Doctoral Thesis

Performance of Physical Layer Security under Correlated Fading Wire-Tap Channel

by

Jinxiao Zhu

Graduate School of Systems Information Science

Future University Hakodate

March 2014

Abstract

The inherent openness of wireless medium makes information security one of the most important and difficult problems in wireless networks. Physical layer security, which achieves the information-theoretic security by exploiting the differences between the physical properties of signal channels such that a degraded signal at an eavesdropper is always ensured and thus the original data can be hardly recovered regardless of how the signal is processed at the eavesdropper, has been studied as a promising approach to providing a strong form of security.

By now, many research works have been devoted to understand the fundamental performance limits of physical layer security under different wire-tap channel models. It is notable that among different wire-tap channel models, the fading channel model has been an important model to efficiently capture the basic time-varying properties of wireless channels. Available works related to physical layer security study of the fading wire-tap channel are mainly based on the assumption that the channel from a transmitter to a legitimate receiver is independent of the one from the transmitter to an eavesdropper. In practice, however, the correlation among channels from a transmitter to different receivers has been frequently observed. Therefore, understanding the performance of physical layer security under the more practical correlated fading channels is of great importance for practical applications of physical layer security in wireless networks.

In this thesis, we aim to provide a comprehensive study on the fundamental performance limits of physical layer security under a fading wire-tap channel, where the channel from transmitter to legitimate receiver is correlated with the one from transmitter to eavesdropper. We start the study from the scenario when the transmission power is asymptotically infinite. In particular, we first provide an information-theoretic formulation of secure transmission over wireless fading channels at one realization of coherence interval in the high transmission power regime and show that the secrecy capacity is limited by the channel gain ratio of the main and eavesdropper channels rather than the transmission power, which is different from the Shannon's capacity that increases with transmission power. We next characterize the asymptotic outage probability and also asymptotic outage secrecy capacity for the correlated fading wire-tap channel as the transmission power goes to infinity.

We then analyze the performance of physical layer security under correlated fading wire-tap channel with a limited transmission power, a more complicate scenario compared with the one with asymptotic-infinite power. Specifically, we provide theoretical modeling for the secrecy capacity, transmission outage probability and secrecy outage probability of such systems. In particular, we first derive a simple closed-form expression of secrecy capacity based on the typical Marcum Q function. This is achieved by exploring the symmetry property between the main channel and eavesdropper channel such that some complicated integration operations involved in the secrecy capacity analysis can be significantly simplified. We then derive the transmission outage probability and secrecy outage probability to depict the reliability and security performances of the concerned wire-tap channel. Finally, extensive numerical results are provided to illustrate the inherent performance tradeoffs under

fading wire-tap channel and also the potential impact of channel correlation on such tradeoffs.

Our results reveal that the channel correlation between the main and eavesdropper channels has a significant impact on both secrecy capacity and outage performances. Remarkably, the impacts of correlation on the outage performances can be helpful or harmful depending on the channel conditions of both the main and eavesdropper channels and also the secrecy rate adopted in the transmission.

Acknowledgments

I am truly and deeply indebted to so many people that there is no way to acknowledge them all, or even any of them properly. Without their support, help and encouragement, this work would not and could not haven been done. I extend my deepest gratitude to all.

First, I wish to express my sincere gratitude to my Ph.D. supervisor, Professor Osamu Takahashi, for his continuous support, guidance and supervision during my graduate studies. Thanks to the financial support and the flexibility he extended to me, I was able to sample a variety of problems before narrowing down to the topic in this dissertation. He was not only a research advisor but also a great person with whom I can discuss diverse issues.

Second, I would like to give my special thanks to my Ph.D. co-supervisor, Professor Xiaohong Jiang, for his insightful guidance, encouragement and support in both my research and my life. I learned a lot from the discussions with him and the comments from him. I appreciate all that he has taught me and all that he has done to aid my development-both professionally and personally. Without him, this thesis could not have been finished.

I would also like to acknowledge my thesis committee members, Professor Yuichi Fujino and Professor Norio Shiratori, for their interests and for their constructive comments that help to improve this thesis.

I would also like to thank all the people I have interacted with at Future University Hakodate, specifically everyone affiliated with Jiang's Laboratory.

This work would not have been possible without the support of my parents and other family members, who have been a source of encouragement during my Ph.D. years. This work is dedicated to my parents, to whom I owe more than ever be able to repay.

THIS PAGE INTENTIONALLY LEFT BLANK

Contents

List of Figures

Chapter 1

Introduction

In this chapter, we will introduce the background of the physical layer security, including the importance of physical layer security and a briefly review about its history and a state-of-art survey. We then describe our motivations this thesis. Finally, the contributions together with the outline of this thesis will be presented.

1.1 Background

1.1.1 Physical Layer Security

The inherent openness of wireless medium allows anybody within the coverage range of a transmitter to capture its signals, which makes information security one of the most important and difficult problems in wireless networks. Traditionally, the information security is usually addressed above the physical layer in the seven-layer OSI model of computer networking, such as the widely adopted cryptography, which is usually employed at the application layer assuming the physical layer has already provided an error-free link [50]. The traditional cryptography is usually achieved by encrypting the plain message by means of special algorithms that are assumed to be computationally infeasible for the adversary to decrypt if the encryption keys are unknown at the adversary. However, because of improvements in computers' computing abilities and methods of breaking encryption algorithms, there are concerns that such

security methods no longer suffice, especially for applications with a requirement of strong form of security (like military networks). For example, the Data Encryption Standard (DES) encryption scheme, which employs a 56-bit key, was approved as standard by the U.S. National Bureau of Standards in 1976; however, a DES cryptogram was broken for the first time in public in 1997, and furthermore, a DES key was broken by the Deep Crack hardware in just 56 hours in 1998 [44].

Recently, the physical layer security has been studied as a promising approach to providing a strong form of security for wireless networks. Unlike the cryptography that ignores the difference between the received signals at different receivers, the physical layer security is achieved by exploring the differences between the physical properties of signal channels to achieve the unconditionally secure, i.e., the security achieved with no limitation about the adversary's computing power. As such, the physical layer security is usually regarded as information-theoretic security, which is now widely accepted as a stronger notion than computational security. The explosive growth of wireless applications coupled with the desire for information privacy indicate a bright future for physical layer security, both as stand-alone security solutions and as part of the layered security schemes. However, the study of such promising physical layer security is still on its initial stage and the fundamental theoretical performances and practical coding techniques remain largely unknown.

To illustrate the general concept of physical layer security, Fig. 1-1 shows the typical example of a three-node network where the transmission from node N_1 to N_2 is being eavesdropped by a third-party malicious node N_3. The communication channel from N_1 to N_2 is called the main channel, whereas the channel from N_1 to N_3 is called the eavesdropper channel. Since the two receivers N_2 and N_3 are located in different places, the signals received by them are usually different. The inherent reason is that the two channels through which signals pass have different fading effects. Basically, there are two different types of fading: small scale fading and large scale shadowing. Small scale fading, which is also called multipath fading, varies with surrounding scatters that reflect wavefront between transmitter and receiver differently, and it may cause deep fades even within small distances. Large scale shadowing, on the

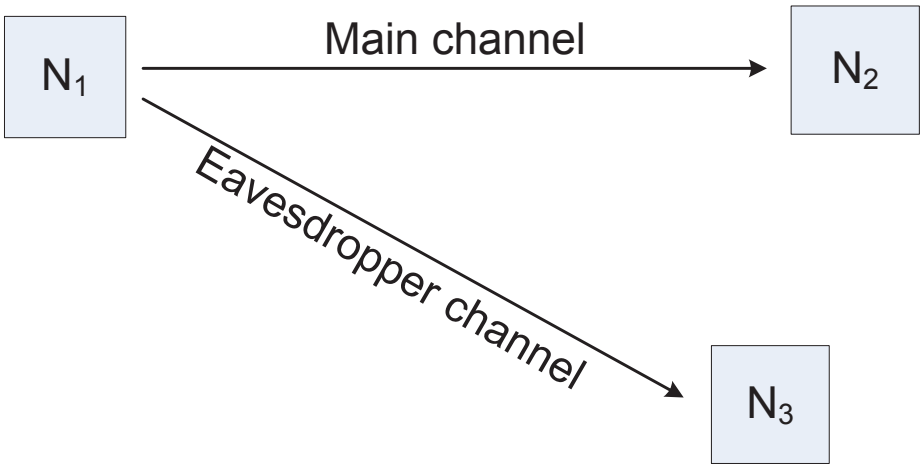

Figure 1-1: Illustration of eavesdropping scenario

other hand, is very dependent on location with respect to obstacles. It is worth noting that these effects are varying all the time according to the surrounding environments. And the physical layer security can be achieved by exploring these effects: The system transmits secret messages when the main channel has better channel condition than the eavesdropper channel, and suspends transmissions otherwise. Note that there also exists the maximum allowed information rate for each system, which is termed as secrecy capacity. Just like Shannon's capacity, secrecy capacity defines the tightest upper bound on the amount of information that can be reliably transmitted without any information leakage.

1.1.2 Related Work

Literally, the physical layer security is also regarded as information-theoretic security, since its security is derived purely from information theory.

Initial works of physical layer security

The theoretical basis of physical layer security starts from Shannon's notion of perfect secrecy: If the eavesdropper's uncertainty (entropy rate) about the plain message after seeing the transmitted signal is equal to the one before seeing the transmitted signal, then "perfect secrecy" is said to be achieved [68]. Based on this notion,

Wyner initiated the study of physical layer security from a basic wire-tap channel, where a source node transmits a message to a destination node through a discrete memoryless channel and another malicious node called wire-tapper eavesdrops this message through another *degraded* version of the discrete memoryless channel [85]. Wyner showed that a positive information rate can be achieved with perfect secrecy if the eavesdropper channel is noisier than the main channel and that there exists channel codes which ensure the message is reliably delivered to the legitimate receiver, while the uncertainty at eavesdropper is not reduced by her observation, as long as the rate of the code is selected to be smaller than the secrecy capacity. We refer to this channel code as a "wiretap code".

Later, Wyner's work was generalized to some other important scenarios. In 1978, Csiszár and Körner studied the *non-degraded* channels and showed that is is possible to achieve a non-zero secrecy capacity if the main channel is less noisy or more capable than the wiretapper channel [7]. In the same year, Wyner's results for discrete memoryless channel was extended to the Gaussian channel, where the secrecy capacity is shown to be the difference between the capacities of the main and wire-tap channels [32]. It is notable that the results in the above early works showed that a positive secrecy capacity can be achieved if the intended receiver has a better channel than the eavesdropper.

State-of-the-art

Recently, various research works are being conducted to understand the physical layer security from both theoretical and practical aspects. The practical efforts mainly focus on designing practical wiretap codes that approach the secrecy capacity as much as possible. Inspired by the early works of [85] and [57], Wei studied the method to encode secrecy information using cosets of certain linear block codes for wire tap II channel [84]. More recently, Thangaraj et al. [76] proposed an LDPC based construction for specific discrete memory-less channels, and Klinc et al. [25] proposed another LDPC based construction for Gaussian channels. In recent work [47] and [18], polar codes have been suggested as methods for approaching the secrecy capacity of general

degraded and symmetric wiretap channels, of which the erasure wiretap channel is a special case. Since the main focus of this thesis is on the theoretical performance of the physical layer security, which serves as design criterions for practical security systems and coding schemes, we will give a more detailed introduction of its theoretical status.

Many works have been done on the study of theoretical performance of the physical layer security. These works can be roughly classified into two categories depending on the network scales, namely point-to-point networks and large-scale networks. It is noticed that a major performance metric for point-to-point networks is secrecy capacity, and we now give a short review based on channel models adopted. Firstly, the initial results for Gaussian channels [32] were generalized to fading channels in [3, 14, 37, 38], and it was shown that fading alone guarantees the information-theoretic security is achievable, even when the main channel has a worse average signal-to-noise ratio than the eavesdropper channel. Secondly, many researchers considered multiple-input multiple-output wiretap channel [22, 24, 41, 43, 45, 54], where each node have multiple antennas to improve their received signals. Next, some works considered multi-user wiretap channels, such as multiple access channel [36, 74], broadcast channel [20, 31, 77, 86], relay channel with confidential messages [1, 5, 28, 55, 56], interference channel with confidential messages [17, 42, 72, 73], cognitive interference channels [35, 40, 51, 63], etc.

For large-scale networks, many recent research efforts have been conducted to characterize their security performances in terms of capacity [27, 39, 60, 78], coverage [64], connectivity [12, 15, 59, 88] and percolation phenomenon [60, 61, 65, 66]. Specifically, various statistical characterizations of the existence of secure connections were given in [15, 59, 60, 88]. Using tools from percolation theory, the existence of a secrecy graph was analyzed in [12, 15, 60]. These connectivity results are concerned with the possibility of having secure communication, while they do not give insight on the network throughput. The authors in [27, 39, 78] derived secrecy capacity scaling laws in static and mobile ad hoc networks, i.e., the order-of-growth of the secrecy capacity as the number of nodes increases. Inspired by some early works of

transmission capacity study [2, 11, 16, 81–83], some recent works [89, 90] propose the notion of secrecy transmission capacity, which is defined as the achievable rate of successful transmission of confidential messages per unit area for given constraints on the quality of service (QoS) and level of security. It is expected that the scaling laws of secrecy capacity provide us insights into the general asymptotic network behavior, while the exact results of secrecy transmission capacity provide a finer view of tradeoff between different system parameters and transmission protocols.

Research efforts were also conducted for techniques to improve the received signals at legitimate receivers or deteriorate the ones at eavesdroppers. With the additional degrees of freedom provided by multi-antenna systems, transmitters can generate artificial noise to degrade the channel condition of the eavesdropper while maintaining little interference to legitimate users [13, 23, 71]. Interference alignment technique has been explored in [26, 27, 46] to achieve positive secure degrees of freedom. Some recent work [28, 75] studied the method of cooperative jamming, in which a relay transmits a jamming signal at the same time when the source transmits the message signal, to interfering the signal received at eavesdroppers. The beamforming transmission has been studied to maximizes the received signal power at the legitimate receiver [34, 67].

1.2 Motivations

By now, much research activity has been devoted to understand the fundamental performance limits of physical layer security under different wire-tap channel models (see Section 1.1.2 for related works). It is notable that among different wire-tap channel models, the fading channel model has been an important model to efficiently capture the basic time-varying properties of wireless channels [70]. Available works related to physical layer security studies of fading channel model are mainly based on the assumption that the channel from transmitter to legitimate receiver is independent of the one from transmitter to eavesdropper. In practice, however, the channels from a transmitter to different receivers are frequently correlated [29, 62, 69]. Such

correlation depends on many factors in the communication environment, such as the presence or absence of scatters around transmitter and receivers, clearance of signal path, and physical deployment of receiver antennas, etc. Moreover, the correlation can be also caused deliberately. For example, eavesdroppers can actively induce correlation by approaching a legitimate receiver [19]. Therefore, understanding the performance of physical layer security under practical correlated fading channels is of great importance for practical applications of physical layer security in wireless networks.

1.3 Contributions and Outline

1.3.1 Contributions

In this thesis, the overall aim is to provide a comprehensive study on the fundamental performance limits of physical layer security under a fading wire-tap channel, where the channel from transmitter to legitimate receiver is correlated with the one from transmitter to eavesdropper. The novelty of the thesis is that unlike most of previous work focuses on the independent fading channels, our study focuses on the correlated fading channel model, which is more realistic compared with the previous one. Another novelty is that the performance metrics we derived in this thesis are closed-form expressions, especially the complex secrecy capacity was also derived in closed-form expression based on the typical Marcum Q function. The methods in our theoretical analysis mainly combined the information theory, statistics, and integration techniques of special functions, such as Marcum Q function.

The main contributions of the thesis are summarized as follows:

- Theoretical models: For unlimited transmission power scenario, we derive asymptotic outage probability and asymptotic outage secrecy capacity in simple closed-form expressions. For limited transmission power scenario, secrecy capacity is derived to depict the maximum information rate that can be achieved both reliably and securely; transmission outage probability and secrecy outage prob-

ability are further derived to depict the reliability and security performances of the concerned wire-tap channel, respectively.

- Impact of channel correlation: Our results reveal that the channel correlation between the main and eavesdropper channels has a significant impact on both secrecy capacity and outage performances. In particular, we reveal that the impact of correlation on secrecy capacity is always harmful; however, the impact of correlation on the outage performances can be either helpful or harmful depending on the channel conditions of both the main and eavesdropper channels and also the secrecy rate adopted in the transmission.

It is notable that our theoretical models, derived for correlated channels, also cover the corresponding models for independent channels as special cases. It is expected that theoretical models we developed could provide guideline for efficient security systems design, and that the impacts of correlation on the security performances we revealed would be helpful for network engineers to design practical secure systems.

1.3.2 Thesis Outline

The outline of the thesis is listed as follows:

- We introduce in Chapter 2 some key notions in physical layer security and also our system model in this thesis. Specifically, the following topics will be included: the fading wire-tap channel coupled with key information theoretic notions, correlated channel model, channel state information and some system assumptions.

- In Chapter 3, we focus on the performance analysis of the physical layer security under correlated fading wire-tap channels when transmission power is large (asymptotically infinite). We first provide an information-theoretic formulation of secure transmission over wireless fading channels at one realization of coherence interval in the high transmission power regime and show that the secrecy capacity is limited by the channel gain ratio of the main and eavesdropper

channels rather than the transmission power, which is different from the Shannon's capacity that increases with transmission power. We next characterize the asymptotic outage probability and also asymptotic outage secrecy capacity for the correlated fading wire-tap channel as the transmission power goes to infinity, which cover the corresponding results when the main and eavesdropper channels are independent as special cases. Based on the theoretical results, the impact of channel correlation on the asymptotic outage probability and asymptotic outage secrecy capacity are then explored.

- We further extend our analysis to a more practical scenario that transmission power is constrained in Chapter 4. Firstly, three metrics, namely secrecy capacity, transmission outage probability and secrecy outage probability, are introduced to fully depict the fundamental performance of applying physical layer security to achieve secure and reliable information transmission over the correlated fading wire-tap channel. Secondly, a simple closed-form expression of secrecy capacity is derived based on the typical Marcum Q function. This is achieved by exploring the symmetry property between the main channel and eavesdropper channel such that some complicated integration operations involved in the secrecy capacity analysis can be significantly simplified. Thirdly, the transmission outage probability and secrecy outage probability are further derived to depict the reliability and security performances of the concerned wire-tap channel, respectively. Finally, with the help of these theoretical models, we then explore the inherent performance tradeoffs under fading wire-tap channel and also the potential impact of channel correlation on such tradeoffs.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 2

Preliminaries

In this chapter, we reviews various key notions in information theoretic aspects of physical layer security, which will serve as building blocks in the remainder of the thesis, and introduces the system model of this thesis.

2.1 The Fading Wire-tap Channel

As initially introduced in Wyner's paper, the wire-tap channel consists three nodes: a transmitter, a receiver and an eavesdropper. The system model we consider is illustrated in Fig. 2-1, where a transmitter (Alice) sends confidential messages to a receiver (Bob) over a wireless fading channel, called main channel, while an eavesdropper (Eve) eavesdrops the messages through another wireless fading channel, called eavesdropper channel. Alice encodes a message, represented by random variable (RV) $W \in \mathcal{W} = \{1, \ldots, M\}$, into a codeword, represented by RV $X^n \in \mathcal{X}^n$, by using a stochastic encoder $f_n(\cdot) : \mathcal{W} \to \mathcal{X}^n$. The codeword X^n is then transmitted over the main channel. The signal received by Bob is denoted by $Y^n \in \mathcal{Y}^n$, while the signal received by Eve is denoted by $Z^n \in \mathcal{Z}^n$. After Bob receives the signal, he tries to decode the received signal by using a decoder $\phi(\cdot) : \mathcal{Y}^n \to \mathcal{W}$. The message estimated by Bob is denoted by $\hat{W} = \phi(Y^n)$. Here, $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$ are the source, the channel input alphabet, the channel output alphabet of the main channel and the channel output alphabet of the eavesdropper channel, respectively. The realiza-

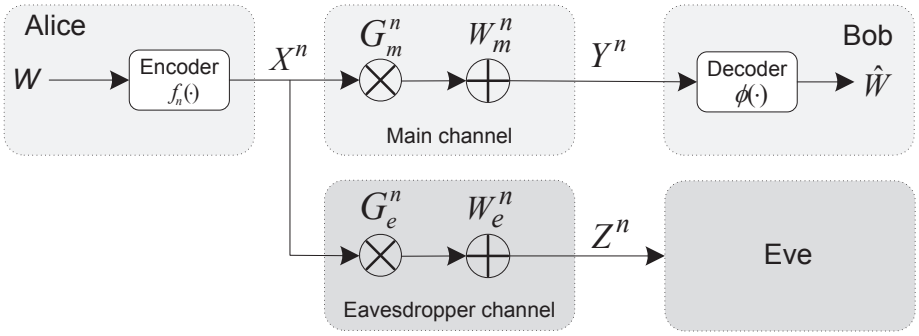

Figure 2-1: The fading wire-tap channel

tions of the RVs W, X, Y and Z are represented by w, x, y and z, respectively. Moreover, we have $X^n = (X(1), X(2), \ldots, X(n))$, $Y^n = (Y(1), Y(2), \ldots, Y(n))$ and $Z^n = (Z(1), Z(2), \ldots, Z(n))$.

The signal $Y(i)$ received by Bob and $Z(i)$ received by Eve can be determined as

$$Y(i) = G_m(i)X(i) + W_m(i),$$
$$Z(i) = G_e(i)X(i) + W_e(i), i = 1, 2, ..., n,$$

where n denotes the length of transmitted signal, $G_m(i)$ and $G_e(i)$ denote the channel gains of the main and eavesdropper channels, respectively, and $W_m(i)$ and $W_e(i)$ represent the independent and identically distributed (i.i.d.) Gaussian noise with zero mean and variances N_m and N_e, respectively. It is assumed that both the main and eavesdropper channels are quasi-static fading channels. In other words, the channel gains, albeit random, are fixed during the transmission of an entire codeword ($G_m(i) = G_m$ and $G_e(i) = G_e$, $\forall i = 1, \ldots, n$), and, moreover, independent from codeword to codeword. This corresponds to situations where the coherence time of the channel is large. It is further assumed that the codewords sent over the channels are subject to the average power constraint

$$\frac{1}{n}\sum_{i=1}^{n} E\{|X(i)|^2\} \leq P. \tag{2.1}$$

2.1.1 Information Theoretic Metrics

For a (M, n) code that is adopted in this thesis, the performance will be quantified by the following measures.

Error Probability

The average error probability is defined as

$$P_e = \Pr(\hat{W} \neq W). \tag{2.2}$$

This probability is used to measure the level of reliable communication between Alice and Bob.

Equivocation Rate

The measure for eavesdropper's uncertainty about W, which is called the equivocation rate, is defined as

$$R_{eq} = \frac{1}{n} H(W|Z^n), \tag{2.3}$$

where $H(W|Z^n)$ is the remaining entropy of W given that the value of Z^n is known. It indicates the secrecy level of confidential messages against the eavesdropper.

Secrecy Rate

The information rate for the secret message is determined by

$$R_s^* = H(W)/n. \tag{2.4}$$

For a uniform distributed message $W \in \mathcal{W}$, we have $M = 2^{R_s^*}$.

Perfect Secrecy

We say perfect secrecy is achieved for a (M, n) code if $R_{eq} = R_s^*$. A perfect secrecy rate R_s is said to be achievable if there exists a $(2^{nR_s}, n)$ code such that $R_{eq} \geq R_s - \epsilon$ and $P_e \leq \epsilon$ for any given $\epsilon > 0$.

Notice that the condition for perfect secrecy used here (and also in [85], [4], [19]) is weaker than the one proposed by Maurer and Wolf in [49], where the information leaked to the eavesdropper is negligibly small not just in terms of rate but in absolute terms. Maurer and Wolf showed that the notions could be used interchangeably for discrete memoryless channels, but this result was then extended to the Gaussian case in [52].

Secrecy Capacity

The secrecy capacity C_s is defined as the maximum achievable perfect secrecy rate [4], i.e.,

$$C_s \triangleq \sup_{P_e \leq \epsilon} R_s. \tag{2.5}$$

2.2 Correlated Channel Model

In this thesis, we consider the scenarios that the main channel is correlated with the eavesdropper channel, and both are ergodic fading channels. It is assumed that G_m and G_e are two complex Gaussian RVs with zero-mean. Thus, the joint distribution of their envelops follows the bivariate Rayleigh distribution [8]. This corresponds to situations of narrow-band systems under a rich scattering environment that produces multiple propagation waves. By the central limit theorem, in-phase and quadrature components of G_m and G_e in such a system can be considered as Gaussian processes.

Denoting $G_m = G_{mc} + jG_{ms}$ and $G_e(i) = G_{ec} + jG_{es}$, we consider the following simple scenarios for the correlation between the main and eavesdropper channels.

- The in-phase components G_{mc} and G_{ec} are independent of the quadrature components G_{ms} and G_{es}.

- The in-phase components G_{mc} and G_{ec} are correlated and the quadrature components G_{ms} and G_{es} are also correlated. The correlation coefficient between in-phase components is the same as that between the quadrature components, and we denote this coefficient as ρ_{G_m,G_e}, i.e.,

$$\rho_{G_m,G_e} = \frac{\mathrm{cov}(G_{mc}, G_{ec})}{\sqrt{\mathrm{var}(G_{mc})\mathrm{var}(G_{ec})}} = \frac{\mathrm{cov}(G_{ms}, G_{es})}{\sqrt{\mathrm{var}(G_{ms})\mathrm{var}(G_{es})}}. \tag{2.6}$$

In this thesis, our analysis is mainly based on the correlation coefficient ρ between the power gains of the main and eavesdropper channels, which is determined by

$$\rho = \frac{\mathrm{cov}(H_m, H_e)}{\sqrt{\mathrm{var}(H_m)\mathrm{var}(H_e)}}. \tag{2.7}$$

Since the power gains are determined by $H_m = |G_m|^2$ and $H_e = |G_e|^2$, we have $\rho = |\rho_{G_m,G_e}|^2$.

In real radio communication scenarios, the correlation coefficient ρ is determined by various physical conditions of transmission environment such as the distance between Bob and Eve, the presence or absence of scatters around them, clearance of signal path, and physical deployment of receiver antennas, etc. For example, if Bob and Eve have the omnidirectional antennas in dense multipath environments, Clarke's 2-D isotropic channel model is suitable to measure the correlation effect [80]. More recently, simple and intuitive geometrical interpretations of the fading statistics are suggested in [9] where the spatical fading correlation is effectively described by several spatial parameters, like the angular spread, angular constriction, and azimuthal direction of maximum fading. The correlation coefficient can also be determined by field measurements.

2.3 Channel State Information

In wireless communication, channel state information (CSI) refers to channel properties of a communication link, including channel gain, fading distribution, noise

strength, and spatial correlation, which can be used to describe how a signal propagates from a transmitter to a receiver. There are basically two levels of CSI, namely instantaneous CSI and statistical CSI. The instantaneous CSI indicates the current channel conditions, while the statistical CSI refers to statistical characterizations of the channel, which can be in turn determined if the instantaneous CSI is known. The instantaneous CSI makes it possible to adapt transmissions to the current channel conditions, which is crucial for reliable communication, while the statistical CSI has no such advantage.

For the quasi-static fading channel considered in this thesis, it is always possible to achieve the CSI of main channel since Bob can cooperate with Alice by feeding back the channel estimates to her, while it is hard to achieve the Eve's if he keeps silence. Nevertheless, there exist scenarios that Alice can achieve Eve's CSI, or at least statistical CSI. For example, Eve is another active user in the wireless network but is not allowed to hear the secret messages, so Alice can estimate the Eve's channel during Eve's past transmissions. In this thesis, our analysis mainly focus on the scenario that before transmission Alice has only partial CSI known in the sense that she knows the instantaneous CSI (i.e., real time channel gain) of the main channel and also the statistical CSI of both channels, but has no idea about the instantaneous CSI of the eavesdropper channel. However, it is noticed that the performance metrics derived in this paper are also important in other CSI assumptions, which will be clearly indicated in the next two chapters.

2.4 Other Assumptions

The scope of the wiretap channel is restricted to passive eavesdropping strategies where the adversary does not tamper with the main channel or the eavesdropper's channel.

Chapter 3

Physical Layer Security under Asymptotic-Infinite Transmission Power

This chapter address the problem of the overall reliable and secure performance of physical layer security (PLS) under the more practical correlated fading wire-tap channel when the transmission power is approaching infinity. Both the asymptotic outage probability and outage secrecy capacity are derived in simple closed-form expressions. Unlike Shannon's result for channel capacity that increases with transmission power, the asymptotic secrecy capacity is found to be controlled by the channel power gain ratio, rather than the transmission power. It is also noticed that channel correlation has exactly the opposite impacts on the asymptotic outage secrecy capacity depends on its asymptotic outage probability.

3.1 Motivation and Outline

The problem of secure communication over the fading wireless channels, where the transmitter does not have the CSI of the eavesdropper channel, has attracted considerable attention recently. For delay-tolerant applications, the performance limits of such systems have been characterized by ergodic secrecy capacity [14, 21], which cap-

tures the capacity limits under the constraint of perfect secrecy. For delay-sensitive applications, however, perfect secrecy cannot always be achieved, and outage-based performance metrics (e.g., outage secrecy capacity) become more appropriate [3, 58]. If no instantaneous CSI of the eavesdropper channel is available, the transmitter will always transmit at a constant rate (possibly set up according to the statistics of the channels), thus an outage happens whenever the channel cannot support transmission at the designated constant secrecy rate, i.e., whenever the instantaneous secrecy capacity is less than the secrecy rate. In [3, 58], an outage probability formula was proposed to give a fundamental characterization of the possibility of having a reliable and secure transmission, where their studies focused on the fading channel that the main channel is independent of the eavesdropper channel. In real radio communication scenarios, however, the correlations between channels from a transmitter to different receivers have been frequently observed [29, 62, 69].

Motivated by the above observations, this chapter is aimed to provide an analysis about the outage performances of the physical layer security under the more practical correlated fading wire-tap channel based on the outage formula that presented in early works [3, 58]. In particular, we will start the study from the extremely case that transmission power is very large and derive simple closed-form expressions for both the asymptotic outage probability and outage secrecy capacity. The study for the power limited scenario, which involve a more complicated derivation process, will be provided at the next chapter. Furthermore, we are interested on the asymptotic behaviors of the outage secrecy capacity as the transmission power goes to infinity, and also the impact of channel correlation on it.

The remainder of this chapter is organized as follows. We introduces in Section 3.2 the previous studies that have directly relation with this chapter's contents. In Section 3.3, we describes the additional system assumption besides the fading wire-tap model proposed in Chapter 2, and provides the formal definition of performance metrics that is going to be studied in this chapter. Then Section 3.4 derives the theoretical models of the asymptotic outage probability and outage secrecy capacity for the concerned correlated fading wire-tap channel. In Section 3.5, the implications

of the above results are discussed, such as the impact of channel correlation on outage secrecy capacity, and the tradeoff between the outage secrecy capacity and outage probability. Finally, concluding remarks of this chapter are given in Section 3.6.

3.2 Related Research Works

For the independent fading wire-tap channel, Gopala *et al.* [14] characterized the corresponding ergodic secrecy capacity under the optimum power allocation strategy with full CSI or partial CSI. Almost at the same time, Bloch *et al.* [4] derives the average secrecy capacity for the same independent fading channel with a power constraint under the full CSI assumption. Notice that wireless channels are always fluctuating and it is very difficult (if not impossible) to acquire the real time CSI of channels. Thus the full CSI assumption is not really realistic with current technologies. For the more realistic scenarios where the transmitter only knows the CSI of the main channel, a better performance measure is the outage secrecy capacity, which is defined as the maximum information rate that can be maintained such that the maximum secrecy outage probability is no more than the specified value. Moreover, for delay sensitive applications, where we need to ensure a high data rate by allowing a certain probability of outage, the outage secrecy capacity is of greater interest.

In some early works [3, 58], the outage probability for the physical layer security method was defined as the probability that the secrecy capacity drops below a given transmission rate of the secret message. Specifically, Parada *et al.* analyzed in [58] the independent fading wire-tap channel with multiple receiver antennas and derived an approximate outage probability; Barros *et al.* provided in [3] a closed-form outage probability for the independent fading wire-tap channel, and a corresponding formula for the outage secrecy capacity.

To the best of our knowledge, however, no work is available on the outage secrecy capacity study under the more realistic correlated fading wire-tap channel. The related study under the correlated fading wire-tap channel is the work by Jeon *et al.* in [19], where they explored the asymptotic ergodic secrecy capacity of correlated

fading channels when the signal-to-noise ratio (SNR) is infinite under the full CSI assumption. Therefore, our analysis in this chapter provides the outage probability and outage secrecy capacity of the correlated fading wire-tap channel for the scenario that only partial CSI is available at transmitter.

3.3 System Assumptions and Performance Metrics

To characterize the asymptotic performances of the concerned system described in Chapter 2 as transmission power approaches infinity, we further assume that the noise powers at Bob and Eve are similar, i.e., $N_m = N_e$. Without loss of generality, we assume $N_m = N_e = 1$ to simplify the analysis.

Since the full CSI is not available at Alice, we consider the transmission scheme that Alice always transmit at a target secrecy rate $R_s > 0$. It is noticed that the setting of R_s can be determined based on the statistical CSIs of both the main and eavesdropper channel if they were available at Alice before transmission. To depict the performance of the concerned wiretap fading channel, the following two performance metrics are adopted. The instantaneous secrecy capacity denotes the secrecy capacity determined by the a realization of the channel gains of both the main and eavesdropper channels [4].

- Outage probability: The overall outage probability is defined as the probability that the target secrecy rate is less than the instantaneous secrecy capacity.

- Outage secrecy capacity: The outage secrecy capacity is the maximum secrecy rate that can be maintained under any fading condition during nonoutage coherence intervals such that the allowed outage probability is satisfied.

3.4 Outage Performance Analysis

We begin with the secrecy capacity for one realization of the fading channels at a coherence interval during which the channel gains are assumed to be constant. It is assumed that the transmission power is P. As stated in [4], it is reasonable to view the main channel in this scenario as a complex additive white gaussian noise (AWGN) channel with its SNR PH_m and capacity

$$C_m = \log(1 + PH_m). \tag{3.1}$$

Similarly, the eavesdropper channel is a complex AWGN channel with its SNR PH_e and capacity

$$C_e = \log(1 + PH_e). \tag{3.2}$$

It is known that the secrecy capacity of a complex AWGN wiretap channel is just the difference between the main and eavesdropper channels there [4]. Thus, the secrecy capacity for one realization of the fading coefficients is derived as

$$C_s = \begin{cases} \log(1 + PH_m) - \log(1 + PH_e), & \text{if } H_m > H_e; \\ 0, & \text{if } H_m \leq H_e. \end{cases} \tag{3.3}$$

3.4.1 High SNR Regime

It is easy to deduce from (3.1) that the channel capacity without secrecy constraint grows nearly logarithmically with the SNR. However, the secrecy capacity shows a different behavior as the SNR increases.

From (3.3), when the main channel gain is better than the eavesdropper channel gain (e.g. $H_m > H_e$), the asymptotic secrecy capacity for one pair of channel gains is

given by

$$\begin{aligned} C_s &= \log(1+PH_m) - \log(1+PH_e) \\ &= \log\left(\frac{\frac{1}{P}+H_m}{\frac{1}{P}+H_e}\right) \\ &\overset{(a)}{\leq} \log\left(\frac{H_m}{H_e}\right) \triangleq C_s^{lim}, \end{aligned} \tag{3.4}$$

where the equality in (a) holds as P goes to infinity (i.e., high SNR), and the asymptotic secrecy capacity is denoted as C_s^{lim}. Thus, the asymptotic secrecy capacity is controlled by the channel power gain ratio.

3.4.2 Asymptotic Outage Probability and Outage Secrecy Capacity

According to the definition in 3.3, the outage probability can be given by

$$\mathcal{P}_{out}(R_s) = \mathcal{P}(C_s < R_s). \tag{3.5}$$

The operational significance of this definition of outage probability is threefold. First, it provides the fraction of fading realizations for which a wireless channel can support a secrecy rate of R_s bits/channel use. Second, it provides a security metric for the situation where Alice have no CSI of eavesdropper channel, which corresponds to the scenario that Eve is a purely passive and malicious eavesdropper in the wireless network. In this case, Alice has no choice but to set the secret transmission rate to a constant R_s. By doing so, Alice is assuming that the capacity of the eavesdropper channel is given by $C_e^{'} = C_m - R_s$. As long as $R_s < C_s$, the eavesdropper channel is worse than Alice's estimate, i.e., $C_e < C_e^{'}$, and the wiretap codes used by Alice can ensure perfect secrecy. Otherwise, if $R_s > C_s$, then $C_e > C_e^{'}$ and the physical layer security is compromised. Third, for a delay-sensitive application, we can achieve much higher communication rates by allowing some outage probability. If no outage is allowed, we can hardly transmit any information in poor channel conditions.

Adopting the same notations as that in [19], we let $U = H_m/H_e$. The average Channel power Gain Ratio (CGR) is denoted as $\kappa = \mathbb{E}[H_m]/\mathbb{E}[H_e]$, and the channel Power Correlation Coefficient (PCC) between H_m and H_e is ρ. Under the Rayleigh fading assumption, the probability density function (PDF) of the channel power gain ratio U is derived as [19]

$$f_U(u) = \kappa \frac{(1-\rho)(u+\kappa)}{[(u+\kappa)^2 - 4\rho\kappa u]^{3/2}}, u \geq 0. \tag{3.6}$$

Thus, we have the following lemma.

Lemma 1. *If the main channel is correlated with the eavesdropper channel, and the joint PDF of them follows the bivariate Rayleigh distribution, as the SNR increases, the probability that the instantaneous secrecy capacity is larger than τ ($\tau \geq 0$) is upper bounded by*

$$\mathcal{P}\left(C_s^{lim} > \tau\right) = \frac{1}{2} - \frac{2^\tau - \kappa}{2\sqrt{(2^\tau+\kappa)^2 - 4\rho\kappa 2^\tau}}. \tag{3.7}$$

Proof.

$$\begin{aligned}
\mathcal{P}\left(C_s^{lim} > \tau\right) &= \mathcal{P}\left(\log\left(\frac{H_m}{H_e}\right) > \tau\right) = \mathcal{P}(\log u > \tau) \\
&= \int_{2^\tau}^{\infty} f_U(u) du \\
&= \left[\frac{u-\kappa}{2\sqrt{(u+\kappa)^2 - 4\rho\kappa u}}\right]_{2^\tau}^{\infty} \\
&= \frac{1}{2} - \frac{2^\tau - \kappa}{2\sqrt{(2^\tau+\kappa)^2 - 4\rho\kappa 2^\tau}}
\end{aligned}$$

□

Remark 1. *When the main and eavesdropper channels are not correlated, that is $\rho = 0$, the probability that the instantaneous secrecy capacity is larger than τ ($\tau \geq 0$) is upper bounded by*

$$\mathcal{P}\left(C_s^{lim} > \tau\right) = \frac{\kappa}{2^\tau + \kappa},$$

which is just the upper bound of the similar probability in [4] when the main channel SNR goes to infinity.

According to the definition in 3.3, the outage secrecy capacity for a outage constraint of ϵ can be given by

$$C_{out}(\epsilon) \triangleq \max_{\mathcal{P}_{out}(R_s)\leq\epsilon}(R_s). \tag{3.8}$$

The above outage secrecy capacity is also called ϵ-outage secrecy capacity in the literally [3, 33].

Since the upper bound of the probability that the instantaneous secrecy capacity is larger than a specified value is derived in Lemma 1, we can obtain the lower bound of the outage probability for a target secrecy rate R_s and also the corresponding upper bound of the outage secrecy capacity in a closed-form, as summarized in Theorem 1. Notice that the bounds of the outage probability and outage secrecy capacity are denoted as $\mathcal{P}_{out}^{lim}(R_s)$ and $C_{out}^{lim}(\epsilon)$, since they are derived based on the asymptotic secrecy capacity as the transmitting power P goes to infinity (i.e., high SNR).

Theorem 1. *If the main channel is correlated with the eavesdropper channel and the joint PDF of them follows the bivariate Rayleigh distribution, as the transmission power P increases, the outage probability for a target secrecy rate R_s is lower bounded by*

$$\begin{aligned}\mathcal{P}_{out}^{lim}(R_s) &= \mathcal{P}\left(C_s^{lim} \leqslant R_s\right) \\ &= \frac{1}{2} + \frac{2^{R_s}-\kappa}{2\sqrt{(2^{R_s}+\kappa)^2 - 4\rho\kappa 2^{R_s}}};\end{aligned} \tag{3.9}$$

and the outage secrecy capacity is upper bounded by

$$C_{out}^{lim}(\epsilon) = \begin{cases} \left[\log\left(-\kappa\left(\sqrt{\varphi^2-1}+\varphi\right)\right)\right]^+, \text{ if } 0<\epsilon\leq\frac{1}{2}; \\ \left[\log\left(\kappa\left(\sqrt{\varphi^2-1}-\varphi\right)\right)\right]^+, \text{ if } \frac{1}{2}<\epsilon<1. \end{cases} \tag{3.10}$$

where $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$, $[x]^+ = max\{0, x\}$ and ϵ is the specified outage probability.

Proof.

$$\begin{aligned}\mathcal{P}_{out}^{lim}(R_s) &= \mathcal{P}\left(C_s^{lim} \leqslant R_s\right) \\ &= 1 - \mathcal{P}\left(C_s^{lim} > R_s\right).\end{aligned}$$

By substituting (3.7) into the above equation, the result (3.9) then follows.

We continue to prove the the Eq. (3.10). we will first show that $C_{out}^{lim}(\epsilon)$ equals the target secrecy rate R_{st} under the condition that $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$, and then determine the actual value of $C_{out}^{lim}(\epsilon)$ based on the monotonicity of $\mathcal{P}_{out}^{lim}(R_{st})$ with respect to R_{st}.

Based on (3.9), the derivative of $\mathcal{P}_{out}^{lim}(R_{st})$ is given by

$$\left(\mathcal{P}_{out}^{lim}(R_{st})\right)' = \frac{2^{R_{st}}\kappa(1-\rho)\left(2^{R_{st}}+\kappa\right)\ln 2}{\left[\left(2^{R_{st}}+\kappa\right)^2 - 4\kappa\rho 2^{R_{st}}\right]^{3/2}}. \tag{3.11}$$

Since $R_{st} > 0$, $\kappa > 0$ and $0 \leq \rho < 1$, it is easy to see that $2^{R_{st}}\kappa(1-\rho)\left(2^{R_{st}}+\kappa\right)\ln 2 > 0$. Moreover, we have $\left(2^{R_{st}}+\kappa\right)^2 - 4\kappa\rho 2^{R_{st}} > 0$ due to that $2^{2R_{st}} + \kappa^2 \geq 2\kappa 2^{R_{st}} > 2\kappa\rho 2^{R_{st}}$. Therefore, we have $\left(\mathcal{P}_{out}^{lim}(R_{st})\right)' > 0$, which indicates $\mathcal{P}_{out}^{lim}(R_{st})$ monotonically increases with R_{st}. In other words, R_{st} monotonically increases with the outage probability. Thus, according to the definition of ϵ-outage secrecy capacity in (3.8), we find that $C_{out}^{lim}(\epsilon) = R_{st}$ with condition that $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$.

By letting $\mathcal{P}_{out}^{lim}(R_{st}) = \epsilon$, we get

$$\left(2^{R_{st}} + \kappa\varphi\right)^2 = \kappa^2\left(\varphi^2 - 1\right), \tag{3.12}$$

where $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$. The derivative of φ with respect to ϵ can be derived by

$$\varphi' = -\frac{8(2\epsilon-1)(1-\rho)}{\left[(2\epsilon-1)^2-1\right]^2}. \tag{3.13}$$

From (3.13), we find the fact that φ monotonically increases with ϵ in the region $\epsilon \in (0, 1/2]$ and strictly decreases with ϵ in the region $\epsilon \in (1/2, 1)$, and the maximum value is achieved as $\varphi = -1$ at the point $\epsilon = 1/2$. We then let $f_1(\varphi) = -\kappa\left(\sqrt{\varphi^2-1}+\varphi\right)$

and $f_2(\varphi) = \kappa\left(\sqrt{\varphi^2-1}-\varphi\right)$. We find the fact that $f_1(\varphi)$ monotonically increases with φ and $f_2(\varphi)$ monotonically decreases with φ in the region $\varphi \in (-\infty, -1)$. Combining the above two facts and also the fact that $C_{out}^{lim}(\epsilon)$ monotonically increases with ϵ, the result (3.10) then follows. □

Remark 2.

1) From (3.9), when $R_s \to 0$ and $\rho \to 0$, it follows that ,

$$\mathcal{P}_{out}^{lim} \to \frac{1}{1+\kappa},$$

which corresponds to the independent channel case in [3].

2) When the main and eavesdropper channels are completely correlated, i.e., $\rho \to 1$, the outage probability for a target secrecy rate R_s becomes

$$\lim_{\rho\to 1} \mathcal{P}_{out}^{lim}(R_s) = \begin{cases} 0, & \text{if } R_s < \log\kappa; \\ 1, & \text{if } R_s \geq \log\kappa. \end{cases} \tag{3.14}$$

On one hand, (3.14) shows that outage must happen when the target secrecy rate R_s is greater than the asymptotic secrecy capacity at the average channel power gain ratio (i.e., $R_s \geq \log\kappa$). On the other hand, if the main and eavesdropper channels are completely correlated, the information outage can be avoided by choosing a target secrecy rate R_s less than the asymptotic secrecy capacity at the average channel power gain ratio (i.e., $R_s < \log\kappa$).

3) Regardless of the correlation coefficient, the outage probability goes to 0 if the target secrecy rate is far below the asymptotic secrecy capacity at the average channel power gain ratio (e.g., $R_s \ll \log\kappa$), and goes to 1 if the target secrecy rate is far above the asymptotic secrecy capacity at the average channel power gain ratio (e.g., $R_s \gg \log\kappa$).

About the impact of correlation on the asymptotic outage secrecy capacity, we have the following lemma.

Lemma 2. *When $0 < \epsilon \leq \frac{1}{2}$, $C_{out}^{lim}(\epsilon)$ increases as the correlation coefficient ρ grows; when $\frac{1}{2} < \epsilon < 1$, it decreases as ρ grows.*

Proof. First, since $\epsilon \in (0,1)$ and $\rho \in [0,1)$, it is easy to derive that $\varphi = \frac{(2\epsilon-1)^2(1-2\rho)+1}{(2\epsilon-1)^2-1}$ is monotonically increasing with respect to ρ and $\varphi < 0$. Second, let $f_1(\varphi) = -\kappa\left(\sqrt{\varphi^2-1}+\varphi\right)$ and $f_2(\varphi) = \kappa\left(\sqrt{\varphi^2-1}-\varphi\right)$. Then, the derivatives of them are given by

$$f_1^{'}(\varphi) = -\kappa\left(1+\frac{\varphi}{\sqrt{\varphi^2-1}}\right) \tag{3.15}$$

and

$$f_2^{'}(\varphi) = \kappa\left(-1+\frac{\varphi}{\sqrt{\varphi^2-1}}\right), \tag{3.16}$$

respectively. Since $\kappa > 0$ and $\varphi < 0$, we can find that $f_1^{'}(\varphi) > 0$, which indicates that $f_1(\varphi)$ monotonically increases with $\varphi < 0$, and $f_2^{'}(\varphi) < 0$, which indicates that $f_2(\varphi)$ monotonically decreases with $\varphi < 0$. Finally, combined with the fact that the logarithm does not change the monotonicity, the above lemma can be proved. □

3.5 Numerical Results and Discussions

Based on the theoretical models derived in this chapter, this section provides some numerical values to explore the potential impact of channel correlation on the outage performances and also some inherent performance tradeoffs.

3.5.1 Impact of Correlation on Outage Probability

From (3.9), it is easy to find that when the target secrecy rate R_s is less than the asymptotic secrecy capacity at CGR κ (i.e., $R_s < \log\kappa$), the outage probability that can be achieved is less than 1/2. When the target secrecy rate R_s is greater than the asymptotic secrecy capacity at CGR κ (i.e., $R_s > \log\kappa$), we can still transmit a secret message but with outage probability greater than 1/2. It means that when the

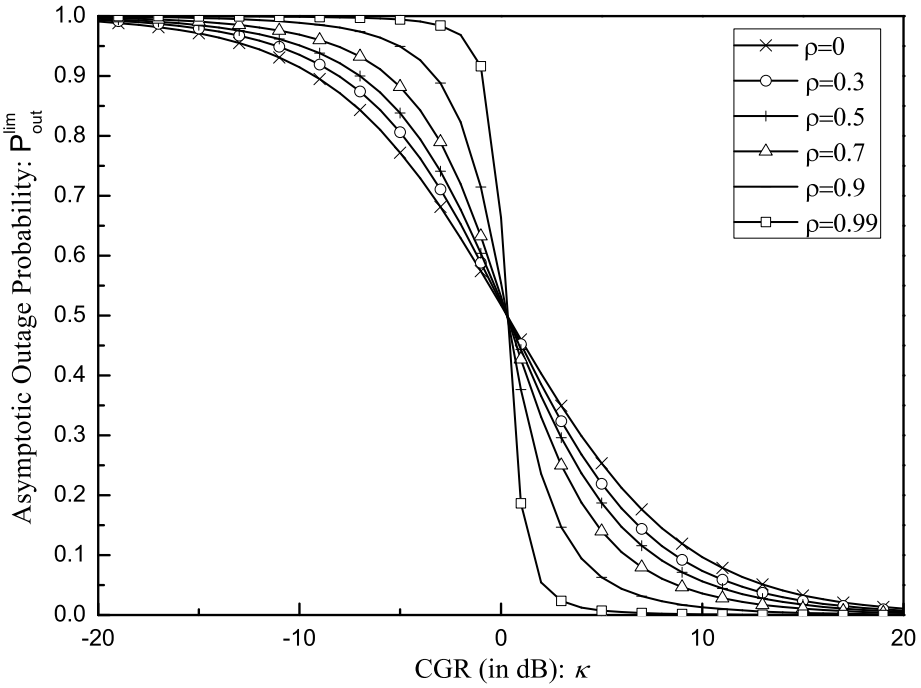

Figure 3-1: Asymptotic outage probability vs. channel power gain ratio (CGR) κ, for some selected values of ρ and $R_s = 0.1$.

main channel is better than the eavesdropper channel (i.e., $\kappa > 1$), we can achieve a positive outage secrecy capacity with outage probability less than 1/2 irrespective of correlation level.

To examine the impact of CGR and PCC on the outage probability, Fig. 3-1 depicts the asymptotic outage probability versus CGR, for some selected values of PCC and for the target secrecy rate R_s equal to 0.1 bits. It is noticed that the asymptotic outage probability decreases as the CGR grows, which is reasonable since the outage probability decreases as the main channel gets better. Moreover, if the asymptotic secrecy capacity at CGR $\log \kappa$ is larger than the target secrecy rate $R_s = 0.1$ bits (i.e., $\kappa > 0.3$ dB), then the asymptotic outage probability is less than 1/2; otherwise the outage probability becomes greater than 1/2. It is also important to observe that the impact of correlation on the asymptotic outage probability has different behaviors in the low and high CGR regimes. In the low CGR regime, the outage probability increases as the correlation grows. However, in the high CGR regime, the outage probability decreases as the correlation grows. Thus, the possible

correlation should be considered to determine the target secrecy rate or the outage probability in real applications. Notice that channel correlation becomes helpful only when $\kappa > 0$ dB and $R_s < \log \kappa$ (i.e., $P_{out} < 1/2$). If the main channel's average gain is worse than the eavesdropper's (i.e., $\kappa < 0$ dB), a positive secrecy rate can still be achieved, though the corresponding outage probability will be over 1/2. The above phenomenon is reasonable since if $\kappa > 0$ dB, then the larger the correlation level, the higher the probability of having $H_m > H_e$.

3.5.2 Impact of Correlation on Outage Secrecy Capacity

Now, we investigate the impact of correlation on the outage secrecy capacity at the low and high outage probabilities, respectively [4].

Figs. 3-2 and 3-3 depict the asymptotic outage secrecy capacity versus CGR, for some selected values of PCC and for the case that the asymptotic outage probability is less than 1/2 (0.1 here) and the case that the asymptotic outage probability is larger than 1/2 (0.75 here), respectively. We can see that the asymptotic outage secrecy capacity grows as the CGR increases for both outage probability requirements there. For the same CGR and the same PCC, it is also noticed that the asymptotic outage secrecy capacity grows as the outage probability increases. Furthermore, the asymptotic outage secrecy capacity increases as the PCC grows when the outage probability is less than 1/2, while it degrades as the PCC grows when the outage probability is greater than 1/2, which indicates that the correlation is helpful when $\epsilon < 1/2$ but becomes harmful when $\epsilon > 1/2$. Notice that the numerical results agree with the theoretical analysis in Lemma 2 well. The physical reason of such phenomenon is given as follows. Let U_{st} denote the target channel power gain ratio (i.e., $U_{st} = 2^{R_s}$). From (3.9), it is obvious that $U_{st} < \kappa$ when $\epsilon < 1/2$ and $U_{st} > \kappa$ when $\epsilon > 1/2$. As the PCC ρ grows, the power gain of the main channel H_m and that of the eavesdropper channel H_e vary much more similarly for any coherence interval, which indicates that the probability of having the real time channel power gain ratio

[4] Although the high outage probability is not pursued in real applications, it is desirable for us to understand the impact of correlation under this scenario.

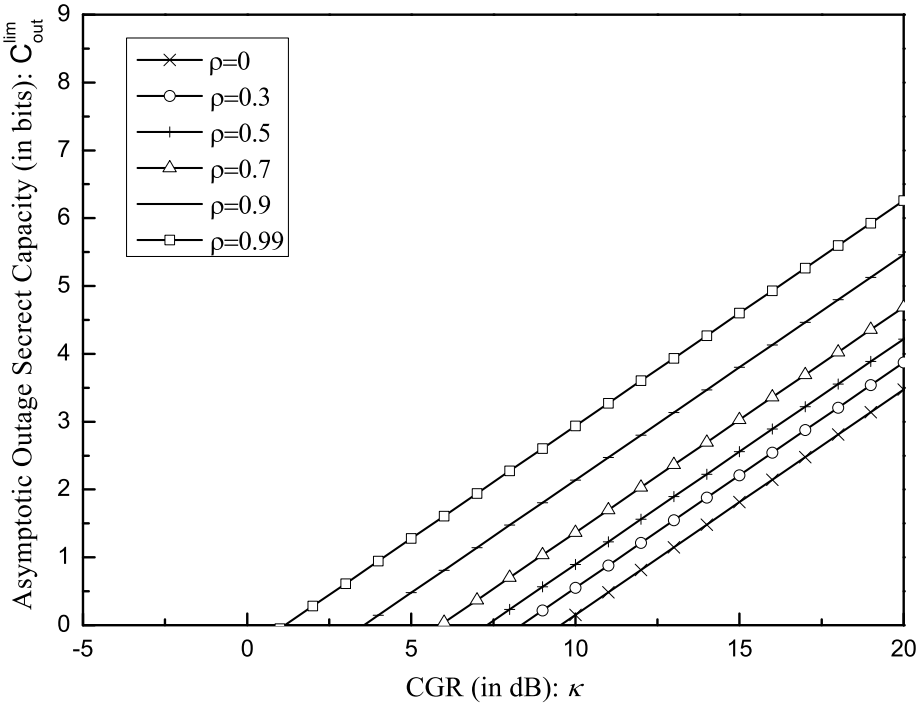

Figure 3-2: Asymptotic outage secrecy capacity vs. channel power gain ratio (CGR) κ, for some selected values of ρ and $\epsilon = 0.1$.

$U = H_m/H_e$ close to the average one $\kappa = \mathbb{E}[H_m]/\mathbb{E}[H_e]$ increases (i.e., the variance of U decreases in statistics). Thus, the value of the target channel power gain ratio U_{st} for a specified ϵ increases as ρ grows when $U_{st} < \kappa$, and decreases as ρ grows when $U_{st} > \kappa$. Therefore, the target secrecy rate R_s and thus the asymptotic outage secrecy capacity increases as the PCC grows when $\epsilon < 1/2$, but decreases when $\epsilon > 1/2$.

3.5.3 Outage Probability vs. Outage Secrecy Capacity

In this subsection, we examine the relation between the asymptotic outage probability and asymptotic outage secrecy capacity under the following three cases: 1) the main channel's condition is better than the eavesdropper's; 2) the main channel's condition is the same as the eavesdropper's; 3) the main channel's condition is worse than the eavesdropper's.

Figs. 3-4, 3-5 and 3-6 show the asymptotic outage secrecy capacity versus outage probability for some selected values of PCC and for the three scenarios that the

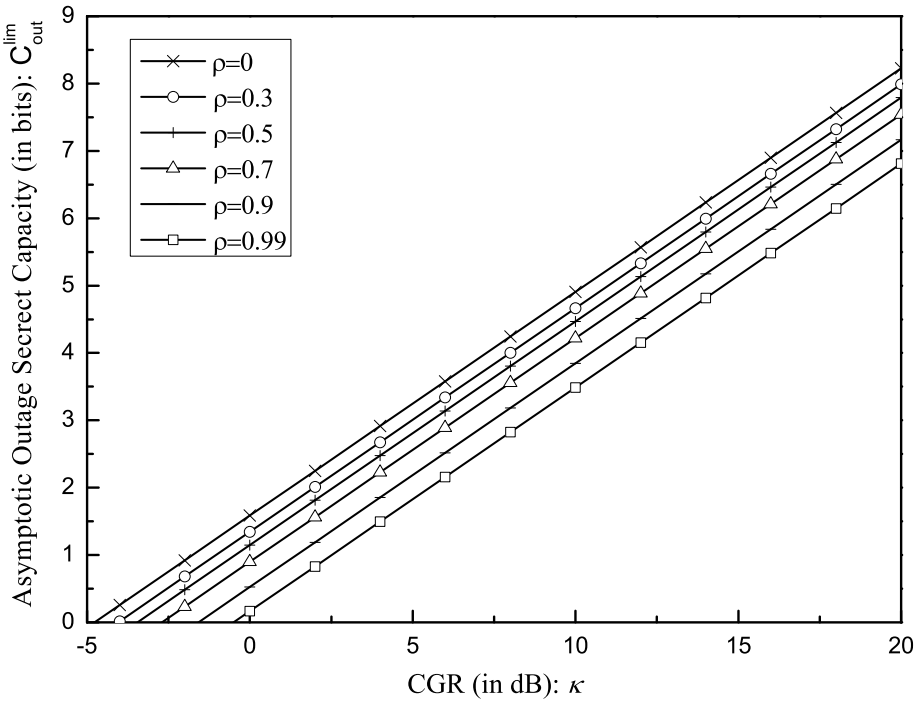

Figure 3-3: The asymptotic outage secrecy capacity vs. channel power gain ratio (CGR), for some selected values of ρ and $\epsilon = 0.75$.

main channel's condition is better than the eavesdropper's ($\kappa = 10$ dB), the main channel's condition is the same as the eavesdropper's ($\kappa = 0$ dB) and the main channel's condition is worse than the eavesdropper's ($\kappa = -10$ dB). In Fig. 3-5, it is noticed that the outage secrecy capacity is 0 when the outage probability is less than 0.5. In Fig. 3-6, it is also noticed that the positive outage secrecy capacity can be achieved even when the main channel's condition is much worse than the eavesdropper's, even though the outage probability is greater than 0.9. This is due to the reason that, although $\mathbb{E}[H_m] < \mathbb{E}[H_e]$ (i.e., $\kappa < 0$ dB), it is possible to have coherence intervals during which H_m is larger than H_e since both the main and eavesdropper channels are fading and not perfectly correlated there. From the three figures, we can find that for a given outage probability the asymptotic outage secrecy capacity at $\kappa = 10$ dB is the largest in comparison with the other two cases, which indicates that the main channel's condition should be maintained as good as possible. Moreover, one can observe from Fig. 3-4 that the correlation between the main and eavesdropper channels is constructive when the outage probability is less than 1/2,

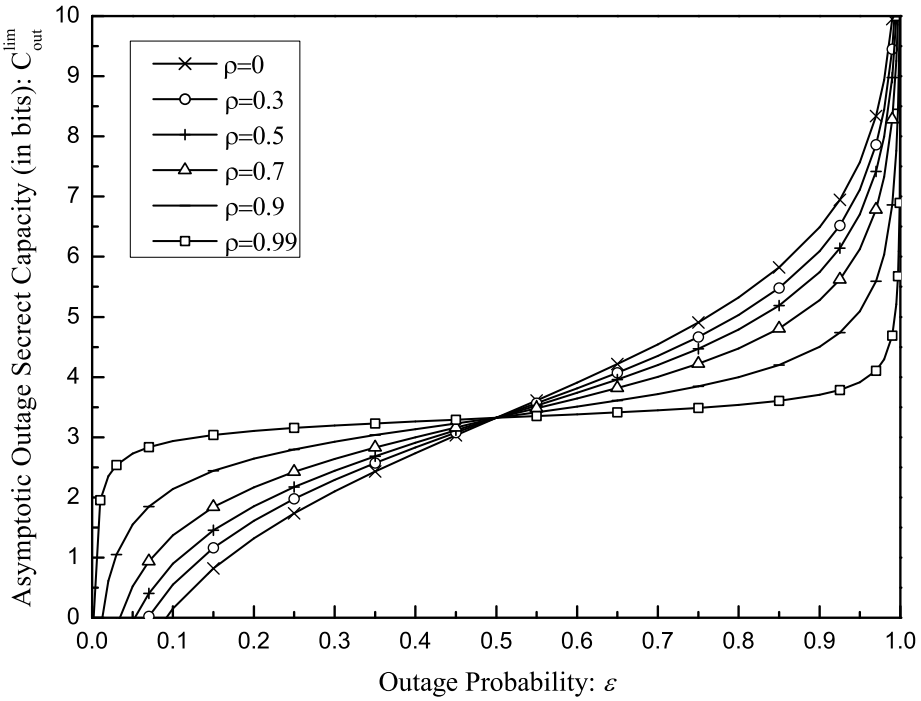

Figure 3-4: Asymptotic outage secrecy capacity vs. outage probability, for some selected values of ρ and $\kappa = 10$ dB.

and becomes destructive when the outage probability is greater than 1/2. It is also observed that the outage secrecy capacity can be enlarged by allowing a larger outage probability.

3.5.4 PCC vs. CGR

It is noticed from the above discussions that channel correlation becomes helpful when the target transmission rate is less than the asymptotic secrecy capacity at the CGR. So, it is desirable to make the PCC as high as possible while keeping the CGR high in a practical design of wireless communication. However, in real wireless networks, an active eavesdropper can not only increase the PCC but also decrease the CGR by approaching the legitimate receiver on purpose. Two natural questions are: What is the tradeoff between the CGR and PCC? Is it necessary to keep a guard zone, defined as the region around the receiver in which the eavesdroppers are not allowed?

Figs. 3-7 and 3-8 show examples of the tradeoff between CGR and PCC for some selected target secrecy rates and for the cases that outage probability is less than 1/2

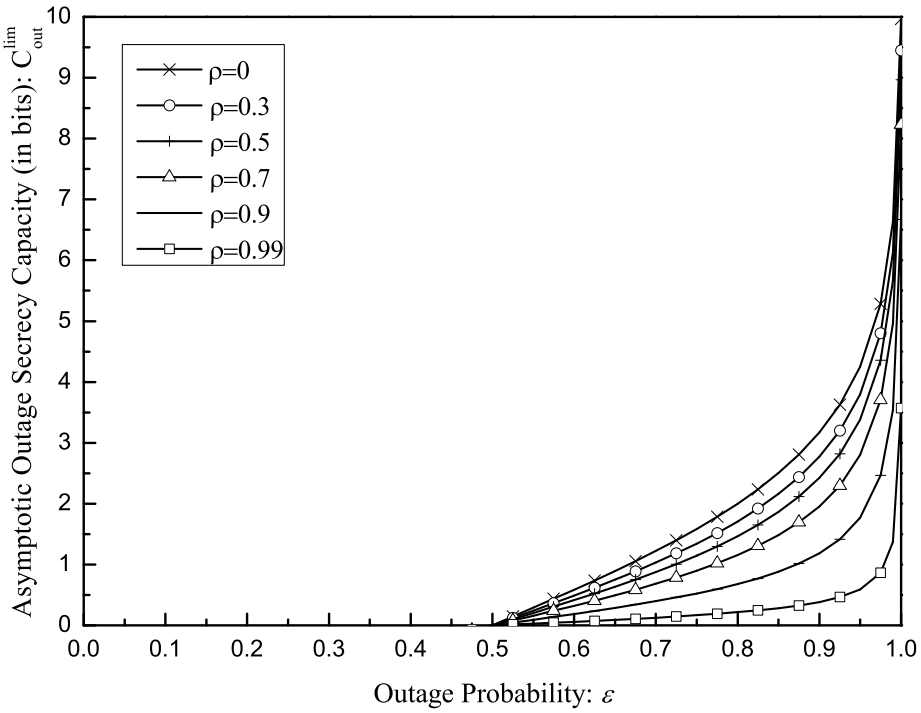

Figure 3-5: Asymptotic outage secrecy capacity vs. outage probability, for some selected values of ρ and $\kappa = 0$ dB.

(0.1 here) and larger than 1/2 (0.75 here), respectively. It is observed that the CGR decreases as the PCC grows for the case when the outage probability is less than 1/2, while the CGR increases as the PCC grows for the case when the outage probability is greater than 1/2, which confirms our previous result that channel correlation becomes helpful if the target transmission rate is less than the asymptotic secrecy capacity at the CGR. Moreover, a more exact tradeoff between CGR and PCC is needed so that it can provide a baseline to determine if an eavesdropper's approaching is harmful or not. We draw lines $\kappa = 12$ dB and $\kappa = 2$ dB in the Figs. 3-7 and 3-8, respectively, and find that to increase one bit in the target transmission rate, a more than fifty percent improvement of correlation level is needed for a fixed CGR, or about 3 dB improvement of CGR is needed for a specified PCC. Thus, in practical network design, if an eavesdropper is approaching the main receiver to eavesdrop messages, the situation for the eavesdropper does not become better if the PCC is increased more than fifty percent when the CGR is decreased less than about a 3 dB, which is a very impressive result for current studies which always assume the eavesdropper's

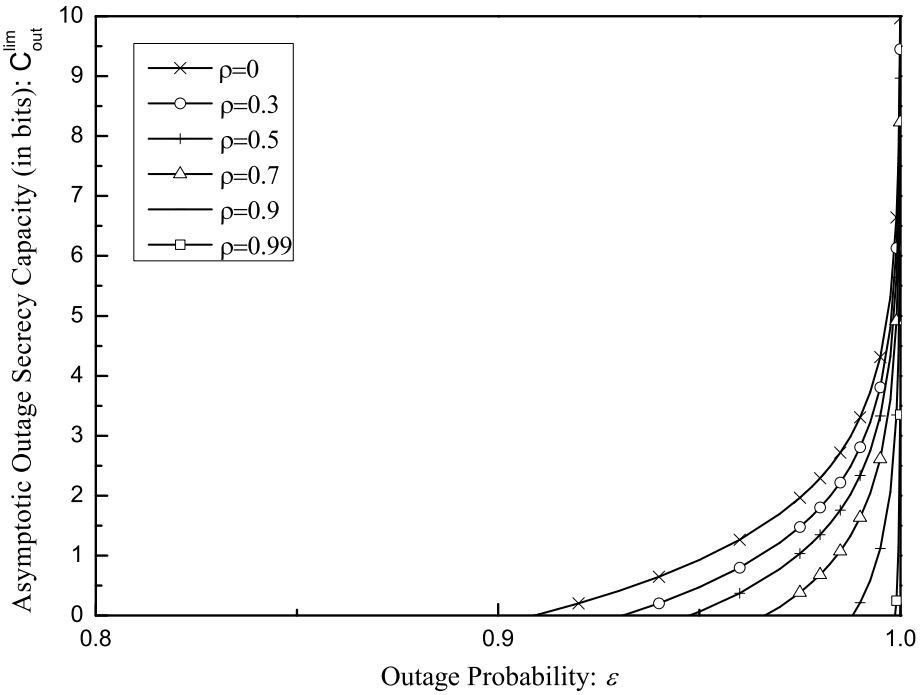

Figure 3-6: Asymptotic outage secrecy capacity vs. outage probability, for some selected values of ρ and $\kappa = -10$ dB.

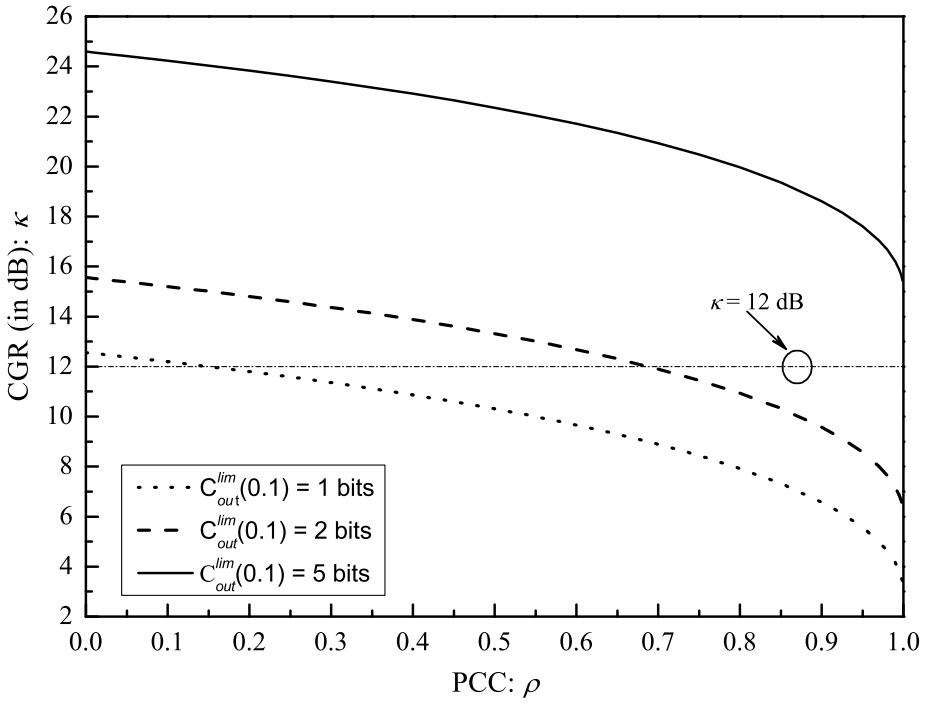

Figure 3-7: Channel power gain ratio (CGR) vs. channel power correlation coefficient (PCC), for some selected values of target secrecy rates with the outage probability $\epsilon = 0.1$.

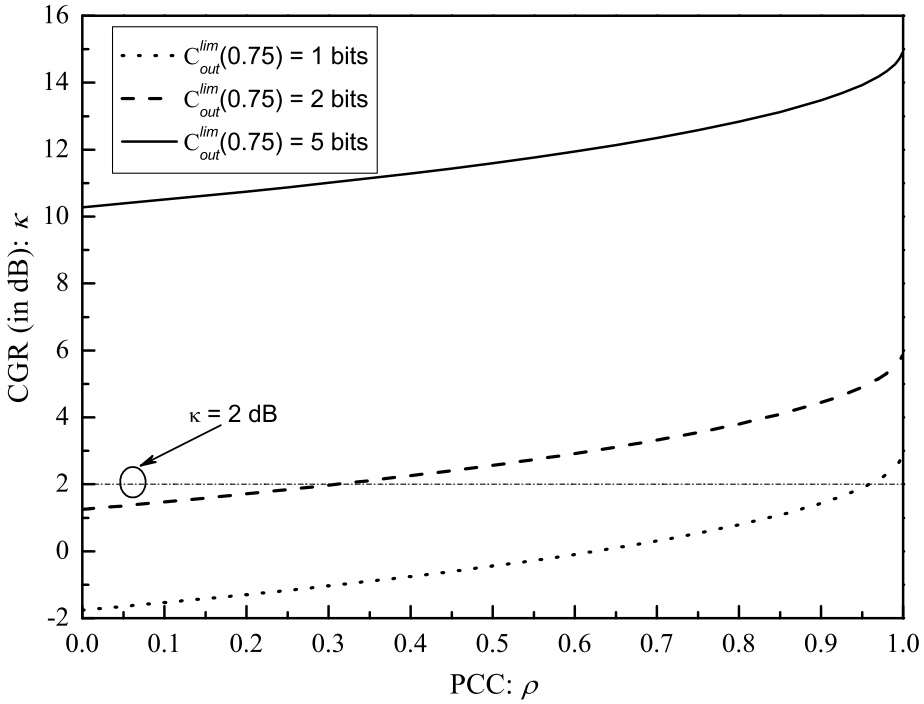

Figure 3-8: Channel power gain ratio (CGR) vs. channel power correlation coefficient (PCC), for some selected values of target secrecy rates with the outage probability $\epsilon = 0.75$.

approach is destructive.

3.5.5 Ergodic Secrecy Capacity vs. Outage Secrecy Capacity

In this subsection, we show the differences between the results in this chapter and the previous results in [19] which consider the asymptotic ergodic secrecy capacity of the correlated Rayleigh fading wiretap channel.

Figs. 3-9 and 3-10 compare the asymptotic ergodic secrecy capacity (i.e., equation (5) in [19]) with the asymptotic outage secrecy capacity (i.e., equation (3.10) in this chapter) under the assumption that the channels are independent and correlated, respectively. It is noticed that the asymptotic outage secrecy capacity is no larger than the asymptotic ergodic secrecy capacity when the allowed outage probability is small (0.1 here). However, if the allowed outage probability can be larger (0.75 here), the corresponding asymptotic outage secrecy capacity is much larger than the asymptotic ergodic secrecy capacity. Moreover, it is also observed that the difference between the

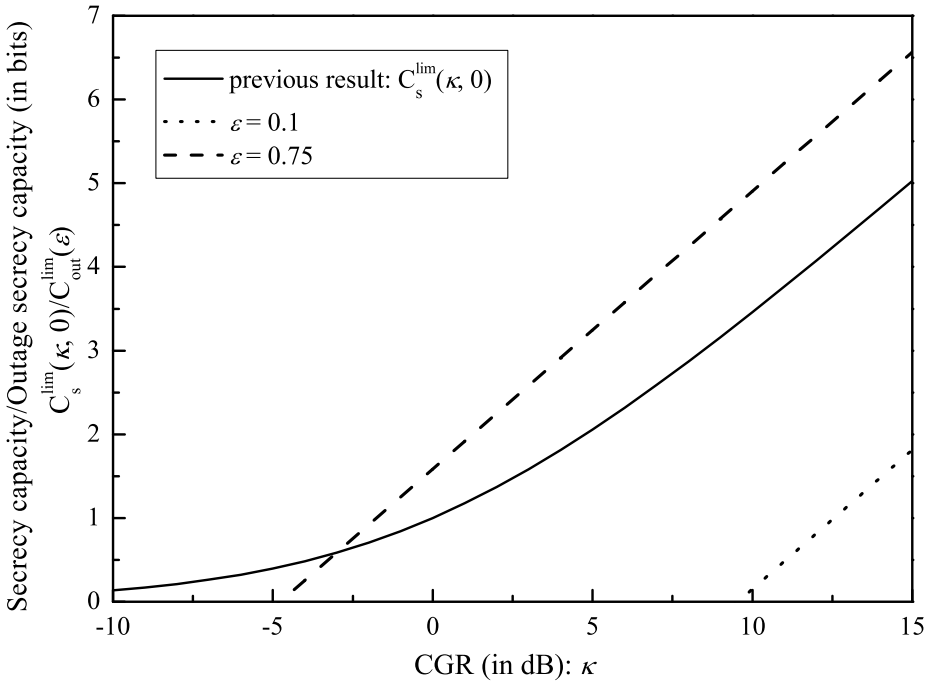

Figure 3-9: Asymptotic ergodic secrecy capacity/asymptotic outage secrecy capacity vs. channel power gain ratio (CGR) when the channels are independent.

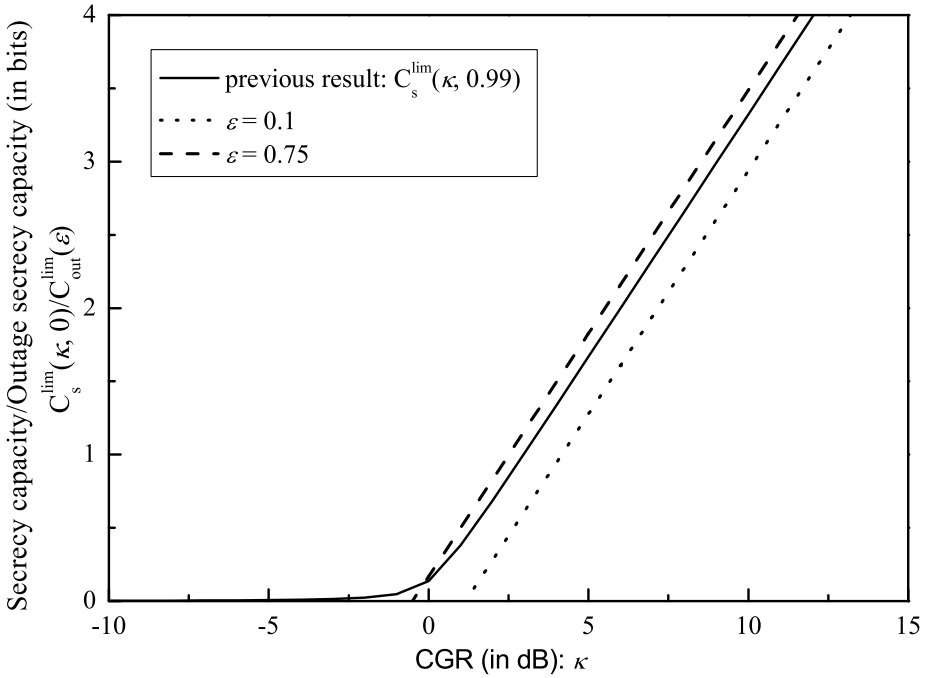

Figure 3-10: Asymptotic ergodic secrecy capacity/asymptotic outage secrecy capacity vs. channel power gain ratio (CGR) when the channels are highly correlated.

asymptotic ergodic secrecy capacity and asymptotic outage secrecy capacity becomes less as the correlation level grows irrespective of outage probability. It is important to notice that the above ergodic secrecy capacity is achieved under the assumption that the CSIs of both the main and eavesdropper channels are available. For situations when full CSI cannot be achieved before transmission or when the delay-limited transmission is required, the transmitter has to transmit the information with some probability of outage and the outage secrecy capacity becomes the main performance measure to refer to.

3.6 Summary

In this chapter, we derived the closed-form expressions of the asymptotic outage probability and asymptotic outage secrecy capacity under the correlated Rayleigh fading wiretap channel, which cover the special cases when the main and eavesdropper channels are independent. Unlike Shannon's result for channel capacity that increases with transmission power, the asymptotic secrecy capacity is found to be controlled by the channel power gain ratio, rather than the transmission power. We analyzed the impact of correlation on the asymptotic outage probability and asymptotic outage secrecy capacity, and observed that the asymptotic outage probability decreases as the channel correlation grows in the high CGR regime, and the asymptotic outage secrecy capacity increases as the channel correlation grows when the outage probability is less than 1/2. Then, we analyzed the tradeoff between the asymptotic outage secrecy capacity and outage probability which showed that the asymptotic outage secrecy capacity can be increased by sacrificing the outage probability. Furthermore, the tradeoff between the PCC and CGR is discussed, from which we find that the situation for the eavesdropper does not become better if the PCC is increased more than fifty percent while the CGR is decreased less than about 3 dB. This represents the scenario that the eavesdropper is approaching the main receiver on purpose. Remarkably, our results reveal that the correlation between the main and eavesdropper channels becomes helpful when the main channel's average channel gain is better than the

eavesdropper channel's and the outage probability is less than 1/2, and becomes harmful otherwise.

Chapter 4

Physical Layer Security under Limited Transmission Power

This chapter extends the study to a more practical case of limited transmission power, and address the problem of reliable and secure transmission design for the correlated fading wire-tap channel under the partial CSI assumption.

4.1 Motivation and Outline

It is noticed that the study of secure information transmission under the basic fading wire-tap channel serves as a foundation for secure information transmission in general wireless networks. The available studies of physical layer security (PLS) under the fading wire-tap channel either focus on the study under the independent fading channels or asymptotic results as the transmission power goes to infinity under the correlated fading channels. The available studies of physical layer security (PLS) under the fading wire-tap channel either focus on the study under the independent fading channels or asymptotic results as the transmission power goes to infinity under the correlated fading channels. Therefore, the performance of physical layer security under the general correlated fading wire-tap channel with a practical power constraint is still unexplored. Motivated by the above observations, this chapter aims to provide a comprehensive study on the fundamental performance limits of physical layer

security under a fading wire-tap channel, where the main channel is correlated with the eavesdropper channel and the transmitter knows only the instantaneous CSI of main channel.

The remainder of this chapter is organized as follows. We introduces in Section 4.2 the previous studies that have directly relation with this chapter's contents. In Section 4.3, we first describes the physical layer security method for the concerned wire-tap channel model in detail, and then proposes three metrics to fully depict the fundamental performance of applying physical layer security to achieve secure and reliable information transmission over the correlated fading wire-tap channel. Then Section 4.4 derives a closed-form secrecy capacity for the concerned correlated fading wire-tap channel based on the typical Marcum Q function. In Section 4.5, the transmission outage probability and secrecy outage probability are derived to depict the levels of reliability and security, respectively. Based on the above theoretical models, numerical results are provided in Section 4.6. Finally, we conclude in Section 4.7 the main results of this chapter.

4.2 Related Research Works

Adopting the physical layer security method to ensure the secure and reliable information transmission over the fading wire-tap channels has been extensively studied, for both the independent channels scenario and correlated channels scenario.

For the independent channels scenario, Bloch *et al.* [4] derived closed-form expressions of both the secrecy capacity and outage probability for the Rayleigh fading wire-tap channel. For the fading wire-tap channel with full CSI or partial CSI, Gopala *et al.* [14] characterized the corresponding ergodic secrecy capacity under the optimum power allocation strategy. Zhou *et al.* [87] considered the Rayleigh fading wire-tap channel and studied the secure and reliable information transmission there when the real time CSI of the eavesdropper channel is not known at the transmitter. They defined the secrecy outage probability as the probability of having only insecure transmissions, which is different from the conventional outage probability defined as

the probability of having either unreliable or insecure transmissions. Remarkably, the above works reached a promising conclusion that using fading property alone can achieve information-theoretic security, even when the main channel has a worse average channel gain than that of the eavesdropper channel.

For the correlated fading wire-tap channel. Jeon *et al.* [19] investigated the secrecy capacity of an ergodic fading wire-tap channel under the full CSI assumption, where a closed-form expression of the asymptotic secrecy capacity was derived under the infinite transmission power assumption. The results in [19] indicate that an excessive large transmission power does not necessarily result in an improvement in the secrecy capacity but the channel correlation always results in a degradation in the secrecy capacity.

4.3 System Assumptions and Performance Metrics

Recall the outage probability defined in Chapter 3 is given by

$$\mathcal{P}_{out}(R_s) = \mathcal{P}(C_s < R_s). \tag{4.1}$$

In this definition, an outage happens whenever the instantaneous secrecy capacity C_s is less than a target secrecy rate R_s, which includs the instants when a message transmission is unreliable (i.e., $C_m < R_s$, which means that the main receiver Bob cannot decode the message) and when it is not perfectly secured (i.e., $C_s < R_s$, which indicates that there is some information leakage to Eve). Although this outage formula gives a fundamental characterization of the possibility of having a reliable and secure transmission, it does not distinguish between reliability and security. Therefore, in this chapter, we will introduce two new outage metrics to characterize the level of reliability and security respectively for the concerned wiretap channel model.

4.3.1 Transmission Scheme

We now give a more detailed introduction about the transmission scheme adopted for the physical layer security method. First, about transmission power control, we consider a simple scheme where the transmission power is always fixed as P under any fading state. With such a power control, the instantaneous signal-to-noise ratio (SNR) γ_m at Bob and SNR γ_e at Eve are then determined as

$$\gamma_m = \frac{Ph_m}{N_m}, \tag{4.2}$$

$$\gamma_e = \frac{Ph_e}{N_e}. \tag{4.3}$$

Second, for the coding of secret messages over codewords, the general idea of coding scheme is adopted as follows. Let R_t denote the rate of transmission codewords and R_s denote the rate of secret messages (thus $M = 2^{nR_s}$). The encoder first generates 2^{nR_t} different binary sequences of length nR_t bits, and then independently assigns each of them to one of the secret messages $\{1, \ldots, M\}$, following a uniform distribution. To encode a particular message w, the encoder randomly selects a binary sequence from the set of sequences assigned to w, and then encodes this sequence into a codeword with length n. The settings of R_t and R_s are subject to the following constraints: if the main channel's capacity C_m is no less than R_t, then Bob will receive the codeword reliably and thus recover the secret message; if the eavesdropper channel's capacity C_e is no larger than[1] $R_t - R_s$, the eavesdropper can be kept ignorant about the secret message w [14, 32].

Finally, the following transmission scheme is adopted for transmission rate control. With the main channel's real time CSI and thus SNR γ_m, Alice will transmit whenever γ_m exceeds some SNR threshold $\mu \geq 0$, where the transmission codewords rate R_t she adopts will be set to C_m, i.e., the capacity of the main channel and thus the maximum information rate that can be reliably received by Bob. The secrecy rate, which measures the rate of confidential messages hidden in the transmission of

[1] $R_t - R_s$ reflects the rate cost of securing the message transmission against eavesdropping.

codewords, will be fixed to R_s for any transmission interval. This is because the absence of real time CSI of eavesdropper channel at Alice sheds doubt on the operational significance of adopting a varying secrecy rate.

Remark 3. *It is notable that the instantaneous CSI of the main channel and the transmission threshold μ are required for the setting of R_t, while the statistical CSIs of both the main and eavesdropper channels are needed for the setting of R_s to optimize the system's performance and meet the security requirement.*

4.3.2 Performance Metrics

In the concerned system, we say a transmission is reliable if $R_t \leq C_m$, otherwise the unreliable transmission happens; we say a transmission is secure if $R_t - R_s \geq C_e$, otherwise the insecure transmission happens. The secrecy rate R_s is said to be achievable iff the transmission with R_s is both reliable and secure.

To fully depict the performance of the concerned wire-tap fading channel, the following three metrics will be adopted.

- Secrecy Capacity: The maximum achievable secrecy rate averaged over all states of the time-varying channel.
- Transmission Outage Probability: We call transmission outage happens if either a unreliable transmission or transmission suspension happens. The transmission outage probability is then defined as the probability that the transmission outage happens.
- Secrecy Outage Probability: We call secrecy outage happens if an insecure transmission is conducted. The secrecy outage probability is thus defined as the probability that the secrecy outage happens.

4.4 Secrecy Capacity

Secrecy capacity, which defines the tightest upper bound on the amount of information that can be reliably and securely transmitted over a communication channel, can help

us to understand the performance limits of the wire-tap channel systems and thus serve as an instruction guideline for the performance optimization and engineering of such systems.

About the evaluation of secrecy capacity for the wire-tap fading channel, we have the following lemma.

Lemma 3. *For the concerned fading wire-tap channel system with SNR γ_m for the main channel and SNR γ_e for the eavesdropper channel, the corresponding secrecy capacity C_s is determined as*

$$C_s = \int_0^{\infty} \int_0^{\gamma_m} \left(\log \frac{1+\gamma_m}{1+\gamma_e} \right) \times f(\gamma_m, \gamma_e) d\gamma_e d\gamma_m. \tag{4.4}$$

where $f(\gamma_m, \gamma_e)$ denotes the joint probability density function (PDF) of γ_m and γ_e.

Proof. During a coherence interval with SNR γ_m for the main channel and SNR γ_e for the eavesdropper channel, the main channel's capacity is $C_m = \log(1+\gamma_m)$ while the eavesdropper channel's is $C_e = \log(1+\gamma_e)$. In the concerned system, where R_t changes adaptively to C_m for each transmission interval, R_s is achievable if $0 < R_s \leq C_m - C_e$. Thus, the best case is that whenever $C_m > C_e$, the transmission is conducted with secrecy rate $C_m - C_e$ such that the maximum secrecy rate in that coherence interval can be achieved, while transmission is suspended whenever $C_m \leq C_e$. The secrecy capacity can then be achieved if the best case happens for each coherence interval. Therefore, by averaging the maximum achievable secrecy rate over all fading states (γ_m,γ_e), the secrecy capacity of the wire-tap channel system is determined as

$$C_s = \iint \left[\log(1+\gamma_m) - \log(1+\gamma_e) \right]^+ f(\gamma_m, \gamma_e) d\gamma_e d\gamma_m, \tag{4.5}$$

where $[x]^+ = \max\{0, x\}$. By substituting the integration intervals of γ_m and γ_e into (4.5), the result (4.4) follows. □

The Lemma 3 indicates that to evaluate the secrecy capacity, we need to first determine the PDF $f(\gamma_m, \gamma_e)$.

Lemma 4. *For the concerned fading wire-tap channel system, where the correlation coefficient between the power gains h_m and h_e is ρ ($0 \leq \rho < 1$), the joint PDF of γ_m and γ_e is determined as*

$$\begin{aligned} f(\gamma_m, \gamma_e) &= \frac{1}{\bar{\gamma}_m \bar{\gamma}_e (1-\rho)} \exp\left[-\frac{1}{1-\rho}\left(\frac{\gamma_m}{\bar{\gamma}_m} + \frac{\gamma_e}{\bar{\gamma}_e}\right)\right] \\ &\quad \times I_0\left(\frac{2}{1-\rho}\sqrt{\frac{\rho\gamma_m\gamma_e}{\bar{\gamma}_m\bar{\gamma}_e}}\right), \end{aligned} \tag{4.6}$$

where $\bar{\gamma}_m = \mathbb{E}[\gamma_m]$, $\bar{\gamma}_e = \mathbb{E}[\gamma_e]$, and $I_0(x) \triangleq \frac{1}{2\pi}\int_0^{2\pi} e^{x\cos\theta} d\theta$ is the zero-order modified Bessel function of the first kind.

Proof. For the concerned system, where the joint distribution of the two channels' gain envelops follows the bivariate Rayleigh distribution, we know from [19] that the joint PDF of h_m and h_e is given by

$$\begin{aligned} f(h_m, h_e) &= \frac{1}{\bar{h}_m \bar{h}_e (1-\rho)} \exp\left[-\frac{1}{1-\rho}\left(\frac{h_m}{\bar{h}_m} + \frac{h_e}{\bar{h}_e}\right)\right] \\ &\quad \times I_0\left(\frac{2}{1-\rho}\sqrt{\frac{\rho h_m h_e}{\bar{h}_m\bar{h}_e}}\right), \end{aligned} \tag{4.7}$$

where $\bar{h}_m = \mathbb{E}[h_m]$ and $\bar{h}_e = \mathbb{E}[h_e]$. From (4.2), (4.3) and (4.7), the joint PDF of γ_m and γ_e can be obtained as follows based on the Jacobian transformation [30],

$$\begin{aligned} f(\gamma_m, \gamma_e) &= f(\frac{N_m\gamma_m}{P}, \frac{N_e\gamma_e}{P})|J(\gamma_m, \gamma_e)| \\ &\overset{(a)}{=} f(\frac{N_m\gamma_m}{P}, \frac{N_e\gamma_e}{P})\frac{N_m N_e}{P^2} \\ &= \frac{1}{\bar{\gamma}_m \bar{\gamma}_e (1-\rho)} \exp\left[-\frac{1}{1-\rho}\left(\frac{\gamma_m}{\bar{\gamma}_m} + \frac{\gamma_e}{\bar{\gamma}_e}\right)\right] \\ &\quad \times I_0\left(\frac{2}{1-\rho}\sqrt{\frac{\rho\gamma_m\gamma_e}{\bar{\gamma}_m\bar{\gamma}_e}}\right), \end{aligned}$$

where (a) follows that

$$|J(\gamma_m, \gamma_e)| = \det\begin{bmatrix} \frac{N_m}{P} & 0 \\ 0 & \frac{N_e}{P} \end{bmatrix}.$$

□

Based on Lemma 3 and Lemma 4, we now establish the following theorem on the evaluation of secrecy capacity.

Theorem 2. *For the concerned fading wire-tap channel system with parameters γ_m, γ_e, $\bar{\gamma}_m$, $\bar{\gamma}_e$ and ρ defined above, its secrecy capacity is determined as follows:*

1) when $0 \leq \rho < 1$,

$$\begin{aligned} C_s &= e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right) - e^{\frac{1}{\bar{\gamma}_e}} E_1\left(\frac{1}{\bar{\gamma}_e}\right) \\ &\quad + \int_0^\infty \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} Q\left(\sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_m}}, \sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e \\ &\quad - \int_0^\infty \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_m}} Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e, \end{aligned} \tag{4.8}$$

where $E_1(x)$ is the exponential-integral function defined as

$$E_1(x) = \int_1^\infty \frac{\exp(-tx)}{t} dt,$$

and $Q(x, y)$ is the first order Marcum Q function defined as [6]

$$Q(x, y) = \int_y^\infty t \exp\left(-\frac{t^2 + x^2}{2}\right) I_0(xt) dt, x \geq 0, y \geq 0. \tag{4.9}$$

2) when $\rho = 1$,

$$C_s = \begin{cases} e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right) - e^{\frac{1}{\bar{\gamma}_e}} E_1\left(\frac{1}{\bar{\gamma}_e}\right), & \text{for } k > 1; \\ 0, & \text{for } 0 < k \leq 1, \end{cases} \tag{4.10}$$

here $k = \bar{\gamma}_m / \bar{\gamma}_e$.

Proof. 1) To evaluate the secrecy capacity in (4.4), we first derive the following antiderivative. Let $F(\gamma_e)$ denote the antiderivative of $f(\gamma_m, \gamma_e)$ with respect to γ_e. Since

$f(\gamma_m, \gamma_e)$ is continuous in the domain $\{(\gamma_m, \gamma_e) : \gamma_m \geq 0, \gamma_e \geq 0\}$, we have

$$\begin{aligned}
F(\gamma_e) &= \int_0^{\gamma_e} f(\gamma_m, \gamma_e) d\gamma_e \\
&\overset{(a)}{=} \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \int_0^{\sqrt{\frac{2\gamma_e}{(1-\rho)\bar{\gamma}_e}}} t e^{-\frac{t^2+x^2}{2}} I_0(xt) dt \\
&= \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \int_0^{\infty} t e^{-\frac{t^2+x^2}{2}} I_0(xt) dt \\
&\quad - \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \int_{\sqrt{\frac{2\gamma_e}{(1-\rho)\bar{\gamma}_e}}}^{\infty} t e^{-\frac{t^2+x^2}{2}} I_0(xt) dt \\
&\overset{(b)}{=} \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \left[1 - Q\left(x, \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right)\right],
\end{aligned}$$

where (a) follows by substituting $x = \sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}$ and $t = \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}$, and (b) follows from the fact that $Q(x, 0) = 1$.

By using the linearity rules of integration, the integral in (4.4) can be decomposed into the following two parts:

$$\begin{aligned}
t1 &= \int_0^{\infty} \int_0^{\gamma_m} \log(1+\gamma_m) \times f(\gamma_m, \gamma_e) d\gamma_e d\gamma_m \\
&= \int_0^{\infty} \log(1+\gamma_m) \left(\int_0^{\gamma_m} f(\gamma_m, \gamma_e) d\gamma_e\right) d\gamma_m \\
&= \frac{1}{\bar{\gamma}_m} \int_0^{\infty} \log(1+\gamma_m) \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \\
&\quad \times \left[1 - Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_e}}\right)\right] d\gamma_m
\end{aligned}$$

and

$$\begin{aligned}
t2 &= \int_0^{\infty} \int_0^{\gamma_m} \log(1+\gamma_e) \times f(\gamma_m, \gamma_e) d\gamma_e d\gamma_m \\
&\overset{(c)}{=} \frac{1}{\bar{\gamma}_m} \int_0^{\infty} \log(1+\gamma_m) \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \\
&\quad \times \left[1 - Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_e}}\right)\right] d\gamma_m \\
&\quad - \int_0^{\infty} \int_0^{\gamma_m} \frac{1}{1+\gamma_e} \times F(\gamma_e) d\gamma_e d\gamma_m,
\end{aligned}$$

where (c) follows the integration by parts. Notice that although the expressions of $t1$ and $t2$ are complex, the complexity of the derivation can be reduced since $t1$ is a part of $t2$. Therefore, the secrecy capacity can be derived as

$$\begin{aligned} C_s &= t1 - t2 \\ &= \int_0^{\infty} \int_0^{\gamma_m} \frac{1}{1+\gamma_e} \times F(\gamma_e) d\gamma_e d\gamma_m. \end{aligned} \tag{4.11}$$

We continue to evaluate (4.11) by decomposing it into the following two parts:

$$\begin{aligned} t3 &= \frac{1}{\bar{\gamma}_m} \int_0^{\infty} \int_0^{\gamma_m} \frac{1}{1+\gamma_e} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) d\gamma_e d\gamma_m \\ &= \frac{1}{\bar{\gamma}_m} \int_0^{\infty} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) \log\left(1+\gamma_m\right) d\gamma_m \\ &= \left[-e^{-\frac{\gamma_m}{\bar{\gamma}_m}} \log\left(1+\gamma_m\right)\right]_0^{\infty} + \int_0^{\infty} e^{-\frac{\gamma_m}{\bar{\gamma}_m}} \frac{1}{1+\gamma_m} d\gamma_m \\ &= e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right), \end{aligned}$$

and

$$\begin{aligned} t4 &= \int_0^{\infty} \int_0^{\gamma_m} \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m}}}{\bar{\gamma}_m\left(1+\gamma_e\right)} Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e d\gamma_m \\ &= \int_0^{\infty} \frac{d\gamma_e}{1+\gamma_e} \int_{\gamma_e}^{\infty} \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m}}}{\bar{\gamma}_m} Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_m \\ &\overset{(d)}{=} \int_0^{\infty} \frac{d\gamma_e}{1+\gamma_e} \int_{\sqrt{\gamma_e}}^{\infty} \frac{2x e^{-\frac{x^2}{\bar{\gamma}_m}}}{\bar{\gamma}_m} Q\left(\sqrt{\frac{2\rho x^2}{(1-\rho)\bar{\gamma}_m}}, \sqrt{\frac{2\gamma_e}{(1-\rho)\bar{\gamma}_e}}\right) dx \\ &\overset{(e)}{=} e^{\frac{1}{\bar{\gamma}_e}} E_1\left(\frac{1}{\bar{\gamma}_e}\right) \\ &\quad - \int_0^{\infty} \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} Q\left(\sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_m}}, \sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e \\ &\quad + \int_0^{\infty} \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_m}} Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_m}}, \sqrt{\frac{2}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e, \end{aligned}$$

where (d) is based on integration by variable substitution, and (e) follows from the equation (36) in [53]. Thus, (4.8) can be derived determined as $C_s = t3 - t4$.

2) Under the condition of $\rho = 1$, the power gains h_m and h_e are linearly dependent,

so the channel SNRs γ_m and γ_e are linearly dependent. Let $k = \bar{\gamma}_m/\bar{\gamma}_e$, we have $\gamma_e = \gamma_m/k$. Since the main channel follows the Rayleigh distribution, γ_m is exponentially distributed with its distribution function given by [4]

$$f(\gamma_m) = \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right). \tag{4.12}$$

When $\gamma_m \leq \gamma_e$ (i.e. $0 < k \leq 1$), it is easy to see that the secrecy capacity equals to 0. When $\gamma_m > \gamma_e$ (i.e. $k > 1$), the secrecy capacity is given by

$$\begin{aligned} C_s &= \int_0^\infty \log\left(\frac{1+\gamma_m}{1+\frac{\gamma_m}{k}}\right) f(\gamma_m) d\gamma_e \\ &= \int_0^\infty \log\left(\frac{k(1+\gamma_m)}{1+\frac{\gamma_m}{k}}\right) \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right) d\gamma_m \\ &= \left[-\left(\log\frac{k(1+\gamma_m)}{k+\gamma_m}\right) e^{-\frac{\gamma_m}{\bar{\gamma}_m}}\right]_0^\infty + \int_0^\infty \frac{(k-1)e^{-\frac{\gamma_m}{\bar{\gamma}_m}}}{(1+\gamma_m)(k+\gamma_m)} d\gamma_m \\ &= e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right) - e^{\frac{1}{\bar{\gamma}_e}} E_1\left(\frac{1}{\bar{\gamma}_e}\right). \end{aligned} \tag{4.13}$$

□

Remark 4. *By setting the correlation coefficient ρ in (4.8) as 0, we have*

$$\begin{aligned} C_s &= e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right) - \int_0^\infty \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_m}} Q\left(0, \sqrt{\frac{2\gamma_e}{\bar{\gamma}_e}}\right) d\gamma_e \\ &\quad - e^{\frac{1}{\bar{\gamma}_e}} E_1\left(\frac{1}{\bar{\gamma}_e}\right) + \int_0^\infty \frac{1}{1+\gamma_e} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} Q\left(\sqrt{\frac{2\gamma_e}{\bar{\gamma}_m}}, 0\right) d\gamma_e \\ &\overset{(b)}{=} e^{\frac{1}{\bar{\gamma}_m}} E_1\left(\frac{1}{\bar{\gamma}_m}\right) - e^{\left(\frac{1}{\bar{\gamma}_m}+\frac{1}{\bar{\gamma}_e}\right)} E_1\left(\frac{1}{\bar{\gamma}_m}+\frac{1}{\bar{\gamma}_e}\right), \end{aligned} \tag{4.14}$$

where (b) is due to the fact that $Q(x,0) = 1$ and $Q(0,y) = \exp\left(-\frac{y^2}{2}\right)$. It is notable that (4.14) is just the average secrecy capacity [4] for independent fading wire-tap channel under the full CSI assumption (i.e., CSI of both the main and eavesdropper channels are available at the transmitter).

4.5 Outage Performances

Transmission outage probability and secrecy outage probability are two important metrics used for efficient design of reliable and secure transmission systems. Actually, available works indicate that by allowing some probability of outage, the communication rates [33] can be increased greatly. For the concerned fading wire-tap channel, this section first evaluates the basic transmission outage probability and secrecy outage probability, and then applies them to derive a related metric, namely the overall outage probability that has been widely adopted in previous studies.

Based on the definitions in subsection 4.3, we can see that the transmission outage probability p_t and secrecy outage probability p_s can be formulated as

$$\begin{aligned} p_t &\triangleq \mathcal{P}(R_t > C_m|\text{message transmission}) \\ &\quad + \mathcal{P}(\text{message suspended}), \end{aligned} \tag{4.15}$$

$$p_s \triangleq \mathcal{P}(C_e > R_t - R_s|\text{message transmission}). \tag{4.16}$$

It is notable that the secrecy outage probability is defined in the same way as in [87].

Regarding the evaluation of p_t, we have the following theorem.

Theorem 3. *For any given transmission SNR threshold $\mu \geq 0$, the transmission outage probability p_t of the concerned fading wiretap channel is given by*

$$p_t = 1 - \exp(-\frac{\mu}{\bar{\gamma}_m}). \tag{4.17}$$

Proof. Based on the transmission scheme adopted in this chapter, the transmission, whenever conducted, is always reliable since R_t is never larger than the capacity C_m, so transmission outage happens only when transmission is suspended. Thus, the transmission outage probability is just the probability that the transmission is suspended, i.e.,

$$p_t = \mathcal{P}(\gamma_m \leq \mu) = 1 - \mathcal{P}(\gamma_m > \mu). \tag{4.18}$$

Based on (4.6), we have

$$\begin{aligned}
&\mathcal{P}(\gamma_m > \mu) \\
&\quad = \int_0^\infty \int_\mu^\infty f(\gamma_m, \gamma_e) d\gamma_m d\gamma_e \\
&\quad \overset{(a)}{=} \int_0^\infty \frac{1}{\bar{\gamma}_e} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} \int_{\sqrt{\frac{2}{1-\rho}\frac{\mu}{\bar{\gamma}_m}}}^\infty t e^{-\frac{t^2+x^2}{2}} I_0(xt) dt d\gamma_e \\
&\quad \overset{(b)}{=} \int_0^\infty \frac{1}{\bar{\gamma}_e} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} Q\left(\sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}, \sqrt{\frac{2}{1-\rho}\frac{\mu}{\bar{\gamma}_m}}\right) d\gamma_e \\
&\quad \overset{(c)}{=} 2\int_0^\infty y e^{-y^2} Q\left(\sqrt{\frac{2\rho}{1-\rho}} y, \sqrt{\frac{2}{1-\rho}\frac{\mu}{\bar{\gamma}_m}}\right) dy \\
&\quad \overset{(d)}{=} e^{-\frac{\mu}{\bar{\gamma}_m}},
\end{aligned} \tag{4.19}$$

where (a) follows by substituting $x = \sqrt{\frac{2\rho}{1-\rho}\frac{\gamma_e}{\bar{\gamma}_e}}$ and $t = \sqrt{\frac{2}{1-\rho}\frac{\gamma_m}{\bar{\gamma}_m}}$, (b) is due to the definition of the first order Marcum Q function as in (4.9), (c) follows by substituting $y = \sqrt{\frac{\gamma_e}{\bar{\gamma}_e}}$, and (d) is based on the following formula [53],

$$\begin{aligned}
&\int_{c_1}^\infty t e^{-\frac{b_1^2 t^2}{2}} Q(b_2 t, b_3) dt \\
&\quad = \frac{1}{b_1^2} e^{-\frac{b_1^2 c_1^2}{2}} Q(b_2 c_1, b_3) \\
&\qquad + \frac{1}{b_1^2} e^{-\frac{b_1^2 b_3^2}{2(b_1^2+b_2^2)}} \left[1 - Q\left(c_1\sqrt{b_1^2+b_2^2}, \frac{b_2 b_3}{\sqrt{b_1^2+b_2^2}}\right)\right].
\end{aligned}$$

The parameter b_1 here is a real number, while b_2 and b_3 are real and positive numbers. By substituting (4.19) into (4.18), the result in (4.17) follows. □

Remark 5. *Notice that (4.19) turns out to be the transmission probability under independent fading wiretap channel [87], which only depends on $\bar{\gamma}_m$ and threshold μ but is independent of correlation coefficient ρ.*

About the evaluation of secrecy outage probability p_s, we have the following theorem.

Theorem 4. *In the concerned fading wire-tap channel system with parameters γ_m, γ_e, $\bar{\gamma}_m$, $\bar{\gamma}_e$ and ρ defined above, its secrecy outage probability p_s for any given transmission*

SNR threshold $\mu \geq 0$ and secrecy rate $R_s > 0$ is determined as follows:

1) when $0 \leq \rho < 1$,

$$
\begin{aligned}
p_s = {} & e^{\frac{(1-\rho)\mu}{\alpha}} \sum_{l=0}^{\infty} \frac{(1-\rho)\rho^l}{(l!)^2} \Gamma\left(l+1, \frac{\mu}{\alpha}\right) \Gamma\left(l+1, \frac{\tau}{\beta}\right) \\
& - e^{\frac{1}{\alpha}(\tau 2^{R_s} - \rho\mu)} \sum_{l=0}^{\infty} \frac{(1-\rho)\rho^l}{l!\beta} \left(\frac{1}{\beta}\right)^l \sum_{j=0}^{l} \frac{1}{j!} \left(\frac{1}{\alpha}\right)^j \\
& \times \sum_{i=0}^{j} \binom{j}{i} 2^{iR_s} (2^{R_s}-1)^{j-i} \left(\frac{1-\rho}{\eta}\right)^{l+i+1} \Gamma\left(l+i+1, \frac{\eta\tau}{1-\rho}\right), \qquad (4.20)
\end{aligned}
$$

where $\alpha = (1-\rho)\bar{\gamma}_m$, $\beta = (1-\rho)\bar{\gamma}_e$, $\eta = \frac{1}{\bar{\gamma}_e} + \frac{2^{R_s}}{\bar{\gamma}_m}$, $\tau = \frac{1+\mu-2^{R_s}}{2^{R_s}}$, and $\Gamma(l,x)$ is the incomplete gamma function.

2) when $\rho = 1$,

$$
p_s = \begin{cases}
1, & \text{for } 0 < k \leq 1; \\
1, & \text{for } k > 1, R_s \geq \log_2 k; \\
1 - \exp\left[-\frac{1}{\bar{\gamma}_m}\left(\mu + \frac{k\left(2^{R_s}-1\right)}{k-2^{R_s}}\right)\right], & \\
 & \text{for } k > 1, \log_2 \psi < R_s < \log_2 k; \\
0, & \text{for } k > 1, R_s \leq \log_2 \psi;
\end{cases}
$$

where $\psi = \frac{k(1+\mu)}{k+\mu}$ and $k = \bar{\gamma}_m/\bar{\gamma}_e$.

Proof. 1) According to the secrecy outage formula (4.16), we have

$$
\begin{aligned}
p_s &= \mathcal{P}(C_e > C_m - R_s | \gamma_m > \mu) \qquad (4.21)\\
&= \mathcal{P}(\gamma_m < 2^{R_s}(1+\gamma_e) - 1 | \gamma_m > \mu)\\
&= \frac{\mathcal{P}(\mu < \gamma_m < 2^{R_s}(1+\gamma_e) - 1)}{\mathcal{P}(\gamma_m > \mu)}\\
&= e^{\frac{\mu}{\bar{\gamma}_m}} \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \int_{\mu}^{2^{R_s}(1+\gamma_e)-1} f(\gamma_m, \gamma_e) d\gamma_m d\gamma_e\\
&\overset{(a)}{=} e^{\frac{\mu}{\bar{\gamma}_m}} \sum_{l=0}^{\infty} \frac{\rho^l}{(l!)^2} \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \frac{1}{\bar{\gamma}_e} e^{-\frac{\gamma_e}{(1-\rho)\bar{\gamma}_e}} \left[\frac{\gamma_e}{(1-\rho)\bar{\gamma}_e}\right]^l d\gamma_e\\
&\quad \times \int_{\mu}^{2^{R_s}(1+\gamma_e)-1} \frac{e^{-\frac{\gamma_m}{(1-\rho)\bar{\gamma}_m}}}{(1-\rho)\bar{\gamma}_m} \left[\frac{\gamma_m}{(1-\rho)\bar{\gamma}_m}\right]^l d\gamma_m\\
&\overset{(b)}{=} e^{\frac{\mu}{\bar{\gamma}_m}} \sum_{l=0}^{\infty} \frac{\rho^l}{(l!)^2} \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \frac{1}{\bar{\gamma}_e} e^{-\frac{\gamma_e}{(1-\rho)\bar{\gamma}_e}} \left[\frac{\gamma_e}{(1-\rho)\bar{\gamma}_e}\right]^l d\gamma_e\\
&\quad \times \left[\Gamma\left(l+1, \frac{\mu}{(1-\rho)\bar{\gamma}_m}\right) - \Gamma\left(l+1, \frac{2^{R_s}(1+\gamma_e)-1}{(1-\rho)\bar{\gamma}_m}\right)\right]\\
&\overset{(c)}{=} e^{\frac{\mu}{\bar{\gamma}_m}} \sum_{l=0}^{\infty} \frac{(1-\rho)\rho^l}{(l!)^2} \Gamma\left(l+1, \frac{\mu}{(1-\rho)\bar{\gamma}_m}\right) \Gamma\left(l+1, \frac{\mu+1-2^{R_s}}{(1-\rho)\bar{\gamma}_e 2^{R_s}}\right)\\
&\quad - e^{\frac{\mu}{\bar{\gamma}_m} - \frac{2^{R_s}-1}{(1-\rho)\bar{\gamma}_m}} \sum_{l=0}^{\infty} \left(\frac{\rho}{1-\rho}\right)^l \frac{1}{l!} \left(\frac{1}{\bar{\gamma}_e}\right)^{l+1} \sum_{j=0}^{l} \frac{1}{j!} \left[\frac{1}{(1-\rho)\bar{\gamma}_m}\right]^j\\
&\quad \times \sum_{i=0}^{j} \binom{j}{i} \left(2^{R_s}-1\right)^{j-i} 2^{iR_s} \int_{\frac{\mu+1}{2^{R_s}}-1}^{\infty} \gamma_e^{\,l+i} e^{-\frac{1}{1-\rho}\left(\frac{1}{\bar{\gamma}_e} + \frac{2^{R_s}}{\bar{\gamma}_m}\right)\gamma_e} d\gamma_e,
\end{aligned}
$$

where (a) follows that $I_0(x) = \sum_{l=0}^{\infty} \frac{x^{2l}}{4^l (l!)^2}$, (b) is due to the definition of the incomplete gamma function

$$\Gamma(l, x) = \int_x^{\infty} t^{l-1} e^{-t} dt,$$

and (c) follows that $\Gamma(l+1, x) = l! e^{-x} \sum_{j=0}^{l} \frac{x^j}{j!}$ for $l = 0, 1, 2, \ldots$. By conducting some simplifications to the above formula, the equation (4.20) follows.

2) When $\rho = 1$, γ_e is completely determined by γ_m (i.e., $\gamma_e = \gamma_m / k$). Thus, we

have

$$\begin{aligned} p_s &= \mathcal{P}(C_e > C_m - R_s | \gamma_m > \mu) \\ &= \mathcal{P}\left(\left(2^{R_s} - k\right)\gamma_m > k\left(1 - 2^{R_s}\right) | \gamma_m > \mu\right), \end{aligned} \tag{4.22}$$

a) When $0 < k \leq 1$ (i.e., $\gamma_m \leq \gamma_e$), we have $2^{R_s} \geq 1 \geq k$ and thus

$$p_s = \mathcal{P}\left(\gamma_m > \frac{k\left(1 - 2^{R_s}\right)}{\left(2^{R_s} - k\right)} \mid \gamma_m > \mu\right) = 1. \tag{4.23}$$

It indicates that the secrecy outage happens as long as the transmission is conducted.

b) When $k > 1$ (i.e., $\gamma_m > \gamma_e$) and $R_s > \log_2 k$ (i.e., $2^{R_s} - k > 0$), we have $1 - 2^{R_s} < 0$ and thus

$$p_s = \mathcal{P}\left(\gamma_m > \frac{k\left(1 - 2^{R_s}\right)}{2^{R_s} - k} | \gamma_m > \mu\right) = 1; \tag{4.24}$$

when $k > 1$ and $R_s = \log_2 k$ (i.e., $2^{R_s} - k = 0$), we have

$$C_m - C_e = \log \frac{k(1 + \gamma_m)}{k + \gamma_m} < \log k = R_s, \tag{4.25}$$

which indicates that $p_s = 1$.

c) When $k > 1$ and $\log_2 \frac{k(1+\mu)}{k+\mu} < R_s < \log_2 k$, we have $2^{R_s} - k < 0$ and $\frac{k\left(1-2^{R_s}\right)}{2^{R_s}-k} > \mu$, so (4.22) can be derived as

$$\begin{aligned} p_s &= \frac{\mathcal{P}\left(\mu < \gamma_m < \frac{k\left(1-2^{R_s}\right)}{2^{R_s}-k}\right)}{\mathcal{P}(\gamma_m > \mu)} \\ &= e^{\frac{\mu}{\bar{\gamma}_m}} \int_{\mu}^{\frac{k\left(2^{R_s}-1\right)}{k2^{R_s}}} f(\gamma_m) d\gamma_m \\ &= 1 - \exp\left[-\frac{1}{\bar{\gamma}_m}\left(\mu + \frac{k\left(2^{R_s} - 1\right)}{k - 2^{R_s}}\right)\right]. \end{aligned} \tag{4.26}$$

d) When $k > 1$ and $R_s \leq \log_2 \frac{k(1+\mu)}{k+\mu}$, we have $2^{R_s} - k < 0$ and $\frac{k\left(1-2^{R_s}\right)}{2^{R_s}-k} \leq \mu$, so

(4.22) can be derived as

$$p_s = \frac{\mathcal{P}\left(\mu < \gamma_m < \frac{k\left(1-2^{R_s}\right)}{2^{R_s}-k}\right)}{\mathcal{P}(\gamma_m > \mu)} = 0. \qquad \square$$

Remark 6. *When setting the correlated coefficient ρ in (4.20) as 0, the corresponding secrecy outage probability reduces to*

$$\begin{aligned} p_s &= e^{\frac{\mu}{\bar{\gamma}_m}}\Gamma\left(1, \frac{\mu}{\bar{\gamma}_m}\right)\Gamma\left(1, \frac{1+\mu-2^{R_s}}{\bar{\gamma}_e 2^{R_s}}\right) \\ &\quad - e^{\frac{1+\mu-2^{R_s}}{\bar{\gamma}_m}}\frac{\bar{\gamma}_m}{\bar{\gamma}_m+\bar{\gamma}_e 2^{R_s}}\Gamma\left(1, \left(\frac{1}{\bar{\gamma}_e}+\frac{2^{R_s}}{\bar{\gamma}_m}\right)\left(\frac{1+\mu}{2^{R_s}}-1\right)\right) \\ &\overset{(a)}{=} \frac{\bar{\gamma}_e 2^{R_s}}{\bar{\gamma}_m+\bar{\gamma}_e 2^{R_s}}\exp\left(-\frac{1+\mu-2^{R_s}}{\bar{\gamma}_e 2^{R_s}}\right), \end{aligned} \tag{4.27}$$

where (a) is due to the fact that $\Gamma(1, x) = e^{-x}$. Notice that (4.27) just corresponds to the secrecy outage probability derived in [87] for independent fading wiretap channel scenario.

It is notable that the outage probability, which is defined as $P_{out} = \mathcal{P}\left(C_s < R_s\right)$ in [4, 58], is used to characterize the overall outage events due to either unreliable or insecure transmission. To distinguish from the outage performance metrics derived in this chapter, we call P_{out} as the overall outage probability here. Based on p_t and p_s, the overall outage probability P_{out} can be also determined.

Corollary 1. *For a given secrecy rate R_s, the overall outage probability P_{out} of the concerned fading wiretap channel is given by*

$$P_{out} = p_t + p_s(1 - p_t), \tag{4.28}$$

where p_t and p_s are determined by (4.17) and (4.20), respectively, and μ in them is fixed as $2^{R_s} - 1$.

Remark 7. *When setting the correlated coefficient ρ in (4.28) as 0, the corresponding*

oveall outage probability reduces to

$$P_{out} = 1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_m + \bar{\gamma}_e 2^{R_s}} \exp(-\frac{2^{R_s} - 1}{\bar{\gamma}_m}). \tag{4.29}$$

Notice that (4.29) is just the overall outage probability [4] for the independent fading wire-tap channel.

4.6 Numerical Results and Discussions

Based on the theoretical models derived in this chapter, this section first illustrates how the SNRs of the main and eavesdropper channels and the channel correlation between them affect the final achievable secrecy capacity, and then explores the inherent tradeoffs between the achievable secrecy rates and outage probabilities and also the impacts of channel correlation on such tradeoffs. Finally, comparisons between the secrecy outage probability and conventional overall outage probability is provided to illustrate their different effects on the final achievable secrecy rate.

4.6.1 Secrecy Capacity Discussion

To illustrate the impacts of SNRs of the main and eavesdropper channels on the final achievable secrecy capacity, we show in Fig. 4-1 how the secrecy capacity C_s varies with $\bar{\gamma}_m$ and $\bar{\gamma}_e$ under a moderate correlation scenario of $\rho = 0.3$. As shown in Fig.4-1, C_s monotonically decreases with $\bar{\gamma}_e$ for a specified $\bar{\gamma}_m$, while it monotonically increases with $\bar{\gamma}_m$ for a specified $\bar{\gamma}_e$. A further careful observation of Fig. 4-1 indicates that besides $\bar{\gamma}_m$, the relative condition of the main channel against the eavesdropper channel (i.e. $k = \bar{\gamma}_m/\bar{\gamma}_e$) also plays a critical role in determining the final secrecy capacity. For example, when $\bar{\gamma}_m = 10$ dB, the secrecy capacity under the condition of $k = 10$ will be 2.08, which is more than three times higher than the 0.65 secrecy capacity under the condition of $k = 1$. It is also noticed that for a specified k, a bigger $\bar{\gamma}_m$ leads to a larger secrecy capacity. It is interesting to see from Fig. 4-1 that even under condition that $\bar{\gamma}_m \leq \bar{\gamma}_e$, a non-zero secrecy capacity can still be achieved.

We now explore the impacts of channel correlation on the secrecy capacity. In Fig. 4-2, we illustrate how C_s varies with the correlation coefficient ρ for three different scenarios of $\bar{\gamma}_m$ and $\bar{\gamma}_e$: a better scenario with $\bar{\gamma}_m = 5$ dB and $\bar{\gamma}_e = 0$ dB, a normal scenario with $\bar{\gamma}_m = 5$ dB and $\bar{\gamma}_e = 5$ dB, and a worse scenario with $\bar{\gamma}_m = 0$ dB and $\bar{\gamma}_e = 5$ dB. For all the three scenarios, as shown in Fig. 4-2, the secrecy capacity monotonically decreases with ρ, which indicates that the channel correlation has a negative impact on the secrecy capacity. This is due to the reason that as the channels becomes more correlated, they tend to behave more similar and thus the chances for the transmitter to transmit at a high secrecy rate tend to decrease. A careful observation of Fig. 4-2 indicates that as ρ approaches 1, C_s goes to 0 for both the normal and worse scenarios, but converges to a fixed value that is determined by (4.10) for the better scenario. Therefore, the potential channel correlation should be carefully considered when designing a secrecy rate, otherwise information leakage may happen due to the overestimated secrecy capacity.

4.6.2 Outage Performances Discusssion

To explore the inherent tradeoffs between the achievable secrecy rate and outage probabilities, we show in Fig. 4-3 how the secrecy rate R_s varies with the transmission outage probability p_t and secrecy outage probability p_s for the typical channel setting of ($\bar{\gamma}_m = 5$ dB,$\bar{\gamma}_e = 0$ dB) [87] and a moderate correlation scenario of $\rho = 0.3$. We can see from Fig. 4-3 that, in general, R_s monotonically increases as p_t increases for a given value of p_s, and also monotonically increases as p_s increases for a given value of p_t. It is notable that for a given transmission outage probability, the secrecy rate can be greatly increased by allowing a small value of secrecy outage probability. Fig. 4-3 also shows that for the channel scenario there, we cannot transmit any secrecy message with positive rate under relative strong outage requirements, e.g., $p_t = 0.1$ and $p_s = 0.1$ there.

To further explore the impacts of the channel correlation on the secrecy rate for different outage requirements, we show in Fig. 4-4 how R_s varies with the correlation coefficient ρ for the scenarios of $\bar{\gamma}_m = 5$ dB,$\bar{\gamma}_e = 0$ dB, $p_t = 0.3$ and $p_s = \{0.1, 0.3, 0.5\}$.

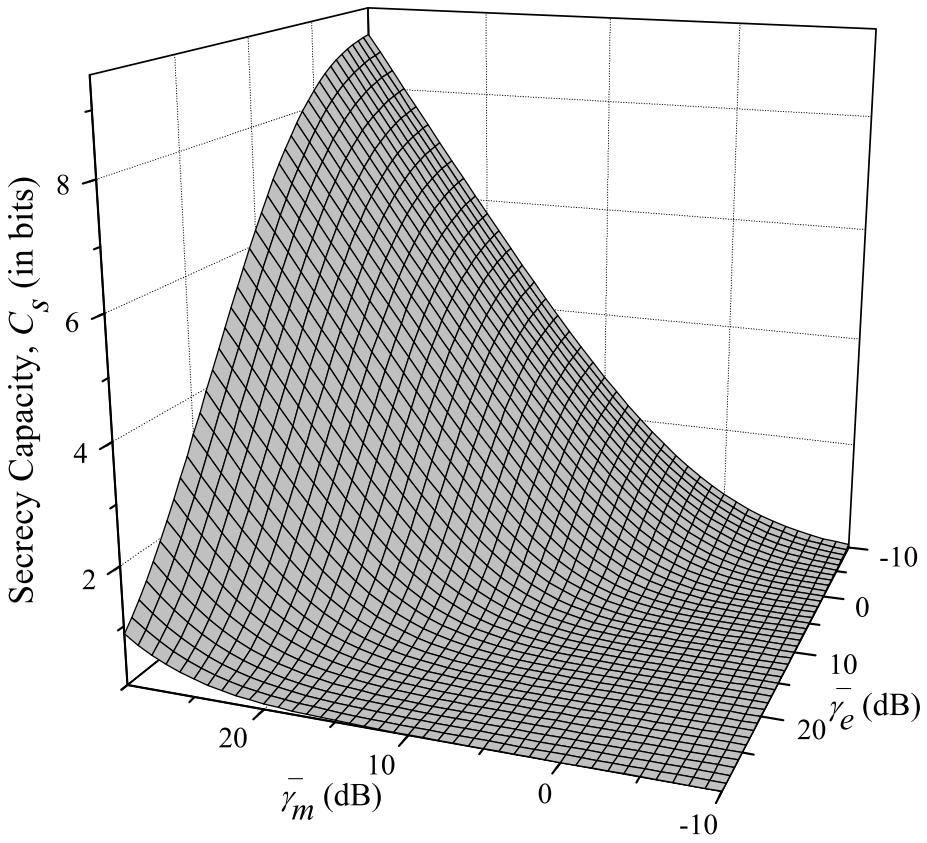

Figure 4-1: Secrecy capacity vs. $(\bar{\gamma}_m, \bar{\gamma}_e)$ under a moderate correlation of $\rho = 0.3$.

It is interesting to see from Fig. 4-4 that channel correlation has different impacts on the secrecy rate under different requirements of secrecy outage probability. For a stringent requirement of p_s (e.g. $p_s = 0.1$ here), R_s increases significantly as ρ increases, while R_s only increases slightly as ρ increases for a moderate requirement of p_s (e.g., $p_s = 0.3$ here). For a less stringent requirement of p_s (e.g., $p_s = 0.5$ here), however, R_s decreases slowly as ρ increases.

The results in Fig. 4-4 indicate that channel correlation is helpful when p_s is small (e.g., $p_s = \{0.1, 0.3\}$), but becomes harmful when p_s becomes large (e.g., $p_s = 0.5$). The main reason for such two different impacts is given as follows. Let random variable $U = \gamma_m/\gamma_e$ denote the instantaneous SNR ratio between the main and eaves-

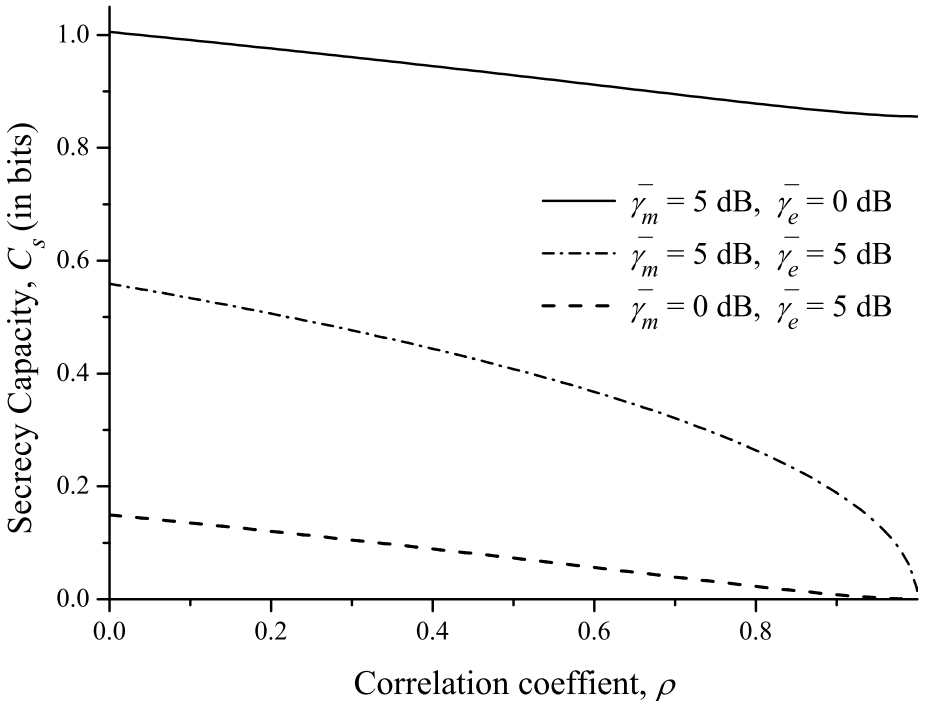

Figure 4-2: Secrecy capacity vs. correlation coefficient ρ.

dropper channels. Based on (4.21), we have

$$\begin{aligned} p_s &= \mathcal{P}\left(U < 2^{R_s}\left(\frac{1}{\gamma_e}+1\right) - \frac{1}{\gamma_e} \,\middle|\, \gamma_m > \mu\right) \\ &= \mathcal{P}\left(U < U_s \mid \gamma_m > \mu, U_s < k\right)\mathcal{P}\left(U_s < k\right) \\ &\quad + \mathcal{P}\left(U < U_s \mid \gamma_m > \mu, U_s > k\right)\mathcal{P}\left(U_s > k\right), \end{aligned} \tag{4.30}$$

where $U_s = 2^{R_s}\left(1/\gamma_e + 1\right) - 1/\gamma_e$. Moreover, the cumulative distribution function of U can be derived as [19]

$$F_U(u) = \frac{1}{2} + \frac{u-k}{2\sqrt{(u+k)^2 - 4\rho k u}}. \tag{4.31}$$

It is notable that as ρ increases, $F_U(u)$ decreases if $u < k$, but increases if $u > k$. Therefore, the first term $\mathcal{P}\left(U < U_s \mid \gamma_m > \mu, U_s < k\right)$ in (4.30) decreases with ρ, while the second term $\mathcal{P}\left(U < U_s \mid \gamma_m > \mu, U_s > k\right)$ increases with ρ, which indicates that the impacts of channel correlation is helpful on the first term, but becomes harmful on the second term. When the secrecy outage probability p_s is small, such as $p_s =$

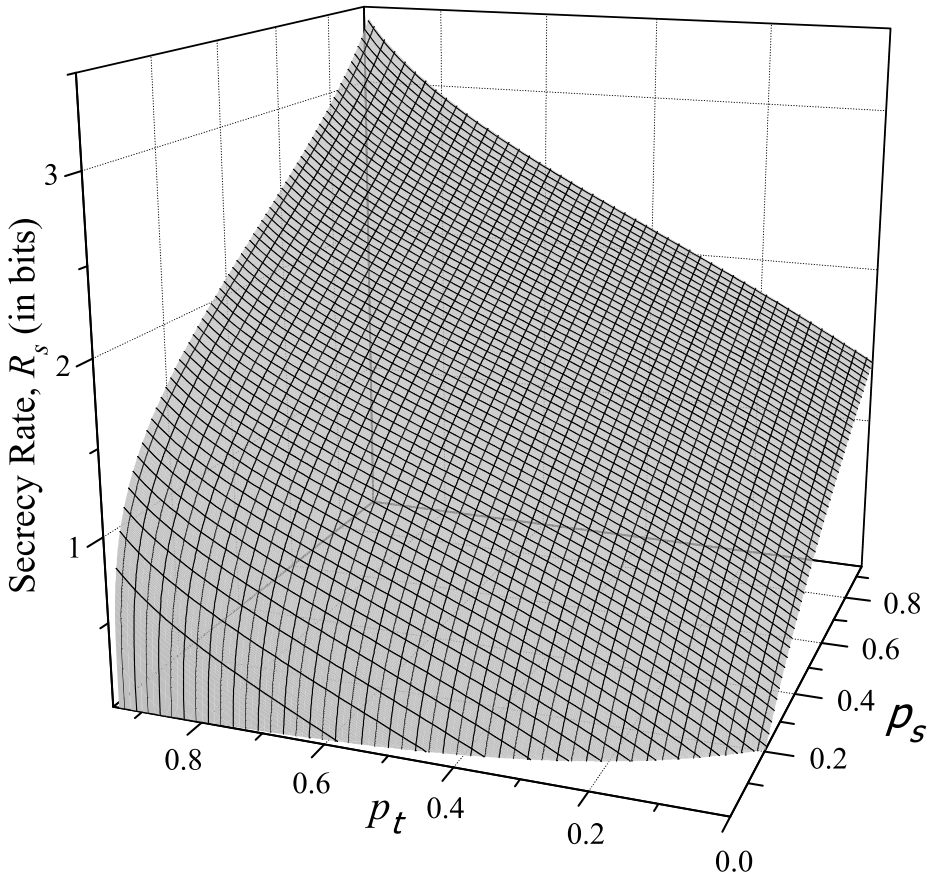

Figure 4-3: Secrecy rate vs. (p_t,p_s) when $\bar{\gamma}_m = 5$ dB, $\bar{\gamma}_e = 0$ dB and $\rho = 0.3$.

$\{0.1, 0.3\}$ in Fig. 4-4, R_s (and thus U_s for a given value of γ_e) should be increased to keep a fixed value of p_s as ρ grows. This is because the helpful impact of correlation on the first term in (4.30) dominates p_s when p_s is small. On the other hand, when p_s is large, such as $p_s = 0.5$ in Fig. 4-4, R_s should be decreased to keep a fixed value of p_s as ρ grows. The region of p_s for the different impacts of correlation can be numerically found based on (4.20), though the closed-form expression is not given in this thesis.

4.6.3 Secrecy Outage Probability vs. Overall Outage Probability

We now conduct a comparison between the secrecy outage probability and overall outage probability, two metrics used to illustrate the security requirement literature.

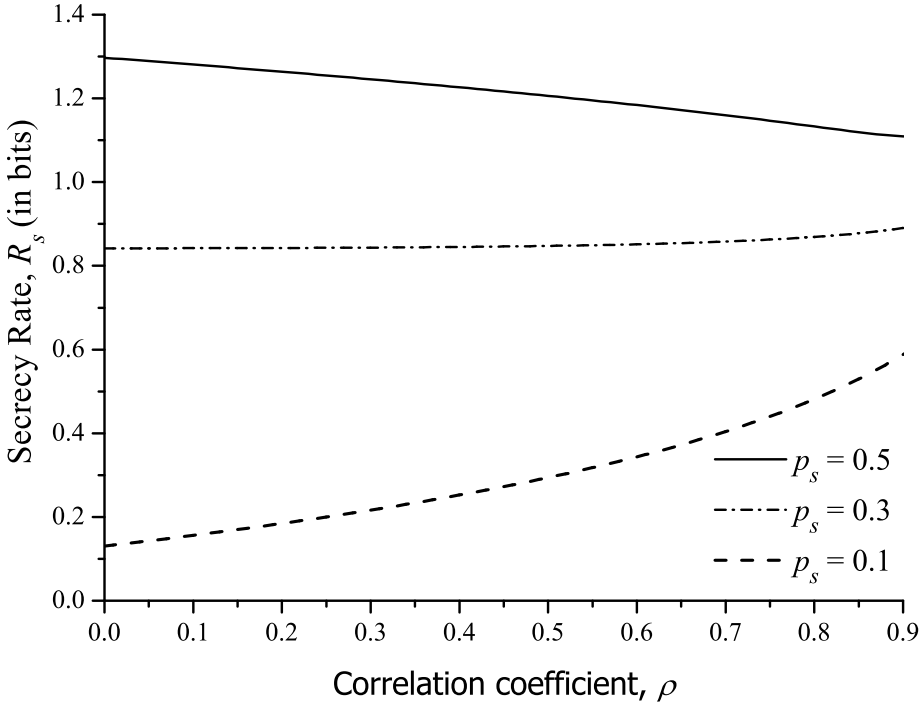

Figure 4-4: Secrecy rate vs. correlation coefficient ρ when $\bar{\gamma}_m = 5$ dB, $\bar{\gamma}_e = 0$ dB and $p_t = 0.3$.

For the case that $\rho = 0.3$ and $\mu = 2^{R_s} - 1$, Fig. 4-5 illustrates how p_s and P_{out} vary with R_s for three different channel scenarios of $\bar{\gamma}_m$ and $\bar{\gamma}_e$: a better scenario with $\bar{\gamma}_m = 5$ dB and $\bar{\gamma}_e = 0$ dB, a normal scenario with $\bar{\gamma}_m = 5$ dB and $\bar{\gamma}_e = 5$ dB, and a worse scenario with $\bar{\gamma}_m = 0$ dB and $\bar{\gamma}_e = 5$ dB. We can see from Fig. 4-5 that for all the three channel scenarios, P_{out} is much larger than p_s, in particular for the scenario that $\bar{\gamma}_e \leq \bar{\gamma}_m$. The results in Fig. 4-5 indicate that using P_{out} in system design will result in a conservative estimation on the maximum achievable secrecy rate. For example, when the secrecy outage probability is required to be less than 0.3, the maximum achievable R_s determined by using p_s will be 0.52, which is almost two times higher than the 0.28 maximum achievable R_s determined by using the metric P_{out}.

Next, we examine in Fig. 4-6 how the difference between P_{out} and p_s varies with correlation coefficient ρ for all the three different scenarios, given that $\mu = 2^{R_s} - 1$ and $R_s = 1$. Fig. 4-6 shows that the difference between P_{out} and p_s is large and almost does not change with ρ for the above better scenario, but such difference under the

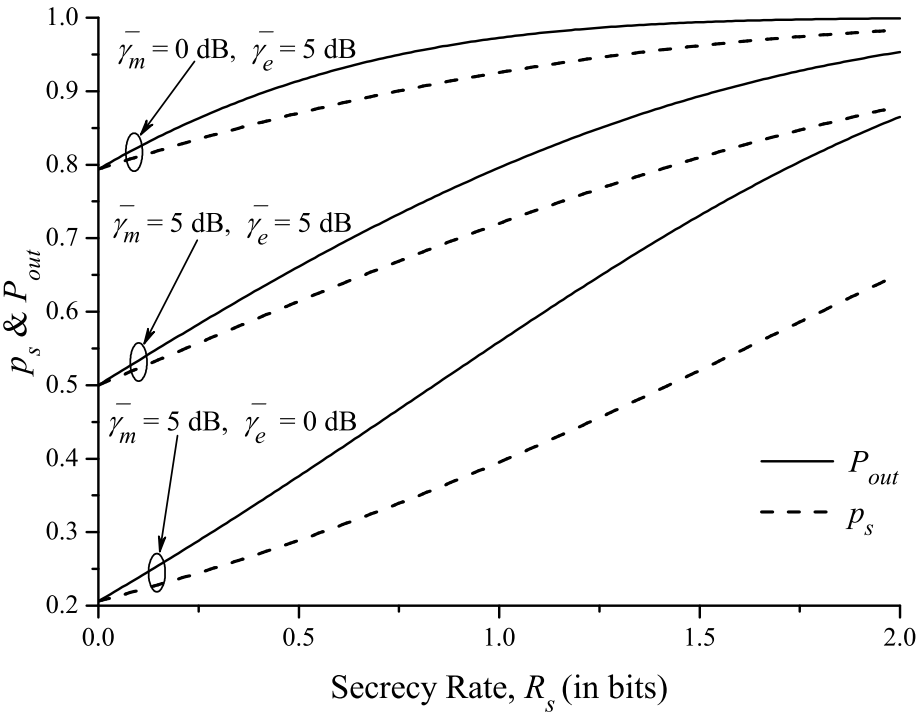

Figure 4-5: Secrecy outage probability p_s and overall outage probability P_{out} vs. secrecy rate R_s when $\rho = 0.3$.

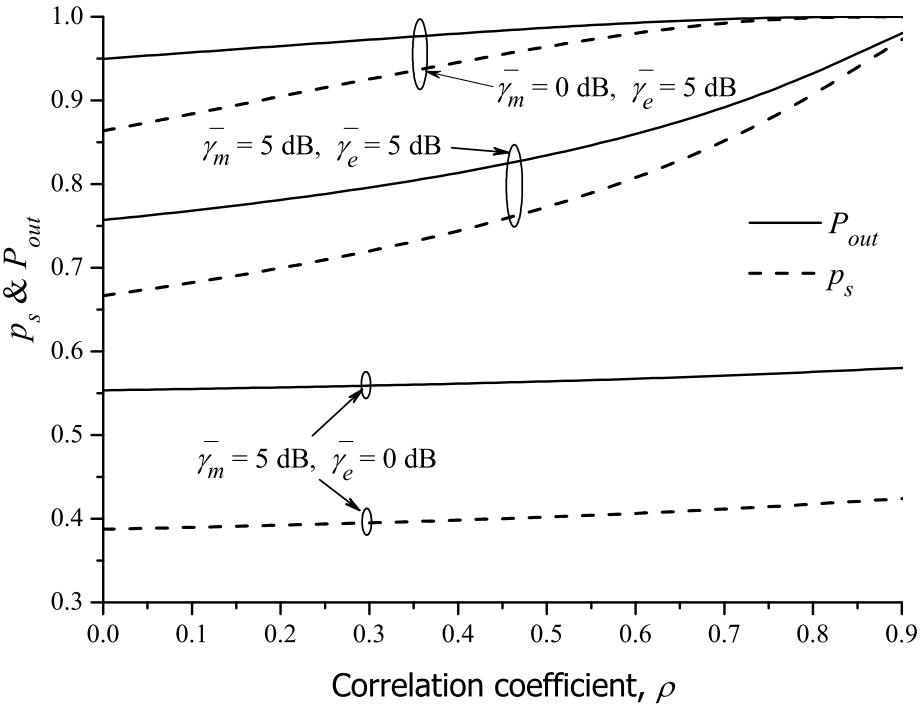

Figure 4-6: Secrecy outage probability p_s and overall outage probability P_{out} vs. correlation coefficient ρ when $R_s = 1$.

other two scenarios approaches 0 as ρ increases to 1. Thus, under the better channel condition that $\bar{\gamma}_e \leq \bar{\gamma}_m$, p_s rather than P_{out} should be adopted for the efficient design of secure transmission system.

4.7 Summary

This chapter derived analytical models of secrecy capacity, transmission outage probability and secrecy outage probability for a correlated wire-tap channel system under partial CSI, such that the fundamental performance limits for secure and reliable information transmission are fully addressed. It is notable that our models, derived for correlated channels, also cover the corresponding models for independent channels as special cases. The results in this chapter indicate that the correlation between main and eavesdropper channels is always harmful to secrecy capacity, but has different effects on outage performance, depending on secrecy rate adopted in the transmission and also the SNR conditions of both main and eavesdropper channels.

THIS PAGE INTENTIONALLY LEFT BLANK

Chapter 5

Conclusion

This final chapter summarizes our contributions and points out several areas for future search.

5.1 Summary of the Thesis

The notion of physical-layer security, which is regarded as information-theoretic security since its security is derived purely from information theory, advocates a paradigm shift in cryptography and calls for a physical layer design of security schemes. The main idea of physical-layer security is to exploit the inherent randomness of the propagation channels to significantly strengthen the security of digital communications systems.

The objective of this thesis was to provide a comprehensive study on the fundamental performance limits of physical layer security under a fading wire-tap channel, where the main channel is correlated with the eavesdropper channel and the transmitter knows only the real time channel state information (CSI) of main channel. With this goal in mind, we first analyze the asymptotic outage probability and outage secrecy capacity for the case when the transmission power is approaching infinity, and then extends the study to the case when the transmission power is constrained. The whole thesis is concluded in more details as follows.

- In Chapter 2, we defined the system models of correlated fading wire-tap channel

and some preliminary knowledge about the physical layer security, including the notions of error probability, equivocation rate, perfect secrecy, secrecy rate and secrecy capacity. These definitions serves as the overall models for the performance analysis in the next two chapters.

- In Chapter 3, we approached our objective by analyzing the asymptotic performance limits of physical layer security. Firstly, we presented the secrecy capacity for one pair of channel gains in high SNR regime, from which we found that the secrecy capacity does not increase with transmission power and instead controlled by the channel power gain ratio. Based on this result, we then derived the closed-form asymptotic outage probability and asymptotic outage secrecy capacity under the correlated Rayleigh fading wiretap channel, which cover the special cases when the main and eavesdropper channels are independent. Based on the above theoretical modelings, channel correlation were then revealed to have constructive effect on the outage secrecy capacity if the asymptotic outage probability is less than 1/2, and have destructive effect otherwise. To the best of our knowledge, such results have never been exposed.

- In Chapter 4, we focused on the performance analysis of physical layer security under a correlated fading wire-tap channel when the transmission power is constrained to a given value. Firstly, we derived the closed-form secrecy capacity based on the typical Marcum Q function, which has been widely used in the wireless communications and detection theories for radar systems [48] and thus has been extensively studied recently [10, 79]. Secondly, two outage performance metrics, namely transmission outage probability and secrecy outage probability, were derived to characterize the reliability level and security level, respectively, for the transmission scheme. Based on these theoretical modelings, we further reveals that channel correlation is always harmful to secrecy capacity, but has both helpful and harmful effects on outage performance, depending on secrecy rate adopted in the transmission and also the SNR conditions of both main and eavesdropper channels. This result confirms with one for the asymptotic

behaviors in Chapter 3 in the sense that both helpful and harmful effects exist, and have more explicit and complicate relation between different parameters.

5.2 Future works

The work presented in this thesis could be extended in many interesting directions.

- **Closed-form results for other fading models.** In this thesis, we mainly focus on the closed-form results for the Rayleigh fading channel model, which is considered as a reasonable model when there are many objects in the environment that scatter the radio signal before it arrives at the receiver [70], such as radio signals in the heavily built-up urban environments. Although the Rayleigh fading model is important for the physical layer study, there exists some other fading models, such as Rician fading, Nakagami fading, Log-normal shadow fading and Weibull fading, which are more suitable for some specific scenarios. For example, Rician fading is more applicable for modeling the signal transmission when there is a dominant propagation along a line of sight between the transmitter and receiver, such as the sparsely built-up rural environments. Thus, the derivation process in this work can be directly help the analysis on the other fading channel model.

- **Multi-user information-theoretic security.** Our study is based on the basic wire-tap model that consists of three users, namely a transmitter, a receiver, and an eavesdropper. The results on such model can be generalized to the models that includes more users, for example the broadcast wire-tap channel, cooperative relay wire-tap channel, and etc. In the broadcast wire-tap channel, multiple receivers and eavesdroppers are expected to receive the signal transmitted from the same source node, while in the cooperative relay wire-tap channel, the malicious node can receive the same message transmitted from both the source node and relay node and more complicate correlation relations are expected. It is noticed that, as long as the signal is transmitted from one source

node to different receivers, channel correlation are observed in real communication environment. Therefore, it is of great significance and also challenging to extend the study to the more general multi-user model.

- **Single-input multiple-output wire-tap channel.** The study for the model that a receiver has multiple antennas, the SIMO wire-tap channel, is also one important future work. It is very possible that both the legitimate receiver and eavesdropper install multiple antennas to improve their signals. In such transmission environment, channel correlation is a common phenomenon. The insights brought by this analysis should shed light on the analysis of physical layer security on those practical channel models.

Bibliography

[1] Vaneet Aggarwal, Lalitha Sankar, A Robert Calderbank, and H Vincent Poor. Information secrecy from multiple eavesdroppers in orthogonal relay channels. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2607–2611, Seoul, Korea, Jun.-Jul. 2009.

[2] Weng Chon Ao and Kwang-Cheng Chen. Broadcast transmission capacity of heterogeneous wireless ad hoc networks with secrecy outage constraints. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, 2011.

[3] Joao Barros and Miguel R. D. Rodrigues. Secrecy capacity of wireless channels. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 356–360, Seattle, WA, Jul. 2006.

[4] Matthieu Bloch, Joao Barros, Miguel R. D. Rodrigues, and Steven W. McLaughlin. Wireless information-theoretic security. *IEEE Trans. Inf. Theory*, 54(6):2515 – 2534, Jun. 2008.

[5] Matthieu Bloch and Andrew Thangaraj. Confidential messages to a cooperative relay. In *IEEE Information Theory Workshop (ITW)*, pages 154–158, Porto, Portugal, May 2008.

[6] G.E. Corazza and G. Ferrari. New bounds for the marcum q-function. *IEEE Trans. Inf. Theory*, 48(11):3003–3008, 2002.

[7] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[8] W.B. Davenport and W.L. Root. *An introduction to the theory of random signals and noise*. McGraw-Hill New York, 1958.

[9] Gregory D Durgin and Theodore S Rappaport. Theory of multipath shape factors for small-scale fading wireless channels. *IEEE Trans. Antennas Propag.*, 48(5):682–693, 2000.

[10] Hua Fu and Pooi-Yuen Kam. Exponential-type bounds on the first-order marcum q-function. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–5, Dec. 2011.

[11] Radha Krishna Ganti, Jeffrey G Andrews, and Martin Haenggi. High-sir transmission capacity of wireless networks with general fading and node distribution. *Information Theory, IEEE Transactions on*, 57(5):3100–3116, 2011.

[12] Satashu Goel, Vaneet Aggarwal, Aylin Yener, and A Robert Calderbank. Modeling location uncertainty for eavesdroppers: A secrecy graph approach. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2627–2631, Jun. 2010.

[13] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.*, 7(6):2180–2189, 2008.

[14] Praveen Kumar Gopala, Lifeng Lai, and Hesham El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory*, 54(10):4687–4698, Oct. 2008.

[15] Martin Haenggi. The secrecy graph and some of its properties. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 539–543, Jul. 2008.

[16] Martin Haenggi, Jeffrey G Andrews, François Baccelli, Olivier Dousse, and Massimo Franceschetti. Stochastic geometry and random graphs for the analysis and design of wireless networks. *IEEE J. Sel. Areas Commun.*, 27(7):1029–1046, Sep. 2009.

[17] Xiang He and Aylin Yener. Secure degrees of freedom for gaussian channels with interference: Structured codes outperform gaussian signaling. In *IEEE Global Telecommunications Conference (GLOBECOM)*, pages 1–6, Nov. 2009.

[18] Eran Hof and Shlomo Shamai. Secrecy-achieving polar-coding. In *Information Theory Workshop (ITW)*, pages 1–5, 2010.

[19] Hyoungsuk Jeon, Namshik Kim, Jinho Choi, Hyuckjae Lee, and Jeongseok Ha. Bounds on secrecy capacity over correlated ergodic fading channels at high snr. *IEEE Trans. Inf. Theory*, 57(4):1975 – 1983, Apr. 2011.

[20] A. Khisti, A. Tchamkerten, and G.W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, 2008.

[21] A. Khisti and G.W. Wornell. Secure transmission with multiple antennas i: The misome wiretap channel. *IEEE Trans. Inf. Theory*, 56(7):3088–3104, July 2010.

[22] Ashish Khisti, Gregory Wornell, Ami Wiesel, and Yonina Eldar. On the gaussian mimo wiretap channel. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2471–2475, 2007.

[23] Ashish Khisti, Gregory Wornell, Ami Wiesel, and Yonina Eldar. On the gaussian mimo wiretap channel. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2471–2475, Jun. 2007.

[24] Ashish Khisti and Gregory W Wornell. Secure transmission with multiple antennas i: The misome wiretap channel. *IEEE Trans. Inf. Theory*, 56(7):3088–3104, 2010.

[25] Demijan Klinc, Jeongseok Ha, Steven W McLaughlin, Joao Barros, and Byung-Jae Kwak. Ldpc codes for the gaussian wiretap channel. *IEEE Trans. Inf. Forensics Security*, 6(3):532–540, 2011.

[26] Onur Ozan Koyluoglu, Hesham El Gamal, Lifeng Lai, and H Vincent Poor. Interference alignment for secrecy. *IEEE Trans. Inf. Theory*, 57(6):3323–3332, 2011.

[27] OOzan Koyluoglu, Can Emre Koksal, and Hesham El Gamal. On secrecy capacity scaling in wireless networks. *IEEE Trans. Inf. Theory*, 58(5):3000–3015, 2012.

[28] L. Lai and H. El Gamal. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, 2008.

[29] W. C.-Y. Lee. Effects on correlation between two mobile radio base-station antennas. *IEEE Trans. Commun.*, 21(11):1214–1224, Nov. 1973.

[30] Albert Leon-Garcia. *Probability and Random Processes for Electrical Engineering*. Addison-Wesley, 2 edition, 1973.

[31] S Leung-Yan-Cheong. On a special class of wiretap channels (corresp.). *IEEE Trans. Inf. Theory*, 23(5):625–627, 1977.

[32] S. K. Leung-Yan-Cheong and M. E. Hellman. The gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, 1978.

[33] Lifang Li, Nihar Jindal, and Andrea Goldsmith. Outage capacities and optimal power allocation for fading multiple-access channels. *IEEE Trans. Inf. Theory*, 51(4):1326 –1347, Apr. 2005.

[34] Zang Li, Wade Trappe, and Roy Yates. Secret communication via multi-antenna transmission. In *41st Annual Conf. Inform. Sciences and Syst. (CISS'07)*, pages 905–910, Baltimore, MD, Mar. 2007.

[35] Y. Liang, A. Somekh-Baruch, H.V. Poor, S. Shamai, and S. Verdu. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inf. Theory*, 55(2):604–619, 2009.

[36] Yingbin Liang and H. Vincent Poor. Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Mar. 2008.

[37] Yingbin Liang, H Vincent Poor, and Shlomo Shamai. Secrecy capacity region of fading broadcast channels. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 1291–1295, 2007.

[38] Yingbin Liang, H. Vincent Poor, and Shlomo Shamai (Shitz). Secure communication over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2470 – 2492, Jun. 2008.

[39] Yingbin Liang, H Vincent Poor, and Lei Ying. Secrecy throughput of manets under passive and active attacks. *IEEE Trans. Inf. Theory*, 57(10):6692–6702, 2011.

[40] Yingbin Liang, Anelia Somekh-baruch, H Vincent Poor, Shlomo Shamai, et al. Cognitive interference channels with confidential messages. In *45th Annual Allerton Conf. on Commun., Control and Computing*. Citeseer, 2007.

[41] Ruoheng Liu, Tie Liu, H Vincent Poor, and Shlomo Shamai. Multiple-input multiple-output gaussian broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 56(9):4215–4227, 2010.

[42] Ruoheng Liu, Ivana Maric, Predrag Spasojevic, and Roy D Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, 2008.

[43] Tie Liu and Shlomo Shamai. A note on the secrecy capacity of the multiple-antenna wiretap channel. *IEEE Trans. Inf. Theory*, 55(6):2547–2553, 2009.

[44] Mike Loukides and John Gilmore. Cracking des: Secrets of encryption research, wiretap politics and chip design, 1998.

[45] Hung D Ly, Tie Liu, and Yingbin Liang. Multiple-input multiple-output gaussian broadcast channels with common and confidential messages. *IEEE Trans. Inf. Theory*, 56(11):5477–5487, 2010.

[46] Mohammad Ali Maddah-Ali. On the degrees of freedom of the compound miso broadcast channels with finite states. In *IEEE Int. Symp. Inf. Theory(ISIT)*, pages 2273–2277, 2010.

[47] Hessam Mahdavifar and Alexander Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *Information Theory, IEEE Transactions on*, 57(10):6428–6443, 2011.

[48] JI Marcum. A statistical theory of target detection by pulsed radar. *IRE Trans. Inf. Theory*, 6(2):59–267, 1960.

[49] U. Maurer and S. Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology-Eurocrypt 2000 (Lecture Notes in Computer Science)*, volume 1807, pages 351–368, Berlin, Germany, 2000. Springer.

[50] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[51] Mahtab Mirmohseni, Bahareh Akhbari, and Mohammad Reza Aref. Capacity bounds for multiple access-cognitive interference channel. *EURASIP J. Wireless Commun. and Networking*, 2011(1):1–18, 2011.

[52] S. Nitinawarat. Secret key generation for correlated gaussian sources. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 702–706, Jul. 2008.

[53] A. Nuttall. Some integrals involving the q_m function (corresp.). *IEEE Trans. Inf. Theory*, 21(1):95–96, 1975.

[54] Frédérique Oggier and Babak Hassibi. The secrecy capacity of the mimo wiretap channel. *IEEE Trans. Inf. Theory*, 57(8):4961–4972, 2011.

[55] Yasutada Oohama. Coding for relay channels with confidential messages. In *IEEE Information Theory Workshop (ITW)*, pages 87–89, Sep. 2001.

[56] Yasutada Oohama. Capacity theorems for relay channels with confidential messages. In *IEEE International Symposium on Information Theory (ISIT)*, pages 926–930, Jun. 2007.

[57] Lawrence H Ozarow and Aaron D Wyner. Wire-tap channel ii. *AT&T Bell Laboratories technical journal*, 63(10):2135–2157, 1984.

[58] P. Parada and R. Blahut. Secrecy capacity of simo and slow fading channels. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 2152–2155, 2005.

[59] Pedro C Pinto, Joao Barros, and Moe Z Win. Secure communication in stochastic wireless networks-part i: Connectivity. *IEEE Trans. Inf. Forensics Security*, 7(1):125–138, 2012.

[60] Pedro C Pinto and Moe Z Win. Continuum percolation in the intrinsically secure communications graph. In *Int. Symp. Inf. Theory and its Applications (ISITA)*, pages 349–354, Oct. 2010.

[61] Pedro C Pinto and Moe Z Win. Percolation and connectivity in the intrinsically secure communications graph. *IEEE Trans. Inf. Theory*, 58(3):1716–1730, 2012.

[62] Sang Bin Rhee and G. I. Zysman. Results of suburban base station spatial diversity measurements in the uhf band. *IEEE Trans. Commun.*, 22(10):1630–1636, Oct. 1974.

[63] Stefano Rini and Andrea Goldsmith. On the capacity of the mimo cognitive interference channel. In *IEEE Int. Symp. Inf. Theory (ISIT)*, pages 2691–2695, 2013.

[64] A Sarkar and M Haenggi. Secrecy coverage. In *Asilomar Conf. Signals, Systems and Computers (ASILOMAR)*, pages 42–46, Nov. 2010.

[65] Amites Sarkar and Martin Haenggi. Percolation in the secrecy graph: Bounds on the critical probability and impact of power constraints. In *IEEE Inf. Theory Workshop (ITW)*, pages 673–677, 2011.

[66] Amites Sarkara and Martin Haenggib. Percolation in the secrecy graph. *Discrete Applied Mathematics*, 161:2120–2132, 2013.

[67] Shabnam Shafiee and Sennur Ulukus. Achievable rates in gaussian miso channels with secrecy constraints. In *IEEE Int. Symp. Inform. Theory (ISIT)*, pages 2466–2470, Nice, France, Jun. 2007.

[68] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[69] D.S. Shiu, G.J. Foschini, M.J. Gans, and J.M. Kahn. Fading correlation and its effect on the capacity of multielement antenna systems. *IEEE Trans. Commun.*, 48(3):502–513, 2000.

[70] Bernard Sklar. Rayleigh fading channels in mobile digital communication systems. i. characterization. *Communications Magazine, IEEE*, 35(7):90–100, 1997.

[71] A Lee Swindlehurst. Fixed sinr solutions for the mimo wiretap channel. In *IEEE Int. Conf. Acoustics, Speech and Signal Processing (ICASSP)*, pages 2437–2440, 2009.

[72] Xiaojun Tang, Ruoheng Liu, Predrag Spasojevic, and H Vincent Poor. The gaussian wiretap channel with a helping interferer. In *IEEE Int. Symp. Information Theory (ISIT)*, pages 389–393, Toronto, Ontario, Canada, Jul. 2008.

[73] Xiaojun Tang, Ruoheng Liu, Predrag Spasojevic, and H Vincent Poor. Interference assisted secret communication. *IEEE Trans. Inf. Theory*, 57(5):3153–3167, 2011.

[74] Ender Tekin and Aylin Yener. The gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, 2008.

[75] Ender Tekin and Aylin Yener. The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, 2008.

[76] Andrew Thangaraj, Souvik Dihidar, A Robert Calderbank, Steven W McLaughlin, and Jean-Marc Merolla. Applications of ldpc codes to the wiretap channel. *IEEE Trans. Inf. Theory*, 53(8):2933–2945, 2007.

[77] Marten Van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 43(2):712–714, 1997.

[78] Sudarshan Vasudevan, Dennis Goeckel, and Donald F Towsley. Security-capacity trade-off in large wireless networks using keyless secrecy. In *ACM Int. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 21–30, Chicago, IL, Sep. 2010.

[79] J. Wang and D. Wu. Tight bounds for the first order marcum q-function. *Wireless Communications and Mobile Computing*, 12(4):293–301, 2012.

[80] Jakes WC Jr. Microwave mobile communications, 1974.

[81] Steven Weber and Jeffrey G Andrews. Transmission capacity of wireless networks. *arXiv:1201.0662*, 2012.

[82] Steven Weber, Jeffrey G Andrews, and Nihar Jindal. An overview of the transmission capacity of wireless networks. *IEEE Trans. Commun.*, 58(12):3593–3604, 2010.

[83] Steven P Weber, Xiangying Yang, Jeffrey G Andrews, and Gustavo De Veciana. Transmission capacity of wireless ad hoc networks with outage constraints. *IEEE Trans. Inf. Theory*, 51(12):4091–4102, 2005.

[84] Victor K Wei. Generalized hamming weights for linear codes. *IEEE Trans. Inf. Theory*, 37(5):1412–1418, 1991.

[85] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[86] Jin Xu and Biao Chen. Broadcast confidential and public messages. In *42nd Conf. Information Sciences and Systems (CISS)*, pages 630–635, Princeton, NJ, Mar. 2008.

[87] X. Zhou, M.R. McKay, B. Maham, and A. Hjorungnes. Rethinking the secrecy outage formulation: A secure transmission design perspective. *IEEE Commun. Lett.*, 15(3):302–304, Mar. 2011.

[88] Xiangyun Zhou, Radha Krishna Ganti, and Jeffrey G Andrews. Secure wireless network connectivity with multi-antenna transmission. *IEEE Trans. Wireless Commun.*, 10(2):425–430, 2011.

[89] Xiangyun Zhou, Radha Krishna Ganti, Jeffrey G Andrews, and Are Hjorungnes. On the throughput cost of physical layer security in decentralized wireless networks. *IEEE Trans. Wireless Commun.*, 10(8):2764–2775, Aug. 2011.

[90] Xiangyun Zhou, Meixia Tao, and Rodney A Kennedy. Cooperative jamming for secrecy in decentralized wireless networks. In *IEEE International Conf. Commun. (ICC)*, pages 2339–2344, 2012.

THIS PAGE INTENTIONALLY LEFT BLANK

Pulications

Jounal Articles

[1] Jinxiao Zhu, Xiaohong Jiang, Osamu Takahashi, and Norio Shiratori. Effects of Channel Correlation on Outage Secrecy Capacity. *Journal of Information Processing*, vol.21, no.4, pp. 640–649, Oct. 2013.

[2] Jinxiao Zhu, Yulong Shen, Xiaohong Jiang, Osamu Takahashi, and Norio Shiratori. Secrecy Capacity and Outage Performance of Correlated Fading Wire-tap Channel. *IEICE Transactions on Communications*, IEICE Transactions on Communications, vol. E97-B, no. 2, Feb. 2014.

Conference Papers

[3] Jinxiao Zhu, Osamu Takahashi, Xiaohong Jiang, Yoshitaka Nakamura, and Yoh Shiraishi. Outage secrecy capacity over correlated fading channels at high SNR. In *Sixth International Conference on Mobile Computing and Ubiquitous Networking (ICMU)*, Okinawa, Japan, May 2012, pp. 92-97.

[4] Jinxiao Zhu, Xiaohong Jiang, Osamu Takahashi, and Norio Shiratori. Secrecy capacity of correlated rayleigh fading channels. In *18th Asia-Pacific Conference on Communications (APCC)*, Oct. 2012, pp. 333-337.

[5] Jinxiao Zhu, Xiaohong Jiang, Yuezhi Zhou, Yaoxue Zhang, Osamu Takahashi, and Norio Shiratori. Outage Performance for Secure Communication over Correlated Fading Channels with Partial CSI. In *IEEE Asia-Pacific Services Computing Conference (APSCC)*, Dec. 2012, pp. 257-262.

Awards

- JIP Specially Selected Paper Award: J. Zhu, X. Jiang, O. Takahashi, and N. Shiratori. Effects of Channel Correlation on Outage Secrecy Capacity. *Journal of Information Processing*, vol.21, no.4, pp. 640–649, Oct. 2013.