then

$$\text{either } \lim_{M \rightarrow \infty} P_e^{[\text{INR}]} = 1 \quad \text{or} \quad \lim_{M \rightarrow \infty} P_s^{[\text{INR}]} = 1. \quad (5.31)$$

For comparison, we consider the situation in which the Wyner code C is transmitted over M -block fading channel without using the HARQ scheme. We refer to this case as the M -fading-block (MFB) coding scheme. Theorem 1 implies that, by using the MFB scheme, the requirement Eq. (5.29) can be achieved if and only if

$$\begin{aligned} R_0 &\leq \frac{1}{2}\mathbb{E}[\log_2(1 + \lambda)] \\ \text{and } R_0 - R_s &\geq \frac{1}{2}\mathbb{E}[\log_2(1 + \nu)]. \end{aligned} \quad (5.32)$$

We note that the condition Eq. (5.30) for the INR scheme is weaker than the condition Eq. (5.32) for the MFB scheme. In other words, the INR scheme can achieve the confidentiality and reliability requirements more easily than can the MFB coding scheme by using the same Wyner code. This result illustrates the benefit of the INR secure HARQ scheme.

Based on Lemma 2, we have the following asymptotic result concerning the achievable throughput for secure HARQ schemes.

Theorem 3 *We consider the secure HARQ schemes over a block-fading wire-tap channel. If the secrecy information rate R_s satisfies*

$$\lim_{M \rightarrow \infty} \frac{1}{MR_s} = 0, \quad (5.33)$$

then the secrecy throughput of RTD and INR schemes can be written as follows:

$$\lim_{M \rightarrow \infty} \max_{R_0, R_s} \eta(R_0, R_s) = \begin{cases} 0 & \text{RTD} \\ \frac{1}{2}\mathbb{E}[\log_2(1 + \lambda) - \log_2(1 + \nu)] & \text{INR}, \end{cases}$$

where λ and ν are the instantaneous SNRs at the legitimate receiver and the eavesdropper, respectively.

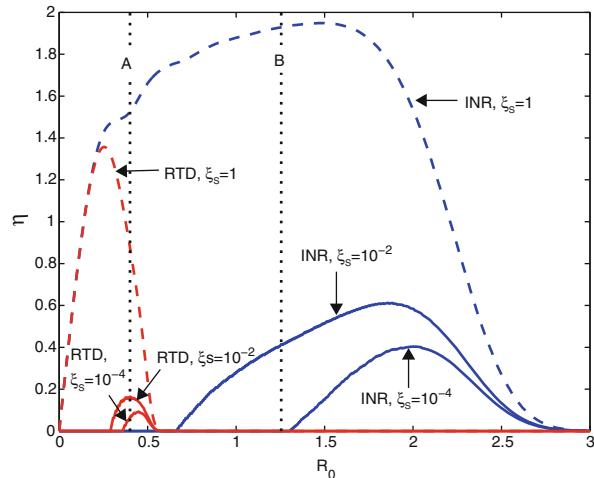
We note that the RTD scheme involves suboptimal coding schemes, for which $\mathbb{E}[\mathcal{M}]$ grows faster than MR_s in Eq. (5.28). Hence, the limiting secrecy throughput η is zero. Theorem 3 again asserts the benefit of INR over RTD.

5.7 Numerical Results

In our numerical examples, we consider Rayleigh block fading, i.e., the main channel instantaneous SNR λ has the probability density function (PDF) $f(\lambda) = (1/\bar{\lambda})e^{-\lambda/\bar{\lambda}}$, and the eavesdropper channel instantaneous SNR ν has the PDF $f(\nu) = (1/\bar{\nu})e^{-\nu/\bar{\nu}}$, where $\bar{\lambda}$ and $\bar{\nu}$ are the average SNRs of the main and eavesdropper channels, respectively.

To illustrate how the secrecy throughput η is related to the choice of R_0 (and R_s), we give a numerical example of η versus R_0 in Fig. 5.4, in which the parameter

Fig. 5.4 Secrecy throughput η versus the main channel code rate R_0 under different secrecy requirements ξ_s , where the main channel average SNR is 15 dB, the eavesdropper channel average SNR is 5 dB, and the maximum number of transmissions is $M = 8$ (©IEEE 2009)



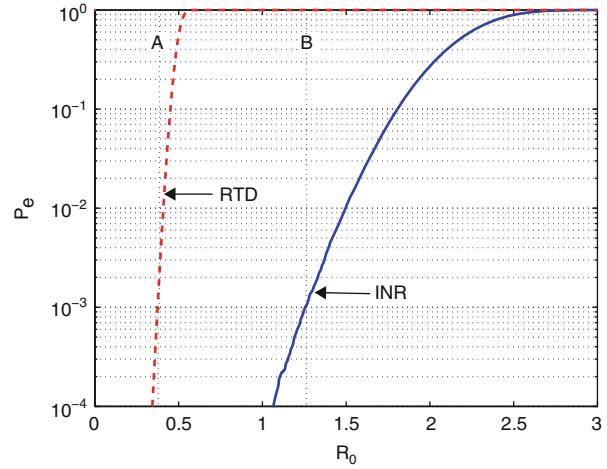
settings are as follows: the main channel average SNR $\bar{\lambda}$ is 15 dB, the eavesdropper channel average SNR \bar{v} is 5 dB, the maximum number of transmissions M is 8. (We observe that similar results are obtained by using other parameter settings.) For each R_0 , we obtain the maximum $R_s^*(R_0)$ that meets the secrecy constraint $\xi_s = 1, 10^{-2}$ or 10^{-4} , respectively. When there is no secrecy constraint ($\xi_s = 1$), due to the sub-optimality of the RTD scheme, the RTD curve is uniformly below the INR curve. This does not happen when there is a secrecy constraint. The reason is that INR not only favors the information transmission to the intended receiver, but also benefits the eavesdropping by the eavesdropper. Hence, INR needs to sacrifice a larger portion of the main channel code rate than RTD in order to keep the eavesdropper ignorant of the confidential messages. This is reflected in Fig. 5.4 where a larger R_0 has to be chosen for INR (than RTD) in order to obtain a positive secrecy throughput.

It is clear from Fig. 5.4 that there exists a unique R_0^* (and therefore $R_s^*(R_0^*)$) which maximizes η for each parameter setting. For all secrecy constraints ($\xi_s = 1, 10^{-2}$ or 10^{-4}), if the best R_0^* and $R_s^*(R_0^*)$ are chosen for each scheme accordingly, INR yields higher secrecy throughput than RTD does, which shows the benefit of INR over RTD.

According to Eq. (5.21), the choice of R_0 decides the reliability performance. This is shown in Fig. 5.5, where we plot the connection outage probability P_e versus the value of R_0 . For both INR and RTD, P_e increases with the value of R_0 . Note that a more strict secrecy constraint requires a larger R_0^* (as shown in Fig. 5.4), which however causes the degradation of the reliability performance. We can see that there exists a tradeoff between secrecy and reliability.

Given a strict connection outage constraint $P_e < \xi_e$, the choice of R_0^* (and $R_s^*(R_0^*)$) might not be feasible. For instance, in order to obtain $P_e < 10^{-3}$, we need to choose $R_0^{[\text{RTD}]} \leq 0.38$ and $R_0^{[\text{INR}]} \leq 1.25$ (marked with ‘A’ and ‘B’ respectively in Figs. 5.4 and 5.5). Specifically, for a connection outage constraint $P_e < 10^{-3}$, R_0^* is not feasible for INR when $\xi_s = 10^{-2}$, and R_0^* is not feasible for both INR and RTD when

Fig. 5.5 Connection outage probability P_e versus the main channel code rate R_0 , where the main channel average SNR is 15 dB, the eavesdropper channel average SNR is 5 dB, and $M = 8$. (©IEEE 2009)



$\xi_s = 10^{-4}$ in Fig. 5.4. Note that for the case of $\xi_s = 10^{-4}$ (and $\xi_e = 10^{-3}$), positive secrecy throughput cannot be obtained for INR, but can be obtained for RTD. This implies that RTD might outperform INR, when we have strict secrecy and connection outage constraints. This is a surprising result in the view of the well-known HARQ performance when there is no secrecy constraint, where INR always outperforms RTD [1].

In Fig. 5.7a, b, we show the secrecy throughput η under different target secrecy outage probabilities ξ_s . There is no connection outage requirement in Fig. 5.7a. There is an additional connection outage requirement of $p_e \leq \xi_e = 10^{-3}$ in Fig. 5.7b. The parameter settings are $\bar{\lambda} = 15$ dB, $\bar{v} = 5$ dB and $M = 8$. We can see that small

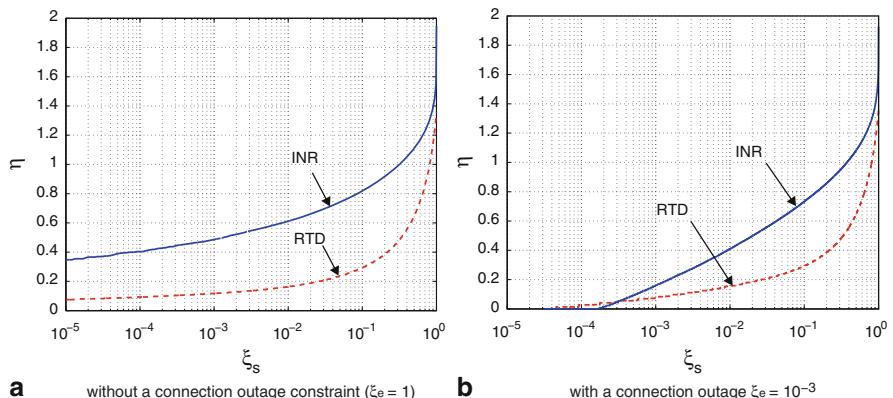
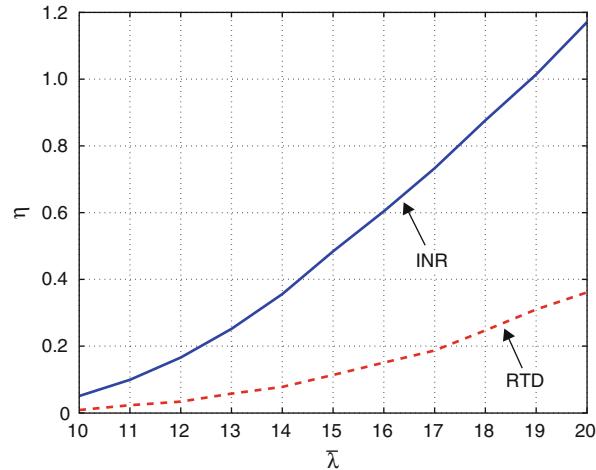


Fig. 5.6 Throughput η versus target secrecy outage probability ξ_s , when the main channel average SNR is 15 dB, the eavesdropper channel average SNR is 5 dB, and $M = 8$ (©IEEE 2009)

Fig. 5.7 Throughput η versus main channel average SNR $\bar{\lambda}$ under a target secrecy outage probability $\xi_s = 10^{-3}$, when the eavesdropper channel average SNR is 5 dB and $M = 8$

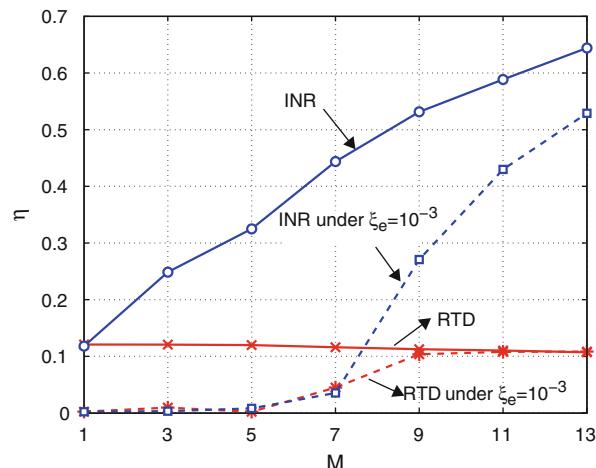


secrecy outage probability can be achieved when the throughput is small for both schemes. The INR scheme outperforms the RTD scheme uniformly when there is no connection outage requirement. However, when there is a strict connection outage requirement, the RTD scheme outperforms the INR scheme when ξ_s is small (e.g., $\xi_s \leq 10^{-4}$).

Figure 5.7 illustrates the relationship between the secrecy throughput η and the main channel average SNR $\bar{\lambda}$ when there is a target secrecy outage probability $\xi_s = 10^{-3}$ and no connection outage requirement. The average SNR of the eavesdropper channel is fixed to be 5 dB. We find that the INR scheme outperforms the RTD scheme significantly, especially when the main channel SNR is large.

In Fig. 5.8, we give the secrecy throughput η versus the maximum number of transmissions M . Comparing with the secrecy throughput without the connection outage

Fig. 5.8 Throughput η versus the maximum number of transmissions M under a target secrecy outage probability $\xi_s = 10^{-3}$, when the main and eavesdropper channel average SNRs are 15 dB and 5 dB, respectively
©IEEE 2009)



constraint, the secrecy throughput with a connection outage constraint ($P_e \leq 10^{-3}$) suffers some loss when M is small due to insufficient diversity. Both secrecy throughputs converge when sufficient diversity can be obtained as M increases. In particular, when $M \rightarrow \infty$, both throughputs are the same and are given by Eq. (5.28) in the asymptotic analysis. For INR, the secrecy throughput $\eta^{[\text{INR}]}$ increases monotonically with M . For RTD, $\eta^{[\text{RTD}]}$ decreases with M due to its strongly suboptimal coding scheme. This concurs with the asymptotic analysis that, when $M \rightarrow \infty$, a constant (nonzero) secrecy throughput $(0.5 * \mathbb{E}[\log_2(1 + \lambda) - \log_2(1 + \nu)] = 1.31$ according to Theorem 3) can be achieved for INR, while zero throughput can be obtained for RTD.

5.8 Conclusions

We have studied secure packet communications over frequency-flat block-fading Gaussian channels based on secure HARQ schemes with the joint consideration of channel coding, secrecy coding and retransmission protocols. From an information theoretic point of view, we have considered two secure HARQ schemes: a repetition time diversity scheme with maximum ratio combining (RTD), and an incremental redundancy scheme based on rate-compatible Wyner secrecy codes (INR). We have proved the existence of good Wyner code sequences, which ensure that the legitimate receiver can decode the message and the eavesdropper can be kept ignorant of it under a set of certain channel realizations of an HARQ session.

To facilitate the formulation of the outage-based throughput, we have defined two types of outage: connection outage and secrecy outage. The connection and secrecy outage probabilities have been used to characterize the tradeoff between the reliability of the legitimate communication link and the confidentiality with respect to the eavesdropper's link. We have evaluated the achievable throughput of RTD and INR schemes under probabilistic requirements (constraints) on secrecy and/or connection outage, and have illustrated the benefits of HARQ schemes to information secrecy through some numerical results and an asymptotic analysis.

In general, INR can achieve a significantly larger throughput than RTD, which concurs with the results not involving secrecy that mutual-information accumulation (INR) is a more effective approach than SNR-accumulation (RTD). However, when one is forced to ensure small connection outage for the main channel even when it is bad, one is forced to reduce the main channel code rate. The INR scheme, having a larger coding gain (to both the intended receiver and the eavesdropper), needs to sacrifice a larger portion of the main channel code rate (i.e., requires a larger secrecy gap) in order to satisfy the secrecy requirement. Hence when the main channel code rate is bounded due to the connection outage constraint, the achievable secrecy throughput of INR may be smaller than that of RTD.

We conclude this work by pointing out some future research directions.

First, as pointed out in [28], many practical encoders are separated from the modulator and, therefore, the performance of HARQ schemes is impacted by modulation

constraints. Although we have assumed Gaussian signaling, it is possible and also meaningful to extend the analysis to take discrete signaling into account.

In our analysis, we have assumed random coding and typical set decoding. Future work should consider practical coding and decoding schemes for secure HARQ schemes. Existing work on the practical secrecy code design includes coset coding [29], low-density parity check (LDPC) code design [30], and nested codes [31]. The design of practical rate compatible secrecy codes for Gaussian channels remains a challenging problem.

References

- [1] G. Caire and D. Tuninetti, "The throughput of hybrid-ARQ protocols for the Gaussian collision channel," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, July 2001.
- [2] J. Hagenauer, "Rate-compatible punctured convolutional codes (RCPC codes) and their applications," *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 389–400, Apr. 1988.
- [3] K. R. Narayanan and G. L. Stuber, "A novel ARQ technique using the turbo coding principle," *IEEE Commun. Lett.*, vol. 1, no. 2, pp. 49–51, Mar. 1997.
- [4] D. Tuninetti and G. Caire, "The throughput of some wireless multiaccess systems," *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 2773–2785, Oct. 2002.
- [5] E. Soljanin, R. Liu, and P. Spasojević, "Hybrid ARQ with random transmission assignments," in *Adv. Netw. Inf. Theory*, ser. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, P. Gupta, G. Kramer, and A. J. van Wijngaarden, Eds. Providence, RI: American Mathematical Society, pp. 321–334, 2004.
- [6] S. Sesia, G. Caire, and G. Vivier, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," *IEEE Trans. Commun.*, vol. 52, no. 8, pp. 1311–1321, Aug. 2004.
- [7] C. F. Leanderson and G. Caire, "The performance of incremental redundancy schemes based on convolutional codes in the block-fading Gaussian collision channel," *IEEE Trans. Wireless Commun.*, vol. 3, no. 3, pp. 843–854, May 2004.
- [8] E. Soljanin, N. Varnica, and P. Whiting, "Incremental redundancy hybrid ARQ with LDPC and raptor code," *IEEE Trans. Inf. Theory*, submitted, Sept. 2005.
- [9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [10] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [11] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.
- [12] Y. Liang and H. V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.
- [13] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, pp. 957–961, July 2006.
- [14] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, pp. 1164–1168, July 2006.
- [15] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.
- [16] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, pp. 356–360, July 2006.

- [17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.
- [18] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. on Commun., Control, Comput.*, Monticello, IL, Sep. 2006.
- [19] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels", *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
- [20] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.
- [21] S. Shamai, L. Ozarow, and A. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994.
- [22] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretic and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 1895–1911, Oct. 1998.
- [23] H. Holma and A. Toskala, *WCDMA for UMTS*, 2nd ed. New York: Wiley, 2002.
- [24] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [25] M. Zorzi and R. R. Rao, "On the use of renewal theory in the analysis of ARQ protocols," *IEEE Trans. Commun.*, vol. 44, no. 9, pp. 1077–1081, Sep. 1996.
- [26] *Physical Layer Standard for CDMA2000 Spread Spectrum Systems (Revision C)*, 3GPP2 Std. C.S0002-C, 2004.
- [27] J. Luo, R. Yates, and P. Spasojevic, "Service outage based power and rate allocation for parallel fading channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2594–2611, July 2005.
- [28] T. Ghanim and M. Valenti, "The throughput of hybrid-ARQ in block fading under modulation constraints," in *Proc. IEEE Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 2006.
- [29] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.
- [30] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.
- [31] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," in *Proceedings IEEE Information Theory Workshop on Frontiers in Coding Theory*, Lake Tahoe, CA, Sep. 2–6, 2007.
- [32] Y. Liang, H. V. Poor, and S. Shamai, "Information Theoretic Security." in *Found. Trends Communi. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2008.

Chapter 6

Secret Communication Under Channel Uncertainty*

Yingbin Liang, H. Vincent Poor and Shlomo Shamai (Shitz)

6.1 Introduction

A basic measure of secrecy for communications was provided by Shannon via the information theoretic entropy rate in [1]. Based on this measure, secure communication over noisy communication channels was studied by Wyner within the wire-tap channel model in [2]. In this channel, a transmitter exploits the difference between the channel randomness to its legitimate receiver and to an eavesdropper, and employs a stochastic encoding scheme to benefit the legitimate receiver while guaranteeing no information leakage to the eavesdropper. Compared to the prevalent cryptographic approaches to achieve secure communication, such an information theoretic approach does not need “keys” to encrypt and decrypt the source messages.

Alternatively, information theory also provides approaches to achieve *secret key agreement* for remote terminals by exploiting source and/or channel randomness available at these terminals. Such a common secret key can hence be used for secure communication via cryptographic secret-key algorithms. In this case, information theory helps key management (including key generation and distribution). We refer the reader to [3–19] and references therein for this topic, whereas the focus of this chapter is on the wire-tap channel.

Compared to contemporary cryptosystems, the information theoretic approaches to guarantee security have the advantages of either eliminating the key management issue entirely or exploiting powerful coding techniques in the physical layer to achieve key agreement, thereby resulting in significantly lower complexity and savings in resources. Furthermore, physical layer security approaches achieve provable

Y. Liang (✉)

Department of Electrical Engineering
University of Hawaii, Honolulu
HI 96822, USA
e-mail: yingbinl@hawaii.edu

*Portions of the material have appeared previously in “Secure communication over fading channels,” IEEE Transactions on Information Theory, vol. 54, no. 6, 2008 ©IEEE 2008; and “Recent results on compound wire-tap channels.”, Proceedings of the Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008 ©IEEE 2008.

security that is robust to eavesdroppers possessing unlimited computational resources, knowledge of the communication strategy employed including coding and decoding algorithms, and access to communication systems either through perfect or noisy channels.

The recent emergence and increasing ubiquity of wireless networks, and in particular of networks with minimal infrastructure, have spurred considerable interest in the information theoretic security in very recent times (see, e.g., [20–58] and the reference therein). In particular, the promise of this potentially very powerful approach for use in mobile and other wireless networks has been brought to the attention of the wireless networking community. However, to fully exploit information theoretic security in wireless networks, one major challenge is to design secure communication strategies for the time-varying channel, which is an important intrinsic characteristic of wireless communications. This chapter focuses on this topic.

A number of models can be used to describe various wireless communication scenarios. One common property of these models is that the channel may take multiple states, while channel state information (CSI) may or may not be available at the transmitter, the receiver, or the eavesdropper. The parallel wire-tap channel and the ergodic fading wire-tap channel are models that capture the situation in which there are no delay constraints. Alternatively, the block fading wire-tap channel is useful for studying outage performance when there are delay constraints. The compound wire-tap channel assumes that the channels to the legitimate receiver and to the eavesdropper take a number of states, and secure communication must be guaranteed no matter which state occurs. The compound channel does not allow coding across different states, and guarantees robust performance under delay constraints. To draw the connection between robustness and outage performance, robustness requires zero-outage probability. Another useful model is the wire-tap channel with side information which models the situation in which the channel state is non-causally known at the transmitter only, and this information helps improve the secrecy performance. This chapter reviews recent progress on characterizing the secrecy of these channel models, and discusses some interesting open problems in this area.

6.2 Wire-Tap Channel Model

In this section, we introduce the wire-tap channel model, and review results on the secrecy capacity of this channel. We will further discuss the Gaussian, the multi-input multi-output (MIMO), and the parallel wire-tap channels, which serve as basic information-theoretic models for the fading wire-tap channel.

6.2.1 Discrete Memoryless Wire-Tap Channel

The wire-tap channel was first introduced and studied by Wyner in [2]. This channel includes a transmitter that wishes to transmit a source sequence (a message W) to a legitimate receiver and wishes to keep this message as secret as possible from an

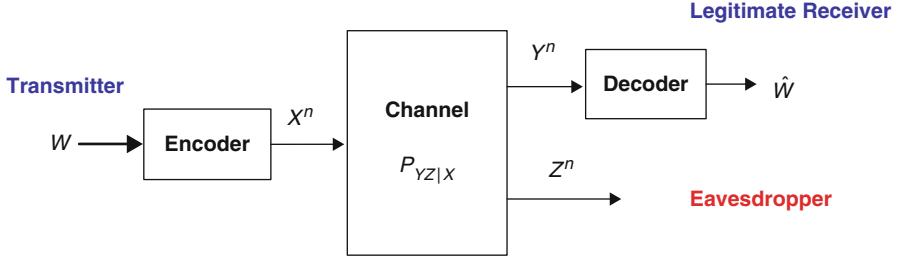


Fig. 6.1 The wire-tap channel

eavesdropper. An illustration of the wire-tap channel is depicted in Fig. 6.1. The wire-tap channel is formally defined as follows.

Definition 1 The wire-tap channel consists of one finite input alphabet \mathcal{X} and two finite output alphabets \mathcal{Y} and \mathcal{Z} . The channel transition probability is characterized by $P_{YZ|X}(y, z|x)$, where $x \in \mathcal{X}$, $y \in \mathcal{Y}$ and $z \in \mathcal{Z}$.

Definition 2 A $(2^{nR}, n)$ code for the wire-tap channel consists of the following:

- One message set: $\mathcal{W} = \{1, 2, \dots, 2^{nR}\}$ with the message W uniformly distributed over \mathcal{W} ;
- One (stochastic) encoder $f: \mathcal{W} \rightarrow \mathcal{X}^n$, which maps each message $w \in \mathcal{W}$ to a codeword x^n ;
- One decoder $g: \mathcal{Y}^n \rightarrow \mathcal{W}$, which maps a received sequence y^n to a message $w \in \mathcal{W}$

where x^n denotes the sequence (x_1, \dots, x_n) .

We note that the wire-tap channel described above generalizes the model studied in [2] in that the broadcast channel characterized by $P_{YZ|X}$ is assumed to be general, not necessarily degraded as assumed in [2], i.e., the channel output at the eavesdropper may not be a degraded version of the channel output at the receiver. This more general model was studied by Csiszár and Körner in [59] as a special case of the broadcast channel with confidential messages.

The communication reliability is measured by the average block probability of error for a length n code, defined as

$$P_e^{(n)} = \Pr \left\{ \hat{W} \neq W \right\} = \frac{1}{|\mathcal{W}|} \sum_{w=1}^{|\mathcal{W}|} \Pr \left\{ \hat{w} \neq w \right\}, \quad (6.1)$$

where \hat{w} denotes the decision made by the legitimate receiver if the source message w is sent over the channel. The communication security represented by the secrecy level of the message W at the eavesdropper is measured by the *equivocation rate* defined as

$$R_e^{(n)} = \frac{1}{n} H(W|Z^n). \quad (6.2)$$

The equivocation rate indicates the eavesdropper's uncertainty about the message W given the information available at the eavesdropper. Hence the larger the equivocation rate, the higher the level of secrecy.

In this chapter, we focus on the case of perfect secrecy, i.e., the message W is perfectly hidden from the eavesdropper. A rate R is *achievable with perfect secrecy* if there exists a sequence of message sets \mathcal{W}_n with $|\mathcal{W}_n| = 2^{nR}$ and encoder-decoder pairs (f_n, g_n) such that the average error probability $P_e^{(n)} \rightarrow 0$ as n goes to infinity and

$$R \leq \liminf_{n \rightarrow \infty} R_e^{(n)}. \quad (6.3)$$

The *secrecy capacity* C_s is the largest achievable rate with perfect secrecy. We note that perfect secrecy does not imply that each information bit is kept secret, but guarantees that the unsecured information cannot have a positive rate.

The secrecy capacity for the wire-tap channel is characterized by Csiszár and Körner in [59], and is given in the following theorem.

Theorem 1 ([59]) *The secrecy capacity of the wire-tap channel is given by*

$$C_s = \max_{P_{UX} P_{YZ|X}} [I(U; Y) - I(U; Z)], \quad (6.4)$$

where the maximization is taken over all jointly distributed P_{UX} between the channel input X and an auxiliary random variable U satisfying the Markov chain condition $U \rightarrow X \rightarrow (Y, Z)$.

To achieve the above secrecy capacity, the transmitter first maps the source message W into an auxiliary random sequence U^n . It then maps U^n into the channel input sequence X^n according to the transition probability $P_{X|U}$. Equivalently, the transmitter creates a *prefix channel* from the auxiliary random variable U to the actual channel input X . Hence, the equivalent channel from the transmitter to the legitimate receiver and the eavesdropper becomes $P_{YZ|U}$. The above secrecy capacity is characterized by the difference between the rate at which the legitimate receiver can decode, i.e., $I(U; Y)$, and the rate at which the eavesdropper can decode, i.e., $I(U; Z)$. We note that with the prefix channel, the legitimate receiver is able to determine the auxiliary sequence U^n , but cannot in general determine the channel input sequence X^n .

We define the wire-tap channel to be *physically degraded* if the channel transition probability satisfies $P_{YZ|X}(\cdot) = P_{Y|X}(\cdot)P_{Z|Y}(\cdot)$, i.e., X, Y and Z form a Markov chain $X \rightarrow Y \rightarrow Z$. We define the wire-tap channel to be *stochastically degraded* if its conditional marginal distribution is the same as that of a physically degraded wire-tap channel, i.e., there exists a distribution $P_{Z|Y}(\cdot)$ such that

$$P_{Z|X}(z|x) = \sum_y P_{Z|Y}(z|y)P_{Y|X}(y|x). \quad (6.5)$$

The degraded wire-tap channel was studied by Wyner in [2].

As the secrecy capacity of the wire-tap channel is not affected by the correlation between the channel outputs at the receiver and the eavesdropper [59], the secrecy

capacity of the physically and stochastically degraded wire-tap channels are the same and is given in the following theorem.

Lemma 1 ([2]) *The secrecy capacity of the (physically/stochastically) degraded wire-tap channel is given by*

$$C_s = \max_{P_X P_Y Z|X} [I(X; Y) - I(X; Z)]. \quad (6.6)$$

Proof The achievability follows from Theorem 1 by setting $U = X$. To show the converse, it is easy to see that

$$\begin{aligned} I(U; Y) - I(U; Z) &= I(UX; Y) - I(X; Y|U) - I(UX; Z) + I(X; Z|U) \\ &\leq I(X; Y) - I(X; Z) \end{aligned} \quad (6.7)$$

where the last inequality follows from the degradedness condition. \square

For the degraded wire-tap channel, it is clear that coding without a prefix channel is optimal.

6.2.2 Gaussian and MIMO Wire-Tap Channels

The Gaussian wire-tap channel was studied in [60]. In this channel, the outputs at the legitimate receiver and at the eavesdropper are corrupted by additive white Gaussian noises. The channel input-output relationship for one channel use is given by

$$\begin{aligned} Y &= X + V_R \\ Z &= X + V_E \end{aligned} \quad (6.8)$$

where V_R and V_E are independent zero-mean Gaussian random variables with variances μ^2 and ν^2 . The channel input is subject to an average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [X_i^2] \leq P. \quad (6.9)$$

where i is the symbol time index.

Theorem 2 ([60]) *The secrecy capacity of the Gaussian wire-tap channel is given by*

$$C_s = \left[\frac{1}{2} \log \left(1 + \frac{P}{\mu^2} \right) - \frac{1}{2} \log \left(1 + \frac{P}{\nu^2} \right) \right]^+ \quad (6.10)$$

where $[x]^+$ equals x if $x \geq 0$ and equals zero if $x < 0$.

Proof The achievability follows from Theorem 1 by setting $U = X \sim \mathcal{N}(0, P)$, where $\mathcal{N}(0, P)$ denotes a Gaussian random variable with zero mean and variance P . The converse uses the entropy power inequality and the details can be found in [60]. \square

We further consider the multiple-input multiple-output (MIMO) wire-tap channel, in which there are N_T , N_R , and N_E antennas at the transmitter, the legitimate receiver, and the eavesdropper, respectively. The channel input-output relationship for one channel use in this case is given by

$$\begin{aligned}\underline{Y} &= H\underline{X} + \underline{V}_R \\ \underline{Z} &= G\underline{X} + \underline{V}_E\end{aligned}\tag{6.11}$$

where \underline{X} is the channel input vector with N_T components, \underline{Y} is the channel output vector at the legitimate receiver with N_R components, and \underline{Z} is the channel output vector at the eavesdropper with N_E components. The channel matrices H and G are fixed $N_R \times N_T$ and $N_E \times N_T$ matrices, respectively. The noise vectors \underline{V}_R and \underline{V}_E consist of independent and identically distributed (i.i.d.) Gaussian components with zero means and identity variances. The channel input is subject to an average power constraint

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\underline{X}_i^T \underline{X}_i] \leq P\tag{6.12}$$

where i is the symbol time index, and \underline{X}_i^T denotes the transpose of the vector \underline{X}_i .

The secrecy capacity of the MIMO wire-tap channel was established in [61, 62]. The secrecy capacity of a special case of this channel, in which the transmitter and the receiver have two antennas and the eavesdropper has one antenna was given in [63].

Theorem 3 ([61, 62]) *The secrecy capacity of the MIMO wire-tap channel is given by*

$$C = \max_{Q: Q \geq 0, \text{Tr}(Q) \leq P} \frac{1}{2} \log \frac{|I + HQH^T|}{|I + GQG^T|}\tag{6.13}$$

where $\text{Tr}(\cdot)$ denotes the trace of a matrix, and $(\cdot)^T$ denotes the transpose of a matrix.

Proof (outline of the main idea) The achievability follows from Theorem 1 by setting $U = X \sim \mathcal{N}(0, Q)$, where $\mathcal{N}(0, Q)$ denotes a Gaussian random vector (in this case, N_T dimensional) with zero mean and covariance matrix Q . The upper bound is based on the Sato-type upper bound [64] by considering an enhanced wire-tap channel, in which the receiver also knows the output at the eavesdropper. It is clear that the enhanced wire-tap channel is degraded and its secrecy capacity provides an upper bound on the secrecy capacity of the original MIMO wire-tap channel. Since the secrecy capacity depends only on the conditional marginal distributions $P_{\underline{Y}|\underline{X}}$ and $P_{\underline{Z}|\underline{X}}$, the enhanced channel may have arbitrarily correlated noise vectors and still provides an upper bound. The tightest upper bound is obtained by the correlation between the noise vectors that results in the worst secrecy capacity. The main converse proof is to characterize this worst-case upper bound and show that it matches the achievable rate. We refer the reader to [61, 62] for details. \square

We note that an alternative converse proof was provided in [65], which is based on the channel enhancement idea proposed in [66] for the MIMO broadcast channel and an extremal entropy inequality proved in [67, 68].

6.2.3 Parallel Wire-Tap Channel

We now consider the parallel wire-tap channel (see Fig. 6.2), in which the broadcast channel from the transmitter to the receiver and the eavesdropper consists of L independent subchannels. More formally, the parallel wire-tap channel consists of L finite input alphabets $\mathcal{X}_1, \dots, \mathcal{X}_L$, and $2L$ finite output alphabets $\mathcal{Y}_1, \dots, \mathcal{Y}_L$ and $\mathcal{Z}_1, \dots, \mathcal{Z}_L$. The transition probability distribution is given by

$$P_{Y_1 \dots Y_L Z_1 \dots Z_L | X_1 \dots X_L} = \prod_{l=1}^L P_{Y_l Z_l | X_l}(y_l, z_l | x_l) \quad (6.14)$$

where $x_l \in \mathcal{X}_l$, $y_l \in \mathcal{Y}_l$, and $z_l \in \mathcal{Z}_l$ for $l = 1, \dots, L$. If the parallel wire-tap channel has only one subchannel, i.e., $L = 1$, this channel becomes the wire-tap channel studied in Sect. 6.2.1.

The parallel wire-tap channel serves as an information-theoretic model for the fading wire-tap channel, in which the channel changes from one state to another, with each channel state corresponding to one subchannel. The parallel wire-tap channel was studied in [69, 70]. A more general model, the parallel broadcast channel with confidential messages was studied in [42], in which the transmitter also has a common message for both the receiver and the eavesdropper in addition to the confidential message for the receiver only.

Theorem 4 ([42, 69, 70]) *The secrecy capacity of the parallel wire-tap channel is given by*

$$C_s = \sum_{l=1}^L \max_{P_{U_l X_l} P_{Y_l Z_l | X_l}} \left[I(U_l; Y_l) - I(U_l; Z_l) \right], \quad (6.15)$$

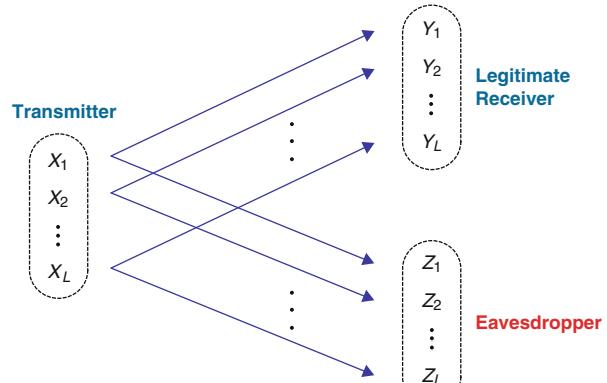


Fig. 6.2 The parallel wire-tap channel

where the maximization for each term in the summation is taken over all jointly distributed $P_{U_l X_l}$ between the channel input X_l to subchannel l and an auxiliary random variable U_l satisfying the Markov chain condition $U_l \rightarrow X_l \rightarrow (Y_l, Z_l)$.

Proof Achievability follows from Theorem 1 by setting $U = (U_1, \dots, U_L)$, $X = (X_1, \dots, X_L)$, $Y = (Y_1, \dots, Y_L)$, and $Z = (Z_1, \dots, Z_L)$ with U and X having independent components. Furthermore, we choose the components of these random vectors to satisfy the Markov chain conditions: $U_l \rightarrow X_l \rightarrow (Y_l, Z_l)$ for $l = 1, 2, \dots, L$. The converse can be found in [69, 70]. \square

We note that Theorem 4 implies that having independent inputs for each subchannel is optimal, and the secrecy capacity of the parallel wire-tap channel equals the summation of the secrecy capacities of the individual subchannels.

We now consider the *parallel wire-tap channel with degraded subchannels*, where each subchannel is either degraded such that the output at the eavesdropper is a degraded version of the output at the receiver, or degraded such that the output at the receiver is a degraded version of the output at the eavesdropper. Note that although each subchannel is degraded, the entire channel may not be degraded because the subchannels may not be degraded in the same fashion.

We define the index set A to include all indices of subchannels for which the output at the eavesdropper is a degraded version of the output at the receiver, i.e.,

$$P_{Y_l Z_l | X_l} = P_{Y_l | X_l} P_{Z_l | Y_l} \quad \text{for } l \in A. \quad (6.16)$$

Hence the Markov chain condition $X_l \rightarrow Y_l \rightarrow Z_l$ is satisfied for $l \in A$. We define A^c to be the complement of the set A , and hence A^c includes all indices of subchannels for which the output at the receiver is a degraded version of the output at the eavesdropper, i.e.,

$$P_{Y_l Z_l | X_l} = P_{Z_l | X_l} P_{Y_l | Z_l} \quad \text{for } l \in A^c. \quad (6.17)$$

Hence the Markov chain condition $X_l \rightarrow Z_l \rightarrow Y_l$ is satisfied for $l \in A^c$.

For the parallel wire-tap channel with degraded subchannels, we apply Theorem 4 and obtain the following secrecy capacity.

Corollary 2 *The secrecy capacity of the parallel wire-tap channel with degraded subchannels is given by*

$$C_s = \sum_{l \in A} \max_{P_{X_l}} \left[I(X_l; Y_l) - I(X_l; Z_l) \right]. \quad (6.18)$$

We next consider the parallel Gaussian wire-tap channel, in which the channel outputs at the receiver and the eavesdropper are corrupted by additive white Gaussian noise terms. The channel input–output relationship for one channel use is given by

$$Y_l = X_l + V_{Rl}, \quad Z_l = X_l + V_{El}, \quad \text{for } l = 1, \dots, L, \quad (6.19)$$

where, for $l = 1, \dots, L$, V_{Rl} and V_{El} are zero mean Gaussian random variables with variances μ_l^2 and ν_l^2 , respectively. We have $\mu_l^2 < \nu_l^2$ for $l \in A$ and $\mu_l^2 \geq \nu_l^2$ for $l \in A^c$. The channel input is subject to the average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \sum_{l=1}^L \mathbb{E}[X_{li}^2] \leq P \quad (6.20)$$

where i is the time index.

Theorem 5 ([42, 69, 70]) *The secrecy capacity of the parallel Gaussian wire-tap channel is given by*

$$C_s = \max_{\substack{p_1, \dots, p_L \geq 0 \\ p_1 + \dots + p_L \leq P}} \sum_{l \in A} \left[\frac{1}{2} \log \left(1 + \frac{p_l}{\mu_l^2} \right) - \frac{1}{2} \log \left(1 + \frac{p_l}{\nu_l^2} \right) \right] \quad (6.21)$$

where p_1, \dots, p_L denote the powers allocated to the subchannels.

6.3 Fading Wire-Tap Channel

In this section, we give an overview of results for fading wire-tap channels. We will discuss both the ergodic performance without a delay constraint and the outage performance with a delay constraint.

6.3.1 Ergodic Performance with Full CSI

We consider the fading wire-tap channel, in which the channels from the transmitter to the receiver and the eavesdropper are corrupted by multiplicative fading processes in addition to the additive white Gaussian noise processes. The channel input-output relationship for one channel use is given by

$$Y = h_1 X + V_R \quad \text{and} \quad Z = h_2 X + V_E, \quad (6.22)$$

where the channel gain coefficients h_1 and h_2 are proper complex random variables. We define $\underline{h} := (h_1, h_2)$. If we let i denote the symbol time index, then $\{\underline{h}_i\}$ indicates a vector fading process across time, which is assumed to be stationary and ergodic. The noise processes $\{V_{Ri}\}$ and $\{V_{Ei}\}$ are zero-mean i.i.d. proper complex Gaussian with V_{Ri} and V_{Ei} having variances μ^2 and ν^2 , respectively. The channel input is subject to the average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[X_i^2] \leq P.$$

We assume that the full channel state information, i.e., the realization of \underline{h} is known at the transmitter, the receiver and the eavesdropper instantaneously. Based on this channel state information, the transmitter can dynamically change its transmission power to achieve better secrecy rate. We assume that there is no delay constraint on the transmitted messages, and the performance criterion we study, i.e., the secrecy capacity, is averaged over all channel states and is referred to as the *ergodic* secrecy capacity. In this scenario, the fading wire-tap channel can be viewed as the parallel Gaussian wire-tap channel with each fading state corresponding to one subchannel. Thus, the secrecy capacity of the fading wire-tap channel follows immediately from Theorem 5.

Corollary 3 ([42, 69, 70]) *The secrecy capacity of the fading wire-tap channel is*

$$C_s = \max_{\mathbb{E}_A[p(\underline{h})] \leq P} \mathbb{E}_A \left[\log \left(1 + \frac{p(\underline{h})|\underline{h}_1|^2}{\mu^2} \right) - \log \left(1 + \frac{p(\underline{h})|\underline{h}_2|^2}{\nu^2} \right) \right] \quad (6.23)$$

where the set $A := \left\{ \underline{h} : \frac{|\underline{h}_1|^2}{\mu^2} > \frac{|\underline{h}_2|^2}{\nu^2} \right\}$, and $p(\underline{h})$ denotes the transmission power allocated for the state \underline{h} .

The optimal power allocation that achieves the secrecy capacity in Eq. (6.23) is given by

$$p^*(\underline{h}) = \begin{cases} \left(\frac{1}{\lambda \ln 2} - \frac{\mu^2}{|\underline{h}_1|^2} \right)^+, & \text{if } |\underline{h}_2|^2 = 0; \\ \left(\frac{1}{2} \sqrt{\left(\frac{\nu^2}{|\underline{h}_2|^2} - \frac{\mu^2}{|\underline{h}_1|^2} \right)} \left(\frac{4}{\lambda \ln 2} - \frac{\mu^2}{|\underline{h}_1|^2} + \frac{\nu^2}{|\underline{h}_2|^2} \right) \right)^+, & \text{if } |\underline{h}_2|^2 > 0, \underline{h} \in A; \\ 0, & \text{otherwise} \end{cases} \quad (6.24)$$

where λ is chosen to satisfy the power constraint $\mathbb{E}_A[p(\underline{h})] = P$.

From the bound in Eq. (6.23), it can be seen that as long as the set A is not a zero probability event, positive secrecy rate can be achieved. That is, the channel from the transmitter to the receiver will be better than the channel to the eavesdropper for some channel states, and hence positive secrecy capacity can be achieved by exploiting these channel states.

The secrecy capacity given in Corollary 3 is established for fading processes where only ergodic and stationary conditions are assumed. The fading process can be correlated across time, and is not necessarily Gaussian. This result is also applicable to the cases in which the two component fading processes $\{\underline{h}_{1i}\}$ and $\{\underline{h}_{2i}\}$ are correlated and in which the noise variables V_R and V_E are correlated.

6.3.2 Ergodic Performance with Partial CSI

The CSI is important for the transmitter to design secure communication strategies. However, in many communication scenarios, the CSI of the channel to the eavesdropper is not available to the transmitter. Such a scenario is studied in [71] for the slow fading wire-tap channel. The channel input-output relationship is the same as that given in Eq. (6.22), but the channel state is assumed to be constant over a block and changes independently to another realization in the next block. The blocklength is large enough for the receiver to successfully decode. The CSI is assumed to be known at the corresponding receiver, and only the CSI of the channel to the legitimate receiver is known at the transmitter.

Theorem 6 ([71]) *For the slow fading wiretap channel described in the above, the secrecy capacity is given by*

$$C_s = \max_{\mathbb{E}_A[p(h_1)] \leq P} \mathbb{E}_A \left[\log \left(1 + \frac{p(h_1)|h_1|^2}{\mu^2} \right) - \log \left(1 + \frac{p(h_1)|h_2|^2}{\nu^2} \right) \right]. \quad (6.25)$$

Comparing this result with the secrecy capacity given in Corollary 3 for the case of full CSI at the transmitter, the power allocation $p(h_1)$ in the preceding theorem is a function of only the channel state to the legitimate receiver, because only this information is available at the transmitter for the partial CSI case. The conditions to determine an optimal power allocation for this case were given in [71].

To achieve the secrecy capacity given in Theorem 6, a variable rate transmission scheme was proposed in [71]. During a coherence interval (one block) in which the channel state to the legitimate receiver is h_1 , the transmitter uses a codebook at rate $\log \left(1 + \frac{p(h_1)|h_1|^2}{\mu^2} \right)$ with the transmission power $p(h_1)$. Hence, the average rate to the receiver over a large number of blocks is given by

$$\mathbb{E} \left[\log \left(1 + \frac{p(h_1)|h_1|^2}{\mu^2} \right) \right], \quad (6.26)$$

and the average rate to the eavesdropper is given by

$$\mathbb{E} \left[\log \left(1 + \frac{p(h_1)\min\{|h_1|^2, |h_2|^2\}}{\nu^2} \right) \right] \quad (6.27)$$

where $\min\{|h_1|^2, |h_2|^2\}$ appears because the codebooks chosen for different blocks are independent, and for the states when $\underline{h} \in A^c$, the rate to the eavesdropper is limited by the rate to the legitimate receiver. The difference of the preceding two rates is thus the expectation over only the set A . The details of the proof can be found in [71].

6.3.3 Outage Performance

From Sects. 6.3.1 and 6.3.2, it is clear that to achieve the ergodic secrecy capacity for the fading wire-tap channel, messages should be allowed to be coded over a

large number of blocks and hence over all channel realizations. Such a scenario applies to systems in which transmission delay can be tolerated. In this subsection, we consider systems in which there is a stringent delay constraint, so that messages must be transmitted within a certain time.

As in Sect. 6.3.2, we consider the block fading wire-tap channel, in which the channel state $\underline{h} = (h_1, h_2)$ remains constant over one block and change to another realization in the next block in an ergodic and stationary manner. The block length is large enough such that coding over one block can achieve small probability of error. We assume that the delay constraint is within the block length so that coding over multiple blocks and hence over multiple channel state realizations is not allowed. We also assume that both the transmitter and the receivers know the channel state information.

We use \check{R} to denote a target secrecy rate, and an outage occurs if the target rate is not achieved. The outage probability is hence given by

$$P_{out} = \Pr\left\{C_s(\underline{h}, p(\underline{h})) \leq \check{R}\right\} \quad (6.28)$$

where $C_s(\underline{h}, p(\underline{h}))$ is the secrecy capacity for the channel with the channel state realization \underline{h} , and $p(\underline{h})$ indicates the transmission power used by the transmitter for this channel state.

For a given channel state \underline{h} , the secrecy capacity is given by

$$C_s = \left[\log\left(1 + \frac{p(\underline{h})|h_1|^2}{\mu^2}\right) - \log\left(1 + \frac{p(\underline{h})|h_2|^2}{v^2}\right) \right]^+. \quad (6.29)$$

If the transmission power is subject to the *short-term constraint*, i.e., $P(\underline{h}) \leq P$ for all \underline{h} , the outage probability was obtained in [21].

Theorem 7 ([21]) Consider the slow Rayleigh fading channel, in which the channel states h_1 and h_2 are independent and $h_1 \sim \mathcal{CN}(0, 1)$ and $h_2 \sim \mathcal{CN}(0, 1)$, where $\mathcal{CN}(0, 1)$ denotes the proper complex Gaussian distribution with mean zero and variance 1. If the transmitter is subject to the short-term power constraint, then the outage probability is given by

$$\begin{aligned} P_{out} &= \Pr\left\{\left[\log\left(1 + \frac{p(\underline{h})|h_1|^2}{\mu^2}\right) - \log\left(1 + \frac{p(\underline{h})|h_2|^2}{v^2}\right)\right]^+ \leq \check{R}\right\} \\ &= 1 - \frac{\frac{P}{\mu^2}}{\frac{P}{\mu^2} + 2^{\check{R}} \frac{P}{v^2}} \exp\left(-\frac{2^{\check{R}} - 1}{\frac{P}{\mu^2}}\right). \end{aligned} \quad (6.30)$$

This channel was further investigated for the case in which the transmitter has only imperfect estimation of the channel states to the legitimate receiver and to the eavesdropper. The details can be found in [21]. The outage probability for a single-input multiple-output (SIMO) fading channel was also studied and details can be found in [72].

We now consider the block fading wire-tap channel, which is subject to the *long-term* power constraint as in [73], i.e., the power constraint is over a large number of blocks and hence over all fading state realizations:

$$\mathbb{E}[p(\underline{h})] \leq P. \quad (6.31)$$

Under this power constraint, the transmitter is able to adapt its transmission power to the instantaneous channel state realization, i.e., $p(\underline{h})$ is a function of \underline{h} , because the CSI is assumed to be known at the transmitter.

As the outage probability depends on the power allocation function $p(\underline{h})$, our goal next is to study the power allocation $p^*(\underline{h})$ that minimizes the outage probability, i.e.,

$$p^*(\underline{h}) = \arg \min_{p(\underline{h}) \in \mathcal{P}} P_{out} \quad (6.32)$$

where $\mathcal{P} = \{p(\underline{h}) : \mathbb{E}[p(\underline{h})] \leq P\}$.

This problem was studied in [42] as a special case of the fading broadcast channel with confidential messages. The approach in [73] was applied and the basic idea is outlined as follows. The minimum power needed to achieve \check{R} is

$$p^{min}(\underline{h}) = \begin{cases} \frac{2^{\check{R}} - 1}{\frac{|h_1|^2}{\mu^2} - 2^{\check{R}} \frac{|h_2|^2}{v^2}}, & \text{if } \check{R} < \log \frac{|h_1|^2 v^2}{|h_2|^2 \mu^2} \\ \infty & \text{otherwise} \end{cases} \quad (6.33)$$

It is clear from the above that if the target rate \check{R} is above a certain threshold, a finite amount of power cannot prevent the outage. This is in contrast to the fading channel without secrecy constraints, where a sufficiently large amount of power can always accommodate a given target rate for a given channel state.

For $s > 0$, we define

$$\begin{aligned} \mathcal{R}(s) &= \left\{ \underline{h} : p^{min}(\underline{h}) < s \right\} \\ \bar{\mathcal{R}}(s) &= \left\{ \underline{h} : p^{min}(\underline{h}) \leq s \right\} \end{aligned} \quad (6.34)$$

The average powers that are needed to support the secrecy rate \check{R} for the channel states in $\mathcal{R}(s)$ and $\bar{\mathcal{R}}(s)$ are, respectively,

$$\begin{aligned} p(s) &= \mathbb{E}_{\underline{h} \in \mathcal{R}(s)} [p^{min}(\underline{h})] \\ \text{and} \quad \bar{p}(s) &= \mathbb{E}_{\underline{h} \in \bar{\mathcal{R}}(s)} [p^{min}(\underline{h})]. \end{aligned} \quad (6.35)$$

For the given power constraint P , define

$$\begin{aligned} s^* &= \sup \{s : p(s) < P\} \\ \text{and} \quad w^* &= \frac{P - p(s^*)}{\bar{p}(s^*) - p(s^*)}. \end{aligned} \quad (6.36)$$

The optimal power allocation $p^*(\underline{h})$ is given in the following theorem.

Theorem 8 *The power allocation $p^*(\underline{h})$ that solves Eq. (6.32), and hence minimizes the outage probability for a given target secrecy rate \bar{R} , is given by*

$$p^*(\underline{h}) = \begin{cases} p^{\min}(\underline{h}), & \text{if } \underline{h} \in \mathcal{R}(s^*) \\ p^{\min}(\underline{h}), & \text{with prob. } w^* \text{ if } \underline{h} \in \bar{\mathcal{R}}(s^*) \setminus \mathcal{R}(s^*) \\ 0 & \text{if } \underline{h} \notin \bar{\mathcal{R}}(s^*) \end{cases} \quad (6.37)$$

where $p^{\min}(\underline{h})$ is given in Eq. (6.33).

It can be seen that the optimal power allocation $p^*(\underline{h})$ is a threshold solution. The power is first allocated to the fading states that need smaller amounts of power to achieve the target rate, and is then allocated to the fading states that need larger amounts of power to achieve the target rate. When the total power P is used up by these fading states, no further power is allocated to other states.

6.4 Compound Wire-Tap Channel

The compound wire-tap channel is a generalization of the wire-tap channel, in which each of the channels from the transmitter to the receiver and to the eavesdropper has a number of states. The source message must be transmitted to the destination reliably and must be kept perfectly secret from the eavesdropper no matter which channel state occurs. The compound wire-tap channel can be viewed as a *multicast channel with multiple eavesdroppers* (see Fig. 6.3), and the source message must be successfully transmitted to all receivers (J receivers) and must be kept secret from all eavesdroppers (K eavesdroppers).

The compound wire-tap channel was studied in [39, 40, 74]. Several special cases of the compound wire-tap channel have also been studied; these special cases include the parallel wire-tap channel with two wire-tappers [56, 75], the fading wire-tap channels with multiple wire-tappers [76], and the wire-tap channel with multiple receivers [31].

6.4.1 Discrete Memoryless Compound Wire-Tap Channels

Suppose a transmitter sends source message W to J receivers, and wishes to keep the information as secret as possible from K non-collaborating eavesdroppers. The channel input is denoted by $X \in \mathcal{X}$, the output at receiver j is denoted by $Y_j \in \mathcal{Y}_j$ for $j = 1, \dots, J$, and the output at eavesdropper k is denoted by $Z_k \in \mathcal{Z}_k$ for $k = 1, \dots, K$, where \mathcal{X} , \mathcal{Y}_j and \mathcal{Z}_k are finite alphabet sets. The transition probability distribution for the broadcast channel to destination j and wire-tapper k is given by

$$P_{Y_j Z_k | X}(\cdot) \quad \text{for } j = 1, \dots, J, \text{ and } k = 1, \dots, K. \quad (6.38)$$

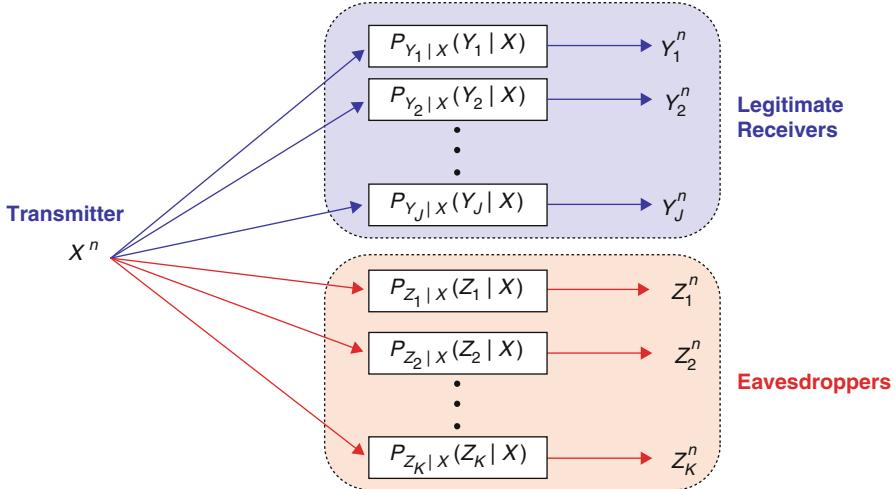


Fig. 6.3 The compound wire-tap channel

As the correlation between Y_j and Z_k does not affect the secrecy capacity, without loss of optimality, we assume the transition probability $P_{Y_j|X}P_{Z_k|X}$ as shown in Fig. 6.3.

A secrecy rate R is *achievable* if there exists a sequence of $(2^{nR}, n)$ codes with the average error probability at each receiver satisfying

$$P_{e,j}^{(n)} \rightarrow 0 \quad \text{for } j = 1, \dots, J$$

as n goes to infinity, and with the equivocation rate satisfying

$$R \leq \lim_{n \rightarrow \infty} \frac{1}{n} H(W|Z_k^n) \quad \text{for } k = 1, \dots, K.$$

The *secrecy capacity* is the maximal achievable secrecy rate.

Theorem 9 ([39]) *The following secrecy rate is achievable for the compound wire-tap channel:*

$$R = \max_{j,k} \min \left[I(U; Y_j) - I(U; Z_k) \right] \quad (6.39)$$

where the maximum is over all distributions $P_{U|X}$ that satisfy the Markov chain relationships:

$$U \rightarrow X \rightarrow (Y_j, Z_k) \quad \text{for } j = 1, \dots, J \text{ and } k = 1, \dots, K.$$

Theorem 9 can be interpreted as a worst case result, in which the worst receiver and the best eavesdropper dominate the secrecy rate.

The following two upper bounds on the secrecy capacity of the compound wire-tap channel were given in [39] and [74], respectively.

Theorem 10 ([39] and [74]) *Two upper bounds on the secrecy capacity of the compound wire-tap channel are given by*

$$\bar{R}_1 = \min_{j,k} \max_{P_{U|X} P_{Y_j|Z_k|X}} \left[I(U; Y_j) - I(U; Z_k) \right] \quad (6.40)$$

and

$$\bar{R}_2 = \max_{P_X} \min_{j,k} I(X; Y_j | Z_k), \quad (6.41)$$

where the maximization in Eq. (6.40) for each (j, k) pair is taken over all jointly distributed $P_{U|X}$ between the channel input X and an auxiliary random variable U satisfying the Markov chain condition $U \rightarrow X \rightarrow (Y_j, Z_k)$.

We note that it may not be possible to achieve the first upper bound given in Theorem 10 in general. This is because the input scheme needs to balance the rates that can be achieved for all channel states, and consequently, none of the channel states can achieve its best rate. This can also be seen from the achievable rate in Eq. (6.39). The input distribution $P_{U|X}$ that maximizes the minimum of the secrecy rates of all channel states may not be optimal for any single state.

The secrecy capacity can be obtained for the two special cases of the compound wire-tap channels. We say that the compound wire-tap channel is *degraded* if the transition probability satisfies the Markov chain condition

$$X \rightarrow Y_j \rightarrow Z_k \quad (6.42)$$

for all $j = 1, \dots, J$ and $k = 1, \dots, K$. For the degraded compound wire-tap channel, we have the following capacity theorem.

Theorem 11 ([39]) *The secrecy capacity of the degraded compound wire-tap channel is given by*

$$C = \max_{P_X} \min_{j,k} \left[I(X; Y_j) - I(X; Z_k) \right]. \quad (6.43)$$

Consider the compound wire-tap channel, which has one destination ($J = 1$) and K wire-tappers. The channel is *semideterministic* if the channel from the transmitter to the receiver is deterministic, i.e., the transition probability distribution $P_{Y|X}(\cdot)$ takes on the values 0 or 1 only, where the output at the destination is denoted by Y .

Theorem 12 ([40]) *The secrecy capacity of the semideterministic compound channel with $J = 1$ is given by*

$$C_s = \max_{P_X} \min_k H(Y|Z_k). \quad (6.44)$$

For both the degraded and semideterministic compound wire-tap channels, the second upper bound given in Theorem 10 is tight.

6.4.2 Parallel Gaussian Compound Wire-Tap Channels

In this section, we study the parallel Gaussian compound channel, in which the channels from the transmitter to each receiver and to each eavesdropper are parallel Gaussian channels. Understanding this channel will be useful to study the compound fading wire-tap channels, as the parallel Gaussian channel serves as a general model for the fading channel. An application of this channel is to wideband wireless communication systems such as frequency-division multiplexing (FDM) systems in which transmission is over a number of frequency bands, and the eavesdroppers can tune their receivers to access some of these frequency bands.

We first consider the case in which $J = 1$ and $K > 1$, i.e., one receiver and K eavesdroppers, and each parallel channel contains N subchannels. The outputs at the receiver from the N subchannels are given by

$$Y_a = X_a + V_{Ra}, \quad \text{for } a = 1, \dots, N, \quad (6.45)$$

where V_{R1}, \dots, V_{RN} are independent Gaussian random variables with variances μ_1^2, \dots, μ_N^2 , and the outputs at eavesdropper k from the N subchannels are given by

$$Z_{ka} = X_a + V_{Eka}, \quad \text{for } a = 1, \dots, N, \quad (6.46)$$

where V_{Ek1}, \dots, V_{EkN} are independent Gaussian random variables with variances $v_{k1}^2, \dots, v_{kN}^2$. The channel input is subject to the average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \sum_{a=1}^N \mathbb{E}[X_{ai}^2] \leq P, \quad (6.47)$$

where i is the symbol time index.

The parallel compound wire-tap channel is *degraded* if $v_{ka}^2 \geq \mu_a^2$ for all $a = 1, \dots, N$ and $k = 1, \dots, K$. For the degraded parallel Gaussian compound wire-tap channel, we have the following secrecy capacity.

Theorem 13 *The secrecy capacity of the degraded parallel Gaussian compound wire-tap channel with $J = 1$ is given by*

$$C = \max_{\sum_{a=1}^N P_a \leq P} \min_k \left[\sum_{a=1}^N \frac{1}{2} \log \left(1 + \frac{P_a}{\mu_a^2} \right) - \frac{1}{2} \log \left(1 + \frac{P_a}{v_{ka}^2} \right) \right]. \quad (6.48)$$

To obtain the secrecy capacity of the parallel Gaussian compound wire-tap channel, we need to solve the “max–min” optimization problem in Eq. (6.48), i.e., we need to derive the optimal power allocation. We refer the reader to [39] for the details in characterizing the optimal power allocation.

Theorem 13 has recently been generalized for the nondegraded parallel Gaussian compound wire-tap channel in [74].

Theorem 14 ([74]) The secrecy capacity of the parallel Gaussian compound wire-tap channel with $J = 1$ is given by

$$C_s = \max_{\sum_{a=1}^N P_a \leq P} \min_k \left[\sum_{a=1}^N \frac{1}{2} \log \left(1 + \frac{P_a}{\mu_a^2} \right) - \frac{1}{2} \log \left(1 + \frac{P_a}{v_{ka}^2} \right) \right]^+. \quad (6.49)$$

The case when $J > 1$ was studied in [40], where the secrecy degree of freedom (*s.d.o.f.*) (the rate at which the secrecy capacity scales with $\log \text{SNR}$) was considered to gain some insight into optimal schemes to achieve the secrecy capacity. The *s.d.o.f.* is defined as

$$\text{s.d.o.f.} = \lim_{\text{SNR} \rightarrow \infty} \frac{C(\text{SNR})}{\frac{1}{2} \log \text{SNR}} \quad (6.50)$$

where without loss of generality, we choose the variance of the noise of one of the subchannels as the reference noise level.

For the sake of clarity of exposition, we consider an example when $J = 2$ and $K = 2$, as depicted in Fig. 6.4. The channel output at receiver 1 is given by

$$Y_1 = X_1 + V_{R1} \quad (6.51)$$

where V_{R1} is a zero-mean Gaussian random variable with variance μ_1^2 . The channel output at receiver 2 is given by

$$Y_{21} = X_{21} + V_{R21} \quad \text{and} \quad Y_{22} = X_{22} + V_{R22} \quad (6.52)$$

where V_{R21} and V_{R22} are zero-mean independent Gaussian random variables with variances μ_{21}^2 and μ_{22}^2 . The outputs at the two eavesdroppers are given by

$$Z_1 = X_{21} + V_{E1} \quad (6.53)$$

and

$$Z_2 = X_{22} + V_{E2} \quad (6.54)$$

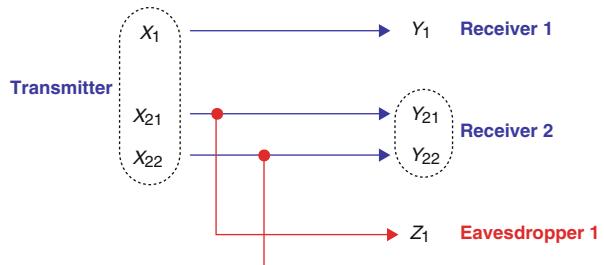


Fig. 6.4 Parallel Gaussian compound wire-tap channel example

where V_{E1} and V_{E2} are zero-mean independent Gaussian random variables with variances ν_1^2 and ν_2^2 , respectively.

For this channel, an achievable rate follows from Eq. (6.39) and is given by

$$R = \max_{P_{UX}} \min \left\{ I(U; Y_1) - I(U; Z_1), I(U; Y_1) - I(U; Z_2), \right. \\ \left. I(U; Y_{21}, Y_{22}) - I(U; Z_1), I(U; Y_{21}, Y_{22}) - I(U; Z_2) \right\} \quad (6.55)$$

Three schemes were studied in [40] to demonstrate the role of the prefix channel $U \rightarrow X$ in achieving the optimal *s.d.o.f.* Without loss of generality, in the following we assume $\mu_1^2 = \mu_{21}^2 = \mu_{22}^2 = \nu_1^2 = \nu_2^2 = 1$.

Scheme 1 Choose $U = X = (X_1, X_{21}, X_{22})$, $X_1 \sim \mathcal{N}(0, P_1)$, $X_{21} \sim \mathcal{N}(0, P_{21})$, and $X_{22} \sim \mathcal{N}(0, P_{22})$ in Eq. (6.55). Based on these distributions, Scheme 1 achieves

$$\text{s.d.o.f.} = \frac{1}{2}.$$

Scheme 2 Choose a Gaussian input and allocate the transmission power equally for X_1 , X_{21} and X_{22} . Each subchannel can hence support the rate $R = \frac{1}{2} \log(1 + P/3)$. Now let the source message be W uniformly distributed over the set $\{0, \dots, 2^{nR} - 1\}$, and generate a key random variable M that is independent of W , and is also uniformly distributed over the set $\{0, \dots, 2^{nR} - 1\}$. Define the operation \oplus to be “addition modulo 2^{nR} ”. We transmit W over the channel $X_1 \rightarrow Y_1$, and transmit $W \oplus M$ and M over the channels $X_{21} \rightarrow Y_{21}$ and $X_{22} \rightarrow Y_{22}$, respectively. Scheme 2 achieves

$$\text{s.d.o.f.} = 1,$$

which is clearly the largest achievable *s.d.o.f.*.

Scheme 3 Choose $U = (X_1, X_{21} + X_{22})$, $X_1 \sim \mathcal{N}(0, P/3)$, $X_{21} \sim \mathcal{N}(0, P/3)$, and $X_{22} \sim \mathcal{N}(0, P/3)$ in Eq. (6.55). Based on these distributions, Scheme 3 achieves

$$\text{s.d.o.f.} = 1.$$

Compared to Scheme 1, Scheme 3 introduces extra randomness in the encoder by introducing a prefix channel $U \rightarrow X$, and hence achieves the optimal *s.d.o.f.* We note that for Gaussian and MIMO wire-tap channels studied in [60–62, 65] the prefix channel is not necessary to achieve the secrecy capacity, i.e., $U = X$. However, the prefix channel is necessary to achieve the optimal *s.d.o.f.* for the parallel Gaussian compound wire-tap channel.

Schemes 2 and 3 suggest that introducing randomness either into the information source or into the encoder strictly improves the *s.d.o.f.* and hence improves the secrecy rate.

6.4.3 MIMO Compound Wire-Tap Channels

In this section, we consider the MIMO compound wire-tap channel, in which the transmitter, the receivers, and the eavesdroppers are equipped with N_T , N_R , and N_E

antennas, respectively. The channel input–output relationship for one channel use is given by

$$\begin{aligned}\underline{Y}_j &= H_j \underline{X} + \underline{V}_{Rj} \quad \text{for } j = 1, \dots, J; \\ \underline{Z}_k &= G_k \underline{X} + \underline{V}_{Ek} \quad \text{for } k = 1, \dots, K;\end{aligned}\tag{6.56}$$

where H_j for $j = 1, \dots, J$ and G_k for $k = 1, \dots, K$ are fixed matrices, and $\underline{V}_{R1}, \dots, \underline{V}_{RJ}$ and $\underline{V}_{E1}, \dots, \underline{V}_{EK}$ are i.i.d. Gaussian random vectors with identity covariance matrices. We assume that the channel input is subject to an average power constraint

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [\underline{X}_i^T \underline{X}_i] \leq P\tag{6.57}$$

where i is the symbol time index.

In the following, we use $A \geq 0$ to indicate that A is a positive semidefinite matrix, $A > 0$ to indicate A is a positive definite matrix, and $A \geq B$ to indicate that $A - B$ is a positive semidefinite matrix. The symbols \leq and $<$ indicate the opposite meanings to those of \geq and $>$, respectively.

The MIMO compound wire-tap channel was studied in [39], and we summarize the results in the following. As defined in [68], the MIMO compound wire-tap channel is *degraded* if for each (j, k) pair, there exists a matrix D_{jk} such that $D_{jk}H_j = G_k$ and $D_{jk}D_{jk}^T \leq I$. It is easy to check that for each (j, k) pair, the channel satisfies the Markov chain relationship $\underline{X} \rightarrow \underline{Y}_j \rightarrow \underline{Z}_k$.

Theorem 15 ([39]) *The secrecy capacity of the degraded MIMO compound wire-tap channel is given by*

$$C = \max_{Q: Q \geq 0, \text{Tr}(Q) \leq P} \min_{j,k} \frac{1}{2} \log \frac{|I + H_j Q H_j^T|}{|I + G_k Q G_k^T|}.\tag{6.58}$$

The above secrecy capacity can be achieved by choosing Gaussian input $X \sim \mathcal{N}(0, Q)$. It is clear that the above rate is also achievable for the general MIMO compound wire-tap channel based on Theorem 9 by choosing $U = X \sim \mathcal{N}(0, Q)$.

Lemma 2 *For the general MIMO compound wire-tap channel, an achievable secrecy rate is given by*

$$R_e = \max_{Q: Q \geq 0, \text{Tr}(Q) \leq P} \min_{j,k} \frac{1}{2} \log \frac{|I + H_j Q H_j^T|}{|I + G_k Q G_k^T|}.\tag{6.59}$$

In general, the maximization problem in Eq. (6.59) is difficult to solve. The *s.d.o.f.* was further investigated in [39], where it was defined as in Eq. (6.50) but with $\text{SNR} = P/N_T$. In the following, we consider a special case when $J = 1$, and refer the reader to [39] for the general case.

Theorem 16 For the MIMO compound wire-tap channel with $J = 1$, an achievable s.d.o.f. is given by

$$\text{s.d.o.f.} = \min_k \left\{ \text{Rank}(H) - \text{Rank}(G_k \Sigma) \right\} \quad (6.60)$$

where Σ is the matrix whose columns are the eigenvectors of $H^T H$ corresponding to nonzero eigenvalues.

To achieve the above s.d.o.f., the beamforming directions of the channel inputs are chosen to be along the eigenvectors of $H^T H$ that correspond to nonzero eigenvalues, i.e., the column vectors in the matrix Σ . The terms $\text{Rank}(H)$ and $\text{Rank}(G_k \Sigma)$ in Eq. (6.60) can be interpreted as the number of signal dimensions observed by the receiver and by eavesdropper k , respectively. Hence, the achievable s.d.o.f. is determined by the difference between these two dimensions.

6.5 Wire-Tap Channel with Side Information

We consider the wire-tap channel with side information (see Fig. 6.5), in which the channel from the transmitter to the receiver and the eavesdropper can take one of a few states. The channel is characterized by the transition probability $P_{YZ|XS}$, where S is the channel state variable. The channel state S_n at each symbol time belongs to a finite alphabet size \mathcal{S} , and changes from one symbol to another. The realization of the state sequence S^n is known non-causally at the transmitter only. Hence, the (stochastic) encoder at the transmitter $f: \mathcal{W} \times \mathcal{S}^n \rightarrow \mathcal{X}^n$ maps $w \times s^n \in (\mathcal{W}, \mathcal{S}^n)$ to a codeword x^n , which is transmitted over the channel. This model can be viewed as a generalization of the model studied by Gel'fand and Pinsker in [77] by introducing an eavesdropper.

This channel was studied in [24, 48]. An achievable secrecy rate is given in the following theorem.

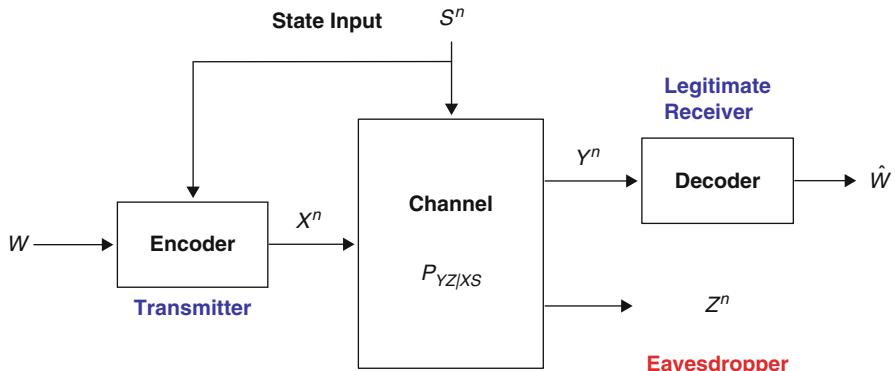


Fig. 6.5 The wire-tap channel with side information

Theorem 17 ([24]) For the wire-tap channel with side information, an achievable secrecy rate is given by

$$R_e = \max_{P_{U,S} X P_{Y|Z|X,S}} \min\{I(U; Y) - I(U; Z), I(U; Y) - I(U; S)\} \quad (6.61)$$

where the maximization is taken over all jointly distributed $P_{U,S} X$ among the channel input X , the side information S , and an auxiliary random variable U satisfying the Markov chain condition $U \rightarrow (X, S) \rightarrow (Y, Z)$.

We note that since the state sequence is not known at the eavesdropper, it may help improve the secrecy rate. This becomes clear for the Gaussian wire-tap channel with side information that we will consider later in this section.

Two upper bounds on the secrecy capacity can be derived and are given in the following theorem.

Theorem 18 For the wire-tap channel with side information, two upper bounds on the secrecy capacity are given by

$$\bar{R}_{1e} = \max_{P_{U,S} X P_{Y|Z|X,S}} I(U; Y) - I(U; S) \quad (6.62)$$

and

$$\bar{R}_{2e} = \max_{P_{U,S} X P_{Y|Z|X,S}} I(U; Y) - I(U; Z) \quad (6.63)$$

where the maximization in both Eqs. (6.62) and (6.63) is taken over all jointly distributed $P_{U,S} X$ among the channel input X , the side information S , and an auxiliary random variable U satisfying the Markov chain condition $U \rightarrow (X, S) \rightarrow (Y, Z)$.

The first upper bound is the capacity of the channel with side information without the secrecy constraint [77], and is clearly an upper bound for the channel with the secrecy constraint. The second bound is the secrecy capacity of the wire-tap channel with the channel inputs (X, S) , which is an enhanced channel compared to the original wire-tap channel with side information, and hence is an upper bound on the secrecy capacity for the original channel.

The Gaussian wire-tap channel with side information was studied in [24, 48], where the state variable is an additive interference to the outputs at the receiver and the eavesdropper. The model is a generalization of the model studied in [78] in which an eavesdropper is introduced. The channel input-output relationship for one channel use is given by

$$\begin{aligned} Y &= X + S + V_R \\ Z &= X + S + V_E \end{aligned} \quad (6.64)$$

where the state sequence S^n consists of i.i.d. components with each component having distribution $\mathcal{N}(0, P_S)$, and V_R and V_E are independent zero-mean Gaussian

random variables with variances μ^2 and v^2 . The channel input is subject to an average power constraint P , i.e.,

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E} [X_i^2] \leq P \quad (6.65)$$

where i is the symbol time index.

Theorem 19 ([24]) *For the Gaussian wire-tap channel with side information, an achievable secrecy rate is given by*

$$R_e = \max_{\alpha} \min \{I(U_{\alpha}; Y) - I(U_{\alpha}; S), I(U_{\alpha}; Y) - I(U_{\alpha}; Z)\} \quad (6.66)$$

where α is a real number, $U_{\alpha} = X + \alpha S$, and $X \sim \mathcal{N}(0, P)$.

The optimization of the preceding equation was further analyzed in [24] to provide the more explicit expression for the secrecy rate. Let

$$R(\alpha) = I(U_{\alpha}; Y) - I(U_{\alpha}; S) \quad (6.67)$$

and

$$R_Z(\alpha) = I(U_{\alpha}; Y) - I(U_{\alpha}; Z). \quad (6.68)$$

The function $R(\alpha)$ is maximized at $\alpha = \alpha^* = \frac{P}{P+\mu^2}$, and

$$R(\alpha^*) = \frac{1}{2} \log \left(1 + \frac{P}{\mu^2} \right). \quad (6.69)$$

The function $R_Z(\alpha)$ is maximized at $\alpha = 1$ and

$$R_Z(1) = \frac{1}{2} \log \left(\frac{(P + P_S + \mu^2)v^2}{\mu^2(P + P_S + v^2)} \right). \quad (6.70)$$

It can also be shown that $R(\alpha_0) = R_Z(\alpha_0)$ when $\alpha_0 = \frac{P_S + P \sqrt{P_S(P + P_S + v^2)}}{P_S(P + v^2)}$.

Let

$$P_{low} = -\mu^2 - \frac{P_S}{2} + \frac{\sqrt{P_S^2 + 4P_S(v^2 - \mu^2)}}{2} \quad (6.71)$$

and

$$P_{high} = -\frac{P_S}{2} + \frac{\sqrt{P_S^2 + 4P_Sv^2}}{2}. \quad (6.72)$$

It is shown in [24, 48] that the secrecy rate given in Eq. (6.66) can be written as

$$R_e = \begin{cases} R(\alpha^*) & \text{if } P \leq P_{low} \\ R(\alpha_0) & \text{if } P_{low} \leq P \leq P_{high} \\ R_Z(1) & \text{if } P \geq P_{high} \end{cases} \quad (6.73)$$

The above three cases correspond to the three possible cases of the optimization problem $\max_{\alpha} \min\{R(\alpha), R_Z(\alpha)\}$: (1) $R(\alpha)$ is optimized at $\alpha = \alpha^*$, and $R(\alpha^*) < R_Z(\alpha^*)$; (2) $R_Z(\alpha)$ is optimized at $\alpha = 1$, and $R(1) > R_Z(1)$; and (3) $R(\alpha)$ is optimized subject to $R(\alpha) = R_Z(\alpha)$.

It can be seen from Eq. (6.73) that the Gaussian wire-tap channel with side information has larger secrecy capacity than the Gaussian wire-tap channel. Hence, the side information helps improve the secrecy capacity. This is in contrast to the channel without the secrecy constraint, in which the side information does not affect the capacity [78].

As argued in [48], the secrecy rate given in Eq. (6.73) achieves the secrecy capacity for the cases when $P \leq P_{low}$ and when $P \geq P_{high}$. The secrecy rate in the former case is the capacity of the channel without secrecy constraint and with both the transmitter and the receiver knowing the state sequence. The secrecy rate in the latter case is the secrecy capacity of an enhanced wire-tap channel, in which the state variable is used as the channel input instead of the channel interference. Both of these two secrecy capacities are clearly upper bounds on the secrecy capacity for the original wire-tap channel with side information. Hence, achieving these two bounds imply achieving the secrecy capacity.

6.6 Conclusions

In this section, we discuss open research topics concerning the wire-tap channel under channel state uncertainty. For the fading wire-tap channel, it is clear that the CSI at the transmitter is critical to the design of secure transmission schemes. However, in many communication scenarios, it is difficult to learn or estimate an eavesdropper's channel due to the lack of feedback from the eavesdropper. Only a few studies (e.g., [31, 71, 80]) have addressed for the fading wire-tap channel when the CSI is not known at the transmitter. Further study of the MIMO fading wire-tap channel in such a scenario is needed. The outage performance for the fading wire-tap channel when the CSI is not available at the transmitter is also open. In [21], the outage performance of the fading wire-tap channel under channel estimation errors was studied. Further work is to be made to understand both the ergodic and outage performances under channel estimation errors for the MIMO fading wire-tap channel.

The compound wire-tap channel remains a challenging topic, as its secrecy capacity is not known in general. Further understanding of achievable schemes and upper bounds on the secrecy capacity is needed for the general compound wire-tap channel. For the parallel Gaussian compound wire-tap channel, the secrecy capacity for the scenario with multiple receivers and multiple eavesdroppers remains open.

Understanding the *s.d.o.f.* of this general scenario may be a useful first step. Furthermore, the insights obtained from the parallel Gaussian compound wire-tap channel will be useful in studying the MIMO compound wire-tap channel.

The secrecy capacity for the wire-tap channel with side information is unknown in general. Tight results on the secrecy capacity for the Gaussian wire-tap channel with side information under certain conditions obtained in [24, 48] suggest that the secrecy capacity of the MIMO case may be obtained for some special cases. The side information has a natural interpretation in multiuser communications as the interference caused from other transmitters' transmissions or from other source messages that need to be sent by the same transmitter. Coding techniques for the wire-tap channel with side information are applicable to these multiuser scenarios when there is a secrecy constraint.

In this chapter, we have focused on the case of perfect secrecy, and considered only the secrecy capacity as the performance measure. The more general capacity-equivocation region, which characterizes the tradeoff between the reliable communication rate and the secrecy level (equivocation rate), needs to be studied. Furthermore, more general scenarios with multiple source messages also need to be studied. Several results are already available along these two lines of inquiry, including the capacity-equivocation region for the broadcast channel with both a confidential message and a common message [59] and its fading case [42], and for the fading broadcast channel with multiple individual messages [22, 31, 45, 47, 79]. The two extensions for the compound wire-tap channel and the wire-tap channel with side information remain open.

Acknowledgement The authors would like to thank Prof. Tie Liu at Texas A&M University and Dr. Lifeng Lai at University of Arkansas at Little Rock for very useful discussions of the ideas presented in this chapter. The work of Y. Liang was supported by the National Science Foundation CAREER Award under Grant CCF-08-46028. The work of H. V. Poor was supported by the National Science Foundation under Grant CNS-06-25637. The work of S. Shamai was supported by the European Commission in the framework of the FP7 Network of Excellence in Wireless Communications NEWCOM++.

References

- [1] C. E. Shannon. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, 28:656–715, 1949.
- [2] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975.
- [3] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography-Part I: Secret sharing. *IEEE Trans. Inf. Theory*, 39(4):1121–1132, July 1993.
- [4] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography-Part II: CR capacity. *IEEE Trans. Inf. Theory*, 44(1):225–240, January 1998.
- [5] I. Csiszár and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory*, 46(2):344–366, March 2000.
- [6] I. Csiszár and P. Narayan. Secrecy capacities for multiple terminals. *IEEE Trans. Inf. Theory*, 50(12):3047–3061, December 2004.

- [7] I. Csiszar and P. Narayan. Secrecy capacities for multiterminal channel models. *IEEE Trans. Inf. Theory, Special Issue on Information Theoretic Security*, 54(6):2437–2452, June 2008.
- [8] A. A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminals-Part I: Source model. *IEEE Trans. on Inf. Theory*, submitted. Available at <http://www.eecs.berkeley.edu/~aminzade/SourceModel.pdf>.
- [9] A. A. Gohari and V. Anantharam. Information-theoretic key agreement of multiple terminals-Part II: Channel model. *IEEE Trans. on Inf. Theory*, submitted. Available at <http://www.eecs.berkeley.edu/~aminzade/ChannelModel.pdf>.
- [10] A. A. Gohari and V. Anantharam. Communication for omniscience by a neutral observer and information-theoretic key agreement of multiple terminals. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, June 2007.
- [11] A. A. Gohari and V. Anantharam. New bounds on the information-theoretic key agreement of multiple terminals. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [12] A. Khisti, S. Diggavi, and G. W. Wornell. Secret key generation with correlated sources and noisy channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [13] U. M. Maurer. Secret key agreement by public discussion based on common information. *IEEE Trans. Inf. Theory*, 39(5):733–742, May 1993.
- [14] U. M. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Inf. Theory*, 45(2):499–514, February 1999.
- [15] U. M. Maurer and S. Wolf. From weak to strong information-theoretic key agreement. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, p. 18, Sorrento, Italy, June 2000.
- [16] M. Naito, S. Watanabe, R. Matsumoto, and T. Uyematsu. Secret key agreement by reliability information of signals in Gaussian Maurer’s model. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [17] S. Nitinawarat, C. Ye, A. Barg, P. Narayan, and A. Reznik. Secret key generation for a pairwise independent network model. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [18] V. Prabhakaran, K. Eswaran, and K. Ramchandran. Secrecy via sources and channels: A secret key-secret message rate trade-off region. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [19] R. Renner and S. Wolf. New bounds in secret key agreement: The gap between formation and secrecy extraction. In *Adv. Cryptol.-EUROCRYPT*, 2656:562–577, 2003.
- [20] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim. Wiretap channel with rate-limited feedback. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [21] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inf. Theory*, 54(6):2515–2534, June 2008.
- [22] Y. Cao and B. Chen. An achievable rate region for discrete memoryless broadcast channels with confidential messages. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [23] A. Carleial and M. Hellman. A note on Wyner’s wiretap channel. *IEEE Trans. Inf. Theory*, 23(3):387–390, May 1977.
- [24] Y. Chen and A. J. H. Vinck. Wiretap channel with side information. *IEEE Trans. Inf. Theory*, 54(1):395–402, January 2008.
- [25] G. Cohen and G. Zemor. The wire-tap channel applied to biometrics. In *Proc. Int. Symp. Inf. Theory App. (ISITA)*, Parma, Italy, October 2004.
- [26] E. Ekrem and S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In *Proc. Conf. Inf. Sci. Syst. (CISS)*, Princeton, NJ, USA, March 2008.
- [27] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.

- [28] M. Hayashi. General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel. *IEEE Trans. Inf. Theory*, 52(4):1562–1575, April 2006.
- [29] X. He and A. Yener. The role of an untrusted relay in secret communication. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [30] X. He and A. Yener. Secrecy when the relay is the eavesdropper. In *Proc. Inf. Theory and Appl. Workshop (ITA)*, San Diego, CA, USA, January 2008.
- [31] A. Khisti, A. Tchamkerten, and G. Wornell. Secure broadcasting. *IEEE Trans. Inf. Theory, Spec. Issue on Information Theoretic Security*, 54(6):2453–2469, June 2008.
- [32] H. Koga and N. Sato. On an upper bound of the secrecy capacity for a general wiretap channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 1641–1645, Adelaide, Australia, September 2005.
- [33] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor. On the secure degrees of freedom in the K -user Gaussian interference channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [34] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, September 2008.
- [35] L. Lai, H. El Gamal, and H. V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. Inf. Theory*, 54(11):5059–5067, November 2008.
- [36] S. K. Leung-Yan-Cheong. On a special class of wire-tap channels. *IEEE Trans. Inf. Theory*, 23(5):625–627, September 1977.
- [37] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity region of a class of one-sided interference channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [38] Y. Liang, H. V. Poor, and S. Shamai, “Information Theoretic Security.” in *Foundat. Trends in Commun. Inf. Theory*. 5(4-5):355–580, 2008.
- [39] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Compound wire-tap channels. In *Proc. 45th Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, Monticello, IL, USA, September 2007.
- [40] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz). Recent results on compound wire-tap channels. In *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Cannes, France, September 2008.
- [41] Y. Liang and H. V. Poor. Multiple access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, March 2008.
- [42] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Secure communication over fading channels. *IEEE Trans. Inf. Theory, Special Issue on Information Theoretic Security*, 54(6):2470–2492, June 2008.
- [43] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai (Shitz), and S. Verdú. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inf. Theory*, 55(2):604–619, February 2009.
- [44] R. Liu, Y. Liang, H. V. Poor, and P. Spasojevic. Secure nested codes for type II wire-tap channels. In *Proc. IEEE Inf. Theory Workshop (ITW)*, Lake Tahoe, CA, USA, September 2007.
- [45] R. Liu, I. Maric, P. Spasojevic, and R. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory, Special Issue on Information Theoretic Security*, 54(6):2493–2507, June 2008.
- [46] R. Liu, I. Maric, R. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, July 2006.
- [47] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, March 2009.
- [48] C. Mitrpant, A. J. H. Vinck, and Y. Luo. An achievable region for the Gaussian wiretap channel with side information. *IEEE Trans. Inf. Theory*, 52(5):2181–2190, May 2006.

- [49] Y. Oohama. Relay channels with confidential messages. *IEEE Trans. Inf. Theory*, Submitted 2007. Available at http://arxiv.org/PS_cache/cs/pdf/0611/0611125v7.pdf.
- [50] Y. Oohama. Coding for relay channels with confidential messages. In *Proc. IEEE Inf. Theory Workshop (ITW)*, Cairns, Australia, pp. 87–89, September 2001.
- [51] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The Gaussian wiretap channel with a helping interferer. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [52] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, December 2008.
- [53] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory, Special Issue on Information Theoretic Security*, 54(6):2735–2751, June 2008.
- [54] A. Thangaraj, S. Dihidar, A. Calderbank, S. McLaughlin, and J.-M. Merolla. Application of LDPC codes to the wiretap channel. *IEEE Trans. Inf. Theory*, 53(8):2933–2945, August 2007.
- [55] M. van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 43(2):712–714, March 1997.
- [56] H. Yamamoto. Coding theorem for secret sharing communication systems with two noisy channels. *IEEE Trans. Inf. Theory*, 35(3):572–578, May 1989.
- [57] R. D. Yates, D. Tse, and Z. Li. Secret communication on interference channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [58] M. Yuksel and E. Erkip. Secure communication with a relay helping the wiretapper. In *Proc. IEEE Inf. Theory Workshop (ITW)*, Lake Tahoe, CA, September 2007.
- [59] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.
- [60] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, July 1978.
- [61] A. Khisti and G. Wornell. The MIMOME channel. In *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, September 2007.
- [62] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wire-tap channel. In *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, September 2007.
- [63] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, Submitted for publication, 2007.
- [64] H. Sato. An outer bound to the capacity region of broadcast channels. *IEEE Trans. Inf. Theory*, 24(3):374–377, May 1978.
- [65] T. Liu and S. Shamai (Shitz). A note on the secrecy capacity of the multi-antenna wire-tap channel. *IEEE Trans. Inf. Theory*, 55(11), November 2009.
- [66] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, September 2006.
- [67] T. Liu and P. Viswanath. An extremal inequality motivated by multiterminal information-theoretic problems. *IEEE Trans. Inf. Theory*, 53(5):1839–1851, May 2007.
- [68] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath. The capacity region of the degraded MIMO compound broadcast channel. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, June 2007.
- [69] Z. Li, R. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, September 2006.
- [70] Y. Liang and H. V. Poor. Secure communication over fading channels. In *Proc. 44th Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, September 2006.
- [71] P. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory*, 54(10):4687–4698, October 2008.

- [72] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Adelaide, Australia, pp. 2152–2155, September 2005.
- [73] G. Caire, G. Taricco, and E. Biglieri. Optimal power control over fading channels. *IEEE Trans. Inf. Theory*, 45(5):1468–1489, July 1999.
- [74] T. Liu, V. Prabhakaran, and S. Vishwanath. The secrecy capacity of a class of parallel Gaussian compound wiretap channels. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Toronto, ON, Canada, July 2008.
- [75] H. Yamamoto. A coding theorem for secret sharing communication systems with two Gaussian wiretap channels. *IEEE Trans. Inf. Theory*, 37(3):634–638, May 1991.
- [76] P. Wang, G. Yu, and Z. Zhang. On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, June 2007.
- [77] S. I. Gelfand and M. S. Pinsker. Coding for channel with random parameters. *Probl. Contr. Inf. Theory*, 9(1):19–31, 1980.
- [78] M. H. M. Costa. Writing on dirty paper. *IEEE Trans. Inf. Theory*, 29(3):439–441, May 1983.
- [79] Y. Liang, H. V. Poor, and L. Ying. Wireless broadcast networks: Reliability, security and stability. In *Proc. of 3rd Inf. Theor. Appl. Workshop (ITA)*, La Jolla, CA, USA, May 2008.
- [80] Y. Liang, L. Lai, H. V. Poor and S. Shamai (Shitz). The broadcast approach to fading wiretap channels. In *Proc. of Inf. Theory Workshop (ITA)*, Taormina, Sicily, Italy, October 2009.

Chapter 7

Cooperative Secrecy in Wireless Communications*

Ersen Ekrem and Sennur Ulukus

7.1 Introduction

The broadcast nature of wireless communications leads to two concepts: cooperation and secrecy. The basis for both cooperation and the potential lack of secrecy is the over-heard information at the unintended parties, which wireless communication channel provides for free. It is well-established that users can help increase each others' rates by intelligently using their over-heard information. It is also well-accepted that the leakage of information through the over-heard signals may cause loss of confidentiality and secrecy. Cooperation and secrecy have been studied individually over the past three decades following the seminal papers of van der Meulen [1] who introduced the relay channel, which is the simplest model for cooperative communications and Wyner [2] who introduced the wire-tap channel, which is the simplest model to study secrecy in communications. It is interesting to note that, both of these are simple three-node networks, where in the former, the sole purpose of the third node (relay) is to increase the achievable rate of the single-user channel between the transmitter and the receiver by transmitting signals based on its over-heard information, while in the latter, the third node (eavesdropper) is a passive entity which uses its over-heard information to extract as much information as possible about the messages transmitted in the single-user communication channel between the transmitter and the receiver. In this chapter, we will summarize the mostly separate literatures on cooperation and secrecy.

More recently, there has been a tremendous amount of interest and some initial work on the interactions of cooperation and secrecy. The recent literature on the

S. Ulukus (✉)
Department of Electrical and Computer Engineering
University of Maryland, College Park
MD 20742, USA
e-mail: ulukus@umd.edu

*Portions of the material have appeared previously in “Secrecy in Cooperative Relay Broadcast Channels,” Proceedings of the IEEE International Symposium on Information Theory, 2008.
©IEEE 2008

interactions of cooperation and secrecy can be divided into two groups: the first group includes channel models where there is a group of cooperating partners (either in a basic relay network or in a multiple access channel) and a separate external eavesdropper. It is clear that the cooperation among the users can increase both the achievable rates and the secrecy of the transmitting user. As we will see, there are various ways in which users can cooperate when secrecy is one of the objectives of cooperation; for instance, users may cooperate by relaying/forwarding each others' messages or by explicitly jamming the external eavesdropper, both of which resulting in the effective end result of improving the communication quality of the main link with respect to the communication quality of the eavesdropping link. In this chapter, we will summarize the recent literature on cooperation to improve secrecy in the presence of an external eavesdropper.

Perhaps a more complex and practically more relevant set of interactions arise between cooperation and secrecy, when we consider channel models where the potential cooperating partners are also treated as potential eavesdroppers. In this model, all nodes are active participants of a network, and are motivated to improve each others' rates, however, would also like to keep their messages as confidential as possible. Practical examples could be imagined, for instance, where there is a broadcast network where it is in the network's interest to improve rates through cooperation, however, the content of the messages may be viewed only by certain authorized users (who might have paid for the service). The central question in this context is: is there a trade-off or a synergy between cooperation and secrecy, i.e., does cooperation cause additional leakage of information (in addition to what wireless communication channel already provides as a result of over-heard information), or can cooperation improve secrecy by limiting or reversing the leakage of information? Although the entire scope of interactions between cooperation and secrecy is not fully understood yet, our and other researchers' recent results suggest that, whether there is a trade-off or synergy between cooperation and secrecy depends on the form of cooperation protocol being used. Very briefly: if cooperation is accomplished via a decode-and-forward type method, i.e., if the cooperating party is allowed (or required) to decode the message it is supposed to forward, then, cooperation and secrecy may be conflicting goals, however, if we require the cooperating party to forward the message without decoding it, as in compress-and-forward and amplify-and-forward type schemes, then cooperation may improve secrecy. This is mainly because, with such cooperating strategies, a cooperating party would increase the rate of the main link to levels which are not decodable at the cooperating party itself. In this chapter, we will summarize the recent literature on the interactions of cooperation and secrecy when the legitimate users of the network are viewed as potential eavesdroppers.

7.2 Cooperation

The relay channel, which is the simplest model of a cooperative network, was introduced more than three decades ago by van der Meulen [1]. The relay channel, which is shown in Fig. 7.1, consists of three nodes: a transmitter, a relay, and a receiver.

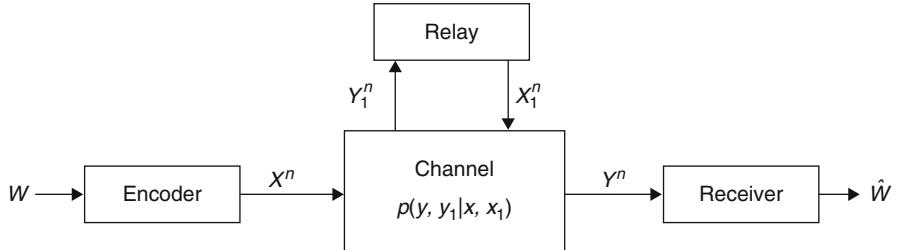


Fig. 7.1 The relay channel

The sole purpose of the relay node is to help increase the rate of communication between the transmitter and the receiver. Despite the simplicity of its model, the capacity of the general relay channel is still an open problem. The landmark paper on the relay channel is Cover and El Gamal's 1979 paper [3] which proposed the two basic cooperation strategies, which are still the best-known achievable schemes today: decode-and-forward (DAF) and compress-and-forward (CAF).

Both DAF and CAF are block coding schemes. In DAF, the relay decodes the message of the current block in its entirety and sends a cooperative signal in the next block, which helps the receiver to decode the message sent by the transmitter in the previous block. The original work of Cover and El Gamal uses irregular encoding (which refers to different codebook sizes at the transmitter and the relay), block Markov superposition encoding, random partitioning, and successive decoding. Later, Carleial [4] and Willems [5] showed that the same rates can be achieved using codebooks of identical sizes at the relay and the transmitter with sliding-window or backward decoding methods. DAF can achieve rates up to

$$\max_{p(x, x_1)} \min\{I(X; Y_1|X_1), I(X, X_1; Y)\} \quad (7.1)$$

The first term inside the min comes from the fact that the relay needs to decode the message in its entirety. The second term can be interpreted as the rate of a multiple access channel (MAC) from the transmitter and the relay to the receiver, where the two transmitters have a common message to send. This rate is achievable since the relay decoded the message sent by the transmitter, and therefore constructed a common message. The main drawback of DAF is that it restricts the overall achievable rate by the achievable rate of the transmitter-relay link. To overcome this difficulty, [3] proposed the CAF scheme.

In CAF, the relay node does not try to decode the message, instead it sends a quantized and compressed version of its observation to the receiver. The receiver exploits the statistical dependence of the channel outputs at the relay and the receiver to decode the message intended for it. In this case, the quality of the quantization and compression at the relay node plays a crucial role. This, in turn, depends on the rate of the relay-receiver link. For example, if the relay could convey its observation to the receiver perfectly (i.e., infinite-capacity relay-receiver link), then rates up to

$$\max_{p(x)} I(X; Y, Y_1) \quad (7.2)$$

would be achievable. This is the rate that would be achievable if the receiver had two antennas. Since the relay-receiver link is noisy, the achievable rate of the CAF scheme is smaller. The rates achievable by CAF are given as

$$\max_{p(x)p(x_1)} I(X; \hat{Y}_1, Y|X_1) \quad (7.3)$$

where the random variables in Eq. (7.3) are subject to the constraint

$$I(X_1; Y) \geq I(\hat{Y}_1; Y_1|X_1, Y) \quad (7.4)$$

where \hat{Y}_1 denotes the compressed version of Y_1 , the observation of the relay. The constraint in Eq. (7.4) relates the quality of compression to the rates achievable between the relay and the receiver. As we alluded to earlier, the main advantage of CAF is that the relay does not need to decode the message itself in order to help the receiver. This aspect of CAF will become crucial when we impose a secrecy constraint on the relay node.

In the basic relay network, we have a dedicated relay node whose sole purpose is to help increase the rate of the transmitter by utilizing its observation which is correlated with the transmitted message. This basic idea can be generalized to larger networks, where all nodes have their own messages to send, and have observations which are correlated with the transmitted messages of the other users in the network. The simplest such example is the multiple access channel with generalized feedback (MAC-GF), which is shown in Fig. 7.2, where each user has a different feedback signal which is correlated with the message of the other user. For this channel, strategies similar to DAF and CAF can be used, after appropriate modifications are done, so that the messages of the users are superimposed with the cooperative signals. This channel model was studied by King [6] and Cover and Leung [7] for the special case of common feedback, i.e., $Y_1 = Y_2 = Y^*$, and by Carleial [4] and Willems [5] for the general case of different feedback signals at the two transmitters. Achievable schemes presented in [4–7] basically rely on the DAF principle of [3], where both users decode (completely or partially) the cooperation signals. The differences in these papers lie in their encoding and decoding strategies. For example, Carleial uses regular encoding with sliding-window decoding, while Willems uses

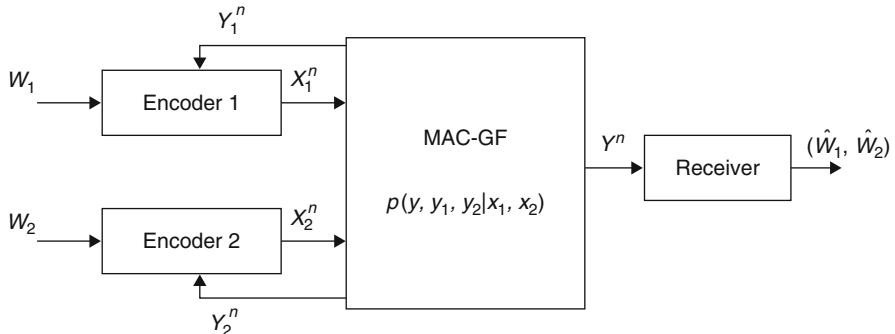


Fig. 7.2 MAC with generalized feedback

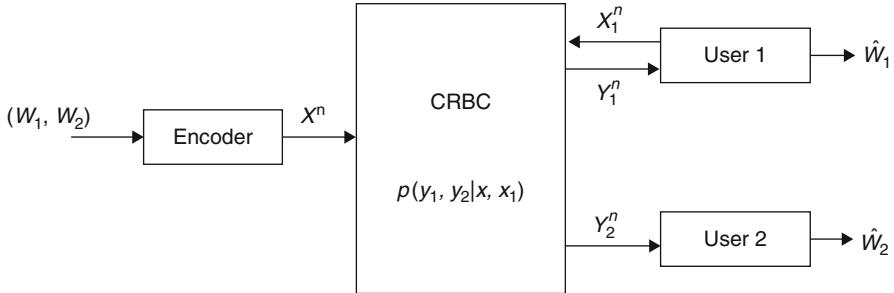


Fig. 7.3 Cooperative relay broadcast channel

regular encoding with backward decoding. In contrast to DAF, CAF has attracted less attention in the context of MAC-GF. References [8] and [9] consider CAF-type cooperation in MAC-GF. The relative performances of DAF and CAF in MAC-GF depends on many parameters. Generally speaking, if the inter-user links are relatively better than the user-receiver links, then DAF performs better, while if the user-receiver links are better than the inter-user links, then CAF performs better.

Recently, Sendonaris, Erkip, and Aazhang [10], employed DAF-based coding schemes developed for MAC-GF in fading cellular wireless communication systems to demonstrate significant gains in achievable rates, and introduced the concept of user cooperation diversity. More recently, [11] combined the concepts of user cooperation and power control to further improve rates with respect to the rates that are achievable by cooperation-only and power-control-only schemes; while user cooperation exploits spatial diversity and power control exploits time diversity in a fading wireless channel, the approach in [11] exploits both forms of diversity simultaneously.

The “dual” of MAC-GF is the broadcast channel with cooperating decoders, where the cooperation is done on the receiver side, using the links between the receivers. We will refer to this channel model as the cooperative relay broadcast channel (CRBC), see Fig. 7.3. Although Fig. 7.3 shows a one-sided cooperation link between the receivers, its extension to two-sided cooperation case is straightforward. This channel model was studied extensively in [12–14]. Similar to the basic relay channel model, since each user’s observation contains some information about the message intended for the other user, the users can serve as relays for each another. Hence, the basic DAF and CAF schemes can be modified accordingly to find achievable rates in this channel model as well.

7.3 Information Theoretic Secrecy

The first information theoretic treatment of communication secrecy is due to Wyner [2] who considered a wiretap channel, see Fig. 7.4, where there is a transmitter, a receiver and a wiretapper, which wants to extract as much information as possible about the ongoing legitimate communication, using its over-heard information.

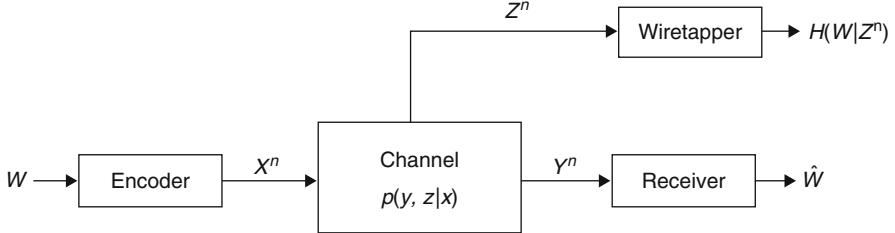


Fig. 7.4 The wiretap channel

Wyner considered a special kind of wiretap channel, called the degraded wiretap channel, where the signal that the wiretapper gets is a degraded version of the signal that the receiver observes. Wyner measured the secrecy of communication by the conditional entropy of the message given the channel output of the wiretapper. This quantity is termed as the equivocation-rate and is given by

$$\frac{1}{n} H(W_1|Z^n) \quad (7.5)$$

The equivocation-rate reflects the remaining uncertainty in the message given the wiretapper's channel observation. A rate pair (R_1, R_e) is said to be achievable if rate R_1 is achievable with vanishingly small probability of error while R_e satisfies

$$\lim_{n \rightarrow \infty} \frac{1}{n} H(W_1|Z^n) \geq R_e \quad (7.6)$$

When the equivocation-rate of the message is equal to the message rate, i.e., $R_1 = R_e$, we say that these rates are achievable with perfect secrecy. Correspondingly, the maximum of such rates is called the secrecy capacity. Wyner's wiretap channel is a degraded wiretap channel in the sense that the involved random variables satisfy the following Markov chain

$$X \rightarrow Y \rightarrow Z \quad (7.7)$$

For this channel, Wyner determined the rate equivocation-rate region, i.e., the set of all achievable (R_1, R_e) pairs. The secrecy capacity of this channel, i.e., the largest achievable R_1 such that $R_1 = R_e$, is

$$C^s = \max_{p(x)} I(X; Y|Z) = \max_{p(x)} [I(X; Y) - I(X; Z)] \quad (7.8)$$

where the second equality follows from the degradedness condition in Eq. (7.7). The secrecy capacity in Eq. (7.8) can be interpreted as being the largest difference between the receiver's and the wiretapper's achievable rates. Therefore, to be able to transmit all of its messages with perfect secrecy, the wiretapper needs to “sacrifice” the following amount of rate

$$I(X; Z) \quad (7.9)$$

from its otherwise achievable rate $I(X; Y)$. The rate in Eq. (7.9) that the transmitter should give up as the price for perfect secrecy corresponds to the amount of rate the wiretapper can decode.

Following Wyner's work, Csiszar and Korner [15] considered the general, not necessarily degraded, wiretap channel and found the rate equivocation-rate region. Csiszar and Korner consider a much general setup, where a transmitter not only wants to send a confidential message to one of the receivers, but also wants to send a common (public) message to both receivers. In this case, the eavesdropper may be thought of as another legitimate user in the system, in the sense that the transmitter wishes to send a message to it. Besides finding the capacity region of such a general wiretap channel, another important contribution of [15] is its converse technique, which in years since then, has been the standard method to prove converses in various secrecy problems. Yet another fundamental contribution of [15] is the introduction of an auxiliary random variable, which plays a crucial role in the secrecy of general, not necessarily degraded, wiretap channels. After showing that the following secrecy rates

$$I(X; Y) - I(X; Z) \quad (7.10)$$

are achievable with perfect secrecy for all $p(x)$, Csiszar and Korner introduce a memoryless channel with input V and outputs Y, Z . Since any encoder defined for this channel can be properly modified using the conditional distribution of X conditioned on V , this new channel can achieve the following secrecy rates

$$I(V; Y) - I(V; Z) \quad (7.11)$$

By the nature of the new channel from V to Y, Z , we need to have the following Markov chain satisfied

$$V \rightarrow X \rightarrow (Y, Z) \quad (7.12)$$

The operation of creation of V is referred to as "channel prefixing" and the processing from the message carrying signal V to the channel input X is called "pre-processing."

We note that Eq. (7.11) has the same interpretation as Eq. (7.8): it can be viewed as the maximum difference between the achievable rates of the receiver and the wiretapper, where now the maximum is taken over all channel input distributions $p(x)$ and pre-processing $p(x|v)$. This *stochastic* encoding from the message carrying signal V to the channel input X can be interpreted as introducing additional randomness to both channels, i.e., the main channel from X to Y and the eavesdropping channel from X to Z . Clearly, this additional randomness will hurt both of the achievable rates. This can be seen by observing that $I(V; Y) \leq I(X; Y)$ and $I(V; Z) \leq I(X; Z)$ from the data processing inequality [16] applied to the Markov chain in Eq. (7.12). The auxiliary random variable V will be useful in channels where the decrease in the rate due to the use of the auxiliary random variable is more in the eavesdropper link than in the main link.

We note that the selection of $V = X$ (i.e., no pre-processing) is in general potentially suboptimal. We also note that, despite this, for all the channels where secrecy capacity has been identified, e.g., the scalar Gaussian channel [17], the parallel Gaussian channel which also models the fading Gaussian wiretap channel where all the parties know the instantaneous realizations of all the fading channel gains [18, 19], and the MIMO Gaussian channel [20–22], this selection has been shown to be optimal. However, there are channels, such as the fading Gaussian wiretap channel without channel state information of the wiretapper at the transmitter [23], it was shown that choosing $V = X$ is strictly suboptimal. Finally, we note that, for some channels, the secrecy capacity is attained when both the main channel and the wiretapper channel operate at their own capacity achieving distributions, i.e., the $p(x)$ that maximizes the difference in Eq. (7.8) is the same as the $p(x)$ that maximizes $I(X; Y)$ and $I(X; Z)$ individually. The scalar Gaussian channel [17] is such an example. Note that this is not true for the MIMO Gaussian channel [20–22].

After the pioneering works in [2, 15], secrecy of multi-user systems has been studied only recently. Even though there has been a recent surge of papers on various aspects of multi-user secrecy, here, for the sake of compactness, we will only refer to the part of the literature which relates to the interactions of cooperation and secrecy. These works can be broadly classified into three groups.

The first group contains the works where cooperation is accomplished without the cooperating party using its over-heard information. This is different than the classical sense of cooperation, where the cooperating party uses its over-heard information to “strengthen” the main link. In this first group, the cooperating party improves the relative strength of the main link by weakening the eavesdropping link. We call this class of cooperation *oblivious cooperation* since the cooperating party does not use its over-heard information. We will further partition this group of works into two: in the first sub-group, cooperation is accomplished by cooperating user sending dummy codewords from a codebook, akin to Wyner’s idea of associating multiple codewords with a message. We will discuss this kind of cooperation under the title of *implicit cooperation and noise forwarding*. In the second sub-group, the cooperating party sends explicit jamming signals. This is akin to Csiszar and Korner’s idea of channel prefixing by introducing an auxiliary random variable. In Gaussian channels, the additional randomness that can be introduced by pre-processing from V to X can be interpreted as *jamming*. We will discuss this kind of cooperation under the title of *cooperative jamming and artificial noise*. Instances of such oblivious cooperation arise in the MAC with an external wiretapper (MAC-WT), the interference channel, and the relay-eavesdropper channel with an external eavesdropper, where the relay does not make use of its over-heard information. We will focus on these two kinds of oblivious cooperation in Sect. 7.4.

The second group contains the works where the cooperating party helps the main link in the classical sense of cooperation, i.e., it strengthens the main link by using its over-heard information. The basic channel model for this group is the relay-eavesdropper channel, where we have a standard relay channel and an external

eavesdropper. In this case, the relay node helps the transmitter-receiver pair by using DAF and CAF cooperation schemes. These schemes increase both achievable rates and the equivocation-rates. We will focus on this kind of active cooperation in Sect. 7.5.

The third group contains the works where secrecy constraints are placed on the cooperating parties themselves. The basic question here is: can an eavesdropper help increase the secrecy of a transmitter by sending cooperation signals? The basic channel models to investigate these seemingly contradicting goals of a relay node are the relay channel, MAC-GF and CRBC. We will focus on this kind of interaction between cooperation and secrecy in Sect. 7.6.

7.4 Oblivious Cooperation for Secrecy

In this section, we discuss cooperation strategies where the cooperating party (we will also refer to it as the helper) does not need to have any information regarding the transmitted message. Here, the helper either does not have a channel output (as in MAC-WT), or even if it does (as in the relay-eavesdropper channel), it ignores it. We will discuss two different cooperation strategies.

In the first one, the helper sends a portion of the dummy codewords that the transmitter needs to send to have secrecy. These dummy codewords refer to Wyner's idea of associating multiple codewords with a single message. Since the cost of these dummy codewords is a decrease in the transmitter's rate, if the helper takes the responsibility of sending these dummy codewords, then the secrecy rate of the transmitter may improve. The amount of improvement depends on the relative strengths of the helper-receiver and the helper-eavesdropper links. If the helper-receiver link is stronger, then the secrecy rate of the transmitter can be improved. However, if the helper-eavesdropper link is stronger, then, since the eavesdropper can decode these dummy codewords, the helper will not be able to improve the secrecy rate of the transmitter.

The second oblivious cooperation strategy we will discuss aims to overcome this drawback. If the helper-eavesdropper link is stronger, then the helper may more explicitly *attack* the eavesdropper. We note though that when the helper attacks the eavesdropper, by the broadcast nature of wireless communications, it attacks the main receiver as well. The hope of the helper is that even though it attacks both the eavesdropper and the main receiver, it hurts the eavesdropper more. In Gaussian channels, this attack can be in the form of injecting additional noise to the channel. In a more abstract level, the attack of the helper can be interpreted as sending independent codewords whose rate is above the decoding capability of both the eavesdropper and the receiver. In addition, this jamming attack can be interpreted as using an explicit auxiliary random variable in the achievable rates, as in the channel prefixing idea of Csiszar-Korner. As we alluded to earlier, the effect of the auxiliary random variable is to introduce additional randomness to both the eavesdropper and the main link; and in a Gaussian channel, jamming will correspond to a certain kind of auxiliary random variable selection, as we will show later.

7.4.1 Implicit Cooperation and Noise-Forwarding

In this section, we discuss the cooperation strategy where the helper sends a portion of the non-information-bearing codewords to improve the secrecy of the transmitter. This cooperation strategy can be used in MAC-WT where the helper does not have a channel output, or in the relay-eavesdropper channel where the helper (the relay) may not want to use its over-heard information. We will start with MAC-WT; see Fig. 7.5.

This channel model is first studied in [24, 25]. In this channel, in addition to equivocation-rates measuring each user's individual secrecy, we need to have a joint equivocation-rate to account for the loss of secrecy if the eavesdropper uses a joint decoding strategy

$$\frac{1}{n} H(W_1|Z^n), \quad \frac{1}{n} H(W_2|Z^n), \quad \frac{1}{n} H(W_1, W_2|Z^n) \quad (7.13)$$

where the last term will dictate that the message pair (W_1, W_2) should not be jointly decodable by the eavesdropper. Using these secrecy constraints, we can show that we have the following *perfect secrecy* achievable region

$$R_1 \leq [I(V_1; Y|V_2) - I(V_1; Z)]^+ \quad (7.14)$$

$$R_2 \leq [I(V_2; Y|V_1) - I(V_2; Z)]^+ \quad (7.15)$$

$$R_1 + R_2 \leq [I(V_1, V_2; Y) - I(V_1, V_2; Z)]^+ \quad (7.16)$$

for any distribution of the form

$$p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y, z|x_1, x_2) \quad (7.17)$$

where $(x)^+$ denotes $\max(0, x)$, and these rates are perfect secrecy rates in the sense that rates R_1 and R_2 are achievable with the equivocation-rates of $R_{e,1} = R_1$ and

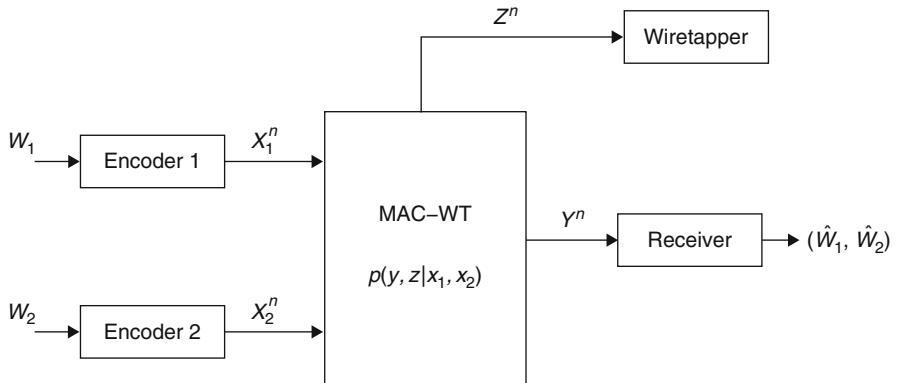


Fig. 7.5 MAC wiretap channel

$R_{e,2} = R_2$. The perfect secrecy rates in Eqs. (7.14–7.16) are the most general achievable rates for MAC-WT reported anywhere so far. Although we skip the details here, these rates can be obtained from the rates presented in [24, 25] by using channel prefixing and by introducing two independent auxiliary random variables V_1 and V_2 for users 1 and 2, respectively. The introduction of the auxiliary random variables is not trivial and it will play a crucial role in our exposition below, especially in the next section.

From a cooperation point of view, an interesting implication of the achievable region in Eqs. (7.14–7.16) is that it represents an *implicit cooperation* between users. To see this, assume that the rate pair (R_1, R_2) is on the sum-rate line. For users to operate on this line, they need to *jointly* “sacrifice” a total rate of

$$I(V_1, V_2; Z) \quad (7.18)$$

from their otherwise achievable sum-rate of $I(V_1, V_2; Y)$. However, how this total rate is shared among the users, i.e., how much rate each user has to give up is not clear at this point. To understand how this rate might be shared among the users, first note that the sum-rate line lies between the following two points:

$$\text{Point A: } R_1 = I(V_1; Y|V_2) - I(V_1; Z) \quad (7.19)$$

$$R_2 = I(V_2; Y) - I(V_2; Z|V_1) \quad (7.20)$$

$$\text{Point B: } R_1 = I(V_1; Y) - I(V_1; Z|V_2) \quad (7.21)$$

$$R_2 = I(V_2; Y|V_1) - I(V_2; Z) \quad (7.22)$$

If the system operates at Point A, then user 1 acts as if it is in a single-user wiretap channel and “sacrifices” a rate of

$$I(V_1; Z) \quad (7.23)$$

which also is the largest rate that the eavesdropper can decode without cancelling user 2’s signal. However, user 2, besides decreasing its achievable rate from a possible $I(V_2; Y|V_1)$ to $I(V_2; Y)$, also puts more dummy codewords to the channel, namely at the rate of $I(V_2; Z|V_1)$, to ensure that the sum-rate secrecy constraint is satisfied. If user 1 starts putting more dummy codewords to the channel, then user 2’s secrecy rate begins to increase, and the operating point moves away from Point A and eventually reaches Point B where the roles of the two users are reversed.

To solidify these ideas, let us introduce the Gaussian MAC-WT

$$Y = X_1 + X_2 + N_1 \quad (7.24)$$

$$Z = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_2 \quad (7.25)$$

where N_1, N_2 are independent zero-mean Gaussian random variables with unit-variance, h_1, h_2 denote the channel gains of the eavesdropper channel. Here, we will assume that h_1 and h_2 satisfy

$$h_1 \leq \frac{1}{1 + P_2}, \quad h_2 \leq \frac{1}{1 + P_1} \quad (7.26)$$

to ensure that both users have positive secrecy rates in their corresponding single-user channels, and that the region in Eqs. (7.14–7.16) takes the form of a non-degenerate pentagon. Moreover, we impose the usual power constraints on X_1, X_2 as $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$.

The optimal selection of the random variables V_1, V_2, X_1, X_2 in Eqs. (7.14–7.16) is an open problem. If we select both $V_1 = X_1$ and $V_2 = X_2$ (i.e., no pre-processing) and X_1 and X_2 to be Gaussian with zero-mean and variances P_1, P_2 , respectively, the rate region in Eqs. (7.14–7.16), becomes

$$R_1 \leq \frac{1}{2} \log(1 + P_1) - \frac{1}{2} \log\left(1 + \frac{h_1 P_1}{h_2 P_2 + 1}\right) \quad (7.27)$$

$$R_2 \leq \frac{1}{2} \log(1 + P_2) - \frac{1}{2} \log\left(1 + \frac{h_2 P_2}{h_1 P_1 + 1}\right) \quad (7.28)$$

$$R_1 + R_2 \leq \frac{1}{2} \log(1 + P_1 + P_2) - \frac{1}{2} \log(1 + h_1 P_1 + h_2 P_2) \quad (7.29)$$

For this selection of random variables, Point A is

$$\text{Point A: } R_1 = \frac{1}{2} \log(1 + P_1) - \frac{1}{2} \log\left(1 + \frac{h_1 P_1}{h_2 P_2 + 1}\right) \quad (7.30)$$

$$R_2 = \frac{1}{2} \log\left(1 + \frac{P_2}{P_1 + 1}\right) - \frac{1}{2} \log(1 + h_2 P_2) \quad (7.31)$$

where user 2 takes the responsibility of transmitting more of

$$\frac{1}{2} \log(1 + h_1 P_1 + h_2 P_2) \quad (7.32)$$

Consequently, operating at Point A, user 1 benefits from the presence of user 2. If the second user did not exist in the system, the maximum secrecy rate user 1 could achieve would be

$$\frac{1}{2} \log(1 + P_1) - \frac{1}{2} \log(1 + h_1 P_1) \quad (7.33)$$

which is strictly smaller than Eq. (7.30). This shows that although user 2 does not know anything about user 1's message, it can still help to improve user 1's secrecy rate by sending independent dummy codewords. The dummy codewords user 2 has, in effect, serves to "enlarge" the size of dummy codewords user 1 associates with any given message, as in the original idea of Wyner.

In the above example, we assumed that $h_1, h_2 < 1$ through Eq. (7.26) to ensure that each user had positive secrecy rates even without the help of the other user, i.e., in a corresponding single-user channel. Let us now look at another case, where one of the users does not have positive secrecy in the absence of the other user. In particular, let us assume that $h_1 > 1$. From Eq. (7.33), it is clear that user 1 cannot have a positive secrecy rate in its corresponding single-user channel. This is

essentially because, the rate user 1 has to “sacrifice” in order to have perfect secrecy, i.e., $(1/2) \log(1 + h_1 P_1)$ is larger than the rate its main receiver can “afford”, i.e., $(1/2) \log(1 + P_1)$. However, if we can get user 2 to carry the responsibility of some of the rate to be “sacrificed,” then we may be able to provide positive secrecy rate for user 1.

To demonstrate that, let us assume that $h_2 < 1$, i.e., user 2 is able to have a positive secrecy rate in the absence of user 1. Since user 2’s overall link is better than user 1’s, user 2 can pay a portion of the rate to be “sacrificed.” Furthermore, if h_1, h_2 satisfy

$$h_1 \leq 1 + h_2 P_2, \quad h_2 \leq \frac{1}{1 + P_1} \quad (7.34)$$

both rates in Eq. (7.30) and in Eq. (7.31) will be positive. Thus, this example demonstrates that, although user 1 cannot have a positive secrecy rate in its corresponding single-user channel, user 2 can help it to have a positive secrecy rate by taking the responsibility of “confusing” the receiver on user 1’s behalf. We remark that for this type cooperation to be effective, the helper’s link to the receiver should be stronger than its link to the eavesdropper. For example, if we had $h_1, h_2 > 1$, then sum-rate would vanish with this kind of scheme and no one can have positive secrecy.

In the above examples, we assumed $V_1 = X_1$, $V_2 = X_2$ and X_1, X_2 are Gaussian random variables. As a more general comment, we can say that, if for every V_2 , we have

$$I(V_2; Y) \leq I(V_2; Z) \quad (7.35)$$

then the eavesdropper can decode whatever user 2 sends, and consequently, its taking part in the transmission of user 1’s dummy codewords cannot provide any gain for the secrecy of user 1. Nevertheless, to summarize the discussion above, with the achievable rates in Eqs. (7.14–7.16) (which are in general sub-optimal), and with the selection of random variables as $V_1 = X_1$, $V_2 = X_2$ and X_1, X_2 as Gaussian (which are also sub-optimal), the existence of user 2 in the system may improve the single-user perfect secrecy rate of user 1 (as in the first example), and provide a positive perfect secrecy to user 1, even when the single-user perfect secrecy rate of user 1 is zero (as in the second example).

A technique called *noise forwarding* is proposed in [26], where in a relay eavesdropper channel (see Fig. 7.6), the relay disregards its channel observation, and sends dummy codewords from a codebook. The ultimate receiver performs successive decoding, where it first decodes the dummy codeword of the relay, and then decodes the message of the transmitter. It was shown in [26] that the following perfect secrecy rate is achievable

$$\begin{aligned} & I(V_1; Y|V_2) + \min [I(V_2; Y), I(V_2; Z|V_1)] \\ & - \min [I(V_2; Y), I(V_2; Z)] - I(V_1; Z|V_2) \end{aligned} \quad (7.36)$$

for any joint distribution of the form

$$p(v_1)p(v_2)p(x|v_1)p(x_1|v_2)p(y, y_1, z|x, x_1) \quad (7.37)$$

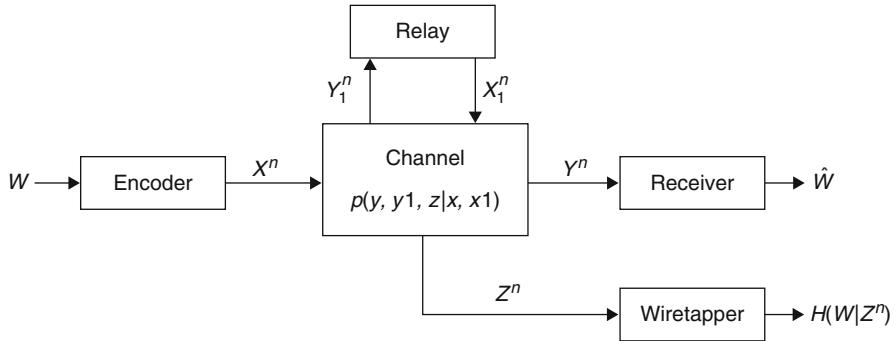


Fig. 7.6 Relay-eavesdropper channel

An alternative decoding strategy for the receiver could be a joint decoding strategy, in which case, the following perfect secrecy rate can be shown to be achievable

$$R_1 \leq I(V_1; Y|V_2) - I(V_1; Z) \quad (7.38)$$

$$R_1 \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \quad (7.39)$$

for any joint distribution of the form given in Eq. (7.37). We note that the rates in Eqs. (7.38, 7.39) can be obtained from Eqs. (7.14–7.16) by setting $R_2 = 0$. Therefore, we conclude that, the noise forwarding scheme proposed in [26] can be interpreted as an implicit cooperation scheme which is described above. References [27, 28] combine *implicit cooperation* with more explicit *jamming-type* cooperative strategies that we will discuss in the next section, to come up with achievable schemes for the interference channel (see Fig. 7.7), where one of the users does not have a message to send but acts as a pure interferer for both receivers.

Finally, we note that for the rates in Eq. (7.36) and in Eqs. (7.38, 7.39) to be larger than

$$I(V_1; Y|V_2) - I(V_1; Z|V_2) \quad (7.40)$$

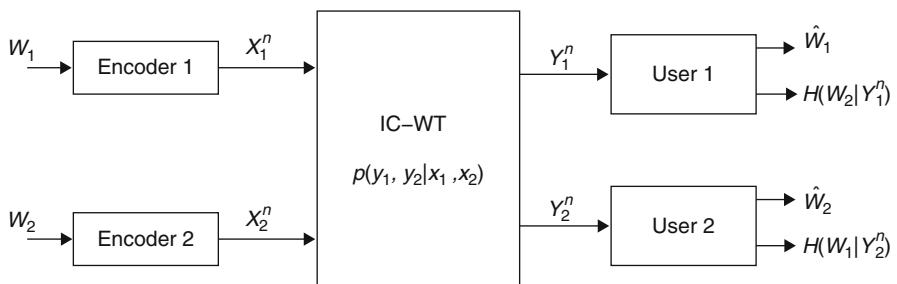


Fig. 7.7 Interference channel with confidential messages

which is the rate obtained when both the eavesdropper and the receiver are able to decode the relay's dummy codewords, we need

$$I(V_2; Z) \leq I(V_2; Y) \quad (7.41)$$

which is equivalent to saying that the helper-receiver link is stronger than the helper-eavesdropper link. Thus, if the helper-eavesdropper link is stronger than the helper-receiver link, then this kind of *implicit* cooperation strategies may not improve the secrecy rates. In such cases, we need more *explicit* cooperation strategies, which can be interpreted as *jamming*, which we will discuss in detail in the next section.

7.4.2 Cooperative Jamming and Artificial Noise

In the previous section, we assumed that at least one of the users has a relatively stronger channel to the main receiver and it was able to help the other user by sending dummy codewords, which had the end effect of enlarging the dummy codebook size of the user being helped. We now move on to an opposite situation and ask whether the user with a relatively weaker main channel can help the other user. To gain insight, we consider the Gaussian MAC-WT with $h_1 < 1 < h_2$. Here, user 2 is the weaker of the two users. We go back to the set of achievable secrecy rates in MAC-WT given in Eqs. (7.14–7.16), and pick the random variables as $X_1 = V_1$ and $X_2 = U_2$, where V_1 and U_2 are independent Gaussian random variables with zero-mean and variances P_1 and P_2 , respectively, and are independent of V_2 . With this selection, the achievable secrecy rate for user 1 given in Eq. (7.14) becomes

$$\frac{1}{2} \log \left(1 + \frac{P_1}{P_2 + 1} \right) - \frac{1}{2} \log \left(1 + \frac{h_1 P_1}{h_2 P_2 + 1} \right) \quad (7.42)$$

as compared to its single-user perfect secrecy rate

$$\frac{1}{2} \log (1 + P_1) - \frac{1}{2} \log (1 + h_1 P_1) \quad (7.43)$$

We note that the rate in Eq. (7.42) is strictly larger than the rate in Eq. (7.43) for certain range of values for h_1 and h_2 . Furthermore, if we select the channel gains as $1 < h_1 < h_2$, then the rate in Eq. (7.43) is negative while the rate in Eq. (7.42) can be positive.

This strategy was proposed in [25] and was named *cooperative jamming*. Reference [25] uses a Wyner-type achievable scheme with Gaussian signalling and does not employ auxiliary random variables. After observing that, in a situation where $h_2 > 1$, the second user cannot have positive secrecy, [25] proposes that, user 2 may transmit Gaussian noise to jam the eavesdropper, and in effect, help the first user, hence the name *cooperative jamming*. As noted in [25], this jamming will hurt both the eavesdropper and the main receiver due to the broadcast nature of wireless communications, and it will result in an improvement in the secrecy rate of user 1, if

it hurts the eavesdropper more. In the above discussion, we showed that cooperative jamming can be extracted via a special kind of auxiliary random variable selection from our achievable rates in Eqs. (7.14–7.16).

As a possible extension, one can consider “mixed” auxiliary random variable selection as $X_1 = V_1 + U_1$ and $X_2 = V_2 + U_2$, where V_1, U_1, V_2 and U_2 are all independent Gaussian random variables with variances $\alpha P_1, (1 - \alpha)P_1, \beta P_2$ and $(1 - \beta)P_2$, respectively, where $0 \leq \alpha, \beta \leq 1$. Note that, with this selection, the powers of X_1 and X_2 come out to be P_1 and P_2 . This selection corresponds to each transmitter dividing its signal into two: a component that carries the message (V_i) and a component that jams the channel (U_i). We note that all transmission schemes discussed so far can be viewed as special case of this general scheme where we took α and β to be either 0 or 1. We need to note that this mixed strategy of joint signal transmission and jamming does not improve the rates achievable by Eqs. (7.14–7.16), i.e., if we insert these “mixed” random variables into the achievable rates in Eqs. (7.14–7.16) and optimize the achievable rates over all α, β in $[0, 1]$, we observe that we should choose α and β to be either 0 or 1. This means that each user should either send a useful message without pre-processing, or it should send complete jamming signal without any signal component [25].

Similar ideas have been developed in the context of the interference channel with secrecy constraints. Consider the interference channel shown in Fig. 7.7 where there are two transmitters and two receivers, and each transmitter wishes to communicate with one of the receivers treating the other receiver as an eavesdropper. Reference [29] showed that the following set of rates are achievable with perfect secrecy

$$R_1 \leq I(V_1; Y_1) - I(V_1; Y_2|V_2) \quad (7.44)$$

$$R_2 \leq I(V_2; Y_2) - I(V_2; Y_1|V_1) \quad (7.45)$$

for any joint distribution of the form

$$p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2) \quad (7.46)$$

To understand how previous cooperation strategy can be effective in this channel, let us introduce the Gaussian interference channel

$$Y_1 = X_1 + \sqrt{\alpha_1}X_2 + N_1 \quad (7.47)$$

$$Y_2 = \sqrt{\alpha_2}X_1 + X_2 + N_2 \quad (7.48)$$

where N_1, N_2 are zero-mean, unit-variance Gaussian random variables. Moreover, we again have power constraints on X_1, X_2 as $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$.

To see how a jamming strategy can improve the rates in this case, let us first assume that both users send only their useful messages using Gaussian codebooks, i.e., let us pick $V_1 = X_1$ and $V_2 = X_2$ and X_1 and X_2 to be Gaussian with zero-mean and variances of P_1 and P_2 , respectively. This selection leads to the following rate

region

$$R_1 = \frac{1}{2} \log \left(1 + \frac{P_1}{\alpha_1 P_2 + 1} \right) - \frac{1}{2} \log (1 + \alpha_2 P_1) \quad (7.49)$$

$$R_2 = \frac{1}{2} \log \left(1 + \frac{P_2}{\alpha_2 P_1 + 1} \right) - \frac{1}{2} \log (1 + \alpha_1 P_2) \quad (7.50)$$

Now, let us assume that user 2's signal has a partial jamming component, which can be achieved by choosing $X_1 = V_1$ and $X_2 = V_2 + U_2$ where V_1 , V_2 , and U_2 are independent zero-mean Gaussian random variables with variances P_1 , βP_2 , $(1 - \beta)P_2$, respectively, and $0 \leq \beta \leq 1$. Then, the achievable rate region becomes

$$R_1 = \frac{1}{2} \log \left(1 + \frac{P_1}{\alpha_1 P_2 + 1} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha_2 P_1}{(1 - \beta)P_2} \right) \quad (7.51)$$

$$R_2 = \frac{1}{2} \log \left(1 + \frac{\beta P_2}{(1 - \beta)P_2 + \alpha_2 P_1 + 1} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha_1 P_2}{(1 - \beta)P_2 + 1} \right) \quad (7.52)$$

We observe that with this selection of random variables user 2 has increased the secrecy rate of user 1. We also note that user 2 accomplished this by jamming its own receiver. In [29], authors call this strategy *artificial noise*.

Both *cooperative jamming* and *artificial noise* can be generalized to arbitrary (not necessarily Gaussian) channels [27, 28]. In fact, injecting additional Gaussian noise into Gaussian channels can be thought of as sending dummy codewords whose rate is above the decoding capability of both the eavesdropper and the receiver. Since neither receiver can decode and remove the dummy codeword from the received signal, the end result of this strategy becomes making both channels noisier than they actually are.

In conclusion, in this section, we reviewed two *oblivious* cooperation techniques where a cooperating partner helps increase the secrecy rate of another user without knowing anything about the signal transmitted by that user. In the first one, the helper sends dummy codewords from a codebook. The rate of these dummy codewords is chosen such that the receiver is able to decode them. Consequently, this strategy improves the secrecy of the user when the helper-receiver link is stronger than the helper-eavesdropper link. In the second one, the helper sends explicit jamming signals. This strategy is equivalent for the helper to send dummy codewords whose rate is larger than the decoding capability of both the eavesdropper and the receiver. Therefore, this strategy is effective when the helper-eavesdropper link is stronger than the helper-receiver link.

7.5 Active Cooperation for Secrecy

In the previous section we reviewed cooperation schemes where the cooperating parties help the main receiver by weakening the eavesdropping link without using any knowledge of the message being transmitted. In this section we will review

cooperation schemes where the cooperating parties will help the main receiver by strengthening the main link by relaying the message. Therefore, the cooperation in this section will be *active* and it will use the over-heard information of the cooperating party.

To this end, we consider the relay-eavesdropper channel (see Fig. 7.6) which was considered in [26] and [30]. In the relay-eavesdropper channel, the relay node will use DAF and CAF methods to strengthen the main link. If the relay uses DAF, then the following secrecy rates are achievable

$$\min [I(V_1, V_2; Y), I(V_1; Y_1|V_2)] - I(V_1, V_2; Z) \quad (7.53)$$

for any joint distribution of the form

$$p(v_1, v_2)p(x, x_1|v_1, v_2)p(y, y_1, z|x, x_1) \quad (7.54)$$

The first term in Eq. (7.53) is simply the achievable rate of the relay channel when the relay uses DAF, and the second term is the rate that the eavesdropper can extract simultaneously from the relay and the transmitter.

Similar to the relay channel without an eavesdropper, the effectiveness of DAF depends on the quality of the transmitter-relay link as the overall rate is limited by the rate of this link. Besides that, in the relay-eavesdropper channel, the relative strengths of the relay-receiver and the relay-eavesdropper links become critical. For example, if the relay-eavesdropper link is stronger than the relay-receiver link, then all of the cooperative information sent by the relay will be decodable by the eavesdropper. In this case, the relay may not improve the secrecy of the transmitter. Consequently, for DAF to be effective in the relay-eavesdropper channel, not only that the relay-transmitter link should be stronger than the transmitter-receiver link, but also the relay-receiver link should be stronger than the relay-eavesdropper link.

To solidify ideas, let us assume that for every V_2 satisfying the Markov chain

$$V_2 \rightarrow (X, X_1) \rightarrow (Y, Y_1, Z) \quad (7.55)$$

we have

$$I(V_2; Y) \leq I(V_2; Z) \quad (7.56)$$

which is similar to the definition of *less noisy* channel [15]. This condition implies that the relay-eavesdropper link is stronger than the relay-receiver link. For such channels, achievable secrecy rate given in Eq. (7.53) can be upper bounded as

$$\min [I(V_1, V_2; Y), I(V_1; Y_1|V_2)] - I(V_1, V_2; Z) \leq I(V_1, V_2; Y) - I(V_1, V_2; Z) \quad (7.57)$$

$$\leq I(V_1; Y|V_2) - I(V_1; Z|V_2) \quad (7.58)$$

The upper bound in Eq. (7.58) corresponds to the case when both the eavesdropper and the receiver are able to decode the signal of the relay. Hence, in a channel where

the relay-eavesdropper link is strong, e.g., as in Eq. (7.56), DAF will not be able to improve the secrecy of the transmitter. This shows that the effectiveness of DAF for secrecy purposes depends on the position of the relay node in the corresponding network topology.

CAF can also be used for the relay-eavesdropper channel as it is done in [26] to improve the quality of the main link. It is well-known that CAF performs better than DAF in the relay channel when the transmitter-relay link is worse than the transmitter-receiver link. To judge the effectiveness of CAF in the relay-eavesdropper channel, we again need to consider the relative strengths of the relay-receiver and the relay-eavesdropper links. If the relay-eavesdropper link is stronger, then CAF may not lead to an increase in the secrecy, similar to the DAF case. Moreover, in this case, noise forwarding will not improve secrecy either. In this case, the most effective method the relay can employ may be cooperative jamming, as in this case the relay may harm the eavesdropper more than it harms the receiver.

As an example, let us introduce the Gaussian relay-eavesdropper channel:

$$Y = X + X_1 + N_1 \quad (7.59)$$

$$Y_1 = \sqrt{h_1}X + X_1 + N_2 \quad (7.60)$$

$$Z = \sqrt{h_2}X + \sqrt{h_3}X_1 + N_z \quad (7.61)$$

where h_1, h_2, h_3 are the channel gains and N_1, N_2, N_3 are independent Gaussian random variables with zero-mean and unit-variance. Let us also assume that $h_1 \leq 1 \leq h_2 \leq h_3$, i.e., the transmitter-relay link is worse than the transmitter-receiver-link, and the eavesdropper is close to the transmitter and the relay.

First, we note that if the relay does not transmit anything, then the corresponding secrecy rate of the transmitter is 0, because $1 < h_2$. Now, let us investigate how relay might help. If we compute the secrecy rate achievable by DAF with the selection of $V_1 = X$, $V_2 = X_1$ and X and X_1 to be Gaussian with zero-mean, variances of P_1 and P_2 , respectively, and having a correlation coefficient of ρ , we get

$$\frac{1}{2} \log(1 + h_1(1 - \rho^2)P_1) - \frac{1}{2} \log\left(1 + h_2P_1 + h_3P_2 + 2\rho\sqrt{h_2h_3}\sqrt{P_1P_2}\right) \quad (7.62)$$

We note that the expression in Eq. (7.62) is less than 0, and therefore, DAF cannot provide a positive secrecy rate for the transmitter with this selection of random variables. In addition, if we use noise forwarding, and pick the random variables in Eq. (7.36) as $V_1 = X$, $V_2 = X_1$ and X and X_1 to be independent Gaussian with zero-mean, variances of P_1 and P_2 , we cannot have any positive secrecy either.

On the other hand, if we select $V_1 = X$ and $X_1 = U$ where X and U are independent (and independent of V_2) Gaussian with zero-mean and variances of P_1 and P_2 , respectively, for either DAF or noise forwarding, we get

$$\frac{1}{2} \log\left(1 + \frac{P_1}{1 + P_2}\right) - \frac{1}{2} \log\left(1 + \frac{h_2P_1}{1 + h_3P_2}\right) \quad (7.63)$$

which is positive if the power of the relay satisfies

$$P_2 \geq \frac{h_2 - 1}{h_3 - h_2} \quad (7.64)$$

Thus, this selection of auxiliary random variables, which in fact implements *cooperative jamming* in a relay-eavesdropper channel, can yield positive secrecy rates.

So far, in this section, we discussed the ways in which a relay node can help increase the secrecy of a transmitter by strengthening the main link by using DAF and CAF. As suggested by [31], the relay may be captured by an adversary and may be forced to help the eavesdropper. In that case as well, one can come up with cooperation strategies by which the relay helps the eavesdropper, as discussed in [31]. Moreover, the relay-eavesdropper channel can be generalized to a two-sided cooperation channel as is done in [32]. In [32], there is an external eavesdropper in a MAC-GF. Reference [32] uses the cooperation method of [5] for MAC-GF which is a generalization of DAF.

7.6 Untrusted Helpers

In previous sections, we discussed the effectiveness of cooperation among a set of nodes against an external eavesdropper. In this section, we will discuss the interactions that arise between cooperation and secrecy, when the eavesdropper is not an external entity. In this section, the eavesdropper will be a member of the network, and we will ask if utilizing the eavesdropper as a cooperating partner will reduce the secrecy of the main link further or if it will improve it.

The basic models to study these interactions are the simple three-node relay channel, MAC-GF and CRBC. In the relay channel case, we treat the relay also as an eavesdropper, and ask the question: can the relay node improve the equivocation-rate of the transmitter measured at the relay by putting cooperation signals into the channel? Note that, in this channel model, we are able to observe the effects of the relay's actions on the secrecy of the transmitter. In MAC-GF and CRBC channel models, we have the added opportunity of studying the effects of a relaying node's actions on the equivocation-rates of not only the transmitting node, but also the relaying node itself. In particular, in MAC-GF, both users treat each other as cooperating partners as well as eavesdroppers. There, we observe the effects of user 1's actions on the secrecy of user 2 as well as on the secrecy of user 1 itself. In CRBC, the setting is reversed, in the sense that the cooperation (and also eavesdropping) take place at the receiver end. Here also, we observe the actions of receiver 1 (which also relays signals to receiver 2) on the secrecy of the messages sent to receiver 1 and the secrecy of the messages sent to receiver 2.

7.6.1 Relay Channel with Secrecy Constraints

Here we consider a basic three-node relay network, as shown in Fig. 7.1. The transmitter wishes to communicate with the receiver at the highest possible reliable rate, R_1 . The goal of the relay node is to assist this communication. At the same time, the relay node acts as an eavesdropper. Therefore, we measure the secrecy of the communication by the equivocation-rate of the message measured at the relay node

$$\frac{1}{n} H(W|Y_1^n, X_1^n) \quad (7.65)$$

The overarching goal is to characterize all achievable (R_1, R_e) pairs which will be spanned by tracing all possible actions of the relay node. This is a very difficult problem, and we will provide only a partial characterization.

This problem was first addressed in [33]. In the model of [33], the transmitter sends a common message to both the relay and the receiver, and also a confidential message to the receiver. Achievable schemes presented [33] rely on the DAF technique. In particular, the relay uses a partial DAF strategy where the common message and a part of the confidential message is decoded and forwarded to the receiver. The secrecy rate achieved by this scheme is

$$I(V; Y|X_1) - I(V; Y_1|X_1) \quad (7.66)$$

where V is a random variable that satisfies the Markov chains

$$V \rightarrow (X, X_1) \rightarrow (Y, Y_1) \quad \text{and} \quad X_1 \rightarrow V \rightarrow X \quad (7.67)$$

We note that the rate in Eq. (7.66) is exactly the secrecy rate achievable in the underlying wiretap channel. This can be seen by noting the conditioning to X_1 of both mutual information terms has the effect of removing the signal of the relay node from the received signals Y_1 and Y . This removes the channel input of the relay channel from the system, and the channel model becomes exactly that of the wiretap channel. Therefore, we conclude that as long as the relay node uses a DAF-type cooperation, even though it can increase the achievable rate of the transmitter, it does not increase the secrecy rate of the transmitter. This conclusion is quite intuitive, because although the relay node can increase the rate of the transmitter, it cannot increase it beyond the amount that it itself can decode. Consequently, the secrecy rate, which is, roughly speaking, the difference between the rates of the receiver and the eavesdropper (relay in this case), cannot be increased if the relay node uses a DAF-type cooperation strategy.

To gain more insight let us consider the Gaussian relay channel:

$$Y = X + X_1 + Z_1 \quad (7.68)$$

$$Y_1 = X + Z_2 \quad (7.69)$$

where Z_1, Z_2 are independent Gaussian random variables with zero-mean and variances of N_1 and N_2 , respectively. In addition, we have the usual power constraints: $E[X^2] \leq P_1$ and $E[X_1^2] \leq P_2$. The achievable rate in Eq. (7.66) yields [33]

$$\frac{1}{2} \log \left(1 + \frac{P_1}{N_1} \right) - \frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right) \quad (7.70)$$

This is also exactly equal to the secrecy rate achievable in the underlying wiretap channel, i.e., the achievable secrecy rate when the relay is not transmitting. Consequently, when $N_1 > N_2$, i.e., when the relay (eavesdropper) has a better channel than the receiver, this rate vanishes. Consequently, DAF-based relaying does not help as far as secrecy is concerned.

Reference [33] also provided outer bounds for the secrecy capacity. The upper bound [33] gave for the secrecy rate evaluates to

$$\frac{1}{2} \log \left(1 + \frac{P_1}{N_1} + \frac{P_1}{N_2} \right) - \frac{1}{2} \log \left(1 + \frac{P_1}{N_2} \right) \quad (7.71)$$

for the Gaussian relay channel under consideration. We note that this upper bound does not vanish when $N_1 > N_2$. Although this outer bound does not lead us to the ultimate achievable secrecy rate, at least, it does not preclude the transmitter node to have secret communication when the relay (eavesdropper) has a better channel. Therefore, it leaves it a possibility that secret communication may be attained by using cooperation schemes other than DAF.

The interaction of cooperation and secrecy has been further studied in [34] focusing on two special classes of the relay channel. In the first special class, there is an orthogonal link between the transmitter and the relay and there is a MAC from the transmitter and the relay to the receiver. The capacity of this relay channel was found in [35]. In [34], the secrecy capacity of this channel is determined. Since the orthogonal link between the transmitter and the relay does not interfere with the rest of the channel, [34] finds that all of the confidential information should be sent without using this orthogonal link. Hence, for this channel, the relay is found to be useless from the secrecy point of view.

In the second special class considered in [34], there is an orthogonal link between the relay and the receiver, and the transmitter has a broadcast channel to the relay and the receiver. Reference [34] proposed to use CAF for this channel and analyzed its performance. The CAF-based cooperation scheme is not specific to this channel model, and can be used in any relay channel. The secrecy rate achievable by CAF is found as

$$I(X; Y, \hat{Y}_1|X_1) - I(X; Y_1|X_1) \quad (7.72)$$

where the random variables in Eq. (7.72) are subject to the constraint

$$I(X_1; Y) \geq I(\hat{Y}_1; Y_1|Y, X_1) \quad (7.73)$$

and X and X_1 are independent. The secrecy rate in Eq. (7.72) can be decomposed as

$$[I(X; Y|X_1) - I(X; Y_1|X_1)] + I(X; \hat{Y}_1|X_1, Y) \quad (7.74)$$

where the first term may be viewed as the secrecy rate of the underlying wiretap channel, and the second term may be interpreted as the additional secrecy rate CAF-based cooperation provides. Consequently, if this second term is non-negative, then the relay, by employing CAF, not only improves the rate of the transmitter, but also improves the secrecy rate of the transmitter.

To examine this possibility in more depth, let us focus on the special class of Gaussian relay channel considered in [34]. In this channel, the receiver observes $Y = (Y_t, Y_r)$, where

$$Y_t = X + Z_t \quad (7.75)$$

$$Y_r = bX_1 + Z_r \quad (7.76)$$

$$Y_1 = aX + Z_1 \quad (7.77)$$

where Z_t, Z_r, Z_1 are independent Gaussian random variables with zero-mean and unit-variance. We also assume $E[X^2] \leq P$ and $E[X_1^2] \leq P$. For this channel, CAF yields the following the secrecy rate

$$\frac{1}{2} \log \left(1 + P + \frac{a^2 P}{1 + N_c} \right) - \frac{1}{2} \log \left(1 + a^2 P \right) \quad (7.78)$$

where N_c is given by

$$N_c = \frac{(a^2 + 1) P + 1}{b^2 P(P + 1)} \quad (7.79)$$

The rate in Eq. (7.78) is obtained from Eqs. (7.72) and (7.73) and using independent Gaussian channel inputs. The compressed signal is selected as $\hat{Y}_1 = Y_1 + Z_c$, where Z_c is the compression noise that is Gaussian with zero-mean and variance of N_c , which is chosen to meet the constraint in Eq. (7.73). We can now compare the rate given in Eq. (7.78) with the corresponding wiretap channel, where the relay node does not transmit a signal. We first note that, in the corresponding wiretap channel, secrecy rate is zero whenever $a > 1$. However, the rate in Eq. (7.78) can be positive even when $a > 1$ if b is sufficiently large, i.e., if the relay-receiver link is strong enough. Although we considered a special class of relay channels in this example, the same conclusion holds for the general Gaussian relay channel in Eqs. (7.68, 7.69). Specifically, the examples provided for the Gaussian MAC-GF and CRBC in the next two sections highlight this fact since these channels subsume the Gaussian relay channel.

In conclusion, we observed that CAF can increase the secrecy rate with respect to the underlying wiretap channel. The basic reason for this is that, using CAF, the relay node can increase the overall achievable rate of the network to levels which are not decodable at the relay node. This, in effect, increases the difference of the rates in the transmitter-relay and transmitter-receiver links, which, roughly speaking, corresponds to the secrecy rate.

7.6.2 MAC-GF with Confidential Messages

In this section, we consider MAC-GF, shown in Fig. 7.2, where both users have their own messages to send, and they both receive feedback signals that are correlated with the message of the other user. These signals can be used to cooperate and increase the rates; however, these signals are also the basis for loss of secrecy. In this section, each user will consider the other user both as a cooperating partner and also as an eavesdropper. This channel model can be considered as a two-sided version of the relay channel, where the relaying nodes have their own messages as well. There are two rates, R_1 and R_2 , and two equivocation-rates $R_{e,1}$ and $R_{e,2}$. Our main motivation to study this channel model is to understand the implications of the actions (i.e., cooperation) of one user on the rate and secrecy of the other user, as well as on the rate and secrecy of itself. This could not be studied in the classical relay channel, as the relay node does not have its own messages, and therefore, its own rate and equivocation-rate.

MAC-GF was studied from a secrecy point of view in [36, 37], and [38]. References [36] and [37] did not use the feedback signals in their encoding functions, i.e., the users were not allowed to cooperate. Consequently, the only effect of the feedback signals in [36, 37] was the loss of secrecy. Reference [38], on the other hand, allows the encoding functions to depend on the feedback signals, i.e., it allows users to cooperate, and it investigates the effects of cooperation on the secrecy of the users. We know that both DAF and CAF can be used as methods of cooperation, and they would both increase the achievable rates. However, as observed in the relay channel as well, DAF is not likely to improve the secrecy rates. CAF, on the other hand, is likely to improve the secrecy rates of the users. We show in [38] that the following secrecy rates are achievable if both users employ CAF-based cooperation

$$R_1 \leq R'_1 - I(X_1; Y_2, \hat{Y}_1 | U_1, U_2, X_2) \quad (7.80)$$

$$R_2 \leq R'_2 - I(X_2; Y_1, \hat{Y}_2 | U_1, U_2, X_1) \quad (7.81)$$

where the pairs (R'_1, R'_2) belong to

$$\mathcal{C}_2(R_1, R_2) = \left\{ \begin{array}{l} R'_1 \leq I(X_1; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2, X_2) \\ R'_2 \leq I(X_2; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2, X_1) \\ R'_1 + R'_2 \leq I(X_1, X_2; Y, \hat{Y}_1, \hat{Y}_2 | U_1, U_2) \end{array} \right\} \quad (7.82)$$

for any distribution of the form

$$\begin{aligned} & p(u_1)p(x_1|u_1)p(\hat{y}_1|u_1, x_1, y_1)p(u_2)p(x_2|u_2) \\ & p(\hat{y}_2|u_2, x_2, y_2)p(y, y_1, y_2|x_1, x_2) \end{aligned} \quad (7.83)$$

subject to the constraints

$$I(\hat{Y}_1; Y_1|U_1, X_1) \leq I(U_1, \hat{Y}_1; Y|U_2) \quad (7.84)$$

$$I(\hat{Y}_2; Y_2|U_2, X_2) \leq I(U_2, \hat{Y}_2; Y|U_1) \quad (7.85)$$

$$\begin{aligned} I(\hat{Y}_1; Y_1|U_1, X_1) + I(\hat{Y}_2; Y_2|U_2, X_2) &\leq I(U_1, U_2; Y) + I(\hat{Y}_1; Y|U_1, U_2) \\ &\quad + I(\hat{Y}_2; Y|U_1, U_2) \end{aligned} \quad (7.86)$$

To examine whether this achievable scheme enlarges the secrecy region of MAC-GF with respect to the case where feedback signals are not used, i.e., users are not allowed to cooperate, we will evaluate the region given by Eqs. (7.80–7.86) for the Gaussian MAC-GF:

$$Y_1 = X_1 + X_2 + Z_1 \quad (7.87)$$

$$Y_2 = X_1 + X_2 + Z_2 \quad (7.88)$$

$$Y = X_1 + X_2 + Z \quad (7.89)$$

where Z_1, Z_2, Z are independent Gaussian random variables with zero-mean and variances of N_1, N_2 , and N , respectively. We also impose power constraints of P_1 and P_2 on X_1 and X_2 .

For this Gaussian channel, if $N_2 < N$ (resp. $N_1 < N$), then user 1 (resp. user 2) cannot have positive secrecy if users *do not* cooperate. To see this point, let us consider the MAC channel from the users to the receiver and the channel from user 1 to user 2. This channel can be viewed as a Gaussian wiretap channel where user 2 is the wiretapper. Consequently, if the wiretapper's channel (the channel from user 1 to user 2), is less noisy than the main channel (the channel from the users to the receiver), i.e., if $N_2 < N$, then all the messages sent to the receiver by user 1 can be decoded by user 2, as well. Thus, the secrecy rate of user 1 is zero. Let us consider the specific example: $N_1 = N_2 = 0.75$, $N = 1$. We plot the secrecy rates given by the achievable region of Eqs. (7.80–7.86) in Fig. 7.8. We observe that, thanks to

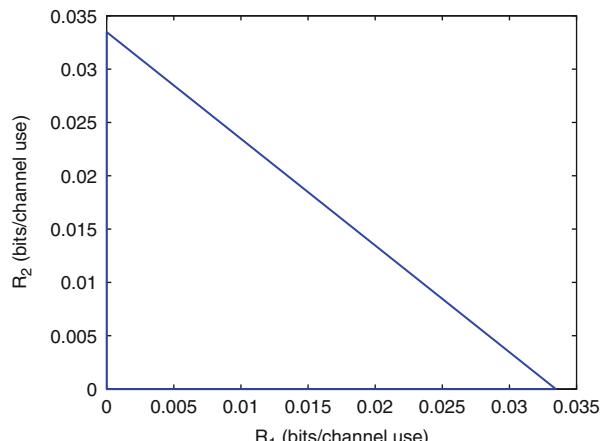
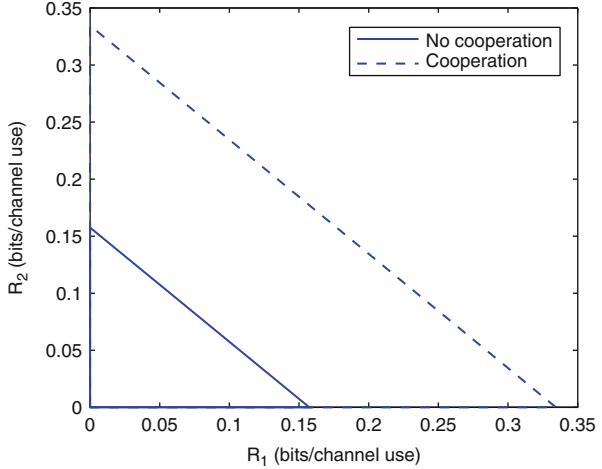


Fig. 7.8 Effect of CAF on the secrecy of MAC-GF

Fig. 7.9 Comparison of cooperation and no-cooperation in MAC-GF



CAF-based cooperation, both users are able to achieve positive secrecy rates. We observe that each user achieves the largest secrecy rate when the other user does not send any confidential messages but act as a pure relay. We consider another channel with parameters $N_1 = N_2 = 1.25$, $N = 1$. In this MAC-GF, both users achieve positive secrecy rates even without cooperation. Figure 7.9 shows that CAF-based cooperation enlarges this secrecy region.

7.6.3 CRBC with Confidential Messages

In this section, we consider CRBC, shown in Fig. 7.3, where the transmitter has messages to send to both receivers, and there is a one-sided cooperation link from user 1 to user 2. In this section, user 2 will consider user 1 as a cooperating partner and also an eavesdropper, and user 1 will consider user 2 as an eavesdropper. As in the previous section on MAC-GF, in this channel model, we have two rates and two equivocation-rates. Our goal is to understand the effects of the actions (e.g., cooperation, jamming, etc.) of user 1 on the rates and secrecy of both users.

We showed in [39] that the following secrecy rates are achievable by using a CAF-based cooperation scheme at user 1,

$$R_1 \leq I(V_1; Y_1|X_1) - I(V_1; Y_2, \hat{Y}_1|V_2, X_1) - I(V_1; V_2) \quad (7.90)$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|X_1) - I(V_2; Y_1|V_1, X_1) - I(V_1; V_2) \quad (7.91)$$

where the random variables involved are subject to the constraint

$$I(\hat{Y}_1; Y_1|X_1, V_1) \leq I(\hat{Y}_1, X_1; Y_2) \quad (7.92)$$

for any joint distribution of the form

$$p(v_1, v_2)p(x_1)p(x|v_1, v_2)p(\hat{y}_1|x_1, y_1, v_1)p(y_1, y_2|x, x_1) \quad (7.93)$$

In this achievable scheme, the transmitter uses Marton's scheme [40] for broadcast channels and user 1 employs CAF for relay channels. To examine the potential improvement in the secrecy rates with this scheme, we consider a Gaussian CRBC:

$$Y_1 = X + Z_1 \quad (7.94)$$

$$Y_2 = X + X_1 + Z_2 \quad (7.95)$$

where Z_1, Z_2 are independent Gaussian random variables with zero-mean and variances of N_1 and N_2 , respectively. We impose power constraints of P and aP on X and X_1 .

If user 1 does not transmit any signals, i.e., $X_1 = \phi$, then the channel becomes a Gaussian broadcast channel, and it will be degraded in one of the directions. Consequently, in this broadcast channel, both users cannot have positive secrecy rates simultaneously. However, if we compute the achievable region in Eqs. (7.90–7.93) for $N_1 = 1, N_2 = 2, P = 8$ for various values of a , we obtain the achievable secrecy region shown in Fig. 7.10. We observe that although user 2 cannot have positive secrecy rate in the underlying broadcast channel since $N_1 < N_2$, the cooperation of user 1 enables user 2 to have positive secrecy rates.

The previous achievable scheme and the Gaussian channel example provide us with a limited picture of what can be achieved. In particular, the above proposed achievability scheme implicitly assumes that the cooperating user (user 1) is the stronger of the two users. Thus, a natural question is, what happens if the cooperating user is the weaker of the two users? If user 1 does not transmit any signals, then it cannot have a positive secrecy rate. However, the question here is: can user 1 *help itself* to have positive secrecy? The answer is positive if user 1 utilizes the cooperative link to jam user 2. An even more interesting question is whether both users can have positive secrecy rates simultaneously, when user 1 (cooperating user) is the weaker of the two users. To make this possible, we proposed an achievable scheme that

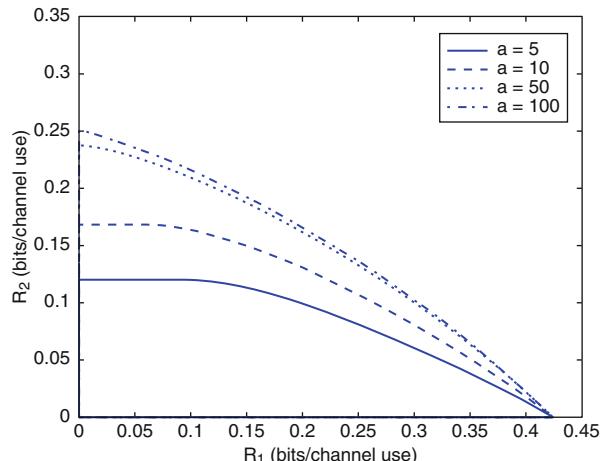


Fig. 7.10 CRBC channel: secrecy region (©IEEE 2008)

combines jamming and relaying in [39]. This scheme yields the rates

$$R_1 \leq I(V_1; Y_1|X_2, U) - I(V_1; \hat{Y}_1, Y_2|U, V_2) - I(V_1; V_2) \quad (7.96)$$

$$R_2 \leq I(V_2; Y_2, \hat{Y}_1|U) - I(V_2; Y_1|U, V_1, X_2) - I(V_1; V_2) \quad (7.97)$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|U, V_1) \leq I(U, \hat{Y}_1; Y_2) \quad (7.98)$$

for any joint distribution of the form

$$p(v_1, v_2)p(x|v_1, v_2)p(u)p(\hat{y}_1|u, v_1, y_1)p(x_1|u) \quad (7.99)$$

First, we note that this achievable scheme can be obtained from the one in Eqs. (7.90–7.93) via prefixing user 1's input, X_1 , with another channel whose input is U . In this achievable scheme, U denotes the actual help signal that should be decoded by user 2 in order to get the compressed version of user 1's observation, \hat{Y}_1 , whereas X_1 , that is correlated with U , contains the jamming attack. Therefore, since user 2's channel is attacked, the information user 2 can gather from its observation about V_1 decreases, making it possible for user 1 to have positive secrecy when it is the weaker one of the two users.

Next, we provide a Gaussian example with $N_1 > N_2$, i.e., user 1 is the weaker of the two users. In this Gaussian channel, the overall strategy works as follows. First, user 1 makes user 2's observation more noisy to provide secrecy for itself via injecting the channel with additional Gaussian noise. Assuming that user 1 has large enough power, this ultimately changes the strengths of two the channels, i.e., now user 1 becomes the stronger of the two users. Now, we are back to the previous case, and user 1 relays its observation to user 2 to provide positive secrecy for user 2 in its attacked channel. The numerical example for this case is given in Fig. 7.11 for $N_1 = 2$, $N_2 = 1$ showing that both users enjoy positive secrecy rates thanks to a combination of cooperation and jamming.

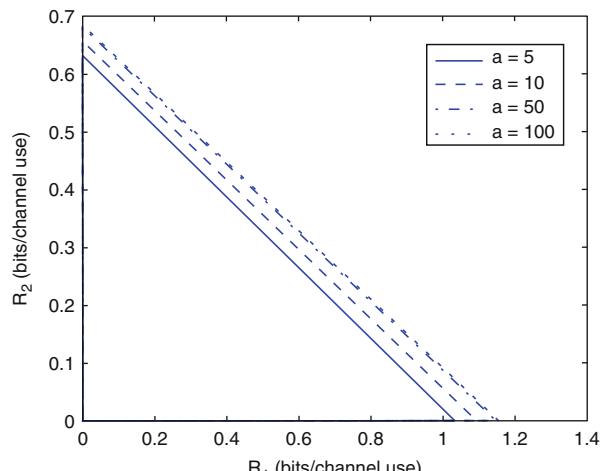


Fig. 7.11 CRBC channel: joint jamming and relaying
©IEEE 2008

7.7 Conclusions

In this chapter, we reviewed the current literature on cooperation, secrecy and the interactions of the two. Our emphasis has mainly been on how cooperation can improve secrecy. We investigated channel models where users cooperate to defeat an external eavesdropper, as well as channels where cooperating parties are treated as potential eavesdroppers. We have demonstrated that there are various ways users can cooperate to improve secrecy: users can cooperate even when they do not know the messages of each other (as in *oblivious* cooperation), they can cooperate in the traditional sense by forwarding information about each others' message (as in *active* cooperation), and finally, users can improve secrecy of the transmitters even when they themselves are treated as eavesdroppers (as in the case of *untrusted helpers*).

References

- [1] E. C. van der Meulen. Three-terminal communication channels. *Adv. Appl. Probab.*, 3:120–154, 1971.
- [2] A. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):1355–1387, Jan. 1975.
- [3] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, IT-25(5):572–584, Sep. 1979.
- [4] A. Carleial. Multiple access channels with different generalized feedback signals. *IEEE Trans. Inf. Theory*, 28(6):841–850, Nov. 1982.
- [5] F. Willems, E. van der Meulen, and J. Schalkwijk. Achievable rate region for the multiple access channel with generalized feedback. In *41st Asilomar Conf. Signals, Syst. Comp.*, Nov. 1983.
- [6] R. C. King. *Multiple access channels with generalized feedback*. PhD thesis, Stanford Univ., Stanford, CA, Mar. 1978.
- [7] T. Cover and C. Leung. An achievable rate region for the multiple access channel with feedback. *IEEE Trans. Inf. Theory*, 27(5):292–298, May 1981.
- [8] M. A. Khojastepour, A. Sabharwal, and B. Aazhang. Improved achievable rates for user cooperation and relay channels. In *IEEE Int. Symp. Inf. Theory*, Jun. 2004.
- [9] L. Ong and M. Motani. Coding strategies for multiple-access channels with feedback and correlated sources. *IEEE Trans. Inf. Theory*, 53(10):3476–3497, Oct. 2007.
- [10] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity-part I: System description. *IEEE Trans. Commun.*, 51(11):1927–1938, Nov. 2003.
- [11] O. Kaya and S. Ulukus. Power control for fading cooperative multiple access channels. *IEEE Trans. Wireless Commun.*, 6(8):2915–2923, Aug. 2007.
- [12] R. Dabora and S. Servetto. Broadcast channels with cooperating decoders. *IEEE Trans. Inf. Theory*, 52(12):5438–5454, Dec. 2006.
- [13] Y. Liang and G. Kramer. Rate regions for relay broadcast channel. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, Oct. 2007.
- [14] Y. Liang and V. V. Veeravalli. Cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(3):900–928, Mar. 2007.
- [15] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.
- [16] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley & Sons, 2006. 2nd edition.
- [17] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.

- [18] Z. Li, R. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *44th Annu. Allerton Conf. Commun. Control Comput.*, Sep. 2006.
- [19] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. 54(6):2470–2492, Jun. 2008.
- [20] A. Khisti and G. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Aug. 2007.
- [21] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2007.
- [22] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, 55(9):4033–4039, Sep. 2009.
- [23] Z. Li, R. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE ISIT*, Jun. 2007.
- [24] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, Dec. 2008.
- [25] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, Jun. 2008.
- [26] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, Sep. 2008.
- [27] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Interference-assisted secret communication. In *IEEE Inf. Theory Workshop*, May 2008.
- [28] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. The Gaussian wiretap channel with a helping interferer. In *IEEE Int. Symp. Inf. Theory*, Jul. 2008.
- [29] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.
- [30] M. Yuksel and E. Erkip. The relay channel with a wire-tapper. In *41st Annu. Conf. Inf. Sci. Syst.*, Mar. 2007.
- [31] M. Yuksel and E. Erkip. Secure communication with a relay helping the wiretapper. In *IEEE Inf. Theory Workshop*, Sep. 2007.
- [32] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Inf. Theory Workshop Front. Coding Theory*, Sep. 2007.
- [33] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2007.
- [34] X. He and A. Yener. On the equivocation region of relay channels with orthogonal components. In *41st Asilomar Conf. Signals Syst. Comp.*, Nov. 2007.
- [35] A. El Gamal and S. Zahedi. Capacity of a class of relay channels with orthogonal components. *IEEE Trans. Inf. Theory*, 51(5):1815–1817, May 2005.
- [36] Y. Liang and H. V. Poor. Multiple access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Mar. 2008.
- [37] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Inf. Theory*, Jul. 2006.
- [38] E. Ekrem and S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In *CISS*, Mar. 2008.
- [39] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. In *IEEE Int. Symp. Inf. Theory*, Jul. 2008.
- [40] K. Marton. A coding theorem for the discrete memoryless channels. *IEEE Trans. Inf. Theory*, 25(1):306–311, May 1979.

Chapter 8

Source Coding Under Secrecy Constraints*

Deniz Gündüz, Elza Erkip and H. Vincent Poor

8.1 Introduction

Distributed compression involves compressing multiple data sources by exploiting the underlying correlation structure of the sources at separate non-cooperating encoders, while decoding is done jointly at a single decoder. Recent years have witnessed an increasing amount of research on the theoretical and practical aspects of distributed source codes, which find applications in distributed video compression, peer-to-peer data distribution systems, and sensor networks [1–3]. In many practical scenarios, limited network resources such as power and bandwidth, or physical limitations of the devices as in the case of sensor networks, pose challenges in terms of network performance and security. Oftentimes, the data aggregated in distributed compression systems may have commercial value as in the case of warehouse inventory monitoring systems, may contain sensitive information as in the case of distributed video surveillance systems, or might infringe personal privacy concerns as in the case of human body sensors measuring various health indicators. In all these scenarios, it is essential to develop distributed compression and communication protocols which exploit the limited power and bandwidth resources efficiently as well

D. Gündüz (✉)

Department of Electrical Engineering
Princeton University
Princeton, NJ 08544, USA
e-mail: dgunduz@princeton.edu

Department of Electrical Engineering
Stanford University
Stanford, CA 94305, USA

*Portions of the material have appeared previously in “Lossless compression with security constraints,” in Proceedings of the IEEE Int’l Symposium on Information Theory (ISIT), 2008 ©IEEE 2008; and “Secure lossless compression with side information,” in Proceedings of the IEEE Information Theory Workshop, 2008 ©IEEE 2008.

This research was supported in part by the U.S. National Science Foundation under Grant 0635177.

as satisfying the security requirements. Our goal in this chapter is to review fundamental limitations and tradeoffs for the overall performance optimization taking into account the quality and the security considerations jointly.

There are two fundamental approaches to guarantee security in wireless networks. In the approach based on computational complexity [4], on which most practical cryptographic applications are based, the security of the system depends on the intractability assumption for a problem such as prime factorization. On the other hand, in the approach based on information theoretic secrecy introduced by Shannon in [5], the emphasis is on unconditional secrecy, which requires that, an eavesdropper with unbounded time and computational resources, and the knowledge of the encryption algorithm, does not gain any additional information about the underlying secret message upon intercepting the encrypted cryptogram. For a general review of recent progress in information theoretic security, see [6]. Although the complexity based approach has been successful in satisfying the security concerns of many practical networking applications such as the Internet, wireless networks pose additional limitations and threats that cannot be solved solely through encryption. The broadcast nature of the wireless medium makes it particularly vulnerable to eavesdropping and authentication attacks, and the energy and bandwidth limitations of wireless devices restrict their computational power, hence rendering high complexity encryption techniques undesirable. Furthermore, especially in the sensor network scenario, where the sensor nodes are generally deployed in remote locations highly vulnerable to tampering, secure key management becomes impractical. Issues such as mobility and lack of infrastructure (e.g., in mobile ad hoc networks) also pose significant challenges to traditional approaches based on maintaining secret keys. In such applications information theoretic security can support and enhance the computational complexity based approach.

In this chapter, we survey information theoretic security in distributed source compression, and in particular how compression and communication can be achieved in an information theoretically secure way. Consider, for example, a sensor network in which correlated sensor observations are to be reconstructed at an access point either in a lossless fashion or within a prescribed distortion requirement. While some sensors might have secure (possibly wired) connections to the access point, others might be transmitting over the wireless medium, which can be accessed by an adversary trying to obtain information about the underlying phenomenon. Furthermore, this adversary might have her own observation of the main source. Our goal is to explore the fundamental information theoretic limitations for secure distributed compression and communication in this kind of situation.

In practical applications, encryption is considered to be a separate block in the protocol stack applied in concatenation with source compression and channel transmission. The information theoretic unconditional secrecy obtained through secure source and/or channel coding or joint source-channel coding hence can be used in parallel with the existing computational encryption schemes enhancing the overall level of security. In order to fully exploit this concept of information theoretic security practical secure source and channel codes need to be developed. While there are many recent developments in this direction for channel coding [7–9] little is known

for secure compression. However, design of such secure source codes is beyond the scope of this chapter, and constitutes a potential research direction.

The chapter is organized as follows. After reviewing Shannon's model and the preliminaries of information theoretic secrecy in Sect. 8.2, in Sect. 8.3 we analyze distributed lossless compression under security constraints and present related fundamental results. In Sect. 8.4, we focus on lossy reconstruction at the legitimate receiver, and analyze the achievable distortion for given secrecy and communication rate constraints. Section 8.5 focuses on secure joint source-channel coding followed by the Conclusions and the Appendix.

8.2 Preliminaries

The fundamentals of information theoretic security date back to Shannon [5]. The model of a Shannon cipher system, illustrated in Fig. 8.1, is composed of two legitimate users, which we will call Alice and Bob, and an eavesdropper (or wiretapper, attacker) called Eve. Alice wants to transmit her message A to Bob without revealing any information to Eve. The public channel between Alice and Bob, over which the enciphered message, or the cryptogram, W is transmitted can be perfectly observed by Eve as well as Bob. Secrecy of the system depends on the shared secure key W_k . The *perfect secrecy* in this model is defined by Shannon as the requirement

$$H(A|W) = H(A),$$

where $H(X)$ is the entropy of the random variable X defined by

$$H(X) \triangleq - \sum_{x \in \mathcal{X}: P_X(x) \neq 0} P_X(x) \log P_X(x).$$

This renders the publicly available cryptogram W useless for eavesdropper to obtain any information about the secret message A . Shannon proved that the so-called *one-time pad* proposed by Vernam [10] achieves perfect secrecy. In the Vernam cipher, the binary message A is enciphered by (modulo) adding a random binary secret key W_k with equiprobable distribution. This requires Alice and Bob sharing a secret key at least as long as the underlying message.

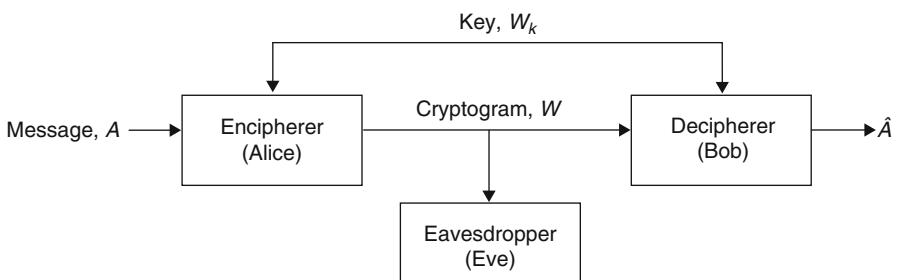


Fig. 8.1 Model of the Shannon cipher system

Shannon also proved that perfect secrecy is possible only if the shared secret key rate is not smaller than the entropy of the message to be encrypted, i.e., $H(W_k) \geq H(A)$. However, sharing such a key requires perfectly protected secure channels, and in many situations it is unrealistic to assume the existence of such channels especially when the required key rate is high.

While Shannon's result seems pessimistic, Wyner argued that it is possible to exploit the noise in the communication channel to obtain perfect secrecy without the need for a shared secure key. In his celebrated paper on the wiretap channel [11], he showed that if Eve's channel is degraded with respect to Bob's, the additional ambiguity at Eve's receiver can be exploited to enable secure communication. The level of security is measured by the *equivocation rate*, which can be roughly defined as the uncertainty of the eavesdropper about the message after receiving the channel output. In the special case of perfect secrecy, we require the equivocation rate to be equal to the rate of the underlying message. The highest communication rate under a perfect secrecy requirement is called the *secrecy capacity*. Wyner's result is extended to more general broadcast channels in [12] and it is shown that nonzero secrecy capacity can be achieved even if the eavesdropper channel is not degraded. Csiszár and Körner also consider a correlated common message intended for both receivers in [12]. In [13], the perfect secrecy rate of the Gaussian wiretap channel is shown to be the difference between the legitimate user's and the eavesdropper's channel capacities. Following these initial developments on the wiretap channel and motivated by the need for secure wireless networking, recent years have witnessed a tremendous amount of work on various extensions of the wiretap channel model to multiuser scenarios and fading channels such as [14–18].

A related concept in information theoretic secrecy is *secret sharing*, which is defined as generating common randomness at the legitimate users without revealing information to an eavesdropper. Generating common randomness plays an important role not only in secure communication, but also in communication over arbitrarily varying channels [19, 20] and in identification capacity [21]. The *secret key capacity* is defined as the maximum rate at which Alice and Bob can agree on a secret key S while keeping the rate of information leaked to Eve arbitrarily small.¹ The noisy communication channel as in the case of the wiretap model of Wyner can be used to generate common randomness to aid in obtaining a secret key, where the secrecy capacity is also the secret key capacity. Once the secret key is generated, it can be used to transmit some other independent information securely over a public channel.

It was first observed in [22, 23] that correlated observations at Alice and Bob can also be used for secret key generation. In this setup, distinct correlated sources can generate a secret key by means of public communication; that is, these terminals can generate common randomness while leaking only a negligible amount of information to an eavesdropper who also has access to the public discussion. In this setup, the secret key capacity is the maximal rate at which Alice and Bob can generate such a secret key by communication over the noiseless and authentic but public

¹This definition is known as the “weak” secret key capacity, while in the strong version the total amount of leaked information is kept arbitrarily small instead of the rate.

channel. Secret key capacity is explored in [23] and [24] for two terminals. In [25], the impact of a helper terminal which observes the output of a correlated source in the generation of the secret key is studied. Secret key capacity for multiple terminals is studied in [26], and the capacity is characterized when the eavesdropper observes all the communication between the terminals but she herself does not have any side information. However, a single letter characterization of the secret key capacity when the eavesdropper also has her own correlated observation is still open.

In the secure distributed compression scenario considered in this chapter, the legitimate users have access to correlated data sources. However, unlike [22, 23] the goal in this chapter is not secure key generation, but to transmit the correlated sources of the legitimate users to the destination node securely. From the Slepian-Wolf theorem [27], it is well-known that correlation among the data can be used to reduce the communication rate requirements from the source nodes to the destination node for lossless reconstruction. We show in Sect. 8.3 that the correlation of the source data can also be used to increase the secrecy even when transmitting at Slepian-Wolf rates. In secret key generation, the goal is to keep the generated key secret from the eavesdropper, while there is no constraint on the knowledge of the eavesdropper about the underlying sources. It is shown in [28] that the secure source transmission model considered here corresponds to a lower bound on the secret key capacity of the underlying model, but this is not a tight bound in general.

A natural extension of the above distributed secure lossless compression setup is to consider lossy reconstruction at the legitimate receiver. A review of the secure lossy source coding literature will be given in Sect. 8.4.

In addition to the secrecy requirements, an important and complementary concept in secure communication is authentication. In general, the eavesdroppers may be active, and rather than simply listening, they may try to either send fake information instead of the legitimate users (*impersonation attack*), or intercept the legitimate transmission and replace it with a different message (*substitution attack*). Information theoretic analysis for authentication systems has been carried out in [29, 30]. In our setup, while the availability of side information at the legitimate receiver increases the probability of detection of such attacks, the side information at the attacker increases the probability of success for the attacker. Albeit essential, analysis of joint authentication and secure compression is beyond the scope of this chapter. Here we assume that all the transmissions are authenticated, or equivalently that the eavesdroppers are passive.

8.3 Secure Distributed Lossless Compression

Our main goal in this section is to analyze the fundamental limits of secure distributed lossless compression. For an arbitrary network, information theoretic characterization of the fundamental limits of compression is difficult even in the absence of security constraints. Hence, we start with a simple network of two nodes called Alice and Charlie who wish to transmit their observations to the destination node Bob. There is a single eavesdropper Eve, who is interested in only the data of Alice,

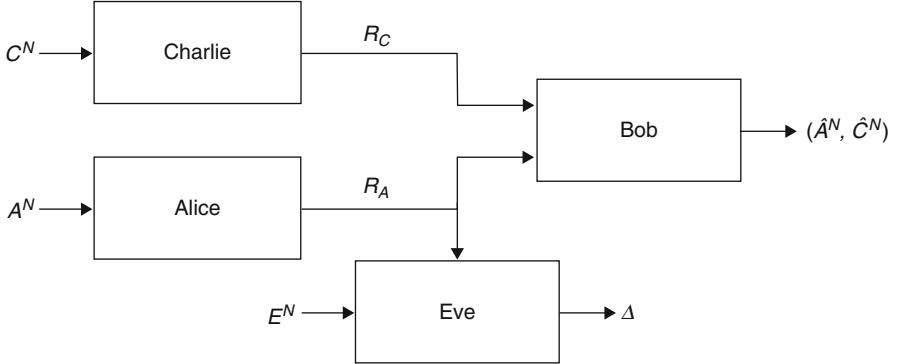


Fig. 8.2 Two terminal secure distributed compression. The eavesdropper (Eve) can only access one of the links and is interested in A^N (©IEEE 2008)

and hence eavesdrops Alice's link to Bob (see Fig. 8.2). We will show in this section that Charlie's correlated observation transmitted through a secure link enables improved secrecy for Alice's transmission. We also investigate the effect of side information at Alice and Bob, as well as extensions to multiple receivers/eavesdroppers. Details of the proofs can be found in [31, 32].

To highlight some of the differences between compression with and without secrecy constraints, we provide the following example.

Example 1 Consider the following scenario. Alice observes a random binary sequence $A \sim \text{Bernoulli}(1/2)$, which she wishes to transmit to Bob. Charlie also senses the environment and has access to C correlated with A . Suppose that $C = A \oplus Z_C$ where \oplus denotes modulo 2 addition, and the binary Z_C , independent of A , has distribution Bernoulli(p), i.e., $Z_C = 1$ with probability p , $0 \leq p \leq 1/2$. The eavesdropper Eve has her own correlated observation $E = A \oplus Z_E$, where Z_E is Bernoulli(q) with $q < p$ and Z_E is independent of (A, Z_C) . Assume that Charlie has a secure link to Bob with capacity 1 bit per channel use, i.e., C can be transmitted to Bob securely without error. In this case, with no secrecy requirement, according to the Slepian-Wolf theorem Alice can send A to Bob using $h(p)$ bits on the average, where $h(p) = -p \log p - (1-p) \log(1-p)$. However, in the presence of the eavesdropper Eve, since $q < p$, E agrees with A more often on the average, and it is not possible to transmit A to Bob without completely revealing it to Eve despite the existence of Charlie's secure link.

Now assume that Alice can also observe the secure link between Charlie and Bob, i.e., Alice has access to Charlie's information. In terms of compression rates, this additional information would not help Alice since she still needs to send $Z_C = A \oplus C$ at a minimum rate of $h(p)$ for reliable reconstruction at Bob. However, even though Eve can perfectly recover Z_C , this information is totally useless since it is independent of A and Z_E . Hence we have achieved *perfectly secure compression*, leaking no information to Eve.

This simple example allows us to make some key observations: (1) without Charlie's secure link to Bob, Alice would not be able to achieve any secrecy while transmitting her observation to Bob; and (2) unlike the usual Slepian-Wolf compression in which knowing C at Alice would not improve the compression rate of Alice, under secrecy constraints, this side information is useful.

8.3.1 Secure Distributed Compression with Two Transmitters

For the two transmitters and one receiver model in Fig. 8.2, we assume that Alice and Charlie have access to length- N correlated source sequences A^N and C^N , respectively. They want to transmit these sources to Bob reliably over separate noise-free, finite capacity channels. Alice's transmission will also be perfectly received by an eavesdropper called Eve. We assume that Eve has her own correlated side information E^N . We model A^N , C^N , and E^N as being generated independent and identically distributed (i.i.d.) according to the joint probability distribution $p_{ACE}(a, c, e)$ over the finite alphabet $\mathcal{A} \times \mathcal{C} \times \mathcal{E}$. Along with lossless transmission, the goal is to maximize the equivocation rate at Eve, which represents the uncertainty of Eve about A^N after receiving Alice's transmission and combining with her (Eve's) own side information E^N .

An (M_A, M_C, N) code for secure source compression in this setup is composed of an encoding function at Alice,

$$f_A : \mathcal{A}^N \rightarrow I_{M_A},$$

an encoding function at Charles,

$$f_C : \mathcal{C}^N \rightarrow I_{M_C},$$

and a decoding function at Bob,

$$g : I_{M_A} \times I_{M_C} \rightarrow \mathcal{A}^N \times \mathcal{C}^N,$$

where I_k denotes the set $\{1, \dots, k\}$ for $k \in \mathbb{Z}^+$. The equivocation rate of this code is defined as

$$\frac{1}{N} H(A^N | f_A(A^N), E^N),$$

and the error probability as

$$P_e^N \triangleq \Pr\{g(f_A(A^N), f_C(C^N)) \neq (A^N, C^N)\}.$$

Here, we assume deterministic coding in the analysis for simplicity, but the proofs follow similarly for randomized coding which is modeled by assuming independent random variables at the terminals and deterministic coding functions that depend on these random variables.

Definition 1 We say that (R_A, R_C, Δ) is *achievable* if, for any $\epsilon > 0$, there exists an (M_A, M_C, N) code such that

$$\begin{aligned} \log(M_A) &\leq N(R_A + \epsilon) \\ \text{and} \quad \log(M_C) &\leq N(R_C + \epsilon) \end{aligned}$$

while the equivocation rate and the error probability satisfy

$$\begin{aligned} H(A^N | f_A(A^N), E^N) &\geq N(\Delta - \epsilon) \\ \text{and} \quad P_e^N &< \epsilon. \end{aligned} \tag{8.1}$$

Let \mathcal{R} denote the set of all achievable (R_A, R_C, Δ) triplets.

When we remove the secrecy requirements, the above problem reduces to the well-known Slepian-Wolf coding of correlated sources. The rate region (R_A, R_C) without secrecy constraints is given as follows:

$$\begin{aligned} R_A &\geq H(A|C), \\ R_C &\geq H(C|A), \\ \text{and} \quad R_A + R_C &\geq H(A, C). \end{aligned}$$

While Slepian-Wolf coding provides an inner bound on the (R_A, R_C, Δ) region, in general one can do better, and the solution to distributed compression with secrecy constraints is not a direct extension of the Slepian-Wolf theorem.

Below, we provide an achievable compression-equivocation rate region for the above distributed secure compression problem. We first provide some definitions that will be used to characterize the rate region.

Definition 2 Let U and V be two random variables jointly distributed with A, C , and E and taking values over the finite alphabets \mathcal{U} and \mathcal{V} . We define \mathcal{P}_{in} as the set of (U, V) that satisfy $H(C|A, V) = 0$ with a joint distribution of the form $P_{ACE} P_{U|A} P_{V|C}$.

Definition 3 We define \mathcal{R}_{in} as the convex hull of the set of all (R_A, R_C, Δ) for which there exists $(U, V) \in \mathcal{P}_{in}$ such that

$$R_C \geq I(C; V), \tag{8.2}$$

$$R_A \geq H(A|V), \tag{8.3}$$

$$\Delta \leq [I(A; V|U) - I(A; E|U)]^+, \tag{8.4}$$

$$\Delta \leq \min\{R_C - H(C|A), I(A; C)\}, \tag{8.5}$$

$$\text{and} \quad \Delta \geq [H(A|E) - R_A]^+, \tag{8.6}$$

hold, where $[x]^+ = \max\{x, 0\}$.

Theorem 1 $\mathcal{R}_{in} \subseteq \mathcal{R}$.

Proof A proof of the theorem is given in [32] and it is included in the Appendix for the interested reader. \square

In [31], the case in which Bob is only interested in reconstructing Alice's information source A^N is also considered. In this setup, Charlie becomes a helper for Alice's transmission both for compressing her source and for increasing the secrecy against Eve by using his secure channel to Bob. We refer the readers to [31] for the bounds on the compression-equivocation rate region for this setup.

8.3.2 Uncoded Side Information at Bob

A special case of the above setup is obtained when we have $R_C \geq H(C)$, that is, C^N can be recovered by Bob with an arbitrarily small probability of error. Equivalently, we can assume that the side information sequence $B^N = C^N$ is available directly to Bob. This setup might model a scenario in which Bob has his own correlated side information about Alice's observation. For this setup, it is possible to characterize the compression-equivocation rate region as given below [31]. This result without the compression rate constraint is also given in [28].

Theorem 2 *For uncoded side information B^N at Bob, (R_A, Δ) is an achievable rate-equivocation pair if and only if,*

$$R_A \geq H(A|B), \quad (8.7)$$

$$\Delta \leq \max\{I(A; B|U) - I(A; E|U)\}, \quad (8.8)$$

$$\text{and} \quad R_A + \Delta \geq H(A|E), \quad (8.9)$$

where we maximize over auxiliary random variables U such that $U - A - (B, E)$ form a Markov chain.

Proof The achievability follows from Theorem 1 by substituting $C = V = B$. The converse proof can be found in the Appendix. \square

Note that the rate regions in Theorem 1 and Theorem 2 require an auxiliary codebook generated by U in the general case to conceal the source from the eavesdropper. This can be interpreted as a type of precoding for compression in which we first transmit a quantization of the information by the auxiliary codebook generated by U , and then we transmit the remaining information. The auxiliary codebook is chosen such that the remaining information is orthogonal to the eavesdropper's side information. While a non-trivial auxiliary codebook is required in general, it is sometimes possible that the ordinary Slepian-Wolf binning achieves the highest possible security in terms of equivocation, i.e., Eq. (8.8) is maximized by a constant U . We first give some definitions to identify such cases.

Definition 4 We say that the side information B is *less noisy* than the side information E if

$$I(U; E) \leq I(U; B) \quad (8.10)$$

for every probability distribution of the form $p(a, b, e, u) = p(a, b, e)p(u|a)$.

Definition 5 Side information E is said to be *physically degraded* with respect to B if, $A - B - E$ form a Markov chain. We say E is *stochastically degraded* with respect to B if, there exists a joint probability distribution $p_{A\tilde{B}\tilde{E}}$ such that $p_{A\tilde{B}} = p_{AB}$, $p_{A\tilde{E}} = p_{AE}$, and $A - \tilde{B} - \tilde{E}$ is a Markov chain.

The *less noisy* condition is strictly weaker than the *stochastically degraded* condition [33]. Furthermore, the compression-equivocation rate region depends on the joint distribution p_{ABE} only via its marginals p_{AB} and p_{AE} . Hence, physical degradation and stochastic degradation are equivalent in this scenario.

Corollary 3 *For uncoded side information at Bob, if Bob has less noisy side information than Eve, then an (R_A, Δ) pair is achievable if and only if*

$$R_A \geq H(A|B), \quad (8.11)$$

$$\text{and} \quad \Delta \leq I(A; B) - I(A; E) = H(A|E) - H(A|B). \quad (8.12)$$

Proof Achievability follows simply by letting U be constant in Theorem 2. For the converse, consider any U with joint distribution of the form $p(u, a, b, e) = p(a, b, e)p(u|a)$. We have

$$\begin{aligned} & [I(A; B) - I(A; E)] - [I(A; B|U) - I(A; E|U)] \\ &= [I(A; B) - I(A; E)] - [I(A, U; B) \\ &\quad - I(B; U) - I(A, U; E) + I(E; U)] \\ &= I(B; U|E) - I(E; U|B) \\ &= I(B; U) - I(E; U) \\ &\geq 0, \end{aligned} \quad (8.13)$$

where the last inequality is due to the less noisy assumption. \square

This results shows that the usual Slepian-Wolf binning scheme provides all the security we might expect if the side information at Bob is less noisy than the eavesdropper's side information. The following corollary provides a condition under which no positive equivocation rate can be achieved.

Corollary 4 *If Bob's side information is a stochastically degraded version of Eve's side information, then no positive equivocation rate is achievable, and $\Delta = 0$.*

Proof First assume that Bob's side information is physically degraded with respect to Eve's. In that case, we have

$$\begin{aligned} I(A; B|U) - I(A; E|U) &= I(A; B, E|U) - I(A; E|B, U) - I(A; E|U) \\ &= I(A; B|E, U) - I(A; E|B, U) - I(A; E|B, U) \\ &\leq 0. \end{aligned}$$

Then, for a physically degraded observation at Bob, $\Delta = 0$. However, since physically and stochastically degraded cases are equivalent, $\Delta = 0$ for stochastically degraded observations as well. \square

To further illustrate some of these results we provide another example (presented in [28]), consisting of a binary source as in Example 1, while the side information sequences at Bob and Eve are independently erased versions of Alice's source.

Example 2 Let the original source sequence $A^N = (A_1, \dots, A_N)$ available to Alice be an i.i.d. binary sequence of $A_i \sim \text{Bernoulli}(1/2)$ random variables. The observation of Bob $B^N = (B_1, \dots, B_N)$ is generated by independently erasing each element of the A^N sequence with probability p_B , that is, $B_i = A_i$ with probability $1 - p_B$, and $B_i = e$ with probability p_B . Similarly, the observation $E^N = (E_1, \dots, E_N)$ of the eavesdropper Eve is an independently erased version of A^N . We have $E_i = A_i$ with probability $1 - p_E$, and $E_i = e$ with probability p_E .

For $p_E > p_B$, the side information of Eve is a stochastically degraded version of the side information of Bob. Using Corollary 3, we know that a constant U is optimal. Then, the optimal equivocation rate is $\Delta = I(A; B) - I(A; E) = (1 - p_B) - (1 - p_E) = p_E - p_B$.

When $p_B \geq p_E$, then B^N is a stochastically degraded version of E^N . From Corollary 4, we get $\Delta = 0$.

8.3.3 Side Information Available to Alice

We know from the Slepian-Wolf source coding that, the availability of Bob's side information at Alice does not help in terms of compression rates. However, Example 1 illustrates that having B^N at Alice potentially enables higher equivocation rates at the eavesdropper. In practical systems this may be accomplished by a secure feedback channel from Bob to Alice. In this section, we consider various cases in which Alice also has access to the side information available to Bob and/or Eve, and characterize the compression-equivocation rate regions. The availability of side information at Alice is indicated by the state of the switches in Fig. 8.3.

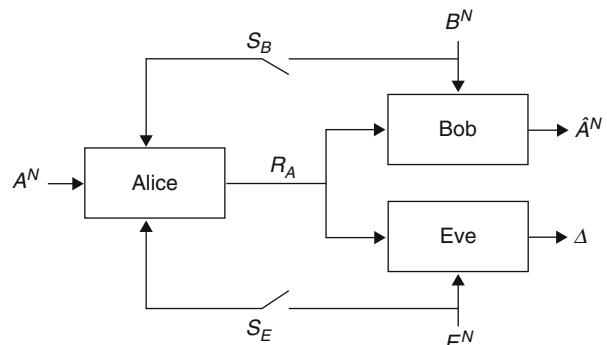


Fig. 8.3 Uncoded side information at Bob. The states of switches S_B and S_E model different scenarios in terms of the side information at the encoder (©IEEE 2008)

Theorem 5 Consider secure source compression for uncoded side information at Bob as illustrated in Fig. 8.3. An (R_A, Δ) pair is achievable if and only if

$$R_A \geq H(A|B), \quad (8.14)$$

$$0 \leq \Delta \leq [I(A; B|U) - I(A; E|U)]^+, \quad (8.15)$$

$$\text{and} \quad R_A + \Delta \geq H(A|E), \quad (8.16)$$

where U is an auxiliary random variable such that the joint distribution $p(u, a, b, e)$ is given in the following table based on which switches are closed:

Closed Switches	$p(u, a, b, e)$
S_B	$p(a, b, e)p(u a, b)$
S_E	$p(a, b, e)p(u a, e)$
S_B and S_E	$p(a, b, e)p(u a, b, e)$

In the case when only the switch S_E is closed, the rate region can be explicitly given as follows:

$$R_A \geq H(A|B), \quad (8.17)$$

$$0 \leq \Delta \leq I(A; B|E), \quad (8.18)$$

$$\text{and} \quad R_A + \Delta \geq H(A|E). \quad (8.19)$$

Proof The proof resembles that of Theorem 1, and will not be included here. \square

Note that the availability of either or both of the side information sequences at the transmitter enlarges the space of the auxiliary random variables U and potentially results in a higher equivocation rate at the eavesdropper. This was also illustrated by Example 1. Next, we consider the availability of side information in Example 2.

Example 2 (continued) Suppose that the observation of Bob B^N is available to Alice as well. Alice can transmit only the erased bits of Bob, hence leaking the least amount of information to Eve. The optimal auxiliary random variable U satisfies $U = A$ when there is an erasure at Bob, and U is constant otherwise. The optimal equivocation rate in this case is $\Delta = p_E(1 - p_B)$. Note that this equivocation is strictly larger than the one without side information. Furthermore, even if Bob's side information is a stochastically degraded version of Eve's, i.e., $p_B > p_E$, we are still able to achieve a non-zero equivocation rate if this side information can be provided to Alice as well.

When only the observation of Eve, E^N is available to Alice, from Eq. (8.18) the optimal equivocation rate is given by $I(A; B|E)$. In the erasure example, the optimal equivocation rate is found to be $\Delta = p_E(1 - p_B)$, which is the same as in the case when only switch S_B is closed. We observe that, for this specific example of erased observations at Bob and Eve, the benefit of having either Bob's or Eve's side information to Alice is the same. For this example, it is also possible to show that, even

when both observation sequences are available to Alice, the optimal equivocation rate is still $\Delta = p_E(1 - p_B)$.

While there is no difference between physically or stochastically degraded observations when both switches are open, this is no longer true when we consider side information at Alice. In the following corollary, we show that for physically degraded observations at Eve, the availability of E^N to Alice does not help. This is in contrast to stochastically degraded side information E^N whose availability at Alice would potentially increase the equivocation rate as seen in the example above.

Corollary 6 *If the observation of Eve is a physically degraded version of Bob's side information, i.e., $A - B - E$ form a Markov chain, then providing this observation to Alice would not improve the equivocation rate.*

8.3.4 Multiple Legitimate Receivers/Eavesdroppers

In Sect. 8.3, existence of a single legitimate receiver Bob and a single eavesdropper Eve, who is interested in only Alice's source and has access to only Alice's channel is considered. In this section, we review various models involving multiple eavesdroppers and multiple receivers.

In the model considered in [34], two non-cooperating eavesdroppers Eve and Dave are interested in Alice's and Charlie's sources, respectively, and each has access to only the corresponding transmitter's channel to Bob. This model is illustrated in Fig. 8.4, where the eavesdroppers Eve and Dave observe the links from Alice and Charlie, respectively, and while Eve is interested in A^N as before, Dave is interested in C^N . Hence we have two equivocation rates, one for each eavesdropper: Δ_A and Δ_C . The following theorem [34] characterizes the compression-equivocation rate region when Dave and Eve do not have their own side information.

Theorem 7 *The compression-equivocation rate region for the above scenario is the closure of the union of all $(R_A, R_C, \Delta_A, \Delta_C)$ tuples satisfying*

$$R_A \geq H(A|C), \quad (8.20)$$

$$R_C \geq H(C|A), \quad (8.21)$$

$$R_A + R_C \geq H(A, C), \quad (8.22)$$

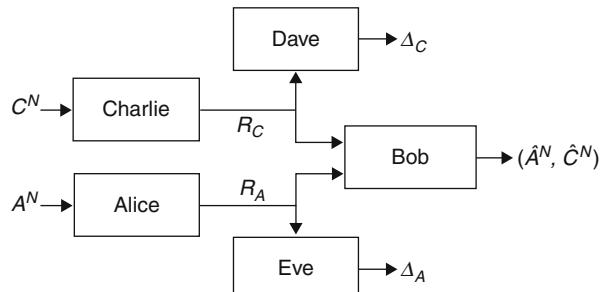


Fig. 8.4 Secure distributed compression with two eavesdroppers (Eve and Dave) each observing a single link and interested in the corresponding sources

$$R_A + \Delta_A \geq H(A), \quad (8.23)$$

$$R_C + \Delta_C \geq H(C), \quad (8.24)$$

$$\text{and} \quad \Delta_A + \Delta_C \leq I(A; C). \quad (8.25)$$

Proof Achievability part of the proof follows simply by using Slepian-Wolf source compression. Since the eavesdroppers do not have correlated side information, Slepian-Wolf compression suffices to achieve the optimal equivocations rate as well as the compression rate. A sketch of a converse proof is given in the Appendix. \square

We now consider broadcasting some sensitive information to $K \geq 1$ receivers, each having its own correlated observation $B_k, k = 1, \dots, K$. Suppose there is only one eavesdropper Eve with side information E^N as before [35]. In the absence of an eavesdropper it is known that a rate of $\max_k H(A|B_k)$ is necessary and sufficient for simultaneous reliable transmission to all the receivers [36].

From Theorem 2, considering each receiver separately, the equivocation rate is bounded as $\Delta \leq \max\{H(A|E, U_k) - H(A|B_k, U_k)\}$ where the maximization is over U_k satisfying the Markov chain condition $U_k - A - (B_k, E)$ for $k = 1, \dots, K$. The minimum of these individual equivocation rate bounds serves as an upper bound; however, achievability of this equivocation rate along with $R_A \geq \max_k H(A|B_k)$ does not follow directly. The achievability proof for a single receiver outlined in the Appendix requires the auxiliary codeword to be decoded by the receiver. However, in the case of multiple receivers, the auxiliary codebook U_k that maximizes the equivocation rate for one of the users, say k , might not be decodable by another user. Imposing such a decoding constraint requires a total transmission rate of $\max_k I(A; U_k|B_k) + \max_k H(A|B_k, U_k)$, which might be greater than $\max_k H(A|B_k)$, the required rate without the secrecy constraint.

We are able to characterize the compression-equivocation rate region in two special cases. First in Corollary 8, we consider the case in which the eavesdropper's side information is physically degraded with respect to each receiver's side information. Since in this case Slepian-Wolf compression is optimal for each receiver separately, it is also optimal for the overall system.

In the second case considered in Corollary 9, we assume that the receivers' side information and Alice's source form a Markov chain. In this case, the receiver with the lowest quality side information requires the highest compression rate and achieves the lowest equivocation rate, and hence this serves as an achievable bound for the overall performance.

Corollary 8 *If $A - B_k - E$ form a Markov chain for all $k = 1, \dots, K$, then (R_A, Δ) is achievable if and only if,*

$$R_A \geq \max_k H(A|B_k),$$

$$\Delta \leq \min_k \{H(A|E) - H(A|B_k)\}$$

$$\text{and} \quad R_A + \Delta \geq H(A|E).$$

Corollary 9 *If $A - B_1 - \dots - B_K$ form a Markov chain, then (R_A, Δ) is achievable if and only if,*

$$\begin{aligned} R_A &\geq H(A|B_K), \\ \Delta &\leq \max\{I(A, B_K|U) - I(A; E|U)\}, \\ \text{and} \quad R_A + \Delta &\geq H(A|E), \end{aligned}$$

where the maximization is over auxiliary random variables U such that $U - A - (B_1, \dots, B_K, E)$ form a Markov chain.

Similarly, there may be one legitimate receiver but multiple non-cooperating eavesdroppers with their own correlated side information. Suppose there are K eavesdroppers, the k -th of which has side information E_k . We have K equivocation rates defined as

$$\Delta_k \triangleq \frac{H(A^N|f_A(A^N), E_k^N)}{N} \quad \text{for } k = 1, \dots, K.$$

This time, we pick the auxiliary codebook that simultaneously achieves the corresponding equivocation rates.

Corollary 10 *(R, Δ) is achievable for the multiple eavesdropper scenario if and only if,*

$$\begin{aligned} R_A &\geq H(A|B), \\ \Delta_k &\leq [H(A|E_k, U) - H(A|B, U)]^+, \\ \text{and} \quad R_A + \Delta_k &\geq H(A|E_k), \end{aligned}$$

for $k = 1, \dots, K$ for some auxiliary random variable satisfying the Markov chain condition $U - A - (B, E_1, \dots, E_K)$.

8.4 Lossy Compression with Security Constraints

In the previous sections we considered secure distributed lossless compression; however in many practical applications a fidelity requirement is imposed instead of lossless reconstruction. This might be the case when the underlying source is a continuous random variable that cannot be transmitted reliably at finite rate, or when lossless reconstruction requires very high transmission rates. In terms of compression, rate can be traded off for distortion and this tradeoff is characterized by the rate-distortion function of the underlying source sequence [37].

Now, consider the basic Shannon cipher system in Sect. 8.2. In the original Shannon setup we require the receiver to reconstruct the underlying source (message) losslessly without revealing any information to the eavesdropper. In the other extreme

of no fidelity requirement, the receiver can simply guess the underlying source, and hence the transmitter need not transmit any information over the insecure communication link. In this case, no information is revealed to the eavesdropper, and perfect secrecy is achieved. In the general case of non-trivial distortion requirements, it is possible to trade off fidelity with secrecy.

In [38], Yamamoto relaxed the reliable transmission assumption and allowed distortion for the source reconstruction. In the model of [38], a point-to-point system is considered with correlated source outputs, in which one of the source outputs is to be transmitted within a prescribed fidelity requirement, while the other source output is to be kept secret from the eavesdropper. Yamamoto defined and evaluated the rate-distortion-equivocation function, which is the minimum rate necessary to attain both the required equivocation and the distortion for this model. He further explored variations of this model in [39], where either both sources or only one of them is to be transmitted, and either both sources or only one of them is to be kept secret. In [40], the secrecy of the system is measured in terms of the distortion at the eavesdropper, and hence the transmitter tries to maximize the distortion at the eavesdropper, while minimizing the distortion at the legitimate receiver.

Note that, the equivocation rate can also be considered as a distortion measure. Hence, lossy coding with secrecy constraint can be considered as a special case of the source coding problem with multiple distortion constraints [41]. However, note also that equivocation is not a single letter distortion measure, and results of [41] do not readily extend to this case.

In [42], Luh and Kundur consider lossy compression of distributed sources in the presence of two eavesdroppers as in Fig. 8.4, extending their work in [34] for lossless compression to lossy reconstruction. They provide inner and outer bounds for the achievable distortion-equivocation rate region.

In [43], both a shared secret key and a wiretap channel are considered, together with lossy reconstruction at the receiver. The main conclusion of [43] is a separation type result suggesting there is no loss in optimality by first applying lossy source compression, then encrypting the compressed bits using the secure key, and finally transmitting this encrypted information over the wiretap channel using an optimal wiretap channel code.

In this section, we focus on the lossy compression part of the cipher system, and state the results of [43] assuming a noise-free finite capacity link among the legitimate users and a shared secure key. The extension to the noisy channel setup is discussed in Sect. 8.5.

Consider the basic Shannon cipher system in Fig. 8.1. The source sequence $\{A_m\}_{m=1}^{\infty}$ is generated i.i.d. with distribution P_A over the set \mathcal{A} as before. The key W_k is a random variable independent of A and uniformly distributed over the set $I_{M_k} = \{0, 1, \dots, M_k - 1\}$. We allow random coding and decoding functions at Alice and Bob, respectively. To model this, we let Alice and Bob generate random variables M_A and M_B , respectively, and consider only deterministic functions for encoding and decoding. Note that, M_A and M_B are independent of the message A^N and the key W_k .

An (R_A, R_k, N) code for this cipher system consists of an encoding function f and a decoding function g , which are defined as

$$\begin{aligned} f : \mathcal{A} \times I_{M_k} \times M_A &\rightarrow I_M \\ \text{and} \quad g : I_{M_k} \times I_M \times M_B &\rightarrow \hat{\mathcal{A}}^N, \end{aligned}$$

where $R_A = \frac{1}{N} \log M$ is the rate of the transmitted message and

$$R_k = \frac{1}{N} \log M_k$$

is the rate of the key.

We allow distortion in the reconstruction at Bob. The distortion of $\hat{\mathcal{A}}^N$ is measured by

$$E[d(A^N, \hat{A}^N)] \triangleq \frac{1}{N} \sum_{m=1}^N Ed(A_m, \hat{A}_m), \quad (8.26)$$

where $d : A \times \hat{A} \rightarrow [0, \infty)$ is the per-letter distortion measure. As before the security of the system is measured by the equivocation rate at the eavesdropper:

$$\frac{1}{N} H(A^N | f(A^N, W_k, M_A)).$$

Alternatively, here, security can also be defined in terms of the distortion achieved at the eavesdropper. For the results related to this measure, see [40, 43].

Definition 6 We say that (R_A, R_k, D, Δ) is achievable if, for any $\epsilon > 0$, there exists an (R_A, R_k, N) code such that $\frac{1}{N} H(A^N | f(A^N, W_k, M_A)) \geq \Delta - \epsilon$ and $E[d(A^N, \hat{A}^N)] \leq D + \epsilon$.

The main result of this section is the following theorem which characterizes the set of all achievable (R_A, R_k, D, Δ) tuples.

Theorem 11 (R_A, R_k, D, Δ) is achievable if and only if,

$$\begin{aligned} R_A &\geq R(D) \\ \text{and} \quad 0 \leq \Delta &\leq H(A) - [R(D) - R_k]^+, \end{aligned}$$

where $R(D)$ is the rate-distortion function [37].

Proof A proof of the theorem can be found in the Appendix. □

Note that the above theorem reduces to Shannon's result in the case of lossless reconstruction, i.e., when $R(D) = H(A)$, and perfect secrecy is possible if and only if $R_k \geq H(A)$. However, in the lossy reconstruction case, perfect secrecy can be achieved if and only if $R_k \geq R(D)$, requiring a lower secret key rate. Hence, this theorem points out that under the perfect secrecy (or another fixed equivocation rate)

requirement, there is a tradeoff between the reconstruction distortion and the required secret key rate.

We can also consider the case in which Bob has access to correlated side information B^N . In this case, replacing the rate-distortion function $R(D)$ with Wyner-Ziv rate-distortion function $R_{A|B}^{WZ}(D)$ [44], we can obtain a result similar to Theorem 11. In this setup, the reconstruction function is defined as $g : I_{M_k} \times I_M \times B^N \times M_B \rightarrow \hat{A}^N$ while the rest of the definitions remain the same. Proof of the theorem can be obtained from [45] as a special case.

Theorem 12 (R_A, R_k, D, Δ) is achievable if and only if,

$$R_A \geq R_{A|B}^{WZ}(D)$$

and $0 \leq \Delta \leq H(A) - [R_{A|B}^{WZ}(D) - R_k]^+$.

8.5 Joint Source-Channel Secret Communication

In the previous sections, we focused mainly on the source coding aspects of secret communication. However, a more general problem is to analyze the end-to-end secrecy considering channel transmission as well as source compression, i.e., a combination/generalization of the wiretap channel coding and the secure source compression problems. In this setup, both the correlated side information at the legitimate receiver and the noisy communication channel can be exploited to increase the overall system secrecy. When considering either the source or the channel models, the optimal secrecy performance can be characterized for many simple models of interest; however, the optimal interaction between the source and the channel components of secrecy generation is far from fully understood.

As outlined in Sect. 8.4, in [43], Yamamoto considers a noisy broadcast channel together with a shared secret key between the legitimate users. For this system, Yamamoto proves a separation result; that is, optimal performance can be achieved by concatenating an optimal lossy source encoder, an optimal encipherer using the secure key and an optimal wiretap channel encoder.

In [45], Merhav extends this result by considering correlated side information at the legitimate receiver and the eavesdropper, and he shows that a similar separation argument is valid by replacing the lossy source encoder with an optimal Wyner-Ziv encoder, when both the channel and the side information of the eavesdropper are physically degraded. However, we do not have a general separation theorem for arbitrarily correlated side information at the legitimate receiver and the eavesdropper.

In recent related work [46–48] secret key generation is considered when the legitimate users observe correlated sources in addition to the availability of a noisy channel. Optimal performance is characterized when either the correlated sources or the noisy channel outputs are not sufficient for secret key generation by themselves. In general, as outlined in Sect. 8.1, various results exist in terms of the secret key capacity for either the noisy channel or the correlated observations models. However,

the optimal rate of secret key generation in the presence of both noisy channel and correlated observations is still open.

8.6 Conclusions

Information theoretic security potentially complements existing computational complexity based cryptographic systems to provide additional means to achieve security. Availability of a shared secure key between the legitimate users, the existence of noise in the communication channel to the eavesdropper, and the availability of correlated observations at the legitimate users have been considered in the literature to achieve secure communication between legitimate users while leaking minimum amount of information to eavesdroppers. Exploiting correlated source observations as well as the noisy communication channel for improving security can be especially valuable for sensor networks, where the broadcast nature of the wireless medium makes it vulnerable to attacks, the low complexity of the sensor nodes limits the possibility of employing cryptographic techniques, and sharing high rate secure keys is impractical due to the distributed nature of the nodes.

We have summarized the fundamental results in secure distributed compression for some simple network settings. We have shown that correlated observations at network nodes with secure links to the access point, or correlated side information at the access point itself, can be used to enable secure transmission of sensitive information from vulnerable network nodes. We have provided the characterization of the compression-equivocation rate region for various simple models involving the availability of (legitimate receiver's and/or eavesdropper's) side information at the legitimate transmitter. We have also considered extensions to scenarios with multiple legitimate receivers or multiple eavesdroppers. We have also summarized the results on secure lossy reconstruction in which case the required secure key rate can be traded off for the achievable reconstruction distortion. Finally, we have outlined the existing results on joint source-channel coding under security constraints which prove the optimality of separate source and channel coding in some special cases.

8.7 Appendix

Proof of Theorem 1

For given p_{ACE} , we fix the probability distributions $p_{U|A}$ and $p_{V|C}$ satisfying the conditions in the theorem. Then we generate $2^{N(I(A;U)+\epsilon_1)}$ independent codewords of length N , $U^N(w_1)$, $w_1 \in \{1, \dots, 2^{N(I(A;U)+\epsilon_1)}\}$, with distribution $\prod_{i=1}^N p(u_i)$. We randomly bin all $U^N(w_1)$ sequences into $2^{N(I(A;U|V)+\epsilon_2)}$ bins, calling them the auxiliary bins. For each codeword $U^N(w_1)$, we denote the corresponding auxiliary bin index as $a(w_1)$. On the other hand, we randomly bin all A^N sequences into $2^{N(H(A|V,U)+\epsilon_3)}$ bins, calling them the source bins, and denote the corresponding bin

index as $s(A^N)$. We also generate $2^{N(I(C; V) + \epsilon_4)}$ independent codewords $V^N(w_2)$ of length N , $w_2 \in \{1, \dots, 2^{N(I(C; V) + \epsilon_4)}\}$, with distribution $\prod_{i=1}^N p(v_i)$.

For each typical outcome of A^N , Alice finds a jointly typical $U^N(w_1)$. Then she reveals $a(w_1)$, the auxiliary bin index of $U^N(w_1)$, and $s(A^N)$, the source bin index of A^N , to both Bob and Eve; that is, the encoding function f_A of Alice is composed of the pair $(a(w_1), s(A^N))$. Using standard techniques, it is possible to show that we have such a unique index pair with high probability. Charlie observes the outcome of his source C^N , finds a jointly typical $V^N(w_2)$ with C^N , and sends the index w_2 of V^N over the private channel to Bob. With high probability there will be a unique w_2 such that C^N and $V^N(w_2)$ are jointly typical.

Bob, having access to w_2 and the auxiliary bin index $a(w_1)$, can find the jointly typical $U^N(w_1)$ correctly with high probability. Then using U^N , the source bin index $s(A^N)$ and $V^N(w_2)$, Bob can reliably decode A^N . Since $H(C|A, V) = 0$, knowing A^N and V^N correctly, Bob can find the correct C^N with high probability as well. Letting $\epsilon_i \rightarrow 0$ for $i = 1, 2, 3$, and 4, we can make the total communication rate of Alice arbitrarily close to $I(A; U|V) + H(A|U, V) = H(A|V)$ and the rate of Charlie arbitrarily close to $I(C; V)$. Since Eqs. (8.2) and (8.3) hold, these rates can be communicated to Bob while having arbitrarily small error probability for sufficiently large N .

The equivocation rate can be lower bounded as follows:

$$\begin{aligned} H(A^N | a(w_1), s(A^N), E^N) &= H(A^N) - I(A^N; a(w_1), E^N) \\ &\quad - I(A^N; s(A^N) | E^N, a(w_1)) \end{aligned} \quad (8.27)$$

$$\geq H(A^N) - I(A^N; U^N, E^N) - H(s(A^N)) \quad (8.27)$$

$$\geq H(A^N | U^N, E^N) - NH(A|V, U) - N\epsilon_3 \quad (8.28)$$

$$= N[H(A|U, E) - H(A|V, U) - \epsilon_3]$$

$$= N[I(A; V|U) - I(A; E|U) - \epsilon_3],$$

where Eq. (8.27) follows from the data processing inequality; and Eq. (8.28) follows from the fact that $s(A^N)$ is a random variable over a set of size $2^{N(H(A|V, U) + \epsilon_3)}$.

For $(U, V) \in \mathcal{P}_{in}$, we can show that

$$I(A; V|U) - I(A; E|U) \leq I(A; C)$$

$$\text{and} \quad I(A; V|U) - I(A; E|U) \leq R_C - H(C|A)$$

Hence Eq. (8.5) is not active in the inner bound.

Finally, we also have

$$\begin{aligned} \frac{1}{N} H(A^N | a(w_1), s(A^N), E^N) &= \frac{1}{N} [H(A^N | E^N) - I(A^N; a(w_1), s(A^N) | E^N)] \\ &\geq H(A|E) - \frac{1}{N} H(a(w_1), s(A^N)) \\ &\geq H(A|E) - R_A. \end{aligned}$$

Proof of Theorem 2

Here we prove the converse part of the theorem. First, define

$$J \triangleq f_A(A^N).$$

From Fano's inequality, we have

$$H(A^N|J, B^N) \leq N\delta(P_e^N), \quad (8.29)$$

where $\delta(\cdot)$ is a non-negative function with $\lim_{x \rightarrow 0} \delta(x) = 0$. We also define

$$U_i \triangleq (J, A^{i-1}, E^{i-1}).$$

Note that $U_i - A_i - (C_i, E_i)$ forms a Markov chain. Using these, we can obtain the following chain of inequalities:

$$\begin{aligned} NR_A &\geq H(J) \\ &\geq H(J|B^N) \\ &= H(A^N, J|B^N) - H(A^N|J, B^N) \\ &\geq H(A^N|B^N) - N\delta(P_e^N) \end{aligned} \quad (8.30)$$

$$= \sum_{i=1}^N H(A_i|B_i) - N\delta(P_e^N) \quad (8.31)$$

$$= N[H(A|B) - \delta(P_e^N)] \quad (8.32)$$

where Eq. (8.30) follows from Fano's inequality in Eq. (8.29) and the nonnegativity of entropy; and Eq. (8.31) follows as $A_i - B_i - (A^{i-1}, B^{i-1}, B_{i+1}^N)$ form a Markov chain.

For the equivocation rate converse, we have

$$\begin{aligned} N\Delta &= H(A^N|J, E^N) \\ &= H(A^N|J) - I(A^N; E^N|J) \\ &= H(A^N|J, B^N) + I(A^N; B^N|J) - H(E^N|J) + H(E^N|A^N, J) \end{aligned} \quad (8.33)$$

$$\begin{aligned} &\leq N\delta(P_e^N) + \sum_{i=1}^N I(A_i; B^N|J, A^{i-1}) - \sum_{i=1}^N H(E_i|J, E^{i-1}) + H(E^N|A^N, J) \end{aligned} \quad (8.34)$$

$$\begin{aligned} &\leq N\delta(P_e^N) + \sum_{i=1}^N I(A_i; B^N | J, A^{i-1}, E^{i-1}) \\ &\quad - \sum_{i=1}^N H(E_i | J, E^{i-1}, A^{i-1}) + H(E^N | A^N) \end{aligned} \quad (8.35)$$

$$= \sum_{i=1}^N [I(A_i; B_i | U_i) - H(E_i | U_i) + H(E_i | A_i)] + N\delta(P_e^N) \quad (8.36)$$

$$= \sum_{i=1}^N [I(A_i; B_i | U_i) - I(A_i; E_i | U_i)] + N\delta(P_e^N) \quad (8.37)$$

where Eq. (8.33) follows from the chain rule; Eq. (8.34) follows from Fano's inequality in Eq. (8.29) and the chain rule; Eq. (8.35) follows from the memoryless property of the source and the side information sequences, and the fact that conditioning reduces entropy; Eq. (8.36) follows from definition of U_i and the memoryless property of the source and the side information sequences; and finally Eq. (8.37) follows since $U_i - A_i - E_i$ form a Markov chain.

And finally we have

$$H(A|E) = \frac{1}{N} H(A^N | E^N) \quad (8.38)$$

$$\leq \frac{1}{N} H(A^N, J | E^N) \quad (8.39)$$

$$= \frac{1}{N} [H(J | E^N) + H(A^N | E^N, J)] \quad (8.40)$$

$$\leq \frac{H(J)}{N} + \Delta \quad (8.40)$$

$$\leq R_A + \Delta. \quad (8.41)$$

where Eq. (8.38) follows from the memoryless assumption for the source and the side information; Eq. (8.39) follows from the fact that conditioning reduces entropy; Eq. (8.40) follows from the fact that conditioning reduces entropy and the definition of the equivocation rate.

Now, we define a new independent random variable Q uniformly distributed over the set $\{1, 2, \dots, N\}$. From Eqs. (8.32), (8.37), and (8.41) we get the following inequalities.

$$\begin{aligned} R_A &\geq H(A|B) + \delta(P_e^N), \\ \Delta &\leq I(A; B|U) - I(A; E|U) + \delta(P_e^N), \\ \text{and} \quad R_A + \Delta &\geq H(A|E) \end{aligned} \quad (8.42)$$

where we have $A \triangleq A_Q$, $B \triangleq B_Q$, $E \triangleq E_Q$, $U \triangleq (U_Q, Q)$. Notice that, $U - A - (B, E)$ satisfy the Markov chain condition.

Finally, letting $N \rightarrow \infty$ and $P_e^N \rightarrow 0$, the converse proof is completed.

Proof of Theorem 7

Proof of the converse part closely follows the classical proof for the Slepian-Wolf converse [37] and the converse proof of Theorem 2. From the Slepian-Wolf converse, we can obtain Eqs. (8.20–8.22). Equations (8.23) and (8.24) can be obtained similarly as in Eqs. (8.38–8.41). Below, we prove the necessity of condition in Eq. (8.25).

First, define J as the codeword of Alice and K as the codeword of Charlie. We consider deterministic encoding functions f_A and f_C , respectively, and thus we have $J = f_A(A^N)$ and $K = f_C(C^N)$. From Fano's inequality, we have

$$H(A^N, C^N | J, K) \leq N\delta(P_e^N). \quad (8.43)$$

Then we have

$$\begin{aligned} N\Delta_A + N\Delta_C &= H(A^N | J) + H(C^N | K) \\ &= H(A^N | J, K) + I(A^N; K | J) + H(C^N | J, K) + I(C^N; J | K) \\ &= H(A^N, C^N | J, K) + I(A^N; C^N | J, K) \\ &\quad + I(A^N; K | J) + I(C^N; J | K) \\ &\leq N\delta(P_e^N) + I(A^N; C^N) - I(J; K) \\ &\leq N[I(A; C) + \delta(P_e^N)], \end{aligned}$$

where we have used Fano's inequality and the chain rule. This concludes the converse proof.

Proof of Theorem 11

To prove the achievability part, we concatenate a lossy source encoder with one time pad encryption using the secret key. Fix an arbitrarily small $\epsilon > 0$ such that D satisfies $R(D) < R_A - \epsilon$. For sufficiently large N , the output of the lossy quantization of A^N at distortion D can be represented by $NR(D) + \epsilon$ bits. Let \bar{A} denote the binary representation of the quantized message, and let W_k be the binary representation of the secret key, which is a Bernoulli(1/2) string of length NR_k . The cryptogram is defined as

$$W = \bar{A} \oplus W_k,$$

where \oplus is the binary addition. Cryptogram W can be transmitted to Bob at rate R_A who can retrieve \bar{A} , and hence reconstruct A with distortion D .

If $R_k \geq R(D)$, then all bits of W are Bernoulli(1/2); from the crypto lemma [49], Eve does not receive any information about the message, hence we have $\Delta = H(A)$. If $R_k < R(D)$, NR_k of the bits of W are Bernoulli(1/2), and Eve can at most receive $N(R(D) - R_k)$ bits. The equivocation rate becomes $H(A) - R(D) + R_k$.

Next, we prove the converse. Let $J \triangleq f(A^N, W_k)$. We have

$$\begin{aligned} I(A^N; J|W_k, M_A, M_B) &= H(J|W_k, M_A, M_B) - H(J|A^N, W_k, M_A, M_B), \\ &= H(J|W_k, M_A, M_B), \end{aligned} \quad (8.44)$$

$$\begin{aligned} &\leq H(J), \\ &\leq NR_A, \end{aligned} \quad (8.45)$$

where Eq. (8.44) follows since J is a deterministic function of (A^N, W_k, M_A) .

On the other hand, we also have

$$\begin{aligned} I(A^N; J|W_k, M_A, M_B) &= H(A^N|W_k, M_A, M_B) - H(A^N|J, W_k, M_A, M_B), \\ &= H(A^N) - H(A^N|J, W_k, M_A, M_B, \hat{A}^N), \end{aligned} \quad (8.46)$$

$$\geq H(A^N) - H(A^N|\hat{A}^N), \quad (8.47)$$

$$\geq \sum_{m=1}^N \left[H(A_m) - H(A_m|\hat{A}_m) \right], \quad (8.48)$$

$$= \sum_{m=1}^N I(A_m; \hat{A}_m), \quad (8.49)$$

where Eq. (8.46) follows since A^N is independent of (W_k, M_A, M_B) and \hat{A}^N is a deterministic function of (J, W_k, M_B) ; Eq. (8.47) follows since conditioning reduces entropy; and Eq. (8.48) follows from the memoryless source assumption.

Combining Eqs. (8.45) and (8.49), and letting $D_m = E[d(A_m, \hat{A}_m)]$, we get

$$R_A \geq \frac{1}{N} \sum_{m=1}^N I(A_m; \hat{A}_m), \quad (8.50)$$

$$\geq \frac{1}{N} \sum_{m=1}^N R(D_m), \quad (8.51)$$

$$\geq R\left(\frac{1}{N} \sum_{m=1}^N D_m\right), \quad (8.52)$$

$$\geq R(D + \epsilon), \quad (8.53)$$

where Eq. (8.51) follows from the rate-distortion function; Eq. (8.52) follows since $R(D)$ is a convex function of D ; and Eq. (8.53) follows since $R(D)$ is a nonincreasing function of D and since $E[d(A^N, \hat{A}^N)] \leq D + \epsilon$.

For the secret key rate, we can write

$$NR_k \geq \log M_k \geq H(W_k),$$

$$\begin{aligned} &\geq H(W_k|J, M_B) - H(W_k|J, \hat{A}^N, M_B), \\ &= H(\hat{A}^N|J, M_B) - H(\hat{A}^N|J, W_k, M_B), \\ &= H(\hat{A}^N|J, M_B), \end{aligned} \tag{8.54}$$

$$\geq N(\Delta - \epsilon) - H(A^N|J) + H(\hat{A}^N|J, M_B), \tag{8.55}$$

$$\begin{aligned} &\geq N(\Delta - \epsilon) - NH(A) + I(A^N; J) - I(\hat{A}^N; J, M_B) + I(A^N; \hat{A}^N) \\ &\quad + H(\hat{A}^N|A^N), \end{aligned} \tag{8.56}$$

$$\begin{aligned} &\geq N(\Delta - H(A) - \epsilon) + \sum_{m=1}^N I(A_m; \hat{A}_m) + I(A^N; J, M_B) - I(\hat{A}^N; J, M_B) \\ &\quad + H(\hat{A}^N|A^N), \end{aligned} \tag{8.57}$$

$$\begin{aligned} &= N(\Delta - H(A) - \epsilon) + \sum_{m=1}^N I(A_m; \hat{A}_m) + H(A^N|A^N, J, M_B) \\ &\quad + I(\hat{A}^N; J, M_B|\hat{A}^N), \end{aligned} \tag{8.58}$$

$$\geq N(\Delta - H(A) - \epsilon) + \sum_{m=1}^N I(A_m; \hat{A}_m), \tag{8.59}$$

$$\geq N(\Delta - H(A) + R(D + \epsilon) - \epsilon), \tag{8.60}$$

where Eq. (8.54) follows since \hat{A}^N is a deterministic function of (J, W_k, M_B) ; Eq. (8.55) follows since (R_A, R_k, D, Δ) is achievable; Eq. (8.56) follows from the chain rule; Eq. (8.57) follows from the memoryless source assumption and the independence of M_B and (J, A^N) ; and Eq. (8.60) follows from Eq. (8.53).

Letting $N \rightarrow \infty$ and $\epsilon \rightarrow 0$, together with the obvious upper bound of $\Delta \leq H(A)$, we obtain the required converse results for Theorem 11.

References

- [1] Pradhan, S.S., Ramchandran, K.: Distributed source coding using syndromes (DISCUS): Design and construction. *IEEE Trans. Inf. Theory* **49**(3), 626–643 (2003)
- [2] Xiong, Z., Liveris, A., Cheng, S.: Distributed source coding for sensor networks. *IEEE Signal Process. Mag.* **21**, 80–94 (2004)
- [3] Girod, B., Aaron, A., Rane, S., Rebollo-Monedero, D.: Distributed video coding. *Proceedings of the IEEE, Special Issue on Video Coding and Delivery* **93**(1), 71–83 (2005)
- [4] Diffie, W., Hellman, M.: New directions in cryptography. *IEEE Trans. Inf. Theory* **22**(6), 644–654 (1976)

- [5] Shannon, C.E.: Communication theory of secrecy systems. *Bell Syst. Tech. J.* **28**, 656–715 (1949)
- [6] Liang, Y., Poor, H.V., Shamai, S.: Information Theoretic Security. In *Found. Trends Commun. Inf. Theory* **5**(4–5), 355–580 (2008).
- [7] Thangaraj, A., Dihidar, S., Calderbank, A.R., McLaughlin, S., J.-M. Merolla: On the application of LDPC codes to a novel wiretap channel inspired by quantum key distribution. <http://arxiv.org/abs/cs/0411003> (2005)
- [8] Bloch, M., Thangaraj, A., McLaughlin, S.W., Merolla, J.M.: LDPC-based secret key agreement over the Gaussian wiretap channel. In: Proc. IEEE Int. Symp. Inf. Theory (ISIT), pp. 1179–1183. Seattle, WA (2006)
- [9] Liu, R., Liang, Y., Poor, H.V., Spasojevic, P.: Secure nested codes for type II wiretap channels. In: Proc. IEEE Inf. Theory Workshop (ITW). Lake Tahoe, CA (2007)
- [10] Vernam, G.S.: Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.* **55**, 109–115 (1926)
- [11] Wyner, A.D.: The wire-tap channel. *Bell Syst. Tech. J.* **54**(8), 1355–1387 (1975)
- [12] Csiszár, I., Körner, J.: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **24**(3), 339–348 (1978)
- [13] Leung-Yan-Cheong, S.K., Hellman, M.E.: The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **24**(4), 51–456 (1978)
- [14] Tekin, E., Yener A.: The Gaussian multiple access wire-tap channel, *IEEE Trans. Inf. Theory* **54**(12), 5747–5755 (2008)
- [15] Liu, R., Maric, I., Spasojevic, P., Yates, R.: Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory* **54**(6), 2493–2507 (2008)
- [16] Liang, Y., Poor, H.V.: Multiple access channels with confidential messages. *IEEE Trans. Inf. Theory* **54**(3), 976–1002 (2008)
- [17] Liang, Y., Poor, H.V., Shamai (Shitz), S.: Secure communication over fading channels. *IEEE Trans. Inf. Theory* **54**(6), 2470–2492 (2008)
- [18] Lai, L., El Gamal, H.: The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory* **54**(9), 4005–4019 (2008)
- [19] Ahlswede, R.: Elimination of correlation in random codes for arbitrarily varying channels. *Z. Wahrscheinlichkeitstheorie verw. Gebiete* **44**(2), 159–175 (1978)
- [20] Csiszár, I., Narayan, P.: The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Trans. Inf. Theory* **34**(2), 181–193 (1988)
- [21] Ahlswede, R., Dueck, G.: Identification via channels. *IEEE Trans. Inf. Theory* **35**(1), 15–29 (1989)
- [22] Maurer, U., Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free. In: Proc. EUROCRYPT, L. N. C. S. Bruges, Belgium (2000)
- [23] Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography part I: Secret sharing. *IEEE Trans. Inf. Theory* **39**(4), 1121–1132 (1993)
- [24] Maurer, U.: Secret key agreement by public discussion. *IEEE Trans. Inf. Theory* **39**(3), 733–742 (1993)
- [25] Csiszár, I., Narayan, P.: Common randomness and secret key generation with a helper. *IEEE Trans. Inf. Theory* **46**(2), 344–366 (2000)
- [26] Csiszár, I., Narayan, P.: Secrecy capacities for multiple terminal. *IEEE Trans. Inf. Theory* **50**(12), 3047–3061 (2004)
- [27] Slepian, D., Wolf, J.K.: Noiseless coding of correlated information sources. *IEEE Trans. Inf. Theory* **19**(4), 471–480 (1973)
- [28] Prabhakaran, V., Ramchandran, K.: On secure distributed source coding. In: Proc. IEEE Inf. Theory Workshop. Lake Tahoe, CA (2007)

- [29] Simmons, G.J.: Authentication theory/coding theory. In: Proc. CRYPTO 84 Adv. Cryptol., pp. 411–431. Springer-Verlag, New York, NY (1985)
- [30] Simmons, G.J.: A cartesian product construction for unconditionally secure authentication codes that permit arbitration. *J. Cryptol.* **2**(2), 77–104 (1990)
- [31] Gündüz, D., Erkip, E., Poor, H.V.: Secure lossless compression with side information. In: Proc. IEEE Inf. Theory Workshop. Porto, Portugal (2008)
- [32] Gündüz, D., Erkip, E., Poor, H.V.: Lossless compression with security constraints. In: Proc. IEEE Int. Symp. Inf. Theory. Toronto, Canada (2008)
- [33] Körner, J., Marton, K.: A source network problem involving the comparison of two channels. In: Trans. Colloq. Inf. Theory. Keszthely, Hungary (1975)
- [34] Luh, W., Kundur, D.: Separate enciphering of correlated messages for confidentiality in distributed networks. In: Proc. IEEE Global Commun. Conf. Washington, DC (2007)
- [35] Grokop, L., Sahai, A., Gastpar, M.: Discriminatory source coding for a noiseless broadcast channel. In: Proc. IEEE Int. Symp. Inf. Theory (ISIT), pp. 77–81. Adelaide, Australia (2005)
- [36] Sgarro, A.: Source coding with side information at several decoders. *IEEE Trans. Inf. Theory* **23**(2), 179–182 (1977)
- [37] Cover, T., Thomas, J.: Elements of Information Theory. John Wiley Sons, Inc., New York (1991)
- [38] Yamamoto, H.: A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers. *IEEE Trans. Inf. Theory* **29**(6), 918–923 (1983)
- [39] Yamamoto, H.: Coding theorems for shannon’s cipher system with correlated source outputs, and common informations. *IEEE Trans. Inf. Theory* **40**(1), 85–95 (1994)
- [40] Yamamoto, H.: A rate-distortion problem for a communication system with a secondary decoder to be hindered. *IEEE Trans. Inf. Theory* **34**(4), 835–842 (1988)
- [41] Gray, R.M.: Conditional rate distortion theory. In: Technical Report 6502-2. Information Systems Laboratory, Stanford, CA (1972)
- [42] Luh, W., Kundur, D.: Distributed keyless security for correlated data with applications in visual sensor networks. In: Proc. ACM Multimedia and Security. Dallas, TX (2007)
- [43] Yamamoto, H.: Rate-distortion theory for the Shannon cipher system. *IEEE Trans. Inf. Theory* **43**(3), 827–835 (1997)
- [44] Wyner, A.D., Ziv, J.: The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. Inf. Theory* **22**(1), 1–10 (1976)
- [45] Merhav, N.: Shannon’s secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Trans. Inf. Theory* **54**(6), 2723–2734 (2008)
- [46] Prabhakaran, V., Ramchandran, K.: A separation result for secure communication. In: Proc. 45th Annual Allerton Conference on Communication, Control, and Computing. Monticello, IL (2007)
- [47] Prabhakaran, V., Eswaran, K., Ramchandran, K.: Secrecy via sources and channels: A secret key-secret message rate trade-off region. In: Proc. IEEE Int. Symp. Inf. Theory. Toronto, Canada (2008)
- [48] Khisti, A., Diggavi, S., Wornell, G.: Secret key generation using correlated sources and noisy channels. In: Proc. IEEE Int. Symp. Inf. Theory. Toronto, Canada (2008)
- [49] Forney, G.D.: On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener. In: Proc. Allerton Conference on Communication, Control, and Computing. Monticello, IL (2003)

Chapter 9

Secret Key Extraction from Level Crossings over Unauthenticated Wireless Channels*

Suhas Mathur, Wade Trappe, Narayan Mandayam,
Chunxuan Ye and Alex Reznik

9.1 Introduction

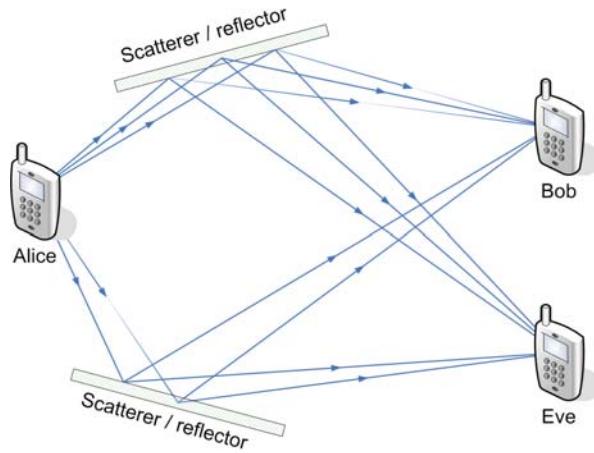
Many of the risks associated with securing wireless systems stem from challenges associated with operating in a mobile environment, such as the lack of a guaranteed infrastructure or the ease with which entities can eavesdrop on communications. Traditional network security mechanisms rely upon cryptographic keys to support confidentiality and authentication services. However, in a dynamic mobile wireless environment, with peer-to-peer associations being formed on-the-fly between mobile entities, it is difficult to ensure availability of a certificate authority or a key management center. Since such scenarios are likely to become more prevalent, it is necessary to have alternatives for establishing keys between wireless peers without resorting to a fixed infrastructure.

We explore an alternative for building cryptographic services by exploiting an untapped resource—the wireless channel itself. The specificity of the radio channel between two wireless devices, and its rapid decorrelation with distance, provide a basis for the creation of shared secret information, such as cryptographic keys, even in the presence of an eavesdropper. In typical multipath environments (see Fig. 9.1), the wireless channel between two users, Alice and Bob, produces a time-varying, stochastic mapping between the transmitted and received signals. This mapping varies with time in a manner that is location-specific and reciprocal, i.e., the mapping is the same whether Alice is the transmitter with Bob as the receiver or vice-versa. The time-varying mapping, commonly termed *fading*, decorrelates over distances of the order of half a wavelength, λ . Thus, an adversary, Eve, who is more than $\lambda/2$

S. Mathur (✉)
Wireless Information Network Laboratory (WINLAB)
Rutgers University, 671 Rt. 1 South
North Brunswick, NJ 08902, USA
e-mail: suhas@winlab.rutgers.edu

*This work is based on an earlier work “Radio-telepathy: Extracting a Cryptographic Key from an Unauthenticated Wireless Channel,” in Proceedings of the 14th Annual International Conference on Mobile Computing and Networking, ©ACM, 2008. <http://doi.acm.org/10.1145/1409944.1409960>.

Fig. 9.1 The multipath fading for a signal from Alice to Bob is different from that for the signal reaching Eve



away from both Alice and Bob, experiences fading channels to Alice and to Bob that are statistically independent of the fading between Alice and Bob. These properties allow us to generate a common, secret cryptographic key at Alice and Bob such that Eve gets no information about the generated key. For example, at 2.4 GHz, we only require that Eve be roughly $\lambda/2 = 6.25$ cm away from Alice and Bob to ensure that she gets no useful information. Thus, while fading is typically considered harmful, we profitably exploit it to extract perfectly secret bits without leaking information to an adversary.

The extraction of secret bits from the wireless channel can be viewed as a ‘black-box’ that can be advantageous in various ways, putting to good use information that is already available from the channel. For example, in the current 802.11i standard, session keys for communication between a station and an AP are derived by hashing together authentication credentials and nonces exchanged in the clear. This ties the confidentiality of future messages to the authentication credentials, and if these credentials are ever compromised then an adversary will be able to derive the session keys and decrypt past encrypted messages. If the nonces can be derived in an information-theoretically secret manner from the channel between two users, then a passive adversary has no means to derive the session keys even if it learns the authentication credentials[1]. Further, session keys can be updated using these secret bits derived from the channel, instead of relying on previously existing keys [1], thus ensuring that the confidentiality of each new session is protected independently of earlier sessions.

Yet another vulnerability in 802.11i stems from the fact that during the establishment of a secure link between a station and an AP, all messages exchanged over the air, including management frames, are sent unencrypted until both parties have obtained the session key (c.f. the *temporal key* (TK) in 802.11) and are therefore susceptible to eavesdropping and to spoofing by other users. While the 802.11w amendment seeks to protect some management frames from such attacks, it too fails to protect messages exchanged before the establishment of TKs. Unfortunately,

securing the initial exchanges between the parties requires them to share a key that is not established until later. Our key extraction mechanism provides a natural solution by allowing the parties to generate a temporary key that protects the interim exchanges before the formal keys are in place.

Ad hoc or peer-to-peer networks present another avenue where our technique can be useful. Alice may not care to establish Bob's identity if she merely wishes to employ his forwarding services. In such a scenario, she may nevertheless wish to establish a confidential link with Bob by using the channel to form a key prior to encrypting subsequent data, thereby preventing eavesdropping.

Prior work in information theory has noted the potential of using the wireless channel for generating shared secret bits (see Sect. 9.7), but most of this work has been aimed at computing theoretical limits and has not provided practical algorithms, nor a demonstrable and quantifiable impact on security. Our contribution may be summarized as follows:

1. We translate prior information-theoretic ideas into a practical protocol applied to wireless channels;
2. We build a new algorithm for key extraction that, unlike prior schemes, does not require an authenticated channel, and study performance for typical fading;
3. We validate our algorithm using channel impulse responses measured using the 802.11a packet preamble on a customized FPGA-based 802.11 development platform and a second study that uses only coarse per-packet RSSI information readily available to off-the-shelf 802.11 platforms.

Existing mobile radio platforms already provide the information we need, but such data are normally discarded after physical layer processing and can be profitably exploited to benefit security. The approach we present augments, rather than replaces existing cryptographic security mechanisms—it provides a new approach to establishing keys that is useful when there is no key management infrastructure.

In Sect. 9.2 we describe our system model and the design issues relevant to our problem, in Sect. 9.3 we describe our key-extraction algorithm in detail, in Sect. 9.4 we evaluate its performance and in Sect. 9.5 we present two experimental studies that validate our algorithm using 802.11a hardware. In Sect. 9.6, we present a discussion on the tradeoffs and security of our key-extraction method, in Sect. 9.7 we review the related literature, and we conclude in Sect. 9.8.

9.2 System Model & Design Issues

The crucial insight that allows the wireless channel to be amenable for generating a secret key is that the received signal at the receiver is modified by the channel in a manner that is unique to the transmitter-receiver pair. This distortion depends critically upon the location of the transmitter, the receiver, and scatterers. Typically, such distortion is estimated at the physical layer of the receiver and the associated distortion information dealt with for reliable physical layer decoding. Since this information is always present and uniquely corresponds to the transmitter-receiver

Table 9.1 A summary of the notation used

Symbol	Meaning
\mathbf{h}	Stochastic channel parameter of interest
$h(t)$	Value of the stochastic process \mathbf{h} at time t
$s(t)$	Probe signal transmitted to estimate $h(t)$
f_d	Maximum Doppler frequency (Hz)
f_s	Rate at which each user sends probes (Hz)
q_+, q_-	Quantizer bin boundaries (Upper and lower resp.)
m	Reqd. min. # of estimates in a excursion
N	Length of key in bits
R_k	Rate of generation of secret bits (s-bits/s)
p_e	Probability of a bit error
p_k	Probability of key mismatch = $1 - (1 - p_e)^N$

pair, it also provides our transmitter (Alice) and receiver (Bob) a means to *privately* establish secret bits associated with this distortion. We now focus on the challenges of using the stochastic nature of the wireless channel to secretly establish bits. We break down our discussion to include a description of: (1) the underlying channel model associated with multipath fading; (2) the tools needed to obtain bits from the channel response; and (3) the design goals that need to be addressed in order to reliably establish these bits. To assist the reader, we provide notation in Table 9.1. Before we begin, we comment on our adversary. We assume an attacker that can either act as an eavesdropper or who may inject messages to impersonate Alice or Bob. We present further considerations of adversarial actions in Sect. 9.6.

9.2.1 Channel Model

Let $h(t)$ be a stochastic process corresponding to a time-varying parameter that describes the wireless channel between Alice and Bob. Although there are many choices for $h(t)$, for our discussion, we shall assume that $h(t)$ is the magnitude of the transfer function of the multipath fading channel between Alice and Bob evaluated at a fixed *test frequency*, f_0 . Implicit in this formulation is the observation that the system transfer function of the channel is the same in the Alice → Bob direction as in the Bob → Alice direction *at a given instant of time*. This follows from reciprocity, which is a fundamental property of electromagnetic wave propagation [2, 3] in a medium and must not be confused with additive noise or interference, which may be different for different receivers. To distinguish between the channel parameter of interest, and its value at a given time, we denote the parameter by \mathbf{h} and refer to its value as $h(t)$. To estimate the parameter \mathbf{h} , Alice and Bob must transmit known probe signals to one another. Each party can then use the received signal along with the probe signal to compute an estimate \hat{h} of \mathbf{h} . Since practical radios are *half duplex* due to hardware constraints, Alice must wait to receive a probe signal from Bob before she can transmit a probe to him and vice-versa. In the time between the two successive probes, $h(t)$ changes slightly in a manner that is modeled by an appropriate probability distribution. The received signal at Alice and Bob due to

successive probes may be written as

$$r_a(t_1) = s(t_1)h(t_1) + n_a(t_1) \quad (9.1)$$

$$r_b(t_2) = s(t_2)h(t_2) + n_b(t_2), \quad (9.2)$$

where $s(t)$ is the known probe signal, n_a & n_b are the independent noise processes at Alice and Bob and t_1 & t_2 are the time instants at which successive probes are received by Alice and by Bob, respectively. Using the received signal, Alice and Bob, each compute (noisy) estimates of \mathbf{h} :

$$\hat{h}_a(t_1) = h(t_1) + z_a(t_1) \quad (9.3)$$

$$\hat{h}_b(t_2) = h(t_2) + z_b(t_2), \quad (9.4)$$

where z_a and z_b represent the noise terms due to n_a and n_b after processing by the function that estimates \mathbf{h} . We refer the reader to [4] for designing good estimators for \mathbf{h} . The estimates \hat{h}_a and \hat{h}_b are in all likelihood unequal, due in part to the independent noise terms and in part to the time lag τ . However they can be highly correlated if Alice and Bob send probes to one another at a fast enough¹ rate, i.e., if $\tau = t_2 - t_1$ is small. By repeatedly sending probes in an alternating manner over the time-varying channel, Alice and Bob can generate a sequence of n estimates $\underline{\hat{h}}_a = \{\hat{h}_a[1], \hat{h}_a[2], \dots, \hat{h}_a[n]\}$ and $\underline{\hat{h}}_b = \{\hat{h}_b[1], \hat{h}_b[2], \dots, \hat{h}_b[n]\}$, respectively, that are highly correlated, as in Fig. 9.2. Although Eve can overhear the probe signals sent by each user, the signals received by Eve are completely different:

$$r_e^b(t_1) = s(t_1)h_{be}(t_1) + n_e(t_1) \quad (9.5)$$

$$r_e^a(t_2) = s(t_2)h_{ae}(t_2) + n_e(t_2), \quad (9.6)$$

where h_{be} and h_{ae} denote the channel between Bob & Eve and between Alice & Eve, respectively, and n_e is the noise added at Eve. If Eve is more than $\sim \lambda/2$ away from Alice and Bob, then h_{ae} and h_{be} are uncorrelated with \mathbf{h} [5]. Therefore, despite possessing knowledge of the probe signal $s(t)$, Eve cannot use her received signals to compute meaningful estimates of the Alice–Bob channel, \mathbf{h} .

9.2.2 Converting the Channel to Bits

Alice and Bob must translate their respective sequences of channel estimates into identical bit-strings suitable for use as cryptographic keys, thus requiring:

1. *Suitably long*: Keys of length 128–512 bits are commonly used in symmetric encryption algorithms. So they should be able to generate at least these many bits in a reasonable amount of time.
2. *Statistically random*: The bits should be random with equal probability of a ‘0’ and a ‘1’. Also, the bit-sequences must not suffer from statistical defects that could be exploited by an attacker.

¹‘Fast enough’ here is in relation to the coherence time of the channel, which is inversely proportional to the maximum Doppler frequency f_d .

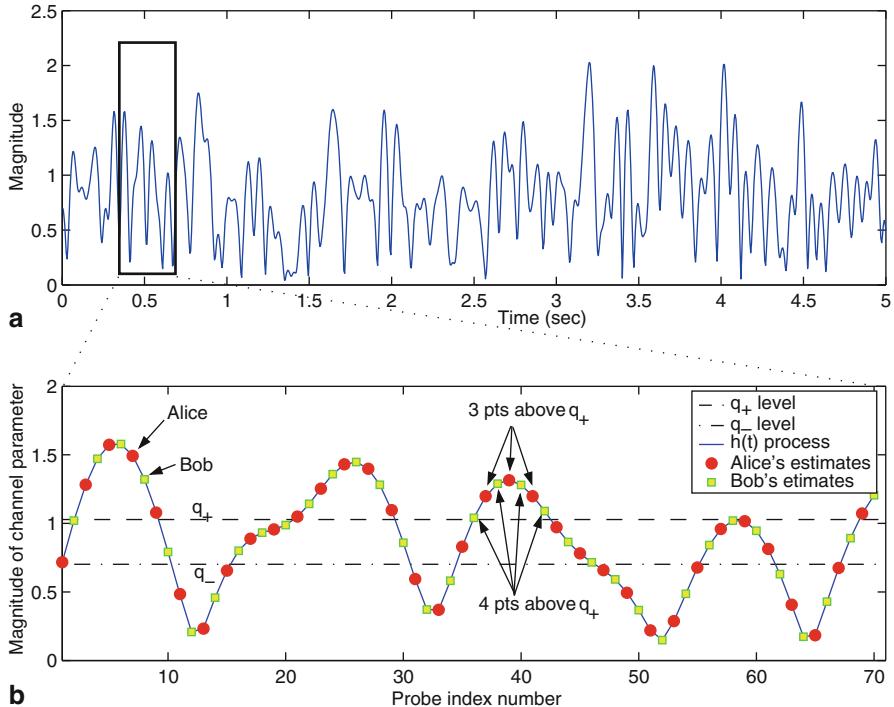


Fig. 9.2 **a** A sample realization of a Rayleigh fading stochastic process. **b** Successive channel estimates of the process by Alice and Bob showing excursions above the q_+ and below the q_- levels on a magnified portion of **a**

The second requirement guarantees that the generated key has desirable security properties. That is, an N -bit key must provide N bits of uncertainty to an adversary who only knows the key generation algorithm and nothing else.

We now briefly describe how to obtain bits from the channel estimates \hat{h}_a and \hat{h}_b , to provide the intuition behind our algorithm, while postponing a formal description to Sect. 9.4. The sequence of channel estimates \hat{h}_a and \hat{h}_b are random variables drawn from an underlying probability distribution that characterizes the channel parameter \mathbf{h} . We assume, for the sake of discussion, that $h(t)$ is a Gaussian random variable and the underlying stochastic process \mathbf{h} is a stationary Gaussian process. A Gaussian distribution for \mathbf{h} may be obtained, for example, by taking \mathbf{h} to be the magnitude of the in-phase component of a Rayleigh fading process between Alice and Bob [2]. We note that the assumption of a Gaussian distribution on \mathbf{h} is for ease of discussion and our algorithm is equally valid in the general case.

Since the channel estimates computed by Alice and Bob are continuous random variables, it is necessary to quantize their estimates using a quantizer $Q(\cdot)$ to obtain bits. However, a straightforward quantization of the vectors \hat{h}_a and \hat{h}_b is not sufficient because it does not guarantee that an identical sequence of bits will be generated at the two users. In our scheme, Alice and Bob use the channel statistics to determine

scalars, q_+ and q_- that serve as reference levels for the quantizer $Q(\cdot)$ as follows:

$$Q(x) = \begin{cases} 1 & \text{if } x > q_+ \\ 0 & \text{if } x < q_- \end{cases} \quad (9.7)$$

This forms the basis for positive and negative excursions, respectively, as explained below. Values between q_- and q_+ are not assigned a bit. Alice parses through her channel estimates \hat{h}_a to determine the locations of *excursions* of her channel estimates above q_+ or below q_- that are of a duration $\geq m$ estimates, i.e., m successive channel estimates in \hat{h}_a are $> q_+$ or $< q_-$, where m is a protocol parameter. She sends Bob a message over the public channel containing the locations of k such excursions in the form of an array of indexes $L = \{l_1, l_2, \dots, l_k\}$. Bob then checks his own sequence \hat{h}_b at the locations specified in L to determine whether it contains an excursion above q_+ or below q_- for a duration greater than or equal to ' $m - 1$ ' samples, i.e., whether $\hat{h}_b(l_i)$ is $> q_+$ or $< q_-$ for a duration that spans $m - 1$ or more estimates, for $i = 1, \dots, k$. Bob identifies ‘good’ indexes by finding all index values l in L that produce such an excursion in \hat{h}_b . He places these indexes into an array \tilde{L} to be sent to Alice publicly. Indexes in L but not in \tilde{L} are dropped from consideration by each party. The indexes in \tilde{L} are used by each user to compute a sequence of bits by quantizing: $Q(\hat{h}_a(\tilde{L}))$ and $Q(\hat{h}_b(\tilde{L}))$. If the bit-vectors $Q(\hat{h}_a(\tilde{L}))$ and $Q(\hat{h}_b(\tilde{L}))$ are equal, then Alice and Bob succeed in generating $|\tilde{L}|$ identical bits. We show later that provided the levels q_+ , q_- and the parameter m are properly chosen, the bits generated by the two users are identical with very high probability. A variation of the protocol that copes with spoofing is detailed in Sect. 9.3.1.

9.2.3 Design Goals

An important quantity of interest will be the rate of generation of secret bits, expressed in secret-bits per second or ‘s-bits/s’. Naturally, it is desirable that Alice and Bob achieve a high secret-bit rate. According to 802.1x recommendations, it is generally desirable for master keys to be refreshed at one hour intervals[6]. Using these examples and AES key sizes of 128 bits as a guideline, a conservative key rate of roughly 0.1 bits per second is needed, though it is desirable to achieve higher secrecy rates. However, we are especially wary of bit errors. If the sequence $Q(\hat{h}_a(\tilde{L}))$ is different from $Q(\hat{h}_b(\tilde{L}))$ even by a single bit, then the two bit-strings cannot be used as cryptographic keys and consequently the entire batch of bits must be discarded. Therefore, we would like the bit error probability p_e to be extremely low, so that the probability p_k that the keys generated by the two users do not match is acceptably small. For example, in order to have a key-mismatch probability of $p_k = 10^{-6}$, assuming keys of length 128 bits, we must target a bit-error probability of p_e where

$$p_k = 1 - (1 - p_e)^{128}, \quad (9.8)$$

which gives $p_e \sim 10^{-8}$. A bit-error is defined as the event that Alice and Bob agree to use a certain index l_i contained in the list \tilde{L} for generating a bit, but they end up

generating different bits, i.e., \hat{h}_a and \hat{h}_b both lie in excursions at the index l_i but the excursions are of opposite types.

The rate at which secret bits can be extracted from the channel is fundamentally limited by the rate of time-variation in the channel. We quantify this variation by the *maximum Doppler frequency*, f_d . In a fading channel, f_d determines both the rate at which the channel varies and the magnitude of the swings produced. A simple measure of the maximum Doppler frequency in a given wireless environment is given by $f_d = \frac{v}{\lambda}$, where v is a measure of the effects of user mobility and the dynamic environment around the users, expressed in meters/s and λ is the wavelength of the carrier wave. In our case $\lambda = \frac{c}{f_0}$, where c is the speed of light. It can be seen that increasing the value m or the magnitudes of the quantizer boundaries q_+ & q_- would not only result in a lower rate, but also a lower probability of error. Intuitively, this is because larger magnitudes of q_+ & q_- , or a larger value of m makes it less likely that Alice's and Bob's channel estimates lie in opposite type of excursions, thereby reducing the error rate. However, both types of excursions also become less frequent, thereby decreasing the number of secret bits that can be generated per second.

Thus, there is a tradeoff between rate and probability of error, and the parameters q_+ , q_- and m provide convenient controls to select suitable operating points over this tradeoff. Beyond rate and robustness, we also require the bits to be random and free from statistical defects, as discussed in Sect. 9.4.3.

Finally, the correlated information obtained by Alice and Bob can be utilized to build a secret key in a number of different ways and it is important to make sure the method employed does not allow Eve to infer any useful information. An alternative bit extraction scheme is to have each user estimate a statistical measure of the channel (e.g., the mean signal-strength, or variance in the estimates) using \hat{h}_a and \hat{h}_b respectively. If the channel is stochastically stationary, then their respective statistical measures would each converge to the true value with time. In this way, Alice and Bob will each possess knowledge about a numerical quantity, without having sent messages over the air containing this quantity. They could then quantize their estimates of the statistical measure to generate bits. However, the trouble with using a statistical measure is that knowledge of the locations of Alice and Bob and their environment may allow Eve to infer the statistics of the channel between them. Indeed, publicly available tools, such as the WISE ray-tracer [7], make it easy to predict the signal statistics at a receiver given the knowledge of the locations of the transmitter and receiver and the building's layout. Thus, it is important to recognize that using a statistical measure for key generation can be perilous. Our algorithm avoids statistical measures by relying on specific instantiations of the fading process.

9.3 Level-Crossing Algorithm

We now detail our level-crossing based key-extraction algorithm. It is assumed that when the algorithm is run, Alice and Bob have collected a sufficiently large number of channel estimates \hat{h}_a and \hat{h}_b , by alternately probing the channel between themselves.

Further, it is assumed that the vectors \hat{h}_a and \hat{h}_b are of equal length and their j^{th} elements $\hat{h}_a(j)$ and $\hat{h}_b(j)$ correspond to successive probes sent by Bob and Alice respectively, for each $j = 1, \dots, \text{length}(\hat{h}_a)$. Algorithm 1 describes the procedure and consists of the following steps:

1. Alice parses the vector \hat{h}_a containing her channel estimates to find instances where m or more successive estimates lie in an excursion above q_+ or below q_- .
2. Alice selects a random subset of the excursions found in step 1 and for each selected excursion, she sends Bob the index of the channel estimate lying in the center of the excursion, as a list L . Therefore, if $\hat{h}_a(i) > q_+$ or $< q_-$ for some $i = i_{\text{start}}, \dots, i_{\text{end}}$, then she sends Bob the index $i_{\text{center}} = \lfloor \frac{i_{\text{start}}+i_{\text{end}}}{2} \rfloor$.
3. For each index from Alice, Bob checks whether his vector of estimates \hat{h}_b contains at least $m - 1$ channel estimates centered around that index in an excursion above q_+ or below q_- , i.e., whether $\hat{h}_b > q_+$ or $< q_-$ for each index $\{l - \lfloor \frac{m-2}{2} \rfloor, \dots, l + \lceil \frac{m-2}{2} \rceil\}$, for each $l \in L$.
4. For some of the indexes in L , Bob's channel estimates do not lie in either excursion. Bob makes a list \tilde{L} of all indexes that lie in excursions and sends it to Alice.
5. Bob and Alice compute $Q(\hat{h}_a)$ and $Q(\hat{h}_b)$ respectively at each index in \tilde{L} , thus generating a sequence of bits.

Algorithm 1: The basic level crossing algorithm

Input : \hat{h}_a and \hat{h}_b
Output : A cryptographic key $K_a = K_b$ at Alice and Bob
Alice:

```

for  $i = 1$  to  $\text{length}(\hat{h}_a) - m$  do
  if  $Q(\hat{h}_a[i]) = Q(\hat{h}_a[i+1]) = \dots = Q(\hat{h}_a[i+m-1])$  then
     $i_{\text{end}} \leftarrow$  last index in excursion
     $L' \leftarrow [L'; \lfloor \frac{i+i_{\text{end}}}{2} \rfloor]$ 
     $i \leftarrow i_{\text{end}} + 1$ 
  else
     $| i \leftarrow i + 1$ 
  end
end

```

$L =$ Random subset of L'
Alice sends L to Bob on PUBLIC_CHANNEL .

Bob:

```

for  $l \in L$  do
  if  $Q(\hat{h}_b(l - \lfloor \frac{m-2}{2} \rfloor)) = \dots = Q(\hat{h}_b(l + \lceil \frac{m-2}{2} \rceil))$  then
     $| \tilde{L} \leftarrow [\tilde{L}; l]$ 
  end
end
 $K_b = Q(\hat{h}_b(\tilde{L}))$ 
Bob sends  $\tilde{L}$  to Alice on PUBLIC_CHANNEL .

```

Alice:

```

 $K_a = Q(\hat{h}_a(\tilde{L}))$ 

```

Since Eve's observations from the channel probing do not provide her with any useful information about \hat{h}_a and \hat{h}_b , the messages L and \tilde{L} do not provide her any useful information either. This is because they contain time indexes only whereas

the generated bits depend upon the values of the channel estimates at those indexes. Further, the selection of a random subset in Step 2 from the set of eligible excursions found in Step 1, guarantees that Eve cannot use L and \tilde{L} to infer the values of the channel estimates of Alice or Bob at those time indexes.

Algorithm 2: Modified algorithm incorporating data-origin authentication and resistance to an active attack.

```

Input :  $\hat{h}_a$  and  $\hat{h}_b$ 
Output : A cryptographic key  $\bar{K}_a = \bar{K}_b$  at Alice and Bob
Alice:
for  $i = 1$  to  $\text{length}(\hat{h}_a) - m$  do
    if  $Q(\hat{h}_a[i]) = Q(\hat{h}_a[i + 1]) = \dots = Q(\hat{h}_a[i + m - 1])$  then
         $i_{end} \leftarrow$  last index in excursion
         $L' \leftarrow [L'; \lfloor \frac{i+i_{end}}{2} \rfloor]$ 
         $i \leftarrow i_{end} + 1$ 
    else
         $i \leftarrow i + 1$ 
    end
end

 $L$  = Random subset of  $L'$ 
Alice sends  $L$  to Bob on PUBLIC_CHANNEL.

Bob:
for  $l \in L$  do
    if  $Q(\hat{h}_b(l - \lfloor \frac{m-2}{2} \rfloor)) = \dots = Q(\hat{h}_b(l + \lceil \frac{m-2}{2} \rceil))$  then
         $\tilde{L} \leftarrow [\tilde{L}; l]$ 
    end
end

if  $\left\{ \frac{|\tilde{L}|}{|L|} < 0.5 + \epsilon \right\}$  then
    | DECLARE ACTIVE ATTACK
else
     $K_b = Q(\hat{h}_b(\tilde{L}))$ 
     $K_{au} = K_b(1, \dots, N_{au})$ 
     $\bar{K}_b = K_b(N_{au} + 1, \dots, N)$ 
     $Package = \{\tilde{L}, MAC(K_{au}, \tilde{L})\}$ 
    Bob sends Package to Alice on PUBLIC_CHANNEL.
end

Alice:
 $K_a = Q(\hat{h}_a(\tilde{L}))$ 
 $K_{au} = K_a(1, \dots, N_{au})$ 
 $\bar{K}_a = K_a(N_{au} + 1, \dots, N)$ 
if MAC validation using  $K_{au}$  fails then
    | DECLARE ACTIVE ATTACK
end
```

9.3.1 Preventing a Spoofing Attack

Since Alice and Bob do not share an authenticated channel, Eve can impersonate Alice in Step 2, or Bob in Step 4 above. Such an attack would allow Eve to insert her own ‘fake’ L or \tilde{L} messages, thus spoofing a legitimate user and disrupting the protocol without revealing her presence. Therefore we require a form of *data-origin*

authentication, that assures each user that the L or \tilde{L} message has originated at the legitimate transmitter.

Our protocol can be made to detect the adversary in each of the two cases above. We first focus on Eve inserting a fake L -message. Since Eve has no information about the locations of channel excursions apart from L , she can only make random guesses about which indexes to place into a fake L -message to Bob (apart from the ones Eve learns from L). If Eve inserts a significant number of random guesses into a fake L -message, Bob can detect her presence by computing the proportion of indexes in L that lead to excursions in \hat{h}_b . Since Eve can only make random guesses, this quantity would be much lower than one resulting from a legitimate L -message from Alice. For each guess, she has a very low probability of choosing an index that lies in an excursion spanning $(m - 1)$ or more estimates at Bob. Of these, the indexes that do not lie in an excursion in \hat{h}_b are discarded by Bob while those that do happen to lie in an excursion are considered eligible for quantization and placed into the \tilde{L} -message sent to Alice. Thus, an unsuccessful guess provides no benefit to Eve, while a successful guess, albeit improbable, causes \tilde{L} to contain an index that was not present in L , thereby alerting Alice. Thus, Eve must also modify the message \tilde{L} by deleting this index before it reaches Alice. Our protocol can be made to resist modification of the \tilde{L} -message using a *message authentication code* (MAC), by the following *additional* steps:

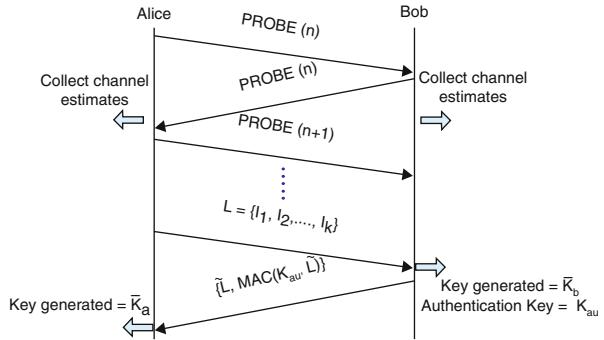
1. To make sure the L -message received is from Alice, Bob computes the fraction of indexes in L where \hat{h}_b lies in an excursion spanning $(m - 1)$ or more estimates. If this fraction is less than $\frac{1}{2} + \epsilon$, for some fixed parameter $0 < \epsilon < \frac{1}{2}$, Bob concludes that the message was not sent by Alice, implying an adversary has injected a fake L -message.
2. If the check above passes, Bob replies to Alice with a message \tilde{L} containing those indexes in L at which \hat{h}_b lies in an excursion. Bob computes $K_b = Q(\hat{h}_b(\tilde{L}))$ to obtain N bits. The first N_{au} bits are used as an authentication key to compute a message authentication code (MAC) of \tilde{L} . The remaining $N - N_{au}$ bits are kept as the extracted secret key. The overall message sent by Bob is $\{\tilde{L}, MAC(K_{au}, \tilde{L})\}$.

Upon receiving this message from Bob, Alice uses \tilde{L} to form the sequence of bits $K_a = Q(\hat{h}_a(\tilde{L}))$. She uses the first N_{au} bits of K_a as the authentication key $K_{au} = K_a(1, \dots, N_{au})$, and using K_{au} she verifies the MAC to confirm that the package was indeed sent by Bob. Since Eve does not know the bits in K_{au} generated by Bob, she cannot modify the \tilde{L} -message without failing the MAC verification at Alice.

Even without an authenticated channel, Alice and Bob can successfully establish a common secret key despite an active adversary, provided there are no bit errors. This explains why we insist on a very low probability of error in Sect. 9.2.3. Further, the reduction in the secret-bit rate is negligible over a long run of the protocol because the N_{au} bits are a one-time expense that allow Alice and Bob to bootstrap data-origin authentication. A modified algorithm that incorporates the above ideas is presented as Algorithm 2 (see Fig. 9.3).

Another active attack involves Eve impersonating Alice or Bob during the channel-probing stage, i.e., Eve may begin sending probes to Bob pretending to be Alice or

Fig. 9.3 Timing diagram for the key-extraction protocol



vice-versa. Such an attack can be detected using a hypothesis testing approach on the recent history probes received at each legitimate user, and this has been extensively studied in [8, 9]. The technique relies on the insight that given a sufficiently fast probing rate, successive probes received by a user are most likely to differ by a small amount. We provide further discussion related to the security of our scheme in Sect. 9.6.

9.4 Performance Evaluation

The central quantities of interest in our protocol are the rate of generation of secret bits, the probability of error and the randomness of the generated bits. The controls available to us are the parameters: q_+ , q_- , m and the rate at which Alice and Bob probe the channel between themselves, f_s . We assume the channel is not under our control, and as explained in Sect. 9.2.3, the rate at which the channel varies can be represented by the maximum Doppler frequency, f_d . The typical Doppler frequency for indoor wireless environments at the carrier frequency of 2.4 GHz is $f_d = \frac{v}{\lambda} \sim \frac{2.4 \times 10^9}{3 \times 10^8} = 8$ Hz, assuming a velocity v of 1 m/s. We thus expect typical Doppler frequencies in indoor environments in the 2.4 GHz range to be roughly 10 Hz and 20 Hz in the 5 GHz range. For automobile scenarios, we can expect a Doppler of ~ 200 Hz in the 2.4 GHz range.

9.4.1 Probability of Error

The probability of error, p_e is critical to our protocol. In order to achieve a robust key-mismatch probability p_k , the bit-error probability p_e must be much lower than p_k . A bit-error probability of $p_e = 10^{-7} \sim 10^{-8}$ is desirable for keys of length $N = 128$ bits. We have explained in Sect. 9.2.3 that there is a fundamental trade-off in the selection of parameters m , q_+ and q_- that affects the rate and probability of error in opposing ways.

The probability of bit-error, p_e is the probability that a single bit generated by Alice and Bob is different at the two users. The symmetry of the distribution of \mathbf{h} allows us to consider just one type of bit error in computing p_e . Consider the probability that Bob generates the bit “0” at an index given that Alice has chosen this index but she has generated the bit “1”. As per our Gaussian assumption on the parameter \mathbf{h} and estimates \hat{h}_a and \hat{h}_b , this probability can be expanded as

$$P(B = 0|A = 1) = \frac{P(B = 0, A = 1)}{p(A = 1)} = \frac{\overbrace{\int_{q_+}^{\infty} \int_{-\infty}^{q_-} \cdots \int_{q_+}^{\infty}}^{(2m-1) \text{ terms}} \frac{(2\pi)^{(1-2m)/2}}{|K_{2m-1}|^{1/2}} \exp \left\{ -\frac{1}{2} x^T K_{2m-1}^{-1} x \right\} d^{(2m-1)} x}{\overbrace{\int_{q_+}^{\infty} \cdots \int_{q_+}^{\infty}}^{(m) \text{ terms}} \frac{(2\pi)^{-m/2}}{|K_m|^{1/2}} \exp \left\{ -\frac{1}{2} x^T K_m^{-1} x \right\} d^m x}, \quad (9.9)$$

where K_m is the covariance matrix of m successive Gaussian channel estimates of Alice and K_{2m-1} is the covariance matrix of the Gaussian vector $(\hat{h}_a[1], \hat{h}_b[1], \hat{h}_a[2], \dots, \hat{h}_b[m-1], \hat{h}_a[m])$ formed by the combining m channel estimates of Alice and the $m-1$ estimates of Bob in chronological order. The numerator in Eq. (9.9) is the probability that of $2m-1$ successive channel estimates (m belonging to Alice, and $m-1$ for Bob), all m of Alice’s estimates lie in an excursion above q_+ while all $m-1$ of Bob’s estimates lie in an excursion below q_- . The denominator is simply the probability that all of Alice’s m estimates lie in an excursion above q_+ .

We compute these probabilities for various values of m and present the results of the probability of error computations in Fig. 9.4. The results confirm that a larger value of m will result in a lower probability of error, as a larger m makes it less

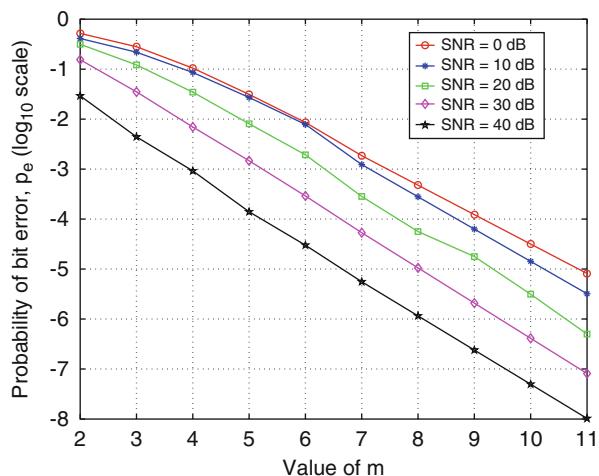


Fig. 9.4 Probability of bit error p_e for various values of m at different SNR levels ($q_{\pm} = \text{mean} \pm 0.8\sigma$)

likely that Alice's and Bob's estimates lie in opposite types of excursions. Note that if either user's estimates do not lie in an excursion at a given index, a bit error is avoided because that index is discarded by both users.

9.4.2 Secret-Bit Rate

The correct way to address the tradeoff between probability of error and rate of generation of secret bits is to upper bound the acceptable probability of error and then attempt to derive the greatest possible rate. How many s-bits/second can we expect to derive from a time-varying channel? An approximate analysis can be done using the level-crossing rate for a Rayleigh fading process, given by $LCR = \sqrt{2\pi} f_d \rho e^{-\rho^2}$ [2], where f_d is the maximum Doppler frequency and ρ is the threshold level, normalized to the root mean square signal level. Setting $\rho = 1$, gives $LCR \sim f_d$.

The above calculation tells us that we cannot expect to obtain more s-bits per second than the order of f_d . In practice, the rate of s-bits/sec depends also on the channel probing rate f_s , i.e., how fast Alice and Bob are able to send each other probe signals. In Fig. 9.5 a, b, we plot the rate in s-bits/sec as a function of the channel probing rate for a wireless channel with maximum Doppler frequencies of $f_d = 10$ Hz and $f_d = 100$ Hz respectively. As expected, the number of s-bits the channel yields increases with the probing rate, but saturates at a value on the order of f_d . More precisely, the number of s-bits/sec is the number of s-bits per observation times the probing rate. Therefore,

$$R_k = H(bins) \times p(A = B) \times \frac{f_s}{m} \quad (9.10)$$

$$= 2 \frac{f_s}{m} \times p(A = 1, B = 1) \quad (9.11)$$

$$= 2 \frac{f_s}{m} \underbrace{\int_{q_+}^{\infty} \dots \int_{q_+}^{\infty}}_{(2m-1) \text{ terms}} \frac{(2\pi)^{\frac{1-2m}{2}}}{|K_{2m-1}|^{1/2}} e^{\left\{-\frac{1}{2}x^T K_{2m-1}^{-1} x\right\}} d^{2m-1} x, \quad (9.12)$$

where $H(bins)$ is the entropy of the random variable that determines which bin ($> q_+$ or $< q_-$) of the quantizer the observation lies in, which in our case equals 1 assuming that the two bins are equally likely.² The probing rate f_s is normalized by a factor of m because a single 'observation' in our algorithm is a sequence of m channel estimates. The expression in (9.12) is reminiscent of the probability of error expression in Eq. (9.9) and has been evaluated in Fig. 9.5.

Figure 9.5 confirms the intuition that the secret bit rate must fall with increasing m , since the longer duration excursions required by a larger value of m are less frequent. In Fig. 9.6a, we investigate how the secret-bit rate R_k varies with the maximum Doppler frequency f_d , i.e., versus the channel time-variation. We found that for a

²The levels q_+ and q_- are chosen so as to maintain equal probabilities for the two bins.

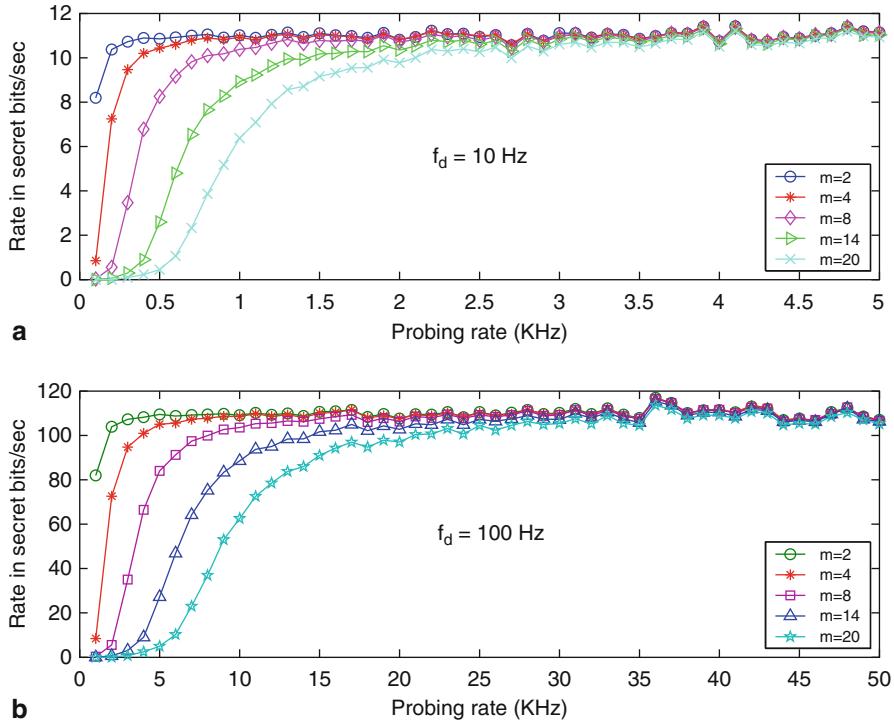


Fig. 9.5 Rate in secret bits per second for various values of m , against probing rate for a channel with Doppler frequency **a** $f_d = 10 \text{ Hz}$ and **b** $f_d = 100 \text{ Hz}$ ($q_{\pm} = \text{mean} \pm 0.8\sigma$)

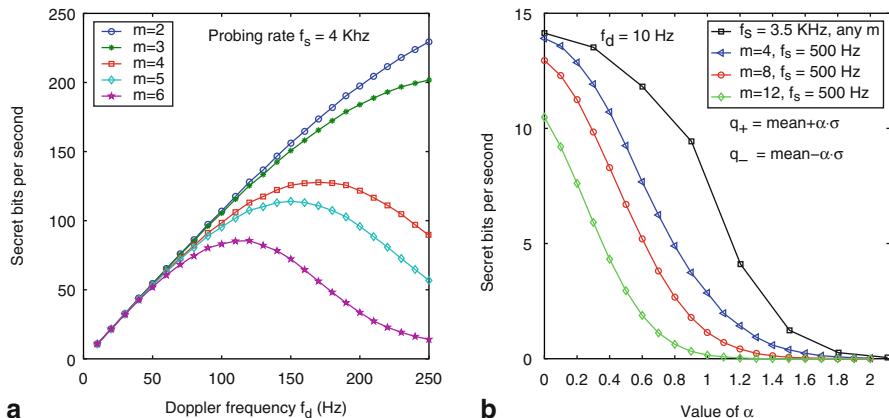


Fig. 9.6 **a** Secret-bit rate for varying Doppler f_d and fixed f_s for various values of m **b** Rate as a function of function of quantizer levels q_+ & q_- parametrized by α

fixed channel probing rate (in this case, $f_s = 4000$ probes/s), increasing f_d results in a greater rate but only up to a point, after which the secret-bit rate begins to fall. Thus, ‘running faster’ does not always help unless we can increase the probing rate f_s proportionally. This suggests that not only does each channel have an optimal minimum probing rate for deriving the best possible secret-bit rate, but each probing rate also corresponds to a most ‘useful’ maximum Doppler frequency. Fig. 9.6b shows the expected decrease in rate as the quantizer levels q_+ and q_- are increased in magnitude. In this figure, α denotes the number of standard deviations from the mean at which the quantizer levels are placed.

9.4.3 Randomness of Generated Bits

Guaranteeing that the generated bits are random is crucial because they are intended for use as a cryptographic key. Since we have assumed the adversary possesses complete knowledge of our algorithm, any non-random behavior in the bit sequences can be exploited by the adversary to reduce the time-complexity of cracking the key. For example, if the algorithm is known to produce a greater proportion of ‘1’s than ‘0’s, then the effective search space for the adversary would be reduced. Consequently, a variety of statistical tests have been devised to test for various defects [10].

In evaluating the randomness of bit sequences generated by our algorithm, we focus on Maurer’s universal statistical test [11], a widely accepted benchmark for testing randomness. The test statistic relates closely to the per-bit entropy of the sequence, and thus measures the actual cryptographic significance of a defect as related to the running time of an adversary’s optimal key-search strategy [11].

Additionally, we ran a few other tests using the NIST public-domain test suite[12]. We refer the interested reader to [13] for a description of these tests and the definitions of *p-value* for each test. The results for these are summarized in Table 9.2. Subsequent runs produced comparable results and thus support the conclusion that our algorithm provides random bits. In particular, Maurer’s test showed the average entropy of our bit-sequences is very close to the value expected for a truly random sequence. This can be possible only if successive bits are almost independent, which in turn requires

Table 9.2 Results from randomness tests on bit sequences (10^8 bits) produced by our algorithm for $f_d = 10$ Hz, $f_s = 30$ Hz, $m = 5$ and $q_+, q_- = \text{mean} \pm 0.2\sigma$

Test	P-value
Maurer’s Test	0.8913
Monobit frequency	0.9910
Runs Test	0.1012
Approx. entropy	0.8721
Random excursions	0.5829
Lempel Ziv	1.0000

In each test, a *p-value* > 0.01 indicates the sequence is random

that they must be separated in time by at least a ‘coherence time’ interval. Since the coherence time of a channel is inversely proportional to the Doppler frequency, extracting bits from a channel at a rate significantly greater than f_d cannot possibly produce random bits using level crossings. We observed in Sect. 9.4.2 that the rate at which our algorithm generates secret bits is bounded from above by approximately the maximum Doppler f_d . Finally, we note that the selection of a random subset of excursions by Alice effectively allows her some control on selecting the final key generated. Thus, even if a particular run happens to produce excursions at Alice containing a statistical defect in the resulting bit sequence, she can fix the defect to some extent by suitably choosing L from among eligible excursions.

9.5 Validation Using 802.11a

We now describe our experimental validation efforts for typical indoor environments. Our experiments were divided in two parts. In the first study, we delved into the structure of an 802.11 packet to access the preamble sequence [14] in the received signal to compute a 64-point *channel impulse response* (CIR) that showed one or more resolvable dominant paths as separate peaks. We used the magnitude of the tallest peak in the CIR (the dominant multipath) as the channel our parameter of interest. To access signal information at the sample level, we used an 802.11 development platform with FPGA-based customized logic added for processing CIR. Our results showed that our algorithm works very well for both static and mobile scenarios, producing error-free secret bits at rates ~ 1 s-bits/sec in the tested indoor environments.

Encouraged by the CIR results, we sought to determine whether unmodified off-the-shelf 802.11 hardware could achieve comparable results. Therefore, for the second study, we used coarse RSSI measurements reported in the Prism headers of 802.11 packets exchanged between commercially available 802.11a radios, with Alice configured as an access point (AP mode) and Bob as a client (station mode), and a third user configured to listen (station mode) on transmissions from both legitimate users.

9.5.1 CIR Method Using 802.11a

9.5.1.1 Experiment Setup

Our experimental platform (Fig. 9.7a) consisted of an 802.11 development board with commercial 802.11a/b/g modem IP, to which we added custom logic to extract the channel impulse response from received packets. This allowed us to pull out received signal information at a level not normally accessible using commodity 802.11 hardware and drivers. Two such boards were set up as Alice and Bob, while a third board was configured to be Eve. Alice was configured to be an access point (AP mode), and Bob was configured to be a client (station mode). The experiment involved Bob sending PROBE request messages to Alice, who then replied with



Fig. 9.7 **a** Our experimental platform—a development board for a commercial 802.11a/b/g modem IP, to which we added custom logic to process CIR information. **b** Timing diagram for collecting CIR information using PROBE packets

a PROBE response message (Fig. 9.7b). Limitations of our development boards allowed us to have Eve listen on either Alice or Bob, but not both. In the results presented here, Eve has been configured to listen in on Alice. In the first experiment, Alice and Eve were placed in a laboratory, while Bob was placed in an office cubicle outside the lab, see Fig. 9.8. In the second experiment, Alice and Eve remained in the same positions while Bob circled the cubicle area along the trajectory in Fig. 9.8 in a cart on wheels.

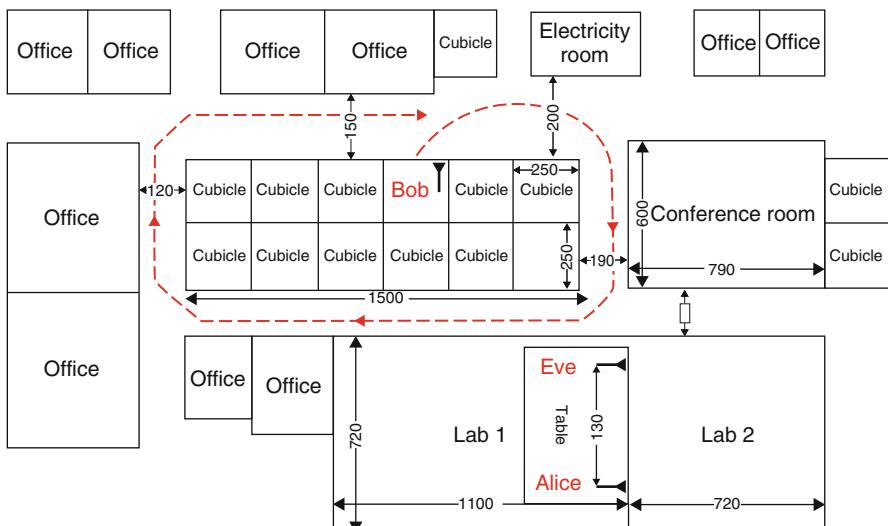


Fig. 9.8 A layout of the experimental setup for the CIR method (distances in cm)

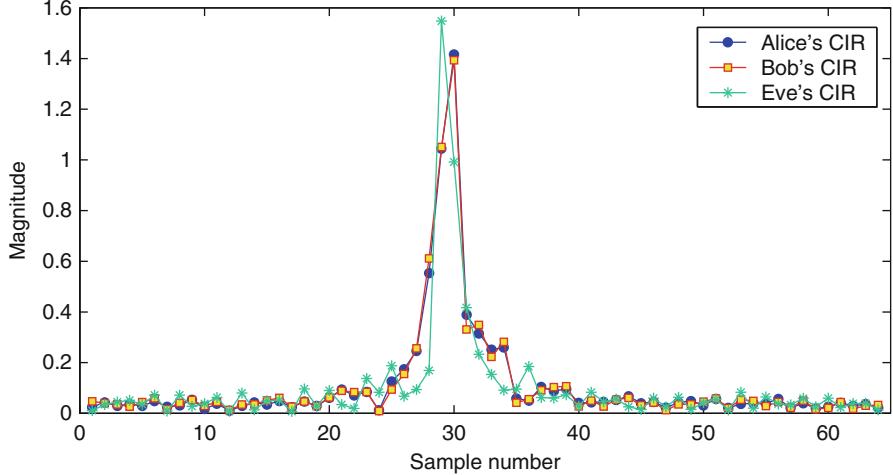


Fig. 9.9 The 64-point CIR from a single 802.11 packet. For our key-extraction algorithm, we use the magnitude of the main peak as the channel parameter of interest

Figure 9.9 shows a 64-point CIR obtained from a single 802.11a PROBE request packet received at Alice, along with the corresponding CIR computed from the PROBE response packet received by Bob in reply. Also shown is the CIR as computed by Eve, using the overheard PROBE response packet from Alice. For the purpose of our algorithm, we use only the magnitude of the main peak in the CIR.

Figure 9.10 shows the traces of the CIR’s main peak’s magnitude at Alice and Bob for our first experiment. While our experiment ran for ~ 22 min, in the interest of space and clarity we show 700 CIRs collected over a duration of ~ 77 s. The traces show significant changes in average signal power, ostensibly due to time-variations in the wireless environment between Alice and Bob (see Fig. 9.8). If each user simply uses this data as input to the level-crossing bit-extraction algorithm, the generated key has long strings of 1s and 0s (see Fig. 9.10). This is because we are attempting to include the effect of *shadow fading* [2] (also called large-scale fading) that produces large but slow swings in the average signal power into the key generation algorithm. In other words, the channel in Fig. 9.10 is not stationary. Each user locally computes q_+ and q_- as:

$$q_+^u = \text{mean}(\hat{h}_u) + \alpha \cdot \sigma(\hat{h}_u) \quad (9.13)$$

$$q_-^u = \text{mean}(\hat{h}_u) - \alpha \cdot \sigma(\hat{h}_u), \quad (9.14)$$

where u can be Alice or Bob, \hat{h}_u is the set of magnitudes of the CIR’s main peak collected by user u , and $\sigma(\hat{h}_u)$ represents the standard deviation of \hat{h}_u . The factor α can be selected to vary the quantizer levels. We chose $\alpha = \frac{1}{8}$ for the CIR-method. The effect of the underlying shadow fading contained in the collected data can be removed by subtracting a moving average of each trace from the original trace. This

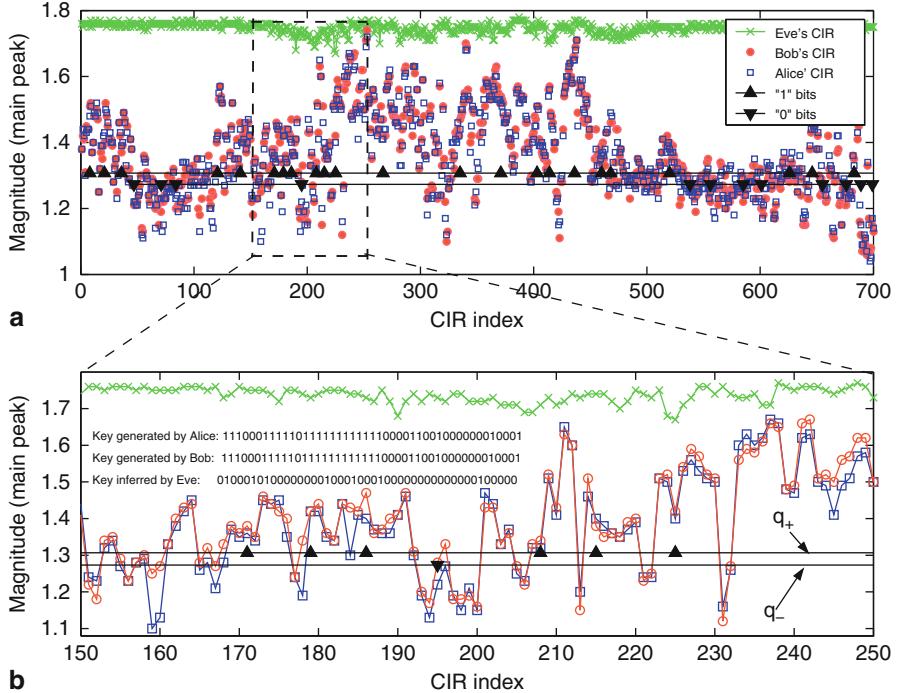


Fig. 9.10 **a** Traces of Alice, Bob and Eve. Variation in avg. signal power produces longs strings of 1s and 0s. **b** A magnified portion of the traces

leaves only the small scale fading that we wish to use in our algorithm. The result is shown in Fig. 9.11. In this way, not only do we do away with the problem of long strings of 1s and 0s, we also prevent the average signal power from affecting our key generation process. Using the small scale fading traces, our algorithm generates $N = 125$ s-bits in 110 s ($m = 4$), yielding a key rate of about 1.13 s-bits/s.

9.5.1.2 Contrasting Eve's Attempts

Figure 9.10 shows a trace of Eve's CIR peak as overheard from Alice along with Alice's and Bob's traces. Figure 9.11 shows the bits that Eve would generate if she carried through with the key-generation procedure. The mutual information [15] (M.I.) between Eve's data and Bob's data is a useful measure of the information learned by Eve about Bob's measurements \hat{h}_b and can be compared to the mutual information between Alice's and Bob's estimates \hat{h}_a and \hat{h}_b . Table 9.3 gives these mutual information values computed using the method in [16]. As a consequence of the data processing inequality [15], any processing of the received signal by Eve would only reduce her information about the Alice-Bob channel, and therefore, the M.I. values in Table 9.3 provide upper bounds on the information about the Alice-Bob channel leaked out to Eve. The results from our second experiment with

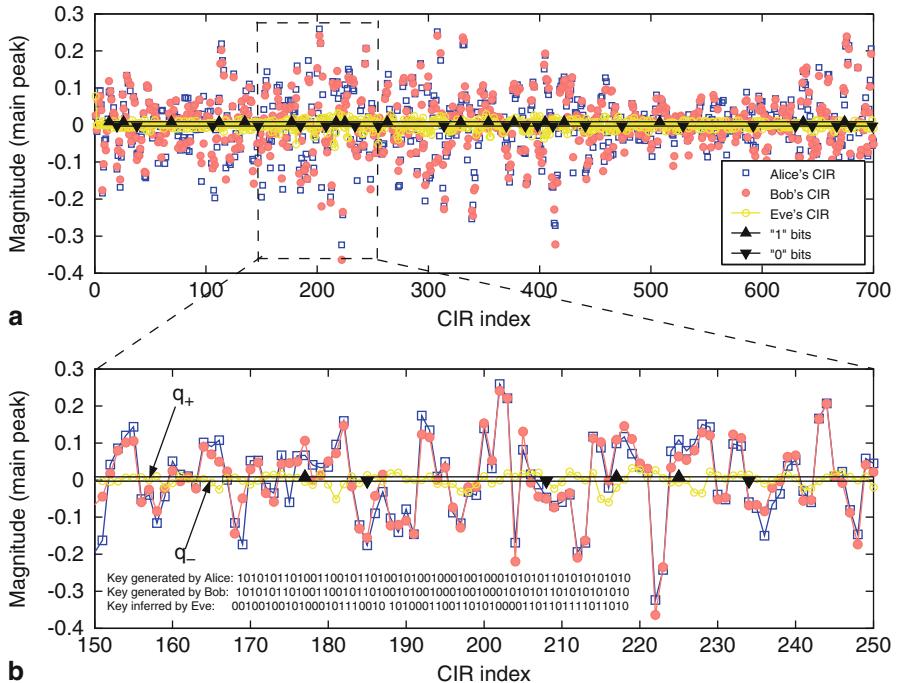


Fig. 9.11 **a** Traces of Alice and Bob after subtracting average signal power. Using $m = 5$, $N = 59$ bits were generated in 110 s ($R_k = 0.54$ s-bits/sec) while $m = 4$ gives $N = 125$ bits ($R_k = 1.13$ s-bits/s.) with no errors in each case. **b** A magnified portion of **a**

a moving Bob are very similar to the ones shown for the first experiment, although with fewer bits produced. Due to space limits, we do not present plots for the mobile experiment but instead summarize our results in Table 9.3. It is notable that in the static case the M.I. between Eve and Bob is orders of magnitude smaller than that between Alice and Bob and very close to zero, indicating that Eve is unable to derive any significant information about the Alice-Bob channel. Further, the M.I. between Eve and Bob is lower in the mobile case compared to the static case, indicating that mobility actually helps strengthen the secrecy of generated keys.

9.5.2 Coarse Measurements Using RSSI

9.5.2.1 Experiment Setup

The setup consisted of three off-the-shelf 802.11 radios. Alice was configured in AP mode along with a virtual monitor interface to capture received packets. Bob was a client, consisting of a laptop with a 802.11a card in station mode, along with virtual monitor for capturing received packets. Eve was a third 802.11a node, identical in configuration to Bob, but capable of receiving packets from both Alice

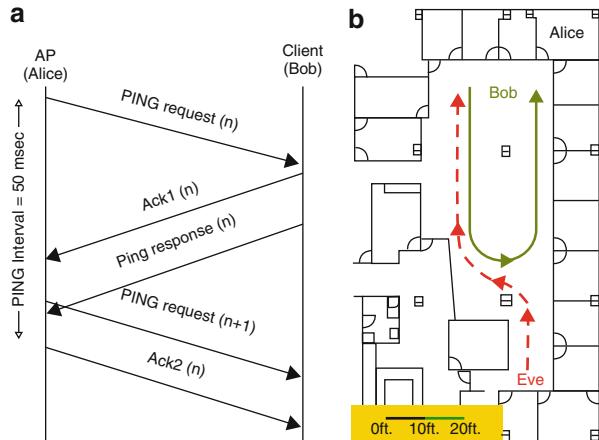
Table 9.3 Summary of experimental results. $I(u_1; u_2)$ denotes the mutual information (M.I.) between the measurements of users u_1 and u_2

CIR-based method	
Value of m used	4
Choice of q_+, q_-	mean $\pm 0.125\sigma$
Duration of experiments	1326 s (~ 22 min.)
Inter-probe duration	110 ms
Static case	
Average secret-bit rate	1.28 s-bits/s
$I(\text{Alice}; \text{Bob})$	3.294 bits
$I(\text{Bob}; \text{Eve})$	0.0468 bits
Mobile case	
Average secret-bit rate	1.17 s-bits/s
$I(\text{Alice}; \text{Bob})$	1.218 bits
$I(\text{Bob}; \text{Eve})$	0.000 bits
RSSI-based method	
Value of m used	4
Choice of q_+, q_-	mean $\pm 0.5\sigma$
Average secret-bit rate	1.3 s-bits/s
Inter-probe duration	50 ms
Duration of experiment	400 s
$I(\text{Alice}; \text{Bob})$	0.78 bits
$I(\text{Alice}; \text{Eve})$	0.00 bits
$I(\text{Bob}; \text{Eve})$	0.07 bits

and Bob. In our experiment, Alice was stationary, while Bob and Eve moved along fixed trajectories. Atheros [17] WiFi cards based on the 5212 chipset were used at each end along with the Madwifi driver [18] for Linux. The experiments were done in the 5.26 GHz channel. The AP-station configuration ensured that MAC-layer clocks at the two nodes were synchronized. Fig. 9.12 b shows the layout of the office building along with the location of the fixed AP and path followed by the mobile client. ICMP PING packets were sent from the AP to the client at a rate of 20 packets per second. Each PING request packet received at the client generates a MAC-layer acknowledgment packet sent back to the AP, followed by a PING response packet. Upon receiving the PING response packet, the AP similarly replies with a MAC-layer ACK packet.

Fig. 9.12 a shows the sequence in which these packets are sent. A `tcpdump` [19] application running on both the AP and the client recorded and time-stamped all packets received on the monitor interface of each user. The experiment consisted of sending 8,000 packets from Alice to Bob. The `tcpdump` traces at each end were filtered using the MAC address to keep only the four types of packets described above. Further, RSSI and MAC-timestamps were pulled out of each packet to generate a *(timestamp, RSSI)* trace.

Fig. 9.12 **a** Timing diagram for collecting RSSI information using PING packets in the RSSI-method. **b** Experimental Layout for RSSI-based method showing trajectories of Bob and Eve, while Alice (the AP) was kept stationary



9.5.2.2 Modification to Handle Timestamps

We note that since the precise time instants at which the PING response and PING request messages are received by Alice and Bob respectively cannot be controlled, there was no way to guarantee that successive PING request messages received by Bob were separated in time by exactly one PING response received in between by Alice. Therefore, MAC-layer timestamps were essential to time-align RSSI information at Alice & Bob since we did not have index numbers with which to reference RSSI values. This required a slight variation in our algorithm to handle MAC-timestamps instead of indexes in the messages exchanged between Alice and Bob. Instead of sending index numbers to Bob, Alice now sends MAC-timestamps in the message L (see Algorithm 1 in Sect. 9.3). For each MAC-timestamp sent by Alice, Bob finds the MAC-timestamp in his own trace that is closest in time to the value of the timestamp sent by Alice. Bob uses the packet determined in Step 2 above as if it were the index sent by Alice. He checks for the presence of excursions above q_+ or below q_- centered at this packet as in Algorithm 1.

The RSSI field in the Prism header of received 802.11 packets reports RSSI as integers, thereby providing only coarse channel information. Moreover, the 802.11 cards at Alice and Bob may not be relatively calibrated and thus may report different values of RSSI. We found in our experiments that although lacking calibration, the temporal *variations* in RSSI are matched in Alice's and Bob's traces. This problem was solved by subtracting out a moving average of the trace to remove the effects of slowly varying average signal power, as in the CIR method. Figure 9.13 shows the raw RSSI traces collected by Alice and Bob plotted against their received MAC-timestamps. As in the CIR-method, the traces exhibit strong variations in average signal power. We average out the large-scale variations and keep only the small scale fading effect. The result is shown in Fig. 9.14. Our algorithm produces secret bits at a rate of almost 1.3 s-bits/sec using $m = 4$, where q_+ and q_- were computed independently by each user as in Eq. (9.13, 9.14) with $\alpha = \frac{1}{2}$.

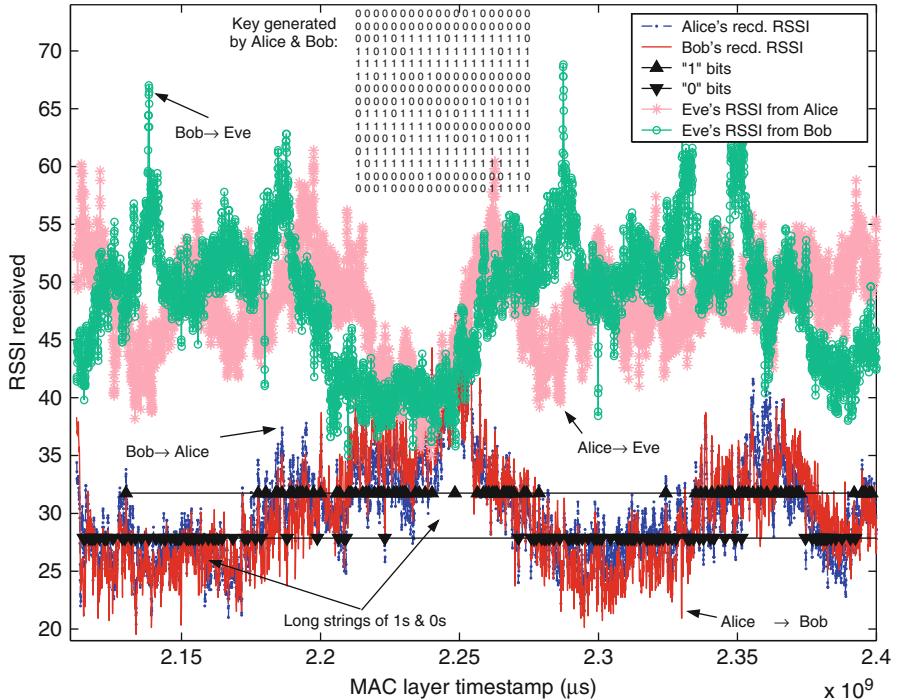


Fig. 9.13 RSSI traces of Alice and Bob and bits generated. This plot includes the effect of shadow fading

9.5.2.3 Contrasting Eve's Attempts

We plot the RSSI traces captured by Eve for both Alice’s and Bob’s signal in Fig. 9.13. The traces from Alice and Bob after considering only variations about a moving average, are shown in Fig. 9.14. Even with coarse RSSI measurements that represent the average received signal power per-packet over the entire 802.11 channel bandwidth, Alice and Bob can exploit reciprocity of their channel to successfully generate secret bits at a fairly good rate. We compute the pair-wise M.I. between the traces of Eve, Alice and Bob in Table 9.3. As in the CIR-method, we find that Eve gets almost no information about the Alice-Bob channel.

9.6 Discussion

We now discuss insights related to our scheme, summarizing fundamental tradeoffs, and further discuss potential security threats. We showed in Sect. 9.4 that the rate at which Alice and Bob derive secret bits from a time-varying channel is limited by the rate of variation in the channel. To maximize rate, we must probe the channel rapidly.

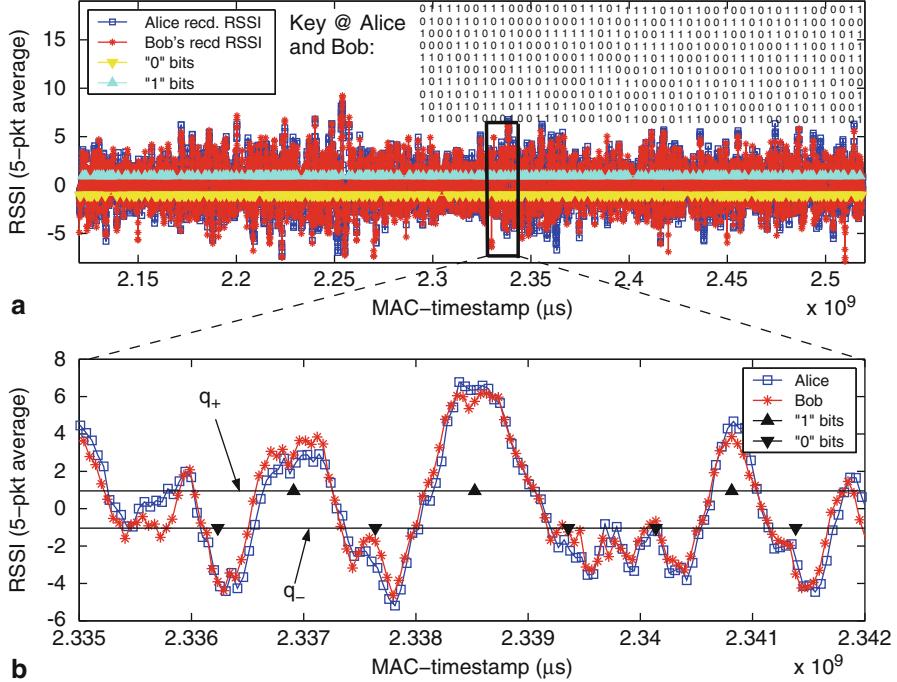


Fig. 9.14 RSSI traces of Alice & Bob after subtracting windowed mean. We get 511 bits in 392 s using $m = 4$ ($R_k = 1.3$ s-bits/s) without any errors

For the fastest probing rate, the parameters m , q_+ and q_- can be tuned to keep the probability of error within an acceptable bound. Increasing m or the magnitudes of q_+ , q_- decreases the error probability at the cost of a decrease in the secret-bit rate. Increasing temporal variation in a channel increases the secret-bit rate up to a point, after which further increase produces a rate decrease, unless accompanied by a proportional increase in the channel probing rate.

The natural decorrelative properties of fading provides our scheme security against eavesdroppers. We confirmed this through our system implementation. Standard randomness tests indicate that our algorithm is resilient to an eavesdropper exploiting randomness defects. However, it is worth noting that key rates significantly greater than the maximum Doppler frequency cannot result in truly random bits. Thus we recommend conservatively setting the probing rates relative to the dynamics of the fading environment. Beyond a passive adversary, we have addressed the threat of an active adversary impersonating Alice or Bob. Coping with spoofing of probes can be dealt with using techniques similar to [9]. We have addressed spoofing of messages following probing by providing a modified algorithm that uses some of the shared secret bits for data-origin authentication. Thus, Eve cannot thwart the key-generation process by impersonating either legitimate user without getting detected.

A further concern common to all key establishment schemes is the man-in-the-middle attack. A man-in-the-middle attack against our algorithm is only possible if Alice and Bob cannot hear each other's probes (e.g., they are not within radio range, or Eve talks to Alice and Bob separately), otherwise Eve's attack causes discrepancies that are easily detectable by Alice and Bob. If Alice and Bob do fall victim to a man-in-the-middle attack, this can be detected by the following identity-based authentication mechanism: Alice asks Bob to send her the keyed hash of the answer to a specific question using their (supposed) shared key as an input to a cryptographic hash function. If Eve relays this question to Bob, then Bob's answer will be useless to Eve (assuming only Alice and Bob know the answer to the question). We note this method requires that Alice and Bob share some secret information known only to them. This is necessary as each user must authenticate the *identity* of the other in order to prevent a man-in-the-middle attack, and is necessary even for classical key establishment schemes like Diffie-Hellman.

Finally, the astute reader might inquire whether varying levels of interference at different locations in the environment would affect our key generation process. We have provided fundamental tradeoffs relating signal-to-interference levels to quantizer parameter selection for an isotropic noise background. However, by conservatively selecting protocol parameters (e.g., selecting a larger value of m (see Fig. 9.4)), we achieve improved robustness in the key generation process at the cost of lowering the rate.

9.7 Related Work

Information-theoretic literature has explored the use of information from the physical layer in deriving security benefits. In [20, 21], the authors introduced the problem of generating identical bits based on correlated information available to two users such that a third eavesdropping user does not learn anything about the generated key. They showed, provided Alice and Bob already share an authenticated public channel, that it is possible to generate identical keys at the two users. The standard method for generating secret keys at Alice and Bob under this assumption consists of three basic steps and has been utilized by a number of proposed systems [22–24]. In *advantage distillation* [20, 25], the legitimate users, Alice and Bob, obtain correlated information while Eve is allowed to eavesdrop, so that Alice & Bob share greater information³ than that shared between Alice & Eve or Bob & Eve. Alice and Bob then convert their information into bits. In the *information reconciliation* stage [23], Alice and Bob exchange error-correcting messages over an authenticated public channel that allow them to agree on an identical string of bits. However, the publicly exchanged messages reveal a certain amount of information about the bit strings to Eve. In *privacy amplification* [26], Alice and Bob diminish

³The amount of information between two observations X and Y is measured by the *mutual information* $I(X; Y)$ [15].

the partial information revealed to Eve by systematically discarding some of their common bits. Efficient protocols have since been designed [23, 27]⁴ to allow key generation without leaking information to an eavesdropping adversary.

A central assumption in this entire body of work is that Alice and Bob have an *authenticated channel available to them* even before key generation begins. This is an unrealistic assumption in practice because the availability of an authenticated channel implies that Alice and Bob already share a secret key to begin with! Therefore, the purpose of generating a common secret key is defeated.

In [29], Maurer and Wolf showed that secret key extraction without an authenticated channel is possible only if Eve cannot possibly transmit a signal to Bob that is statistically indistinguishable from signals coming from Alice (and vice-versa). This provides an important insight that has not been translated into a practical algorithm. Our work is the first to build upon this result: we use the wireless channel to guarantee that Eve does not possess the required information to prevent key generation.

More recently, [30] examined PHY-layer based authentication and confidentiality in wireless systems. The work in [8, 9] looked at authentication using channel signatures between the transmitter and receiver(s). Our work is perhaps most closely related to [31], which proposes a scheme for generating secret bits from correlated observations of deep fades by two users communicating via a TDD link. This work focuses on the theoretical construction for extracting randomness through universal hash families. However, they do not demonstrate or evaluate the amenability of the wireless channel to detection of deep fades by both users, nor the precision needed in the TDD process for their scheme. A quantification of the secret key rate versus parameters associated with the underlying fading process or parameters involved in their algorithm was not provided. Additionally, we note that their method focuses primarily on a passive adversary. The reliance on deep fades may be exploited by an active adversary that produces greater interference power at one legitimate user than the other so that a deep fade for one user may not be a deep fade for the other. In [32], a method exploiting channel reciprocity using ultra-wideband (UWB) channels to generate secret bits was presented. In [33], specialized electronically steerable antennas were proposed for use in generating key bits by exploiting channel reciprocity. The methods in [31–33] all rely on conventional reconciliation for correcting bit-errors, and thus require an authenticated channel. In [34, 35], a method for secret key generation based on phase *reciprocity* of frequency selective fading channels was proposed. While this is attractive, it is difficult to implement as accurate phase information is hard to harvest from existing platforms.

In contrast to prior work, the algorithm we propose transcends the requirement of an authenticated channel, does not require specialized hardware and is not limited to UWB channels. We provide a fundamental analysis between the performance of our scheme and underlying parameters governing fading and quantization. Further, we provide two real-world experimental implementations of our scheme and show that existing mobile platforms already provide sufficient information for producing

⁴Much of this work was done in the context of quantum key distribution [28].

secret bits. We evaluate the randomness of the bit-sequences produced by our algorithm, a generally overlooked aspect in prior work on secret key generation, and show that they are suitable for use as cryptographic keys. Lastly, we note that our technique may be compared with classical key establishment techniques such as Diffie-Hellman, which also use message exchanges to establish keys. However these rely upon unproven arguments of computational hardness of problems such as inverting discrete logarithms or factoring a product of large prime numbers. Our algorithm, on the other hand, provides information-theoretic secrecy, does not assume bounded computation power at the adversary and further, represents practical methods to achieve this type of security. The cost of enabling unconditional security must be borne out in some form—in our case this may take the form of collecting correlated information by probing—but in fact, depending upon how our method is used, much of the required information is already available in present day systems. In this way we provide a means to realize in wireless networks the same benefits that quantum cryptography has enabled using optical fiber links.

9.8 Conclusions

We proposed a protocol that exploits the reciprocity of the transfer function of the wireless multipath channel to establish a common cryptographic key between two communicating entities. Our protocol obtains a security advantage from the fact that the channel response decorrelates rapidly with distance from each communicator, implying that there is strong protection against a passive eavesdropper as well as an active adversary attempting a spoofing attack. The performance of our scheme was evaluated and important insights relating the probing rate, quantizer parameters and the resulting secret key rate were provided.

We also presented the results of a thorough effort to experimentally validate the utility of the wireless channel for secret key generation. First, we constructed a system to extract channel impulse responses on a customized 802.11 development platform, where we used the 802.11a preamble to compute channel impulse responses on a per-packet basis. Second, we used off-the-shelf 802.11a cards for collecting coarse RSSI measurements. In both cases, our algorithm generated secret bits at a useful rate without any errors. We showed that an eavesdropper shares minuscule mutual information with legitimate communicators, thereby supporting security against eavesdroppers. Our work demonstrates that the multipath information that is inherent in any wireless system (and is normally discarded after physical layer processing), can successfully support key establishment. More importantly, we showed that although this capability is possible with custom architectures, it can be achieved using off-the-shelf radio platforms, and thus could have immediate impact on the security of commodity wireless systems. Looking beyond our fundamental observations and feasibility studies, we note that our algorithm naturally applies to emerging wireless systems that use MIMO or OFDM to enhance data rates since the associated multiple uncorrelated channels between two users would lead to a proportional increase in the secret-bit extraction rate.

Acknowledgement The authors would like to express their gratitude to Yogendra Shah for valuable discussions, and to NSF and DARPA (CNS-0626439 and W31P4Q-07-1-0002) for supporting this research.

References

- [1] M. Rudolf and R. P. Mukherjee, *Method and system for deriving an encryption key using joint randomness not shared by others*. US Patent Application Publication US2007/0058808A1, 2007.
- [2] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Upper-Saddle River, Prentice Hall PTR., 2001.
- [3] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.
- [4] J. K. Tugnait, L. Tong, and Z. Ding, “Single-user channel estimation and equalization,” *IEEE Signal Processing Magazine*, vol. 17, pp. 16–28, 2000.
- [5] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley, 1974.
- [6] T. Moore, “IEEE 802.11-01/610r02: 802.1x and 802.11 key interactions,” *Microsoft Research*, 2001.
- [7] S. Fortune, D. M. Gay, B. Kernighan, O. Landron, R. A. Valenzuela, and M. Wright, “Wise design of indoor wireless systems: Practical computation and optimization,” *Computational Science and Engineering, IEEE*, vol. 2, no. 1, pp. 58–68, Apr. 1995.
- [8] N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in *MobiCom '07: Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pp. 111–122, 2007.
- [9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Fingerprints in the ether: Using the physical layer for wireless authentication,” in *Proceedings of the IEEE International Conference on Communications*, pp. 4646–4651, 2007.
- [10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
- [11] U. M. Maurer, “A universal statistical test for random bit generators,” *Journal of Cryptology*, vol. 5, pp. 89–105, 1992.
- [12] “<http://csrc.nist.gov/groups/st/toolkit/rng/>.”
- [13] NIST, “A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications,” 2001.
- [14] “IEEE standard 802.11a: Part 11 wireless LAN medium access control (MAC) and physical layer (PHY) specifications: High-speed physical layer in the 5 GHz band.”
- [15] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley, 1991.
- [16] Q. Wang, S. R. Kulkarni, and S. Verdú, “A nearest-neighbor approach to estimating divergence between continuous random vectors,” in *International Symposium on Information Theory*, pp. 242–246, 2006.
- [17] “<http://www.atheros.com/>.”
- [18] “<http://www.madwifi.org/>.”
- [19] “<http://www.tcpdump.org/>.”
- [20] U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 733–742, 1993.
- [21] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography – Part I: Secret sharing,” *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [22] J. Cardinal and G. V. Assche, “Construction of a shared secret key using continuous variables,” *Information Theory Workshop*, 2003.

- [23] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," *Advances in Cryptology Eurocrypt '93, Lecture Notes in Computer Science*, vol. 765, pp. 410–423, 1994.
- [24] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proceedings of IEEE International Symposium on Information Theory*, Jul. 2006, pp. 2593–2597.
- [25] C. Cachin and U. M. Maurer, "Linking information reconciliation and privacy amplification," *Journal of Cryptology: The Journal of the International Association for Cryptologic Research*, vol. 10, no. 2, pp. 97–110, Spring 1997.
- [26] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988.
- [27] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Physical Review A*, vol. 67, pp. 052303.1–052303.8, 2003.
- [28] G. V. Assche, *Quantum Cryptography and Secret Key Distillation*. New York: Cambridge University Press, 2006.
- [29] U. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel – Part II: The simulatability condition," *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
- [30] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *WiSe '06: Proceedings of the 5th ACM workshop on Wireless security*, pp. 33–42, 2006.
- [31] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pp. 401–410, 2007.
- [32] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.
- [33] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.
- [34] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, pp. 207–212, 1996.
- [35] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Communication Letters*, vol. 4, no. 2, Feb. 2000.

Chapter 10

Secret Key Generation Among Multiple Terminals with Applications to Wireless Systems*

Chunxuan Ye and Alex Reznik

10.1 Introduction

The security of most existing cryptosystems relies on the (unproven) difficulty in solving a computational problem, e.g., factoring large integers or computing discrete logarithms in certain groups (cf. e.g., [1]). This notion of security is called *computational complexity security*, as it is based on the assumption that an adversary has restricted computational power and lacks “efficient algorithms.” However, this assumption is being weakened with the development of efficient algorithms as well as the increase in computational power of modern computers (e.g., quantum computer).

The basic notion of *unconditional* or *information-theoretic* security was formulated by Shannon [2]. In Shannon’s secrecy model, a ciphertext message C , as a function of a plaintext message M and a secret key K , is observed by a legitimate receiver and an adversary. To ensure that the adversary, without the secret key K , gathers no information about the plaintext message M , the mutual information between C and M is required to be zero. Shannon proved that under such perfect secrecy condition, the entropy of the secret key K has to be no less than that of the plaintext message M .

C. Ye (✉)
InterDigital
781 Third Avenue King of Prussia
PA 19406, USA
e-mail: Chunxuan.Ye@InterDigital.com

*Portions of the material have appeared previously in “Secret key generation for a pairwise independent network model,” Proceedings of the IEEE International Symposium on Information Theory, 2008 ©IEEE 2008; “Extracting secrecy from jointly Gaussian random variables,” Proceedings of the IEEE International Symposium on Information Theory, 2007 ©IEEE 2007; “The private key capacity region for three terminals,” Proceedings of the IEEE International Symposium on Information Theory, 2004 ©IEEE 2004; and “The secret key-private key capacity region for three terminals,” Proceedings of the IEEE International Symposium on Information Theory, 2005 ©IEEE 2005.

Note that this pessimistic conclusion is obtained when the adversary observes precisely the same message as the legitimate receiver and the mutual information between M and C is strictly equal to zero. Information-theoretic security is easier to achieve with the relief of these stringent conditions or when additional “resources” are assumed to be present for information-theoretic cryptography. In the context of wireless communication the time-varying wireless fading environment serves to provide both a justification for the relief of the stringent assumption of Shannon’s model and as a source of additional cryptographic resources. Depending on which of the two views are taken,¹ two different cryptographic techniques result. Before we explore these techniques in a network context, we provide a brief overview of each.

If we wish to use the wireless fading channel to relax the stringent assumptions of Shannon’s model, the *wiretap channel* model, first proposed by Wyner [3], is the appropriate starting point. In this model, a legitimate transmitter sends information to a legitimate receiver over a discrete memoryless channel, which is called the main channel. A wiretapper can observe the legitimate receiver’s signal through an independent discrete memoryless channel, which is called the wiretap channel. The overall wiretap channel, from the legitimate transmitter to the wiretapper, is a cascade of the main channel and the wiretap channel. The amount of secrecy is defined as the conditional entropy of decoded message at the legitimate receiver given the received signal at the wiretapper. The maximum secrecy rate is called the secrecy capacity. It is shown [3] that if both the main channel and the wiretap channel are binary symmetric channels, the secrecy capacity is given as the capacity of the main channel minus the capacity of the overall wiretap channel. The same result holds if both the main channel and the wiretap channel are additive white Gaussian noise (AWGN) channels [4].

Wyner’s wiretap channel model was generalized by Csiszár and Körner [5] who considered a discrete memoryless broadcast channel. In such setting, the overall wiretap channel does not need to be a degraded version of the main channel. It is shown [5] that the secrecy capacity is positive whenever the main channel is *less noisy* than the overall wiretap channel.

Various extensions of the wiretap channel model have been investigated recently. For example, the multiple access wiretap channels were studied in [6–8]; the wiretap channel with side information was examined in [9, 10]; the wiretap channel with noisy feedback was analyzed in [11]; the wiretap channel in a semi-deterministic setting was considered in [12], etc.

The wiretap channel model is of significant interest in wireless communication systems once fading is considered. The recent work by Barros and Rodrigues [13] sparked interest in this topic and a large amount of research has been done. For instance, the secrecy capacity of wireless channels, in terms of outage probability, was analyzed in [14]. An interesting result of [14] is that the secure communication over wireless channels is possible even when the overall wiretap channel has a better average signal to noise ratio (SNR) than the main channel. Reference [15] considered

¹ . . . and we note that the two views are not exclusive of each other

the secrecy capacity of slow fading for two cases: (i) the channel state information (CSI) of both the main channel and the wiretap channel is available at the transmitter, and (ii) only the CSI of the main channel is available at the transmitter. Parallel results on fast fading were provided by [16]. In [17] the authors investigated the fading broadcast channel with confidential messages, for the case that the CSI is known at the transmitter and both receivers. Secure communication over wiretap channel, under various multiple antennas conditions, was examined in [18–21]. The wiretap channel with a helper terminal was explored in [23–25].

In addition to the characterizations of the secrecy capacities under various assumptions, some practical coding schemes for the secure communication in wiretap channel model are also developed. Thangaraj et al. [26] showed that capacity-achieving codes can be used to achieve the secrecy capacity for any wiretap channel. The applications of LDPC codes for the secret key generation over the Gaussian and quasi-static fading wiretap channel were examined in [27]. Nested codes have been developed in [28] for the secure communication through the wiretap channel where the main channel is noiseless and the wiretap channel is a general binary input symmetric output memoryless channel.

In summary, the secure communication in wiretap channel model is based on the assumption that the overall wiretap channel is not less noisy than the main channel, since otherwise, the secrecy capacity is equal to zero [5]. However, this presents significant issues for the applicability of the model. More problematically from a security context it is often not possible to establish whether the potential adversaries satisfy any given assumption. In the case of a wireless fading channel, the results outlined above depend on the frequency with which the main fading channel is better than that the overall wiretap channel. Such knowledge typically requires the wiretapper to provide (*honestly*) some information about the channel it observes from the transmitter—an assumption that is often unreasonable. In fact, it is only in the context of *networks* of terminals that the wiretap channel appears to produce models of practical relevance in the sense that reasonable security services may be delivered under meaningful assumptions. Some initial research results in this direction were given in [5, 17, 29] and we shall expound further on this concept in Sect. 5.

An alternative approach to trying to exploit the wireless channel to push through secret data when conditions are favourable is to use it as a resource to generate secrecy directly. This approach leads to the *source type* and *channel type* models for secrecy generation.

The problem of secret key generation in source type models was first studied by Maurer [30], and Ahlswede and Csiszár [31]. In a basic source type model for secrecy generation, two legitimate terminals² observe a common random source which is inaccessible to an eavesdropper. Their observations are dependent but not identical due to the observation noise. Based on their dependent observations, these two terminals generate a common secret key after the mutual communication over a public error-free channel. The eavesdropper may observe the transmissions on the public

²Unless otherwise specified, all the terminals hereafter refer to legitimate terminals, and hence the term “legitimate” is omitted.

channel, but is unable to tamper with the transmissions. The secret key generated by these two terminals should be concealed from the eavesdropper. Specifically, the mutual information between the secret key and the public transmissions is required (asymptotically) close to zero. The largest entropy rate of the achieved secret key is called the secret key capacity. With the classic one-time pad in mind, the secret key capacity in source type models can be translated to the secrecy capacity in wiretap channel models.

Comparing with the wiretap channel model, the source type model does not require that the main channel is less noisy than the overall wiretap channel. On the other hand, the basic source type model relies on the existence of a public error-free channel and a common random source which is accessible to the two terminals but not the eavesdropper. The public error-free channel is attainable since a noisy channel can be regarded as an error-free channel with the help of error-correction codes. The main restriction of the source type model is the lack of the common random source, which must be pre-existent, i.e., provided as a “natural resource.”

One source of such a natural secret resource that has already been exploited for practical security systems is quantum cryptography [32]. Less realized is the fact that the wireless fading channel is another such resource [33, 34]. Suppose that a pair of wireless terminals communicate with each other on the same frequency in a wireless communication environment. The wireless channel between two terminals produces a random mapping between the transmitted and received signals. This mapping, known as *channel impulse response* (CIR), changes with time in a manner that is location-specific and reciprocal, i.e., the mapping is essentially the same in both directions. Hence, if both terminals possess some means of observing the fading of their mutual channel at approximately the same time, their resulting observations are highly statistically dependent. Additionally, this time-varying mapping decorrelates completely over distances of the order of a few wavelengths. Thus, the observations of the shared channel made by two terminals are well modeled as being independent from the observations that an eavesdropper may attempt to make.

We note here that the assumption required for secrecy by the source model is much more appropriate for a wireless context than the assumption of the wiretap model. All we’ve required is that the adversary not be located within a few wavelength of any legitimate terminal. For modern wireless communications, with wavelength on the order of centimeters, such an assumption is readily satisfied in most cases—and can be assumed to be satisfied in practical systems.

In a generalization of the source type model, the common random source observed by two terminals is also accessible to the eavesdropper. Maurer et al. proposed a three-phase secret key generation protocol for this general source type model. The first phase, named *advantage distillation* in [35], was introduced in [30]. This phase is aimed to provide two terminals advantage over the eavesdropper by exploiting the public communication channel between them. Since the public communication in the advantage distillation phase exposes some correlated information between two terminals, which will subsequently reduce the resulting secret key rate, this phase is only needed if neither of the terminals has an advantage compared to the eavesdropper. Note that in the basic source type model mentioned above, this phase

is omitted as the eavesdropper does not have any correlated observations and the advantage between the two terminals over the eavesdropper already exists.

The second phase, named *information reconciliation* in [32, 36, 37], is aimed to generate an identical random sequence between the two terminals by exploiting the public channel. For a better secret key rate, the entropy of this random sequence should be maximized, while the amount of information transmitted on the public channel should be minimized. Obviously, this phase involves the error-correction techniques. The innate connections between the information reconciliation phase and Slepian-Wolf data compression were highlighted in [38]. With the clarification [39] of the duality between Slepian-Wolf data compression and channel coding, the capacity-achieving channel codes, like Turbo codes or LDPC codes, can be used to achieve the Slepian-Wolf data compression bound. Some practical Slepian-Wolf codes have been developed in [40–43] etc. The capacity-achieving channel codes, and consequently the bound-achieving Slepian-Wolf codes, will benefit the information reconciliation phase.

The last phase, named *privacy amplification* in [44, 45], is aimed to extract a secret key from the identical random sequence agreed by two terminals in the information reconciliation phase. Note that the eavesdropper has partial information about the random sequence shared by both terminals, through its observations of the public channel and its observations of the random source. The requirement of the secret key being nearly statistically independent of the eavesdropper's information necessitates the privacy amplification phase. The privacy amplification phase can be implemented by linear mapping and universal hashing [45–48] or by an extractor [48–52] etc. The combination of the information reconciliation phase and the privacy amplification phase has been considered in [31, 35, 53, 54], etc.

One assumption of the source type models mentioned above is the passive eavesdropper, i.e., the eavesdropper does not communicate on the public channel or equivalently, the public channel is authenticated. Maurer and Wolf [48, 55–57] studied the secret key capacity of the source type model with an active attacker. It is shown [56] that if the random variables observed at the two terminals and the active attacker do not satisfy certain *simulability* conditions, then either the secret key capacity of the active attacker model is the same as that for the passive eavesdropper model, or the two terminals could detect the existence of the attacker. Otherwise, no secret key can be generated in the active attacker model. The criterion of checking the simulability condition was analyzed in [57]. An implementation of the privacy amplification phase for the active attacker model was proposed in [48].

Much work has been devoted to various extensions of the source type model. For example, the source type model with the presence of a helper terminal was studied in [31, 58]; the source type model with the rate constraints on the public channel was investigated in [58], etc.

A natural extension of the source type model is the secret key generation among more than two terminals, each of which has distinct observations of the common random source. This multiterminal secret key generation problem was first studied in [58] for the case of three terminals, and then generalized in [38, 59] for an arbitrary number of terminals. In a multiterminal source type model, a subset of the

terminals can serve as “helpers” for the remaining terminals in generating secrecy. Three varieties of secret keys were considered in [38] according to the extent of an eavesdropper’s knowledge: *secret key*, *private key*, and *wiretap secret key*. A secret key generated by a set of terminals with assistance—in the form of additional correlated information—from a set of helper terminals, requires concealment from an eavesdropper with access to the public interterminal communication. A private key generated by the terminals must be additionally protected from the assisting helper terminals. A wiretap secret key must satisfy the even more stringent requirement of being protected from an eavesdropper’s observations of the common random source. The single-letter characterizations of the secret key capacity and the private key capacity, as well as an upper bound for the wiretap secret key capacity, were provided in [38]. A detailed description of these results is in Sect. 2. Furthermore, the applications of the multiterminal source type model to wireless networks have been studied in [60, 61] with details in Sect. 3.

In a typical source type model, the joint distribution of the random variables observed by terminals and the eavesdropper is fixed. In a more general case, called *channel type model* in [31, 62], one of the terminals may control the joint distribution of these random variables in the following way. One of the terminals can govern the inputs of a secure broadcast channel, while all other terminals have distinct but correlated observations of the outputs of the secure broadcast channel. Based on the inputs, as well as the correlated observations of the outputs, of the secure broadcast channel, these terminals generate a secret key after communication over a public error-free channel. An eavesdropper can observe the transmissions on the public channel, and may or may not observe the outputs of the secure broadcast channel. Note that the observations of a common random source in a typical source type model are replaced by the inputs and observed outputs of a secure broadcast channel in a channel type model, where the inputs of the secure broadcast channel are under the control of one terminal.

It should be mentioned that the channel type model is equivalent to a wiretap channel model with the existence of an additional public error-free channel. It is known [30] that the secrecy capacity for a wiretap channel model can be increased by the public discussions between terminals. Thereby, unlike a typical wiretap channel model, a positive secrecy rate can be achieved in the channel type model even if the eavesdropper has less noisy observations of the secure broadcast channel than terminals. The secret key capacities for multiterminal channel type models were discussed in [62, 63]. A detailed description of the results in [62] is contained in Sect. 2.

In all of the source type models, the terminals are required to derive only a single key, of any variety. However, there are situations, e.g., group communication, that multiple keys should be generated in a multiterminal network. Each key is derived for a specific group of terminals, and is concealed from the terminals not belonging to this group and also from the eavesdropper. This key can be used for secure encrypted communication within the group. Since the overlaps of groups are allowed, some terminals may generate more than one key. The simultaneous generation of multiple keys within a three-terminal network was investigated in

[64, 65]. Specifically, reference [64] studied the simultaneous generation of two private keys and reference [65] studied the simultaneous generation of one secret key and one private key. The details of this work are given in Sect. 4.

Along with the characterizations of the secret key capacities for various source type models, some practical construction schemes for secret key generation have recently been developed. For instance, reference [53] proved that the secret key construction can be conducted by a pair of linear matrices. Reference [54] discussed the secret key and the private key constructions in source type models where the observed random variables at terminals are (virtually) connected by a binary symmetric channel. Simple secret key construction schemes were proposed in [34, 66] for the source type model where the observed random variables at terminals are jointly Gaussian distributed. Such jointly Gaussian distribution assumption is feasible for wireless channels, as a (narrowband) wireless channel usually experiences Rayleigh or Rician fading. The secret key construction schemes for ultrawideband wireless channels have been developed in [67]. A simple but robust scheme on the secret key construction from wireless channels was proposed in [68]. The secret key constructions from wireless channels can also be found in [69, 70].

There are other efforts of using wireless channels for security purpose. For example, reference [71] exploited reciprocity of a wireless channel for secure data transformation; reference [72] discussed a secrecy extraction scheme based on the phase information of received signals; the application of the reciprocity of a wireless channel for terminal authentication purpose was studied in [73], etc.

As we proceed to the discussion of multi-terminal secrecy, we note that the main emphasis of this chapter is on the theoretical models for multi-terminal secrecy. However, in deciding how to focus our attention we have been influenced by the applicability of potential models to wireless communications and we emphasize this connection where appropriate.

10.2 General Results on Secret Key Generation Among Multiple Terminals

In this section we present general results on secret key generation among multiple terminals. The source type model is discussed in Sect. 2.1, the channel type model is discussed in Sect. 2.2.

10.2.1 Secret Key Generation in the Multiterminal Source Model

Suppose $m \geq 2$ terminals respectively observe n independent and identically (i.i.d.) distributed repetitions of the random variables (X_1, \dots, X_m) , denoted by (X_1^n, \dots, X_m^n) with $X_i^n = (X_{i,1}, \dots, X_{i,n})$. A set $\mathcal{A} \subseteq \mathcal{M} = \{1, \dots, m\}$ of terminals wishes to generate a common secret key with the help of the remaining terminals, based on their correlated observations. For the secret key generation purpose, these

m terminals can communicate through an error-free public channel, possibly interactively in many rounds. All the transmissions on the public channel are observed by all the terminals, as well as a potential passive eavesdropper which is unable to corrupt the transmissions. Let \mathbf{F} denote collectively all the transmissions on the public channel.

Given $\varepsilon > 0$ and the random variables U, V , we say that U is ε -recoverable from V if $\Pr\{U \neq f(V)\} \leq \varepsilon$ for some function $f(V)$ of V .

A random variable K , which is a function of (X_1^n, \dots, X_m^n) ³ and with finite range \mathcal{K} , represents an ε -secret key (ε -SK) for a set of terminals $\mathcal{A} \subseteq \mathcal{M}$, achievable with communication \mathbf{F} , if

- K is ε -recoverable from (\mathbf{F}, X_i^n) for each $i \in \mathcal{A}$;
- K satisfies the secrecy condition

$$\frac{1}{n} I(K \wedge \mathbf{F}) \leq \varepsilon; \quad (10.1)$$

- K satisfies the uniformity condition

$$\frac{1}{n} H(K) \geq \frac{1}{n} \log |\mathcal{K}| - \varepsilon. \quad (10.2)$$

The conditions above thus mean that terminals in set \mathcal{A} generate a common secret key K with the terminals in $\mathcal{A}^c = \mathcal{M} \setminus \mathcal{A}$ acting as helpers by providing the terminals in \mathcal{A} with additional correlated information; this secret key is nearly uniformly distributed by Eq. (10.2) and is effectively concealed from an eavesdropper that observes the public communication \mathbf{F} by Eq. (10.1).

An ε -SK K for \mathcal{A} is called an ε -private key (ε -PK) for \mathcal{A} private from a set of terminals $\mathcal{D} \subseteq \mathcal{A}^c$, if it satisfies a more stringent secrecy condition

$$\frac{1}{n} I(K \wedge \mathbf{F}, X_{\mathcal{D}}^n) \leq \varepsilon, \quad (10.3)$$

where $X_{\mathcal{D}}^n = \{X_i^n : i \in \mathcal{D}\}$. The condition Eq. (10.3) indicates that the private key is additionally protected from the set \mathcal{D} of the assisting helper terminals.

Definition 1 [38] A nonnegative number R constitutes an *achievable SK-rate* for \mathcal{A} if for every $\varepsilon_n > 0$ and sufficiently large n , an ε_n -SK $K^{(n)}$ is achievable with suitable communication such that $\frac{1}{n} H(K^{(n)}) \geq R - \varepsilon_n$. The largest achievable SK-rate for \mathcal{A} is the *SK-capacity* for \mathcal{A} , denoted by $C_{SK}(\mathcal{A})$.

An achievable SK-rate for \mathcal{A} will be called *strongly achievable* if ε_n above can be taken to vanish exponentially in n . The largest strongly achievable SK-rate for \mathcal{A} is called *strong SK-capacity* for \mathcal{A} .

A (strongly) *achievable PK-rate* for \mathcal{A} private from $\mathcal{D} \subseteq \mathcal{A}^c$ is defined analogously. The largest (strongly) achievable PK-rate for \mathcal{A} private from \mathcal{D} is called (strong) *PK-capacity* for \mathcal{A} private from \mathcal{D} , denoted by $C_{PK}(\mathcal{A}|\mathcal{D})$.

³This implies that no randomization is allowed at the terminals. This restriction can be removed, as discussed later.

Remark The secrecy conditions Eqs. (10.1, 10.3) may be inadequate for cryptographic purposes, as the mutual information between K and \mathbf{F} (or, $(\mathbf{F}, X_{\mathcal{D}}^n)$) may not tend to 0 as n tends to infinity. It is pointed out [74, 75] that the factor $\frac{1}{n}$ in Eqs. (10.1) and (10.3) could be omitted without any rate penalty. Note that the concept of strong achievability above demands even more.

Theorem 1 [38] *The (strong) SK-capacity $C_{SK}(\mathcal{A})$ is given by*

$$C_{SK}(\mathcal{A}) = H(X_{\mathcal{M}}) - R_{min}(\mathcal{A}), \quad (10.4)$$

where

$$R_{min}(\mathcal{A}) = \min_{(R_1, \dots, R_m) \in \mathcal{R}(\mathcal{A})} \sum_{i=1}^m R_i,$$

with

$$\mathcal{R}(\mathcal{A}) = \left\{ (R_1, \dots, R_m) : \sum_{i \in \mathcal{B}} R_i \geq H(X_{\mathcal{B}}|X_{\mathcal{B}^c}), \mathcal{B} \subset \mathcal{M}, \mathcal{A} \not\subseteq \mathcal{B} \right\},$$

and $X_{\mathcal{B}} = \{X_j : j \in \mathcal{B}\}$.

Theorem 1 gives a single-letter characterization of the SK-capacity. For the case of $\mathcal{M} = \mathcal{A} = \{1, 2\}$, the result in Theorem 1 reduces to the mutual information $I(X_1 \wedge X_2)$, which was first shown in [30, 31]. For the case of $\mathcal{M} = \mathcal{A} = \{1, 2, 3\}$, the SK-capacity can be expressed in a straightforward form

$$C_{SK}(\{1, 2, 3\}) = \min \left[\begin{array}{l} I(X_1 \wedge X_2, X_3), I(X_2 \wedge X_1, X_3), I(X_3 \wedge X_1, X_2), \\ \frac{1}{2}[H(X_1) + H(X_2) + H(X_3) - H(X_1, X_2, X_3)] \end{array} \right]. \quad (10.5)$$

However, the computation of the SK-capacity for the cases of $|\mathcal{M}| \geq 4$ is not trivial, and it involves linear programming as follows.

Let $\mathbf{B}(\mathcal{A}) = \{\mathcal{B} \subset \mathcal{M} : \mathcal{B} \neq \emptyset, \mathcal{A} \not\subseteq \mathcal{B}\}$ be a collection of subsets of \mathcal{M} . Let $\mathbf{B}_i(\mathcal{A})$, $i \in \mathcal{M}$, denote a subset of $\mathbf{B}(\mathcal{A})$ consisting of those $\mathcal{B} \in \mathbf{B}(\mathcal{A})$ that contain i . Let $\Lambda(\mathcal{A})$ be the set of all collections $\lambda = \{\lambda_{\mathcal{B}} : \mathcal{B} \in \mathbf{B}(\mathcal{A})\}$ of weights $0 \leq \lambda_{\mathcal{B}} \leq 1$, satisfying

$$\sum_{\mathcal{B} \in \mathbf{B}_i(\mathcal{A})} \lambda_{\mathcal{B}} = 1, \quad i \in \mathcal{M}.$$

According to the Duality theorem [76], the SK-capacity in Theorem 1 can be written as [62]

$$C_{SK}(\mathcal{A}) = H(X_{\mathcal{M}}) - \max_{\lambda \in \Lambda(\mathcal{A})} \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c}). \quad (10.6)$$

Besides the exact characterization of the SK-capacity, the following upper bound for the SK-capacity [38] provides another viewpoint of the SK-capacity. Let $(\mathcal{P}_1, \dots, \mathcal{P}_k)$ be a k -partition of \mathcal{M} , such that each element \mathcal{P}_l , $1 \leq l \leq k$, intersects with the set \mathcal{A} . Denote by $\mathcal{P}^k(\mathcal{A})$ the set of all such k -partitions. Then an upper bound on the secret key capacity is

$$C_{SK}(\mathcal{A}) \leq \min_{2 \leq k \leq |\mathcal{A}|} \frac{1}{k-1} I_k(\mathcal{A}), \quad (10.7)$$

where

$$\begin{aligned} I_k(\mathcal{A}) &= \min_{(\mathcal{P}_1, \dots, \mathcal{P}_k) \in \mathcal{P}^k(\mathcal{A})} \sum_{l=1}^k H(X_{\mathcal{P}_l}) - H(X_{\mathcal{M}}) \\ &= \min_{(\mathcal{P}_1, \dots, \mathcal{P}_k) \in \mathcal{P}^k(\mathcal{A})} D(P_{X_{\mathcal{M}}} || P_{X_{\mathcal{P}_1}} \cdot \dots \cdot P_{X_{\mathcal{P}_k}}), \end{aligned}$$

with $D(P_{X_{\mathcal{M}}} || P_{X_{\mathcal{P}_1}} \cdot \dots \cdot P_{X_{\mathcal{P}_k}})$ being the Kullback-Leibler divergence between the joint distribution of all the random variables and the product of the distributions associated with a given k -partition. This upper bound is tight for some special cases, while its general tightness is still open.

Theorem 2 [38] *The (strong) PK-capacity $C_{PK}(\mathcal{A}|\mathcal{D})$ is given by*

$$C_{PK}(\mathcal{A}|\mathcal{D}) = H(X_{\mathcal{M}}|X_{\mathcal{D}}) - R_{min}(\mathcal{A}|\mathcal{D}), \quad (10.8)$$

where

$$R_{min}(\mathcal{A}|\mathcal{D}) = \min_{\{R_i : i \in \mathcal{D}^c\} \in \mathcal{R}(\mathcal{A}|\mathcal{D})} \sum_{i \in \mathcal{D}^c} R_i,$$

with

$$\mathcal{R}(\mathcal{A}|\mathcal{D}) = \left\{ \{R_i : i \in \mathcal{D}^c\} : \sum_{i \in \mathcal{B}} R_i \geq H(X_{\mathcal{B}}|X_{\mathcal{B}^c}), \mathcal{B} \subset \mathcal{D}^c, \mathcal{A} \not\subset \mathcal{B} \right\}.$$

For the case of $\mathcal{M} = \{1, 2, 3\}$, $\mathcal{A} = \{1, 2\}$ and $\mathcal{D} = \mathcal{A}^c = \{3\}$, the PK-capacity is given by

$$I(X_1 \wedge X_2|X_3), \quad (10.9)$$

which was first proved in [31].

The computation of the PK-capacity also involves linear programming as follows. Let $\mathbf{B}(\mathcal{A}|\mathcal{D}) = \{\mathcal{B} \subset \mathcal{D}^c : \mathcal{B} \neq \emptyset, \mathcal{A} \not\subset \mathcal{B}\}$ be a collection of subsets of \mathcal{D}^c , and let $\mathbf{B}_i(\mathcal{A}|\mathcal{D})$, $i \in \mathcal{D}^c$ denote a subset of $\mathbf{B}(\mathcal{A}|\mathcal{D})$ consisting of those $\mathcal{B} \in \mathbf{B}(\mathcal{A}|\mathcal{D})$ that contain i . Let $\Lambda(\mathcal{A}|\mathcal{D})$ be the set of all collections of weights $\lambda = \{\lambda_{\mathcal{B}} : \mathcal{B} \in \mathbf{B}(\mathcal{A}|\mathcal{D})\}$ of weights $0 \leq \lambda_{\mathcal{B}} \leq 1$ satisfying

$$\sum_{\mathcal{B} \in \mathbf{B}_i(\mathcal{A}|\mathcal{D})} \lambda_{\mathcal{B}} = 1, \quad i \in \mathcal{D}^c.$$

The PK-capacity can be written as [62]

$$C_{PK}(\mathcal{A}|\mathcal{D}) = H(X_{\mathcal{M}}|X_{\mathcal{D}}) - \max_{\lambda \in \Lambda(\mathcal{A}|\mathcal{D})} \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A}|\mathcal{D})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c}).$$

The result in Theorem 1 affords the following interpretation. The SK-capacity is obtained by subtracting from the maximum rate of shared common randomness achievable by these terminals, viz. $H(X_{\mathcal{M}})$, the smallest sum-rate $R_{min}(\mathcal{A})$ of the data-compressed interterminal communication which enables each of the terminals in \mathcal{A} to acquire this maximal common randomness. A similar interpretation holds for the PK-capacity $C_{PK}(\mathcal{A}|\mathcal{D})$ as well, with the difference that the terminals in \mathcal{D} , which act as helpers but must not be privy to the secrecy generated, can simply “reveal” their observations. Hence, the entropy terms in Eq. (10.4) are now replaced in Eq. (10.8) with additional conditioning on $X_{\mathcal{D}}$. It should be noted that $R_{min}(\mathcal{A})$ and $R_{min}(\mathcal{A}|\mathcal{D})$ are obtained as solutions to multiterminal Slepian-Wolf data compression problems not involving any secrecy constraints. The characterizations of the SK-capacity and the PK-capacity in terms of the decompositions above also mirror the consecutive stages in the random coding arguments used in establishing these results (cf. [54]).

In the above discussions, randomization at the terminals is not permitted. Suppose that each terminal can generate a random variable which is independent of $X_{\mathcal{M}}^n$ and the random variables generated at other terminals. The random variable generated at a terminal can be utilized in its public transmissions as well as its final secret key or private key generation. It is proved [38] that such randomization at the terminals does not increase the secret key capacity or the private key capacity. Furthermore, it is shown [38, 62] that the secret key capacity Eq. (10.4) and the private key capacity Eq. (10.8) can be achieved with noninteractive communication, by means of each terminal sending a single message and the message from terminal $i \in \mathcal{D}$ being simply its correlated observations X_i^n .

The multiterminal source type model above makes an assumption that an eavesdropper does not obtain any correlated information on $X_{\mathcal{M}}^n$, except the interterminal transmissions on the public channel. However, in many practical situations, besides the public transmissions, an eavesdropper may also wiretap some side information of the correlated sources $X_{\mathcal{M}}^n$, probably in the same way as one of the terminals. This is modeled as the passive eavesdropper can observe n i.i.d. repetitions of the random variable Z , denoted by $Z^n = (Z_1, \dots, Z_n)$, where the joint distribution of $(X_{1,i}, \dots, X_{m,i}, Z_i)$ is identical for all $1 \leq i \leq n$. Now, the secret key generated by terminals should satisfy a more stringent secrecy condition

$$\frac{1}{n} I(K \wedge \mathbf{F}, Z^n) \leq \varepsilon. \quad (10.10)$$

An ε -SK K for \mathcal{A} is called an ε -wiretap secret key (ε -WSK) for \mathcal{A} which is private from the wiretapper, if it satisfies Eq. (10.10).

A (strongly) *achievable WSK-rate* for \mathcal{A} private from the wiretapper is defined analogously as in Definition 1 above. The largest (strongly) achievable WSK-rate for \mathcal{A} is called (strong) *WSK-capacity* for \mathcal{A} , denoted by $C_{WSK}(\mathcal{A})$.

Theorem 3 [38] The (strong) WSK-capacity $C_{WSK}(\mathcal{A})$ is upper bounded by

$$C_{WSK}(\mathcal{A}) \leq \inf_{U \rightarrow Z \rightarrow X_{\mathcal{M}}} C_{PK}(\mathcal{A}|U), \quad (10.11)$$

where $C_{PK}(\mathcal{A}|U)$ is the PK-capacity for the set of terminals \mathcal{A} private from the wiretapper, with $\mathcal{M} = \{1, ldots, m\}$ and $X_{\mathcal{M}} = (X_1, \dots, X_m)$ being replaced by $\{1, \dots, m+1\}$ and (X_1, \dots, X_m, U) for some random variable U satisfying the Markov condition $U \rightarrow Z \rightarrow X_{\mathcal{M}}$.

It should be noted that the WSK-capacity is not fully resolved even in the case of two legitimate terminals, and the upper bound Eq. (10.11) is not tight in general (cf. [77]). An improvement of the upper bound Eq. (10.11) for the case of $\mathcal{A} = \mathcal{M} = \{1, 2\}$ is known [77] as the *reduced intrinsic information*. A recent work [59] provided a further improvement of the upper bound for the case of $\mathcal{A} = \mathcal{M}$, though it is in terms of a non-single-letter characterization.

On the other hand, a lower bound for the WSK-capacity for the case of $\mathcal{A} = \mathcal{M} = \{1, 2\}$ is given by [30]

$$I(X_1 \wedge X_2) - \min[I(X_1 \wedge Z), I(X_2 \wedge Z)]. \quad (10.12)$$

This lower bound is tight under the Markov condition $X_1 \rightarrow Z$ or $X_2 \rightarrow Z$. Another lower bound for the case of $\mathcal{A} = \mathcal{M} = \{1, 2\}$ involves auxiliary random variables, given by [31]

$$\max_{\substack{V_1 \rightarrow U_1 \rightarrow X_1 \rightarrow X_2 Z \\ V_2 \rightarrow U_2 \rightarrow X_2 \rightarrow X_1 Z}} \left[\begin{array}{l} I(U_1 \wedge X_2 | V_1) - I(U_1 \wedge Z | V_1), \\ I(U_2 \wedge X_1 | V_2) - I(U_2 \wedge Z | V_2) \end{array} \right]. \quad (10.13)$$

The quantity Eq. (10.13) reduces to (10.12) by letting $V_1 = V_2 = \text{constant}$, $U_1 = X_1$ and $U_2 = X_2$. A recent work [59] further improved the lower bound Eq. (10.13), as well as generalizes its result to the case of $\mathcal{A} = \mathcal{M}$, with an arbitrary number of terminals.

10.2.2 Secret Key Generation in the Multiterminal Channel Model

Consider a network with $m \geq 2$ terminals. Each terminal can generate a random variable, and these random variables are mutually independent. Let U_i denote the random variable generated by terminal i .

There is a discrete memoryless broadcast channel (DMBC) connecting these m terminals, where terminal 1 governs the inputs of the DMBC and other terminals observe the distinct outputs of the DMBC. These terminals could also communicate with each other through an error-free public channel.

Suppose that the DMBC can be used n times, i.e., terminal 1 transmits n symbols $X_1^n = (X_{1,1}, \dots, X_{1,n})$. Let $X_i^n = (X_{i,1}, \dots, X_{i,n})$, $2 \leq i \leq m$, denote the corresponding observations at terminal i . After each use of the DMBC, these terminals

communicate over the public channel, possibly interactively in several rounds. The transmission from terminal i is a function of all this terminal's information, specifically, the local random variable U_i , all the previous transmissions on the public channel, and all the previous observations of the DMBC (if $i \neq 1$). Furthermore, the message $X_{1,j}$, $1 \leq j \leq n$, transmitted on the DMBC is a function of U_1 and all the previous transmissions on the public channel. Let \mathbf{F} denote collectively all the transmissions on the public channel.

The definitions of the (strong) SK-capacity for \mathcal{A} , denoted by $C_{SK}(\mathcal{A})$, and the (strong) PK-capacity for \mathcal{A} private from a set of terminals $\mathcal{D} \subseteq \mathcal{A}^c$, denoted by $C_{PK}(\mathcal{A}|\mathcal{D})$, are similar to those in the multiterminal source type model.

Theorem 4 [62] *The (strong) SK-capacity $C_{SK}(\mathcal{A})$ is given by*

$$\begin{aligned} C_{SK}(\mathcal{A}) &= \max_Q \min_{\lambda \in \Lambda(\mathcal{A})} [H(X_{\mathcal{M}}) - \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c})] \\ &= \min_{\lambda \in \Lambda(\mathcal{A})} \max_Q [H(X_{\mathcal{M}}) - \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c})], \end{aligned} \quad (10.14)$$

and the (strong) PK-capacity $C_{PK}(\mathcal{A}|\mathcal{D})$ is given by

$$\begin{aligned} C_{PK}(\mathcal{A}|\mathcal{D}) &= \max_Q \min_{\lambda \in \Lambda(\mathcal{A}|\mathcal{D})} [H(X_{\mathcal{M}}|X_{\mathcal{D}}) - \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A}|\mathcal{D})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c})] \\ &= \min_{\lambda \in \Lambda(\mathcal{A}|\mathcal{D})} \max_Q [H(X_{\mathcal{M}}|X_{\mathcal{D}}) - \sum_{\mathcal{B} \in \mathbf{B}(\mathcal{A}|\mathcal{D})} \lambda_{\mathcal{B}} H(X_{\mathcal{B}}|X_{\mathcal{B}^c})], \end{aligned} \quad (10.15)$$

where the maxima are over Q of all the probability mass functions on the inputs of the secure broadcast channel.

It is shown [62] that the secret key capacity Eq. (10.14) and the private key capacity Eq. (10.15) can be achieved with all public communications occurring after the completion of all the DMBC use, terminal 1 not communicating over the public channel, and other terminals communicating only once on the public channel without interaction or randomization. Terminal 1's strategies on determining the inputs of the DMBC so as to achieve the secret key capacity and the private key capacity were also discussed in [62].

If in a multiterminal channel type model, the eavesdropper also observes the outputs of the DMBC $Z^n = (Z_1, \dots, Z_n)$, then the resulting secret key generated at a set of terminals \mathcal{A} should satisfy Eq. (10.10). This secret key is called a wiretap secret key, and the wiretap secret key capacity is defined analogously as in the source type model. An upper bound on the WSK-capacity, in a similar form as Eq. (10.11), was given by [62]. An improvement on the upper bound for the case of $\mathcal{A} = \mathcal{M}$ can be found in [63]. Lower bounds for the WSK-capacity for the case of $\mathcal{A} = \mathcal{M} = \{1, 2\}$ can be obtained by adding “ \max_Q ” before the quantities Eqs. (10.12) and (10.13), where the maxima are over Q of all the probability mass functions on the inputs of the secure DMBC. A recent work [63] further improved these lower bounds, as

well as generalized its results to the case of $\mathcal{A} = \mathcal{M}$, with an arbitrary number of terminals.

10.3 Pairwise Independent Model

In this section, we discuss a pairwise independent model which is a special case of the multiterminal source type model described in Sect. 2.1. This model is motivated by wireless communications.

To justify this model, let us consider a wireless network in which terminals communicate on the same frequency. As mentioned before, if a pair of terminals possesses some means of observing the fading of their mutual wireless channel at approximately the same time, their observations are highly statistically dependent due to the channel reciprocity. Such observations decorrelate rapidly with distance. Hence, if a third terminal is located a few wavelengths away from either terminal, then its observations on the channels from the first two terminals to it are almost independent of the observations of the first two terminals. Suppose every pair of terminals in a wireless network can observe their mutual wireless channel. Then the channel-specific observations are pairwisely independent. Based on these pairwise independent observations, a set of terminals could generate a common secret key with the help of the remaining terminals. To generate such a secret key, these terminals are allowed to communicate through broadcasts over a public error-free channel. A formal description of the pairwise independent network is given below.

Consider a network with $m \geq 2$ terminals. Each terminal observes n i.i.d. repetitions of the random variables (X_1, \dots, X_m) . The observation X_i by terminal i has $m - 1$ components $(Y_{i,1}, \dots, Y_{i,i-1}, Y_{i,i+1}, \dots, Y_{i,m})$. Each component $Y_{i,j}$ denotes the observation of the source that is accessible only to terminals i and j . In the wireless network example above, the wireless channel between a pair of terminals serves as such source. Furthermore, it is assumed that

$$I(Y_{i,j}, Y_{j,i} \wedge \{Y_{k,l} : (k, l) \neq (i, j), (j, i)\}) = 0. \quad (10.16)$$

This implies that each source accessible to a pair of terminals is independent of all other sources—hence, the network is called pairwise independent network. Based on the pairwise independent observations, a set \mathcal{A} of these m terminals generate a common secret key after interterminal communication over a public error-free authenticated channel. The secret key should satisfy certain secrecy condition and uniformity condition as in Eqs. (10.1) and (10.2). The SK-capacity for \mathcal{A} is defined in Definition 1.⁴

The following proposition is derived from the SK-capacity Eq. (10.6) for the pairwise independent model.

⁴For better statement, we shall not distinguish between the strong SK-capacity and the SK-capacity hereafter.

Proposition 1 [61] *The SK-capacity $C_{SK}(\mathcal{A})$ for the pairwise independent model is given by*

$$C_{SK}(\mathcal{A}) = \min_{\lambda \in \Lambda(\mathcal{A})} \left[\sum_{1 \leq i < j \leq m} \left(\sum_{\substack{\mathcal{B} \in \mathbf{B}(\mathcal{A}): \\ i \in \mathcal{B}, j \in \mathcal{B}^c}} \lambda_{\mathcal{B}} \right) I(Y_{i,j} \wedge Y_{j,i}) \right]. \quad (10.17)$$

The following proposition is derived from the upper bound of the SK-capacity Eq. (10.7) for the pairwise independent model.

Proposition 2 [60] *The SK-capacity $C_{SK}(\mathcal{A})$ for the pairwise independent model is upper bounded by*

$$C_{SK}(\mathcal{A}) \leq \min_{2 \leq k \leq |\mathcal{A}|} \frac{1}{k-1} I'_k(\mathcal{A}), \quad (10.18)$$

where

$$I'_k(\mathcal{A}) = \min_{(\mathcal{P}_1, \dots, \mathcal{P}_k) \in \mathcal{P}^k(\mathcal{A})} \sum_{\substack{i, j \in \mathcal{P}_l: \\ j \in \mathcal{P}_r; l < r}} I(Y_{i,j} \wedge Y_{j,i}).$$

The results in Eqs. (10.17) and (10.18) imply that the SK-capacity for the pairwise independent model depends on the joint probability distribution of the underlying random variables only through the values of the pairwise reciprocal mutual information terms. This suggests a two-step secret key generation scheme. In the first step, every pair of terminals generates a pairwise secret key (without any helps from other terminals), using their correlated observations. Because of the independence assumption Eq. (10.16), these pairwise secret keys are mutually independent. In the second step, a set \mathcal{A} of terminals generates a common secret key based on the pairwise secret keys generated in the first step. The advantage of this architectural partition of secret key generation process is that no knowledge of the network topology is required in the first step and no knowledge of source statistics is required in the second step.

The problem of the secret key generation between two terminals (without helper terminals) has already been studied extensively [30, 31] etc. Specifically, various construction schemes of the pairwise secret key generation have been proposed [34, 53, 54, 66–70] etc. Of particular relevance to the discussion here is the work in [34, 54, 66] as it proposes capacity-achieving secret key construction schemes. Reference [54] proposed secret key construction schemes between two terminals whose observed random variables are (virtually) connected by a binary symmetric channel. Reference [34] proposed simple secret key construction schemes between two terminals with their observed random variables being jointly Gaussian distributed. Such jointly Gaussian distribution assumption is feasible for wireless channels, as the fading of a (narrowband) wireless channel is usually Rayleigh or Rician distributed. According to [34], terminal i first equiprobably quantizes its Gaussian random variables $Y_{i,j}^n$. The quantization outputs are converted to a bit string Y_b using Gray coding.

The syndrome of the bit string Y_b , in terms of a given LDPC code, is then transmitted through an error-free public channel to Terminal j . Based on the syndrome and its own Gaussian random variables $Y_{j,i}^n$, terminal j then tries to decode Y_b by applying a modified belief-propagation algorithm, in which the log-likelihood ratio is softly encoded. Finally, both terminals hash out the publicly revealed information (i.e., the syndrome) from the common bit string Y_b , leaving purely secret bits $K_{i,j}$. It is reported in [34] that a secret key resulting from this scheme has a rate within 1.2 bits of the capacity $I(Y_{i,j} \wedge Y_{j,i})$. This performance was further improved in [66].

The problem of the secret key generation among a set of terminals, based on their mutually independent pairwise secret bits, is related to graph theory. Thereby, some definitions on graph are given below. A *multi-graph* is an undirected graph which is permitted to have parallel edges, i.e., edges that have the same end nodes. Let $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ be a multi-graph, where \mathcal{N} is the node set and \mathcal{E} is the edge set. For a subset of nodes $\mathcal{N}_1 \subseteq \mathcal{N}$, a *Steiner tree* of \mathcal{G} on \mathcal{N}_1 is a subgraph of \mathcal{G} which is a tree whose node set containing \mathcal{N}_1 . A Steiner tree is called a *spanning tree* if $\mathcal{N}_1 = \mathcal{N}$. A *Steiner packing* of \mathcal{G} on \mathcal{N}_1 is any collection of disjoint Steiner trees of \mathcal{G} on \mathcal{N}_1 . Let $\mu(\mathcal{N}_1, \mathcal{G})$ denote the maximum size of such packings.

Without loss of generality, suppose in the pairwise secret key generation step, every pair of terminals i, j generate $\lfloor nI(Y_{i,j} \wedge Y_{j,i}) \rfloor$ pairwise secret bits using standard techniques [30, 31]. Consider a multi-graph G with m nodes, each corresponding to a terminal in the network. The number of parallel edges connecting nodes i, j is equal to $\lfloor nI(Y_{i,j} \wedge Y_{j,i}) \rfloor$.

By using a pairwise secret bit shared between every two nodes with edges on a Steiner tree of G on \mathcal{A} , the terminals in \mathcal{A} could generate a single common secret bit. This is fulfilled by the secret key propagation schemes in [38] (proof of Theorem 5) and [60]. Hence, the total number of secret bits that can be generated by terminals in \mathcal{A} , with the help of other terminals, is no less than the maximum size of Steiner packings of G on \mathcal{A} . This proves the following proposition.

Proposition 3 [61] *The SK-capacity $C_{SK}(\mathcal{A})$ for the pairwise independent model is lower bounded by*

$$C_{SK}(\mathcal{A}) \geq \sup_n \frac{1}{n} \mu(\mathcal{A}, G).$$

It follows from a theorem of Nash-Williams [78] and Tutte [79] that the upper bound in Proposition 2 and the lower bound in Proposition 3 coincide under the condition of $\mathcal{A} = \mathcal{M}$. This shows the tightness of both bounds for the secret key generation among all the terminals for the pairwise independent model. Furthermore, the polynomial-time algorithm [80] for finding the largest collection of disjoint spanning trees carries out a polynomial-time secret key construction algorithm which achieves the secret key capacity for $\mathcal{A} = \mathcal{M}$ in the pairwise independent model (cf. [61]).

Additionally, the upper bound in Proposition 2 is shown [60] tight for the case of $|\mathcal{A}| = 2$. The proof is based on the max-flow min-cut theorem (cf. e.g., [81]), and

consequently, some well-known polynomial-time algorithms (e.g., Dinitz's algorithm, Karzanov's algorithm, Goldberg's algorithm) for achieving the maximum flow in a directed graph constitutes a polynomial-time secret key construction algorithm which achieves the secret key capacity for $|\mathcal{A}| = 2$ in the pairwise independent model. It is clear that the lower bound in Proposition 3 is also tight for the case of $|\mathcal{A}| = 2$ by regarding every flow path (or flow unit) in the maximum flow as a Steiner tree connecting the two nodes in \mathcal{A} .

We conjecture that both the upper bound in Proposition 2 and the lower bound in Proposition 3 are tight for the pairwise independent model.

10.4 Multiple Keys Generation Among Three Terminals

As discussed before, there are situations, arising for instance in group communication, where multiple keys must be simultaneously devised in a coordinated manner by different groups of terminals. A key devised for a group must be concealed from terminals outside that group as well as from an eavesdropper. Such group-wide keys can be applied for the secure communication within those groups.

In general, in a network with m terminals, we could have one (common) secret key for all the terminals, and private keys for every proper subset of the m terminals. These situations produce a rich vein of secrecy generation problems, the information theoretic underpinnings of which are substantial enough for investigation already in the case of just three terminals.

Suppose three terminals respectively observe n i.i.d. repetitions of the random variables (X_1, X_2, X_3) , which we denote by (X_1^n, X_2^n, X_3^n) with $X_i^n = (X_{i,1}, \dots, X_{i,n})$, $1 \leq i \leq 3$. The terminals can communicate with each other through broadcasts over an error-free public channel, possibly interactively in many rounds. Let \mathbf{F} denote collectively all the transmissions on the public channel.

Let random variables $K_{1,2,3}$, $K_{1,2}$, $K_{1,3}$, and $K_{2,3}$, with respective finite ranges $\mathcal{K}_{1,2,3}$, $\mathcal{K}_{1,2}$, $\mathcal{K}_{1,3}$, and $\mathcal{K}_{2,3}$, be functions of (X_1^n, X_2^n, X_3^n) . These random variables represent an ε -secret key, 3-private keys (ε -SK, 3-PKs) quadruple, where $K_{1,2,3}$ is the secret key for all three terminals and $K_{i,j}$, $1 \leq i < j \leq 3$, is the private key for terminals i and j , with privacy from the third terminal, achievable with communication \mathbf{F} , if:

- $K_{1,2,3}$ is ε -recoverable from each of (\mathbf{F}, X_1^n) , (\mathbf{F}, X_2^n) , (\mathbf{F}, X_3^n) ;
- $K_{1,2,3}$ satisfies the secrecy condition and the uniformity condition

$$\begin{aligned} \frac{1}{n} I(K_{1,2,3} \wedge \mathbf{F}) &\leq \varepsilon; \\ \frac{1}{n} H(K_{1,2,3}) &\geq \frac{1}{n} \log |\mathcal{K}_{1,2,3}| - \varepsilon; \end{aligned}$$

- $K_{i,j}$, $1 \leq i < j \leq 3$, is ε -recoverable from each of (\mathbf{F}, X_i^n) , (\mathbf{F}, X_j^n) ; and

- $K_{i,j}$, $1 \leq i < j \leq 3$, satisfies the secrecy condition and the uniformity condition

$$\begin{aligned} \frac{1}{n} I(K_{i,j} \wedge \mathbf{F}, X_k^n) &\leq \varepsilon; \\ \frac{1}{n} H(K_{i,j}) &\geq \frac{1}{n} \log |\mathcal{K}_{i,j}| - \varepsilon, \end{aligned} \quad (10.19)$$

where the index k in Eq. (10.19) is given by $\{1, 2, 3\} \setminus \{i, j\}$.

The conditions above thus mean that all the terminals generate a nearly uniformly distributed secret key $K_{1,2,3}$ which is concealed from an eavesdropper that observes the public communication \mathbf{F} . Based on the same public communication, every pair of terminals generate a private key with the third terminal acting as helper; this private key is nearly uniformly distributed and is concealed from an eavesdropper as well as from the helper terminal. Note that the above conditions readily imply that all these four keys are “nearly” statistically independent.

Definition 2 A quadruple of nonnegative numbers $(R_{1,2,3}, R_{1,2}, R_{1,3}, R_{2,3})$ constitutes an achievable (SK, 3-PKs)-rate quadruple if for every $\varepsilon > 0$ and sufficiently large n , an ε -(SK, 3-PKs) quadruple $(K_{1,2,3}, K_{1,2}, K_{1,3}, K_{2,3})$ is achievable with suitable communication, such that $\frac{1}{n} H(K_{1,2,3}) \geq R_{1,2,3} - \varepsilon$, $\frac{1}{n} H(K_{i,j}) \geq R_{i,j} - \varepsilon$, $1 \leq i < j \leq 3$. The set of all achievable (SK, 3-PKs)-rate quadruples is the (SK, 3-PKs)-capacity region.

Remarks

1. The (SK, 3-PKs)-capacity region is a closed convex set. Closedness is obvious from the definition, while convexity follows from a time-sharing argument (cf. [82]).
2. If the private keys are set equal to constants in the definition above, i.e., only a single secret key is generated by these terminals, then the entropy rate of such a secret key is an achievable SK-rate, and the largest achievable SK-rate is the SK-capacity. The SK-capacity for the three terminals case is given by Eq. (10.5).
3. If the secret key, as well as two private keys say, $K_{1,3}$ and $K_{2,3}$, are set equal to constants in the definition above, i.e., only a single private key is generated by terminals 1 and 2 with terminal 3 serving as a helper terminal, then the entropy rate of such a private key is an achievable PK-rate, and the largest achievable PK-rate is the PK-capacity. The PK-capacity for the three terminals case is given by Eq. (10.9).

The (SK, 3-PKs)-capacity region defined above remains open, while some results on the capacity region of only two (out of four) keys are known [64, 65]. We discuss the results of [64] in Sect. 4.1 and the results of [65] in Sect. 4.2.

10.4.1 The 2-PKS Capacity Region

Instead of generating one secret key and private keys for all pairs of these three terminals, suppose that only two private keys $K_{1,2}$ and $K_{1,3}$ are generated between terminal pairs (1, 2) and (1, 3).

An ε -PK pair is defined similarly as above, with the other two keys $K_{1,2,3}$ and $K_{2,3}$ being set as constants. The definition of an achievable PK-rate pair follows from Definition 2 with $R_{1,2,3}$ and $R_{2,3}$ being zero. The set of all achievable PK-rate pairs is the PK-capacity region, denoted by \mathcal{C}_{PK} .

Theorem 5 (*Outer bound for \mathcal{C}_{PK}*): Let $(R_{1,2}, R_{1,3})$ be an achievable PK-rate pair. Then

$$R_{1,2} \leq I(X_1 \wedge X_2 | X_3), \quad R_{1,3} \leq I(X_1 \wedge X_3 | X_2), \quad (10.20)$$

$$R_{1,2} + R_{1,3} \leq \min_U I(X_1 \wedge X_2, X_3 | U), \quad (10.21)$$

where the minimum is over all random variables U that satisfy the Markov conditions $U \rightarrowtail X_2 \rightarrowtail X_1 X_3$ and $U \rightarrowtail X_3 \rightarrowtail X_1 X_2$.

Note that the bounds Eq. (10.20) on the individual largest achievable PK-rate follows directly from Eq. (10.9), while the bound Eq. (10.21) implies the sum of these two rates is additionally restricted.

A function of X is a *sufficient statistic* for X with respect to Y if it renders X and Y conditionally independent; such a sufficient statistic is a *minimal sufficient statistic* $U_{mss}(X, Y)$ for X with respect to Y if it is a function of every other sufficient statistic for X with respect to Y .

Theorem 6 (*Inner bound for \mathcal{C}_{PK}*): The PK-capacity region \mathcal{C}_{PK} is inner-bounded by the convex hull of the union of the regions

$$\left\{ (R_{1,2}, R_{1,3}) : \begin{array}{l} R_{1,2} \leq I(X_1 \wedge X_2 | U_{mss}(X_2, X_3), X_3), \quad R_{1,3} \leq I(X_1 \wedge X_3 | X_2), \\ R_{1,2} + R_{1,3} \leq I(X_1 \wedge X_2, X_3 | U_{mss}(X_2, X_3)) \end{array} \right\}$$

and

$$\left\{ (R_{1,2}, R_{1,3}) : \begin{array}{l} R_{1,2} \leq I(X_1 \wedge X_2 | X_3), \quad R_{1,3} \leq I(X_1 \wedge X_3 | U_{mss}(X_3, X_2), X_2), \\ R_{1,2} + R_{1,3} \leq I(X_1 \wedge X_2, X_3 | U_{mss}(X_3, X_2)) \end{array} \right\},$$

where $U_{mss}(X_2, X_3)$ is the minimal sufficient statistic for X_2 with respect to X_3 , and $U_{mss}(X_3, X_2)$ is the minimal sufficient statistic for X_3 with respect to X_2 .

Under some special conditions, the outer bound in Theorem 5 coincides with the inner bound in Theorem 6, thereby giving an exact characterization of the PK-capacity region.

Theorem 7 If there exists a random variable U such that

$$U \rightarrowtail X_2 \rightarrowtail X_1 X_3, \quad U \rightarrowtail X_3 \rightarrowtail X_1 X_2, \quad X_2 \rightarrowtail U \rightarrowtail X_3, \quad (10.22)$$

then the PK-capacity region equals the set of pairs $(R_{1,2}, R_{1,3})$ which satisfy Eq. (10.20) and

$$R_{1,2} + R_{1,3} \leq \min_U I(X_1 \wedge X_2, X_3 | U),$$

where the minimum is over all random variables U satisfying Eq. (10.22).

A *common function* of random variables X and Y is any random variable which equals both a function of X and a function of Y ; a *maximal common function* $U_{mcf(X,Y)}$ of X and Y is such that every other common function of X and Y is a function of $U_{mcf(X,Y)}$ (cf. e.g., [58, 83]). The random variables X and Y are *deterministically correlated* if there exists a common function of X and Y which renders them conditionally independent (cf. [82, p. 405]).

Theorem 8 If the random variables X_2 and X_3 are deterministically correlated, the PK-capacity region \mathcal{C}_{PK} equals the set of pairs $(R_{1,2}, R_{1,3})$ which satisfy Eq. (10.20) and

$$R_{1,2} + R_{1,3} \leq I(X_1 \wedge X_2, X_3 | U_{mcf(X_2, X_3)}),$$

where $U_{mcf(X_2, X_3)}$ is the maximal common function of X_2 and X_3 .

10.4.2 The (SK, PK)-Capacity Region

Instead of generating one secret key and private keys for all pairs of these three terminals, suppose that only a secret key $K_{1,2,3}$ and a private key $K_{1,2}$ are generated among all three terminals and terminal pair (1,2), respectively.

An ε -(SK, PK) pair is defined similarly as above, with the other two keys $K_{1,3}$ and $K_{2,3}$ being set as constants. The definition of an achievable (SK,PK)-rate pair follows from Definition 2 with $R_{1,3}$ and $R_{2,3}$ being zero. The set of all achievable (SK, PK)-rate pairs is the (SK, PK)-capacity region, denoted by \mathcal{C}_{SP} .

For notational simplicity, we set

$$A \triangleq I(X_3 \wedge X_1, X_2),$$

$$B \triangleq \min[I(X_1 \wedge X_2, X_3), I(X_2 \wedge X_1, X_3)],$$

$$C \triangleq \frac{1}{2}[H(X_1) + H(X_2) + H(X_3) - H(X_1, X_2, X_3)],$$

Note that the SK-capacity for the three terminals case is equal to $\min[A, B, C]$, as in Eq. (10.5).

Theorem 9 (Outer bound for \mathcal{C}_{SP}): Let $(R_{1,2,3}, R_{1,2})$ be an achievable (SK, PK)-rate pair. Then

$$R_{1,2,3} \leq A, \tag{10.23}$$

$$R_{1,2} \leq I(X_1 \wedge X_2 | X_3), \tag{10.24}$$

$$R_{1,2,3} + R_{1,2} \leq B, \tag{10.25}$$

$$2R_{1,2,3} + R_{1,2} \leq 2C. \tag{10.26}$$

The bounds Eqs. (10.23) and (10.24) on the individual largest achievable SK-rate and PK-rate are obvious from Eqs. (10.5) and (10.9). The conditions Eqs. (10.25) and (10.26) above are more stringent than the corresponding conditions in Eq. (10.9).

Theorem 10 (*Inner bound for \mathcal{C}_{SP}*): *The (SK, PK)-capacity region \mathcal{C}_{SP} is inner-bounded by the region*

$$\left\{ \begin{array}{l} (R_{1,2,3}, R_{1,2}) : \frac{\min\{A, B, C\} - \min\{I(X_1 \wedge X_3), I(X_2 \wedge X_3)\}}{I(X_1 \wedge X_2 | X_3)} \cdot R_{1,2} \\ + R_{1,2,3} \leq \min\{A, B, C\}, \\ R_{1,2} \leq I(X_1 \wedge X_2 | X_3) \end{array} \right\}.$$

Under a certain condition, the outer bound in Theorem 9 coincides with the inner bound in Theorem 10, which provides a characterization of the (SK, PK)-capacity region \mathcal{C}_{SP} .

Theorem 11 *If $\min\{A, B, C\} = B$, then \mathcal{C}_{SP} is equal to the set of pairs $(R_{1,2,3}, R_{1,2})$ satisfying Eqs. (10.24) and (10.25).*

10.5 The Wiretap Channel Model in Networks

As discussed in the introduction, the wiretap channel model suffers from a significant limitation in that some information about the quality of the overall wiretap channel must either be known or assumed by the legitimate parties. Ideally, one would like to make assumptions that include *almost all* potential adversaries within a particular class. In the case of the wiretap channel, especially as applied to wireless communication, a natural class definition is using the Signal-to-Interference and Noise Ratio (SINR) (e.g., the average/long-term SINR). For example, one might define the class of adversaries as those having SINR of no more than S dB. Unfortunately, unless we let S approach infinity such a definition cannot include *almost all* potential adversaries, especially in the context of wireless communication. And if we do let S approach infinity, the secrecy rate will approach 0 for any fixed SINR of the legitimate receiver(s).

To get around this issue, it is useful to consider applying the wiretap channel model to a network of terminals. In particular, in the context of broadcast networks several approaches present themselves. The first is to consider a broadcast channel in which there are no illegitimate users, however some communication must remain secret from some subset of the users. This is a reasonable model for networks where a user must in some way “register” with the network and maintain such a registration in order to have the basic capability to access any data. Within such an over-arching access model, a second level of confidentiality for the legitimate user’s data is then provided by wiretap channel techniques. The theoretical aspects of such a model

were initially explored by Csiszár and Körner [5]. Recent results by [8, 29] provide further results in this area. These are summarized in Sect. 5.1

An alternative approach is to consider situations where only receivers within particular locations are permitted access to common data. One such model, that of the trust-zone [84] permits a natural connection between the location and the SINR and leads itself nicely to an interpretation of a broadcast network with wiretappers. This model is described in Sect. 5.2.

10.5.1 Broadcast Channel with Confidential Messages

Consider a discrete memoryless broadcast channel with one input and two outputs. This channel is denoted by $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1, \mathcal{Y}_2)$, where \mathcal{X} is the finite channel input alphabet, \mathcal{Y}_1 and \mathcal{Y}_2 are the finite channel output alphabets, and $p(y_1, y_2|x)$ is the channel transition probability distribution. The transmitter wishes to send message $W_1 \in \mathcal{W}_1 = \{1, \dots, M_1\}$ to receiver 1 and simultaneously send message $W_2 \in \mathcal{W}_2 = \{1, \dots, M_2\}$ to both receivers through n uses of the broadcast channel. The two messages W_1 and W_2 are independent, and message W_1 should be concealed from receiver 2. Such a channel model is called the broadcast channel with confidential messages [5].

A stochastic encoder is specified by a matrix of conditional probabilities $f(x^n|w_1, w_2)$, where $x^n \in \mathcal{X}^n$, $w_i \in \mathcal{W}_i$, such that $\sum_{x^n \in \mathcal{X}^n} f(x^n|w_1, w_2) = 1$. A decoding function at receiver 1 is a mapping $\psi_1: \mathcal{Y}_1^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2)$, while a decoding function at receiver 2 is a mapping $\psi_2: \mathcal{Y}_2^n \rightarrow \mathcal{W}_2$. An (M_1, M_2, n) code for the broadcast channel consists of one encoding function f and two decoding functions ψ_1, ψ_2 .

The average error probability at receiver 1 is defined as

$$P_{e,1}^{(n)} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} \Pr[\psi_1(Y_1^n) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}],$$

and the average error probability at receiver 2 is defined as

$$P_{e,2}^{(n)} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} \Pr[\psi_2(Y_2^n) \neq w_2 | (w_1, w_2) \text{ sent}].$$

Definition 3 A pair of nonnegative numbers (R_1, R_2) constitutes an achievable rate pair for the broadcast channel with confidential messages, if for every $\varepsilon > 0$ and sufficiently large n , there exists an (M_1, M_2, n) code such that (i) $M_i \geq 2^{nR_i}$, $i = 1, 2$, (ii) $\max[P_{e,1}, P_{e,2}] \leq \varepsilon$ and (iii) $\frac{1}{n} H(W_1|Y_2^n) \geq R_1 - \varepsilon$. The set of all achievable rate pairs is the secrecy capacity region, denoted by \mathcal{C}_{BC} .

Theorem 12 [5] *The secrecy capacity region \mathcal{C}_{BC} equals the set of all pairs (R_1, R_2) satisfying*

$$R_1 \leq I(V \wedge Y_1|U) - I(V \wedge Y_2|U),$$

and

$$R_2 \leq \min\{I(U \wedge Y_1), I(U \wedge Y_2)\},$$

where the random variables U, V satisfy the Markov condition $U \rightarrowtail V \rightarrowtail X \rightarrowtail Y_1 Y_2$.

As discussed, the broadcast channel model is of significant interest in wireless communication systems once fading is considered. To this end, suppose the channels from the transmitter to both receivers are corrupted by multiplicative fading gain processes as well as additive white Gaussian noises, i.e., $Y_{i,j} = h_{i,j}X_j + Z_{i,j}$, $i = 1, 2$, $j = 1, \dots, n$. The channel fading coefficients $h_{1,j}, h_{2,j}$ are complex random variables, and $\{h_{1,j}, h_{2,j}\}$ is a stationary and ergodic vector random fading process. The additive noises $Z_{1,j}, Z_{2,j}$ are zero mean complex Gaussian random variables with respective variances μ_1^2, μ_2^2 , and $\{Z_{1,j}\}, \{Z_{2,j}\}$ are i.i.d. random noise processes. The channel input sequence $\{X_i\}$ is subject to the average power constraint P , i.e., $\frac{1}{n} \sum_{i=1}^n E[X_i^2] \leq P$.

Assume the channel state information $\mathbf{h}_j = (h_{1,j}, h_{2,j})$ is known at both the transmitter and the receivers instantaneously. Based on the channel state information, the transmitter dynamically adjust its transmission power for better performance. Note that for a given channel fading state, the fading channel is a Gaussian channel, and the secrecy capacity region for the fading broadcast channel above is averaged over all channel states.

Theorem 13 [17] *The secrecy capacity region \mathcal{C}_{BC} for the fading broadcast channel equals the set of all pairs (R_1, R_2) satisfying*

$$R_1 \leq E_{\mathbf{h} \in \mathcal{H}_1} \left[\log \left(1 + \frac{p_1(\mathbf{h})|h_1|^2}{\mu_1^2} \right) - \log \left(1 + \frac{p_1(\mathbf{h})|h_2|^2}{\mu_2^2} \right) \right],$$

and

$$R_2 \leq \min \begin{cases} E_{\mathbf{h} \in \mathcal{H}_1} \log \left(1 + \frac{p_2(\mathbf{h})|h_1|^2}{\mu_1^2 + p_1(\mathbf{h})|h_1|^2} \right) + E_{\mathbf{h} \in \mathcal{H}_2} \log \left(1 + \frac{p_2(\mathbf{h})|h_1|^2}{\mu_1^2} \right), \\ E_{\mathbf{h} \in \mathcal{H}_1} \log \left(1 + \frac{p_2(\mathbf{h})|h_2|^2}{\mu_2^2 + p_1(\mathbf{h})|h_2|^2} \right) + E_{\mathbf{h} \in \mathcal{H}_2} \log \left(1 + \frac{p_2(\mathbf{h})|h_2|^2}{\mu_2^2} \right) \end{cases},$$

where $\mathcal{H}_1 = \left\{ \mathbf{h} : \frac{|h_1|^2}{\mu_1^2} > \frac{|h_2|^2}{\mu_2^2} \right\}$, $\mathcal{H}_2 = \left\{ \mathbf{h} : \frac{|h_1|^2}{\mu_1^2} \leq \frac{|h_2|^2}{\mu_2^2} \right\}$, $\mathbf{h} = (h_1, h_2)$ has the same distribution as the marginal distribution of the process $\{h_{1,j}, h_{2,j}\}$ at one time instant, and the powers $p_1(\mathbf{h}), p_2(\mathbf{h})$ used for transmitting messages W_1, W_2 satisfy $E_{\mathcal{H}_1}[p_1(\mathbf{h}) + p_2(\mathbf{h})] + E_{\mathcal{H}_2}[p_2(\mathbf{h})] \leq P$.

It should be mentioned that in the fading broadcast channel model, the fading process $\{h_{1,j}, h_{2,j}\}$ is not restricted to Gaussian distribution, and the two component processes $\{h_{1,j}\}$ and $\{h_{2,j}\}$ do not need to be independent. Furthermore, the noise processes $\{Z_{1,j}\}$ and $\{Z_{2,j}\}$ also do not need to be independent. The results in

Theorem 13 hold under these general conditions. The power allocation to achieve the boundary of the secrecy capacity region and to minimize the outage probability was also discussed in [17].

In the broadcast channel model above, the message W_2 is sent to both receivers. A variation of this model where W_2 is sent only to receiver 2 and is concealed from receiver 1 is analyzed in [29]. We describe it below:

A stochastic encoder is given by a matrix of conditional probabilities $f(\mathbf{x}|w_1, w_2)$, where $\mathbf{x} \in \mathcal{X}^n$, $w_i \in \mathcal{W}_i$, such that $\sum_{\mathbf{x} \in \mathcal{X}^n} f(\mathbf{x}|w_1, w_2) = 1$. Decoding functions are mappings $\psi_i: \mathcal{Y}_i^n \rightarrow \mathcal{W}_i$, $i = 1, 2$. An (M_1, M_2, n) code for the broadcast channel consists of one encoding function f and two decoding functions ψ_1, ψ_2 . The average error probability at receiver i , $i = 1, 2$ is defined as

$$P_{e,i}^{(n)} = \sum_{w_1, w_2} \frac{1}{M_1 M_2} \Pr[\psi_i(\mathbf{Y}_i) \neq w_i | (w_1, w_2) \text{ sent}].$$

The secrecy capacity region for this model, denoted by \mathcal{C}'_{BC} , is defined analogously as in Definition 3, with an additional secrecy condition $\frac{1}{n} H(W_2|Y_1^n) \geq R_2 - \varepsilon$ in (iii) of the definition.

Theorem 14 [29] (*Outer bound for \mathcal{C}'_{BC}*): Let (R_1, R_2) be an achievable secrecy rate pair. Then,

$$R_1 \leq \min \left[\begin{array}{l} I(V_1 \wedge Y_1|U) - I(V_1 \wedge Y_2|U), \\ I(V_1 \wedge Y_1|V_2, U) - I(V_1 \wedge Y_2|V_2, U) \end{array} \right],$$

$$R_2 \leq \min \left[\begin{array}{l} I(V_2 \wedge Y_2|U) - I(V_2 \wedge Y_1|U), \\ I(V_2 \wedge Y_2|V_1, U) - I(V_2 \wedge Y_1|V_1, U) \end{array} \right],$$

where the minima are over all auxiliary random variables U, V_1, V_2 satisfying $U \rightarrowtail V_1 \rightarrowtail X, U \rightarrowtail V_2 \rightarrowtail X$, and

$$P_{UV_1V_2XY_1Y_2} = P_U P_{V_1V_2|U} P_{X|V_1V_2} P_{Y_1Y_2|X}. \quad (10.27)$$

Theorem 15 [29] (*Inner bound for \mathcal{C}'_{BC}*): The secrecy capacity region \mathcal{C}'_{BC} is inner bounded by the union of all (R_1, R_2) satisfying

$$R_1 \leq I(V_1 \wedge Y_1|U) - I(V_1 \wedge V_2|U) - I(V_1 \wedge Y_2|V_2, U),$$

$$R_2 \leq I(V_2 \wedge Y_2|U) - I(V_1 \wedge V_2|U) - I(V_2 \wedge Y_1|V_1, U),$$

over all auxiliary random variables U, V_1, V_2 satisfying Eq. (10.27).

The secrecy capacity region for multi-antenna Gaussian broadcast channel with confidential messages was discussed in [85]. The sum of the secrecy rates for the parallel broadcast channels case was studied in [86].

10.5.2 Secure Broadcasting Through Wireless Channels

Let us consider a situation in which a user (transmitter) wishes to share some data with a set of wireless terminals (receivers). Instead of explicitly specifying which receivers should have access to the data, the transmitter would like to tie access capabilities to the relative location (a geographical context) of the receiver with respect to itself. In particular the transmitter would like to

- Provide immediate, unsecured access to any receiver in near proximity of the receiver.
- Provide access to other receiver with a medium proximity range upon specific request and with appropriate authorization.
- Prevent access to any receiver with a far proximity.

The notion of *proximity* in the above definition may be a simple distance metric. Alternatively it may embody a more complex geographical context. One example, which is naturally related to the inherent human proximity-based trust model, is as follows. The transmitter would like to provide immediate access to the data to all terminals in the same room with it. It will provide access upon request (and presumably with authentication) to terminals in the building. Finally, it needs to make sure that no terminal outside of the building is able to access the data. Because SNR will fall off sharply at the walls—i.e., at the room boundary and at the building boundary, a SNR-based broadcast secrecy approach suggests itself here.

An intuitive approach to solving this problem, which *almost* works is as follows. The transmitter uses a good (capacity-achieving) code such as LDPC to encode its message. The usage of such a curve ensures a sharp “waterfall” share to the Block Error Rate (BLER) vs. SNR curve. Thus for any such code, we may define some “critical SNR” such that if a receiver’s SNR is above this limit, a successful decoding is assured with probability close to 1, while for receivers with SNRs below this limit, the probability of successful decoding is near 0. The value of the critical SNR depends on the code rate. Our goal is, therefore to vary the effective code rate depending on which of the trust zone the receiver is located in. We wish to do this within a single transmission—i.e., while broadcasting a common message in a single stream.

This goal can be achieved through the use of puncturing as follows. The transmitter encodes the message using a fairly low rate code. It then selects certain output symbols and scrambles them using a random scrambling sequence. For example, if a binary code is used, certain output (codeword) bits are scrambled by bit-wise XOR with a random bit-sequence. The resulting sequence is then transmitted. The location of the scrambled symbols is advertised, however the scrambling sequence itself is held secret by the transmitter.

Receivers in the near-proximity trust zone possess a sufficiently high SNR to decode the transmitted codeword without the scrambled symbols—these are simply treated as punctured. Thus, the extent of scrambling defines the extent of this innermost trust zone.

Receivers in the mid-range zone do not have a sufficiently high SNR to simply decode the transmitted codeword. However, these may use a secure side channel

(which must be provided) to request information about the scrambling sequence from the transmitter. This mechanism may then be used to control access beyond the inner-most trust zone. In fact, by revealing an ever-increasing portion of the scrambling sequence, multiple intermediate trust zones can be defined.

Finally, the coding rate of the mother code defines the boundary of the no-access zone. Below a certain SNR (beyond a certain distance), even the original, unscrambled codeword can no longer be successfully decoded.

As we noted, the approach above does not quite deliver the required secrecy. In particular, it suffers from two significant drawbacks. First, the secrecy here relies on the inability of the receivers to decode the transmitted codeword below a certain SNR. However, such secrecy is rather weak, as quite a lot of information may be leaked anyway. Second, in practice the sharp SNR boundaries required here exist only *on the average*. At any given time, fading blurs such boundaries and makes them rather indeterminate.

Fortunately, both of these issues are addressed by the work on the wiretap model which we outlined. In particular, the work of [26–28] demonstrates how practical coding schemes may be used to provide strong, well-defined security in a wiretap channel model. The work on fading wiretap channels, in particular [15, 16] but also other, demonstrates how to use the average long-term SNR to define the trust-zone boundaries in a fading wiretap channel. By putting these results together with the basic system described above we can enable a well-defined secure geographical trust-zone communication system.

10.6 Conclusions

In this chapter, we discussed the generation of information-theoretic secret keys among multiple terminals under the source type model and the channel type model. Specific results in the case of three terminals were presented. We then developed the pairwise-independent source model and explored its connection to key generation in wireless communication systems. Key generation algorithms and capacity results for this model were presented. We concluded with a look at the wiretap channel model. We discussed certain problems with applicability of this model in real-world systems and, we demonstrated that in the context of networks of terminals the wiretap model does offer meaningful results. We overviewed relevant theoretical developments in this area.

References

- [1] J. A. Buchmann, *Introduction to Cryptography*, New York: Springer, 2000.
- [2] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
- [3] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- [4] S. L. Leung-Yan-Cheong and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, July 1978.

- [5] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. IT-24, pp. 339–348, May 1978.
- [6] E. Tekin and A. Yener, “The Gaussian multiple access wire-tap channel with collective secrecy constraints,” *Proc. Int. Symp. Inf. Theory*, pp. 1164–1168, July 2006.
- [7] R. Liu, I. Maric, R. Yates and P. Spasojevic, “The discrete memoryless multiple access channel with confidential messages,” *Proc. Int. Symp. Inf. Theory*, pp. 957–961, July 2006.
- [8] Y. Liang and H. V. Poor, “Multiple access channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 54, pp. 976–1002, Mar. 2008.
- [9] Y. Chen and A. J. Han Vinck, “Wiretap channel with side information,” *Proc. Int. Symp. Inf. Theory*, pp. 2607–2611, July 2006.
- [10] C. Mitrpanit, A. J. H. Vinck and Y. Luo, “An achievable region for the Gaussian wiretap channel with side information,” *IEEE Trans. In. Theory*, vol. 52, pp. 2181–2190, May 2006.
- [11] L. Lai, H. El Gamal and H. V. Poor, “The wiretap channel with feedback: Encryption over the channel,” e-print arXiv: cs.IT/07042259, 2007.
- [12] J. Grubb, S. Vishwanath, Y. Liang and H. V. Poor, “Secrecy capacity for semi-deterministic wire-tap channels,” *Proc. IEEE Inf. Theory Workshop Wireless Networks*, 2007.
- [13] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” *Proc. IEEE Int. Symp. Inf. Theory*, pp. 356–360, July 2006.
- [14] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, “Wireless information-theoretic security–Part I: Theoretical aspects,” e-print arXiv: cs.IT/0611120, 2006.
- [15] P. Gopala, L. Lai and H. El Gamal, “On the secrecy capacity of fading channels,” e-print arXiv: cs.IT/0610103, 2006.
- [16] Z. Li, R. Yates and W. Trappe, “Secure communication with a fading eavesdropper channel,” *Proc. IEEE Int. Symp. Inf. Theory*, pp. 1296–1300, June 2007.
- [17] Y. Liang, H. V. Poor and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inf. Theory*, June 2008.
- [18] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2152–2155, Sept. 2005.
- [19] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas: The MISOME wiretap channel,” e-print arXiv: cs.IT/07084219, 2007.
- [20] A. Khisti, G. W. Wornell, A. Wiesel and Y. Eldar, “On the Gaussian MIMI wiretap channel,” *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2471–2475, June 2007.
- [21] Z. Li, W. Trappe and R. Yates, “Secret communication via multi-antenna transmission,” *Proc. Conf. Inf. Sci. Syst.*, Mar. 2007.
- [22] S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2466–2470, June 2007.
- [23] X. Tang, R. Liu, P. Spasojevic and H. V. Poor, “Interference-assisted secret communication,” *Proc. IEEE Inf. Theory Workshop*, May 2008.
- [24] L. Lai and H. El Gamal, “The relay-eavesdropper channel: Cooperation for secrecy,” *IEEE Trans. Inf. Theory*, submitted.
- [25] M. Yuksel and E. Erkip, “The relay channel with a wire-tapper,” *Proc. Conf. Inf. Sci. Syst.*, Mar. 2007.
- [26] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin and J. M. Merolla, “Capacity achieving codes for the wiretap channel with applications to quantum key distribution,” e-print arXiv: cs.IT/0411003, 2004.
- [27] M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, “Wireless information-theoretic security–Part II: Practical implementation,” e-print arXiv: cs.IT/0611121, 2006.
- [28] R. Liu, Y. Liang, H. V. Poor and P. Spasojevic, “Secure nested codes for Type II wiretap channels,” *Proc. IEEE Inf. Theory Workshop*, pp. 337–342, Sept. 2007.

- [29] R. Liu, I. Marić, P. Spasojević and R. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions,” *IEEE Trans. Inf. Theory*, June 2008.
- [30] U. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, pp. 733–742, May 1993.
- [31] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography, Part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, pp. 1121–1132, July 1993.
- [32] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental quantum cryptography,” *J. Cryptol.*, vol. 5, pp. 3–28, 1992.
- [33] J. E. Hershey, A. A. Hassan and R. Yarlagadda, “Unconventional cryptographic keying variable management,” *IEEE Trans. Commun.*, vol. 43, pp. 3–6, Jan. 1995.
- [34] C. Ye, A. Reznik and Y. Shah, “Extracting secrecy from jointly Gaussian random variables,” *Proc. Int. Symp. Inf. Theory*, pp. 2593–2597, July 2006.
- [35] C. Cachin and U. Maurer, “Linking information reconciliation and privacy amplification,” *J. Cryptol.*, vol. 10, pp. 97–110, 1997.
- [36] C. H. Bennett, G. Brassard and J. M. Robert, “How to reduce your enemy’s information,” *Adv. Cryptol.—CRYPTO*, pp. 468–476, 1986.
- [37] G. Brassard and L. Salvail, “Secret-key reconciliation by public discussion,” *Adv. Cryptol.—EUROCRYPT*, pp. 410–423, 1994.
- [38] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” *IEEE Trans. Inf. Theory*, vol. 50, pp. 3047–3061, Dec. 2004.
- [39] J. Chen, D. He and E. Yang, “On the codebook-level duality between Slepian-Wolf coding and channel coding,” *Proc. IEEE Inf. Theory Appl. Workshop*, pp. 84–93, Feb. 2007.
- [40] J. Garcia-Frias and Y Zhao, “Compression of correlated binary sources using turbo codes,” *IEEE Commun. Lett.*, vol. 5, pp. 417–419, Oct. 2001.
- [41] A. D. Liveris, Z. Xiong and C. N. Georghiades, “Compression of binary sources with side information at the decoding using LDPC codes,” *IEEE Commun. Lett.*, vol. 6, pp. 440–442, Oct. 2002.
- [42] S. S. Pradhan and K. Ramchandran, “Distributed source coding using syndromes (DISCUS): Design and construction,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 626–643, Mar. 2003.
- [43] T. P. Coleman, A. H. Lee, M. Médard and M. Effros, “Low-complexity approaches to Slepian-Wolf near-lossless distributed data compression,” *IEEE Trans. Inf. Theory*, vol. 52, pp. 3546–3561, Aug. 2006.
- [44] C. H. Bennett, G. Brassard and J. M. Robert, “Privacy amplification by public discussion,” *SIAM J. Comput.*, vol. 17, pp. 210–229, Apr. 1988.
- [45] C. H. Bennett, G. Brassard, C. Crepeau and U. Maurer, “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, pp. 1915–1923, Nov. 1995.
- [46] J. L. Carter and M. N. Wegman, “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, pp. 143–154, 1979.
- [47] M. N. Wegman and J. Carter, “New hash functions and their use in authentication and set equality,” *J. Comput. Syst. Sci.*, vol. 22, pp. 265–279, 1981.
- [48] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 839–851, Apr. 2003.
- [49] R. Raz, I. Reingold and S. Vadhan, “Extracting all the randomness and reducing the error in Trevisan’s extractors,” *Proc. Symp. Theory of Comput.*, pp. 149–158, 1999.
- [50] Y. Dodis, J. Katz, L. Reyzin and A. Smith, “Robust fuzzy extractors and authenticated key agreement from close secrets,” *Adv. Cryptol.—CRYPTO*, pp. 232–250, Aug. 2006.
- [51] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM J. Comput.*, pp. 97–139, 2008.

- [52] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," *Adv. Cryptol.—EUROCRYPT*, Apr. 2008.
- [53] J. Muramatsu, "Secret key agreement from correlated source outputs using LDPC matrices," *IEICE Trans. Fundamen.*, vol. E89-A, pp. 2036–2046, July 2006.
- [54] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *Proc. Int. Symp. Inf. Theory*, pp. 2133–2137, Sept. 2005.
- [55] U. M. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," *Adv. Cryptol.—EUROCRYPT*, 1997.
- [56] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, pp. 822–831, Apr. 2003.
- [57] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, pp. 832–838, Apr. 2003.
- [58] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, pp. 344–366, Mar. 2000.
- [59] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part I: Source model," *IEEE Trans. Inf. Theory*, submitted.
- [60] C. Ye and A. Reznik, "Group secret key generation algorithms," *Proc. Int. Symp. Inf. Theory*, pp. 2596–2600, June 2007.
- [61] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Secret key generation for a pairwise independent network model," *Proc. Int. Symp. Inf. Theory*, pp. 1015–1019, July 2008.
- [62] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2437–2452, June 2008.
- [63] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—Part II: Channel model," *IEEE Trans. Inf. Theory*, submitted.
- [64] C. Ye and P. Narayan, "The private key capacity region for three terminals," *Proc. Int. Symp. Inf. Theory*, p. 44, June 2004.
- [65] C. Ye and P. Narayan, "The secret key-private key capacity region for three terminals," *Proc. IEEE Int. Symp. Inf. Theory*, pp. 2142–2146, Sept. 2005.
- [66] C. Ye, A. Reznik, Y. Shah and G. Sternberg, "Method and system for generating a secret key from joint randomness," U.S. patent application 20070165845, 11/612671, July 2007.
- [67] R. Wilson, D. Tse and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Foren. and Secu.*, vol. 2, pp. 364–375, Sept. 2007.
- [68] S. Mathur, W. Trappe, N. Mandayam, C. Ye and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," *Proc. ACM Conf. Mobile Comput. Network.*, Sept. 2008.
- [69] T. Aono, K. Higuchi, T. Ohira, B. Komiyama and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, pp. 3776–3784, 2005.
- [70] H. Imai, K. Kobara and K. Morozov, "On the possibility of key agreement using variable directional antenna," *Proc. Joint Workshop Inf. Security*, 2006.
- [71] H. Koroparty, A. A. Hassan and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52–55, Feb. 2000.
- [72] A. A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *IEEE Digital Signal Processing Mag.*, vol. 6, pp. 207–212, 1996.
- [73] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Using the physical layer for wireless authentication under time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, July 2008.

- [74] U. M. Maurer, “The strong secret key rate of discrete random triples,” *Communications and Cryptography: Two Sides of One Tapestry*, R. E. Blahut et al., Ed, Norwell, MA: Kluwer, Ch. 26, pp. 271–285, 1994.
- [75] U. M. Maurer and S. Wolf, “Information-theoretic key agreement: from weak to strong secrecy for free,” *Advances in Cryptology - EUROCRYPT*, pp. 351–368, May 2000.
- [76] A. Schrijver, *Theory of Linear and Integer Programming*, New York: Wiley, 1986.
- [77] R. Renner and S. Wolf, “New bounds in secret-key agreement: the gap between formation and secrecy extraction,” *Adv. Cryptol.—EUROCRYPT*, pp. 562–577, 2003.
- [78] C. St. J. A. Nash-Williams, “Edge disjoint spanning trees of finite graphs,” *J. London Math. Soc.*, 36, pp. 445–450, 1961.
- [79] W. T. Tutte, “On the problem of decomposing a graph into n connected factors,” *J. London Math. Soc.*, vol. 36, pp. 221–230, 1961.
- [80] H. N. Gabow and H. H. Westermann, “Forests, frames, and games: Algorithms for matroid sums and applications,” *Algorithmica*, vol. 7, pp. 465–497, 1992.
- [81] A. Schrijver, *Combinatorial Optimization—Polyhedra and Efficiency*, New York: Springer, 2003.
- [82] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.*, New York, NY: Academic, 1982.
- [83] P. Gács and J. Körner, “Common information is far less than mutual information,” *Probl. Contr. Inf. Theory*, vol. 2, pp. 149–162, 1973.
- [84] A. Reznik, A. Carlton, A. Briancon, Y. Shah, P. Chitrapu, R. Mukherjee and M. Rudolf, “Method and system for securing wireless communications,” U.S. patent application 20060133338, 11/283017, June 2006.
- [85] R. Liu and H. V. Poor, “Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages,” e-print arXiv: cs.IT/07094671, 2007.
- [86] A. Khisti, A. Tchamkerten and G. W. Wornell, “Secure broadcasting,” e-print arXiv: cs.IT/0702093, 2007.

Chapter 11

Secret Key Agreement Techniques Based on Multipath Propagation Characteristics*

Hideichi Sasaoka and Hisato Iwai

11.1 Introduction

As information society progresses, wireless communications such as cell-phone and WLAN (Wireless Local Area Network) systems will become more widely and rapidly accepted as the means to communicate. Unfortunately, there are many perceived weaknesses inherent in the security of wireless communications—largely due to the fact that the signals are transmitted through the air and are easily captured by third parties. Examples of such threats are found in eavesdropping of transmitted data on a radio channel, illegal and/or unauthorized access to public WiFi networks, and so on. In fact, security for wireless systems has been recognized as a major technical challenge that needs to be addressed in order for wireless systems to be the basis for many future applications.

In the realm of countermeasures for wireless security problems, encryption techniques such as symmetric and public key schemes are commonly used to secure communications. In mobile communications, where the processing capability of a terminal is limited, symmetric key encryption schemes are generally used since public key methods require a large amount of processing. However, even for symmetric key cryptography, there exist some problems in how to securely share and manage the associated keys. Further, there also exist risks associated with the loss and theft of encryption keys. Theoretically, both these schemes provide “security based on computational complexity”. Therefore, when the computational capability of an adversary increases or a new algorithm to crack the encryption is discovered in the future, there may be a resulting loss of security for protocols built solely upon these encryption schemes. On the other hand, another approach to confidentiality based

H. Sasaoka (✉)

Department of Electronics, Doshisha University

Kyoto, Japan

e-mail: hsasaoka@mail.doshisha.ac.jp

*Portions of the material have appeared previously in: H. Iwai and H. Sasaoka, “Secret information and sharing techniques based on radio wave propagation,” IEICE Transactions B (Japanese Edition), vol. J90-B, no. 9, pp. 770–783, Sept. 2007. ©2007 IEICE 09RA0011.

on “information-theoretic security” has been investigated [1–3]. Some examples of this approach are the one-time pad cipher (Shannon’s cipher system) [4], secret key sharing in a noisy channel [5], and secret key agreement based on common information [6]. Quantum cryptography techniques [7] can also be considered as examples of this approach to confidentiality. Among the approaches to information-theoretic secrecy, encryption techniques associated with noisy channels [5] is based on relatively practical assumptions. Unfortunately, for the other examples, most research on the techniques have been quite limited when considering their feasibility [2].

More recently, cryptographic key agreement schemes [8, 9] and secure information transmission schemes [10] utilizing the propagation characteristics of a mobile communication channel have been proposed. The principles behind these schemes are close to the above encryption technique using a noisy channel, but are founded on more practical assumptions. In the category of key agreement schemes, highly correlated information can be shared between legitimate users based on the reciprocity of a wireless propagation path, whereas it is difficult for third parties at a separate location to estimate the shared information because of the locality and complexity of the propagation characteristics. Similarly, in the category of secure information transmission schemes, by transmitting pre-distorted signals to compensate for the transfer characteristics of the channel between the two legitimates, undistorted signals can be received at the legitimate receiver, whereas at a third party located at a different point, the signals are not correctly received and recovery of the transmitted information is not possible. This mechanism can also utilize the reciprocity of a radio propagation path.

Following the above pieces of work, several approaches based upon the principles have been presented. As a form of secure information transmission, a scheme utilizing phase variation of a propagation channel as the distortion to differentiate the communication quality of the legitimate user from the eavesdropper was proposed [10]. A similar method utilizing multipath delay as the source of the distortion was also presented. In the realm of key agreement schemes, various schemes have been proposed and may be classified according to what propagation characteristic is measured. Some examples are: a method to measure phase differences of multitone signals [8, 9], a method to measure the time variant frequency characteristics of the amplitude of the received signal [11], a method to measure the impulse response of the propagation channels assuming UWB-IR (Ultra Wideband, Impulse Radio) transmission [12, 13]. Recently methods to measure artificial signal fluctuations generated by antenna array systems have also been proposed [14, 15].

In this chapter, we examine secret key agreement schemes based on the characteristics of radio propagation. First, the fundamental principles of such a scheme is introduced. Then actual examples of system configurations and the processing procedures needed to realize such a scheme are presented in detail. Lastly, we overview a prototype system that has been developed for key agreement based on radio propagation. Throughout the discussion, we note that many research activities have been recently presented in the field of physical layer security, and that the discussion presented in this chapter is mainly focused on aspects related to realizing the transition of such theoretical works into practical, actual communication systems.

11.2 Principle of Secret Key Agreement Scheme Based on Radio Propagation Characteristics

Figure 11.1 shows a schematic depicting the principle of secret key agreement based on radio propagation characteristics. In the figure there are two radio stations A and B and the propagation path between them is assumed to be a multipath fading channel. Assuming the stations are moving, the received signals at A and B suffer from fluctuations due to the multipath fading. If the two transmissions from A to B and from B to A are performed at the same moment and at an identical carrier frequency, the fading fluctuations, i.e., the variation of the propagation characteristics, at the two receiving stations will be identical due to the reciprocity of the radio transmission path. In actual systems, it is impossible to transmit and receive at the same time and at the same frequency. In the systems described in the next section, TDD (Time Division Duplex) is generally assumed. By generating a digital sequence at each station based on the information of the propagation characteristics, common information, such as a secret key, can be remotely shared between the two stations. On the other hand, a third party (eavesdropper) located at a different point receives the different fading from the two. As a result, the eavesdropper cannot obtain the same propagation characteristics as those of the legitimate stations and it is thus impossible to steal the secret key.

The shared secret key can be used as a common key for encryption. In practice, the key can be updated at an arbitrary moment if required. In existing symmetric key encryption, the key is pre-assigned before starting communication and the key cannot be replaced unless it is transmitted through the radio communication channel. Periodical updating of the key is necessary to improve the security of any communication protocol.

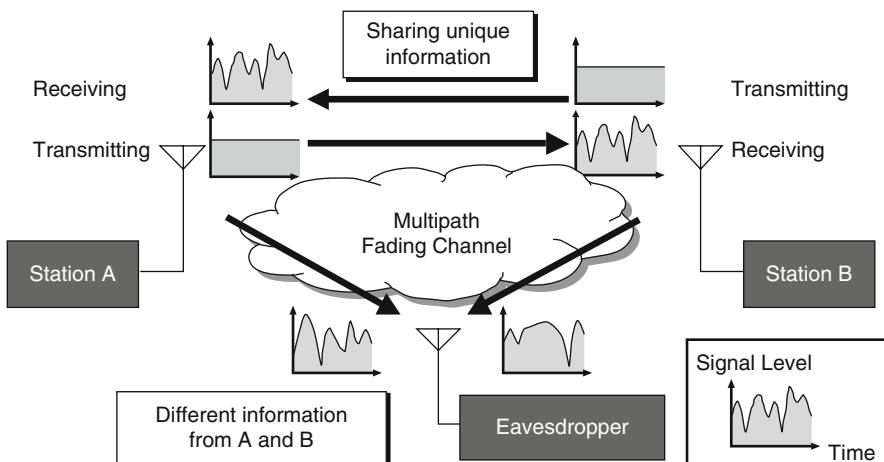
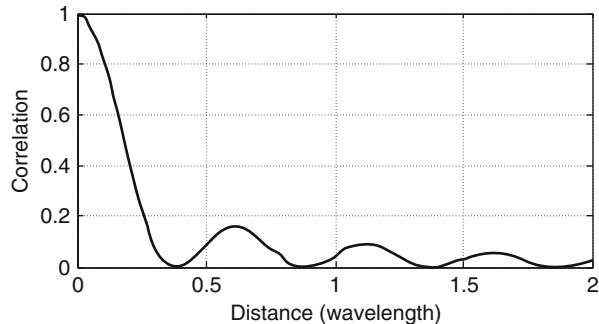


Fig. 11.1 Principle of secret key agreement scheme based on radio propagation characteristics

Fig. 11.2 Spatial correlation characteristics in Rayleigh multipath environment where direction of arrival is omni-directional



Unfortunately, wireless communication is usually unstable and unreliable. It easily suffers from noise and other distortions existing in the transmission path. Therefore, in order to realize the agreement of secret keys in actual wireless communication environments, countermeasures against the fading and noise are indispensable to increase reliability.

Figure 11.2 illustrates the spatial correlation of the Rayleigh fading process where the direction of arrival of the multipath waves is omni-directional. The spatial correlation coefficient of the signal level fluctuation, $\rho_A(\Delta x)$, is given as $\rho_A(\Delta x) = [J_0(k\Delta x)]^2$ where x is spatial separation and k is the wavenumber at the carrier frequency[15, 16] and J_0 is the zero-order Bessel function of the first kind. From the figure it is seen that, when the spatial separation is more than the quarter wavelength, the correlation becomes considerably small.

Let us consider a binarization of the fading process, where a fluctuation is quantized into a set of binary values (binarized) according to the signal level. Figure 11.3 depicts the basic method. The median value of the signal level distribution is firstly determined and then using the median value as the threshold the signal level is binarized to 1 or 0. This is one of the simplest methods of the secret key agreement

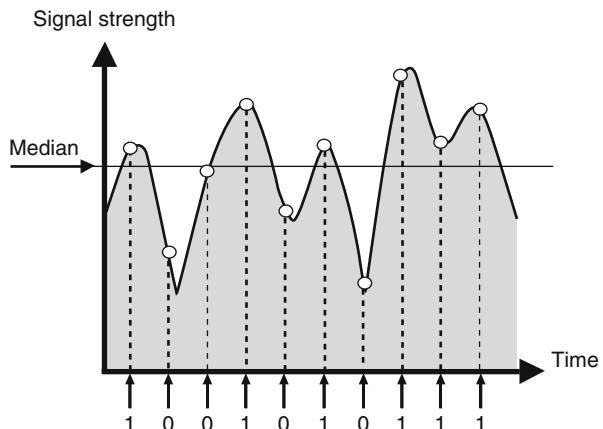
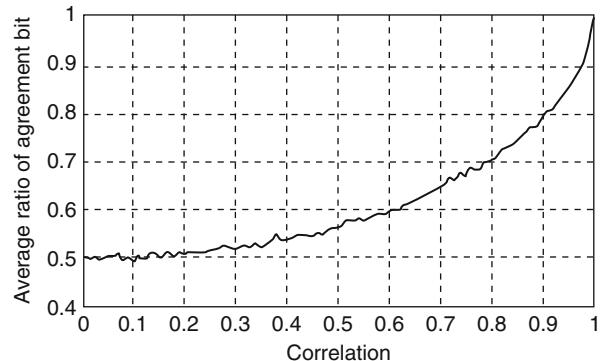


Fig. 11.3 Binary code generation determined by median

Fig. 11.4 The average agreement ratio for varying levels of spatial correlation



scheme based on radio propagation characteristics, and such a method is described in other chapters in this book.

We can estimate the properties governing the agreement assuming a simple model for two Rayleigh-distributed signals with fluctuations having correlation ρ . The simulated average agreement ratio between the bits generated from the two correlated Rayleigh fading by the binarization method of Fig. 11.3 is given in Fig. 11.4. The characteristics are calculated when the correlation value is changed from 0.0 to 1.0. It is seen from the figure that considerably high correlation is required to precisely estimate a sequence. Even when the correlation is 0.9, the agreement ratio remains around 0.8. Assuming a 128-bit sequence, the probability of achieving perfect agreement when the average agreement ratio is 0.8 is almost zero. In the propagation environment where the arriving direction of the multipath waves is omni-directional, the distance over which the spatial correlation decreases to 0.9 is around 0.1 of a wavelength, as seen from Fig. 11.2. This length corresponds to about 4 cm in the 800 MHz band and 1.25 cm in the 2.4 GHz band, respectively. Eavesdropping is, in usual cases, done in a position separate from the legitimate user, and therefore it is almost impossible to steal the secret key.

In this section, some examples of actual realization of the secret key agreement based on radio propagation characteristics are presented. Various system configurations and methodologies are described to realize the principle of the scheme.

11.2.1 Secret Key Generation Using ESPAR Antenna

The fundamental principle behind sharing confidential information between two radio stations without being stolen by third parties based on the propagation characteristics was presented in the previous section. However, when the temporal fluctuation due to fading is slow, the generated key sequences become flat (all 0 or 1, or close to them) and the possibility of eavesdropping increases. When it is applied to indoor wireless systems, such as WLAN, the speed of fading is particularly low and the problem becomes more serious. To solve this problem, a method using a directional-pattern controllable antenna system (specifically, the ESPAR antenna: Electronically

Steerable Parasitic Array Radiator) was developed. In this system, the antenna pattern is varied to generate artificial fading. To control the directional pattern, a digital beam forming antenna (DBF) is another realization, however as such a device is complex and expensive and thus not suitable for consumer wireless systems such as WLAN. The ESPAR antenna is an analog beam forming antenna and can be realized at much cheaper cost than DBF.

An overview of a 7-element ESPAR antenna is shown in Fig. 11.5. The ESPAR antenna has a single central active radiator surrounded by 7 parasitic elements loaded with varactor diodes as variable reactors. By adjusting the DC voltage applied to the varactors in the reverse bias, the antenna's directional pattern can be varied. Since it has just a single RF radiator, the cost is can be much smaller than that of a DBF antenna. The peak gain of the ESPAR antenna is around 9 dBi. Figure 11.6 shows an example of the measured radiation pattern of an ESPAR antenna. In the system shown in Fig. 11.5, the bias voltage is controlled digitally with 8-bit resolution. As the result, the possible selection of the radiation patterns is $(2^8) - (7 + 1) = 248$.

We now describe the process of secret key agreement in detail. The preconditions are as follows: We assume two users. One of the two is an “access point A” having the ESPAR antenna and the other is “user terminal B” with an omni-directional antenna. They try to generate a secret key collaboratively, but they do not exchange information relating to the key through the air. In the scheme, identical multipath fading must be experienced at both A and B. We assume TDD is adopted to realize this condition. When the TDD frame is sufficiently short, the two characteristics can be assumed identical. However, in actual TDD systems, there exists a small time difference. The effect of the difference is discussed later. In the ESPAR antenna, the combination of the 6 reactance values of the parasitic elements are called a reactance

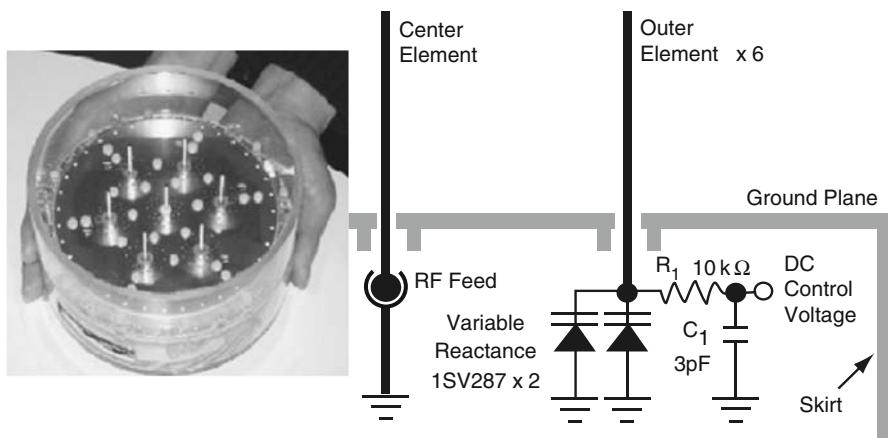
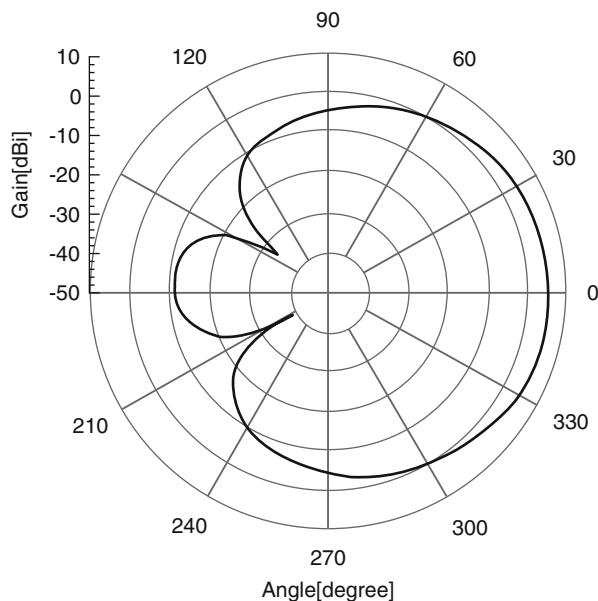


Fig. 11.5 7-element ESPAR antenna

Fig. 11.6 An example of the measured directional pattern of a 7-element ESPAR antenna



vector. The key generation process is shown in Fig. 11.7. The following is the detailed procedure for generating a shared key:

1. A packet is transmitted from A and is received at B . When B receives the packet, it measures the RSSI (Received Signal Strength Indicator) for that packet.
2. After A transmits, A switches to receiving mode while keeping the same directional pattern. Then B transmits a packet to A and A measures the RSSI.
3. After step (2) is completed, the directional pattern is varied by changing the reactance vector randomly.
4. For key length K , an RSSI sequence having $K + \alpha$ RSSI values is captured. Additional α values are used as redundancy to increase the agreement probability by the data deletion process shown below.
5. Due to the reciprocity of radio propagation, the sequences at A and B are (ideally) identical, as shown in Fig. 11.8. However, there may exist some disagreements. One of the possible sources of the errors is random noise. The effect of the noise can be reduced by averaging multiple RSSI samples during the same antenna pattern. Other significant factors that causes disagreement are the differences in the transmission powers, the gain of the amplifier at the receiver, the antenna performance (sensitivity or directivity), etc. In usual wireless systems, it is not easy to precisely calibrate the effect of these various factors. Therefore, here we use a normalization approach to cancel them out. Using binarization by the median value of the RSSI sequence as the threshold of the binarization, only the relative fluctuation is taken into account and the absolute value is not required.
6. At A , a subset of the sequence is produced by selecting the largest $K/2 + \beta$ and the smallest $K/2 + \beta$ RSSI values, where $\beta < \alpha/2$. In other words, the

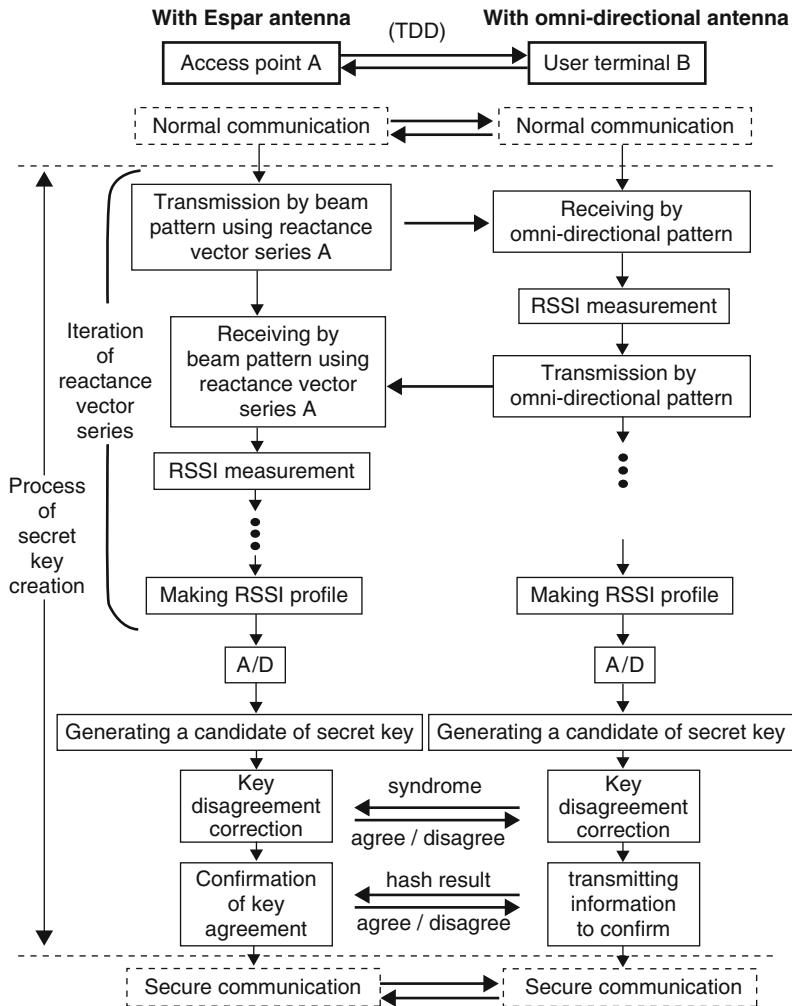


Fig. 11.7 The procedure for generating keys from RSSI profiles

RSSI values around the threshold (median) are removed and not used to generate the key. These values are likely affected by the noise and the probability of the disagreement is higher for these samples than for the rest of the values.

7. The positions of the deleted RSSI values at A are sent to B using a public communication channel. The corresponding values of the RSSI sequence at B are then deleted.
8. At B, a similar deletion process to that of A is conducted. Instead of $K/2 + \beta$ values in the process at A, the largest $K/2$ and the smallest $K/2$ RSSI values from the remaining sequence are selected to generate the resultant sequence of length is K . Then the positions of the deleted values are sent to A, and they are deleted from the sequence at A.

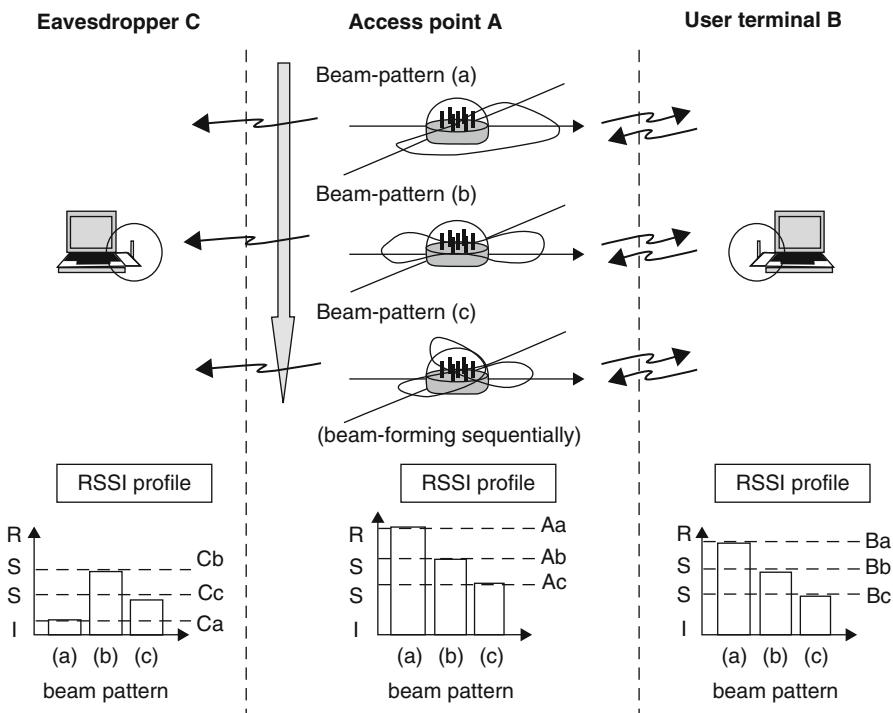


Fig. 11.8 Schematic for the procedure for generating an RSSI profile

9. Both *A* and *B* now have candidate RSSI sequences for establishing a secret key.
10. The RSSI sequences are then binary-coded by the threshold level as in Fig. 11.3.
11. A disagreement correction process is carried out by applying an error correction technique. When we use regular error correction methods, it is necessary to exchange the coded words between the two stations. However, it has to be done through radio communication so that it causes the leakage of the information of the secret key to third parties. We therefore adopt an error correction technique where, instead of the whole coded word, only the syndrome of the original sequence is transmitted. At *B*, the syndrome, $S_b = x_b \mathbf{H}^T$, is generated where x_b is the bit sequence of the candidate of the secret key generated at *B*. \mathbf{H} denotes a check matrix of the error correction code. In the actual hardware shown later, we adopt BCH coding. The superscript T denotes the transpose of the matrix. The syndrome is transmitted from *B* to *A*. Also at *A*, the syndrome, $S_a = x_a \mathbf{H}^T$, is generated where x_a is the bit sequence of the candidate at *A*. We define the differences of the original sequences and the syndromes as $e = x_a - x_b$ and $S = S_a - S_b$, respectively. According to the characteristics of the check matrix, we have a relationship as $S = e \mathbf{H}^T$. At *A*, S is obtained by comparing the received and transmitted syndromes and, if $S = 0$, it corresponds to $e = 0$ and the key agreement is successful. Otherwise, between the two sequences some errors exist.

They can be corrected by the error correction code up to the maximum number of the correctable bits of the check matrix. Because the syndrome is transmitted through a wireless channel, which is publicly accessible, it is reasonable to assume the information is monitored also at eavesdroppers. However, by only monitoring the syndrome, the whole sequence of A and B cannot be obtained, although the number of the useful bits in the key decreases by the number of bits in the syndrome.

12. After the disagreement correction process, the agreement is tested utilizing a cryptographic hash function. One-way transformation by hashing is adopted to check the agreement securely. Firstly at B , the key is hashed and it is transmitted to A . Then it is compared with the hashed version of the key at A generated by the same hashing process. Note that the check process by hash function is not mandatory in this scheme. The disagreement of the keys can be detected by the several other methods. For example, if the encrypted secret communication after the key agreement stage is unnaturally inaccurate, the disagreement of the keys should be firstly checked.
13. If the examination of the key agreement process is successful, the secret key agreement process is complete and it can be used as the encryption key for the secret communication like the common key. If agreement is not obtained, the generated keys are discarded and the entire process is resumed until agreement is realized.

The procedure has been realized in a prototype system. The hardware configuration and the agreement performance obtained by experiments using the hardware are presented in the later section.

11.2.2 Secret Key Agreement Scheme Using Time-Variant Frequency Characteristics of a Broadband OFDM Signal

In current WLAN systems, OFDM (Orthogonal Frequency Division Multiplex) is used as the radio transmission systems. As an example, a broadband OFDM transmission using 20 MHz of bandwidth is adopted in IEEE802.11a/g WLAN systems. In such a broadband transmission system, the propagation characteristics become frequency-selective. One approach to obtain a signal fluctuation effectively in such a system is to utilize the frequency characteristics of the broadband fading process. In OFDM systems, FFT (Fast Fourier Transform) is used in receiving. Prior to the process the frequency characteristics due to the frequency-selective fading have to be equalized. This is accomplished using pilot symbols multiplexed with the data symbols in the frequency and time domains. Therefore, the source to generate the secret key is easily obtained from the equalization process. The frequency characteristics, however, often do not have sufficient fluctuation to generate a *secure* key. Combining the time domain fluctuation with the frequency domain is a good way to generate a sufficient amount of the variation of propagation characteristics. As in the ESPAR antenna system, TDD is required for two legitimate users to share identical information. An example of the time-variant frequency characteristics assuming

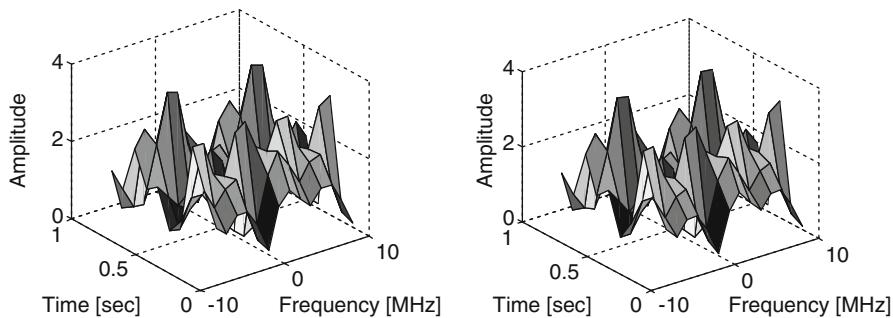


Fig. 11.9 The time-variant frequency characteristics of a wideband propagation channel

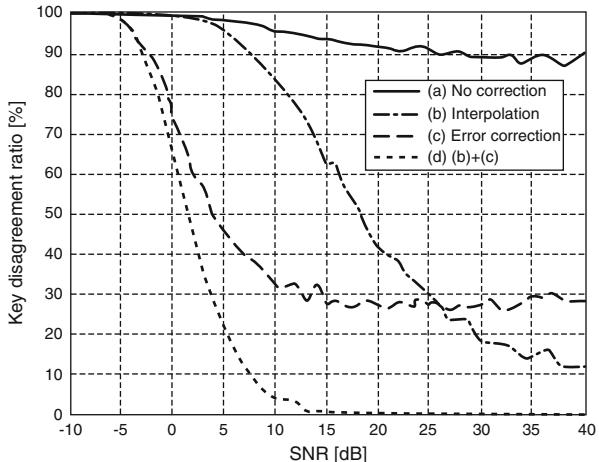
IEEE 802.11a OFDM bandwidth is presented in Fig. 11.9. The characteristics are obtained through a computer simulation where a three Rayleigh-wave delay profile model having the delay spread of 60 nsec is assumed. Figure 11.10 presents examples of the simulated bit sequences of the secret key at the two legitimate users. The sequences are generated by the binarization of the signal strength of the time-variant frequency characteristics by the median value of the distribution. In this case, the SNR (Signal to Noise power Ratio) at the receiver is assumed 15 dB. The bit patterns for (a) and (b) are almost identical, however some disagreements are observed. In addition to the noise, the time difference between the transmissions from the two stations is another source of the disagreement. Figure 11.11 shows the simulated disagreement ratio of the generated keys at the two users. Specifically, it corresponds to the average ratio describing the amount of differences that exist between the two key sequences. The key length is assumed to be 128 in the figure. Curve (a) is the disagreement characteristics of the sequences generated by the procedure above. In the simulation the time difference of the two-way transmissions of TDD

0	0	0	1	0	0	0	1	0	0	0	0	0	0
1	0	1	1	0	0	1	1	1	0	1	1	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	0	0	0	0	0	0	1	1	0	0	0
0	0	0	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	0	0	0	1	1	0	0	0	0	0
0	1	1	1	1	0	1	1	0	1	1	1	1	0
1	1	1	0	0	0	0	0	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1	0	0	0	0	0	0

0	0	0	1	0	0	0	1	0	0	0	0	0	0
1	0	1	1	0	0	1	1	1	0	1	1	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	0	0	0	0	0	0	0	1	1	0	0
0	0	1	1	1	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	1	1	0	0	0	0	0
0	1	1	1	1	0	1	1	0	1	1	1	1	0
1	1	1	0	0	0	0	0	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1	1	0	0	0	0	0

Fig. 11.10 An example of the bit patterns shared as a result of the key generation procedure being used with an OFDM wideband signal

Fig. 11.11 Key disagreement as SNR is changed



is set as 1.4 msec. The assumed maximum Doppler frequency of the fading process is 10 Hz in the simulation, corresponding to an indoor environment. The fluctuation is relatively slow, but the difference between the transmission timings introduces errors beyond those introduced by just noise. Curve (b) shows the disagreement performance where linear-interpolation using 2 adjacent TDD frames is employed to estimate and compensate for the difference between the transmission characteristics. It is seen from the figure the performance is improved in curve (b). The curve (c) is a case where an error correction technique is applied. We have assumed that 5 or fewer errors among the 128 bits will be ideally corrected by an appropriate error correction scheme. Even when error correction is combined with the original method (without the timing compensation), the disagreement is not sufficiently improved. This indicates that the number of the errors in the original scheme is often more than 5. On the other hand, when the two techniques are combined, the performance is significantly improved, as shown by curve (d). Here, the error correction is realized by sending the syndrome as is done in the ESPAR antenna system presented in this chapter. By using the two schemes, the disagreement of the keys can be successfully improved and perfect key agreement between the two stations is essentially realized when $SNR > 15$ dB, which is a reasonable condition for actual communication channels.

11.2.3 Secret Key Agreement Scheme Using Antenna Switching

To share a secret key securely, sufficient amount of the fluctuation is required. For the key sharing scheme using the ESPAR antenna, an artificial fluctuation is generated by changing the directional antenna pattern of the access point's antenna using the beam steering antenna. In this section, another method applicable to slow fading environments with relatively simpler system configuration is presented. Here, instead of using an array antenna, two simple antennas are used and the signal levels to and from the antennas are compared to determine the bit.

Figure 11.12 conceptually shows the principle behind the method. We assume radio station A has multiple antennas and station B has a single antenna (e.g., it may be merely a user terminal). First, a signal is transmitted from A to B using one of its antennas and station B measures the signal level. Then A switches the transmission antenna to the other one and the received signal level is again measured at B. At B, the two received levels are compared and a bit is decided according to the result of the comparison. For example, the bit is 1 if the received signal level transmitted from the 1st antenna is larger than the 2nd, and vice versa. After the process, the transmission and the reception are inverted. In this turn, A receives the signal from B while the receiving antenna is switched. After receiving, the two received signal levels are compared to generate a bit in the same way as in receiving at B. When the two-way propagation characteristics are identical, the results of the comparisons at A and B have to be the same. By repeating the process sufficiently, correlated information is shared between A and B. On the other hand, for an eavesdropper located at a different place, since the propagation characteristics are different due to the low spatial correlation of the multipath fading channel, the obtained bit sequence is independent of that from A to B. Note that, in the above procedure, the sequence for selection of the antennas, 1 to 2 or 2 to 1, should be random. By using a random selection, the resultant bit sequence is randomized even in a slow fading environment.

As in the key agreement scheme using the ESPAR antenna, the agreement probability can be improved by data deletion and the error correction methods.

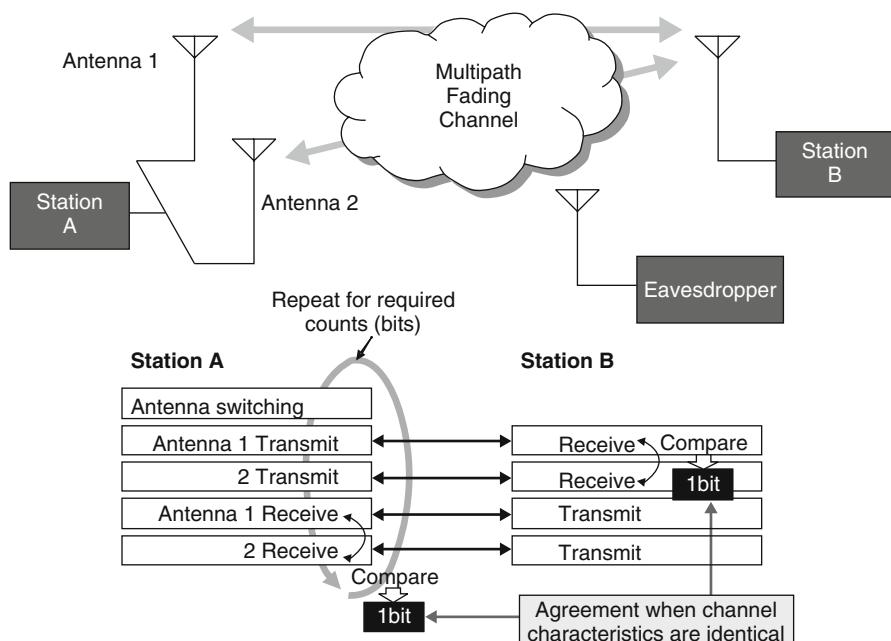


Fig. 11.12 An outline of the concept of secret key agreement scheme using antenna switching

11.2.4 Secret Key Agreement Scheme by Impulse Response Measured by UWB-IR Signal

Impulse Radio has been considered as a transmission technique for Ultra Wideband systems (UWB-IR). In this technique, a pulse signal having ultra-short time width is used for the radio communication. By utilizing the short pulse, it is easily possible to obtain the impulse response of the propagation channel. We use the response as the common source for the secret key between the two legitimate users.

Figure 11.13 shows an example of a simulated impulse response for an UWB-IR systems. A Gaussian mono-cycle pulse is assumed and the time width of the pulse is 0.5 nsec. The simulated area is an indoor environment and the propagation characteristics are obtained by ray-tracing. It can be seen from the figure that multiple delay peaks are detected. To generate a key from the impulse response, we consider a method where the maximum three peaks are selected and the differences between them (the difference between the 1st and the 2nd, and the difference between the 2nd and the 3rd) are used to generate a key sequence. The two delay differences are binarized by expressing them as binary numbers [13]. However, through quantitative analyses via computer simulations, it has been shown that, when the difference of the multiple peaks is small, the key agreement performance degrades due to the noise. To address this problem, an improved method is developed in [14]. In this method, at one of the two stations, the largest 3 peaks are first selected and the differences of the peaks are binarized in the same way as the original method to generate a binary sequence. Then the syndrome of the generated binary sequence is calculated and it is transmitted to the other terminal over a public channel. At the other station, the largest 5 peaks are detected from the received impulse response. The syndromes corresponding to all possible combinations of the 3 peaks from the 5 are examined and the best agreement is selected to be the candidate of the key sequence. Figure 11.14 presents the key disagreement characteristics versus SNR variation assuming

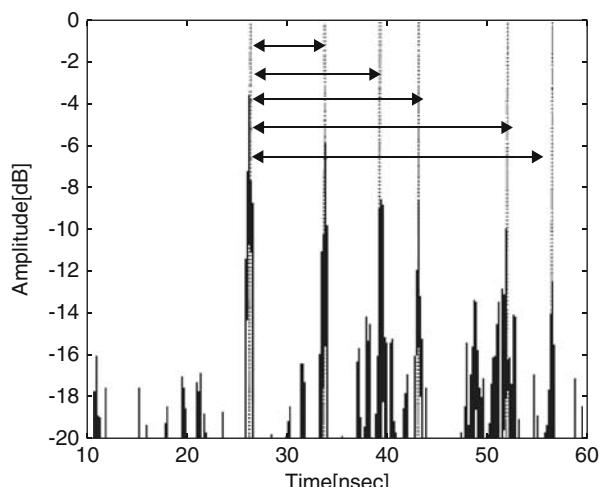


Fig. 11.13 An example of an impulse response corresponding to an UWB signal

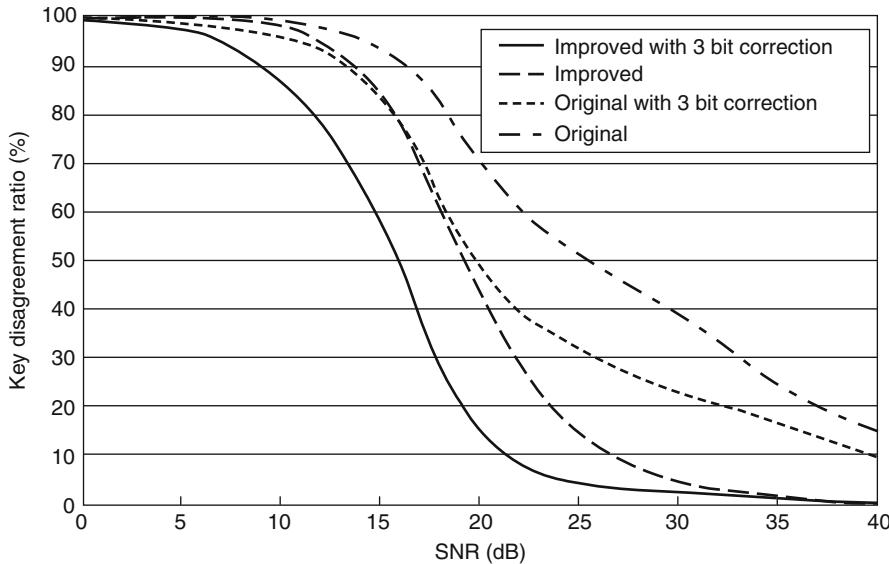


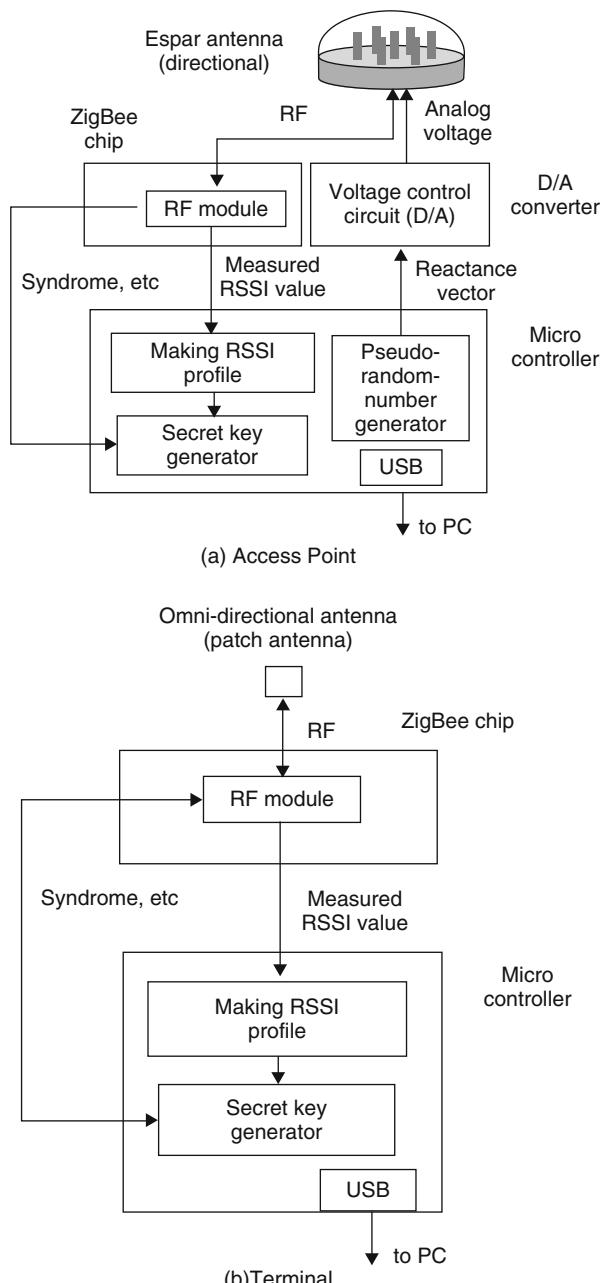
Fig. 11.14 Key disagreement performance versus SNR

the key length is 128. In the figure, the original corresponds to the method where 3 peaks are detected and used to generate key sequences at the both stations. The performance of the improved method where 5 peaks are used at a station is enhanced. The performance when error correction is applied to both the original and improved methods is presented also in the figure. The error correction scheme applied to calculate the performance in the simulation has the ability to correct up to 3 error bits. It can be seen from the figure that the disagreement ratio is very small when the two techniques are combined. The error correction capability, 3 bits among 128, is relatively small. However, because by the improved scheme the number of the disagreement bits decreases to a significantly small amount, such a light error correction scheme is sufficiently effective to assure agreement of the two key sequences.

11.3 Prototype Systems of Secret Key Agreement Scheme Using ESPAR Antenna

To examine the feasibility of the schemes described, prototype hardware has been developed. The hardware is based on the scheme using the ESPAR antenna. The block diagrams for the access point and the terminal are presented in Fig. 11.15. As the underlying radio system, ZigBee has been adopted. The specifications of the ZigBee chipset used in the prototype hardware are summarized in Table 11.1. The hardware of the access point consists of three parts. In the micro-controller, a random sequence is generated to vary the directional pattern of the ESPAR antenna. The sequence is converted to a combination of analog voltage (=reactance vector) at

Fig. 11.15 Block diagrams for the prototype system



the D/A converter to feed to the varactor diodes of the parasitic elements. The ZigBee chipset used in the hardware has an output port where RSSI values are available. The micro-controller uses the values to generate the secret key sequence. The terminal hardware is relatively simple in comparison with that of the access point since it does

Table 11.1 Radio communication specifications for the ZigBee chipset used in the system prototype

Radio frequency	2.4 GHz
Transmission power	1mW (0 dBm)
Data modulation	Offset-QPSK
Data rate	250 kbps
Spread spectrum system	Direct Sequence
Spreading chip rate	2 Mchips/s

not need the variation of the antenna pattern. The external view of the access point and the terminal is presented in Fig. 11.16.

Both pieces of hardware have a USB interface for connection to PCs. The interface is utilized to output the generated secret key to the PC where the key is graphically displayed on the screen for demonstration purposes. In Fig. 11.17, a view of an experiment is shown as an example. The scenario for the experiment, which is conceptually shown in Fig. 11.18, is as follows: Two legitimate users (as an access point and a user terminal) try to realize agreement of a 128 bit key sequence. In the data deletion process to improve the key agreement, 256 RSSI values are eliminated. Thus we measured 384 RSSI samples when constructing the original sequence. Additionally, an eavesdropper, which has the identical hardware and software to those of the legitimate user terminal, attempts to steal the key.

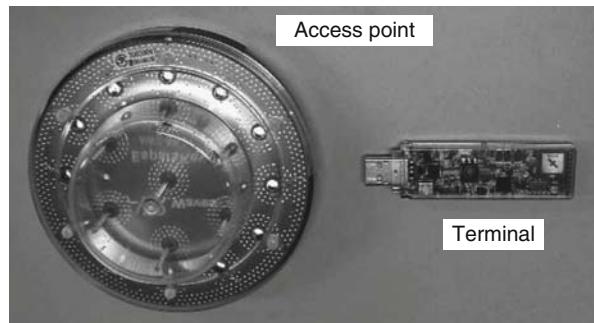


Fig. 11.16 External view of prototype hardware

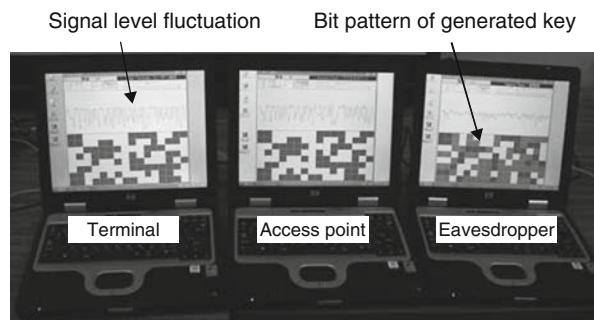
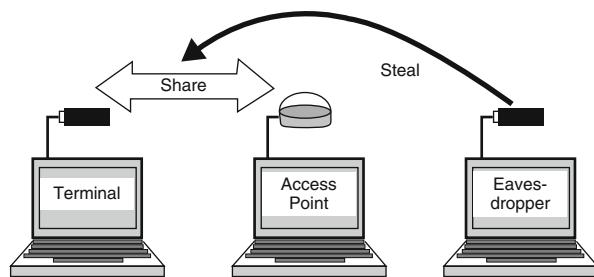


Fig. 11.17 A typical run illustrating the formation of a shared key between two legitimate users, as well as what an eavesdropper would witness

Fig. 11.18 Experimental scenario



As seen in Fig. 11.17, on the display of the host PCs the signal level fluctuations and the bit patterns of the generated keys are displayed. It can be seen from the figure that the two keys remotely generated at the access point and the terminal perfectly agree, whereas the key at the eavesdropper has significant disagreement.

Figure 11.19 shows the distributions for the number of the disagreement bits among 128 bits of the shared key. This is an experimental result obtained in an office room. The room is 8.4 m by 6.7 m and is surrounded by metal and concrete walls. The access point is set at the center of the room and the positions of the terminal and the eavesdropper are varied arbitrarily in the room. The upper panel of the figure is the disagreement bit distribution between the key sequences at the access point and the terminal. In most cases, the disagreement is zero or very small. The lower panel presents the disagreement distribution between the user terminal and the eavesdropper. The distribution is spread almost symmetrically around the

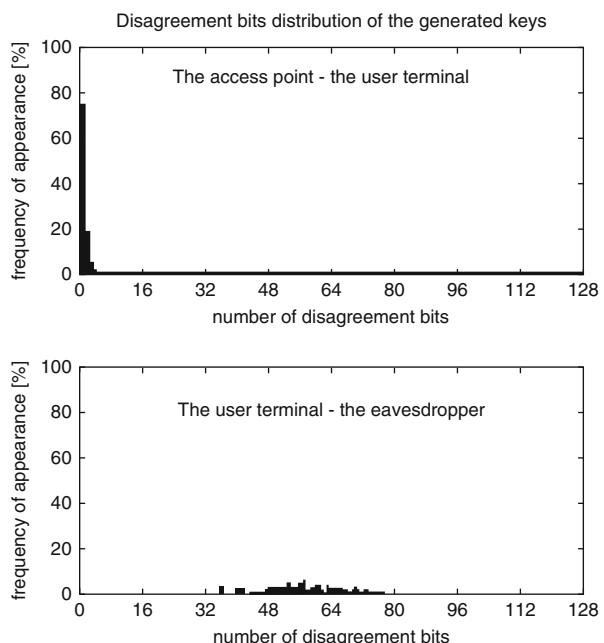


Fig. 11.19 Distribution for the amount of bits in disagreement

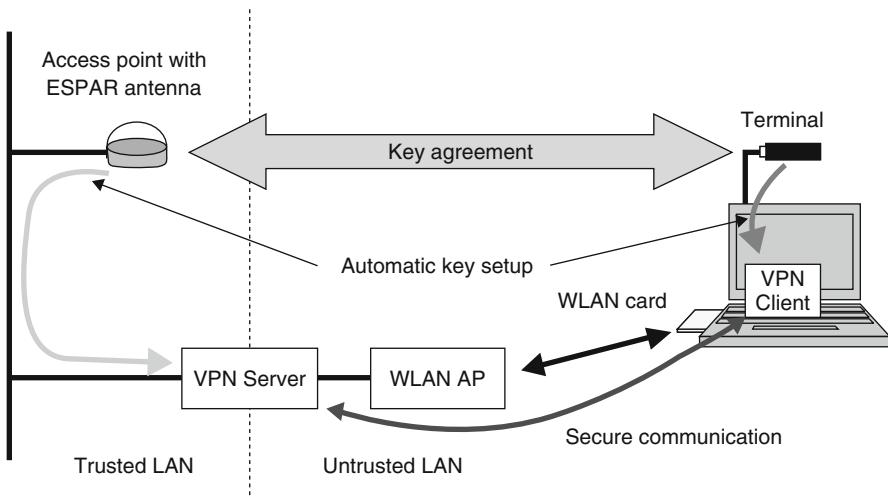


Fig. 11.20 Secret communication network system using secret key agreement

value 64, which corresponds to half of the total bits being established. As the results show, the sequence measured by the eavesdropper is uncorrelated with that of the user terminal.

As one way to use the key in actual confidential communication, we developed a secret communication network system where a generated shared key is used as the password for an IPSec-based VPN (virtual private network) system. A schematic view for the network is presented in Fig. 11.20. A key is shared between the access point and the terminal of the ESPAR antenna key agreement system. At the access point side, the secret key is automatically sent to a VPN server through a trusted wired network and the key is set as the login-password for accepting the client at the VPN server. At the client side the shared key is transferred through the USB interface to the PC and the secret key is set as the password for login to the VPN network. After the VPN connection is successfully set up by using the secret key as the password, IPSec ensures that secure communication can be done even on open WLAN channels.

11.4 Conclusions

In this chapter, a secret key agreement scheme utilizing radio propagation has been introduced. The principle is described and actual realization techniques of the principle are also presented. The schemes utilize the high correlation of the propagation characteristics of a two-way radio communication channel to remotely share a common key. The schemes also utilize the locality of the multipath fading process to decrease the correlation that an eavesdropper may have with the legitimate key establishment process. To obtain desirable correlation properties, various techniques exist

and the best choice among them will vary from system to system. Nevertheless, these techniques are an essential means to practically establishing and guaranteeing the fluctuations needed to establish secret keys, even for scenarios where the underlying fading process does not have significant spatial, temporal or frequency variability.

References

- [1] H. Yamamoto, “Information theory of cryptology,” *IEICE Transactions*, vol. E74, pp. 2456–2464, 1991.
- [2] H. Imai, G. Hanaoka, J. Shikata, A. Otsuka, and A. C. Nascimento, “Cryptography with information theoretic security,” in *Proceedings of the 2002 IEEE Information Theory Workshop*, p. 73, 2002.
- [3] P. Tuyls, B. Skoric, and T. Kevenaar (editors), *Security with noisy data—On private biometrics, secure key storage and anti-counterfeiting*, Springer Verlag, 2007.
- [4] C. E. Shannon, “Communication theory of secrecy system,” *Bell System Technical Journal*, vol. 28, pp. 565–715, 1949.
- [5] A. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [6] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [7] C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computer System and Signal Processing*, pp. 174–179, 1984.
- [8] J. Hershey, A. Hassan, and R. Yarlagadda, “Unconventional cryptographic keying variable management,” *IEEE Transactions on Communications*, vol. 43, pp. 3–6, 1995.
- [9] A. Hassan, W. Stark, J. Hershey, and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” *Digital Signal Processing*, vol. 6, pp. 207–212, 1996.
- [10] H. Koorapaty, A. Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” *IEEE Communications Letters*, vol. 4, pp. 52–55, 2000.
- [11] A. Kitaura and H. Sasaoka, “A scheme of private key agreement based on the channel characteristics in OFDM land mobile radio,” *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 88, pp. 1–10, 2004.
- [12] A. Kitaura, T. Sumi, K. Tachibana, H. Iwai, and H. Sasaoka, “A scheme of private key agreement based on delay profiles in the UWB system,” in *Proceedings of the IEEE Sarnoff Symposium 2006*, 2006.
- [13] A. Kitaura, T. Sumi, T. Tango, H. Iwai, and H. Sasaoka, “A private key sharing scheme based on multipath time delay in UWB systems,” in *Proceedings of International Conference on Communication Technology 2006 (ICCT'06)*, pp. 1–4, 2006.
- [14] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.
- [15] T. Ohira, “ESPARSKI: Encryption scheme parasite array radiator secret key implementation,” in *IEEE International Conference on Microwave Radar Wireless Communications (MIKON2006)*, pp. 1065–1070, 2006.
- [16] W. C. Jakes Jr., *Microwave Mobile Communications*, Piscataway, NJ: Wiley-IEEE Press, 1994.
- [17] Y. Karasawa and H. Iwai, “Modeling of spatial envelope correlation on line-of-sight fading with applications to frequency correlation analysis,” *IEEE Transactions on Antennas and Propagation*, vol. 42, no. 6, pp. 2201–2203, 1994.

Chapter 12

Secret Communication over Fading Channels*

B. Azimi-Sadjadi, A. Kiayias, A. Mercado and B. Yener

12.1 Secret Communication Over Fading Channels

The broadcast nature of any wireless communication network provides a natural eavesdropping and intervention capability to an adversary. Anyone with a tuned receiver within a radius that permits adequate signal to interference and noise ratio (SINR) may *eavesdrop*. Thus, effecting efficient key generation and renewal algorithms to ensure confidentiality, integrity, and authentication for every wireless link is essential for impenetrability. Yet, most wireless network systems are already burdened with heavy overhead, encroaching into the extremely precious bandwidth resources (e.g., 802.11 [1, 2] and 802.16 [3]).

Hence, it is desirable to find any way to curtail such overhead wherever possible, and one source of overhead is the interchange necessary to secure the communication link, either between two communicating nodes, or from any node to the public key infrastructure (PKI) support. Conventional key agreement algorithms can be very costly in a setting where bandwidth and oftentimes battery expenditure are at a premium. This chapter addresses approaches that couple the wireless physical layer, the unique variations of the electromagnetic signal experienced in a wireless channel in particular, with key generation algorithms.

The intent here is to exploit the random nature of the radio frequency (RF) channel for our own purposes. This stochastic characteristic manifests itself in the received signal's delay, its envelope (i.e., the outer boundary of the received amplitude),

B. Azimi-Sadjadi (✉)
Intelligent Automation Inc.
15400 Calhoun Drive, Suite 400 Rockville
MD 20855, USA
e-mail: babak@i-a-i.com

*This work is based on an earlier work “Robust Key Generation from Signal Envelopes in Wireless Networks,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ©ACM, 2007. <http://doi.acm.org/10.1145/1315245.1315295>

This work was done in part while the author was with Rensselaer Polytechnic Institute.

and its phase.¹ The broadcast signal is at places obstructed by objects, at other places reflected off of surfaces, arriving at the destination after traversing different path lengths and experiencing attenuation and phase changes, and in other places diffracted (skimming off the edges of obstructions) producing a scattering of constructive and destructive superposition of the wave. The attenuation experienced by each reflected signal depends on the reflective coefficient of its reflector as well as the overall length of the path it traverses.

The receiver's antenna will perceive the collection of all of these *multi-path* in all their richness of delays, and amplitude and phase distortions, resulting in a combined signal whose magnitude varies randomly. We will see how we can model this random behavior, and how to utilize its properties.

So, how do we mean to exploit this seemingly unruly behavior to our advantage? Many of the techniques seen here are based on the wireless communication phenomenon known as the *principle of reciprocity* which states that, in the absence of interference, both transmitter and receiver experience the *same signal envelope* at the same time. This can be reasoned by the fact that the trajectory of any given multi-path can be traversed in both directions, therefore, all distortions experienced on one side of the communication link will be (almost literally) mirrored on the other side of the link.

In practice the impact of interference cannot be ignored since it is ever-present in all wireless networks, and its presence negates strict reciprocity. Yet, we may still rely on a more relaxed reciprocity, which preserves some aspects of the fading channel for both transceivers. This chapter culminates with an approach that is robust to interference for generating secret keys, since it is based on extracting correlated bit strings for both transceivers by detecting the *deep fades*—destructive combinations of multi-path signals, making the signal vanish for an instant—which are preserved even in the presence of interference.

The key-observation here is that the signal envelope information can provide the two transceivers two correlated random sources, unique to the fading environment experienced by the link between the two of them.

Moreover, in practical settings, it can be quite difficult for an observer which is not located at either transceivers' position to know, predict, or even hazard an educated guess of the exact envelopes perceived by the two legitimate transceivers. Any outsider attempting to recreate this fading environment would have to know to very high resolution the relative three-dimensional positions and speeds of the transceivers, the number, position, and angles of reflective, shadowing and refractive surfaces (some of which may be non-stationary, such as a passing truck), and the reflective coefficients of each reflector's surface material, in order to calculate the attenuation. Then they would have to engage in painstaking ray-tracing, all culminating in a work overhead of potentially excruciating proportions.

¹The received signal's frequency can also be said to have some stochastic component due to Doppler as well as oscillator inaccuracies, but this component is not considered here appreciable enough for our purposes.

In most natural settings, this wireless channel will be decidedly non-stationary in nature, as any field technician will readily attest. Indeed, an enlightening anecdote comes to mind where a team member of a wireless project presented the findings of his measurement campaign to his colleagues, among whom was this author; the way he did so was to project two side-by-side signal strength plots on the screen: one was of the collected data and the other were points generated completely at random. He then defied his listeners to discern which one as which. He made his point beautifully.

Due to the richness of the sources of multi-path, the signal envelope will usually experience a startling number of unpredictable variations even within arm's length of a given location, and will at times experience a changing signal strength in the very same spot. These substantial changes in the shared envelope allow for sufficient amounts of entropy that can potentially be used to extract a sequence of cryptographic keys.

This chapter will show how the two communication ends can reconcile such bit strings and finally flatten their distribution to reach key agreement. In these constructions we use cryptographic tools related to randomness extraction and information reconciliation. We later introduce “secure fuzzy information reconciliators,” a tool that enables the description of robust key generation systems in this setting. Finally, the chapter provides a study that presents a simulation of a wireless channel that demonstrates the feasibility of this approach and justifies the assumptions made here.

12.2 Background

Spectrum resources, such as frequency channels or spreading codes, are an extremely limited resource. Therefore, communications link designers must strive to minimize the overhead associated with the establishment, management, and termination of a communication channel.

Particularly since any security system will require repeated authentication, and other intrusion or eavesdropping avoidance techniques, it befalls the system operation to employ such techniques as would require the minimum possible exchanges, occupying the least bandwidth to accomplish the desired task.

Given this premise, the question arises if there is any element of the wireless channel itself which can be exploited to remove—at least reduce—the associated overhead communication burden between two terminals.

Currently, there is no widely available algorithm to achieve key generation and renewal *without exchanging messages* and withstand the pernicious effects of interference, not to mention, investing great computational cost. For example, the Diffie-Hellman key exchange protocol [4] can be costly for the limited resources of an ad-hoc node in terms of computation and bandwidth due to the fact that the underlying algebraic operations required have high complexity (e.g., modular exponentiation over modular groups, or scalar multiplication over elliptic curves).

Most of the techniques we'll survey exploit the *reciprocity principle* of wireless communications. We remind the reader of this principle: two transmitters working

with the same carrier frequency, in the absence of interference (we relax this later) will experience *the same (relative) signal strength from each other at the same time*.

But in order to fully understand how to use this principle, we first present a brief overview of the physical channel characteristics. The following section provides a brief overview of the typical wireless channel experienced by two ground terminals: the multi-path fading channel.

12.2.1 Multi-Path Fading Channel

In a wireless environment, the received signal suffers degradation due to a variety of effects, such as mean propagation pathloss, slow fading, fast fading, interference from other users' signals, thermal noise, and distortion due to nonlinearities of the inherent receiver hardware.

Since some of these sources of distortion are often confused and mistakenly interchanged, we take a moment to review them here. First, we broadly group the sources of distortion as those caused at the receiver itself, and those originating outside of the desired receiver. The former, which is the *noise*, is most oftentimes modeled as an uncorrelated Gaussian random process, which is added to the incoming signal received over the airwaves. The rest form part of the latter, and it includes unintended *interference from other users* who share the desired user's spectrum; this arrives to the antenna over the airwaves along with the desired signal, and though this is also added to the desired signal, it is not always modeled as an uncorrelated Gaussian process—unless the number of interferers is so enormous that we may apply the Central Limit Theorem, or if we are dealing with a Code-Division-Multiple-Access (CDMA) system.

From the remaining sources of external distortion, we further distinguish *path-loss* from *fading*. The former is the attenuation due to the distance from the transmitter to the receiver. There are a number of empirical, semi-empirical, and deterministic models for signal path-loss, which depend on the carrier frequency, the environment of the transceivers, and their respective antenna heights. A popular collection of path-loss models are depicted in Fig. 12.1a. Note that, if the receiver were to travel in a circle around the transmitter, assuming the setting remained say suburban, then the path-loss is not expected to change. Conversely, *fading* has nothing to do with the distance from the transmitter, and may often change dramatically even though the receiver remains perfectly still.

It is this last form of distortion, *fading*, which we exploit for security key generation.

These effects will generally depend on the frequency, the location, direction, and reflecting coefficients of the surrounding objects. The unpredictability of these elements, the fact that they often uncontrollably change, and that oftentimes the terminal itself is moving, and causing the incident angles of itself with respect to reflectors to change requires us to model such a channel as a stochastic process—and most often, a non-stationary process.

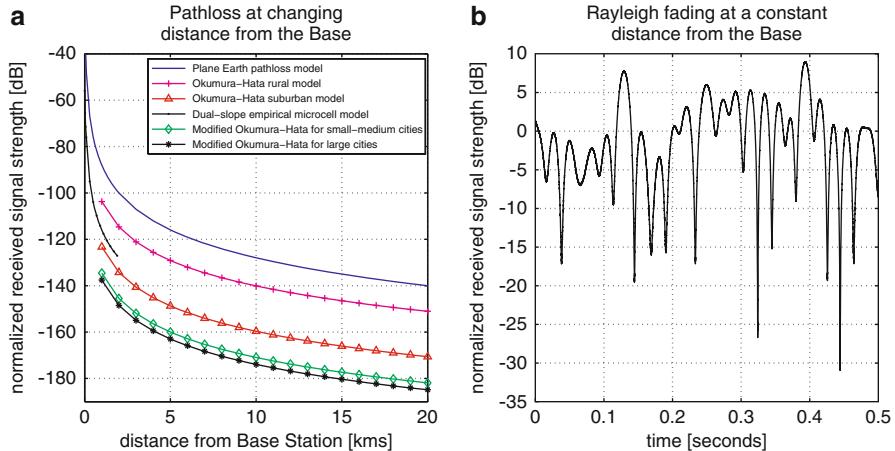


Fig. 12.1 **a** The Plane Earth model is the result of a direct path of propagation and one ground-reflected path. It serves well for very small distances between transceivers, but is too optimistic for most applications beyond that. The Okumura-Hata model [5] is perhaps the most used empirical macro-cell model for path-loss for VHF, UHF, and low microwave frequencies. For urban settings where the transceiver distances are expected to remain below one kilometer, the urban micro-cell model is better suited. **b** The frequency of deep fades in a fast fading environment will depend on the Doppler spread of the channel [6]

12.2.2 Frequency Selectivity of Channels

The next question is how we mathematically represent the fading characteristics of a wireless channel. In this section, we summarize the basic measures with which we describe the fading characteristics of a channel, namely its *coherence time* and its *coherence bandwidth*.

Consider a slowly fading channel, that is, the channel attenuation and phase shift is roughly constant over the time required to transmit a symbol, T_b , called the signaling interval. This is true when the signaling interval is assumed to be much smaller than the coherence time, $T_b \ll \Delta t_h$ [7], where we define the coherence time, Δt_h , as the time interval over which there is positive correlation between the channels experienced by two transmitted signals.

In other words, the coherence time is a measure of how slowly the channel response changes. Let $h(\tau, t)$ be the time-varying, delay dependent channel impulse response, so $h(\tau, t)$ is the channel response at time t for an impulse applied at time $t - \tau$, and we assume this function is wide-sense stationary. The autocorrelation function of $h(\tau, t)$ is then defined as

$$\phi_h(\tau_1, \tau_2, \Delta t) = \frac{1}{2} E\{h(\tau_1, t)^* h(\tau_2, t + \Delta t)\}. \quad (12.1)$$

Here, the asterisk denotes the complex conjugate. We assume that the channel attenuation and phase shifts for different multi-path signals are uncorrelated, and

that the impulse response is complex-valued and zero-mean. So, $\phi_h(\tau_1, \tau_2, \Delta t) = \phi_h(\tau_1, \Delta t)\delta(\tau_1 - \tau_2)$, which yields the average power output as a function of time delay and the difference in observation time, Δt . The range of time over which $\phi_h(\tau, 0)$ is essentially non-zero is called the *multi-path spread*, T_m .

Assume that $h(\tau, t)$ is a complex-valued zero-mean Gaussian random process, in the variable t . If we take the Fourier transform of $h(\tau, t)$ with respect to τ , we obtain $H(f, t) = \int_{-\infty}^{\infty} h(\tau, t)e^{-j2\pi f\tau} d\tau$. It can be shown that the autocorrelation function of $H(f, t)$ with respect to f is, in fact, the Fourier transform of $\phi_h(\tau, \Delta t)$ in the τ variable. Since we assume uncorrelated scattering, then the autocorrelation of $H(f, t), \phi_H(\Delta f, \Delta t)$, depends on Δf , instead of f_1 and f_2 , [7].

Again set the observation time, Δt , to zero, and denote the frequency range for which $\phi_H(\Delta f, 0)$ is essentially non-zero as Δf_h . Then $\phi_H(\Delta f, 0)$ yields a measure of the *frequency coherence* of the channel. In other words, just as T_m denotes the largest time separation between multi-paths so they are still somewhat correlated, so also Δf_h denotes the largest frequency difference between two sinusoids so that they are still somewhat correlated. Because of the Fourier transform relationship between $\phi_H(\Delta f, 0)$ and $\phi_h(\tau, 0)$, we may relate the multi-path spread to Δf_h , which we will call the *coherence bandwidth*, with

$$\Delta f_h \approx \frac{1}{T_m}. \quad (12.2)$$

If Δf_h is small with respect to the bandwidth of the transmitted signal, then the channel is called a *frequency selective channel*. In this case, different portions of the spectrum of the signal will suffer distinct distortion. If Δf_h is large with respect to the bandwidth of the transmitted signal, then the channel is called a *frequency non-selective channel*.

Our attention is limited to all the multi-path that collectively arrive within one symbol period, and the rest may be considered as inter-symbol interference (ISI).

12.2.3 Principle of Reciprocity

In practice, the presence of interference cannot be neglected in a wireless network and the reciprocity principle does not strictly apply. Yet the techniques presented here do not require identical signal envelopes for both parties, but only *matching deep fades*, which are impervious to reasonable levels of interference, i.e., SINR.

By reasonable levels of SINR, we mean SINR levels that allow the communication link to have acceptable bit error rate (BER). We note that the acceptable SINR depends on the specific modulation technique.

For example, if the target symbol error rate (SER) is 10^{-5} then for PSK modulation we require the SINR to be about 24 dB for a typical Rayleigh channel (i.e., the received signal power is 24 dB stronger than the combined receiver noise and perceived ambient interference). This means that the deep fades that can be measured go as far as -24 dB deep (that is, when the receiver predominantly perceives noise plus interference, the desired signal having dropped below those two). The modulation technique QAM 64 (that provides higher rates at the expense of greater sensitivity to noise,) will require an SINR of about 33 dB for the same SER.

Therefore, detecting the deep fade even in the presence of noise and interference is possible. *This robustness is one of the strengths of our approach.* A channel where deep fades might be affected by interfering nodes would experience an inordinately low average SINR, and could not function properly as a communication channel anyway. Therefore, in practical systems, where average SINR levels are adequate for communication with acceptable bit error rates (BER), both transmitter and receiver experience the same deep fades.

As we've discussed, in a typical environment, reflective surfaces vary from moment to moment: a truck may be passing by a window, a reflective surface may tilt removing or adding multi-path, or the network node itself may be in a moving vehicle. Hence the fading characteristics are, in practice, very difficult to predict. However, whatever realization of that process occurs for a network receiver, the signal it sends back to its counterpart will experience the same realization of that fading at that instant. Note also that the phase differences of the arriving multi-paths are quite sensitive to the position. For example, for a carrier of 850 MHz, the wavelength is about a foot long, thus constructive interference (signal high) may change to destructive interference (deep fade) by shifting a mere half a foot. Thus, *a transceiver acting as an eavesdropper, in any other position will experience different fading characteristics.*

Measurements have verified that the received signal at a location other than the legitimate users is relatively uncorrelated to the signal received in any other location. Pragmatically, the only way for an eavesdropper to measure the same deep fade is by attaching itself to one of the legitimate nodes.

Figure 12.2 demonstrates the reciprocity measurement using two Ultra Wide Band (UWB) transceivers. As depicted in Fig. 12.2, two transmitters experience the same (relative) signal strength, and the received signals at the receivers are highly correlated. Also it is clear from the figure that the eavesdropper's received signal has very little correlation with the received signal in the legitimate receivers. By passing the UWB signal through a filter with the bandwidth of the channel we get two signals (at both legitimate receivers). These two signals will have a deep fade at the same time instance.

As we can expect, the same phenomenon occurs when the measurements are done in the frequency domain, since the frequency domain measurement is the dual of time domain measurement, cf. Fig. 12.3. The measurements are done at both legitimate receivers. As can be seen from the measured frequency response, the deep fades occur at the same frequency. The reason that some of the deep fades do not match in this figure is because the measurements are not done at exactly the same time (transceivers cannot transmit and receive simultaneously, but must allow for a small delay). So the change in environment appears in the measurement.

Our thesis is that these fading graphs, as the one depicted in Fig. 12.4, can be used to generate cryptographic keys, and the non-stationary nature of a typical wireless network can be used to our benefit by bringing the entropy of such keys to substantial levels for use in cryptographic applications. Moreover by continuously exploiting these characteristics, we can generate a sequence of keys (key renewal) so that even if the adversary were to eventually retrieve a key, by the time it

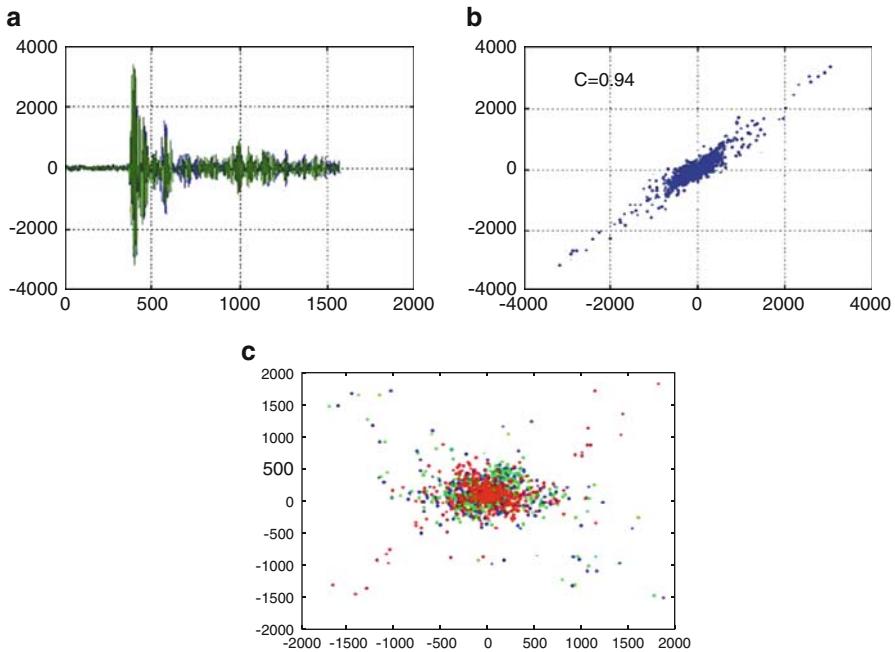


Fig. 12.2 **a** Signal received by radio 1 (blue), and radio 2 (green) vs. time. Vertical axis: proportional to voltage on antenna. Horizontal axis: time in units of 36ps. **b** Signal from radio 1 vs. signal from radio 2. The small deviations from a line through $(0,0)$ with unit slope are caused by: (1) operator moving during data acquisition, and (2) Small differences between the radios. The signals are highly correlated, with a correlation coefficient of 0.94. **c** same as center **b**, but with one of the radios moved to another room 20 ft away. We compare the second data set with one of previous sets. The multipath has changed dramatically, and only random correlations are left ($C = 0.1$) Thus **eavesdropping will be virtually impossible** for an adversary unless it comes very close to the sender or receiver, but then it will be detectable

had it, the two legitimate nodes would have already abandoned the compromised key as out-dated. Furthermore, once the first key is securely obtained, such properties can be used to ensure authenticity, and prevent man-in-the-middle and replay attacks.

A typical mobile node is expected to sporadically remain stationary, perhaps even surrounded by a stationary environment. However, in the vast majority of practical cases, the channel between the nodes will be non-stationary, and vary enough to produce new keys. Yet, if a situation should arise when both legitimate nodes stop moving and the environment around both nodes freezes, then the algorithm may employ the frequency domain measurement technique as mentioned above, where the same type of deep fade phenomenon is observed. For example, for wide-band channels, a narrow-band filter sliding along the signal bandwidth will generate a sequence of distinct keys that can each be used in turn. The number of keys that can be created while the channel is thus stationary depends on the signal bandwidth and coherence frequency of the channel; however, this method is not designed for the case where both nodes and their respective environments become permanently stationary.

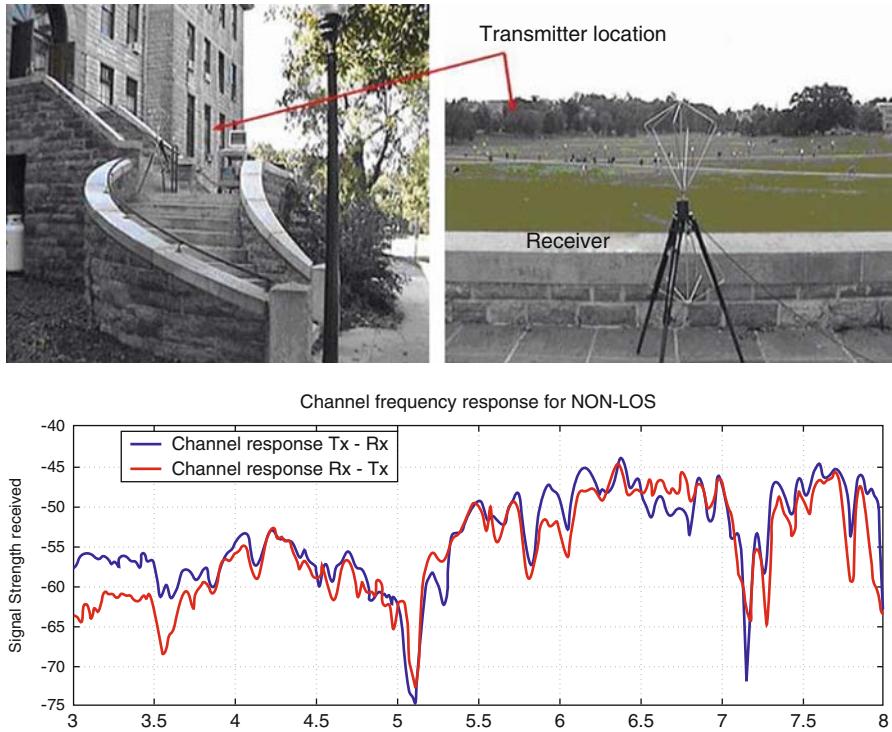


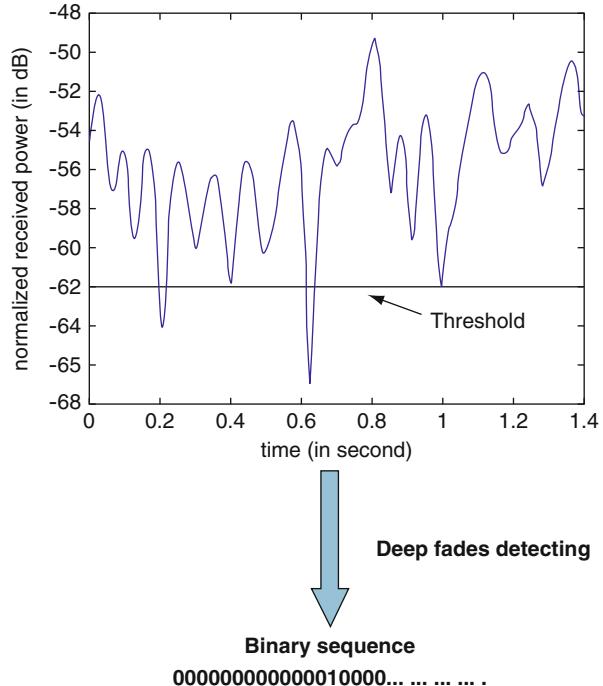
Fig. 12.3 LOS measurement terrain. The channel power spectrum is reasonably flat with 2 null positions. The response is reciprocal

Given the above, in this work, we tackle the challenges of (i) error reconciliation between the correlated random sources that are available to the two transceivers, (ii) flattening of the key distribution for the purpose of extracting a high quality key. Our methods partly rely on the classic by now results of privacy amplification and information reconciliation that originated in solving the quantum key-exchange problem. As part of our study we focus on the primitive of secure fuzzy information reconciliators we introduce as a building block for our key exchange system. Contrary to the physical requirements of systems such as a quantum key exchange we note that no special or added hardware beyond threshold detectors—which are already present in transceivers—is required, and the nodes use cheap and common omnidirectional antennae, and do not require smart antennae, or arrays.

12.2.4 Current Work in This Area

Security in wireless networks depends on efficient key management schemes [8]. There is no one-size-fits-all solution for all wireless networks (refer to [9] for a detailed survey). The proposed solutions depend on the network architecture, existence

Fig. 12.4 Channel envelope and reciprocity: the normalized channel envelope will be the same for both sender and receiver, for the same frequency and in the absence of interference



of trusted third parties, available resources on wireless clients and the capabilities of adversaries.

In ad-hoc wireless networks where there is no infrastructure and the network configuration may be dynamic (due to mobility or failures), the general approach is to equip each node with either (i) a master key, or (ii) a list of keys (a key-chain), or (iii) keying materials; so that a pair of wireless nodes can either find a key in common, or generate it. In master key based solutions [10, 11], wireless nodes are pre-distributed a master key. Two nodes first exchange random nonce or node ID and use the master key along with a pseudo random function to generate a symmetric session key. In key-chain based solutions, each wireless node is pre-distributed a list of keys, called a key-chain. Two nodes just exchange their list of key IDs and use the combination of common keys as the symmetric session key. Key-chains must be carefully designed so that either two nodes have a key in common in their key-chains and they have a wireless link between them, or there is a path, called a key-path, among these two nodes where each pair of neighboring nodes on this path have a key in common.

Key pre-distribution approaches are outside the scope of this work, since they are not pertinent to our scheme. Algorithms to generate the key-chains fall into one of the three classes: (i) probabilistic [12, 13] where key-chains, are randomly selected among a pool of keys, (ii) deterministic where key chains are designed from a set of keys by using algorithms such as Balanced Incomplete Block Design (BIBD) of design theory [14–16] and (iii) hybrid probabilistic and deterministic schemes [14].

In dynamic key generation solutions a set of public and private keying materials is formed in a probabilistic, deterministic or hybrid manner and is pre-distributed to each wireless node. Two nodes exchange their public information such as node ID and then derive a key based on the private data, e.g., taking advantage of an algebraic structure using polynomials [17] or matrices [18].

Using narrow antenna beams, either due to narrow antenna gain patterns or due to smart antennae has been addressed before, for example in [19]. However, this does not combine privacy with key management or encryption. Furthermore, if the link is long enough (in distance) then an adversary may position himself anywhere along the transmission direction, and the directionality provides no protection. Furthermore, directional antennas and antenna arrays usually provide a *low gain* in undesired directions, but oftentimes the signal is still quite clear even as far as a couple of blocks away, depending on the effective radiated power (ERP) being used.

The concept of combining key management and physical layer characteristics is first presented in [20]. More recently (independently from our research) in [21] which uses steerable parasitic array radiator antennae in contrast with our method that requires only ubiquitous and cheap omnidirectional antennae. Furthermore, their method relies on strict reciprocity, with no more distortion than noise and differences in transmission powers. In a real network, the most pernicious presence causing distortion is interference, not noise, which is often orders of magnitude lower than interference. This breaks down reciprocity, which is why our method addresses this problem by focusing on the deep fades, rather than the entire envelope. In [22] communication between an Access Point and a User Terminal is considered. This approach requires also steerable parasitic array radiator antennae. In addition to the special antenna, that technique requires overhead bandwidth expenditure in that the Access Point must transmit a constant amplitude wave, which serves no purpose other than generating the key. Once again, strict reciprocity is required for the uplink and downlink signal profiles to match. In a practical setting with interference present, that simply won't be available. Another method which is based on the time-varying frequency characteristics, and is suitable for OFDM systems is proposed in [23]. It utilizes channel reciprocity and the time-variant frequency characteristics to generate a security key. It also measures time difference compensation of the channel and uses a synchronous addition process for noise reduction to prevent errors in key generation, which is different from ours. In comparison, our approach is much more inexpensive and less sensitive to estimation errors. In conclusion, we emphasize that the approach we promote here reduces message exchanges, eliminates the need for special antennas and removes strict reciprocity assumptions.

Our approach takes advantage of cryptographic tools that relate to randomness extractors, [24, 25] and fuzzy extractors [26]. Key agreement in our work targets the setting where the two parties that wish to exchange a key have access to two correlated random sources (the deep fade information derived from the channel envelope) while the adversary has only partial access to this source. Key agreement with restricted adversaries has been studied in the works of Bennett et al. [27], Maurer [28], Maurer and Wolf [29], Holenstein and Renner [30] under minimum entropy assumptions and specific restrictions imposed on the correlation of the two sources (e.g., agreement with high probability); non formal approaches appeared much earlier [31] and [32].

Our work differs from these previous works since we are using the specifics of our setting and we thus we need to constantly error-correct as well as flatten the key distribution taking into account the specifics of our channel characteristics. We note that a different line of works have studied other type of resource-bounded adversaries in terms of memory is [33, 34] (whereas the adversarial restriction in our case is knowledge of correlated random source). Our primitive of secure fuzzy information reconciliators is related (and inspired) from the work of [35]; it differs from the notion of the fuzzy extractor as it is only requires to work for a specific error type and metric (and thus it needs not the generality of a fuzzy extractor). The introduction of this primitive is helpful as we strive to loose as few bits of entropy as possible. Moreover, the metrics of similarity considered in [35] are not suitable for our methods as those are motivated from biometric key generation and do not apply to our domain. The appropriate metrics for fuzzy extraction in our domain resemble error vectors that are encountered in the setting of shift-error correction systems, see for example [36], and thus our information reconciliation strategy is suitable for such error patterns and the corresponding metric.

12.3 Sampling the Random Source

In our approach secret keys are generated periodically by detecting deep fades in the data transmission between both transceivers. Each transceiver samples its random source the signal it receives and checks to see if each sample exceeds an agreed-upon threshold for *deep fades*. Although signal envelopes of fading channels may change due to interference, the probability of detecting a false positive or missing a deep fade is low for practical systems with reasonable average SINR levels (we argue about this with simulation results in sect. 12.5). Thus, we can utilize deep fades in the received signal envelopes in Time Division Duplex (TDD) systems—which distinguish uplink and downlink messages by using different time slots—to extract some correlated random variables at the two transceivers.

We remark that we discuss the TDD system for clarification purposes only; in fact, we are not limited to the case where TDD is used, nor are we limited to the case where the Doppler frequency is positive. Even when TDD is not used or the Doppler frequency is zero, the physical layer aided key generation technique is still possible. In fact, one of the authors and his colleagues have used the onchip Receives Signal Strength Indicator (RSSI) measurement done by Chipcon 2420 which implements Zigbee (or equivalently IEEE 802.15.4) standard to generate the signal strength used for encryption. The signal strength generated in this fashion was only the RSSI measurement of the received packets and its acknowledgment counterpart.

12.3.1 Thresholding

The two transceivers will use the channel fading information to extract a bit stream (that will later be used for key generation). The bit stream is generated based on a threshold that is set by both sides of the wireless link. The statistics of the generated

bit stream and consequently the generated key depends on this threshold as well as the transmit power and the attenuation in the link. To determine this threshold an automatic gain control (AGC) mechanism can be used so that the statistics of the generated key is independent of the transmit power and the link attenuation.

Let's say that, as an experiment, we wish to get an idea for an adequate threshold from measuring a training sequence over the desired channel.

In order to experimentally estimate the average effect of slow fading for a mobile location, we subtract the pathloss and we also remove the fast fading fluctuations by averaging over distance.² With this, we have isolated the slow fading effect, and we can estimate the pathloss with a best fit estimate. Slow fading histograms derived in this way show a log-normal density function cf. [7, 37]. Assuming that this density function estimate is accurate, we can choose a security margin of, say, 3%. This means that we estimate a worst case scenario loss which is exceeded only 3% of the time. From a cumulative distribution graph, we see that this occurs at a loss of about 13 dB. So, if we wish to add a slow fading loss to our model, which is conservative 97% of the time, we would set $L_{sf} = 13$ dB.

In order to experimentally estimate the average effect of fast fading for a mobile location, we should remove the effects of pathloss by subtracting it, as we did for slow fading, and we also should remove the slow fading effect. In order to do that, a common method is to normalize the received signal to its local RMS value, by windowing the received samples: $RMS_i = (\frac{1}{W+1} \sum_{i-W/2}^{i+W/2} (r_i)^2)^{1/2}$, where W is the chosen window length. The data points normalized by the RMS value, r_i/RMS_i , are subjected to distribution fitting techniques. The size of W will affect the accuracy of the result. For conventional cell sizes, a window of four to ten wavelengths often suffices.

For a signal where there is a dominant multipath (usually the line of site path), and several weaker paths, the envelope of the fast fading is Rician distributed,

$$f_{RICE}(x) = \frac{x}{\sigma^2} e^{\frac{-x^2}{2\sigma^2}} e^{-K} I_0\left(\frac{x}{\sigma}\sqrt{2K}\right), \quad x \geq 0, \quad (12.3)$$

where $\sigma^2 = E\{x^2\}$, $I_0(\cdot)$ is the modified 0th order Bessel function of the first kind,³ and K is the Rician factor, which is an indicator of the ratio of the dominant path power to the scattered path powers. Usually, distances of about 100 m, the Rician factor is taken to be $K \geq 5$, while for greater distances of a kilometer or so, the factor is taken to be $K = 2, 3$. If in the worst case scenario there is no dominant path, $K = 0$, then the envelope is Rayleigh distributed,

$$f_{RAYLEIGH}(x) = \frac{x}{\sigma^2} e^{\frac{-x^2}{2\sigma^2}}, \quad x \geq 0. \quad (12.4)$$

As for slow fading, if we wish to determine a fast fading loss for our model which is conservative, we would check the cumulative distribution function for a value that would be exceeded only, say, 3% of the time. For $K = 4$, this occurs at a loss of about 8 dB. So, if we wish to add a fast fading loss to our model, which is conservative 97% of the time, we would set $L_{ff} = 8$ dB.

²In [6], they mention averaging over distances of 6.4 m for cellular telephony.

³The modified nth order Bessel function of the first kind is

$$I_n(x) = \sum_{j=0}^{\infty} \frac{(\frac{x}{2})^{n+2j}}{j! \Gamma(n+j+1)} x \geq 0, \quad \text{where} \quad \Gamma(y) = \int_0^{\infty} t^{y-1} e^{-t} dt, \quad y > 0.$$

The occurrence of a fade and its duration is a random process. Once the threshold is set, the average fade duration and level crossing rates depend on the channel statistics [38]. For a Rayleigh fading channel it is shown that the mean fade duration and the level crossing rates are given as follows:

$$\bar{\tau}(R) = \frac{e^{\rho^2} - 1}{\rho f_m \sqrt{2\pi}} \quad (12.5)$$

where $\rho = \frac{R}{R_{rms}}$ and f_m is the maximum Doppler frequency, R is the threshold, and R_{rms} is the RMS value of the received signal. The rate of occurrence of fades (signal crossing threshold R) is given by

$$N(R) = \sqrt{2\pi} f_m \rho e^{-\rho^2} \quad (12.6)$$

Consider the scenario where node A transmits its signal to node B while receiver C (an adversary) is listening to the same broadcast. If C is more than a wavelength away from B, then the occurrences of deep fades at B and C are independent. Therefore, the adversary cannot guess the exact moment of deep fade occurrences or their duration assuming this modeling.

12.3.2 Deep Fades to Bit Vectors

The next step after selecting a fade crossing threshold for the signal envelope is to compare the received signal envelope over each time slot with said threshold. If the envelope of the received signal is below the threshold, which means a deep fade occurred, we set a bit to 1 for this time slot. Conversely, if the envelope of received signal is above the threshold, which means no deep fade happened over this time slot, we set a bit to 0 for this time slot. After a period of time, a bit stream from each downlink and uplink channel is obtained to construct the bit vectors (BV). The bit vectors from the downlink and from the uplink channels are quite similar because they receive signals with similar characteristics due to channel reciprocity. *Although the downlink node and uplink node access the channel in different time slots, channel reciprocity results in similar channel response for both as long as the duration of each time slot is much smaller than the channel coherence time.*

One important innovation this approach is that the key generation circuit passes the received signal through a very-narrow-band filter for a narrow-band system, or through a bank of several very-narrow-band filters if the channel is frequency selective. In the former case, many narrow-band interferers are likely to be filtered out entirely. This is a very economical way for both cases to reduce the effect of interference (or even an adversary's jamming signal).

For the case of a wide-band wireless system, the technique of passing through narrow-band filters has an added advantage in that *the outputs of the collection of narrow-band filters can each be mapped to a substring in itself—which may provide additional entropy*.

12.3.3 The Random Source Characteristics

Given the above it follows that the two transceivers will be capable of retrieving two bitstrings that will have a number of “runs” (sequences of 1’s) corresponding to the deep fades they experienced in their signal envelope.

The bitstrings would be correlated due to the reciprocity principle but they will also have a number of discrepancies. For example, there will be a discrepancy at the beginning or the end of each deep fade if the deep fade lasts over a number of time slots. Another reason for bit discrepancy is because the stream in the downlink may be a slightly shifted version of the one in the uplink. Yet another reason for discrepancy is to have one of the two transceivers believing that a certain deep fade occurred over some time slots where the other transceiver has no such information (such discrepancy is due to chattering and/or other local noise conditions). We will deal with such discrepancies in two different ways: we will apply error-correction (or information reconciliation techniques) to correct shift type of errors; chattering on the other hand, will be dealt with filtering. The adversary in all cases is assumed to have the information on the number of deep fades that have occurred in a certain time-frame but he will not be privy to the locations of (all) such fades.

12.4 Key Generation

Let A and B be the two parties that wish to generate a key; we abstract the problem as follows. The two parties have access to two correlated random sources R_A and R_B over $\{0, 1\}^n$; in addition to the two parties, we also assume the existence of an adversary that may eavesdrop or even interfere with the random sources R_A and R_B . Whenever A and B sample their random sources, R_A and R_B , they obtain two bitstrings ρ_A and ρ_B respectively. Moreover, the adversary obtains a bitstring ρ_C . The triple of random variables (ρ_A, ρ_B, ρ_C) is distributed according to Env , a joint distribution that is based on the properties of the channel as well as assumptions about the environment that affect the wireless transmission. In some settings the adversary will have no information whatsoever about ρ_A, ρ_B ; this translates to the setting where the variable ρ_C is independent of the variables ρ_A, ρ_B .

12.4.1 Preliminaries

In this section, we recall some definitions regarding statistical distance and randomness extractors. Given two random variables ρ_1, ρ_2 we define by $\|\rho_1 - \rho_2\|$ the statistical distance between the random variables which is equal to $\frac{1}{2} \cdot \sum_v |[\text{Prob}][\rho_1 = v] - [\text{Prob}][\rho_2 = v]|$ where v in the summation ranges across all possible values in the support set of the random variables ρ_1 and ρ_2 (that are assumed to be defined over the same support). For a random variable ρ we define the min-entropy of ρ as $H_\infty(\rho) = -\log(\max_v [\text{Prob}][\rho = v])$.

The “average min-entropy” (as defined in [39]) of a random variable ρ_1 given a random variable ρ_2 is equal to

$$\tilde{H}_\infty(\rho_1 \mid \rho_2) = -\log (\mathbb{E}_{v \leftarrow \rho_2} [2^{-H_\infty(\rho_1 \mid \rho_2=v)}]).$$

Note that $(\rho_1 \mid \rho_2 = v)$ denotes the random variable that results when ρ_1 is projected over the conditional space defined by the event $\rho_2 = v$; the expression $2^{-H_\infty(\rho_1 \mid \rho_2=v)}$ is a function in v . Given $g(v)$ we denote by $\mathbb{E}_{v \leftarrow \rho_2}(g(v))$ the expectation of the random variable $g(\rho_2)$. A useful property that we will take advantage of is that the average min-entropy $\tilde{H}_\infty(\cdot)$ satisfies that $\tilde{H}_\infty(\rho_1 \mid \rho_2, \rho_3) \geq \tilde{H}_\infty(\rho_1 \mid \rho_3) - l$ assuming that $\rho_2 \in \{0, 1\}^l$ always (cf. lemma 2.2b [40]). As argued in this latter work, $\tilde{H}_\infty(\cdot)$ is a more suitable measure for cryptographic applications.

A randomness extractor (or just extractor) is a mechanism that flattens the distribution of an imperfect random source at the “expense” of reducing its size. Extractors are very useful in our setting since the distribution of ρ_A, ρ_B is very far from being uniform but we still wish to extract a key stream that is as close to uniform as possible. Extractors are divided into two categories, probabilistic and deterministic ones. Deterministic extractors are highly desirable since they are much simpler to implement and deploy within a larger system; unfortunately they are shown not to exist in the general case that assumes the weakest possible assumption on the imperfect source (i.e., that the min-entropy of the source is above a certain threshold) [24] (nevertheless we note that it is possible to construct deterministic extractors for more restricted classes of imperfect random sources as was shown in e.g., [41] where (n, k) -bit-fixing sources are considered). Probabilistic extractors on the other hand are more powerful but require the additional agreement of an additional random source. In order for them to be useful in our setting we require the additional random source to be public (so that it can be agreed upon using public discussion). The resulting primitive is called a strong extractor. Formally we have that:

Definition 1 Randomness Extractor: a function Ext is called a (n, m, l_0, ϵ) -strong-extractor if Ext is a mapping $\{0, 1\}^n \times \mathcal{R} \rightarrow \{\ell, \infty\}^\downarrow$ such that if ρ is any random variable satisfying $H_\infty(\rho) \geq m$ it holds that $\|\langle \text{Ext}(\rho, \tau), \tau \rangle - \langle \rho_u, \tau \rangle\| \leq \epsilon$, where ρ_u is uniformly distributed over $\{0, 1\}^{l_0}$ and τ is uniformly distributed over \mathcal{R} . Alternatively, if ρ is a specific random variable and the function Ext satisfies the above property, we will say that Ext is a (n, l_0, ϵ) -strong-extractor for ρ .

The above definition can be reformulated so that the lower bound on the entropy is based on average min-entropy $\tilde{H}_\infty(\cdot)$.

A well-known methodology for deriving strong-extractors is through the employment of the leftover hash-lemma [42]. This result shows that a family of functions known as universal hash family provides is a strong randomness extractor. A universal hash family is defined as follows: a family of functions $\{U_k\}_{k \in \{0, 1\}^v}$, with domain $\{0, 1\}^n$ and range $\{0, 1\}^{l_0}$ such that for all $x \neq x' \in \{0, 1\}^{l_0}$, then it holds that $[\text{Prob}][U_k(x) = U_k(x')] \leq 2^{-l_0}$ where k is distributed uniformly over $\{0, 1\}^v$. The leftover-hash lemma [42] shows that universal hash families constitute extractors that can extract essentially all randomness from an imperfect random source while

using a (relatively small) number of additional truly random bits. This result was generalized in [35] to employ average-case min-entropy that would be conditional to some external variable. The explicit statement is as follows:

Lemma 1 [35, 42] Leftover Hash Lemma: *Let ρ and ρ' be random variables over $\{0, 1\}^n$. Then, a universal hash family $\{\text{Ext}(\cdot, \tau)\}_{\tau \in \mathcal{R}}$ with $\text{Ext} : \{0, 1\}^n \times \mathcal{R} \rightarrow \{0, 1\}^{l_0}$ satisfies the following: if the average min-entropy $\tilde{H}_\infty(\rho \mid \rho') \geq m$ and $l_0 = m + 2 - 2\log(1/\epsilon)$ then $\|\langle \text{Ext}(\rho, \tau), \tau, \rho' \rangle - \langle \sigma, \tau, \rho' \rangle\| \leq \epsilon$, i.e., Ext is a (n, m, l_0, ϵ) -strong-extractor.*

The above results provide a way for designing extractors by employing universal hash families, cf. [25]. We note that a lot of work on extractors focuses on minimizing the length of the seed (cf. [43]), something not particularly important in our setting (where we assume that the transponders have access to local random coins).

12.4.2 Key Exchange Protocols

We now formally define the notion of a key exchange protocol in our setting. Such protocols involve two parties A, B , where A will be the initiator and B will be the responder. In a nutshell, we are interested in two properties: correctness and uniformity. The latter property will also capture security.

The key-exchange protocols that we will consider will permit the two party protocol π to take advantage of an oracle \mathcal{O}^{Env} that is parameterized by the probability distribution Env and operates as follows:

Parameter: Probability Distribution Env

- Upon receiving a request from player A , if $\langle \rho_A, \rho_B, \rho_C \rangle$ has not been determined yet, sample such triple from Env and return ρ_A .
- Upon receiving a request from player B , if $\langle \rho_A, \rho_B, \rho_C \rangle$ has not been determined yet, sample such triple from Env and return ρ_B .
- Upon receiving a request from the adversary, if $\langle \rho_A, \rho_B, \rho_C \rangle$ have not been determined yet, sample such triple from Env and return ρ_C .

Formally, a $(l_0, \epsilon_c, \epsilon_s)$ -key-generation protocol is a two party protocol π between A, B utilizing an oracle \mathcal{O}^{Env} such that the following properties hold true:

Definition 2 *Correctness.* The event that the output of the two parties A, B after executing the protocol π is equal has probability at least $1 - \epsilon_c$, where the probability is taken over all the coin tosses of π .

Uniformity. The random variable that corresponds to the ouput of the two parties conditioned on (i) the event that the output of the two parties is equal, (ii) on the transcript of the protocol π that generates it, and (iii) on the adversary's output from \mathcal{O}^{Env} , has statistical distance from the uniform distribution over $\{0, 1\}^{l_0}$ at most ϵ_s .

12.4.3 Secure Fuzzy Information Reconciliators

Below we define a variation of the fuzzy extractor primitive that is more suitable for our setting and can be used to build key exchange protocols combining privacy amplification and agreement with respect to a specific distribution. We call this primitive a “secure fuzzy information reconciliator” or SFIR.

Definition 3 Let $\langle \rho_A, \rho_B, \rho_C \rangle$ be a joint random variable denoted by Env . A $(l_0, \epsilon_1, \epsilon_2)$ -secure-fuzzy-information-reconciliator (SFIR) for Env is a pair (Gen, Rep) that satisfies the following:

1. Consider the following random variable C :

```

Sample  $\langle \rho_A, \rho_B, \rho_C \rangle \leftarrow \text{Env}$ .
 $\langle f, p \rangle \leftarrow \text{Gen}(\rho_A)$ .
 $f' \leftarrow \text{Rep}(\rho_B, p)$ .
if  $f \neq f'$  set  $C \leftarrow 1$  else  $C \leftarrow 0$ .

```

We require that $\text{Prob}[C = 1] \leq \epsilon_1$.

2. Consider the following random variable K :

```

Sample  $\langle \rho_A, \rho_B, \rho_C \rangle \leftarrow \text{Env}$ .
 $\langle f, p \rangle \leftarrow \text{Gen}(\rho_A)$ .
set  $K \leftarrow f$ .

```

We require that $\|(K|p, \rho_C) - U_{l_0}\| \leq \epsilon_2$, where U_{l_0} is the uniform over $\{0, 1\}^{l_0}$.

Suppose that we have a SFIR for a random variable Env . Below we show that this easily yields a key exchange protocol π utilizing the oracle \mathcal{O}^{Env} . Note that A will be the initiator and B will be the responder in the protocol.

Protocol π description using oracle \mathcal{O}^{Env} .

Parameter: a $(l_0, \epsilon_1, \epsilon_2)$ -SFIR scheme (Gen, Rep) .

Party A : read value ρ_A from \mathcal{O}^{Env} and compute $\langle f, p \rangle \leftarrow \text{Gen}(\rho_A)$. Transmit the value p to B and terminate by returning f .

Party B : upon receiving p read value ρ_B from \mathcal{O}^{Env} and compute $f' \leftarrow \text{Rep}(\rho_B, p)$. Terminate by returning f' .

Theorem 1 *The protocol π described above parameterized by a $(l_0, \epsilon_1, \epsilon_2)$ -SFIR is a $(l_0, \epsilon_1, \epsilon_2)$ -key-exchange protocol.*

Proof First, observe that the probability that the two parties A, B disagree in an execution of the protocol is equal to the probability of the event $G_{\text{cor}} = 1$. It follows immediately that this is bounded by ϵ_1 , i.e., the two parties are in agreement with probability at least $1 - \epsilon_1$.

Second, we need to show that the random variable that corresponds to the output of the two parties conditioned on the event that the two parties has statistical distance that is at most ϵ_2 from the uniform distribution over $\{0, 1\}^l$ when it is additionally conditioned to the protocol transcript and the adversary's input. Observe that this follows from the second property of the SFIR, as the protocol transcript is the value p and the adversary's input is ρ_C . \square

12.4.4 SFIR Constructions for the Wireless Envelope Distribution

Recall our main observation that the differences between the random sources, R_A and R_B , that are observed between the two players will predominantly happen at the beginning and(or) at the end of some deep fades, and that we assume that such fades occur randomly over a period of time. Consider Env the probability distribution of triples $\langle \rho_A, \rho_B, \rho_C \rangle$ that describes the envelope distribution as experienced respectively by A, B and the eavesdropper.

For a bitstring, a run is a sequence of consecutive of 1's within the bitstring. Based on the mapping of deep fades into sequences of 1's, it is clear that ρ_A contains a run for each deep fade that occurred in the envelope of the wireless transmission. Suppose the length of each ρ_A and ρ_B bitstring is n and the number of deep fades is t . Given that we assume that the t deep fades are uniformly distributed within the time interval that extends over n time slots we have the following:

Lemma 2 *Assume that the bitstring $\rho \in \{0, 1\}^n$ contains t runs of length at most k ; furthermore $2k + 2 \mid n$ and $n > 2(t - 1)(k + 1)$. If ρ is sampled uniformly from the set of all such bitstrings the min-entropy of ρ is $E_{n,k,t} = \log \binom{n/(2k+2)}{t} + t \log k$ which implies $E_{n,k,t} = \Omega(t \log \frac{n}{t})$.*

Proof Observe that there is a total of i_1, \dots, i_t choices to signify the start of the t deep fades and j_1, \dots, j_t for the end of each deep fade. We would like to count all subsets of t pairs $\{(i_1, j_1), \dots, (i_t, j_t)\}$ with the property that $1 \leq j_e - i_e \leq k$. Observe that there are $(nk)((n - 2(k + 1))k) \dots ((n - (t - 1)2(k + 1))k)$ ways to choose a vector of elements $\langle i_1, j_1, \dots, i_t, j_t \rangle$. Moreover, this is equivalent to a selection of a vector of the form $\langle (i_1, j_1 - i_1), \dots, (i_t, j_t - i_t) \rangle$. We divide by $t!$ to obtain the a total number of $\frac{n(n-2(k+1))\dots(n-(t-1)(2k+1))k^t}{t!}$. Given that we assume $(2k + 1) \mid n$ we have that the total number of choices is $\binom{n/(2k+1)}{t} k^t$. Next we employ the inequality $\binom{m^t}{t} \geq m^t$ that holds for $m, t \geq 1$ and by taking logs in both sides the proof of the statement follows. \square

Based on the above we easily obtain the following corollary:

Corollary 11 *Consider $\text{Env} = \langle \rho_A, \rho_B, \rho_C \rangle$ so that ρ_C specifies only the number of deep fades t . The average min-entropy of ρ_A given ρ_C is $E_{n,k,t}$.*

For the remaining of the section we will operate under the assumption regarding the envelope distribution $\text{Env} = \langle \rho_A, \rho_B, \rho_C \rangle$ where ρ_A, ρ_B are sets of indices of the

same cardinality and ρ_C is only the cardinality of ρ_A, ρ_B . Without loss of generality we will implicitly assume that $\rho_A, \rho_B, \rho_C \in \{0, 1\}^n$, but keeping in mind that each of these strings can be represented in a list of indexes format (that can be shorter than n bits). To formalize this, we define the space $\mathcal{M}_{n,k,t}$ containing all pairs of the form (i_ℓ, j_ℓ) for $\ell = 1, \dots, t$ for which it holds that $|i_\ell - j_\ell| \leq k$, $i_\ell < j_\ell$ for $\ell = 1, \dots, t$ and $j_{\ell-1} < i_\ell$ for $\ell = 2, \dots, t$. The natural embedding of elements of $\mathcal{M}_{n,k,t}$ into $\{0, 1\}^n$ corresponds a given $w \in \mathcal{M}_{n,k,t}$ to a bitstring of $\{0, 1\}^n$ that contains t runs so that the ℓ -th run starts at location i_ℓ and terminates at location j_ℓ .

SFIR Construction #1.

In our first SFIR construction we assume that the deviations between ρ_A, ρ_B will be small and we will employ a brute-force search for the decoding. We will thus utilize universal hash families both for privacy amplification and information reconciliation.

Let $n, k, t, s \in \mathbb{N}$. The envelope distribution $\text{Env} = \langle \rho_A, \rho_B, \rho_C \rangle$ satisfies that if the representations of ρ_A, ρ_B as sets are $\{(i_\ell^A, j_\ell^A) \mid \ell = 1, \dots, t\}$ and $\{(i_\ell^B, j_\ell^B) \mid \ell = 1, \dots, t\}$ respectively, it holds that (i) $\rho_C = \langle k, t, n \rangle$ always and (ii) the following event holds with probability ϵ_1 :

$$(\rho_A, \rho_B \in \mathcal{M}_{n,k,t}) \wedge \forall \ell \in [t] : \left(|i_\ell^A - i_\ell^B| \leq s \wedge (j_\ell^A - i_\ell^A = j_\ell^B - i_\ell^B) \right)$$

It is easy to see that conditioning on a certain $\rho_A \in \mathcal{M}_{n,k,t}$, for each $\ell \in \{1, \dots, t\}$ it holds that there are $2s + 1$ possible allowed locations for i_ℓ^B (each one uniquely defining a location for j_ℓ^B). It follows that conditioning on ρ_A there is a subset of $\mathcal{M}_{n,k,t}$ that ρ_B belongs to, which has cardinality at most $(2s + 1)^t$ elements. We denote this subset by \mathcal{S}_{ρ_B} . For sufficiently small values of t, s it is possible for the responder B to recover ρ_A by brute-force searching within the space \mathcal{S}_{ρ_B} . Note that keeping t small does not necessarily make the entropy of the channel too low as we can still rely on a large value of n for maintaining the entropy $E_{n,k,t}$ at a sufficient high level as suggested by lemma 2.

From the discussion above, it follows that the responder will require some “key verification information” so that it is assisted in finding the correct match for the string of the initiator. This suggests the following SFIR parameterized by two universal hash families $\{U_k\}_{k \in \{0,1\}^v} \{U'_{k'}\}_{k' \in \{0,1\}^{v'}}$ with ranges $\{0, 1\}^{l_0}$ and $\{0, 1\}^{l'_0}$ respectively.

SFIR Construction #1

- **Gen:** on input ρ_A , sample k, k' uniformly at random from $\{0, 1\}^v \times \{0, 1\}^{v'}$ and return (f, p) with $p = \langle k, k', U'_{k'}(\rho_A) \rangle$ and $f = U_k(\rho_A)$.
- **Rep:** on input ρ_B and $p = \langle k, k', u' \rangle$ find an element $\rho \in \mathcal{S}_{\rho_B}$ such that $U'_{k'}(\rho) = u'$ and output $U_k(\rho)$ otherwise output \perp .

Theorem 2 Under the envelope assumption 12.4.4 with probability ϵ_1 and parameters n, k, t, s , the above (Gen, Rep) construction constitutes a $(l_0, 2^{-l'_0} + \epsilon_1, \epsilon_2)$ -SFIR for the distribution Env provided that $E_{n,k,t} \geq l_0 + l'_0 + 2 \log(1/\epsilon_2) - 2$.

Proof First we consider correctness. Define the event **BAD** over all choices of $\langle \rho_A, \rho_B, \rho_C \rangle, k, k'$ as the event that $U'_{k'}(\rho_A) = U'_{k'}(\rho)$ but $\rho \neq \rho_A$ or that the output of **Rep** is \perp . Given the envelope assumption 12.4.4 we know that with probability ϵ_1 it holds that $\rho_A, \rho_B \in \mathcal{M}_{n,k,t}$ and that $\rho_A \in S_{\rho_B}$. Therefore the probability of returning \perp is at most ϵ_1 . On the other hand, given the universal hash property the likelihood of picking a k' for which the strings ρ, ρ_A have a collision is at most $2^{-l'_0}$. It follows that **BAD** is bounded by $2^{-l'_0} + \epsilon_1$.

We next consider the security property that is associated with the random variable K . The average min-entropy of the variable K would be equal to the entropy of the random variable $U_k(\rho_A)$ conditioned on the values k, k', u' that constitute the communication transcript. Note that the conditional space includes all those triples $\langle \rho_A, \rho_B, \rho_C \rangle$ that are consistent with k, k', u' . First observe that due to the fact that we reveal at most l'_0 bits of ρ_A through $u' = U'_{k'}(\rho_A)$, this subtracts at most l'_0 from the average min-entropy of ρ_A . Moreover, we have that $\{U_k\}_{k \in \{0,1\}^v}$ is a universal-hash family. This fact implies that the distribution of K conditioned on the communication transcript would be ϵ_2 away from the uniform provided that $E_{n,k,t} \geq l_0 + l'_0 + 2 \log(1/\epsilon_2) - 2$. \square

In order to apply the above in practice it is helpful to be able to construct universal hash families for given specification $\{0, 1\}^n \rightarrow \{0, 1\}^{l_0}$. For example, consider the key-space $(GF(2^{l_0}))^n$ where $k = \langle k_1, \dots, k_n \rangle$ with $k_i \in GF(2^n)$ for $i = 1, \dots, l_0$, and the function $U_k(w) = \sum_{i:w_i \neq 0} k_i$, where $i \in \{1, \dots, n\}$ denotes the i -th bit of w . Fix $w, w' \in \{0, 1\}^n$ so that $w \neq w'$. We have that there is at least one bit i_0 such that $w_{i_0} \neq w'_{i_0}$ and as a result the event $U_k(w) = U_k(w')$ conditioned on all values k_i with $i \neq i_0$, would imply that $k_{i_0} = v$ for some fixed value $v \in GF(2^{l_0})$. The probability of this event is equal to 2^{-l_0} which implies that we have a universal hash family. Constructions with much shorter keys are also feasible, cf. [25].

Example Implementation As seen from lemma 2, we have that for $k = 5, t = 12, n = 512$ it holds that the average conditional min-entropy of ρ_A given ρ_C is 94 bits. Assume now that the envelope assumption 12.4.4 holds with probability ϵ_1 and parameter $s = 2$. Using two universal hash families, one with length $l_0 = 55$ and one with length $l'_0 = 15$ the SFIR we presented above yields a key exchange protocol that provides 55-bit key that is 2^{-12} away from the uniform distribution over $\{0, 1\}^{55}$. Moreover, the two parties will agree on it with probability at least $1 - 2^{-15} - \epsilon_1$. Note that in order for the responder to recover this key for $s = 2$, it will have to execute a brute-force step of 5^{12} operations, where each one involves one application of the universal hash family $U'_{k'}(\cdot)$ on a string derived from ρ_B . Given the above mentioned implementation of a universal hash it is easy to see that each operation would require a small number of additions in $GF(2^{15})$. Note that additions over a binary extension field can be performed by exclusive-or's. Assuming an implementation of an equality test with an average of 100 cpu clock cycles per test it would be feasible to complete the complete brute-force test in about 10 s using a 2.4 GHz Pentium.

SFIR Construction #2.

A shortcoming of the previous SFIR construction is the requirement of a brute-force step for information reconciliation. In this section, we alleviate this by sacrificing a bit more entropy—this allows a more efficient error-correction. Moreover, we generalize the envelope assumption to allow for deviations in the run length. Formally we have,

Let $n, k, t, s, z \in \mathbb{N}$. The envelope distribution $\text{Env} = \langle \rho_A, \rho_B, \rho_C \rangle$ satisfies that if the representations of ρ_A, ρ_B as sets are $\{(i_\ell^A, j_\ell^A) \mid \ell = 1, \dots, t\}$ and $\{(i_\ell^B, j_\ell^B) \mid \ell = 1, \dots, t\}$ respectively, it holds that (i) $\rho_C = \langle k, t, n \rangle$ always and (ii) the following event holds with probability ϵ_1 :

$$(\rho_A, \rho_B \in \mathcal{M}_{n,k,t}) \wedge \forall \ell \in [t] : \left(|i_\ell^A - i_\ell^B| \leq s \wedge (|j_\ell^A - i_\ell^A - (j_\ell^B - i_\ell^B)| \leq z \right)$$

Our second SFIR construction is parameterized by a universal hash families $\{U_k\}_{k \in \{0,1\}^v}$ with range $\{0, 1\}^{l_0}$. It operates as follows:

SFIR Construction #2

- **Gen:** on input ρ_A , parse ρ_A as $\{(i_\ell^A, j_\ell^A) \mid \ell = 1, \dots, t\}$ calculate the values:

$$\tilde{s}_\ell = i_\ell^A \bmod (2s + 1) \quad \tilde{z}_\ell = (j_\ell^A - i_\ell^A) \bmod (2z + 1)$$

as well as sample k uniformly at random from $\{0, 1\}^v$. Return (f, p) with $p = (k, \tilde{s}_1, \dots, \tilde{s}_t, \tilde{z}_1, \dots, \tilde{z}_t)$ and $f = U_k(\rho_A)$.

- **Rep:** on input ρ_B and $p = (k, \tilde{s}_1, \dots, \tilde{s}_t, \tilde{z}_1, \dots, \tilde{z}_t)$ compute ρ to correspond to the set $\{(i_\ell, j_\ell) \mid \ell = 1, \dots, t\}$ with $i_\ell = i_\ell^B - (i_\ell^B \bmod (2s + 1)) + \tilde{s}_\ell$ and $j_\ell = i_\ell + j_\ell^B - i_\ell^B - (j_\ell^B - i_\ell^B \bmod (2z + 1)) + \tilde{z}_\ell$ and output $U_k(\rho)$.

Theorem 3 Under the envelope assumption 12.4.4 with probability ϵ_1 and parameters n, k, t, s, z , the above $\langle \text{Gen}, \text{Rep} \rangle$ construction constitutes a $(l_0, \epsilon_1, \epsilon_2)$ -SFIR for the distribution Env provided that $E_{n,k,t} \geq l_0 + t \cdot \log((2s + 1)(2z + 1)) + 2 \log(1/\epsilon_2) - 2$.

Proof The proof follows easily from the fact that $t \cdot \log((2s + 1)(2z + 1))$ bits are made public for the purpose of reconciling the differences between the two bitstrings. \square

Example Implementation Suppose that for parameters $t = 38, k = 10, n = 2000, s = 4, z = 2$ it holds that the average min-entropy under envelope assumption 12.4.4 is 355 bits. Based on theorem 3 we can obtain a $l_0 = 80$ bit key that will have distance less than 2^{-48} from the uniform distribution over $\{0, 1\}^{l_0}$. Note that contrary to SFIR construction #1 the overall computation required is minimal.

SFIR Construction #3.

We next present a SFIR construction based on a secure sketch. Given a suitable secure sketch (SS, Rec) we will use the sketching function SS as part of the Gen function

of the SFIR and the **Rec** function of the sketch as part of the implementation of **Rep**. In order to construct a suitable secure sketch we need a metric space \mathcal{M} over which we the samples ρ_A, ρ_B can be embedded and furthermore we should be able to argue that their distance is appropriately bounded. We will operate over $\{0, 1\}^n$ using the Hamming metric (denoted by $d(\cdot, \cdot)$) under the following assumption regarding the envelope distribution:

Let $n, k, t, s \in \mathbb{N}$. The envelope distribution $\text{Env} = \langle \rho_A, \rho_B, \rho_C \rangle$ satisfies that if the representations of ρ_A, ρ_B as sets are $\{(i_\ell^A, j_\ell^A) \mid \ell = 1, \dots, t\}$ and $\{(i_\ell^B, j_\ell^B) \mid \ell = 1, \dots, t\}$ respectively, it holds that (i) $\rho_C = \langle k, t, n \rangle$ always and (ii) the following event holds with probability ϵ_1 :

$$(\rho_A, \rho_B \in \mathcal{M}_{n,k,t}) \wedge \forall \ell \in [t] : \left(|i_\ell^A - i_\ell^B| \leq s \wedge |j_\ell^A - j_\ell^B| \leq s \right)$$

Observe that as long the assumption holds we have that $d(\rho_A, \rho_B) \leq 2st$. The SFIR construction is parameterized by a universal hash family $\{U_k\}_{k \in \{0, 1\}^v}$ with range $\{0, 1\}^{l_0}$ and a binary linear code $C \subseteq \{0, 1\}^n$, with $|C| = 2^k$ that can correct up to $2st$ errors. It follows that the distance of C should be $4st + 1$. We will employ syndrome decoding with $\text{syn}(\cdot)$ the syndrome function of C (defined as the application of the parity check matrix of C to a given string), i.e., there is an algorithm that given $\text{syn}(c + v) = \text{syn}(v)$ for any $c \in C$ and $v \in \{0, 1\}^n$ with Hamming weight less than $2st$ it holds that v can be efficiently recovered and thus c can be recovered as well (assuming $c + v$ is known). We will employ binary BCH codes (assuming $n = 2^m - 1$, for which we can obtain $k = n - 2stm$, [44]).

SFIR Construction #3

- **Gen:** on input ρ_A set $p = (\text{syn}(\rho_A), k)$ where $\text{syn}(\cdot)$ is the syndrome function of C and set $f = U_k(\rho_A)$ and k is a random key of $\{0, 1\}^v$.
- **Rep:** on input ρ_B and $p = (y, k)$ find the error vector e of Hamming weight less than $2st$ such that $\text{syn}(e) = \text{syn}(\rho_B) - y$ (addition is over $GF(2^n)$) and output $U_k(\rho_B - e)$.

Based on theorem 5.1 of [40] (that argues the syndrome construction we utilized above constitutes a secure sketch that sacrifices at most $n - k$ bits of entropy) we obtain the following:

Theorem 4 *Under the envelope assumption 12.4.4 with probability ϵ_1 and parameters n, k, t, s , the above $\langle \text{Gen}, \text{Rep} \rangle$ construction constitutes a $(l_0, \epsilon_1, \epsilon_2)$ -SFIR for the distribution Env provided that $E_{n,k,t} \geq l_0 + 4st \log(n + 1) + 2 \log(1/\epsilon_2) - 2$.*

Proof The proof is similar to the proof of theorem 3 but taking into account the fact that instead of revealing the “trailing” values $\tilde{s}_1, \dots, \tilde{s}_t, \tilde{z}_1, \dots, \tilde{z}_t$ associated with the t runs we reveal the syndrome of ρ_A based on the given BCH code. The syndrome itself is a binary string of length $2stm$ where $n = 2^m - 1$. \square

12.5 Simulation Results

In this section we provide a simulated realization of two nodes transmitting signals through a Rayleigh fading channel, each receiving their own version of the signal, and extracting a bit vector from it. We then compare the two vectors to each other. We show choices of parameters that satisfy with overwhelming probability the assumptions we made in the previous section about the envelope distribution.

12.5.1 Wireless Channel Simulation

We simulate a communication system with a Rayleigh fading channel, that both legitimate nodes experience. From each one's perception of a signal transmitted through this channel, they will generate their own bits streams. The parameters of this channel are:

- BPSK communication with the bit rate of 1 Mbps.
- SINR of 25 dB (equivalent to a BER of 10^{-5} for a multi-path fading channel).
- Doppler shift of 1 Hz.
- To reduce the effect of noise in estimating the bit streams at both sides of the channel, we filtered the received signal with a narrow low pass filter with a bandwidth of 100 Hz. Using a very narrow filter has the benefit of reducing the noise dramatically. Figure 12.5 shows the received signal strength of both sides of the communication channel after the low pass filter has been applied.

Note that in key generation we are only interested in estimating the received signal strength and not the actual transmitted bits. Also note that the Doppler frequency is in the order of a few Hz (at most 20 Hz for very fast changing environment), therefore, a narrow band filter with bandwidth of 100 Hz is enough to capture the signal fluctuation due to the change in the environment.

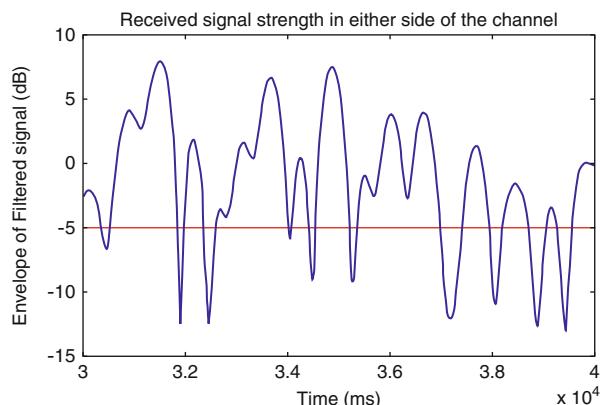


Fig. 12.5 This figure shows one second the received signal strength at both sides of the communication channel after applying a low pass filter. The low pass filter is used to reduce the noise

12.5.2 Generating Bit Streams

To generate bit streams in each side of the channel, each node samples the output of its low pass filter and compares it with a set threshold. Figure 12.6 shows the generated bits at both nodes when the threshold is set to -5 dB. As can be seen from the figure, the two generated sequences are very similar, in spite of the fact that each node experienced its own levels of interference and neither communicated with each other any decision regarding the generation of these bit streams. The only occasional differences occur when there is a transition from 0 to 1 or 1 to 0—that is, at the edge of a deep fade. These mismatches between the sequences are due to many reasons, including the different timing between the two nodes (since there is a slot delay between each one's transmission) and each node's distinct interference and noise that passes through its low pass filter.

Note that Fig. 12.6 depicts the *raw output of the low pass filter and threshold detector*, without engaging in any aforementioned techniques to match the two bit vectors up.

For the setup in this simulation, from a study of 100 s, deep fades occur with an average rate of 19 per one thousand bits.⁴ This means that for $n = 1000$, the resulting number of fades is $t = 19$. Note that this simulation, using an actual Rayleigh fading channel, shows that k , the length of the run of 1s due to a deep fade, is a random variable, as was detailed in Sect. 12.3.1.

Hence these results confirm that *even in the presence of interference* in a wireless network with time division duplex (TDD) for communication, the similarity between envelopes of the transmitter and receiver is enough to obtain equal keys for both.

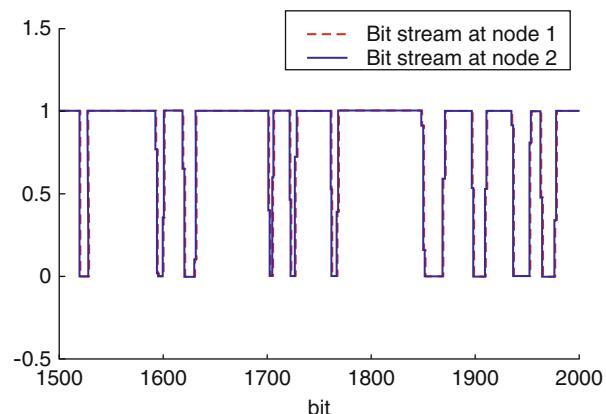


Fig. 12.6 Comparison of the generated bits at node 1 and node 2

⁴The statistical data is extracted from long runs of the simulation explained in this section. The figures only show a portion of these runs, for visual clarity.

12.6 Conclusions

In this chapter, we have introduced a novel method that uses physical layer characteristics of a wireless channel for generating a secret key between a pair of nodes in a wireless ad-hoc network.

Using the channel reciprocity and deep fades, our algorithms enable key agreement for a strong cryptographic key without the need of resorting to traditional key exchange cryptographic algorithms. The shared source of randomness between two nodes is the wireless channel which is unique to them. Given the lightweight computational requirements of our second procedure of Sect. 12.4.3, it follows that relatively effortlessly the two wireless nodes can create *a sequence of keys* that can be used successively. Moreover, this process can be done in conjunction to regular data transmission to each other. In practice, the two nodes will initiate data transmission and after some point, a string of sufficient entropy would be collected by the two nodes so that the first secret-key can be spawned; subsequently more keys may be generated and combined with previous keys. We remark that our technique applies to any signal bandwidth since only the fluctuation in the received signal is of use and the bandwidth and content of the transmitted signal is irrelevant for the purposes of key extraction.

We note that no special hardware is required for this technique and a narrow-band filter along with a threshold detector are sufficient. The presence of a narrow-band filter before the threshold detector dramatically reduces levels of interference and noise for generating the bit vector. This provides robustness for different levels of SINR that permit communication between the two nodes. Our technique is also robust to channel estimation noise, since it is based on detecting deep fades, and not the complete channel impulse response which tolerates estimation errors, that may arise at the edges of deep fades and are shown to be correctable. Finally, in case the nodes move, their signal envelopes change which increases the entropy and can give rise to better keys at a quicker pace. If the nodes are stationery it may still be possible for the nodes to introduce interference on purpose so a key may be spawned. It should be stressed that security of our key generation mechanisms is not based on traditional intractability assumptions such as those used to argue about security in schemes such as the Diffie Hellman key-exchange. In particular, the key created from our second procedure as detailed in Sect. 12.4.3 is information theoretically secure for an adversary that is oblivious to the location of the deep fades. Nevertheless, obliviousness to the location of the deep fades is a physical assumption that cannot be applicable to all adversaries. As discussed it may be possible to extrapolate the location of deep fades utilizing ray tracing techniques and a sufficiently detailed knowledge of the environment. Culminating the above concerns into an explicit intractability assumption over which the security of the proposed constructions can be argued formally is part of future work.

References

- [1] Kameran A, Aben G (2000) Net Throughput with IEEE 802.11 Wireless LANs. IEEE Wireless Communications and Networking Conference, 2: 747–752
- [2] Xiao Y, Rosdahl J (2002) Throughput and Delay Limits of IEEE 802.11. IEEE Communications Letters, 6(8): 355–357
- [3] Nuaymi L, Bouida N, Lahbil N, Godlewski P (2007) Headers Overhead Estimation, Header Suppression and Header Compression in Wimax. IEEE Conference on Wireless and Mobile Computing, Networking, and Communications: 17–23
- [4] Diffie W, Hellman M (1976) New directions in cryptography. IEEE Transactions on Information Theory 22: 644–654
- [5] Hata M (1980) Empirical Formula for Propagation Loss in Land Mobile Radio Services. IEEE Transactions on Vehicular Technology, VT-29: 317–325
- [6] Steele R (1992) Mobile Radio Communications. IEEE Press
- [7] Proakis J (1995) Digital Communications. McGraw-Hill
- [8] Karpikjoki V (2000) Security in Ad Hoc Networks. Helsinki University of Technology, Tik-110.501 Seminar on Network Security, Telecommunications Software and Multimedia Laboratory
- [9] Camtepe SA, Yener B (2005) Key Distribution Mechanisms for Wireless Sensor Networks: A Survey. TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department
- [10] Dutertre B, Cheung S, Levy J (2004) Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. System Design Laboratory, Technical Report, SRI-SDL-04-02
- [11] Lai B, Kim S, Verbauwheide I (2002) Scalable Session Key Construction Protocol for Wireless Sensor Networks. IEEE Workshop on Large Scale Real-Time and Embedded Systems
- [12] Eschenauer L, Gligor VD (2002) A Key-Management Scheme for Distributed Sensor Networks. ACM Conference on Computer and Communications Security: 41–47
- [13] Chan H, Perrig A, Song D (2003) Random Key Predistribution Schemes for Sensor Networks. IEEE Symposium on Security and Privacy: 197
- [14] Camtepe SA, Yener B (2004) Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. In: Samarati et al. (ed) Computer Security-ESORICS, Springer-Verlag, LNCS 3193
- [15] Camtepe SA, Yener B (2007) Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. ACM/IEEE Transactions on Networking, in press
- [16] Camtepe SA, Yener B, Yung M (2006) Expander Graph Based Key Distribution Mechanisms In Wireless Sensor Networks. IEEE International Conference on Communications
- [17] Blundo C, De Santis A, Herzberg A, Kutten S, Vaccaro U, Yung M (1992) Perfectly-Secure Key Distribution for Dynamic Conferences. Advances in Cryptology: 471–486
- [18] Blom R (1984) An Optimal Class of Symmetric Key Generation Systems. EUROCRYPT: 335–338
- [19] Li X, Chen M, Ratazzi EP (2005) Array-Transmission Based Physical-Layer Security Techniques for Wireless Sensor Networks. Proceedings of the IEEE International Conference on Mechatronics and Automation: 1618–1623
- [20] Hershey JE, Hassan AA, Yarlagadda R (1995) Unconventional Cryptographic Keying Variable Management. IEEE Transaction on Communications, 43(1): 3–6
- [21] Aono T, Higuchi K, Ohira T, Komiyama B, Sasaoka H (2005) Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels. IEEE Transactions on Antennas and Propagation, 53(11): 3776–3784

- [22] Ohira T (2005) Secret Key Generation Exploiting Antenna Beam Steering and Wave Propagation Reciprocity. 2005 European Microwave Conference, 1: 9–12
- [23] Kitaura A, Sasaoka H (2005) A Scheme of Private Key Agreement Based on the Channel Characteristics in OFDM Land Mobile Radio. Electronics and Communications in Japan, Part 3 (Fundamental Electronic Science), 88(9): 1–10
- [24] Santha M, Vazirani UV (1986) Generating quasi-random sequences from semi-random sources. Journal of Computer and System Sciences, 33: 75–87
- [25] Stinson D (2002) Universal Hash Families and the Leftover Hash Lemma, and Applications to Cryptography and Computing. Journal of Combinatorial Mathematics and Combinatorial Computing, 42: 3–31
- [26] Dodis Y, Reyzin L, Smith A (2004) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Advances in Cryptology EUROCRYPT 2004
- [27] Bennett CH, Brassard G, Robert, J-M (1988) Privacy Amplification by Public Discussion. SIAM Journal on Computing 17(2): 210–229.
- [28] Maurer U (1993) Secret key agreement by public discussion. IEEE Transaction on Information Theory, 39(3): 733–742
- [29] Maurer U, Wolf S (1999) Unconditionally Secure Key Agreement and the Intrinsic Conditional Information. IEEE Transactions on Information Theory, 45(2): 499–514
- [30] Holenstein T, Renner R (2005) One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption Advances in Cryptology. CRYPTO, Lecture Notes in Computer Science, Springer-Verlag
- [31] Wyner AD (1975) The Wire-Tap Channel. Bell Systems Technical Journal, 54: 1355–1387
- [32] Csiszár I, Körner J (1978) Broadcast Channels with Confidential Messages. IEEE Transactions on Information Theory, 22(6): 644–654
- [33] Aumann Y, Ding YZ, Rabin M O (2002) Everlasting Security in the Bounded Storage Model. IEEE Transactions on Information Theory 48(6): 1668–1680
- [34] Cachin C, Maurer UM (1997) Unconditional Security Against Memory-Bounded Adversaries. CRYPTO: 292–306
- [35] Dodis Y, Ostrovsky R, Reyzin L, Smith A (2007) Fuzzy Extractors. Security with Noisy Data, Springer
- [36] Howe DG, Hilden H, Weldon Jr E (1994) Shift Correction Code System for Correcting Additive Errors and Synchronization Slips. United States Patent 5373513, 12/13/1994
- [37] Naguib A (1996) Adaptive Antennas for CDMA Wireless Networks. PhD thesis, Stanford University
- [38] Bodtmann WF, Arnold HW (1982) Fade-Duration Statistics of a Rayleigh Distributed Wave. IEEE Transactions on Communications, COM-30(3): 549–553
- [39] Dodis Y (2005) On Extractors, Error-Correction and Hiding All Partial Information. Information Theory Workshop (ITW 2005)
- [40] Dodis Y, Ostrovsky R, Reyzin L, Smith A (2006) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. The Computing Research Repository (CoRR), abs/cs/0602007
- [41] Gabizon A, Raz R, Shaltiel R (2004) Deterministic extractors for bit-fixing sources by obtaining an independent seed. FOCS 2004
- [42] Impagliazzo R, Levin LA, Luby M (1989) Pseudo-Random Generation from One-Way Functions. Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89): 12–24
- [43] Shaltiel R (2004) Recent developments in extractors. In: Paun G, Rozenberg G, Salomaa A (ed) Current trends in theoretical computer science. The Challenge of the New Century, Vol 1: Algorithms and Complexity, World Scientific
- [44] van Lint JH (1998) Introduction to Coding Theory. Springer

- [45] Smith J, Jones M Jr, Houghton L et al. (1999) Future of Health Insurance. *The New England Journal of Medicine* 340(9): 325–329
- [46] Carter L, Wegman M (1979) Universal Hash Functions. *Journal of Computer and System Sciences*, 18(2):143–154
- [47] Datta A, Derek A, Mitchell JC, Warinschi B (2006) Computationally Sound Compositional Logic for Key Exchange Protocols. *CSFW 2006*: 321–334
- [48] Naor M, Yung M (1989) Universal One-Way Hash Functions and their Cryptographic Applications. *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*: 33–43
- [49] Stanica P (2001) Good Lower and Upper Bounds on Binomial Coefficients, *Journal of Inequalities in Pure and Applied Mathematics*, 2(3) Article 30

Chapter 13

Fingerprints in the Ether: Channel-Based Authentication*

Liang Xiao, Larry Greenstein, Narayan Mandayam and Wade Trappe

13.1 Introduction

Most wireless systems lack the ability to reliably identify clients without employing complicated cryptographic tools. This introduces a significant threat to the security of wireless networks, as the wireless channel is a broadcast medium, i.e., intruders can access wireless networks without a physical connection. One serious consequence is that spoofing attacks (or masquerading attacks), where a malicious device claims to be a specific client by spoofing its MAC address, becomes possible. Spoofing attacks can seriously degrade network performance and facilitate many forms of security weakness. For instance, by attacking control messages or management frames smartly, the intruder can corrupt the services of legal clients [1–3].

It is desirable to conduct authentication at the lowest possible layer (i.e., physical layer). In rich multipath environments typical of wireless scenarios, channel responses are *location-specific*. That is, channel frequency responses decorrelate from one transmit-receive path to another, if the paths are separated by the order of an RF wavelength or more [4]. Hence it is difficult for an adversary to create or precisely model a waveform that is transmitted and received by entities that are more than a wavelength away from the adversary. This is the basis of what we call “fingerprints in the ether”, i.e., channel-based authentication [5–9].

Authentication is traditionally associated with the assurance that a communication comes from a specific entity [10]. Physical-layer authentication, however, is used to discriminate among different transmitters, and must be combined with a traditional

L. Xiao (✉)
Department of Communication Engineering
Xiamen University, Fujian 361005, China
e-mail: lxiao@winlab.rutgers.edu

*Portions of the material have appeared previously in: L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication under time-variant channels,” IEEE Transactions on Wireless Communications, vol. 7, no. 7, 2008 ©IEEE 2008 and “A Physical-Layer Technique to Enhance Authentication for Mobile Terminals,” in Proceedings of IEEE International Conference on Communications, 2008 ©IEEE 2008.

handshake authentication process to completely identify an entity. Throughout this chapter, we assume that an entity's identity is obtained at the beginning of a transmission using traditional higher layer authentication mechanisms. Channel-based authentication is then used to ensure that all signals in both the handshake process and data transmission are actually from the same transmitter. Thus, this may be viewed as a cross-layer design approach to authentication.

We note that channel time variation is a challenge to the channel-based authentication. In practice it will be necessary to guarantee the continuity of the authentication procedure by probing the channel at time intervals less than the channel's coherence time.

In this chapter, we first describe the channel-based authentication in a static multipath environment, Sect. 13.2. Then we discuss the issues of environmental changes in Sect. 13.3, and terminal mobility in Sect. 13.4. As multiple-input multiple-output (MIMO) techniques will be widely deployed in future wireless networks, in Sect. 13.5, we also study the security gains possible when multiple antennas are available.

13.2 Fingerprints in Static Channels

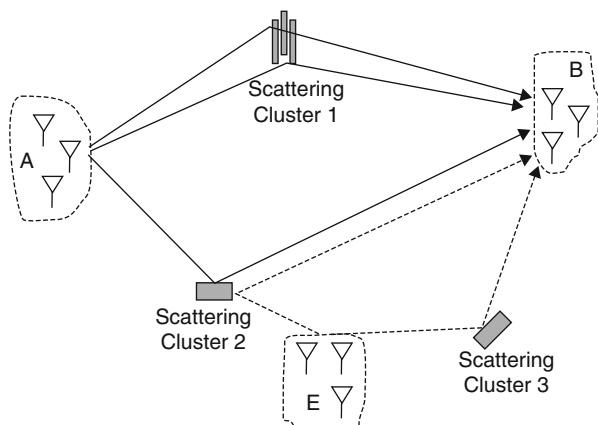
As a benchmark, we first describe a channel-based authentication scheme for time-invariant channels. As the basis of the discussions throughout this chapter, we cover in this section important issues such as the Alice-Bob-Eve model, our channel estimation model, and hypothesis testing in spoofing detection. Through the simple (yet important) example of a static channel, we can obtain the main idea of how channel estimation can be used to detect spoofing attacks in wireless networks.

13.2.1 Attack Model

We shall borrow from the conventional terminology of the security community by introducing three different parties: Alice, Bob, and Eve, which may be thought of as wireless transmitters/receivers that are potentially located in spatially separated positions, as depicted in Fig. 13.1. Alice will serve as the legitimate transmitter that initiates communication, while Bob will serve as the intended receiver. Their nefarious adversary, Eve, will serve as an active opponent who injects undesirable communications into the medium in the hopes of impersonating Alice.

Our security objective is to provide authentication between Alice and Bob, despite the presence of Eve. Authentication is traditionally associated with the assurance that a communication comes from a specific entity, while the objective of channel-based authentication may be interpreted as follows: Since Eve, a potential adversary within range of Alice and Bob, is capable of injecting her own signals into the environment to impersonate Alice, it is desirable for Bob to have the ability to differentiate between legitimate signals from Alice and illegitimate signals from Eve. Physical-layer authentication provides Bob evidence that the signal he receives did, in fact, come from Alice.

Fig. 13.1 The adversarial multipath environment involving multiple scattering surfaces. The transmission from Alice (A) to Bob (B) experiences different multipath effects than the transmission by the adversary, Eve (E). (©IEEE 2008)



13.2.2 Channel Estimation Model

As we mentioned, channel-based authentication utilizes the rapid spatial decorrelation of channel responses in multipath environments. To illustrate this, let us consider a simple transmitter identification protocol in Fig. 13.1, where Bob seeks to verify that Alice is the transmitter. Suppose that Alice probes the channel sufficiently frequently to assure temporal coherence between channel estimates and that, prior to Eve's arrival, Bob has estimated the Alice-Bob channel. Now, Eve wishes to convince Bob that she is Alice. Bob will require that each information-carrying transmission be accompanied by an authenticator signal. The channel and its effect on a transmitted signal between Alice and Bob is a result of the multipath environment.

Bob uses the received version of the authenticator signal to estimate the channel response, following standard, existing channel estimation mechanisms employed in most wireless systems. For the sake of our discussion, we shall formulate our problem in the frequency domain. We note, that due to Parseval's theorem, the our frequency-domain formulation has equivalent time-domain formulations. However, it should also be emphasized that by formulating our problem in the frequency domain, we align our work with modern wireless systems design, such as used in OFDM systems, where the use of multiple-carriers facilitates better communication by allowing for the transmitter and receiver to cope with harsh channel conditions (e.g., multipath fading).

Specifically, Bob first (at time k) measures and stores the frequency response of the channel connecting Alice with him. Denote the accurate and noisy version of the channel response by $H_A(f)$ and $\hat{H}_A(f)$, respectively. After a while, (at time $k+1$), Bob has to decide whether a transmitting terminal is still Alice, his decision being based on a noisy measured version, $\hat{H}_t(f)$, of that terminal's channel response to Bob (the true response being $H_t(f)$), where the subscript t denotes “transmitter to be authenticated”.

By sampling these two consecutive channel frequency responses at M tones, Bob obtains two M -dimension channel vectors $\hat{\mathbf{H}}_A$ and $\hat{\mathbf{H}}_t$. More specifically, $\mathbf{H} = [H_1, \dots, H_M]^T$ are samples from $H(f)$, where $H_m = H(f_o - W/2 + m\Delta f)$, $m = 1, \dots, M$, $\Delta f = W/M$, W is the system bandwidth, and f_o is the center frequency of the measurement.

Since the phase of Bob's receiver local oscillator (LO) drifts between one measurement and another, we introduce $\phi_n \in [0, 2\pi)$, $n = 1, 2$, to represent measurement errors in the phase of the channel frequency response. Considering the thermal noise in the channel estimation, we can write two estimated channel vectors as

$$\hat{\mathbf{H}}_A = \mathbf{H}_A e^{j\phi_1} + \mathbf{N}_1, \quad (13.1)$$

$$\hat{\mathbf{H}}_t = \mathbf{H}_t e^{j\phi_2} + \mathbf{N}_2, \quad (13.2)$$

where $\mathbf{N}_n \sim CN(\mathbf{0}, \sigma_N^2 \mathbf{I})$, $n = 1, 2$, \mathbf{I} is an $M \times M$ identity matrix, and σ_N^2 is the thermal noise variance in channel measurements.

We define σ_N^2 as the receiver noise power per tone, P_N , divided by the transmit power per tone, P_T/M , where P_T in mW is the total transmit power for the M tones that are measured. Noting that $P_N = \kappa \mathbf{T} N_F b$, where $\kappa \mathbf{T}$ is the thermal noise density in mW/Hz, N_F is the receiver noise figure, and b is the measurement noise bandwidth per tone in Hz [11], we can write

$$\sigma_N^2 = \frac{\kappa \mathbf{T} N_F b}{P_T/M}. \quad (13.3)$$

13.2.3 Spoofing Detection

In order to detect spoofing attacks, Bob compares the two resulting channel vectors: If the two channel estimates are “close” to each other, then Bob will conclude that the source of the second message is still Alice. If the channel estimates are not similar, then Bob should conclude that the second source is likely a would-be intruder, i.e., Eve.

Our channel-based spoofing detector utilizes a simple hypothesis test: The null hypothesis, \mathcal{H}_0 , is that the terminal is not an intruder, i.e., the claimant is Alice; and Bob accepts this hypothesis if the test statistic he computes, Z , is below some threshold, \mathcal{T} . Otherwise, he accepts the alternative hypothesis, \mathcal{H}_1 , that the claimant terminal is someone else.

$$\mathcal{H}_0 : \mathbf{H}_t = \mathbf{H}_A, \quad (13.4)$$

$$\mathcal{H}_1 : \mathbf{H}_t \neq \mathbf{H}_A. \quad (13.5)$$

As shown in [5], the test statistic in a generalized likelihood ratio test (GLRT) can be written as

$$Z = \frac{1}{\sigma_N^2} \|\hat{\mathbf{H}}_t - \hat{\mathbf{H}}_A e^{j\text{Arg}\hat{\mathbf{H}}_A^H \hat{\mathbf{H}}_t}\|^2, \quad (13.6)$$

where the superscript H represents Hermitian transformation and $\|\cdot\|$ denotes Frobenius norm. The test statistic can be viewed as a normalized difference between two channel vectors, $\hat{\mathbf{H}}_t$ and $\hat{\mathbf{H}}_A$. The exponential term is included to account for measurement errors in the phase of the frequency response. Without this adjustment by Bob, the transmitting terminal can be rejected even if it is in fact Alice.

Definition 1 In the channel-based spoofing detection scheme, the “false alarm rate” (or Type I error) and the “miss rate” (or Type II error) are defined as

$$\alpha = \Pr_{\mathcal{H}_0}(Z > \mathcal{T}), \quad (13.7)$$

$$\beta = \Pr_{\mathcal{H}_1}(Z \leq \mathcal{T}), \quad (13.8)$$

where \Pr is the probability averaged over all realization of channel estimation errors.

It is shown in [5] that the test statistic Z under \mathcal{H}_0 is a chi-square random variable with $2M$ degrees of freedom [12]. When \mathcal{H}_1 is true, Z is a non-central chi-square variable with a non-centrality parameter

$$\mu = \frac{1}{\sigma_N^2} \left\| \hat{\mathbf{H}}_t - \hat{\mathbf{H}}_A e^{j \operatorname{Arg} \hat{\mathbf{H}}_A^H \hat{\mathbf{H}}_t} \right\|^2. \quad (13.9)$$

Hence we have the following results:

Theorem 1 The threshold of the test for a specified α is given by

$$\mathcal{T} = F_{\chi_{2M}^2}^{-1}(1 - \alpha), \quad (13.10)$$

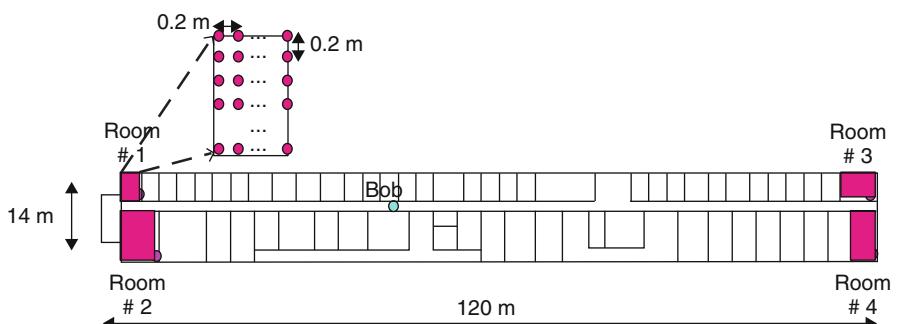
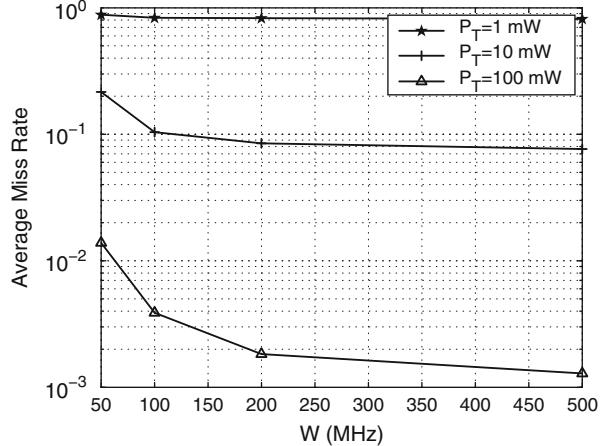


Fig. 13.2 System topology assumed in the simulations. Bob is located at 2-m height near the center of a $120 \text{ m} \times 14 \text{ m} \times 4 \text{ m}$ office building. Alice and Eve are located on dense grids at a height of 2 m. The sizes of the grids are $N_s = 150, 713, 315$, and 348, respectively, for Room # 1, 2, 3, and 4 (©IEEE 2008)

Fig. 13.3 The average miss rate for Room # 4 in an indoor environment shown in Fig. 13.2, is reported as a function of bandwidth (W) for three tones ($M = 3$), given false alarm rate as 0.01. Alice and Eve are placed within Room #4, while Bob is located in the center of the building. For each combination of Alice and Eve locations, the corresponding channel frequency responses to Bob were used to estimate the miss rate



where $F_X(\cdot)$ is the CDF of the random variable X , and $F_X^{-1}(\cdot)$ is the inverse function of $F_X(\cdot)$. The corresponding miss rate can be written as

$$\beta = F_{\chi_{2M,\mu}^2}(F_{\chi_{2M}^2}^{-1}(1 - \alpha)). \quad (13.11)$$

□

The performance of our physical layer authentication scheme has been verified using a ray-tracing software tool called WiSE [13] to generate the channel responses in specific environments. The WiSE ray-tracing tool has been extensively calibrated and its validity verified for a broad range of indoor and outdoor environments. As an illustration of the performance possible using physical layer authentication, consider a simulation scenario in a typical static indoor environment shown in Fig. 13.2. Simulation results in Fig. 13.3 indicate that measuring three channel frequency response samples over a bandwidth of 50 MHz and using a transmit power of 100 mW, valid users can be verified with 99% confidence while rejecting false users with approximately 99% confidence.

13.3 Fingerprints Against Environmental Changes

Environmental changes, such as the movement of other objects within the same building, may result in channel variations over time. If not well treated, this channel variation may lead to a higher false alarm rate in the channel-based authentication.

Hence, in this section, we analyze the channel time variation due to environmental changes and consider how to turn it into a benefit under certain circumstances. Based on a generalized time-variant channel model, we describe physical layer authentication schemes designed to cope with environmental changes, and then explore some specific cases.

13.3.1 Measurement Model for the Time-Variant Channel

We first extend the channel estimation formulation in Sect. 13.2.2 to a generalized time-variant channel model. Assume each estimated frequency response sample is made up of three parts: the fixed part that is the average channel response over time and contains the spatial variability information, the variable part with zero mean, and the measurement thermal noise:

$$\hat{\mathbf{H}}_A[k] = \bar{\mathbf{H}}_A + \epsilon_A[k] + \mathbf{N}_1[k], \quad (13.12)$$

where we use the notation that the m -th element of $\mathbf{X}[k]$, $X_m[k]$, is the sample from $X(t; f)$ at the m -th tone at a sampling time of kT . More specifically, $X_m[k] = X(kT; f_o - W/2 + m\Delta f)$, $m = 1, \dots, M$, where T is the sampling interval. The term $\bar{\mathbf{H}}_A$ is the average value of the channel frequency response over time, and $\epsilon_A[k]$ is the zero-mean variable part at time kT . Without loss of realism, we can assume that the noise samples, $\mathbf{N}_1[k]$, are independent across time, tone (frequency), and terminal (space), and that $\epsilon_A[k]$ is independent of $\mathbf{N}_1[k]$.

We model the variable part of the channel response as *wide-sense stationary uncorrelated scattering* (WSSUS), and can thus use a multipath tapped delay line to model its impulse response, $h(t, \tau)$ [14]:

$$h(t, \tau) = \sum_{l=0}^{\infty} A_l(t) \delta(t - l\Delta\tau), \quad (13.13)$$

where t is the observation time, and $l\Delta\tau$ and $A_l(t)$ are, respectively, the delay and complex amplitude of the l -th multipath component, with $E[A_l(t)] = 0$ over time. We set $\Delta\tau = 1/W$, since the receiver cannot resolve two components with time difference smaller than the inverse of the bandwidth.

The frequency response of the variable part is the Fourier transform of $h(t; \tau)$ in terms of τ ,

$$\epsilon_{A,m}[k] = \mathcal{F}\{h(t; \tau)\}|_{t=kT, f=f_o-W/2+m\Delta f} \quad (13.14)$$

$$= \sum_{l=0}^{\infty} A_l[k] e^{-j2\pi(f_o - W/2 + m\Delta f)l\Delta\tau}, \quad (13.15)$$

where $A_l[k] = A_l(kT)$ is the amplitude sample of the multipath component at time kT .

For illustrative purposes, we use the one-sided exponential distribution to model the power delay spectrum of $A_l[k]$,¹ i.e.,

$$P_\tau[l] = \text{Var}[A_l[k]] = \sigma_T^2 (1 - e^{-\gamma\Delta\tau}) e^{-\gamma\Delta\tau l}, \quad (13.16)$$

¹The literature abounds with empirical data [15] and theoretical examples [16] in which the exponential delay profile appears. We invoke it here for the sake of concreteness, which will allow us to compute numerical results, but we also recognize it to be a realistic condition.

where $\gamma = 2\pi B_c$ is the inverse of the average delay spread, B_c is the coherence bandwidth of the variable part, and σ_T^2 is the average power of $A_l[k]$ over all taps.

Let b_T^2 denote the ratio between σ_T^2 and the value of $|H_m|^2$ averaged over the M frequency samples (or “tones”) and the N_s receiver locations. We can thus write the standard deviation of the time variation as

$$\sigma_T = b_T \sqrt{\frac{1}{MN_s} \sum_{m=1}^M \sum_{l=1}^{N_s} |H_{l,m}|^2}, \quad (13.17)$$

where b_T represents the relative magnitude of the time variation in a given room.

Also for illustrative purposes, we use an autoregressive model of order 1 (AR-1) to characterize the temporal process of $A_l[k]$, i.e.,

$$A_l[k] = aA_l[k - 1] + \sqrt{(1 - a^2)P_\tau[l]}u_l[k], \quad (13.18)$$

where the AR coefficient a denotes the similarity of two A_l values spaced by T and the random component $u_l[k] \sim CN(0, 1)$ is independent of $A_l[k - 1]$.

As to the *variable* part of the channel frequency response, we consider the two extreme cases of $\hat{\mathbf{H}}_E[k]$, the frequency response sample of the channel between Eve and Bob, where the subscript E denotes “Eve”:

- *Spatially independent and identically distributed variation:*

$$\hat{\mathbf{H}}_E[k] = \bar{\mathbf{H}}_E + \epsilon_E[k] + \mathbf{N}_2[k], \quad (13.19)$$

where $\epsilon_E[k]$ and $\epsilon_A[k]$ are independent identically distributed (i.i.d.).

- *Complete spatially correlated variation:*

$$\hat{\mathbf{H}}_E[k] = \bar{\mathbf{H}}_E + \epsilon_A[k] + \mathbf{N}_2[k]. \quad (13.20)$$

13.3.2 Enhanced Spoofing Detection Schemes

If time variations are spatially independent and Bob knows the key channel variation parameters a , B_c , and σ_T , [6] proposed an enhanced spoofing detection scheme, with test statistic given by

$$Z = 2(\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k - 1])^H \mathbf{R}^{-1} (\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k - 1]), \quad (13.21)$$

where

$$\mathbf{R} = \text{Cov}[\hat{\mathbf{H}}_A[k] - \hat{\mathbf{H}}_A[k - 1]]. \quad (13.22)$$

Theorem 2 For a specified false alarm rate, α , the threshold of the test Eq. (13.21) can be written as

$$\mathcal{T} = F_{\chi_{2M}^2}^{-1}(1 - \alpha). \quad (13.23)$$

The corresponding miss rate is given by

$$\begin{aligned}\beta = \Pr\{ & 2(\hat{\mathbf{H}}_E[k] - \hat{\mathbf{H}}_A[k-1])^H \mathbf{R}^{-1} (\hat{\mathbf{H}}_{E,t}[k] - \hat{\mathbf{H}}_A[k-1]) \\ & < F_{\chi_{2M}^2}^{-1}(1-\alpha) \}. \end{aligned}\quad (13.24)$$

Proof Assume \mathbf{R}_d is the Cholesky factorization of \mathbf{R} (i.e., we have $\mathbf{R} = \mathbf{R}_d^H \mathbf{R}_d$), and $\mathbf{z} = \sqrt{2}(\mathbf{R}_d^H)^{-1}(\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k-1])$.

It is clear that, $\mathbf{z} \sim CN(\mathbf{0}, 2\mathbf{I})$ under \mathcal{H}_0 . Thus the test statistic $Z = \mathbf{z}^H \mathbf{z}$ is a chi-square random variable with $2M$ degrees of freedom, i.e., $Z \sim \chi_{2M}^2$. More details of the proof are given in [6]. \square

Now we consider several special cases:

- Asymptotic Results for Low Correlation Bandwidth:

Theorem 3 When the variation is independent over tones (i.e., $B_c/W \ll 1$), the miss rate for specified α , Eq. (13.24), can be written as

$$\beta = \Pr\{Z < \mathcal{T}|\mathcal{H}_1\} = F_{\chi_{2M,\mu}^2}(\rho F_{\chi_{2M}^2}^{-1}(1-\alpha)), \quad (13.25)$$

where

$$\mu = \|\bar{\mathbf{H}}_E - \bar{\mathbf{H}}_A\|^2 / (\sigma_T^2 + \sigma_N^2), \quad (13.26)$$

$$\rho = ((1-a)\sigma_T^2 + \sigma_N^2) / (\sigma_T^2 + \sigma_N^2). \quad (13.27)$$

Proof In this case, the covariance matrices become

$$\begin{aligned}\mathbf{R} &= (2(1-a)\sigma_T^2 + 2\sigma_N^2)\mathbf{I} \\ \mathbf{G} &= \text{Cov}[\hat{\mathbf{H}}_E[k] - \hat{\mathbf{H}}_A[k-1]] = (2\sigma_T^2 + 2\sigma_N^2)\mathbf{I}. \end{aligned}\quad (13.28)$$

Thus the test statistic Eq. (13.21) becomes

$$Z = \frac{\|\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k-1]\|^2}{(1-a)\sigma_T^2 + \sigma_N^2} = Z_2/\rho. \quad (13.29)$$

It is clear that under \mathcal{H}_1 , the test statistic Z_2 follows a non-central chi-square distribution with order $2M$, i.e., $Z_2 \sim \chi_{2M,\mu}^2$ with non-central parameter μ . More details are given in [6]. \square

- Asymptotic Results for High Correlation Bandwidth: When the variation is totally correlated over tones (i.e., $B_c/W \gg 1$), the covariance matrices degrade to

$$\mathbf{R} = 2\sigma_N^2\mathbf{I} + 2(1-a)\sigma_T^2\mathbf{1}, \quad (13.30)$$

$$\mathbf{G} = 2\sigma_N^2\mathbf{I} + 2\sigma_T^2\mathbf{1}, \quad (13.31)$$

where $\mathbf{1}$ is an $M \times M$ matrix with each element equals to 1. Again, we can use Eq. (13.24) to numerically calculate the miss rate β for specified false alarm rate α .

- *Unknown Channel Parameters:* When Bob does *not* know the channel parameters a , B_c , and σ_T , it is reasonable for him to use as the test statistic

$$Z = \frac{1}{\sigma_N^2} \|\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k-1]\|^2. \quad (13.32)$$

In this case, we can obtain numerical results for the false alarm rate and miss rate for specified threshold \mathcal{T} , plotting β vs. α with \mathcal{T} as an implicit parameter.

- *Full Spatial Correlation:*

Theorem 4 *If the temporal variation is fully spatially correlated, i.e., $\epsilon_E[k] = \epsilon_A[k]$, the miss rate of the test Eq. (13.21) for given false alarm rate α can be written as*

$$\beta = F_{\chi_{2M,\mu}^2}(F_{\chi_{2M}^2}^{-1}(1-\alpha)), \quad (13.33)$$

$$\mu = \|\sqrt{2}(\mathbf{R}_d^H)^{-1}(\bar{\mathbf{H}}_E - \bar{\mathbf{H}}_A)\|^2. \quad (13.34)$$

Proof The spatial correlation has no impact under the hypothesis \mathcal{H}_0 . If \mathcal{H}_1 is true, the correlation matrix of the difference between two measurements becomes \mathbf{R} , and $\hat{\mathbf{H}}_E[k] - \hat{\mathbf{H}}_A[k-1] \sim CN((\bar{\mathbf{H}}_E - \bar{\mathbf{H}}_A), \mathbf{R})$. Thus, the test statistic Eq. (13.21) is non-central chi-square distributed, $Z \sim \chi_{2M,\mu}^2$, with non-central parameter μ . \square

13.3.3 Impact of Channel Time Variations

Let us now study the impact of specific channel time variations. For convenience of analysis, we ignore phase measurement rotation in this section.

As one special case, if the channel is time-invariant, the miss rate of Eq. (13.25) becomes

$$\beta = F_{\chi_{2M,\mu}^2}(F_{\chi_{2M}^2}^{-1}(1-\alpha)), \quad (13.35)$$

which matches Eq. (13.11).

In the presence of time variation, however, the miss rate may become smaller. The asymptotic miss rate for the time-variant channel at high bandwidth, Eq. (13.25), increases with ρ , Eq. (13.27), and decreases with μ , Eq. (13.26). As the time variation σ_T^2 rises from 0 to ∞ , ρ decreases from 1 to $1-a$ and μ falls from $\|\bar{\mathbf{H}}_E - \bar{\mathbf{H}}_A\|^2/\sigma_N^2$ to 0, which may result in a smaller miss rate.

Actually, the temporal-variation has a two-fold impact:

- It adds uncertainty to the channel from Alice, and thus Bob has to increase the test threshold to accept Alice (negative impact on the performance);

- The variation is usually strongly correlated in time while very weakly correlated in space, and thus $\epsilon_A[k] - \epsilon_A[k-1] < \epsilon_E[k] - \epsilon_A[k-1]$ (positive impact on performance).

When σ_T is negligible, the channel can be viewed approximately as a time-invariant one, wherein the miss rate is given by Eq. (13.35). As σ_T rises, the miss rate falls since the positive impact dominates. If the variation continues to rise and becomes very large, the miss rate begins to rise, as the need to raise the threshold helps Eve and counteracts the positive impact. When σ_T becomes so large that both the fixed part of the channel response and the thermal noise are relatively negligible (i.e., $\sigma_T^2 \gg \sigma_N^2$, $\sigma_T^2 \gg ||\bar{\mathbf{H}}_E - \bar{\mathbf{H}}_A||^2$), then using Eq. (13.25) we can rewrite the miss rate as

$$\beta \approx F_{\chi_{2M}^2}((1-a)F_{\chi_{2M}^2}^{-1}(1-\alpha)), \quad (13.36)$$

which is a function of the time-correlation of the temporal variation parameter (a), frequency sample size (M), and the false alarm rate (α). If the variation is strongly correlated in time ($a \approx 1$), the miss rate can be less than that for the noise-dominated case, as described in Eq. (13.35), where the thermal noise is usually not negligible due to the limited transmit power.

Now let us summarize the impact of the spatial correlation of time variations. The miss rate with total spatial correlation, as described in Eq. (13.33), decreases with μ in a manner that is proportional to the inverse of \mathbf{R} , and thus rises with σ_T . Since a strong spatial correlation of the time variation damages the spatial variability character of the channel, which is the basis of our scheme, it will degrade the system performance.

Figure 13.4 confirms the efficacy of the algorithm in the presence of channel time variations, under realistic system parameter values ($P_T = 1 \text{ mW} \sim 1 \text{ W}$, $M = 10$, $W = 10 \text{ MHz}$; more information is given in [6]) for Room # 4 in an indoor environment shown in Fig. 13.2. It is shown that most average miss rates are smaller than 0.01. In this example, the per tone signal-to-noise ratio (SNR) in the

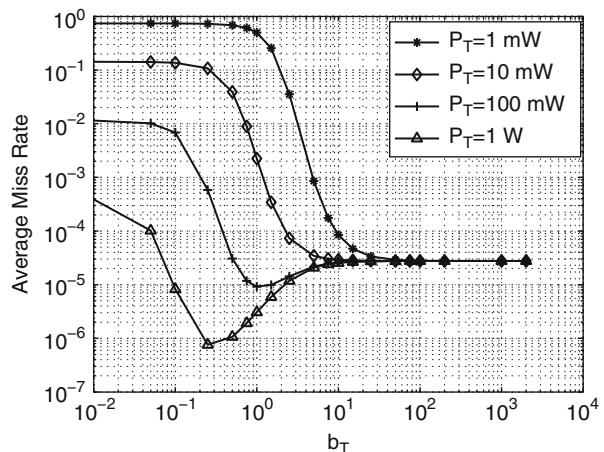


Fig. 13.4 The average miss rate as function of the relative standard deviation of the time variation, for the channel with spatially independent temporal variation. $M = 10$, $W = 10 \text{ MHz}$, $a = 0.9$ and $B_c = 0$, for Room # 4 in an indoor environment shown in Fig. 13.2, [6] (©IEEE 2008)

channel measurements ranges from -12.8 to 14.2 dB, with a median value of 6.4 dB, if using $P_T = 10$ mW. Also, as we have pointed out, our proposed algorithm can exploit the time variations to improve performance. For example, the miss rate falls from around 0.01 to 10^{-5} when the relative standard deviation of the time variation, $b_T = \sigma_T / \sqrt{\text{Var}[\bar{H}]}$, rises from 0.01 to 1 , with $P_T = 100$ mW. The trend of these curves with time variation confirms the discussion in this section, e.g., the minimum average miss rate is a tradeoff between the positive impact of the time variation and its negative impact resulting from the rise of the threshold. Moreover, the miss rate falls with increasing transmit power P_T , as expected, since it reduces the measurement noise at the receiver.

13.4 Fingerprinting in Spite of Terminal Mobility

Physical-layer authentication faces additional challenges as user mobility is introduced. Specifically, channel-based authentication utilizes the differences between a measured (test) channel response and a prior channel response to discriminate between transmitters at different locations. Unfortunately, due to the rapid spatial decorrelation properties of the wireless multipath channel, even a minor movement of a mobile can lead to a quite different channel response, resulting in large false alarm rates.

In this section, we consider an enhanced scheme to solve this problem, which consists of two parts—inter-burst authentication and intra-burst authentication—and generates private keys from the channel response to relax the limit on user displacement between two bursts.

13.4.1 System Model

We assume that Bob is stationary while Alice moves in any direction with a maximum velocity of v_a . However, our method is generic and our results can be easily extended to the case of mobility of all terminals.

Although our scheme can be implemented in many wireless systems, we continue to focus on orthogonal frequency division multiplexing (OFDM) systems as our motivating example. Suppose Alice sends a signal to Bob with the frame structure shown in Fig. 13.5, where the whole session consists of several data bursts. Each burst has N_x frames (N_x may vary with the burst), while each frame, with M frequency subbands and duration T , consists of N_d data symbols and one pilot in each subband. The number of pilots in the first symbol can, in fact, be less than the number of subbands, with the rest used for data. For concreteness, however, we assume initially that all subbands on the first symbol are used for pilots.

As shown in Fig. 13.6, Bob uses the pilots for channel estimation, obtaining test vectors $\hat{\mathbf{H}}_t[k]$, where k is the frame index. The frame duration T is assumed to be small enough to make the displacement of the transmitter (Alice) per frame much smaller than the channel decorrelation distance (i.e., $r = v_a T \ll \lambda/2$). Thus, two consecutive channel responses are highly correlated.

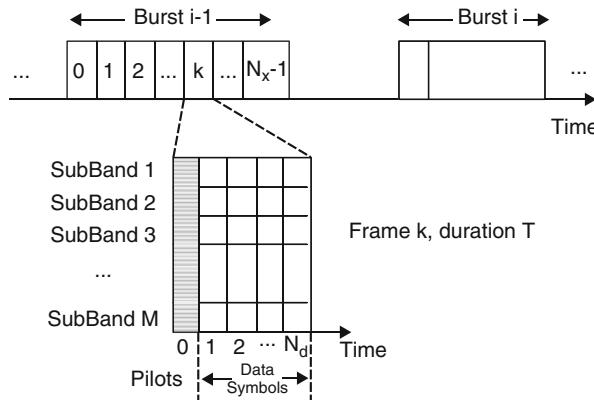


Fig. 13.5 Frame structure of the transmission from Alice to Bob. Each data burst consists of an arbitrary number of frames, while each frame has one pilot and N_d data symbols on each of M subbands. Frame 0 in each data burst contains the channel response value in the previous burst ($\hat{H}_A[-1]$) as a key for the inter-burst authentication. Bob uses the intra-burst authentication method in the following frames to authenticate Alice, and saves at least one frequency response as the key for the next burst (©IEEE 2008)

13.4.2 Enhanced Spoofing Detection

13.4.2.1 Inter- and Intra-Burst Authentication

Terminal mobility may force the self-decorrelation of Alice's channel with respect to itself. Hence we must employ a different strategy to bridge the gap between bursts of communications. To accomplish this, an improved process consists of two consecutive parts: an inter-burst authentication phase and an intra-burst authentication phase.

Inter-burst authentication is carried out using the first frame of each data burst to determine whether the current transmitter is still Alice. Note that at the outset of this

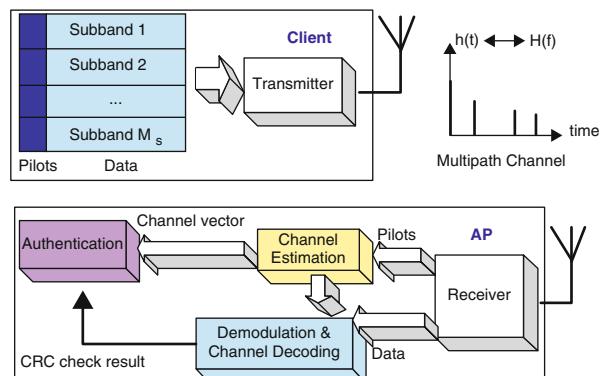


Fig. 13.6 Implementation of a physical layer authenticator in an OFDM system. Each frame with M frequency subbands consists of one pilot and several data symbols in each subband

protocol, in order for Bob to get an initial channel estimate for Alice, it is necessary to employ a higher-layer authentication protocol to bootstrap the association between Alice and a corresponding channel response. However, this is a one-time step, and generally the inter-burst process will focus on authenticating a subsequent data burst given that a prior data burst has been verified.

Thus we assume that Bob has an estimate of the Alice-Bob channel response of a particular frame in the previous data burst, which we shall denote as $\hat{\mathbf{H}}_A[-1]$, where the subscript A corresponds to “Alice”. The time interval between two bursts may be so large that Alice has moved a significant distance. Thus the channel response of the first frame in the current burst, $\hat{\mathbf{H}}_A[0]$, may be totally uncorrelated with $\hat{\mathbf{H}}_A[-1]$.

To solve this problem, we assume that both Alice and Bob save at least one channel response in each data burst as the key in the authentication process for the next successive burst. Alice may obtain this $\hat{\mathbf{H}}_A[-1]$ either by feedback from Bob, or by measurement of the reverse link pilots in a time division duplexing (TDD) system. In the first frame of each burst, Alice sends the saved $\hat{\mathbf{H}}_A[-1]$ from the last burst to Bob. If it matches with Bob’s version, Bob will assume it is from Alice. The channel response $\hat{\mathbf{H}}_A[-1]$ is not readily predicted by Eve. Thus she will fail the inter-burst authentication with high probability. Thus, the channel responses are used as a “key” or pass-phrase in an authentication procedure. Detailed performance analysis of how our scheme fits into a holistic cross-layer security framework is ongoing research.

The intra-burst authentication happens within a data burst, after the first frame passes the inter-burst authentication process. For any frame index $k > 1$, Bob is assumed to obtain the Alice-Bob channel gain in the previous frame, $\hat{\mathbf{H}}_A[k - 1]$, and use the observation of the current channel gain, $\hat{\mathbf{H}}_A[k]$, to determine whether the current transmitter is still Alice. This is an extension of the discussion of channel-based authentication scheme in previous sections.

We consider two types of intra-burst authentication: one is based on the GLRT, or more specifically the Neyman-Pearson (NP) test; the other utilizes an adaptive filter in the channel estimation.

13.4.2.2 NP-Based Test

We begin by building a Neyman-Pearson test for an “idealized case” wherein the set of channel response values form a Gaussian random vector, which motivates our choice of a practical test for the intra-burst authentication against terminal mobility.

During frame k , suppose Alice moves in an arbitrary direction from her location in the previous frame, with a maximum distance of $r = v_a T$. With $r \ll \lambda/2$, we can safely assume that $\hat{\mathbf{H}}_A[k]$ is highly correlated with $\hat{\mathbf{H}}_A[k - 1]$.

As before, for illustrative purposes, we use an autoregressive model of order 1 (AR-1) to characterize the temporal process of channel response $\mathbf{H}_A[k]$:

$$\mathbf{H}_A[k] = \rho \mathbf{H}_A[k - 1] + \sqrt{(1 - \rho^2)\sigma_A^2} \epsilon[k], \quad (13.37)$$

where the AR coefficient ρ denotes the similarity of the channel responses in consecutive frames; the noise in the AR-1 model, $\epsilon[k] \sim CN(\mathbf{0}, \mathbf{I})$, is independent of $\mathbf{H}_A[k-1]$; and σ_A^2 is the variance over space of \mathbf{H}_A .

By Eqs. (13.1) and (13.37), we have

$$\hat{\mathbf{H}}_A[k] \sim CN(\rho \mathbf{H}_A[k] e^{j\phi[k]}, (\sigma_N^2 + \sigma_A^2) \mathbf{I}), \quad (13.38)$$

where $\phi[k] \in [0, 2\pi)$ represents measurement errors. Since $r \ll \lambda/2$, we henceforth approximate ρ as 1.

Without a priori location information, at frame k , Eve is assumed to be randomly and uniformly distributed over the whole area of interest (e.g., a building). Since Eve is very likely to be far from Alice's previous location, her channel gain to Bob, $\hat{\mathbf{H}}_E[k]$, is independent of $\hat{\mathbf{H}}_A[k-1]$. Thus we model it as

$$\hat{\mathbf{H}}_E(k) \sim CN(\mathbf{0}, (\sigma_N^2 + \sigma_E^2) \mathbf{I}), \quad (13.39)$$

where $\sigma_E^2 \gg \sigma_A^2$ is the channel variance due to the location uncertainty of Eve.

As shown in [8], by Eqs. (13.38), (13.39), and $\sigma_E^2 \gg \sigma_A^2$, the test statistic of the corresponding generalized likelihood ratio test can be approximated as follows:

$$Z = \frac{\|\hat{\mathbf{H}}_t - \hat{\mathbf{H}}_A e^{j(\hat{\mathbf{H}}_A^H \hat{\mathbf{H}}_t)}\|^2}{\sigma_N^2 + \sigma_A^2}. \quad (13.40)$$

Theorem 5 In the Neyman-Pearson test with test statistic described by Eq. (13.40), the test threshold \mathcal{T} is given by

$$\mathcal{T} = F_{\chi_{2M}^2}^{-1}(1 - \alpha). \quad (13.41)$$

The corresponding miss rate can be simplified as

$$\beta = F_{\chi_{2M}^2}((\sigma_N^2 + \sigma_A^2) F_{\chi_{2M}^2}^{-1}(1 - \alpha) / (\sigma_N^2 + \sigma_E^2)). \quad (13.42)$$

Proof Under \mathcal{H}_0 , we have

$$(\hat{\mathbf{H}}_t[k] - \hat{\mathbf{H}}_A[k-1] e^{j(\hat{\mathbf{H}}_A^H[k-1] \hat{\mathbf{H}}_t[k])}) \sim CN(\mathbf{0}, (\sigma_N^2 + \sigma_A^2) \mathbf{I}), \quad (13.43)$$

and thus Z is approximately chi-square distributed with $2M$ degree of freedom, i.e., $Z \sim \chi_{2M}^2$. Hence from Eq. (13.7), we have Eq. (13.41).

Similarly, under \mathcal{H}_1 , we have

$$Z \sim (\sigma_N^2 + \sigma_A^2) \chi_{2M}^2 / (\sigma_N^2 + \sigma_A^2). \quad (13.44)$$

It is clear that, from Eqs. (13.8) and (13.44), we have Eq. (13.42). More details are given in [8]. \square

The miss rate rises with $(\sigma_N^2 + \sigma_A^2)/(\sigma_E^2 + \sigma_N^2)$. Since $\sigma_E^2 > \sigma_A^2$, it is clear that β for given α rises with σ_N^2 ; and the smaller σ_A is, the greater is the rise of β . It means that the system performance degrades with thermal noise, and this degradation is more distinct as Alice moves more slowly.

In reality, both σ_A , σ_E are unknown. Therefore, instead of using $\sigma_N^2 + \sigma_A^2$, we normalize the test statistic with a known parameter, $\|\hat{\mathbf{H}}_A[k-1]\|^2$, i.e.,

$$Z_1 = \frac{\|\hat{\mathbf{H}}_t - \hat{\mathbf{H}}_A e^{j\text{Arg}(\hat{\mathbf{H}}_A^H \hat{\mathbf{H}}_t)}\|^2}{\min(\|\hat{\mathbf{H}}_t\|^2, \|\hat{\mathbf{H}}_A\|^2)} \stackrel{\mathcal{H}_0}{\gtrless} \eta. \quad (13.45)$$

The new test statistic Z_1 is a practical one, totally based on $\hat{\mathbf{H}}_A[k-1]$ and $\hat{\mathbf{H}}_t[k]$. It represents their difference in both power (i.e., the distance effect) and shape (i.e., the multipath effect). The test threshold η of Z_1 has no closed-form expression and has to be determined by simulations or empirically.

13.4.2.3 RLS Adaptive Filter-Based Test

We now explore an alternative method for the intra-burst authentication, where M sets of linear least-squares adaptive filters are used independently to estimate the channel response for the M subbands. For convenience, we focus our discussion on the m -th subband, and ignore the frequency index m unless necessary.

As shown in Fig. 13.7, the estimated channel response at time k , which is the output of the m -th adaptive linear filter with order L , can be written as

$$y[k] = \sum_{l=0}^{L-1} w_l^* u(k-l), \quad (13.46)$$

where $u(k)$ is the input of the adaptive filter at time k , and w_l is the l -th tap weight of the filter, which can be determined using various adaptive algorithms, like the recursive least-squares (RLS) algorithm [17].

If it is Alice transmitting during the time interval $[(k-L)T, kT]$, the filter inputs are $\hat{\mathbf{H}}_A[k-L], \dots, \hat{\mathbf{H}}_A[k-1]$, and the estimation error is $\mathbf{e}[k] = \hat{\mathbf{H}}_A[k] - \mathbf{y}[k]$. Because of the strong correlation of the inputs $\hat{\mathbf{H}}_A[k-L], \dots, \hat{\mathbf{H}}_A[k]$, the ensemble-averaged squared error of the channel estimation filter is usually quite small.

If on the other hand, Eve comes in at time k , due to the spatial variability of the channel response, the estimation error,

$$e_m[k] = \hat{H}_{E,m}[k] - \sum_{l=0}^{L-1} w_l^* \hat{H}_{A,m}[k-l-1], \quad (13.47)$$

is very likely to jump to a much larger value.

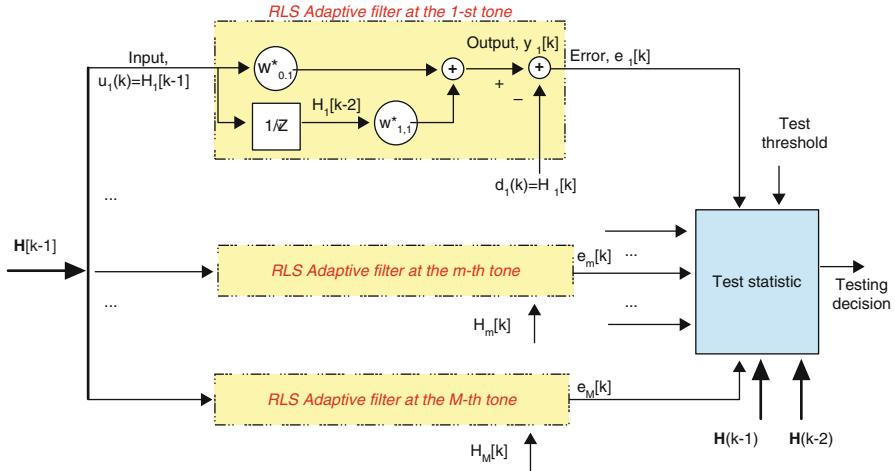


Fig. 13.7 Illustration of the RLS adaptive filter-based spoofing detection

Therefore, we build another test statistic Z_2 , using M parallel adaptive channel estimators. The null hypothesis \mathcal{H}_0 is accepted if the normalized squared sum of estimation error from these filters is less than a certain threshold η ; otherwise, the alternative hypothesis is chosen. Thus

$$Z_2 = \frac{\|\mathbf{e}[k]\|^2}{\sum_{l=0}^{L-1} \|\mathbf{u}[k-l]\|^2 / L} \stackrel{\mathcal{H}_0}{\gtrless} \stackrel{\mathcal{H}_1}{\lessdot} \eta. \quad (13.48)$$

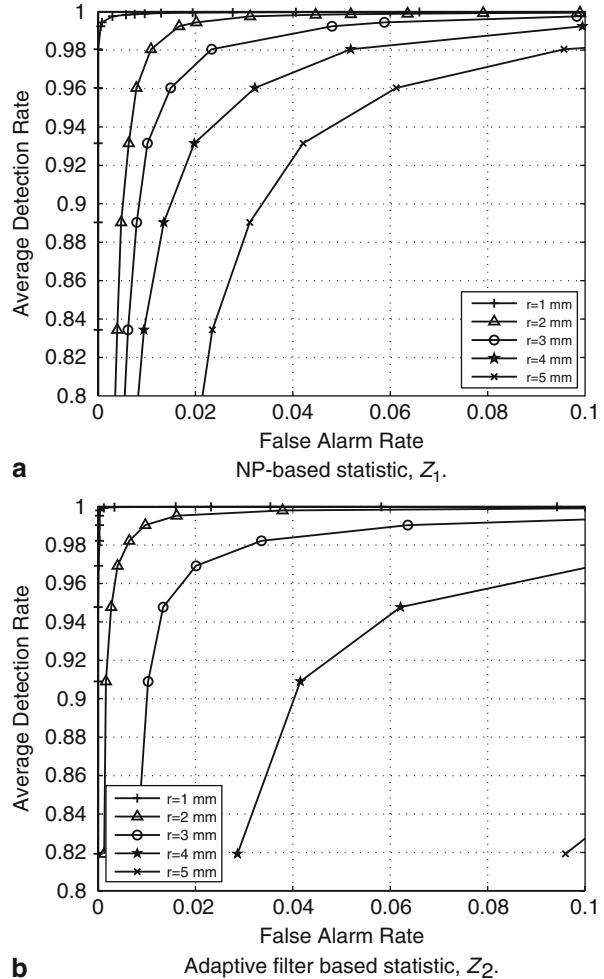
We normalize the estimation error to make η easier to determine. It does not have a closed-form expression but can be obtained empirically through simulations.

Note that this test can be carried out only after the successful authentication of at least L frames; thus, even though the RLS algorithm converges fast, it still takes approximately $2L$ frames [17]. Since we have to take data after the algorithm converges, we usually choose $k > 3L$ in Eq. (13.48). Thus Z_2 has larger system overhead ($3L$ frames) than Z_1 (1 frame), as well as greater implementation complexity.

The use of RLS estimators in this context may not be practical or cost-effective, but the results we will present for this case are instructive. They show that, even under the most favorable assumptions (RLS estimation), using least-squares adaptive filtering is not measurably superior to using the simpler NP test.

Figure 13.8 presents the receiver operating characteristic (ROC) curves of the intra-burst authentication method, i.e., the detection rate, $1 - \beta$, as a function of the miss detection rate, α , for the NP-based statistic Z_1 and the adaptive filter based statistic Z_2 , with Alice displacement per frame $r \in \{1, 2, 3, 4, 5\}$ mm. This corresponds to a frame duration $T \in \{0.70, 1.4, 2.1, 2.8, 3.5\}$ ms given a typical pedestrian velocity $v_a = 1.43$ m/s.

Fig. 13.8 Receiver operating characteristic (ROC) curves of the intra-burst authentication method, i.e., the average detection rate, $P_D = 1 - \beta$, as a function of false alarm rate, α , with Alice's displacement per frame $r \in \{1, 2, 3, 4, 5\}$ mm in arbitrary directions, and Eve randomly placed in the building with topology shown in [8] (©IEEE 2008)



It is shown in Fig. 13.8 that both Z_1 and Z_2 have good authentication performance, given that $r \leq 2$ mm. For example, Z_1 and Z_2 result in detection rates greater than 0.98 and 0.99, respectively, with $\alpha = 0.01$, $r \leq 2$ mm and $\eta = 0.1$. The performance degrades as Alice moves faster, since it leads to smaller correlation between successive channel realizations of Alice's channel to Bob. In addition, although Z_2 has better performance under smaller terminal velocity (e.g., $r \leq 2$ mm), Z_1 is more robust against terminal mobility. For instance, the detection rates of Z_1 and Z_2 are around 0.96 and below 0.8, respectively, given false alarm rate of 0.06, transmitter speed of 1.43 m/s, and frame duration of 3.5 ms. Considering that Z_2 has larger system overhead than Z_1 , we believe Z_1 is a better statistic to use than Z_2 .

13.5 Fingerprints Using MIMO

With the ability to provide diversity gain and/or multiplexing gain, multiple-input multiple-output (MIMO) techniques [18] will be widely deployed in future wireless networks, e.g., IEEE 802.11 n, to improve traffic capacity and link quality. Therefore, we now extend the analysis of channel-based authentication to MIMO systems and investigate the impact of MIMO techniques on the performance of spoofing detection.

We assume that Alice and Bob use N_T and N_R antennas, respectively. Eve, will inject undesirable communications into the medium with N_E antennas, in the hopes of impersonating Alice. In order to obtain the multiplexing gain associated with multiple antennas, the channel state information must be known at receivers [19]. Thus we assume that legal transmitters send non-overlapping pilots from N_T antennas, and Bob uses these to estimate channel responses, for non-security purposes.

MIMO techniques introduce an extra benefit to spoofing detection. Considering the Alice-Bob-Eve attack model, if Eve does not know the number of transmit antennas at Alice, N_T , she has to predict N_T . If Eve has the wrong prediction, or she simply does not have N_T antennas, Bob will foil her with certainty, based on the degraded channel estimation and data decoding results. In other words, Eve has a chance of fooling Bob only if she knows N_T and uses N_T transmit antennas, as is our assumption in the following discussions.

In an $N_T \times N_R$ MIMO system, if using the test statistic of Eq. (13.6), the miss rate for given false alarm rate can be written as [7]

$$\beta(\alpha) = F_{\chi^2_{2N_T N_R M, \mu}}(F_{\chi^2_S}^{-1}(1 - \alpha)), \quad (13.49)$$

where

$$\mu = \frac{P_T}{P_N N_T} \|\mathbf{H}_t - \mathbf{H}_A e^{j \operatorname{Arg}(\mathbf{H}_A^H \mathbf{H}_t)}\|^2. \quad (13.50)$$

We define a MIMO security gain in terms of our PHY-authentication scheme as $G = \beta_{SISO}/\beta_{MIMO} - 1$, and make the following observations:

- The MIMO security gain decreases with the system bandwidth (W), because the SISO system provides sufficient decorrelation at high bandwidth, making the resolution of Alice and Eve better.
- The MIMO security gain decreases with increasing noise bandwidth (b) in narrowband systems, since the noise power is larger as b increases.
- The MIMO security gain decreases with the frequency sample size (M), if the transmit power (P_T) is as large as 1 mW. If using high power and small M , the SISO system has accurate but insufficient channel response samples. Thus the additional dimensions of channel samples in MIMO systems allow for much better performance. On the contrary, if using high P_T and large M , the performance of SISO systems is too good to be significantly improved.

On the other hand, the MIMO security gain slightly rises with M , if P_T is as small as 0.1 mW. This is because when the channel estimation is not accurate due to low SNR, the systems need much more data to make a correct decision.

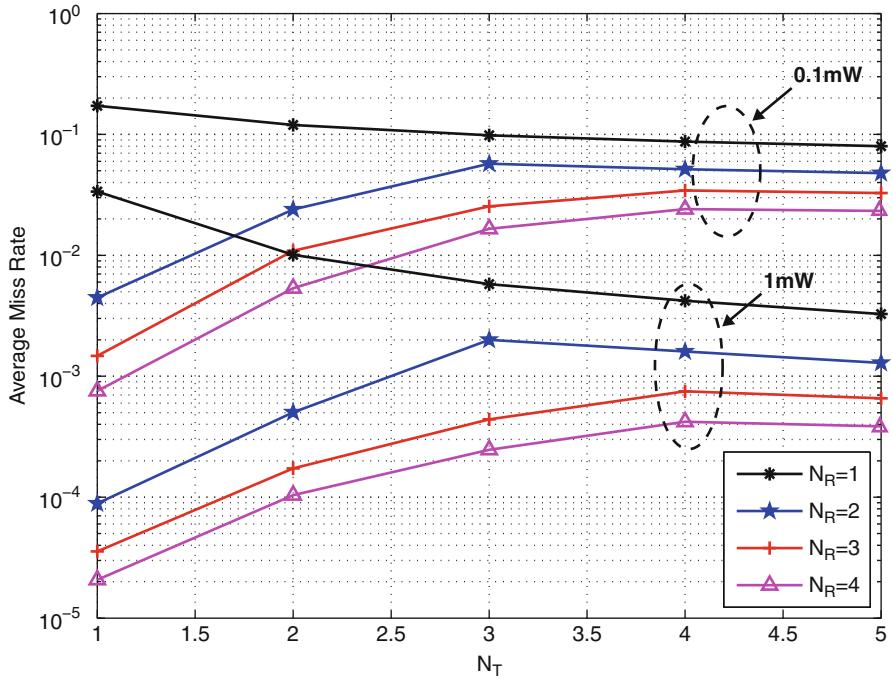


Fig. 13.9 Average miss rate of spoofing detection for various configuration of N_T and N_R , with $\alpha = 0.01$, $M = 3$, $P_T \in \{0.1, 1\}$ mW, $b = 0.25$ MHz, and $W = 2$ MHz

- Similarly, the MIMO security gain rises with P_T , under small M (e.g., $M = 1$). Otherwise, it decreases with P_T , under large M (e.g., $M = 10$).

We can also compare the security gain with the MIMO diversity gain, as a function of the number of transmit and receive antennas, as shown in Fig. 13.9. It is well known that the diversity gain rises with both the number of transmit antennas and the number of receive antennas. We have found that

- The use of multiple (i.e., $N_R > 1$) receive antennas improves the detection of spoofing attacks. This is a case where both the security gain and the diversity gain increase due to additional receive antennas.
- On the other hand, the security gain by using multiple (i.e., $N_T > 1$) transmit antennas may be positive or negative, based on the values of P_T , M , and N_R , since the transmit power per antenna decreases with N_T , while more transmit antennas provide extra channel estimation samples. This is a case where the security gain sometimes decreases but the diversity gain always rises due to additional transmit antennas.

Thus the MIMO-assisted channel-based authentication schemes provide a wide range of parameter choices and performance tradeoffs that have to be considered in the context of both security gains and MIMO performance gains.

13.6 Related Work

In commodity networks, such as 802.11 networks, it is easy for a device to alter its MAC address and claim to be another device by simply issuing an `ifconfig` command. This weakness is a serious threat, and there are numerous attacks, ranging from session hijacking[2] to attacks on access control lists[20], which are facilitated by the fact that an adversarial device may masquerade as another device.

In response, researchers have proposed using physical layer information to enhance wireless security. For example, spectral analysis has been used to identify the type of wireless network interface card (NIC), and thus to discriminate among users with different NICs [21]. A similar method, radio frequency fingerprinting, discriminates wireless devices according to the transient behavior of their transmitted signals [22]. For more general networks, the clock skew characteristic of devices has been viewed as a remote fingerprint of devices over the Internet [23]. In addition, the inherent variability in the construction of various digital devices has been used to detect intrusion [24].

More recently, the wireless channel has been explored as a new form of fingerprint for wireless security. The reciprocity and rich multipath of the ultrawideband channel has been used as a means to establish encryption keys [25]. In [26], a practical scheme to discriminate between transmitters was proposed and identifies mobile devices by tracking measurements of signal strength from multiple access points. A similar approach was considered for sensor networks in [27]. Concurrent to these efforts, the present authors have proposed a channel-based authentication scheme that exploits the spatial variability of channel frequency response to detect both spoofing attacks and Sybil attacks in wireless networks [5–9].

13.7 Conclusions

We have described a physical layer technique for enhancing authentication in wireless networks. The technique uses channel estimation mechanism and hypothesis testing to detect spoofing attacks.

The algorithm has been verified in a typical in-building environments, where we used the ray-tracing tool WiSE to generate realistic average channel responses and used a multipath tapped delay line channel model for the temporal variation part of the channel response. Simulation results have confirmed the efficacy of the algorithm: for realistic values of the measurement bandwidth (e.g., $W \sim 50$ MHz), number of response samples (e.g., $M \leq 10$) and transmit power (e.g., $P_T \sim 100$ mW), the miss detection rate of spoofing attacks is generally smaller than 0.01, given false alarm rate as 0.01.

In addition, the channel time variations due to environmental changes can improve the performance of the technique. For instance, the miss rate falls from around 0.01 to 10^{-5} when the relative standard deviation of the time variation, b_T , rises from 0.01 to 1, with $P_T = 100$ mW. In addition, the miss rate decreases with the transmit power of the probing signal and the measurement bandwidth, and usually requires

frequency samples of fewer than 10. We have also shown that the time correlation of the channel variation is helpful, while coherence in the frequency and spatial domains are harmful. Moreover, this technique works even when the receiver does not know the key channel variation parameters, namely, the AR temporal coefficient a , the coherence bandwidth B_c and the standard deviation of the variation σ_T , although these parameters help reduce the miss rate if known.

Another important issue is the challenge of terminal mobility. To address this problem, the authentication process is divided into two parts: the inter-burst authentication uses the channel response in the previous burst as a key for the first frame, solving the problem of possibly long intervals between bursts. The intra-burst authentication, on the other hand, compares the channel response in two consecutive frames via either of two practical methods: one is based on the Neyman-Pearson test; and the other uses adaptive filters. The NP-based method is more robust against terminal mobility, and more efficient in terms of system overhead and implementation complexity. Simulation results show that the proposed scheme can detect spoofing attacks efficiently under slow terminal velocity. For instance, the detection rate is around 0.96, given a false alarm rate of 0.06, when the transmitter moves at a speed of 1.43 m/s and the frame duration equals to 3.5 ms.

Finally, we briefly introduced the security gains possible for MIMO techniques in channel-based authentication. One promising ongoing research is to integrate this scheme into a holistic cross-layer framework for wireless security. The aim is to quantify the net benefit in thus augmenting traditional “higher-layer” network security mechanisms with physical layer methods.

References

- [1] Y. Chen, W. Trappe, and R. Martin, “Detecting and localizing wireless spoofing attacks,” in *Proceedings of Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 193–202, 2007.
- [2] A. Mishra and W. A. Arbaugh, “An initial security analysis of the IEEE 802.1x standard,” Tech. Rep. CS-TR-4328, University of Maryland, College Park, 2002.
- [3] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: real vulnerabilities and practical solutions,” in *Proceedings of USENIX security symposium*, pp. 15–28, 2003.
- [4] W. C. Jakes Jr., *Microwave Mobile Communications*, Piscataway, NJ: Wiley-IEEE Press, 1994.
- [5] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Fingerprints in the ether: Using the physical layer for wireless authentication,” in *Proceedings of IEEE International Conference on Communications (ICC)*, pp. 4646–4651, June 2007.
- [6] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels,” *IEEE Transactions on Wireless Communication*, vol. 7, pp. 2571–2579, July 2008.
- [7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “MIMO-assisted channel-based authentication in wireless networks,” in *Proceedings of IEEE Conference on Information Sciences and Systems (CISS)*, pp. 642–646, March 2008.
- [8] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “A physical-layer technique to enhance authentication for mobile terminals,” in *Proceedings of IEEE International Conference on Communications (ICC)*, May 2008.

- [9] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. “Channel-based detection of Sybil attacks in wireless networks,” *IEEE Transactions on Wireless Communication*, vol. 7, pp. 2571–2579, July 2008.
- [10] W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Upper Saddle River, NJ: Prentice Hall, 2002.
- [11] T. S. Rappaport, *Wireless Communications- Principles and Practice*, Englewood Cliffs, NJ: Prentice Hall, 1996.
- [12] M. Abramowitz and I. A. Stegun, *New York: Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*, Courier Dover Publications, 1965.
- [13] S. J. Fortune, D. H. Gay, B. W. Kernighan, O. Landron, M. H. Wright, and R. A. Valenzuela, “WiSE design of indoor wireless systems: Practical computation and optimization,” *IEEE Computational Science and Engineering*, March 1995.
- [14] P. A. Bello, “Characterization of randomly time-variant linear channels,” *IEEE Transactions on Communications System*, vol. CS-11, pp. 360–393, December 1963.
- [15] V. Ercog, D. G. Michelson, S. S. Ghassemzadeh, L. J. Greenstein, A. J. Rustako, P. B. Guerlain, M. K. Dennison, R. S. Roman, D. J. Barnickel, S. C. Wang, and R. R. Miller, “A model for the multipath delay profile of fixed wireless channels,” *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 399–410, 1999.
- [16] P. A. Bello and B. D. Nelin, “The effect of frequency selective fading on the binary error probability of incoherent and differentially coherent matched filter receivers,” *IEEE Transactions Communications System*, vol. CS-11, pp. 170–186, June 1963.
- [17] S. Haykin, *Adaptive Filter Theory*, Englewood Cliffs, NJ: Prentice Hall, 1986.
- [18] G. J. Foschini and M. J. Gans, “On limits of wireless communications in a fading environment when using multiple antennas,” *IEEE Wireless Personal Communications*, vol. 6, pp. 311–335, March 1998.
- [19] A. Goldsmith, *Wireless Communications*, Cambridge: Cambridge University Press, 2005.
- [20] A. Mishra, M. Shin, and W. A. Arbaugh, “Your 802.11 network has no clothes,” *IEEE Communications Magazine*, vol. 9, pp. 44–51, December 2002.
- [21] C. Corbett, R. Beyah, and J. Copeland, “A passive approach to wireless NIC identification,” in *Proceedings of IEEE International Conference on Communications*, vol. 5, pp. 2329–2334, June 2006.
- [22] J. Hall, M. Barbeau, and E. Kranakis, “Detection of transient in radio frequency fingerprinting using signal phase,” in *Wireless and Optical Communications*, ACTA Press, pp. 13–18, July 2003.
- [23] T. Kohno, A. Broido, and C. Claffy, “Remote physical device fingerprinting,” in *IEEE Transactions on Dependable and Secure Computing*, vol. 2, pp. 93–108, April–June 2005.
- [24] T. Daniels, M. Mina, and S. F. Russell, “Short paper: A signal fingerprinting paradigm for general physical layer and sensor network security and assurance,” in *Proceedings of IEEE/Create Net Secure Commun.*, pp. 219–221, September 2005.
- [25] R. Wilson, D. Tse, and R. Scholtz, “Channel identification: Secret sharing using reciprocity in UWB channels,” *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 364–375, September 2007.
- [26] D. Faria and D. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proceedings of ACM Workshop on Wireless Security*, pp. 43–52, Los Angeles, California, September 2006.
- [27] M. Demirbas and Y. Song, “An RSSI-based scheme for sybil attack detection in wireless sensor networks,” in *Proceedings of International Workshop on Advanced Experimental Activity*, pp. 564–570, June 2006.

Chapter 14

Message Authentication: Information Theoretic Bounds*

Lifeng Lai, Hesham El Gamal and H. Vincent Poor

14.1 Introduction

The goal of *message authentication* is to ensure that an accepted message truly comes from its acclaimed *transmitter*. It has wide applications in e-commerce and other areas. For example, when a stock broker receives a trading instruction for an account, he or she needs to verify that it is the owner of the account, and not someone else, who sends the instruction.

There are usually three parties involved in message authentication: a transmitter, a receiver, and an opponent. The opponent in authentication is active. It will initiate various attacks in order to mislead the receiver. For example, the opponent can initiate an impersonation attack, in which the opponent sends a fake packet to the receiver directly, hoping that the packet will be accepted by the receiver. The opponent can also initiate a substitution attack. In a substitution attack, the opponent will first intercept the packet transmitted from the source, and then modify the content in the packet. After the modification, the opponent will then forward the modified packet to the receiver. The receiver in a properly designed authentication system should be able to distinguish, with high probability, fake packets or modified packets from true packets coming from the transmitter.

Similar to secure transmission, there are two different design approaches for message authentication systems: the computational approach and the information theoretic approach. Computational approach based authentication systems are built on two assumptions: (1) certain mathematics problems are difficult to solve; and (2) the opponent has limited computational power. Hence the security of a computational approach based authentication system essentially relies on the validity of these

L. Lai (✉)

Department of Systems Engineering
University of Arkansas at Little Rock, Little Rock, AR 72204, USA
e-mail: lxlai@ualr.edu

*Portions of the material have appeared previously in “Authentication over Noisy Channels,” IEEE Transactions on Information Theory, vol. 55, no. 2, 2009 ©IEEE 2009.

assumptions. On the other hand, information theoretic based authentication systems do not make these two assumptions. Various coding techniques are employed in information theoretic based systems to ensure the detection of attacks.

We will focus on information theoretic based authentication systems in this chapter. To distinguish the source from the opponent, it is assumed that the source and the receiver share a key. Except for the value of the key and source message, the opponent is assumed to be aware of the system design, including the encoding/decoding schemes, etc. There is a relationship between the key size and the success probability¹ of each attack mentioned above. Intuitively, the larger the key size, the more difficult for an attack to be successful, and hence the system is more secure. Of course, one would like to make the success probability of the opponent as small as possible. But it is impossible to design an authentication scheme so that the success probability of the opponent is zero. To see this, consider the following simple attack strategy of the opponent for any authentication scheme: guess the value of the key. If the guess of the key is correct, there is no difference between the opponent and the source. Then, the impersonation attack will be successful, since now the opponent knows the key value and the coding scheme. If the total number of possible key values is $|\mathcal{K}|$, then the probability of a correct guess is $1/|\mathcal{K}|$. Hence, one important question is, can we design a scheme so that the success probability of the opponent is limited by $1/|\mathcal{K}|$? This question was first studied by Simmons [1]. As we will discuss in the sequel, Simmons's model assumes that there is no transmission noise. Under this model, Simmons showed that the success probability of the opponent is at least as large as $1/\sqrt{|\mathcal{K}|}$. This result is pessimistic since the $1/\sqrt{|\mathcal{K}|}$ is typically much larger than $1/|\mathcal{K}|$. More importantly, this is only a lower bound on the success probability of the opponent. The success probability of the opponent's attack could be much larger than this bound.

However, physical transmission systems are noisy. A common way of dealing with this fact is to use channel coding to convert the noisy channel into a noiseless one, and then to design an authentication code on top of channel coding. Liu and Boncelet [2, 3] also considered the situation in which channel coding is not perfect, and hence, there are some residual errors induced by the channel. The main conclusion of these works is that channel noise is *detrimental* to authentication, since it will cause the receiver to reject authentic messages from the transmitter.

In this chapter, we take an alternative view of the noisy channel model and design channel and authentication coding jointly. This way, we are able to *exploit* the channel noise to hide the key information from the opponent. The codebook of our channel code is designed such that the conditional distribution of the keys after observing the noisy output at the opponent is very close to a uniform distribution,² and hence the opponent is unable to use the noisy observations to increase the success probability of a substitution attack. By using this approach, we derive an upper-bound on the cheating probability which is significantly smaller than the existing lower bounds for the noiseless channel model. Moreover, this upper-bound is shown

¹We will rigorously define the conditions for an attack to be successful in the sequel.

²Rigorous definitions of distance and closeness will be given in the sequel.

to coincide with a simple lower bound on the cheating probability. In particular, we show that the success probability of the opponent is limited by $1/|\mathcal{K}|$, and thus all the key information can be used to protect against substitution and impersonation attacks simultaneously. We further consider the authentication of multiple messages using the same key K over the noisy channel. Similar to the single-message case, lower and upper bounds on the cheating probability are derived and shown to coincide. Again, all the key information can be used to protect against all the attacks simultaneously.

Throughout this chapter, upper-case letters (e.g., X) will denote random variables, lower-case letters (e.g., x) will denote realizations of the corresponding random variables, and calligraphic letters (e.g., \mathcal{X}) will denote finite alphabet sets over which corresponding variables range. Also, upper-case boldface letters (e.g., \mathbf{X}) will denote random vectors whereas lower-case boldface letters (e.g., \mathbf{x}) will denote realizations of the corresponding random vectors.

The rest of the chapter is organized as follows. In Sect. 14.2, we review results for authentication over noiseless channel. In Sect. 14.3, we introduce our system model and notation. Section 14.4 is devoted to the single message authentication scenario. Next, we analyze the authentication of multiple message using the same key in Sect. 14.5. Finally, in Sect. 14.6, we offer some concluding remarks.

14.2 Existing Approach: Noiseless Model

In this section, we briefly review existing results for authentication over noiseless channels. Readers can refer to [4] for a comprehensive review.

14.2.1 Single Message Authentication

The model for authentication over noiseless channels, Fig. 14.1, was developed by Simmons [1]. In this model, the source S and the receiver R share a secret key K , which is used to identify the transmitter. The secret key K is chosen from a set \mathcal{K} having $|\mathcal{K}|$ possible values with probability distribution $P(K)$. The transmitter and receiver are assumed to be honest, i.e., they will follow the rules and will not attack

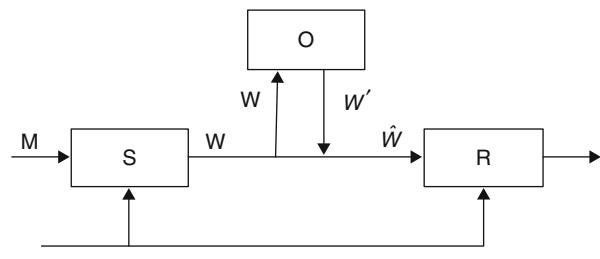


Fig. 14.1 The authentication channel (©IEEE 2009)

the system by faking messages. When the transmitter intends to send the message M ranging from a finite set \mathcal{M} with probability distribution $P(M)$, it transmits $W = f(K, M)$ over a noiseless public channel, where f is the encoding function. Let $\mathcal{W} = \{w : w = f(k, m), k \in \mathcal{K}, m \in \mathcal{M}\}$, i.e., \mathcal{W} is the set of possible codewords. For a particular key value k , only a subset of \mathcal{W} is valid. On receiving \hat{W} , which might be different from W due to various possible active attacks from the opponent O , the receiver needs to decide whether the message came from the legitimate transmitter or not. A particular codeword \hat{w} is deemed to be authentic if \hat{w} is a valid codeword for the key value the receiver has. That is, \hat{w} is deemed to be authentic if there exists a value $m \in \mathcal{M}$ so that $\hat{w} = f(m, k)$. If the receiver accepts the message (i.e., the receiver believes that the signal is authentic), then it computes an estimate of the source message M ; otherwise, it rejects the message.

Since there is no channel noise in this model, the opponent obtains a perfect copy of W . Two types of attacks are considered: the impersonation attack and the substitution attack. In the *impersonation attack*, the opponent sends W' to the destination before the source sends anything. This attack is successful if W' is accepted by the receiver as authentic. The success probability of this attack is denoted as P_I . Let us define

$$\gamma(w', k) = \begin{cases} 1, & \text{if there exists } m \in \mathcal{M} \text{ so that } w' = f(m, k), \\ 0, & \text{otherwise.} \end{cases} \quad (14.1)$$

The impersonation attack is successful if and only if the opponent chooses to send w' so that $\gamma(w', k) = 1$. Since the opponent does not know the value of the key, the success probability of the attack by choosing w' is

$$\Pr\{w' \text{ is valid}\} = \sum_{k \in \mathcal{K}} \gamma(w', k) P(k). \quad (14.2)$$

In an impersonation attack, the opponent will choose to send w' so that $\Pr\{w' \text{ is valid}\}$ is maximized, and hence

$$P_I = \max_{w' \in \mathcal{W}} \Pr\{w' \text{ is valid}\} = \max_{w' \in \mathcal{W}} \sum_{k \in \mathcal{K}} \gamma(w', k) P(k). \quad (14.3)$$

The second attack is referred to a *substitution attack*, in which after receiving W , the opponent modifies it to W' and sends it to the destination. The attack is successful if the receiver accepts W' and decodes this into another erroneous source message. The success probability of this attack is denoted as P_S . More specifically, let k be the key value the source and receiver share, and let m be the message the codeword w represents, i.e., $w = f(m, k)$. Then, if the opponent modifies w into w' , the attack is successful, if and only if there exists $m' \in \mathcal{M}$ so that $w' = f(m', k)$ and $m' \neq m$. Define

$$\gamma(w, w', k) = \begin{cases} 1, & \text{there exists } m' \in \mathcal{M} \text{ so that } w' = f(m', k) \text{ and } m' \neq m, \\ 0, & \text{otherwise.} \end{cases} \quad (14.4)$$

Now, after observing w , the success probability of the substitution attack by sending w' is

$$\Pr(w' \text{ is valid}|w) = \sum_{k \in \mathcal{K}} \gamma(w, w', k) P(k|w). \quad (14.5)$$

Obviously, for any observation w , the opponent will choose to send w' that maximizes $\Pr(w' \text{ is valid}|w)$. Hence, we have

$$\begin{aligned} P_s &= \sum_{w \in \mathcal{W}} P(w) \max_{w' \in \mathcal{W}} \Pr(w' \text{ is valid}|w) \\ &= \sum_{w \in \mathcal{W}} P(w) \max_{w' \in \mathcal{W}} \sum_{k \in \mathcal{K}} \gamma(w, w', k) P(k|w). \end{aligned} \quad (14.6)$$

Among these two types of attacks, the opponent will choose the attack that has higher success probability. Hence the success probability P_D of the opponent (i.e., the *cheating probability*) is $P_D = \max\{P_I, P_S\}$. The following theorem characterizes a lower bound for the success probability of the opponent for any encoding function f .

Theorem 1 ([1]) *The success probability of each attack in any authentication scheme is lower bounded as follows:*

$$P_I \geq 2^{-I(K; W)}, \quad (14.7)$$

and

$$P_S \geq 2^{-H(K|W)}, \quad (14.8)$$

in which $I(K; W)$ is the mutual information between K and W , while $H(K|W)$ is the conditional entropy of K given W . \square

This theorem was first proved in [1] from first principles and was recovered by Maurer [5] using an hypothesis testing perspective. From this theorem, one can easily identify a tradeoff between P_I and P_S . To minimize the probability of a successful impersonation attack, the transmitted ciphertext must contain a sufficient amount of information about the secret key in order to convince the receiver that the transmitted message comes from the legitimate source. That is $I(K; W)$ should be large, which unfortunately decreases $H(K|W)$, since

$$H(K|W) = H(K) - I(K; W).$$

Hence, the opponent can take advantage of the leaked information over its noiseless channel (contained in W) to increase the probability of a successful substitution attack. From Theorem 1, it is easy to see that, in order to minimize the lower bound $P_D = \max\{P_I, P_S\}$, one should set $H(K|W) = I(K; W)$, which gives

$$P_D \geq 2^{-H(K)/2}.$$

Hence, the strategy that minimizes the lower bound on $P_D = \max\{P_I, P_S\}$ is to use half of the key information to protect against the impersonation attack and the other half of the key information to protect against the substitution attack. Thus, for a given key size $|\mathcal{K}|$, the minimum value of P_D is $1/\sqrt{\mathcal{K}}$, which is achieved by letting the distribution of the key be a uniform distribution over the set \mathcal{K} . These bounds are of a negative nature, since they give only lower bounds on the cheating probability. The opponent may be able to achieve much better performance. There is no upper-bound available in the literature, partly due to the fact that typical bounding techniques such as the Jensen or log-sum inequalities are not applicable here. We will elaborate on this point in the sequel. The other unsatisfactory aspect of this lower bound is that not all the key information can be used to provide simultaneous protection against the two potential attacks. A slightly better lower bound on the impersonation attack was developed in [6].

14.2.2 Multiple Message Authentication

The study has been extended to the situation in which the same key K is used to authenticate a sequence of J messages M_1, \dots, M_J , one per time slot. Here, we assume that J is finite. The opponent will choose a time slot j in which to initiate either an impersonation attack or a substitution attack. For an impersonation attack in slot j , the opponent sends a message to the receiver before the source sends anything. The opponent will choose the message based on the information it has gained through the last $j - 1$ rounds of transmission. The attack will be successful if the opponent's message is accepted as authentic at the receiver. We denote by $P_{I,j}$ the success probability of the impersonation attack at the j th time slot. For a substitution attack in slot j , the opponent will intercept the source's j th packet, modify it and send the modified packet to the receiver. The opponent can make the modification using the information gathered in the j rounds of transmission that have occurred so far. The attack will be successful if the modified signal is accepted as authentic and the message part is decoded into an incorrect message. We denote by $P_{S,j}$ the success probability of the substitution attack in the j th time slot. Obviously, the opponent will choose the attack that maximizes its cheating probability $P_D = \max\{P_{I,1}, \dots, P_{I,J}, P_{S,1}, \dots, P_{S,J}\}$.

The authentication of multiple messages with the same key under the noiseless model has been studied in [5] and [7–9]. In these works, to avoid a replay attack, in which the opponent simply resends one of the codewords it has received before, one of the following assumptions is made: (1) the messages in all blocks are distinct (e.g., [7, 8]); or (2) the authentication schemes used in all blocks are distinct (e.g., [5, 9]). Under the second assumption, a lower bound for P_D with the noiseless transmission model was derived in [5].

Theorem 2 ([5]) *The success probability of any authentication scheme is bounded by*

$$P_D \geq 2^{-H(K)/(J+1)}. \quad (14.9)$$

□

This bound suggests that, after several rounds of authentication, the opponent may be able to obtain almost all the information about the key, and hence, may be able to choose an attack with a high success probability.

14.2.3 Extensions

The results introduced in Sects. 14.2.1 and 14.2.2 have been extended in several interesting directions. Here, we briefly discuss some representative examples while omitting the details. For a complete list of recent developments, please refer to [10].

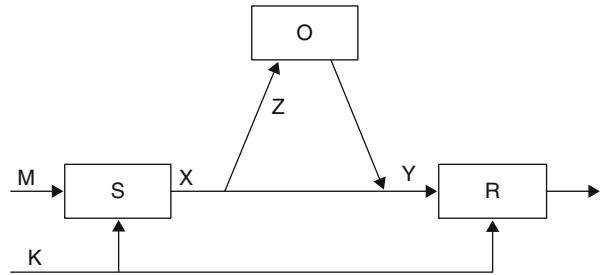
The scenario in which neither the source nor the receiver is honest is studied in [11]. In certain scenarios, both the transmitter and the receiver have the incentive to cheat. For example, in the broker scenario discussed in the introduction section, the investor has the incentive to deny that he has sent a certain trading instruction, if the trading results in a loss. Similarly, if the broker feels that certain trading can make a profit, he has the incentive to fake an instruction to do the trading even if the client has not instructed him to do so. By doing this, the broker can make an extra broker's fee. To solve possible disputes, an honest arbiter is introduced into this model. In this case, beyond the impersonation attack and substitution attack from the opponent, one needs to consider impersonation and substitution attacks from the transmitter or receiver. Following an approach similar to that of [1], Johansson et al. derived lower bounds for the success probability of each attack under the noiseless model. Desmedt and Yung [12] further studied the scenario in which the arbiter is also assumed to be dishonest, and hence, can potentially initiate an attack.

The other interesting direction is group authentication. In group authentication, more than one transmitter is required to authenticate a message. For example, if a group of people own an account jointly, any instructions for this account should be sent from this group of people jointly. This problem was first studied in [13, 14]. Information theoretic bounds for the various attacks are derived in [15]. The basic idea [15] in group authentication is to combine results from secret sharing [16] with classical authentication codes. In secret sharing, a secret is encoded into several different pieces, which are distributed to different persons. The code is designed so that there exists a threshold, in which one can recover the secret only after observing more pieces than this threshold. In group authentication, we can then encode the key into pieces and distribute these pieces to different transmitters. Only when a sufficiently large number of transmitters agree to authenticate a certain message, can they recover the key and authenticate the message.

14.3 System Model

Figure 14.2 shows the new model under consideration here. It differs from Simmons's model only in the channel, which is assumed to be noisy in our model. More specifically, we consider the discrete memoryless channel (DMC) and assume that

Fig. 14.2 The new authentication channel model
©IEEE 2009



when the transmitter sends \mathbf{x} , the opponent receives \mathbf{z} with probability

$$P(\mathbf{z}|\mathbf{x}) = \prod_{t=1}^n P(z(t)|x(t)),$$

where n is the length of the transmitted vector. If the opponent does not initiate any attack, the legitimate destination will receive \mathbf{y} with probability

$$P(\mathbf{y}|\mathbf{x}) = \prod_{t=1}^n P(y(t)|x(t)).$$

If the opponent initiates an attack, the value of \mathbf{y} will depend on the strategy of the opponent. Here $P(y(t)|x(t))$ and $P(z(t)|x(t))$ denote the indicated channel transition probabilities, while $x(t)$, $y(t)$, and $z(t)$ range through the finite sets \mathcal{X} , \mathcal{Y} , and \mathcal{Z} , respectively. In order to derive more general bounds, we assume that the channel between the opponent and receiver is noiseless, and that the opponent can send anything over this channel. It is worth noting that this assumption does not incur any loss of generality, and actually gives the opponent an advantage, since any noisy channel can be simulated with this noiseless channel by simply randomizing the transmitted signal.

To identify the transmitter, we assume that the source and the destination have a common secret key K chosen from a set \mathcal{K} having $|\mathcal{K}|$ possible values. To transmit the message M , the source uses a stochastic encoding function f to convert the message and key into a length n vector \mathbf{X} , i.e., $\mathbf{X} = f(K, M)$. Upon receiving \mathbf{Y} , which may come from either the source or the opponent, the destination uses a decoding function g to obtain an estimate of the message and key, that is $(M', K') = g(\mathbf{Y})$. If $K' = K$, the receiver accepts the message. Otherwise, the receiver rejects the message. We require the condition that, if the signal is authentic, the decoding error probability at the destination must approach zero as the length of the code increases, i.e., for any $\epsilon > 0$, there is a positive integer n_0 , such that for all $n \geq n_0$, we have

$$P_e = \Pr\{M' \neq M | \mathbf{Y} \text{ comes from } \mathbf{X}\} \leq \epsilon.$$

There are two components of the error probability P_e : P_1 and P_2 , where P_1 is the probability of a miss, which is the probability that the receiver wrongly rejects an

authentic message, and P_2 is the probability that the decoder correctly accepts the signal as being authentic but incorrectly decodes it.

The opponent is assumed to be aware of the system design, except for the particular realizations k and m of the key K and message M . We consider the two forms of attack described above. That is, we consider the impersonation attack, in which the opponent sends a codeword \mathbf{X} to the receiver before the transmitter sends anything. Such an attack is successful if \mathbf{X} is accepted as authentic by the receiver, and we denote this probability of success by P_I as noted above. We also consider the substitution attack, in which the opponent blocks the transmission of the main channel while receiving \mathbf{Z} . After that, the opponent modifies the signal and transmits it to the receiver. This attack is considered to be successful if the modified signal is accepted as authentic by the receiver and is decoded into m' that is not equal to the original message m . Again, the success probability of this attack is denoted by P_S .

14.4 Authentication of a Single Message

In this section, we discuss the authentication of a single message under the noisy channel model. We first review some results from the wiretap channel [17], which is instrumental in building our authentication scheme. We then introduce our authentication scheme. Finally, we derive information theoretic bounds for the success probability of each attack under our model.

14.4.1 The Wiretap Channel

We begin by reviewing some results related to the wiretap channel introduced in [17]. The wiretap channel is defined by two DMCs $\mathcal{X} \rightarrow (\mathcal{Y}, \mathcal{Z})$, where \mathcal{X} is the input alphabet from the transmitter, \mathcal{Y} is the output alphabet at the legitimate receiver and \mathcal{Z} is the output alphabet at the wiretapper. In the wiretap channel, the wiretapper is assumed to be passive, and the goal is to transmit information to the destination while minimizing the information leakage to the wiretapper. More specifically, to send a message $m \in \mathcal{M}$, the transmitter sends $\mathbf{x} = f(m)$, where f is a stochastic encoder. After receiving \mathbf{y} , the destination obtains an estimate $m' = g(\mathbf{y})$. The opponent is fully aware of the system design, and hence, knows the codebook used by the source. A perfectly secure rate R_s is said to be achievable if there exist f and g , such that for each $\epsilon > 0$, there is a positive integer n_0 , such that $\forall n > n_0$

$$|\mathcal{M}| \geq 2^{nR_s} \quad (14.10)$$

$$\Pr\{M' \neq M\} \leq \epsilon, \text{ and} \quad (14.11)$$

$$\frac{1}{n} I(M; \mathbf{Z}) \leq \epsilon. \quad (14.12)$$

The perfect secrecy capacity C_s is defined to be the supremum of the set of R_s values that satisfy conditions Eqs. (14.10–14.12). It is proved in [18] that the perfect secrecy

capacity is given by

$$C_s = \max_{U \rightarrow X \rightarrow YZ} [I(U; Y) - I(U; Z)]^+,$$

where the function $[x]^+ = \max(x, 0)$ and U is an auxiliary random variable satisfying the Markov chain relationship $U \rightarrow X \rightarrow (YZ)$.

The source-wiretapper channel is said to be less noisy than the main channel if, for all possible U that satisfy the above Markov chain relationship, one has $I(U; Z) > I(U; Y)$. On the other hand, if the source-wiretapper channel is not less noisy than the main channel, there exists a distribution satisfying $U \rightarrow X \rightarrow (Y, Z)$ such that $I(U; Y) > I(U; Z)$, and thus the perfect secrecy capacity is nonzero. One of the main insights gleaned from the wiretap channel is that perfectly secure communication is possible, without sharing a secret key a priori between the source and destination, by using a codebook whose codeword rate is higher than the secret message rate R_s (i.e., one message will correspond to several different codewords). Usually, the codeword rate is set to be the rate that can be supported by the source-destination channel allowing the legitimate receiver to recover the correct codeword while confusing the opponent with the high codeword rate.

14.4.2 Proposed Authentication Scheme

In authentication applications, when the source is sending information, the opponent tries to overhear the message and uses the information gained to initiate a substitution attack. This eavesdropping stage corresponds to the wiretap channel model. This observation motivates our approach of using a *wiretap channel code* to protect our authentication key. More specifically, if the wiretapper channel is not less noisy than the main channel, there exists an input distribution P_X such that $I(X; Y) - I(X; Z) > 0$. Therefore, for a given key size $|\mathcal{K}|$, there exists a positive integer n_1 , such that $\forall n \geq n_1$,

$$2^{n[I(X; Y) - I(X; Z)]} > |\mathcal{K}|. \quad (14.13)$$

Also for a given message size $|\mathcal{M}|$ and key size $|\mathcal{K}|$, there exists a positive integer n_2 , such that $\forall n \geq n_2$,

$$2^{nI(X; Y)} > |\mathcal{M}||\mathcal{K}|. \quad (14.14)$$

In our transmission scheme, the source first generates³ a codebook for the wiretap channel with $2^{nI(X; Y)}$ codewords, whose length n satisfies conditions Eqs. (14.13), (14.14) and a low decoding error probability requirement. The source then partitions the codeword into $|\mathcal{K}|$ subsets, associating one subset with each key. Since the length satisfies Eq. (14.14), there are more than $|\mathcal{M}|$ codewords in each subset.

³An explicit procedure for generating and partitioning the codebook will be given in the sequel.

The source then further divides each subset into $|\mathcal{M}|$ bins, each corresponding to a message. There are multiple codewords in each bin. Fig. 14.3 shows the structure of the codebook. In the transmission, if the intended message is m , and the key is k , the source then randomly chooses a codeword \mathbf{x} from the m th bin of the k th subset using a uniform distribution. The source then transmits \mathbf{x} over the channel. The opponent receives \mathbf{z} with probability

$$P(\mathbf{z}|\mathbf{x}) = \prod_{t=1}^n P(z(t)|x(t)).$$

The receiver receives \mathbf{y} . If the opponent does not initiate any attack, then

$$P(\mathbf{y}|\mathbf{x}) = \prod_{t=1}^n P(y(t)|x(t)).$$

On the other hand, if the opponent chooses to attack, the value of \mathbf{y} depends on the opponent's attack strategy.

After receiving \mathbf{y} , the destination first obtains an estimate $\hat{\mathbf{x}}$ of the transmitted codeword using typical set decoding; that is the destination decodes \mathbf{y} into $\hat{\mathbf{x}}$ if $(\hat{\mathbf{x}}, \mathbf{y})$ are jointly typical. It then obtains an estimate m' of the message and an estimate k' as the corresponding bin index and subset index, respectively, of $\hat{\mathbf{x}}$. We denote the decoding process at the destination as $(m', k') = g(\mathbf{y})$. If $k' = k$, the receiver accepts the message as authentic; otherwise it rejects the message.

Note that in the noiseless model, this scheme does not work, since the opponent can obtain a perfect copy of \mathbf{x} , and hence can determine the values of k and m . Thus the substitution attack will be successful. In the noisy channel model, if we design the code properly, the output at the opponent will not provide it with such information, as shown in the sequel.

First, let us consider the impersonation attack. The optimal strategy for the opponent is to transmit a codeword from the subset corresponding to the key that has the largest probability of being accepted by the receiver, i.e., \mathbf{y}_o , which will be transmitted by the opponent, should be chosen from the subset corresponding to k' such that

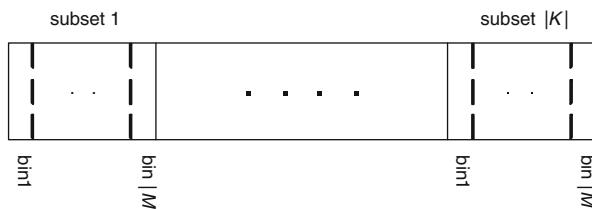


Fig. 14.3 The codebook used in our authentication scheme. The codebook is divided into $|K|$ subsets, each of which is further partitioned into $|\mathcal{M}|$ bins. Each subset corresponds to a key k . Each bin in each subset corresponds to a message m (©IEEE 2009)

the following probability is maximized:

$$\sum_{k \in \mathcal{K}} P(k) \gamma_1(k, k'),$$

where $\gamma_1(k, k')$ is an indicator function that equals 1 if k' is accepted as authentic, and equals 0 in other cases. In our scheme, $\gamma_1(k, k') = 1$ if $k' = k$; otherwise $\gamma_1(k, k') = 0$, and hence

$$P_I = \max_{k' \in \mathcal{K}} \left\{ \sum_{k \in \mathcal{K}} P(k) \gamma_1(k, k') \right\}.$$

For a substitution attack, the opponent knows \mathbf{z} , and hence can choose \mathbf{y}_o based on this information. Let h be the transformation employed by the opponent to transform \mathbf{z} to \mathbf{y}_o . Here, h can be any function, either deterministic or stochastic. Also, denote $(m', k') = g(\mathbf{y}_o) = g(h(\mathbf{z}))$. Note that g is the decoding function at the destination, and hence m' and k' are the decoded message and key at the destination after the opponent's attack. Obviously, for each observation \mathbf{z} , the opponent should choose h so that

$$\sum_{m, k} P(m, k | \mathbf{z}) \gamma_2(m, m') \gamma_1(k, k')$$

is maximized. Here $\gamma_2(m, m') = 1$ if $m' \neq m$ and equals 0 otherwise. Meanwhile, as defined above, $\gamma_1(k, k') = 1$ if $k' = k$, and equals 0 otherwise. Hence, the success probability of the substitution attack is

$$P_S = \sum_{\mathbf{z}} P(\mathbf{z}) \sup_h \left\{ \sum_{m, k} P(m, k | \mathbf{z}) \gamma_2(m, m') \gamma_1(k, k') \right\}. \quad (14.15)$$

To simplify the analysis, we have the following lemma.

Lemma 1 *For any substitution attack strategy h of the opponent, we have*

$$P_S \leq \sum_{\mathbf{z}} P(\mathbf{z}) \max_{k \in \mathcal{K}} \{P(k | \mathbf{z})\}. \quad (14.16)$$

□

Proof We can bound P_S as follows

$$\begin{aligned} P_S &= \sum_{\mathbf{z}} P(\mathbf{z}) \sup_h \left\{ \sum_{m, k} P(m, k | \mathbf{z}) \gamma_2(m, m') \gamma_1(k, k') \right\} \\ &\stackrel{(a)}{\leq} \sum_{\mathbf{z}} P(\mathbf{z}) \sup_h \left\{ \sum_{m, k} P(m, k | \mathbf{z}) \gamma_1(k, k') \right\} \end{aligned}$$

$$\begin{aligned}
&= \sum_{\mathbf{z}} P(\mathbf{z}) \sup_h \left\{ \sum_k \left(P(k|\mathbf{z}) \gamma_1(k, k') \sum_m P(m|k, \mathbf{z}) \right) \right\} \\
&\stackrel{(b)}{=} \sum_{\mathbf{z}} P(\mathbf{z}) \sup_h \left\{ \sum_k P(k|\mathbf{z}) \gamma_1(k, k') \right\} \\
&\stackrel{(c)}{\leq} \sum_{\mathbf{z}} P(\mathbf{z}) \max_{k \in \mathcal{K}} \{P(k|\mathbf{z})\}.
\end{aligned} \tag{14.17}$$

In this expression, inequality (a) follows from the fact that $\gamma_2(m, m') \leq 1$ for any h , m , and m' ; inequality (b) comes from the fact that $\sum_m P(m|k, \mathbf{z}) = 1$ for any k and \mathbf{z} ; and inequality (c) comes from the fact that

$$\sum_k P(k|\mathbf{z}) \gamma_1(k, k') \leq \max_{k \in \mathcal{K}} \{P(k|\mathbf{z})\}, \tag{14.18}$$

since only one term of $\gamma_1(k, k')$ is 1, and all the remaining terms are zero. \square

This result shows that, after receiving \mathbf{Z} , the optimal strategy of the opponent is to choose the most likely key. With \mathbf{Z} , the opponent gains an amount $I(K; \mathbf{Z})$ of information about the key, and thus can use this information to choose k that maximizes $P(k|\mathbf{z})$. From Eq. (14.12), we have that

$$I(K; \mathbf{Z}) \leq n\epsilon. \tag{14.19}$$

The inequality in Eq. (14.19) is not enough to analyze Eq. (14.17) for the following two reasons. First, though ϵ is small, $n\epsilon$ might go to infinity as n grows, and hence the opponent may eventually gain a sufficient amount of information about the key. This point has been pointed out in [19–21]. The second reason is that there is a maximization in the summand in Eq. (14.17), which means that we need to consider the worst case scenario, whereas $I(K; \mathbf{Z})$ is an average quantity. Actually, this fact is exploited in [1] and [5] to derive lower bounds by replacing this maximization with an averaging, which readily gives us a lower bound and is more amenable to analysis.

In the following section, we borrow techniques from [20] and [22] to analyze this term.

14.4.3 Bounds

We begin with some definitions. Let \mathcal{C} be a codebook for the wiretap channel, and let $\tilde{P}(\mathbf{x}, \mathbf{z})$ be the joint distribution on $\mathcal{C} \times \mathcal{Z}^n$. We denote by $Q(\mathbf{z})$ the marginal distribution of \mathbf{z} when the input distribution is limited to, and is uniform on, \mathcal{C} , and by

$$P(\mathbf{x}|\mathbf{z}) = \tilde{P}(\mathbf{x}, \mathbf{z}) / Q(\mathbf{z})$$

the conditional distribution of \mathbf{X} given $\mathbf{Z} = \mathbf{z}$.

Let $\{\mathcal{C}_1, \dots, \mathcal{C}_N\}$ be a partition of \mathcal{C} , and denote this partition as a mapping, i.e., $f : \mathcal{C} \rightarrow \{\mathcal{C}_1, \dots, \mathcal{C}_N\}$. Also denote by Q_k the conditional distribution of \mathbf{Z} when the input distribution is uniform on \mathcal{C}_k , i.e.,

$$Q_k(\mathbf{z}) = \sum_{\mathbf{x} \in \mathcal{C}_k} \tilde{P}(\mathbf{x}, \mathbf{z}) / P(\mathcal{C}_k).$$

Define

$$d_{av}(f) = \sum_{k=1}^N P(\mathcal{C}_k) d(Q_k, Q),$$

with

$$d(Q_k, Q) = \sum_{\mathbf{z} \in \mathcal{Z}^n} |Q_k(\mathbf{z}) - Q(\mathbf{z})|.$$

Here $d(Q_k, Q)$ is the \mathcal{L}_1 (i.e., variational) distance between the two distributions Q_k and Q . When $d(Q_k, Q)$ is zero, the opponent cannot distinguish between the uniform input distributions on \mathcal{C}_k and \mathcal{C} by observing only the channel output.

Intuitively, if $d_{av}(f)$ can be made arbitrarily small by appropriate choice of \mathcal{C} and f , the receiver gains no information about the subset \mathcal{C}_k from which the transmitted codeword \mathbf{x} comes, given the channel output \mathbf{z} .

We need the following lemma from [20].

Lemma 2 ([20]) Consider a wiretap channel $\mathcal{X} \rightarrow (\mathcal{Y}, \mathcal{Z})$, and choose $\delta > 0$. Suppose $\mathcal{T}_P \subset \mathcal{X}^n$ is a type class with $P(x)$ bounded away from 0, and such that $I(X; Y) > I(X; Z) + 2\delta$. Then, there exist a codebook \mathcal{C} with size $|\mathcal{C}| = 2^{n[I(X; Y) - \delta]}$, drawn from \mathcal{T}_P , and equal-size disjoint subsets $\mathcal{C}_1, \dots, \mathcal{C}_N$ of \mathcal{C} with

$$N \leq 2^{n[I(X; Y) - I(X; Z) - 2\delta]},$$

such that $\mathcal{C} = \bigcup_{k=1}^N \mathcal{C}_k$ is the codeword with exponentially small average probability of error for the main channel $\mathcal{X} \rightarrow \mathcal{Y}$. Moreover, the partition function $f : \mathcal{C} \rightarrow \{1, \dots, N\}$ of \mathcal{C} with $f^{-1}(k) = \mathcal{C}_k, k = 1, \dots, N$ has exponentially small $d_{av}(f)$ for the distribution \tilde{P}_C defined on $\mathcal{C} \times \mathcal{Z}^n$ by

$$\tilde{P}_C(\mathbf{x}, \mathbf{z}) = \frac{1}{|\mathcal{C}|} P(\mathbf{z}|\mathbf{x}), \mathbf{x} \in \mathcal{C}, \mathbf{z} \in \mathcal{Z}^n.$$

Furthermore, $I(N; \mathbf{Z})$ is exponentially small. □

Our main result is the following theorem.

Theorem 3 If the secrecy capacity of the wiretap channel is nonzero, then there exist constants $c > 0$ and $\beta > 0$ so that

$$2^{-H(K)} \leq P_D \leq 2^{-H(K)} + c \exp^{-n\beta},$$

if n is sufficiently large. In particular, if the codeword length n goes to infinity, then $P_I = P_S = 2^{-H(K)}$, and hence, $P_D = 2^{-H(K)}$.

Proof To obtain a lower-bound, we can consider the situation in which the opponent guesses the value of the key. If the guess is correct, the opponent can invoke any attack and the attack will be successful. The probability that the opponent guesses the value of the key correctly is $2^{-H(K)}$. This provides a lower bound.

To prove the upper-bound provided in the theorem, we need to show that the success probability of the opponent's attack with any strategy is upper bounded by the bound provided in the theorem, if we use the authentication scheme proposed in the current work with code generated according to Lemma 2. More specifically, we choose $\delta > 0$, and let P_X be a type of \mathbf{X} satisfying $I(X; Y) > I(X; Z) + 2\delta$. Denote by \mathcal{T}_P the set of \mathbf{x} 's having type P_X . Since the source-wiretapper channel is not less-noisy than the main channel, such a P_X exists.

Now choose n_1 and n_2 such that

$$|\mathcal{K}| \leq 2^{n_1[I(X; Y) - I(X; Z) - 2\delta]},$$

and

$$|\mathcal{K}||\mathcal{M}| \leq 2^{n_2[I(X; Y) - \delta]},$$

and then choose $n > \max\{n_1, n_2\}$. (n also needs to satisfy other conditions specified later.) Let \mathcal{C} and \mathcal{C}_k , $k = 1, \dots, |\mathcal{K}|$ be the codebook and corresponding partition satisfying the conditions of Lemma 2. That is, for this \mathcal{C} and f , there is an $\alpha > 0$ such that

$$d_{av}(f) \leq \epsilon = \exp\{-n\alpha\}. \quad (14.20)$$

When the key is k , the transmitted codeword comes from \mathcal{C}_k . The receiver will accept any signal $\hat{\mathbf{y}}$ that can be decoded into a codeword belonging to the subset corresponding to k . It is easy to see that $P_I = 1/|\mathcal{K}|$.

To analyze the substitution attack, we divide all possible output sequences at the opponent \mathbf{z} into two subsets: \mathcal{O} and \mathcal{O}^c . If $\mathbf{z} \in \mathcal{O}$, $\max_{k \in \mathcal{K}} P(k|\mathbf{z})$ is much larger than $1/|\mathcal{K}|$. Hence, if the opponent observes a sequence $\mathbf{z} \in \mathcal{O}$, the success probability of a substitution attack will be high. On the other hand, if $\mathbf{z} \in \mathcal{O}^c$, $\max_{k \in \mathcal{K}} P(k|\mathbf{z})$ is close to $1/|\mathcal{K}|$. Thus, if the opponent observes a sequence $\mathbf{z} \in \mathcal{O}^c$, the opponent does not gain any information about the key from the output. We show that if the source uses a code with exponentially small $d_{av}(f)$, the probability that the opponent will observe $\mathbf{z} \in \mathcal{O}$ is exponentially small. Thus, almost all the sequences \mathbf{z} have the property that $\max_{k \in \mathcal{K}} P(k|\mathbf{z})$ is close to $1/|\mathcal{K}|$. Simple calculation then shows that P_S is arbitrarily close to $1/|\mathcal{K}|$. For the impersonation attack, the optimal strategy for the opponent is to chooses a codeword at random, and hence P_I is $1/|\mathcal{K}|$.

Please refer to [23] for technical details. □

Remark Theorem 3 implies that the opponent is reduced to guessing the key, which essentially means it has been defeated.

From Theorem 3, one can see that for a given key size $|\mathcal{K}|$, the success probability of the opponent's attack can be made to be arbitrarily close to $1/|\mathcal{K}|$ by increasing the length of the code n . This bound is much smaller than the bound for the noiseless model. Furthermore, by providing an upper-bound, we are assured that the success probability of the opponent is limited.

14.5 Authentication of Multiple Messages

In this section, we consider the situation in which the same key K is used to authenticate a sequence of J messages M_1, \dots, M_J , one per time slot. As discussed in Sect. 14.2, the authentication of multiple messages with the same key under the noiseless model has been studied in [5] and [7–9]. These results suggest that, after several rounds of authentication, the opponent may be able to obtain almost all the information about the key, and hence, may be able to choose an attack with a high success probability. On the other hand, in the following we show that with a noisy channel model, one can limit the information leaked to the opponent, and thus, the success probability of the opponent will not increase even by observing more packets. In the current work, we do not need to make either of the two assumptions made in the noiseless model (i.e., all messages can be the same, as can all the authentication schemes). The channel noise renders the output at the opponent to be almost independent of the input, and hence the success probability of the replay attack or any other attack is bounded, as we argue next.

We use the same scheme as for the single message case; that is, the source transmits the message and key using a wiretap channel code. More specifically, the source uses the same code generated as in Lemma 2, with $|\mathcal{K}|$ subsets, each corresponding to a key. Also, each subset contains $|\mathcal{M}|$ bins, each corresponding to a message. In block j , if the intended message is m_j , the source randomly chooses a codeword \mathbf{x}_j from the m_j th bin in the k th subset using a uniform distribution. The source then transmits \mathbf{x}_j over the channel. The opponent receives \mathbf{z}_j with probability

$$P(\mathbf{z}_j | \mathbf{x}_j) = \prod_{t=1}^n P(z_j(t) | x_j(t)).$$

The receiver receives \mathbf{y}_j . If the opponent does not initiate any attack, then

$$P(\mathbf{y}_j | \mathbf{x}_j) = \prod_{t=1}^n P(y_j(t) | x_j(t)).$$

On the other hand, if the opponent chooses to attack, then the value of \mathbf{y}_j depends on the opponent's attack strategy. At each time slot, the receiver performs jointly typical set decoding and obtains an estimate $\hat{\mathbf{x}}_j$ based only on \mathbf{y}_j , and then sets m'_j and k' to be the bin index and subset index associated with $\hat{\mathbf{x}}_j$. If k' is the same as the key that the receiver knows, then the message is accepted as authentic; otherwise,

the message is rejected. As before, we use $(m'_j, k') = g(\mathbf{y}_j)$ as the decoding process at the receiver.

To initiate an impersonation attack in block j , the opponent can use the information gained through $\mathbf{z}_1, \dots, \mathbf{z}_{j-1}$. Let $h_{j, im}$ be the strategy employed by the source that maps $\mathbf{z}_1, \dots, \mathbf{z}_{j-1}$ to $\mathbf{y}_{o, j}$. We also denote by

$$(m'_j, k') = g(\mathbf{y}_{o, j}) = g(h_{j, im}(\mathbf{z}_1, \dots, \mathbf{z}_{j-1}))$$

the decoded message and key at the destination. For each $(\mathbf{z}_1, \dots, \mathbf{z}_{j-1})$, the opponent will adopt a strategy $h_{j, im}$ so that the following probability is maximized:

$$\sum_{k \in \mathcal{K}} P(k|\mathbf{z}_1, \dots, \mathbf{z}_{j-1}) \gamma_1(k, k'),$$

in which $\gamma_1(k, k')$ is the indicator function defined in Sect. 14.4. Hence, the success probability of the impersonation attack after receiving $j-1$ rounds of transmission is

$$\begin{aligned} P_{I, j} &= \sum_{\mathbf{z}_1, \dots, \mathbf{z}_{j-1}} P(\mathbf{z}_1, \dots, \mathbf{z}_{j-1}) \sup_{h_{j, im}} \left\{ \sum_{k \in \mathcal{K}} P(k|\mathbf{z}_1, \dots, \mathbf{z}_{j-1}) \gamma_1(k, k') \right\} \\ &\leq \sum_{\mathbf{z}_1, \dots, \mathbf{z}_{j-1}} P(\mathbf{z}_1, \dots, \mathbf{z}_{j-1}) \max_{k \in \mathcal{K}} \{P(k|\mathbf{z}_1, \dots, \mathbf{z}_{j-1})\}. \end{aligned} \quad (14.21)$$

The inequality follows from the same reasoning as that used to obtain Eq. (14.18).

The opponent can also choose to invoke a substitution attack after receiving the j th transmission, i.e., it changes the content of the j th packet and sends it to the destination. Let $h_{j, sb}$ be the strategy employed by the source that maps $\mathbf{z}_1, \dots, \mathbf{z}_j$ to $\mathbf{y}_{o, j}$. We also denote by $(m'_j, k') = g(\mathbf{y}_{o, j}) = g(h_{j, sb}(\mathbf{z}_1, \dots, \mathbf{z}_j))$ the decoded message and key at the destination after the opponent's attack.

The attack is successful if $m'_j \neq m_j$ and $k' = k$. For each possible observation $(\mathbf{z}_1, \dots, \mathbf{z}_j)$, the opponent will adopt a strategy $h_{j, sb}$ so that the following probability is maximized:

$$\sum_{m_j, k} P(m_j, k|\mathbf{z}_1, \dots, \mathbf{z}_j) \gamma_2(m_j, m'_j) \gamma_1(k, k'),$$

in which γ_1 and γ_2 are defined as in Sect. 14.4.

Hence, the success probability of the j th substitution attack $P_{S, j}$ is

$$P_{S, j} = \sum_{\mathbf{z}_1, \dots, \mathbf{z}_j} P(\mathbf{z}_1, \dots, \mathbf{z}_j) \sup_{h_{j, sb}} \left\{ \sum_{m_j, k} P(m_j, k|\mathbf{z}_1, \dots, \mathbf{z}_j) \gamma_2(m_j, m'_j) \gamma_1(k, k') \right\}.$$

With regard to this quantity, we have the following result.

Lemma 3 *The success probability of any substitution attack is bounded as follows*

$$P_{S, j} \leq \sum_{\mathbf{z}_1, \dots, \mathbf{z}_j} P(\mathbf{z}_1, \dots, \mathbf{z}_j) \max_{k \in \mathcal{K}} \{P(k|\mathbf{z}_1, \dots, \mathbf{z}_j)\}. \quad (14.22)$$

□

Note that Eqs. (14.21) and (14.22) are valid for any attack strategy of the opponent, including the replay attack mentioned above. Also note that Eqs. (14.21) and (14.22) have similar forms. Hence, one can analyze these terms in a unified framework. The bounds for $P_{I,j}$ follow similarly.

Theorem 4 *If the secrecy capacity of the wiretap channel is nonzero, then there exist constants $c_m > 0$ and $\beta_1 > 0$ so that*

$$2^{-H(K)} \leq P_D \leq 2^{-H(K)} + c_m \exp^{-n\beta_1},$$

if n is sufficiently large. In particular, if the codeword length n goes to infinity, then $P_D = 2^{-H(K)}$.

Proof We first show that the mutual information between the key and observations at the opponent in the j blocks is exponentially small. Using a result relating divergence and \mathcal{L}_1 distance, it is then shown that $d_{av}(f)$ with a proper definition is exponentially small. We then follow the same steps as that in the proof of Theorem 3 to show the bounds. Please refer to [23] for details. \square

From Theorem 4, we see that one can properly exploit the existence of channel noise to significantly enhance the performance of authentication schemes.

14.6 Conclusions

In this chapter, we have reviewed existing results for message authentication under a noiseless model. We have also developed a theory of message authentication over noisy channels. Information theoretic lower and upper bounds on the cheating probability in the single message authentication scenario have been derived. Remarkably, these bounds have been shown to coincide, resulting in a complete characterization of the fundamental limits on authentication over noisy channels. We have also derived the corresponding bounds for the multiple message authentication case and have shown that they match. Interestingly, our results imply that the key information can be used to protect against various attacks simultaneously. We have further shown that, compared with the classical authentication model in which the channel is assumed to be noiseless, the opponent's success probability is largely reduced in both scenarios.

Exploiting other characteristics of channels, such as multi-path fading, to facilitate message authentication is an interesting avenue for further research. Also, developing authentication techniques for the case in which the source-opponent channel is less noisy than the main channel remains an open problem. Extending our study to more complicated scenarios such as insider cheating or group authentication is of significant practical interest as well.

Acknowledgement This work was partly performed while Hesham El Gamal was visiting Nile University, Cairo, Egypt. This research was supported in part by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637, and CCF-07-28208.

References

- [1] Simmons, G. J.: Authentication theory/coding theory, in *Proceedings of CRYPTO 84 on Advances in Cryptology*, (New York, NY, USA), pp. 411–431, Springer-Verlag Inc., Aug. 1985.
- [2] Boneleit, C. G.: The NTMAC for authentication of noisy messages, *IEEE Trans. Inf. Forensics Secur.*, vol. 1, pp. 35–42, Mar. 2006.
- [3] Liu, Y. and Boneleit, C. G.: The CRC-NTMAC for noisy message authentication, *IEEE Trans. Inf. Forensics Secur.*, vol. 1, pp. 517–523, Dec. 2006.
- [4] Simmons, G. J.: A survey of information authentication, in *Proceedings of the IEEE*, vol. 76, pp. 603–620, May 1988.
- [5] Maurer, U. M.: Authentication theory and hypothesis testing, *IEEE Trans. Inf. Theory*, vol. 46, pp. 1350–1356, July 2000.
- [6] Johannesson, R. and Sgarro, A.: Strengthening Simmons' bound on impersonation, *IEEE Trans. Inf. Theory*, vol. 37, pp. 1182–1185, July 1991.
- [7] Fak, V.: Repeated use of codes which detect deception, *IEEE Trans. Inf. Theory*, vol. 25, pp. 233–234, Mar. 1979.
- [8] Rosenbaum, U.: A lower bound on authentication after having observed a sequence of messages, *J. Cryptol.*, vol. 6, pp. 135–156, Mar. 1993.
- [9] Smeets, B.: Bounds on the probability of deception in multiple authentication, *IEEE Trans. Inf. Theory*, vol. 40, pp. 1586–1591, Sept. 1994.
- [10] Stinson, D. and Wei, R.: Bibliography on authentication codes, available at "<http://www.cacr.math.uwaterloo.ca/dstinson/acbib.html>"
- [11] Johansson, T.: Lower bounds on the probability of deception in authentication with arbitration, *IEEE Trans. Inf. Theory*, vol. 40, pp. 1573–1585, Sep. 1994.
- [12] Desmedt, Y. and Yung, M.: Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks, in *Proceedings of International Cryptology Conference*, (Santa Barbara, CA), pp. 177–188, 1990.
- [13] Boyd, C.: *Cryptography and Coding*. Oxford, UK: Clarendon Press, 1989.
- [14] Desmedt, Y.: Threshold cryptography, *Eur. Trans. Telecomm.*, vol. 5, pp. 449–457, July 1994.
- [15] Dijk, M. V., Gehrmann, C. and Smeets, B.: Unconditionally secure group authentication, *Des. Codes Cryptogr.*, vol. 14, pp. 281–296, 1998.
- [16] Shamir, A.: How to share a secret, *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979.
- [17] Wyner, A. D.: The wire-tap channel, *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- [18] Csiszar, I. and Korner, J.: Broadcast channels with confidential messages, *IEEE Trans. Inf. Theory*, vol. 24, pp. 339–348, May 1978.
- [19] Bennett, C. H., Brassard, G., Crepeau, C. and Maurer, U. M.: Generalized privacy amplification, *IEEE Trans. Inf. Theory*, vol. 41, pp. 1915–1923, Nov. 1995.
- [20] Csiszar, I.: Almost independence and secrecy capacity, *Probl. In. Transm.*, vol. 32, pp. 40–47, Jan. 1996.
- [21] Maurer, U. M. and Wolf, S.: Information-theoretic key agreement: From weak to strong secrecy for free, in *Proceedings of Advances in Cryptology-EUROCRYPT*, (Bruges (Brugge), Belgium), pp. 356–373, May 2000.
- [22] Ahlswede, R. and Csiszar, I.: Common randomness in information theory and cryptography, Part II: CR capacity, *IEEE Trans. Inf. Theory*, vol. 44, pp. 225–240, Jan. 1998.
- [23] Lai, L., El Gamal, H. and Poor, H. V.: Authentication over noisy channels, *IEEE Trans. Inf. Theory*, vol. 55, pp. 906–916, Feb. 2009.

Chapter 15

Trusted Cooperative Transmissions: Turning a Security Weakness into a Security Enhancement*

Yan Lindsay Sun and Zhu Han

15.1 Introduction

Since the invention of wireless telegraphy, the effort to improve wireless channel capacity has never stopped. In the last decade, significant advancement has been made and this advancement has featured two milestones. The first milestone is *Multiple-Input-Multiple-Output (MIMO)* techniques, which create spatial diversity by taking advantage of multiple antennas and improves the wireless channel capacity by an amount on the order of the number of antennas on a wireless device. The second milestone is *cooperative transmission*. Instead of relying on the installation of multiple antennas on one wireless device, cooperative transmission achieves spatial diversity through physical layer cooperation. In cooperative transmission, when the source node transmits a message to the destination node, the nearby nodes that overhear this transmission will “help” the source and destination by relaying the replicas of the message, and the destination will combine the multiple received waveforms so as to improve the link quality. In other words, cooperative transmission techniques utilize nearby nodes as virtual antennas, and mimic the effects of MIMO in achieving spatial diversity. It is well-documented that cooperative transmission can improve channel capacity significantly and has a great potential to improve wireless network capacity [1–5].

Cooperative transmission departs from the traditional point-to-point link abstraction. Whereas early work on cooperative transmission focused on understanding the design choices and performance gain of this new communication technique, recent work is moving towards building the network support required to attain the associated performance gains. The research community is exploring integrating cooperative transmission into cellular, WiMAX, WiFi, Bluetooth, ultra-wideband (UWB), and

Y. L. Sun (✉)
University of Rhode Island
4 East Alumni Ave., Kingston
RI 02881, USA
e-mail: yansun@ele.uri.edu

*Portions of this work were supported by NSF grants CNS-0910461 and CNS-0831315.

ad hoc and sensor networks. Cooperative transmission is also making its way into standards; e.g., IEEE WiMAX standards body for future broadband wireless access has established the 802.16j Relay Task Group to incorporate cooperative relaying mechanisms [6].

The majority of work on cooperative transmission focuses on communication efficiency, including capacity analysis, protocol design, power control, relay selection, and cross layer optimization. In those studies, all network nodes are assumed to be trustworthy. Security threats are not taken into consideration in the process of design, protocol development, and performance evaluation.

- It is well known that malicious nodes can enter many wireless networks by merely transmitting or through node compromise. In cooperative transmission, malicious nodes have the opportunity to serve as *relays* (i.e., the nodes helping the source node by forwarding messages). One means to subvert cooperative communications would involve malicious relays sending arbitrary information to the destination as opposed to correct information.
- Cooperative transmission can also suffer from selfish behavior. When wireless nodes do not belong to the same network or have the same network authority, some nodes may refuse to cooperate with others, e.g., by not working as relay nodes, as a means to preserve their own resources.
- In cooperative transmissions, channel information is often required to perform signal combination and relay selection at the destination. Malicious relays can provide false channel state information, hoping that they will be selected as relays or that the destination will combine the received messages inadequately.

This chapter is dedicated to studying the security issues related to cooperative transmission for wireless communications. Particularly, we will discuss the vulnerabilities of cooperation transmission schemes, evaluate potential network performance degradation due to these vulnerabilities, present an effective way to strengthen the security of cooperative transmission through jointly managing trust and channel estimation, and finally investigate possible advantages of utilizing cooperation transmission to assist other network security protocols.

15.2 Cooperative Transmission and Its Vulnerabilities

To better understand the features of cooperative transmission and its potential vulnerabilities, we will first review the basis of cooperative transmission and provide a reference list for the interested readers. Then, we will discuss the attacks against cooperative transmission and their consequences. Finally, the requirements for defense mechanisms will be presented.

15.2.1 Cooperative Transmission Fundamentals

Cooperative transmission takes advantages of the broadcast nature of wireless channels. Nodes that overhear the transmission between other nodes do not simply ignore

the transmission, but instead serve as “helpers” through additional transmissions. The helpers are formally referred to as relay nodes.

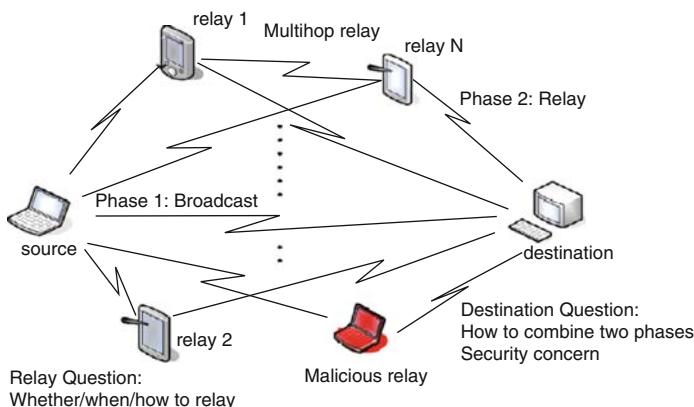
Figure 15.1 illustrates the basic idea and a highly simplified topology with one source node, several relay nodes, and one destination node. Cooperative transmission is conducted in two phases. In Phase 1, the source broadcasts a message to the destination and the relay nodes overhear this message. In Phase 2, the relay nodes send information to the destination (at different time slots or different orthogonal channels), and the destination combines messages from the source and relays.

Next, we present the signal model of the simple one-hop case, as shown in the lower plot in Fig. 15.1. More complicated network topology will be discussed in later sections.

The source node is denoted by s , the destination node is denoted by d , and the relay nodes are denoted by r_i , where i is the index of the relay nodes.

In **Phase 1**, the source s broadcasts a message to destination d and relay nodes r_i . The received signal y_d at destination d and the received signal y_{r_i} at relay r_i can be expressed as

$$y_d = \sqrt{P_s G_{s,d}} h_{s,d} x + n_d, \quad (15.1)$$



One Source-Relay-Destination Example

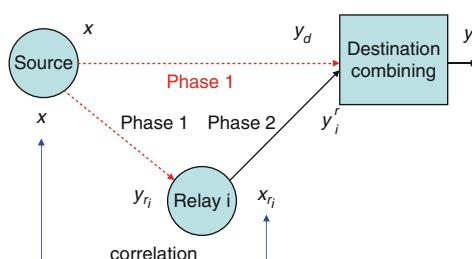


Fig. 15.1 Cooperative transmission system model

and

$$y_{r_i} = \sqrt{P_s G_{s,r_i}} h_{s,r_i} x + n_{r_i}, \quad (15.2)$$

where P_s represents the transmit power at the source, x is the transmitted information symbol with unit energy, $G_{s,d}$ is the channel gain between s and d , G_{s,r_i} is the channel gain between s and r_i , $h_{s,d}$ and h_{s,r_i} are fading factors that are modeled as zero mean and unit variance complex Gaussian random variables, and n_d and n_{r_i} are additive white Gaussian noises (AWGN). Without loss of generality, we assume that the noise power is the same for all the links, denoted by σ^2 . We also assume that the channels are stable over each transmission frame.

When there is no relay, the transmission only contains Phase 1 and is thus referred to as *direct transmission*. In direct transmission, without the help from relay nodes, the signal-to-noise ratio (SNR) at the destination is

$$\Gamma_d = \frac{P_s G_{s,d} E[|h_{s,d}|^2]}{\sigma^2}. \quad (15.3)$$

In **Phase 2**, relay nodes send information to the destination (at different time slots), and the destination combines messages from the source and relays. We examine the *decode-and-forward* (DF) cooperative transmission protocol [1, 3], in which the relays decode the source information received in Phase 1 and send the information to the destination in Phase 2. The received signal at the destination from relay i is

$$y_r^i = \sqrt{P_{r_i} G_{r_i,d}} h_{r_i,d} x_{r_i} + n'_d, \quad (15.4)$$

where x_{r_i} is the decoded signal, $h_{r_i,d}$ is the fading factor modeled as zero mean and unit variance Gaussian random variable, and n'_d is the thermal noise with variance σ^2 .

Due to noise, channel degradation, and estimation errors, the relay's output x_{r_i} may not be the same as the source's output x . Correlation can be used to quantify the difference between x and x_{r_i} . In the ideal case, the correlation should be 1. However, the correlation can be less than 1 due to various reasons. For example, the decoding from y_{r_i} to x_{r_i} may not be accurate due to noise and channel estimation error, or the relay node i may not honestly forward messages.

When only considering the decoding errors, we can derive the correlation between the original signal from the source x and the retransmitted signal from the relay x_{r_i} as

$$E(xx_{r_i}) = 1 - P_e^{s,r_i}, \quad (15.5)$$

where P_e^{s,r_i} is the bit-error-rate (BER) from the source to relay i and represents the difference between x and x_{r_i} .

In Eq. (15.5), only decoding error is counted. When the channel estimation error and nodes' misbehavior are all considered, the correlation becomes extremely difficult to analyze. In practice, this correlation can be determined through some empirical methods.

In this subsection, we have discussed the basic concepts of cooperative transmission. For the readers who are interested in learning advanced topics, we summarize the representative research articles related to cooperative transmissions as follows.

- *Capacity analysis and new cooperative communication protocols:* The major concerns are to analyze how much gain cooperative transmission can bring to a link and to the overall network [7–9], or how to have realistic implementation under practical constraints [10–12].
- *Relay selection and power control:* Among the neighboring nodes, which should be select as relays? After the relay selection, how should the limited power resource be distributed over sources and relays? Those questions are important to cooperative transmission [13, 14] and also extended to multiuser detection and OFDM scenarios [15, 16].
- *Routing protocols:* Cooperative transmission can provide extra routes for network protocols such that the network performance can be significantly improved. The route can be found through the traditional routes [17, 18] or completely from the cooperative routes [19]. It has been shown that sensor network lifetime can significantly be improved [20]. Multi-hop cooperative transmission can be considered as a special case of routing in [21–24].
- *Distributed resource allocation:* Game theoretic approaches are natural ways to achieve distributed cooperative resource allocation. The individual node can use only local information for optimizing cooperative transmission [25].
- *Others:* The cooperative transmission is jointly considered with other layer problems such as with source coding in [26], and with the energy-efficient broadcast problem in [27].

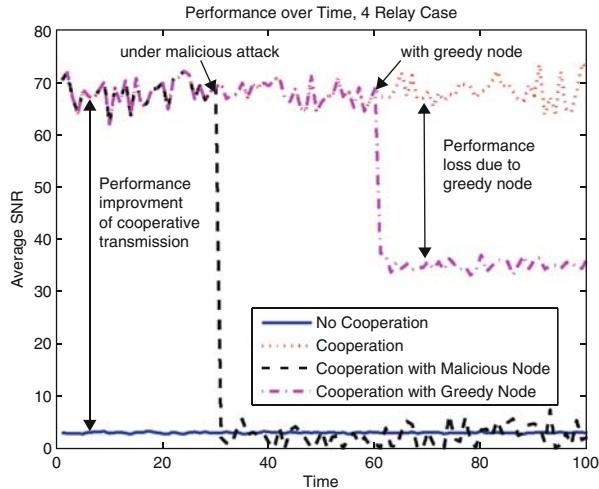
15.2.2 Security Vulnerability in Cooperative Transmission

The security concerns in cooperative transmission have some similarities to the security concerns in other scenarios that require collaboration among distributed entities. The examples of such scenarios include routing in mobile ad hoc networks, data aggregation in sensor networks, and data sharing in peer-to-peer networks. In all above scenarios, if one or several nodes intentionally behave oppositely to what they are expected to do, they (malicious nodes) can greatly damage the system performance. If many nodes only ask others to help them but not help others, they (greedy nodes) can reduce the overall performance and discourage cooperation. Of course, the solutions needed to address security concerns are very different for different application scenarios.

As discussed in Sect. 15.1, for cooperative transmission, we identify the following three types of misbehavior [28, 29].

- *Selfish Silence:* there are selfish nodes that do not relay messages for others in order to reserve their own energy.
- *Malicious Forwarding:* there are malicious nodes that send garbage information to the destination when they serve as relays.

Fig. 15.2 Vulnerability to attacks



- *False Feedback:* malicious nodes report false channel information to make the destination use the forwarded messages inadequately.

Figure 15.2 shows the performance change when cooperative transmission is under attack. The experiment is conducted for an example with 4 relays, and the average SNR at the destination is shown. Several important observations are made.

1. At the beginning without misbehavior, cooperative transmission has significant performance advantage over the case without relays (referred to as direct transmission). This significant performance gain has been the driving force behind the research on cooperative transmission.
2. The effect of malicious relays is devastating. At time 30, one malicious relay starts to send opposite bits, i.e., sending 1 (or 0) if receiving 0 (or 1). The received SNR (black dashed line) immediately drops, even lower than the performance of the direct transmission. Obviously, using relay nodes opens a door to malicious attacks. *Without proper protection, cooperative transmission in its traditional design cannot be applied in the wireless networks with potential malicious network entities.*
3. Selfish nodes degrade performance and undermine the usage of cooperative transmission. At time 60, one relay node becomes selfish and refuses to forward messages for the source node (see the dash-dot red line). With selfish behaviors, cooperative transmission still has performance gain over the direct transmission but the performance gain is largely reduced. *If a large portion of users are selfish, the advantage of cooperative transmission may not be worth of its implementation overhead.*
4. In most cooperative transmission schemes, channel information is required to perform signal combination and relay selection at the destination. The malicious relays can simply provide dishonest feedback about channel status between themselves and the source nodes, hoping that (1) they will be selected as relays or (2) the destination will give a larger weight to the messages forwarded by them.

After getting selected and weighted as an important relay, the malicious node can launch severe attacks. It has been observed that *dishonest feedbacks make the cooperative transmission have even worse performance than the direct transmission.*

15.2.3 Requirements on Defense

Can the security vulnerability inherent in cooperative transmission be fixed? To answer this question, we take a deeper look at the fundamental reasons causing security vulnerability.

First, cooperation among distributed entities is vulnerable to selfish and malicious behaviors. When a network function relies on multiple nodes' collaboration, the performance of the function can be degraded if some nodes are selfish and refuse to collaborate with others, and can be severely damaged if some nodes intentionally behave oppositely to what they are expected to do. For example, the mobile ad hoc routing protocol relies on nodes jointly forwarding packets honestly, and the data aggregation protocol in sensor networks relies on sensors all reporting measured data honestly. It is well known that selfish and malicious behaviors are major threats against the above protocols. Similarly, since cooperative transmission relies on collaboration among source, relay and destination nodes, it can be threatened by selfish and malicious network nodes.

Second, when the decision-making process relies on feedback information from distributed network entities, this decision-making process can be undermined by dishonest feedback. This is a universal problem in many systems. In many wireless resource allocation protocols, transmission power, bandwidth and data rate can all be determined based on channel state information obtained through feedbacks [24, 25, 30]. In cooperative transmission, the relay selection and signal combination process depend on channel state information obtained through feedbacks.

Third, from the view point of wireless communications, traditional representation of channel state information cannot address misbehavior of network nodes. In most cooperative transmission schemes, information about relay channel status is required in relay selection and transmission protocols. However, the traditional channel state information, either SNR or BER, only describes the features of physical wireless channel, but cannot capture the misbehavior of relay nodes.

The above discussion on the causes for security weaknesses provides a starting point for understanding the **primary design goals** of a defense mechanism to patch these weaknesses. A defense mechanism should be able

1. to provide the distributed network entities a strong incentive to collaboration, which suppresses selfish behaviors,
2. to detect malicious nodes and hold them responsible,
3. to provide the cooperative transmission protocols with accurate channel information that (a) reflects both physical channel status as well as the prediction on likelihood of misbehavior and (b) cannot be misled easily by dishonest feedbacks.

15.3 Trust-Assisted Cooperative Transmission

In this section, we present a solution to the security concerns in cooperative transmission. This solution integrates trust management, channel estimation, and signal combination at the destination. Particularly, we will first introduce basis of trust establishment, then discuss the trust-based representation of wireless link quality, and finally present how to perform signal combination at the receiver with trust information.

15.3.1 Trust Establishment Basis

Trust establishment has been recognized as a powerful tool to secure collaboration among distributed entities. It has been used in a wide range of applications for its unique advantages.

- If network entities can evaluate how much they trust other network entities and behave accordingly, three advantages can be achieved. First, it *provides an incentive* for collaboration because the network entities that behave selfishly will have low trust values, which could affect their probabilities of receiving services from other network entities. Second, it can *limit the impact* of malicious attacks because the misbehaving nodes, even before being formally detected, will have less chance to be selected as collaboration partners by other honest network nodes. Finally, it provides a way to *detect malicious nodes* according to trust values.

We chose trust management as a component in the defense mechanism because the purpose of trust management matches perfectly with the requirements for defending cooperative transmission. For interested readers, surveys on trust establishment can be found in [31–33].

Designing a trust establishment method for cooperative transmission is not an easy task. Although there are many trust establishment methods in the current literature, most of them sit in the application layer and few were developed for physical/MAC layer communication protocols. This is mainly due to the high implementation overhead. Trust establishment methods often require monitoring and message exchange among distributed nodes. In physical layer, monitoring and message exchange should be minimized to reduce overhead. Thus, trust establishment should mainly depend on the information that is already available in the physical layer.

While the detailed trust establishment method will be described in a later section, we introduce some trust establishment background here.

A *trust relationship* is always established between two parties for a specific action. That is, one party trusts the other party to perform an action. The first party is often referred to as the subject and the second party as the agent. A formal notation $\{subject : agent; action\}$ is introduced to represent a trust relationship [34]. The *trust value* of $\{subject : agent; action\}$ is one or multiple numerical values that describe how much the subject trust the agent to perform the action.

When the subject can observe the agent's behavior, the subject establishes *direct trust* in the agent based on observations. For example, in the beta-function-based trust model [35], if the subject observes that the agent has behaved well for $(\alpha - 1)$ times and behaved badly for $(\beta - 1)$ times, the subject calculates the direct trust value as $\alpha/\alpha + \beta$. Of course, there are many other methods to calculate direct trust values.

Trust can also be established through third parties. For example, if A and B_1 have established a trust relationship and B_1 and Y have established a trust relationship, then A can trust Y to a certain degree if B_1 tells A its trust opinion (i.e., recommendation) about Y . This phenomenon is called *trust propagation*. Trust propagation becomes more complicated when there are more than one trust propagation path. Through trust propagation, *indirect trust* can be established. The specific ways to calculate indirect trust values are determined by *trust models* [36].

15.3.2 Trust-Based Representation of Link Quality

In cooperative transmission, it is important for the destination to know the channel conditions. Traditionally, channel condition is described by either SNR or BER. However, the traditional representation cannot capture the rich features of relay paths, which can be affected by decoding errors at relays and misbehavior of relay nodes. In this section, we provide a different approach to describing relay channel quality.

The Beta function model is often used in the scenarios where the subject has collected binary opinions/observation about the agent. For example, node B has transmitted $(\alpha + \beta - 2)$ packets to node A . Among them, node A received $(\alpha - 1)$ packets with SNR greater than a certain threshold. These transmissions are considered to be successful. The transmission of other packets is considered to be failure. That is, there are $(\alpha - 1)$ successful trials and $(\beta - 1)$ failed trials. It is often assumed that the transmission of all $(\alpha + \beta - 2)$ packets are independent and a Bernoulli distribution with parameter p governs whether the transmissions succeed or fail. Under these assumptions, given α and β , the parameter p follows a Beta distribution as

$$B(\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1} (1-p)^{\beta-1}. \quad (15.6)$$

It is well known that $B(\alpha, \beta)$ has mean m and variance v as

$$m = \frac{\alpha}{\alpha + \beta}; \quad v = \frac{\alpha\beta}{(\alpha + \beta)^2(\alpha + \beta + 1)}. \quad (15.7)$$

In the context of trust establishment, given α and β values, the trust value is often chosen as the mean of $B(\alpha, \beta)$, i.e., $\alpha/\alpha + \beta$. This trust value represents how much a wireless link can be trusted to deliver packets correctly. In addition, some trust models introduce confidence values associated with trust values [37]. The confidence value is often calculated from the variance of $B(\alpha, \beta)$. The confidence value represents how much confidence the subject has in the trust value.

Due to the physical meaning of the trust values and the close tie between trust and the Beta function, we use the Beta function to represent the link quality. This is equivalent to using trust values and confidence values to describe the link quality. In the rest of chapter, the terms “link quality” and “trust values” are sometimes used interchangeably.

Since an interleaver is often employed in the transceiver and noise is independent over time, we can justify that the successful transmission of different packets is independent, which further justifies the use of Beta distribution. Compared with traditional frame error rate (FER), BER and SNR, the trust-based link quality representation has both advantages and disadvantages. As an advantage, the trust-based link quality can describe the joint effect of wireless channel condition, channel estimation error, and misbehavior of relay nodes. On the other hand, the trust-based link quality cannot describe the rapid changes in channel conditions because the α and β values need to be collected over multiple data packages. Thus, it is suitable for scenarios with slow fading channels or high data rate transmission, in which channel condition remains stable over the transmission time of several packets.

15.3.3 Signal Combination at Receiver

In traditional cooperative transmission schemes, maximal ratio combining (MRC) [38], which only deals with the channel quality between the destination and the relay nodes, is often used to perform signal combination at the receiver. However, when there are possible misbehaving nodes, MRC is not optimal any more.

In this section, we introduce a new signal combination method with 3 steps: (1) calculating the trust-assisted channel quality of all rely paths, which may even contain concatenated rely nodes; (2) calculating the optimal weight factors used in waveform signal combination by solving an optimization problem, in which the received BER is minimized; (3) combining the waveforms using the weight factors and decoding the combined waveform.

Without loss of generality, we assume the modulation method is BPSK. From [38], the BER of BPSK in Rayleigh fading can be approximated by a function of the SNR as

$$\text{BER} = \frac{1}{2} \left(1 - \sqrt{\frac{\Gamma}{1 + \Gamma}} \right), \quad (15.8)$$

where Γ is the SNR. Here FER has a one-to-one mapping with BER given by $\text{FER} = 1 - (1 - \text{BER})^L$, where L is the frame length. Hence, in the rest of chapter, we only mention BER.

15.3.3.1 Waveform Level Combination

In traditional cooperative transmission schemes, maximal ratio combining (MRC) [38] is often used for waveform level combination. Specifically, for one relay case,

remember that y_d is the signal received from the direct path and y_r^i is the signal received from the relay. Under the assumption that the relay can decode the source information correctly, the MRC combined signal with weight factor w_i is

$$y^{mrc} = w_0 y_d + \sum_i w_i y_r^i, \quad (15.9)$$

where $w_0 = 1$ and $w_i = \sqrt{\frac{P_{r_i} G_{r_i, d}}{P_s G_{s, d}}}$. The resulting SNR is given by

$$\Gamma^{\text{MRC}} = \Gamma_d + \sum_i \Gamma_{r_i}, \quad (15.10)$$

where $\Gamma_d = \frac{P_s G_{s, d} E[|h_{s, d}|^2]}{\sigma^2}$ and $\Gamma_{r_i} = \frac{P_{r_i} G_{r_i, d} E[|h_{r_i, d}|^2]}{\sigma^2}$ are SNR of direct transmission and relay transmission, respectively. When channel decoding errors and node misbehavior are present, the MRC is not optimal any more. This is because the received signal quality is not only related to the final link to the destination, but also related to the decoding errors or misbehavior at the relay nodes as shown in Eq. (15.5).

Next, we present a new waveform level combining method based on the Beta function representation of link quality. We first consider the one-relay path case. Depending on whether or not the relay decodes correctly, the combined signal to noise ratio can be written as

$$\Gamma = \begin{cases} \Gamma^c = \frac{\Gamma_d + w_1^2 \Gamma_{r_1} + 2w_1 \sqrt{\Gamma_d \Gamma_{r_1}}}{1 + w_1^2}, & \text{if the relay decodes correctly;} \\ \Gamma^w = \frac{\Gamma_d + w_1^2 \Gamma_{r_1} - 2w_1 \sqrt{\Gamma_d \Gamma_{r_1}}}{1 + w_1^2}, & \text{if the relay decodes incorrectly.} \end{cases} \quad (15.11)$$

Let $B(\alpha_1, \beta_1)$ represent the link quality of the source-relay channel. The SNR at the destination after combination can be optimized by setting the optimal weight vector to combine the relay path as

$$w_1^* = \arg \min_{w_1} \int_0^1 [p \Gamma^c + (1-p) \Gamma^w] B(\alpha_1, \beta_1) dp. \quad (15.12)$$

By differentiating the right hand side of Eq. (15.12), we obtain the optimal combination weight factor as

$$w_1^* = \frac{\Gamma_{r_1} - \Gamma_d + \sqrt{\Gamma_d^2 + \Gamma_{r_1}^2 + 2(1 - 8m_1 + 8m_1^2)\Gamma_d \Gamma_{r_1}}}{2(2m_1 - 1)\sqrt{\Gamma_d \Gamma_{r_1}}}, \quad (15.13)$$

where m_1 is the mean of the relay success decoding probability or the mean of the Beta function $B(\alpha_1, \beta_1)$. When the relay decodes perfectly, i.e., $m_1 = 1$, we have

$$w_1^* = \sqrt{\frac{\Gamma_{r_1}}{\Gamma_d}}, \quad (15.14)$$

which is the same as that in MRC. When $m_1 = 0.5$, we have zero-divide-zero case in Eq. (15.13). In this case, we define $w_1^* = 0$, since the relay decodes completely incorrectly and retransmits completely independent data. As a result, the weight for the relay should be zero, and the system degrades to the direct transmission only case.

For the multiple relay case, assume each relay has the mean of Beta function m_i , SNR Γ_{r_i} , and weight w_i . The overall SNR can be written as

$$\Gamma = \max_{w_i} \sum_{q_i \in \{-1, 1\}} \prod_i Q(q_i, m_i) \frac{(\sqrt{\Gamma_d} + \sum_i q_i w_i \sqrt{\Gamma_{r_i}})^2}{1 + \sum_i w_i^2}, \quad (15.15)$$

where q_i indicates if relay i decodes correctly, and

$$Q(q_i, m_i) = \begin{cases} m_i, & q_i = 1, \text{ decode correctly;} \\ 1 - m_i, & q_i = -1, \text{ decode incorrectly.} \end{cases} \quad (15.16)$$

In this case, the optimal w_i can be calculated numerically by minimizing Eq. (15.15) over parameter w_i . Some numerical methods such as the Newton Method [39] can be utilized.

As a summary, the waveform level combination is performed in the following four steps.

- For each path, calculating m_i values.
- Minimizing the BER in Eq. (15.15) to obtain the optimal weight factors. If there is only one relay path, the optimal weight factor is given in Eq. (15.13).
- Calculating the combined waveform y .
- Decoding the combined waveform y .

15.3.3.2 Extension to Multiple-Hop Relay Scenario

In the previous discussion, we focused on the one-hop relay case, in which the relay path is source-relay-destination. Of course, there may be multiple such relay paths. This is the most common application scenario in cooperative transmission.

It is noted that the relay path may contain several concatenation relay nodes. An example of such relay path is $s - r_a - r_b - d$, where s is the source node, d is the destination, r_a and r_b are two relay nodes. This scenario has been studied in [40, 41].

Considering this general cooperative transmission scenario, we develop an approach to calculate the link quality through concatenation propagation. In particular, let $B(\alpha_1, \beta_1)$ represent the link quality between s and r_a , and $B(\alpha_2, \beta_2)$ represent the link quality between r_a and r_b . If we can calculate the link quality between s and r_b , denoted by $B(\alpha'_r, \beta'_r)$, from $\alpha_1, \beta_1, \alpha_2, \beta_2$, we will be able to use the approach developed in Sect. 15.3.3.1, by replacing (α_r, β_r) with (α'_r, β'_r) . Next, we present the link quality concatenation propagation model for calculating (α'_r, β'_r) .

Let \hat{x} denote the probability that transmission will success through path $s - r_a - r_b$. The cumulative distribution function of \hat{x} can be written as

$$\begin{aligned} CDF(\hat{x}) &= \int \int_0^{\hat{x}=pq} \frac{\Gamma(\alpha_1 + \beta_1)\Gamma(\alpha_2 + \beta_2)}{\Gamma(\alpha_1)\Gamma(\beta_1)\Gamma(\alpha_2)\Gamma(\beta_2)} p^{\alpha_1-1} q^{\alpha_2-1} \\ &\quad \times (1-p)^{\beta_1-1} (1-q)^{\beta_2-1} dp dq. \end{aligned} \quad (15.17)$$

Since it is very difficult to obtain the analytical solution to Eq. (15.17), we find a heuristic solution to approximate the distribution of \hat{x} . Three assumptions are made.

First, even though the distribution of the concatenated signal is not a Beta function, we approximate the distribution of \hat{x} as a Beta distribution $B(\alpha'_r, \beta'_r)$. Let (m_1, v_1) , (m_2, v_2) , and (m'_r, v'_r) represent the (mean, variance) of distribution $B(\alpha_1, \beta_1)$, $B(\alpha_2, \beta_2)$, and $B(\alpha'_r, \beta'_r)$, respectively. The mean and variance of beta distribution is given in Eq. (15.7).

Second, we assume that $m_{12} = m_1 \cdot m_2$. The physical meaning behind this assumption is that $\Pr(\text{successful transmission along } s - r_1 - d) = \Pr(\text{successful transmission between } s - r_1) \cdot \Pr(\text{successful transmission between } r_1 - d)$.

Third, we assume $v_1 + v_2 = v_{12}$. The third assumption means that the “noises” added by two concatenated links are independent and their variance can be added together.

With above assumptions, we can derive that

$$\alpha'_r = m_1 m_2 \left(\frac{m_1 m_2 (1 - m_1 m_2)}{v_1 + v_2} - 1 \right), \quad (15.18)$$

and

$$\beta'_r = (1 - m_1 m_2) \left(\frac{m_1 m_2 (1 - m_1 m_2)}{v_1 + v_2} - 1 \right). \quad (15.19)$$

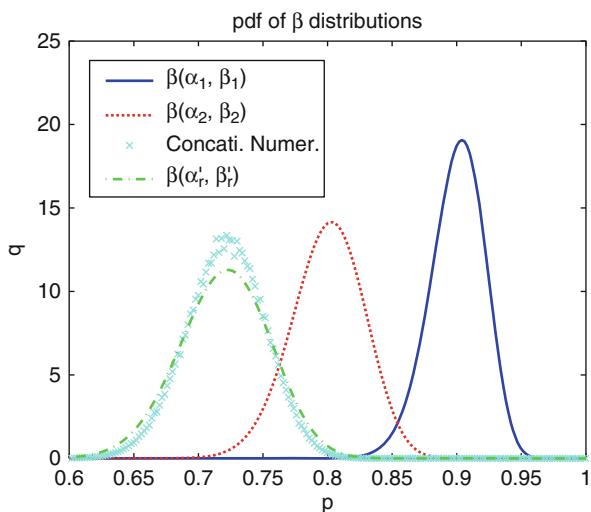
In order to validate the accuracy of this approximation, we examine several numerical examples. One such example is illustrated in Fig. 15.3, which shows the probability density functions of $B(\alpha_1, \beta_1)$ and $B(\alpha_2, \beta_2)$. Here $\alpha_1 = 180$, $\beta_1 = 20$, $\alpha_2 = 140$, and $\beta_2 = 60$. We can see that the means for two Beta functions are 0.9 and 0.7, respectively. Figure 15.3 also shows the distribution of \hat{x} in Eq. (15.17) obtained numerically, and its approximation (i.e., $B(\alpha'_r, \beta'_r)$) calculated from Eqs. (15.18) and (15.19). We can see that the heuristic approximation is a good fit.

As a summary, by using concatenation of Beta functions, the multi-hop relay scenario can be handled.

15.3.4 Defense Against Bad Mouthing Attack

In the *bad mouthing attack*, the relay node does not report accurate link quality between itself and the source node. Instead, the relay node can report a very high link quality, i.e., large α value and very small β value. As a consequence, the m_r value calculated by the destination will be much higher than what it should be. Then, the

Fig. 15.3 Link quality propagation



weight factor calculated in Eq. (15.13) will be larger than what it should be. That is, the information from the lying relay is given a large weight. However, the information from the relay can be wrong. As a result, the bad mouthing attack can reduce the BER performance. To overcome this problem, the Procedure 1 is developed.

It is important to point out that Procedure 1 detects more than the bad mouthing attack. Whenever the m_r value does not agree with the node's real behavior, which may result from maliciousness or severe channel estimation errors, Procedure 1 can detect the suspicious node.

15.3.5 Trust-Assisted Cooperative Transmission

Cooperative transmission can benefit greatly from the link quality information, which describes the joint effects of the channel condition and the misbehavior of untrustworthy relays. Figure 15.4 illustrates the overall design of *trust-assisted cooperative transmission*.

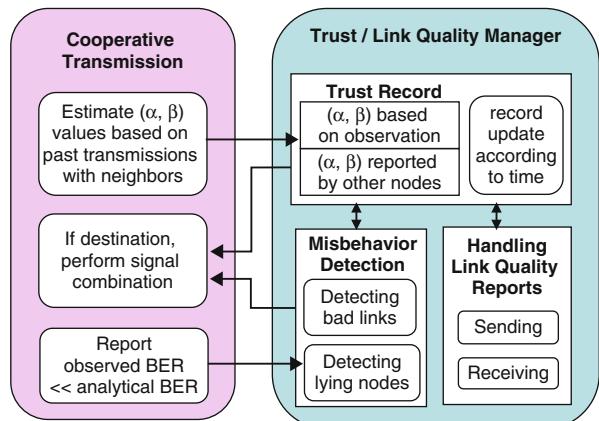


Fig. 15.4 Overview of trust-assisted cooperative transmission

transmission. Here, each node maintains a cooperative transmission (CT) module and a trust/link quality manager (TLM) module. The basic operations are described as follows.

Procedure 1 Defense Against Bad Mouthing Attack

```

1: The destination compares  $BER_{est}$ , which is the BER estimated using Eqs. (15.8) and
   (15.13), and  $BER_{obs}$ , which denotes the BER observed from real communications.
2: if  $BER_{est} - BER_{obs} > threshold_1$  then
3:   if there is only one relay node then
4:     this relay node is marked as suspicious
5:   else
6:     for each relay node do
7:       excluding this relay node, and then performing BER estimation and signal
         combination
8:       if the difference between the newly estimated BER and  $BER_{obs}$  is smaller
         than  $threshold_2$  then
9:         mark this relay as suspicious, and send a warning report about this node to
         others.
10:      end if
11:    end for
12:  end if
13:  For each suspected relay, reduce the  $m_r$  value of the relay node as  $m_r^{new} = m_r^{old} *$ 
     $(1 - \epsilon)$ , where  $\epsilon$  is a small positive number (e.g. choosing  $\epsilon = 0.2$ ),  $m_r^{old}$  is the
    current mean value of the link quality, and  $m_r^{new}$  is the value after adjustment.
14: end if
  
```

- In the CT module, the node estimates the link quality between itself and its neighbor nodes. For example, if node s sends node r_1 a total of N packets and r_1 received K packets correctly, node r_1 estimates the link quality between s and r_1 as $B(K + 1, N - K + 1)$. The estimated link quality information (LQI) is sent to the TLM module. Since the link quality information is estimated directly from observation, it is called *direct LQI*.
- The *trust record* in the TLM module stores two types of the link quality information, i.e., (α, β) values. The first type is direct LQI, estimated by the CT module. The second type is *indirect LQI*, which is estimated by other nodes.
- Each node broadcasts its direct LQI to their neighbors. The broadcast messages, which are referred to as *link quality reports*, can be sent periodically or whenever there is a large change in the LQI.
- Upon receiving the link quality reports from neighbor nodes, one node will update the indirect LQI in its trust record. The indirect LQI is just the direct LQI estimated by other nodes.
- In the TLM module, the links with low quality are detected. The detection criteria is

$$\frac{\alpha}{\alpha + \beta} < threshold_r \text{ and } \alpha + \beta > threshold_c. \quad (15.20)$$

The first condition means that the trust value is lower than a certain threshold. The second condition means that there is a sufficient number of trials to

build this trust. Or, in other words, the confidence in the trust value is higher than a threshold. This detection will affect relay selection. For example, if node s detects the link quality between s and r_1 is lower than a certain threshold, r_1 should not be chosen as a relay between s and other nodes. This detection will also affect signal combination. For example, if node d detects the link quality between r_1 and d is lower than a certain threshold, d should not use the signal received from r_1 in signal combination, even if r_1 has been working as a relay for node d .

- When some malicious nodes launch the bad mouthing attack, the link quality reports may not be truthful. As discussed in Sect. 15.3.4, the CT module detects the suspicious nodes. The information about the suspicious nodes is sent to the TLM module. If a node has been detected as suspicious for more than a certain number of times, the TLM module declares it as a lying node.
- Finally, when the node is the destination node, the node will take link quality information from the trust record and perform signal combination using the approach in Sect. 15.3.3.1.

15.3.5.1 Implementation Overhead

The major implementation overhead for trust-assisted cooperative transmission scheme comes from the transmission of link quality reports. This overhead, however, is no more than the overhead in the traditional cooperative transmission schemes. In the traditional schemes, the destination node needs to know the channel information between the source node and the relay nodes. Channel state information needs to be updated as frequently as the link quality reports. Thus, the trust-assisted scheme has the same level of communication overhead as the traditional schemes.

Besides the communication overhead, the trust-assisted scheme introduces some additional storage overhead. The storage overhead comes from the trust record. Assume each node has M neighbors. The trust record needs to store M direct LQI and M^2 indirect LQI. Each LQI entry contains at most two IDs and (α, β) values. This storage overhead is small. For example, when $M = 10$ and each LQI entry is represented by 4 bytes, the storage overhead is about 440 bytes. This storage overhead is acceptable for most wireless devices.

All calculations in the TLM model and CT module are simple except the optimization problem in Eq. (15.15). This optimization problem is easy to solve when the number of relays is small, since the complexity for the programming method to solve Eq. (15.15) is about the power of 2 to the number of relays. When there is only one relay, the close form solution has been derived.

15.3.6 Performance

We set up the following simulations. The transmission power is 20 dBm, thermal noise is -70 dBm, and the propagation path loss factor is 3. Rayleigh channel and BPSK modulation with packet size $L = 100$ are assumed. The source is located at location $(1000, 0)$ (in meters) and the destination is located at location $(0, 0)$. All

relays are randomly located with left bottom corner at $(0, -500)$ and top right corner at $(1000, 500)$. The unit of distance and location information is one meter.

Each node estimates the link quality between itself and its neighbors periodically. This time period is denoted by B_t . The value of B_t is chosen according to the data rate. B_t should be long enough such that a few packets are transmitted during this time. For the time axis in the figures, one time unit is B_t .

Recall that the link quality reports are sent when relay nodes observe significant change in their link quality. In the experiments, each relay node sends out one link quality report at the beginning of the transmission. If a malicious relay starts to send garbage message, it will not broadcast link quality reports. If a malicious relay starts to send the garbage message and launches the bad mouthing attack, it will send a report containing false link quality information.

In this set of simulations, there are 4 relays. The link quality (mean value $\alpha/\alpha + \beta$) is shown in Fig. 15.5 and the average SNR at the destination is shown in Fig. 15.6. At time 10, one relay starts to send the opposite bits (i.e., sending 1 (or 0) if receiving 0 (or 1)). This could due to severe channel estimation error or maliciousness. Obviously the destination's performance drops significantly. According to Procedure 1, the m_r value of this malfunctioning or malicious relay will be dropped. Within 5 time slots, the destination recognizes the malfunctioning relay because its m_r value has been dropped for several times continually. Then, the destination reduces its weight to zero. As a result, the malfunctioned relay's information is not used in the signal combination process. The other relays' m_r values, which might be affected by the malfunctioning relay, will recover gradually after more packets are transmitted correctly. At time 50, another node leaves the network due to mobility or simply stop forwarding anything (i.e., greedy behavior). It takes about 45 time slots for the destination to remove this relay.

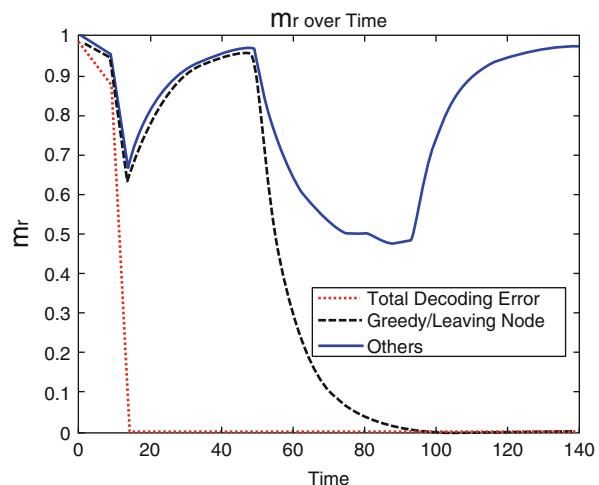
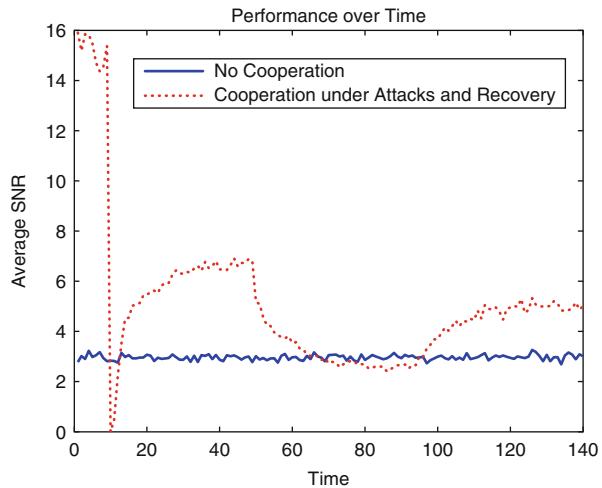


Fig. 15.5 Trust $E(x_{x_r}) = m_r$ over time with estimation error and untrustworthy relays (attacks at time 10 and time 50)

Fig. 15.6 Average SNR over time with estimation error, maliciousness and greediness (attacks at time 10 and time 50)



Several important observations are made.

1. When there are malicious relays, the SNR at the destination drops significantly. It is even worse than not using cooperative transmission. This can be seen by comparing the dashed line and solid line around time 10 in Fig. 15.6.
2. When the trust-assisted scheme is used, the m_r value maintained by the destination can capture the dynamics in the relay nodes. As shown in Fig. 15.5, the m_r values of malicious nodes rapidly drop to zero, and the m_r value of the greedy node drop quickly too. The m_r values of good nodes will be affected at the beginning of the attacks, but can recover even if the attack is still going on.
3. The trust-assisted cooperative transmission scheme results in higher SNR at the destination, compared with the non-cooperative (direct) transmission scheme, except during a very short time at the beginning of the attacks.

We can see that the *cooperative transmission in its original design is highly vulnerable to attacks from malicious relays*. The trust-assisted scheme can greatly reduce the damage of malicious attacks, and partially maintain the performance advantage of cooperative transmission.

15.4 Enhancing Robustness Against Jamming Attacks with Spatial Diversity

Cooperative transmission provides *spatial diversity* because the destination node receives multiple copies of the messages from relays at different locations. In wireless networks, spatial diversity often provides higher robustness against physical layer denial-of-service(DoS) attacks [42, 43].

Intuitively, in cooperative transmission, a message (or waveform) arrives at the destination through multiple physical channels. Thus, when there is a jamming attack, the destination may have a better chance to receive the source node's message in cooperative transmission than in direct transmission. On the other hand, cooperative transmission can significantly improve the SNR at the receiver. As long as the jamming power is not too high, the destination has a better chance to decode the signal correctly.

Of course, not all cooperative transmission schemes have equal anti-jamming capability. The previously discussed trust-assisted scheme can adjust signal combination dynamically according to the channel condition variation caused by various factors including jamming. Therefore, we are interested to see whether the trust-assisted scheme can reduce the damage caused by the jamming attack.

In this set of experiment, we setup the network similar to that in Sect. 15.3.6. One jammer is randomly located within the network area. An outage is reported if the SNR at the destination is lower than a threshold of 0 dB, under which the link is not reliable.

Figure 15.7 shows the outage probability versus jamming power. When using the trust-assisted cooperative transmission scheme, the outage probability is reduced compared with the direct transmission case. In the example of 10 relays, when the jamming power is 200 mW, which is twice of the source transmission power, more than 10% of packets are still correctly received at the destination. Even with 2 relays, there is an obvious reduction in the outage probability.

Figure 15.8 shows that the outage probability decreases as the number of relays increases. For example, to achieve 50% outage with jamming power 100 mW, 20 relay nodes are needed. We can see that trust-assisted cooperative transmission can effectively reduce the outage probability, when the jamming power is comparable

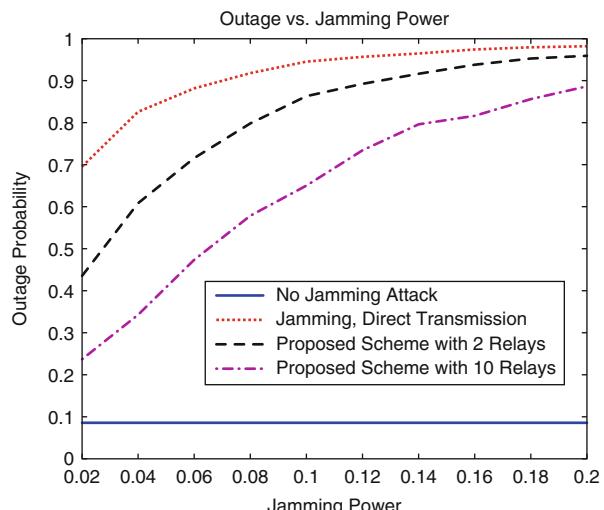
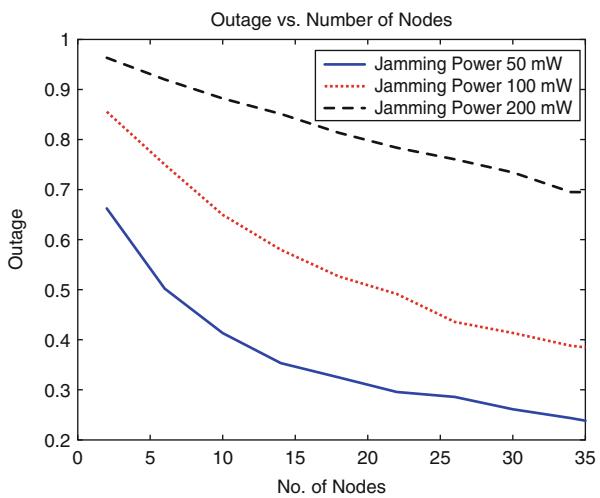


Fig. 15.7 Outage probability vs. jammer's power

Fig. 15.8 Outage probability vs. no. of relays



to the regular transmission power. This is the *advantage of cooperative transmission from the security points of view*.

The discussion in this section is just the first step toward understanding how cooperative transmission can potentially benefit network security. The research along this direction is not limited to jamming attacks. For example, spatial diversity might help to detect misbehaving nodes. Cooperative transmission in physical layer may work together with other mechanisms such as multipath routing to improve network security and robustness. Many open questions can be exploited.

15.5 Conclusions

In this chapter, we have seen that traditional cooperative transmission is very sensitive to malicious insider attacks. When there are malicious relays, it is even better to use direct transmission than to use traditional cooperative transmission. Without proper protection, cooperative transmission is a bad choice from the security points of view. This is largely due to the fact that the SNR-based and BER-based channel information cannot capture greedy/malicious behavior of relay nodes. Fortunately, trust establishment can help to solve the problem. Even under attack, the performance of the trust-assisted cooperative transmission scheme has a large advantage over standard direct transmission. Furthermore, after its vulnerabilities are fixed, cooperative transmission can improve network robustness against jamming attacks. The potential of cooperative transmission in terms of improving network security deserves future investigation.

References

- [1] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity, Part I: system description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927–1938, November 2003.
- [2] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity, Part II: implementation aspects and performance analysis," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1939–1948, November 2003.
- [3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, December 2004.
- [4] J. N. Laneman and G. W. Wornell, "Distributed space-time coded protocols for exploiting cooperative diversity in wireless networks," *IEEE Transactions on Information Theory*, vol. 49, pp. 2415–2525, October 2003.
- [5] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Information Theory*, vol. 25, issue 5, pp. 572–584, September 1979.
- [6] <http://ieee802.org/16/relay/>
- [7] W. Su, A. K. Sadek, and K. J. R. Liu, "SER performance analysis and optimum power allocation for decode-and-forward cooperation protocol in wireless networks," in Proceedings of *IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, LA, March 13–17, 2005.
- [8] A. Host-Madsen, "Upper and lower bounds for channel capacity of asynchronous cooperative diversity networks," *IEEE Transactions on Information Theory*, vol. 50, no. 4, pp. 3062–3080, December 2004.
- [9] A. Host-Madsen, "A new achievable rate for cooperative diversity based on generalized writing on dirty paper," in Proceedings of *IEEE International Symposium Information Theory*, p. 317, Yokohama, Japan, June 2003.
- [10] T. E. Hunter and A. Nosratinia, "Performance analysis of coded cooperation diversity," in Proceedings of *2003 International Conference on Communications (ICC'03)*, vol. 4, pp. 2688–2692, Seattle, WA, May 2003.
- [11] T. E. Hunter, S. Sanayei, and A. Nosratinia, "Outage analysis of coded cooperation," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 375–391, February 2006.
- [12] M. A. Khojastepour, A. Sabharwal, and B. Aazhang, "On the capacity of 'cheap' relay networks," in Proceedings of *37th Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2003.
- [13] J. Luo, R. S. Blum, L. J. Greenstein, L. J. Cimini, and A. M. Haimovich, "New approaches for cooperative use of multiple antennas in ad hoc wireless networks," in Proceedings of *IEEE Vehicular Technology Conference*, vol. 4, pp. 2769–2773, Los Angeles, CA, September 2004.
- [14] Y. Zhao, R. S. Adve, and T. J. Lim, "Improving amplify-and-forward relay networks: optimal power allocation versus selection", in Proceedings of *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.
- [15] Z. Han, X. Zhang, and H. V. Poor, "Cooperative transmission protocols with high spectral efficiency and high diversity order using multiuser detection and network coding", in Proceedings of *IEEE International Conference on Communications*, Glasgow, Scotland, June 2007.
- [16] Z. Han, T. Himsoon, W. Siriwongpairoat, and K. J. Ray Liu, "Energy efficient cooperative transmission over multiuser OFDM networks: who helps whom and how to cooperate", in Proceedings of *IEEE Wireless Communications and Networking Conference*, vol. 2, pp. 1030–1035, New Orleans, LA, March 2005.

- [17] Z. Yang, J. Liu, and A. Host-Madsen, "Cooperative routing and power allocation in ad-hoc networks," in Proceedings of *IEEE Global Telecommunications Conference*, Dallas, TX, November 2005.
- [18] A. E. Khandani, E. Modiano, L. Zheng, and J. Abounadi, "Cooperative routing in wireless networks," *Advances in Pervasive Computing and Networking*, Kluwer Academic Publishers, Eds. B. K. Szymanski and B. Yener, 2004.
- [19] A. S. Ibrahim, Z. Han, and K. J. R. Liu, "Distributed power-efficient cooperative routing in wireless ad hoc networks," in Proceedings of *IEEE Globecom Telecommunication Conference (Globecom)*, Washington DC, November 2007.
- [20] Z. Han and H. V. Poor, "Lifetime improvement in wireless sensor networks via collaborative beamforming and cooperative transmission," *IEE Microwaves, Antennas and Propagation, Special Issue on Antenna Systems and Propagation for Future Wireless Communications*, vol. 1, issue 6, pp. 1103–1110, 2007.
- [21] J. Boyer, D. D. Falconer, and H. Yanikomeroglu, "Cooperative connectivity models for wireless relay networks," *IEEE Transactions on Wireless Communications*, vol. 6, no. 6, pp. 1992–2000, June 2007.
- [22] F. Li, K. Wu, and A. Lippman, "Energy-efficient cooperative routing in multi-hop wireless ad hoc networks," in Proceedings of *IEEE International Performance, Computing, and Communications Conference*, pp. 215–222, Phoenix, AZ, April 2006.
- [23] A. K. Sadek, W. Su, and K. J. R. Liu, "A class of cooperative communication protocols for multi-node wireless networks," in Proceedings of *IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Newyork, June 2005.
- [24] A. Bletsas, A. Lippman, and D. P. Reed, "A simple distributed method for relay selection in cooperative diversity wireless networks, based on reciprocity and channel measurements", in Proceedings of *IEEE Vehicular Technology Conference*, vol. 3, pp. 1484–1488, Stockholm, Sweden, May 2005.
- [25] B. Wang, Z. Han, and K. J. Ray Liu, "Distributed relay selection and power control for multiuser cooperative communication networks using buyer/seller game," in Proceedings of *Annual IEEE Conference on Computer Communications, INFOCOM'07*, Anchorage, AK, May 2007.
- [26] D. Gunduz and E. Erkip, "Joint source-channel cooperation: Diversity versus spectral efficiency," in Proceedings of *2004 IEEE International Symposium Information Theory*, Chicago, IL, June–July 2004, p. 392.
- [27] I. Maric and R. D. Yates, "Cooperative multihop broadcast for wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1080–1088, August 2004.
- [28] Z. Han and Y. Lindsay Sun, "Self-learning cooperative transmission—coping with unreliability due to mobility, channel estimation errors, and untrustworthy nodes," in Proceedings of *IEEE Globecom Telecommunication Conference (Globecom)*, Washington DC, November 2007.
- [29] Z. Han and Y. Sun, "Securing cooperative transmission in wireless communications, channel," in Proceedings of *1st ACM Workshop on Security for Emerging Ubiquitous Wireless Networks*, Philadelphia, PA, August 2007.
- [30] Z. Han and H. V. Poor, "Coalition game with cooperative transmission: a cure for the curse of boundary nodes in selfish packet-forwarding wireless networks," in Proceedings of *5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, (WiOpt07)*, Limassol, Cyprus, April 2007.
- [31] M. Langheinrich, "When trust does not compute—the role of trust in ubiquitous computing," in Proceedings of *the Fifth International Conference on Ubiquitous Computing (UBICOMP'03)*, Seattle, Washington, October 2003.
- [32] Y. Wang and J. Vassileva, "A review on trust and reputation for web service selection," in Proceedings of *the first Int. Workshop on Trust and Reputation Management in Massively Distributed Computing Systems (TRAM'07)*, June 2007.

- [33] A. Jsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," in *Decision Support Systems*, 2005.
- [34] Y. Sun, W. Yu, Z. Han, and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications, Special Issue on Security in Wireless Ad Hoc Networks*, vol. 24, no. 2, pp. 305–317, April 2006.
- [35] A. Jsang and R. Ismail, "The beta reputation system," in Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002.
- [36] A. Jsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, March 2007.
- [37] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in ad-hoc networks," in Proceedings of the ACM Workshop on Wireless Security (WiSE'04), Philadelphia, PA, October 2004.
- [38] J. G. Proakis, *Digital Communications, 3rd edition*, McGraw-Hill, New York, USA, 1995.
- [39] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge University Press, 2006. (<http://www.stanford.edu/~boyd/cvxbook.html>)
- [40] J. Boyer, D. D. Falconer, and H. Yanikomeroglu, "Multihop diversity in wireless relaying channels," *IEEE Transactions on Communications*, vol. 52, no. 10, pp. 1820–1830, October 2004.
- [41] A. K. Sadek, W. Su, and K. J. Ray Liu, "A class of cooperative communication protocols for multi-node wireless networks," in Proceedings of IEEE International Workshop on Signal Processing Advances in Wireless Communications, SPAWC'05, New York, NY, June 2005.
- [42] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Networks*, vol. 20, no. 3, pp. 41–47, May–June 2006.
- [43] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in Proceedings of 2004 ACM Workshop on Wireless Security, pp. 80–89, Philadelphia, PA, October 2004.
- [44] Z. Han and K. J. R. Liu, *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications*, Cambridge University Press, UK, April, 2008.

Chapter 16

Modulation Forensics for Wireless Digital Communications in Frequency-Selective Fading Channels*

W. Sabrina Lin and K. J. Ray Liu

16.1 Introduction

Within the past decades, the explosive development of wireless communication technologies facilitates the transmissions of all types of information over wireless medium: voice, multimedia, data with confidential content, military command and control, no matter where the receivers are. However, the broadcast nature of wireless media also allows everyone within the network to listen to others' signal. From the national security point of view, any suspicious damaging activities should be under surveillance, and friendly signals should be securely transmitted and received, whereas hostile signals must be located, identified and jammed. Thus, it is crucial to develop a forensic scheme that is able to decode the information from the received signals only. The very first step of communication forensic detector is to determine which kind of modulation is in use, which is an intermediate step between signal detection and demodulation.

A modulation forensic detector is not only useful for security or military purposes, but also for many other civilian applications. For example, in cognitive radios, detecting the modulation scheme of the current user helps to identify whether the primary user is presented or not, yet facilitates spectrum sharing. The more accurate the modulation forensic detector is, the more efficient the cognitive radio. Also, the modulation forensic detector can be used in commercial communication systems like intelligent receivers, which yield an increase in the transmission efficiency by reducing the overhead and software defined radios that cope with the variety of communication systems.

W. S. Lin (✉)

ECE Department, University of Maryland, College Park
MD 20742, USA
e-mail: wylin@umd.edu

*Portions of the material have appeared previously in "Modulation Forensics for Wireless Digital Communications," In Proceedings of IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, 2008.

The first step of the modulation forensic detector is preprocessing. In all the prior arts, the preprocessing may include noise reduction, estimation of carrier frequency, symbol period, and signal power, equalization, etc. The second step is a modulation classification. Depending on the classification algorithm chosen in the second step, preprocessing tasks with different levels of accuracy are required; some classification algorithms require precise estimates, while others are less sensitive to unknown parameters. In literature, two categories of classification approaches have been adopted to tackle the problem of modulation forensics. One is the statistics-based pattern recognition approach, in which features are extracted from the received signal and their differences are used for decision making [1–3]. Although the statistics-based approach may not be optimal, it is usually simple to implement, with near-optimal performance, when designed properly. The other category is the likelihood-based approach, in which the likelihood function (LF) of the received signal is computed and a likelihood ratio test is used for detection [4–9]. The likelihood-based method is shown to be asymptotically optimal under additive Gaussian noise in [4], and a theoretical performance bound is derived under the assumption that all communication parameters are known.

Since the forensic detector works blindly by listening to others' signals, the communication parameters are not available in such applications. Most of the previous works identify the digital modulation types in additive white Gaussian noise (AWGN) channels [5], and several more recent works move further to flat fading channels [6–8]. However, the more realistic frequency-selective fading channels for wideband wireless communications have not been addressed in previous works.

In recent years, new technologies for wireless communications have emerged. Orthogonal frequency division multiplexing (OFDM) has become one of the most popular digital modulation schemes due to the efficiency of the OFDM technique to transmit information in frequency selective fading channels without complex equalizers [10, 11]. Multiple-input multiple-output (MIMO) with multi-antenna space-time coding [12] is also widely used in modern wireless communication systems to achieve the spatial diversity. These emerging technologies in wireless communications have raised new challenges for the designers of signal surveillance and intelligence systems, such as, the forensic identifier of discriminating between OFDM and single carrier modulations [13] and identifying signals transmitted from multi-antenna systems.

Most of the prior works only discuss the communication scenario of single-input single-output (SISO) systems, but space-time coding has been very widely used. For the forensic purpose, it is crucial to detect whether it is a MIMO or SISO system, as well as how many transmit antennas are used in the transmitter end, and which space-time coding or modulation scheme is employed.

In this chapter, we propose a SISO/MIMO modulation forensic detector in frequency-selective fading channels. In Sect. 16.2 the modulation forensic detector problem formulation is presented. The forensic detector methodology is proposed in Sect. 16.3. Simulation results are discussed in Sect. 16.4, followed by conclusions in Sect. 16.5.

16.2 Problem Formulation and System Model

In this section we will introduce the modulation forensic problem and system model, including the types of candidate modulation and space-time codes, following by the signal pre-processing.

Figure 16.1 shows the system model of the forensic detector: the original symbols are modulated (and possibly space-time coded) then pass through the fading channel via unknown number of transmit antennas. The input of the modulation forensic detector is the signal directly received from the receiver antenna.

16.2.1 Assumption

We consider a slowly-changing, frequency-selective fading channel with finite-length impulse responses. The transmitter can use single or multiple antennas and the number of transmit antennas is unknown. The additive noise at the receiver's side is modelled as zero-mean white Gaussian noise, in which the signal-to-noise ratio can be estimated. There are only a few possible symbol intervals in the current commercial wireless digital communication protocols, thus in this chapter, we assume the symbol interval is known. Unknown parameters include phase distortion, channel distortion, number of transmit antennas, the types of space-time codes if multiple antennas are used, and the types of modulation.

16.2.2 Received Signal Model

Since the modulation forensic detector does not have any prior information about the communication protocol, the number of receive antennas is unknown. However, as we will show in the following sections, the number of received antennas is not important for our forensic detector, which can identify how many transmit antenna by using one receive antenna only. And once we identify the number of transmit antenna and the space-time code, we can always decode the signal.

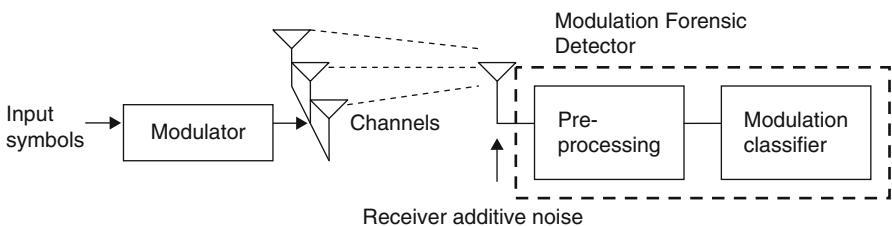


Fig. 16.1 Modulation forensic system model

Therefore, the received baseband signal sequence by one receive antenna can be expressed as

$$r(t) = \sum_{l=1}^q \sum_{k=-\infty}^{\infty} x_k^{(l)} h_l(t - kT) e^{j\theta_l} + n(t), \quad (16.1)$$

where $x^{(l)} = (\dots, x_1^{(l)}, x_2^{(l)}, \dots)^T$ is the transmitted symbol sequence through the l th channel, q is the number of transmit antennas, T is the symbol interval, $h_l(\cdot)$ is the impulse response of the l th channel, θ_l is the phase distortion of the l th channel, and $n(\cdot)$ is the white Gaussian additive noise.

16.2.3 Candidate Space-Time Codes

Severe attenuation in a multipath wireless environment makes it extremely difficult for the receiver to determine the transmitted signal unless the receiver is provided some form of diversity, which means, some self-decodable replica of the transmitted signal is provided to the receiver. Therefore, to utilize the diversity in wireless fading channels, multiple antennas are used at the transmitters. Before the symbols being transmitted through multiple antennas, the space-time encoding should be applied to achieve the full transmit diversity over fading channels. Therefore, it is crucial for a modulation forensic detector to determine how many antennas and which kind of space-time code is used over fading channel. Here we focus on the two most popular full-diversity space-time code: orthogonal block code [12] and diagonal algebraic code [14, 15].

1. *Orthogonal block code*: An orthogonal block code is usually represented by a orthogonal matrix which encodes m' symbols into n streams of length m . The n streams are simultaneously transmitted through n transmit antennas. The m encoded signals within a block are orthogonal to each other, and the code rate is m'/m . For the space-time code to be bandwidth-efficient, the code rate should be as closed to 1 as possible, however, the full-rate real orthogonal codes only exists when $n = m = m' = 2, 4, 8$, and the full-rate complex orthogonal block codes can only be 2×2 . For example, the 4×4 full-rate orthogonal block space-time code is:

$$\begin{bmatrix} \mathbf{x}^{(1)} & \mathbf{x}^{(2)} & \mathbf{x}^{(3)} & \mathbf{x}^{(4)} \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ -s_2 & s_1 & -s_4 & s_3 \\ -s_3 & s_4 & s_1 & -s_2 \\ -s_4 & -s_3 & s_2 & s_1 \end{bmatrix}, \quad (16.2)$$

where s_k , $k = 1, 2, 3, 4$ are information symbols on the modulation constellation. In order to utilize arbitrary number of antennas, the generalized complex orthogonal design is proposed by [16]. Transmission using a complex generalized

orthogonal design is similar to that of a generalized orthogonal design. Maximum-likelihood decoding is analogous to that of full-rate orthogonal scheme and can be done using linear processing at the receiver. For instance, a rate 4/8 code for three transmit antennas is given by

$$\begin{bmatrix} \mathbf{x}^{(1)} & \mathbf{x}^{(2)} & \mathbf{x}^{(3)} \end{bmatrix} = C_{3,1/2} = \begin{bmatrix} s_1 & s_2 & s_3 \\ -s_2 & s_1 & -s_4 \\ -s_3 & s_4 & s_1 \\ -s_4 & -s_3 & s_2 \\ s_1^* & s_2^* & s_3^* \\ -s_2^* & s_1^* & -s_4^* \\ -s_3^* & s_4^* & s_1^* \\ -s_4^* & -s_3^* & s_2^* \end{bmatrix}. \quad (16.3)$$

2. *Diagonal algebraic code*: Diagonal algebraic space-time codes aim to reach the maximum achievable coding rate to sufficiently use the bandwidth, i.e., the code rate is 1. The basic idea of diagonal algebraic space-time codes is that as long as at least one of the encoded streams (x_1, x_2, \dots, x_n) does not experience a deep fade, the receiver can recover the whole original symbol sequence (s_1, s_2, \dots, s_n) . This property is called the full modulation diversity, which can be measured by evaluating the minimum product distance of a given code [17]. At the encoder, the input sequence is first multiplied by a rotation matrix \mathbf{U}_n as in [18, 19] to achieve the full modulation diversity. The diagonal algebraic space-time code of dimension n can be written as follows:

$$\begin{bmatrix} \mathbf{x}^{(1)} & \mathbf{x}^{(2)} & \dots & \mathbf{x}^{(n)} \end{bmatrix} = U_T(s_1, s_2, \dots, s_n) \quad (16.4)$$

For instance, when $n = 4$, the diagonal algebraic space-time code is

$$\begin{bmatrix} \mathbf{x}^{(1)} & \mathbf{x}^{(2)} & \mathbf{x}^{(3)} & \mathbf{x}^{(4)} \end{bmatrix} = \begin{bmatrix} s_1 & s_2 & s_3 & s_4 \\ s_1 & -s_2 & s_3 & -s_4 \\ s_1 & s_2 & -s_3 & -s_4 \\ s_1 & -s_2 & -s_3 & s_4 \end{bmatrix}. \quad (16.5)$$

16.2.4 Candidate Modulation Types

Our modulation forensic detector focuses on a family of phase-shift keying (PSK) modulation based on the following observation: for an arbitrary complex constellation such as PSK, the space-time block codes can be designed to achieve 1/2 of the maximum possible transmission rate for any number of transmit antennas, and the diagonal algebraic space-time codes are proofed to maintain their rate, diversity, and coding gains for all real and complex constellations carved from the complex

integers ring as quadrature-amplitude modulation (QAM). Furthermore, the performance of QAM is the same as QPSK when the channel introduces phase distortion. Therefore, for single antenna modulation types, we discuss about the PSK family including BPSK, QPSK, and 8PSK [20].

16.3 Forensic Detectors

In this section, we will discuss the methodology of the modulation forensic detector. First we introduce the subspace algorithm to jointly estimate the channel coefficients, channel phase distortion and the possible SISO modulation scheme in Sect. 16.3.1. Then based on the estimated channel coefficients and phase distortion, we identify the space-time coding scheme and the number of antennas based on the equalized received signal in Sect. 16.3.2.

16.3.1 SISO Modulation Identification

For frequency-selective fading channels, the first step of the modulation forensics is to recover the transmitted symbol from the received signal. Here we combine the subspace blind equalization algorithm [21] and the likelihood-based approach to identify SISO modulation scheme over frequency-selective fading channels.

Assume there is only one transmit antenna, then the received signal at the modulation forensic detector can be represented as follows:

$$r(t) = \sum_{k=-\infty}^{\infty} s_k h(t - kT) e^{j\theta} + n(t), \quad (16.6)$$

where s_k is an information symbol in an unknown PSK signal constellation S , $h(\cdot)$ is the discrete-time channel impulse response, T is the known symbol interval, θ is the phase distortion, and $n(\cdot)$ is the additive white Gaussian noise with variance N and zero mean. We assume that the impulse response $h(\cdot)$ has finite support, i.e., $h(t) = 0$ for $t \geq JT$, $J \in N$.

In the modulation forensic problem, there are no training sequence to help identify channel coefficients $h(\cdot)$ and recover the transmit symbols s_k , therefore, a blind algorithm should be applied to estimate the channel coefficient and phase distortion in order to recover s_k .

16.3.1.1 Noiseless Environment

To illustrate the insight of algorithm development, first we estimate the transmitted phase-distorted symbols in the noiseless environment (noise variance $N = 0$), and extend the estimation method to the general noisy environment.

Step 1: Estimate the Phase-Distorted Transmit Symbols:

Following the subspace algorithm of [21], we observe and sample the received noiseless signal $r(t)$ in Eq. (16.6) for duration MT by J times of the baud rate, i.e., taking samples at $nT + \delta_1, nT + \delta_2, \dots, nT + \delta_J$, $0 < \delta_1 < \delta_2 < \dots < \delta_J < T$, where the FIR channel has length JT . Therefore, we have JM equations:

$$\begin{aligned} y(j) &= e^{j\theta} s_{J-1} h_j + s_{J-2} h_{J+j} + \dots + s_0 h_{(J-1)J+j}, \\ y(j+J) &= e^{j\theta} s_J h_j + s_{J-1} h_{J+j} + \dots + s_1 h_{(J-1)J+j}, \\ &\vdots \\ &\vdots \\ y(j+J(M-1)) &= e^{j\theta} s_{M+J-2} h_j + s_{M+J-3} h_{J+j} + \dots + s_{M-1} h_{(J-1)J+j}, \end{aligned} \quad (16.7)$$

where

$$\begin{aligned} y(Jn - J + j - 1) &= r(nT + \delta j), \text{ and} \\ h_{Jn+j-1} &= h(nT + \delta j) \quad \forall 1 \leq j \leq J. \end{aligned} \quad (16.8)$$

Let \mathbf{z}_j and \mathbf{s}_j be

$$\begin{aligned} \mathbf{z}_j &= [y(j) \quad y(J+j) \quad y(2J+j) \quad \dots \quad y((M-1)J+j)]^T; \\ \mathbf{s}_j &= [s_j \quad s_{j+1} \quad s_{j+2} \quad \dots \quad s_{M+j-1}]^T, \\ 0 \leq j &\leq J-1. \end{aligned} \quad (16.9)$$

Therefore, we have

$$\mathbf{Z} = e^{j\theta} \mathbf{S} \mathbf{H} \quad (16.10)$$

where

$$\begin{aligned} \mathbf{Z} &= [\mathbf{z}_0 \quad \mathbf{z}_1 \quad \dots \quad \mathbf{z}_{J-2} \quad \mathbf{z}_{J-1}], \\ \mathbf{S} &= [\mathbf{s}_0 \quad \mathbf{s}_1 \quad \dots \quad \mathbf{s}_{J-2} \quad \mathbf{s}_{J-1}], \\ \mathbf{H} &= [\mathbf{h}_1 \quad \mathbf{h}_2 \quad \dots \quad \mathbf{h}_{J-1} \quad \mathbf{h}_J], \text{ where} \\ \mathbf{h}_k &= [h_{J(J-1)+k-1} \quad h_{J(J-2)+k-1} \quad \dots \quad h_{J+k-1} \quad h_{k-1}]^T, \\ 1 \leq k &\leq J. \end{aligned} \quad (16.11)$$

Equation (16.11) tells that for $0 \leq j \leq J-1$,

$$e^{j\theta} \mathbf{s}_j \in \text{span}\{\mathbf{z}_0, \mathbf{z}_1, \dots, \mathbf{z}_{J-1}\}. \quad (16.12)$$

Therefore, for $0 \leq j \leq J-1$, we have

$$e^{j\theta} \mathbf{s}_j = \sum_{k=0}^{J-1} \lambda_k^{(j)} \mathbf{x}_k, \quad (16.13)$$

where $\lambda_k^{(j)}$ is the element on the k th row and j th column of the matrix \mathbf{H}^{-1} .

Note that, from the definition of \mathbf{s}_j in Eq. (16.9), the bottom $M - 1$ elements of \mathbf{s}_j is the same as the top $M - 1$ elements of \mathbf{s}_{j+1} . Let u_j and v_j be the bottom $M - 1$ and top $M - 1$ elements of \mathbf{z}_j , respectively, then we have

$$\Phi\lambda = 0, \quad (16.14)$$

where

$$\lambda = \left[\lambda_0^{(0)} \dots \lambda_{J-1}^{(0)} \lambda_0^{(1)} \dots \lambda_{J-1}^{(1)} \dots \lambda_0^{(J-1)} \dots \lambda_{J-1}^{(J-1)} \right]^T, \quad (16.15)$$

and

$$\Phi_{(M-1)J \times J^2} = \begin{bmatrix} u & v & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & u & v & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & u & v & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & u & v \end{bmatrix}, \quad (16.16)$$

which has totally J block-columns, 0 represents the $M - 1$ by J zero matrix, and

$$\begin{aligned} u &= [u_0 \ u_1 \ \dots \ u_{J-2} \ u_{J-1}], \\ v &= [v_0 \ v_1 \ \dots \ v_{J-2} \ v_{J-1}]. \end{aligned} \quad (16.17)$$

From Eq. (16.14), we know that λ is in the null space of the $(M - 1)J$ by J^2 matrix Φ . If Φ has one-dimensional null space, then λ can be correctly calculated, leading to perfect reconstruction of the phase-distorted transmit symbol sequence $e^{j\theta}\{s_i\}_{i=0}^J$. It has been proved in [21] that if the channel matrix \mathbf{H} is invertible, then

$$P(\Phi \text{ has a one-dimensional null space}) \geq 1 - \frac{1}{(\text{size of the symbol set})^{M-2J}}. \quad (16.18)$$

This means as long as the observation is long enough, the phase-distorted symbol sequence can be recovered with probability 1.

Step 2: SISO Modulation Type Detection:

Given the phase-distorted symbol sequence $\{s'_i\}_{i=0}^J e^{j\theta} \{s_i\}_{i=0}^J$ and the modulation candidate set of size N_{Mod} $\eta = \eta_1, \dots, \eta_{N_{mod}}$, we apply the maximum likelihood hypothesis test to detect the modulation scheme. For every hypothesis H_i that the modulation scheme is η_i , we calculate the likelihood of

$$f(\{s'_i\}_{i=0}^J | \text{modulation type} = \eta_i, \theta), \quad (16.19)$$

and then choose the maximum likelihood hypothesis and the corresponding phase. The likelihood in Eq. (16.19) is very easy to calculate under the noiseless assumption.

Fig. 16.2 Recovered phase-distorted transmit symbols on the constellation plane with $J = 10$, $M = 20$, H being invertible

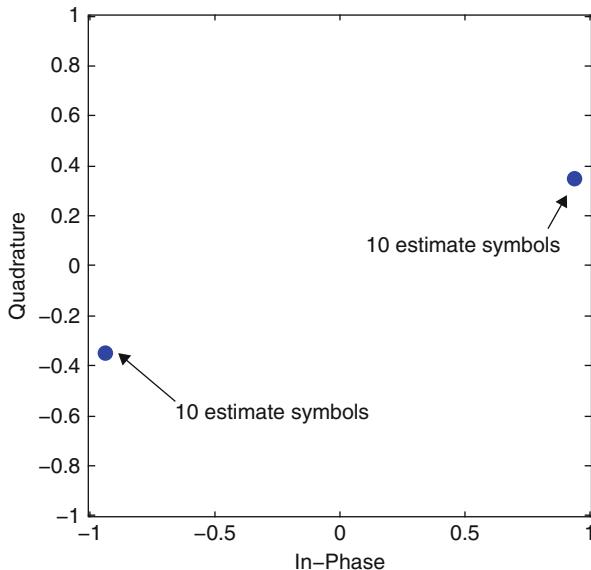


Figure 16.2 shows the simulation result for recovering phase-distorted transmitted symbols on the complex plane where we assume a uniform distributed random phase, BPSK modulation, $J = 10$, observation length $M = 20$, and the channel impulse response

$$h = [-0.02788, 0.009773, 0.04142, 0.0216, -0.06035, \quad (16.20)$$

$$0.08427, 0.3874, 0.5167, 0.152, -0.001258]. \quad (16.21)$$

It is clear that the likelihood of the modulation being BPSK, QPSK, and 8PSK are 2^{-20} , 2^{-40} , 2^{-60} , respectively.

16.3.1.2 Noisy Environment

Here we will discuss how to detect the type of SISO modulation over a frequency-selective fading channel with an additive noise. Different from the noiseless case, the subspace algorithm cannot estimate the phase-distorted transmitted symbols perfectly because the channel matrix \mathbf{H} is very likely to be ill-conditioned. If we use the estimated symbol sequence $e^{j\theta}\{s_i\}_{i=0}^J = \{s'_i\}_{i=0}^J$ to the likelihood detector, due to error propagation, the performance may degrade a lot, especially in the low signal-to-noise (SNR) region. Therefore, instead of estimating $\{s'_i\}_{i=0}^J$, in the noisy environment, we apply the estimated $\{s'_i\}_{i=0}^J$ to identify the fading channel and equalize the received symbols. Then apply the likelihood-based modulation detector to the equalized received symbols.

Step 1: Blind SISO Equalization:

In the noisy situation, the same algorithm as in Sect. 16.3.1.1 can be applied with a small modification in solving for λ . Instead of finding the null space of Φ , we look for the singular vector corresponding to the smallest singular value of Φ . Therefore, we can still estimate $\{s'_i\}_{i=0}^J$ by the same algorithm [21].

Assuming that the received signal is sampled at the baud rate, then we have the following matrix equation:

$$e^{j\theta} \mathbf{Sh} + \mathbf{n} = \mathbf{r}, \quad (16.22)$$

where

$$\mathbf{S} = \begin{bmatrix} s_1 & s_2 & \cdots & s_{J-1} & s_J \\ s_2 & s_3 & \cdots & s_J & s_{J+1} \\ s_3 & s_4 & \cdots & s_{J+1} & s_{J+2} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ s_{M-J+1} & s_{M-J+2} & \cdots & s_{M-1} & s_M \end{bmatrix},$$

$$\begin{aligned} \mathbf{h} &= [h_{J-1}, h_{J-2}, \dots, h_1, h_0]^T, h_i = h(iT), \\ \mathbf{n} &= [n_J, n_{J+1}, \dots, n_{M-1}, n_M]^T, n_i = n(iT), \text{ and} \\ \mathbf{r} &= [r_J, r_{J+1}, \dots, r_{M-1}, r_M]^T, r_i = z(iT). \end{aligned} \quad (16.23)$$

If the channel matrix \mathbf{H} is well-conditioned, we can replace the elements in $e^{j\theta} \mathbf{S}$ by the estimated symbols $\{s'_i\}_{i=0}^J$ to find the least-squares solution for the vector \mathbf{h} which minimizes the norm-square error $\|\mathbf{Sh} - \mathbf{r}\|^2$.

However, the impulse response of a real world channel usually has a very long tail and has a very small magnitude. Near the tail end, the magnitude of the response is very small and so all the last few columns of \mathbf{H} which are obtained by sampling the impulse response near its tails are very close to zero and hence to each other, which makes the channel matrix \mathbf{H} ill-conditioned.

Note that the tail of the impulse response contributes very little to the actual received signal and so we can neglect its contribution to estimating the transmitted symbols. If we neglect the tail, the total length of the impulse becomes much less than it was before. Therefore the effective length of the impulse response is reduced from the original JT to $J'T$. We therefore need to sample the received signal at J' times the baud rate and perform the Basic Subspace algorithm under the assumption that the length of the response is only $J'T$. This will give us an estimate of the transmitted sequence s_k and an estimate of the shortened impulse response \hat{h}_s . We can then use the estimate of the transmitted sequence \hat{s}_k to obtain a very good estimate of the unshortened impulse response by solving the matrix least squares estimation problem of minimizing $\|\mathbf{Sh} - \mathbf{r}\|^2$ over all matrices \mathbf{H} [21].

Step 2: Likelihood-Based SISO Modulation Type Detection:

After we have the estimated channel coefficient for the fading channel, we can apply equalization to the received baseband signal r , and the output of the equalizer sampled by the baud rate can be formulated as follows:

$$\mathbf{r}' = e^{j\theta} \mathbf{s} + \mathbf{n}', \quad (16.24)$$

where \mathbf{n}' is a zero-mean Gaussian random vector with variance N (by assuming equalizer is perfect).

Given the equalized signal in Eq. (16.24), the SISO modulation forensic detector, with the likelihood-based approach, can be formulated as a multiple-composite hypothesis testing problem [22]. Under hypothesis H_i , meaning the i th modulation is employed at the transmitter, where $i = 1, \dots, N_{mod}$, the likelihood function can be computed by estimating the unknown parameter θ . By assuming that the equalized received symbols are statistically independent, under hypothesis H_i , the conditional likelihood function is given by

$$\begin{aligned} f(\mathbf{r}' | \{s_k^{(i)}\}_{k=1}^K, \theta) &= \prod_{k=1}^K \frac{1}{\pi N'} \exp \left\{ -\frac{1}{N'} |r'_k - e^{j\theta} s_k^{(i)}|^2 \right\} \\ &= \frac{1}{(\pi N')^K} \exp \left\{ -\frac{1}{N'} \|\mathbf{r}' - e^{j\theta} \mathbf{s}^{(i)}\|^2 \right\}. \end{aligned} \quad (16.25)$$

Here, the likelihood function is computed by averaging over the unknown signal constellation points $\{s_k^{(i)}\}_{k=1}^K$ and replacing the unknown phase distortion with its respective estimate. Thus, the likelihood function under the i th hypothesis can be written as

$$LF^{(i)}(\mathbf{r}') = E_{\{s_k^{(i)}\}_{k=1}^K} \left[f \left(\mathbf{r}', \tilde{\theta} \mid \{s_k^{(i)}\}_{k=1}^K \right) \right], \quad (16.26)$$

where $E_{\{s_k^{(i)}\}_{k=1}^K} [\cdot]$ is the expectation with respect to the unknown transmitted symbol constellation points and $\tilde{\theta}$ is the unknown phase distortion estimates under the i th hypothesis H_i .

The final decision of modulation scheme \tilde{i} is made based on the maximum likelihood criteria, that is, \tilde{i} satisfies:

$$\tilde{i} = \arg \max_{i=1, \dots, N_{mod}} LF^{(i)}(\mathbf{r}'). \quad (16.27)$$

Since the likelihood function in Eq. (16.26) is computed by using the maximum likelihood estimate of phase distortion, $\tilde{\theta}$ should satisfies:

$$\frac{\partial f(\mathbf{r}' | \{s_k^{(i)}\}_{k=1}^K, \theta)}{\partial \theta} \Big|_{\theta=\tilde{\theta}^{(i)}} = 0. \quad (16.28)$$

By solving Eq. (16.28), we show that

$$\tilde{\theta}^{(i)} = -\frac{j}{2} \ln \left(\frac{\mathbf{s}^{(i)\mathbf{H}} \mathbf{r}}{\mathbf{r}^{\mathbf{H}} \mathbf{s}^{(i)}} \right). \quad (16.29)$$

16.3.2 Space-Time Code Identification

If only a single transmit antenna is used, the SISO modulation forensic detector described in Sect. 16.3.1 can be used to detect the modulation scheme. Then the next question to answer is how to identify the number of transmit antennas? If multiple transmit antennas are used, how to identify the space-time coding scheme?

16.3.2.1 Estimating Number of Transmit Antennas

Here we will propose an algorithm to estimate the number of transmit antennas based on the received signal Eq. (16.1) with unknown q by using the subspace property.

It is easy to prove that if there are multiple transmit antennas, i.e., $q > 1$ in Eq. (16.1), the subspace SISO equalization in Sect. 16.3.1 fails. This implies that the null space of Φ in Eq. (16.16) is not rank 1 in the noiseless case. Furthermore, in the noisy case, the smallest singular value of Φ is relatively large.

The subspace blind equalization can be extended to the multi-antenna case [23]. Similarly, if there are q transmit antennas, the Φ matrix in the MIMO case will have q -dimensional null space when there is no additive noise. Based on this property of the subspace algorithm, our modulation forensic detector estimates the number of transmit antennas by thresholding the singular values of Φ as follows:

- Assume there are q transmit antennas, then calculate the Φ matrix by the subspace algorithm.
- Threshold the singular numbers of Φ by TH , which is a threshold defined by the forensic detector. The TH should vary with SNR. Let q' be the number of singular numbers of Φ that is less than TH .
- If $q' \approx q$, return the number of transmit antenna being q . Otherwise, apply the same estimation procedure on $q + 1$ transmit antennas.

16.3.2.2 Space-Time Code Detection

After estimating the number of transmit antennas, the next step of MIMO modulation detector is to detect the space-time coding scheme. In this subsection, we use the support vector machine to classify the space-time code based on the MIMO-equalized received signal.

If we sample the MIMO-equalized received signal by one received antenna at the baud rate, we will have

$$\mathbf{r}' = \sum_{l=1}^q \mathbf{x}^{(l)} e^{j\theta_l} + n', \quad (16.30)$$

where q is the number of transmit antennas, and θ_l is the phase distortion corresponding to the path from the l th transmit antenna to the receive antenna.

- **Time-domain codeword length estimation:** Since we know how many transmit antennas are used, the codeword length of the block code is the most important information of the space-time code. Here we propose a second moment test to identify the codeword length for orthogonal block space-time codes and diagonal algebraic space-time codes in time domain.

We define the second moment test as

$$M(k, d) = E[r_k'^2 r_{d+k}^2] - E[r_k'^2]E[r_{d+k}^2]. \quad (16.31)$$

Note that the diagonal codes and the orthogonal codes are both block-based. This implies that r_k and r_{d+k} are independent if $d \geq p$, where p is the codeword length in time domain. Therefore,

$$E[r_k'^2 r_{d+k}^2] = E[r_k'^2]E[r_{d+k}^2] \quad \forall d \geq p, \quad (16.32)$$

and hence, $M(k, d) = 0$ for $\forall d \geq p$.

If r_k and r_{d+k} are in the same block, then r_k and r_{d+k} are linearly dependent since they share at least one common symbol. This linear dependency makes $M(k, d) \neq 0$ when r_k and r_{d+k} are in the same block. Without loss of generality, we take the 2×2 orthogonal block code

$$C_2 = \begin{bmatrix} s_1 & s_2 \\ -s_2^* & s_1^* \end{bmatrix} \quad (16.33)$$

as an example, in which the second moment test $M(1, 1)$ is:

$$\begin{aligned} M(1, 1) &= E\left[\left(s_1 e^{j\theta_1} + s_2 e^{j\theta_2}\right)^2 \left(-s_2^* e^{j\theta_2} + s_1^* e^{j\theta_1}\right)^2\right] \\ &\quad - E\left[\left(s_1 e^{j\theta_1} + s_2 e^{j\theta_2}\right)^2\right] E\left[\left(-s_2^* e^{j\theta_2} + s_1^* e^{j\theta_1}\right)^2\right] \\ &= \varepsilon^4 (e^{4j\theta_1} + e^{4j\theta_2} - 4e^{2j(\theta_1+\theta_2)}) \\ &\quad - (s_1^*)^2 (e^{2j\theta_1} + e^{2j\theta_2}) (s_1)^2 (e^{2j\theta_1} + e^{2j\theta_2}) \\ &= -6\varepsilon^4 e^{2j(\theta_1+\theta_2)} \neq 0, \end{aligned} \quad (16.34)$$

where ε^2 is the symbol power.

Based on the above observation, we propose the algorithm of estimating time domain codeword length as follows:

1. Iteratively calculate $M(1, d)$, $d \geq 1$ from $d = 1$, and increase d by 1 for each iteration until $M(1, d) = 0$.
2. Iteratively calculate $M(k', d)$ as the same as the above step; k' is the smallest positive integer satisfying $M(1, k') = 0$.
3. The code length p is the smallest positive integer satisfying $M(k, p) = 0$.

- **SVM classifier:** Now we have the estimated codeword length p and the number of transmit antennas q for the space-time code. Given p , q , there is only finite number of space-time codes and every code has its unique formulation of $\{M(k, d)\}_{k'=1, d=1}^{k'=p-2, d=p-1-k}$. Thus, we construct a support vector machine (SVM) classifier using $\{M(k, d)\}_{k'=1, d=1}^{k'=p-2, d=p-1-k}$ calculated from the received signals r' as the input feature to determine

Once we know the space-time coding scheme, we can decode the received baseband equalized signal into symbol sequence $s^{(i)}$, and perform the same likelihood-based modulation detection as SISO system in Sect. 16.3.1.2.

16.3.3 Overall Forensic Detector Scheme

Figure 16.3 shows the overall methodology of the modulation forensic detector over frequency selective fading channels: upon receiving the baseband signal, first apply the subspace algorithm to determine the number of transmit antennas. If only one transmit antenna is used, apply the SISO equalization following by the likelihood detector. If multiple antennas are used, first determine the codeword length in time domain and then identify the space-time code using SVM as discussed in Sect. 16.3.2. Next apply the space-time decode process to recover the symbol sequence before space-time encoding, and then apply the likelihood modulation detector.

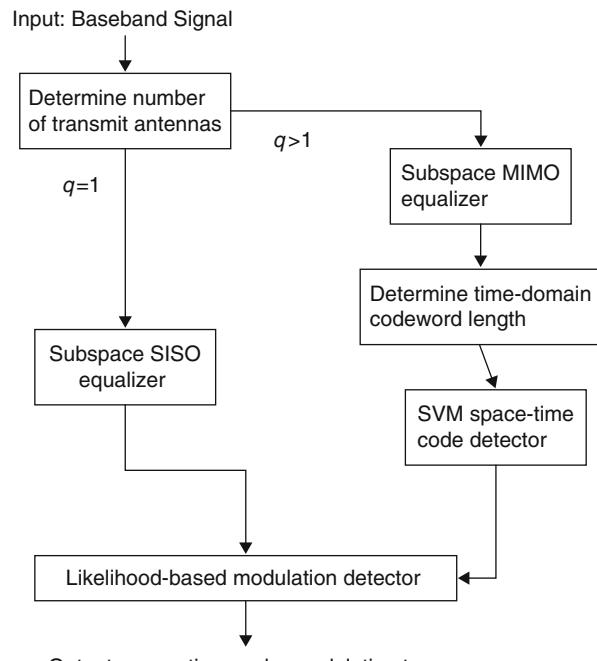


Fig. 16.3 Overall modulation forensic detector scheme

The task of the forensic detector is not only to estimate the modulation scheme as precisely as possible, but also to provide a confidence measure to every estimation. We define the detector's confidence measure \mathbf{C} as follows:

$$\mathbf{C} = 1 - \frac{H(\mathbf{LF})}{\log_2 N_{mod}} \quad (16.35)$$

where

$$\mathbf{LF} = \frac{\{LF^{(1)}, \dots, LF^{(N_{mod})}\}}{\sum_{i=1}^{N_{mod}} LF^{(i)}} \quad (16.36)$$

is the normalized likelihood vector of all hypotheses. From the above analysis, when $LF^{(\tilde{i})}$ is much larger than the other $LF^{(i)}$'s, the vector \mathbf{LF} has a smaller entropy $H(\mathbf{LF})$, which means one of the modulation scheme is much more likely than each other, thus we are more confident with the detection result. The lower the entropy $H(\mathbf{LF})$, the more confident the forensic detector is. Based on this idea, the confidence measure \mathbf{C} is defined as the normalized entropy of $H(\mathbf{LF})$ as in Eq. (16.35).

16.4 Simulation Result

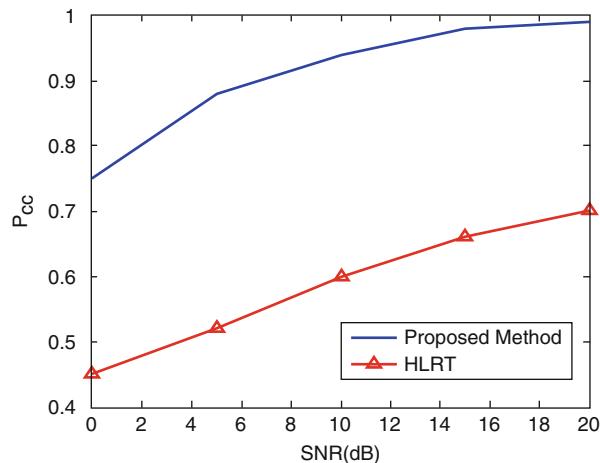
To compare the performance of the SISO modulation forensic detector over frequency selective fading channels, the performance of hybrid likelihood ratio test (HLRT) of [4] is also studied. We consider widely used digital modulation schemes: BPSK, QPSK, and 8PSK as candidates for SISO systems. Without loss of generality, normalized constellations are generated in simulations, i.e., $E[|s_k^{(i)}|^2] = 1$, thus, the SNR is changed by varying the noise power only. The pulse shape is rectangular, of unit amplitude and duration T seconds. The unit of the symbol period T is millisecond. The performance of modulation forensic detectors is evaluated by the average probability of correct classification, defined as

$$P_{cc} = \frac{\sum_{i=1}^{N_{mod}} P_c^{(i|i)}}{N_{mod}} \quad (16.37)$$

where $P_c^{(i|i)}$ is the conditional probability of the event that the i th modulation is detected when indeed the i th modulation is used at the transmitter. The number of symbols used to calculate $P_c^{(i|i)}$ is 30 and another 30 symbols are used for blind equalization. The channel is frequency-selective with Rayleigh fading, and the filter length is 10.

Figure 16.4 shows the performance of modulation detector under SISO systems. It's clear that our method outperform HLRT by 20% and can achieve over 95% accuracy rate in the high SNR region with only 60 symbols. The reason is that HLRT has the assumption of AWGN channel, which degrades the performance a lot in selective fading channels, although HLRT can achieve very high accuracy rate in AWGN channels.

Fig. 16.4 Performance comparison of likelihood-based algorithms in frequency-selective Rayleigh fading, when discriminating BPSK, QPSK, and 8PSK with $K = 60$ symbols



The performance of overall modulation forensic detector described in Sect. 16.3.3 is evaluated in Fig. 16.4. Figure 16.5 plots the output of system confidence measure. We test over four widely used orthogonal space-time codes: C_2 , $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$, which maintain the same transmit power and full diversity, and diagonal algebraic codes of size 2×2 , 4×4 , and 8×8 . Since the space-time code scheme is determined based on the expectations of the received signal, we need a little bit more symbols for the MIMO case, so here we show the result of $K = 100$ symbols.

Comparing Figs. 16.4 and 16.6, one can find that there is just 2% performance degradation cased by the MIMO system identification, which means our space-time matrix estimation method has the similar performance with the optimal one. And, the performance of MIMO system identification rarely degrades with the channel SNR, because our method is based on the orthogonality of transmit symbols, which is independent of the channel SNR. Furthermore, the performances in high SNRs

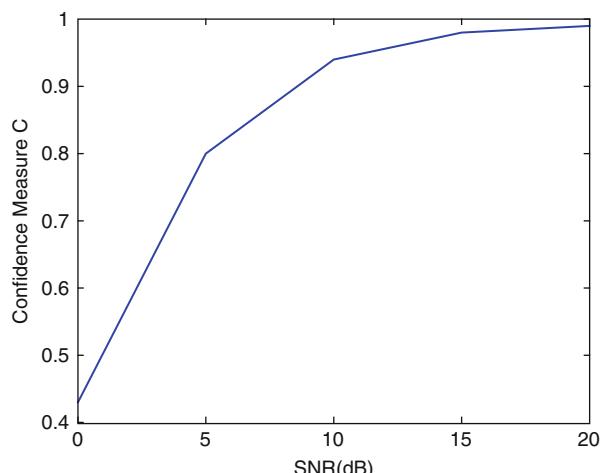
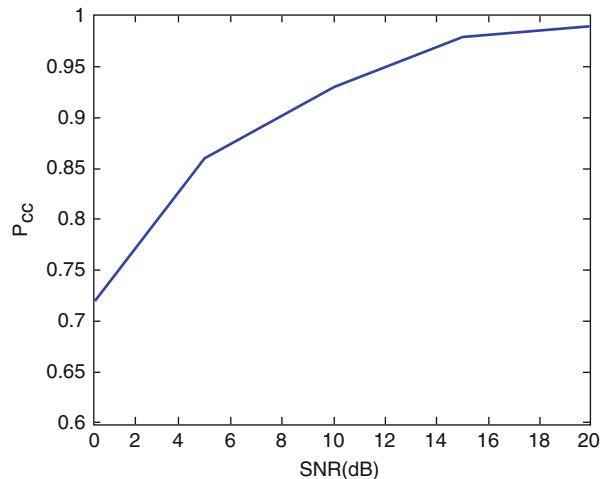


Fig. 16.5 Output confidence measure of the modulation forensic detector including BPSK, QPSK, 8PSK, diagonal algebraic codes of size 2×2 , 4×4 , 8×8 and orthogonal space-time code C_2 , $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$ with $K = 100$ symbols

Fig. 16.6 Overall performance of the modulation forensic detector including BPSK, QPSK, 8PSK, diagonal algebraic codes of size 2×2 , 4×4 , 8×8 and orthogonal space-time code C_2 , $C_{3,1/2}$, $C_{4,1/2}$, $C_{4,3/4}$ with $K = 100$ symbols



begin the same also implies that increasing the number of test symbols from 60 to 100 does not help much in detection, which means our likelihood-based test can work well with short symbol length 60. This feature is very important for forensics purpose, since the shorter the delay, the more the information.

Although the modulation forensic detector makes some error in low SNR ($\text{SNR} < 10$ dB), the corresponding system confidence measure is also low as shown in Fig. 16.4. This implies that the forensic detector is very uncertain about the answer when making errors. Hence, the modulation forensic detector still works well in low SNRs.

16.5 Conclusions

In this chapter, we proposed a composite likelihood ratio and second moment test for MIMO/SISO digital linear modulation forensics detection in frequency-selective fading channels, with unknown channel amplitude vector and phase distortion. The overall modulation forensic detector achieves very high detection accuracy. The successful detection probability approaches to 1 when $\text{SNR} > 15$ dB, in a fading channel with only 60 symbols used. Moreover, the simulation results show that the proposed space-time code identification based on second-moment nonlinearity test is nearly perfect.

References

- [1] C. M. Spooner, “On the utility of sixth-order cyclic cumulants for rf signal classification,” in *Proc. IEEE ASILOMAR*, pp. 890–897, 2001.
- [2] A. Swami and B. M. Sadler, “Hierarchical digital modulation classification using cumulants,” *IEEE Transaction on Communication*, vol. 48, pp. 416–429, 2000.

- [3] W. Dai, Y. Wang, and J. Wang, "Joint power estimation and modulation classification using second- and higher statistics," in *Proc. IEEE WCNC*, pp. 155–158, 2002.
- [4] W. Wei and J. M. Mendel, "Maximum-likelihood classification for digital amplitude-phase modulations," *IEEE Transaction on Communication*, vol. 48, pp. 189–193, 2000.
- [5] A. Polydoros and K. Kim, "On the detection and classification of quadrature digital modulations in broad-band noise," *IEEE Transaction on Communication*, vol. 38, pp. 1199–1211, 1990.
- [6] O. A. Dobre, J. Zarzoso, Y. Bar-Ness, and W. Su, "On the classification of linearly modulated signals in fading channels," in *Proc. Conference on Information Sciences and Systems (CISS)*, 2004.
- [7] A. Abdi, O. A. Dobre, R. Chauchy, Y. Bar-Ness, and W. Su, "Modulation classification in fading channels using antenna arrays," in *Proc. IEEE MILCOM*, pp. 211–217, 2004.
- [8] O. A. Dobre and F. Hameed, "Likelihood-based algorithms for linear digital modulation classification in fading channels," in *Proc. IEEE CCECE, Ottawa, Canada*, 2006.
- [9] C. Y. Huang and A. Polydoros, "Likelihood methods for mpsk modulation classification," *IEEE Transaction on Communication*, vol. 43, pp. 1493–1504, 1995.
- [10] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, 2000.
- [11] L. J. Cimini, "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Transactions on Communications*, vol. 33, pp. 665–675, 1987.
- [12] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, 1998.
- [13] D. Grimaldi, S. Rapuano, and G. Truglia, "An automatic digital modulation classifier for measurements on telecommunication networks," in *Proc. IEEE Instrumentation and Measurement Technology*, pp. 957–962, 2002.
- [14] M. O. Damen, K. Abed-Meraim, and J.-C. Belfiore, "Diagonal algebraic space-time block codes," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 628–636, 2002.
- [15] H. El Gamal and A. R. Jr. Hammons, "On the design of algebraic space-time codes for mimo block-fading channels," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 151–163, 2003.
- [16] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1456–1467, 1999.
- [17] K. Boulle and J.-C. Belfiore, "Modulation schemes designed for the rayleigh fading channel," in *Proc. CISS92*, 1992.
- [18] J. Boutros and E. Viterbo, "Signal space diversity: A power and bandwidth efficient diversity technique for the rayleigh fading channel," *IEEE Transactions on Information Theory*, vol. 44, pp. 1453–1467, July 1998.
- [19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holand, 1977.
- [20] W. Sabrina Lin and K. J. Ray Liu, "Modulation forensics for wireless digital communications," in *Proceeding of International Conference on Acoustic, Speech, and Signal Processing*, 2008.
- [21] B. Sampath, K. J. R. Liu, and Y. Goeffrey Li, "Error correcting least-squares subspace algorithm for blind identification and equalization," *Signal Processing*, vol. 8, no. 10, pp. 2069–2087, 2001.
- [22] H. V. Poor, *An Introduction to Signal Detection and Estimation*, Springer-Verlag, 2nd edition, 1999.
- [23] B. Sampath, K. J. Ray Liu, and Y. Goeffrey Li, "Deterministic blind subspace mimo equalization," *EURASIP Journal on Applied Signal Processing*, vol. 2, no. 5, pp. 538–551, 2002.