PHYSICAL-LAYER SECURITY WITH FULL-DUPLEX
DECODE-AND-FORWARD RELAYING: SECRECY RATES AND POWER
ALLOCATION

A Thesis
Presented to
The Graduate Faculty of The University of Akron

In Partial Fulfillment
of the Requirements for the Degree
Master of Science

Lubna Elsaid
August, 2016
PHYSICAL-LAYER SECURITY WITH FULL-DUPLEX

DECODE-AND-FORWARD RELAYING: SECRECY RATES AND POWER ALLOCATION

Lubna Elsaid

Thesis

Approved:                          Accepted:

Advisor
Dr. Nghi Tran                      Interim Chair of the Department

Committee Member
Dr. Shivakumar Sastry               Dr. Joan E. Carletta

Committee Member
Dr. Jin Kocsis                      Interim Dean of the College

Date

Dean of the Graduate School
Dr. Chand Midha
This thesis studies the secrecy rate and respective optimal power allocation schemes to maximize the secrecy rate of a full-duplex (FD) relay wiretap channel. The FD relay is assumed to operate in decode-and-forward (DF) mode to support a secured communication from a source to a destination under the presence of an eavesdropper. Both slowly varying fading and ergodic fading channels where the channel gains are assumed to be available at the receivers but not the transmitters are considered. The residual self-interference due to FD transmission is taken into account in formulating the secrecy rate and the optimal power allocation schemes.

The first part of the thesis establishes closed-form expressions of the secrecy rates for a given power allocation scheme at the source and the relay. For a slowly varying fading environment, the channel conditions for which a positive secrecy rate is attained are identified. In the case of ergodic fading, we first propose a simple method to calculate the expectation of an exponentially distributed random variable using the exponential integral function. Using this result, the ergodic secrecy rates of the considered FD relay channel are then established in closed-form. The proposed method provides a simple yet effective way to compute the secrecy rates without the need of lengthy Monte Carlo simulations.
The second part of the thesis investigates the problem of power allocation between the source and relay to optimize the secrecy rate. For the slowly varying fading channel, Lagrange multipliers are used to establish the optimal power allocation schemes between the source and relay nodes under both individual and joint power constraints. It is then demonstrated that full power at the relay is not necessarily optimal. An asymptotic analysis is then provided to provide important insights on the derived power allocation solutions. Using the method of dominant balance, it is demonstrated that full power at the relay is only optimal when the power at relay is sufficiently smaller compared to that of the source. When the power at the relay is larger than the power at the source, the secrecy rate is insensitive to the power at the relay. Similar results are also obtained over ergodic fading channels. In all cases, numerical results reveal that FD DF relaying provides significantly higher secrecy rate than FD AF relaying.
ACKNOWLEDGMENTS

I would like to articulate my praise and gratitude to Almighty Allah for all physical and mental strength he offered me throughout my life.

I am grateful to my advisor, Dr. Nghi H. Tran, for the kindness he showed me, his understanding to my situation and his knowledgeable and experienced guidance throughout this masters.

This work could not have been possible without my loving, sweet and generous husband, Abdo, who supported and encouraged me in every step of the way and was the light that guided me through my darkest times.

I am really grateful to Allah for giving me my precious son, Ahmed, whose smile always brightens my life and also for his soon arriving sister.

I would also like to thank my thesis committees, Drs. Shivakumar Sastry and Jin Kocsis, for their valuable suggestions on my work. The support from the Department of Electrical and Computer Engineering at the University of Akron is also highly appreciated.

I want also to thank my parents for always encouraging me towards the right directions in life and for their unconditional love for me.

Last but not least, special thanks to my family, my family-in-law, my lab mates, for their constant support and encouragement.
# TABLE OF CONTENTS

| LIST OF TABLES                                | viii |
| LIST OF FIGURES                              | ix  |
| CHAPTER                                      |     |
| I. INTRODUCTION                              | 1   |
| 1.1 Motivation                              | 1   |
| 1.2 Contributions                           | 5   |
| 1.3 Thesis Outline                          | 6   |
| II. BACKGROUND                               | 8   |
| 2.1 Basis of Information Theory              | 8   |
| 2.2 Physical Layer Security and Wire-Tap Channels | 11 |
| 2.3 Wireless Fading Channels                 | 13  |
| 2.4 Cooperative Relaying                     | 15  |
| 2.5 Full-Duplex Radio                        | 15  |
| III. SECRECY RATES OF FD DF WIRETAP RELAY CHANNELS IN SLOW FADING AND FAST FADING | 18  |
| 3.1 System Model                             | 19  |
| 3.2 Secrecy Rates                            | 22  |
| 3.3 Numerical Examples                       | 28  |
LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>23</td>
</tr>
<tr>
<td>The secrecy rate under different channel conditions and self-interference performance in slow fading</td>
<td>23</td>
</tr>
</tbody>
</table>

viii
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Wire-tap channel</td>
<td>12</td>
</tr>
<tr>
<td>3.1</td>
<td>The FD DF relay wiretap channel.</td>
<td>19</td>
</tr>
<tr>
<td>3.2</td>
<td>Secrecy rate versus $P_s/N_0$ while $P_r/N_0$ is fixed at 5dB.</td>
<td>29</td>
</tr>
<tr>
<td>3.3</td>
<td>Secrecy rate versus $P_r/N_0$ while $P_r/N_0$ is fixed at 5dB.</td>
<td>30</td>
</tr>
<tr>
<td>3.4</td>
<td>Secrecy rates with DF relaying over ergodic fading: Closed-form expression vs Monte Carlo simulations.</td>
<td>31</td>
</tr>
<tr>
<td>4.1</td>
<td>Secrecy rate versus $P_s/N_0$ in different systems.</td>
<td>45</td>
</tr>
<tr>
<td>4.2</td>
<td>Secrecy rate versus $P_r/N_0$ for different systems.</td>
<td>46</td>
</tr>
<tr>
<td>4.3</td>
<td>Secrecy rate versus $P_s/N_0 = P_r/N_0 = P/N_0$.</td>
<td>47</td>
</tr>
<tr>
<td>4.4</td>
<td>Secrecy rate versus $P_t/N_0(\lambda = [0, 0.5, 1])$.</td>
<td>48</td>
</tr>
<tr>
<td>4.5</td>
<td>Ergodic secrecy rate versus $P/N_0$ for different power allocation schemes under the individual power constraints.</td>
<td>50</td>
</tr>
<tr>
<td>4.6</td>
<td>Ergodic secrecy rate versus $P_t/N_0$ for different power allocation schemes under joint power constraints.</td>
<td>51</td>
</tr>
</tbody>
</table>
CHAPTER I
INTRODUCTION

1.1 Motivation

Recent years have witnessed an explosive growth in mobile data traffic generated by wireless devices, which is predicted to reach almost 50 billion users within the next decade [1]. To keep pace with such demands, significant efforts have been made to address the primary challenge in the design of wireless communication systems: how to increase the data transmission rate over a bandwidth limited wireless radio channel with high reliability and, at the same time, at as low power consumption as possible. Among various solutions, cooperative relaying has been considered as an effective method to increase the range and reliability in wireless networks [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. While research on cooperative relaying is still an active area, and in fact, fundamental limits of many relaying protocols are still unknown [14], benefits offered by cooperative relaying are tremendous and a number of relaying strategies have been adopted in major wireless standards [15].

Among different relaying strategies, amplify-and-forward (AF) and decode-and-forward (DF) relaying are two of the most popular relaying protocols. In fact, these two relaying schemes have been widely adopted in practice [16, 17, 18, 19, 20]. In AF
relaying, the relay forwards a scaled version of the received signal to the destination without modifying the code and modulation implemented at the source. On the other hand, in DF relaying, the transmitted signal from the source is decoded at the relay before being re-transmitted to the destination. As such, DF relaying has been considered to be superior in small deployments areas.

Although AF and DF relaying strategies have been well studied in the literature, most of the previous works assume that the relay operates in half-duplex (HD) mode, i.e., the relay can either transmit or receive on a single channel, but not simultaneously. The HD constraints result in an inefficient use of the limited resources since a dedicated frequency band or time slot is required for relaying. While the ideas of full-duplex (FD) radio have been around for a while, it is not until recently that a number of encouraging FD designs have been proposed to overcome the self-interference problem [21, 22, 23, 24, 25]. The feasibility of FD relaying has also drawn significant interest in both academia and industry [26, 27, 28, 29, 30, 31, 20, 32]. Specifically, it has been demonstrated in [27, 28, 29, 20] that the information rate achieved by FD relaying is better than that of HD relaying in different wireless environments.

In wireless networks, securely transferring confidential data has been considered a challenging task due to the broadcast nature of wireless environments. Besides traditional approaches of using cryptographic methods [33], physical layer (PHY) security based on information theory has been widely acknowledged as an attractive alternative for security enhancement in wireless networks [34, 35, 36, 37, 38]. In wireless PHY security, the key idea is to exploit the characteristics of wireless channels
such as fading gains to transmit a message from a source to an intended destination while keeping this message confidential from passive eavesdroppers. Applications of cooperative relaying have also been considered in PHY security. [39, 40, 41, 42, 43, 44, 45, 46, 47, 48]. For instance, in wireless PHY security, relay nodes can be used as trusted nodes to support a secured transmission from a source to a destination in the presence of one or more eavesdroppers. Similar to cooperative relay communications, a relay can either retransmit an amplified version of the signal received from the source with a suitable power amplification coefficient (in AF relaying), or transmit a weighted version of the decoded signal (in DF relaying). Another method is to generate a weighted jamming signal from the relay to confound the adversary. This technique is usually referred to as cooperative jamming.

While the literature on cooperating relaying under the context of PHY security is vast, most the works only consider HD relaying where the relay cannot transmit and receive at the same time in a single channel. Given the recent development of several encouraging FD radio front-ends [49, 50, 51, 52], the capability of a FD relay in transmitting and receiving simultaneously to further enhance the secrecy is certainly appealing. However, to date, little work has been done for FD relaying. In recent works in [53, 54], FD relaying has been exploited to send jamming signals to the eavesdropper while forwarding information to the destination. However, one of the main drawbacks of these studies is the assumption of significant suppression of self-interference in FD operation. In a realistic FD operation, residual self-interference needs to be explicitly taken into account. Besides the capability of receiving data
and sending jamming signals as in [53, 54], a trusted FD relay can also send and receive data coherently. Under this line of research, the optimal power allocation scheme and the secrecy rate of a FD relay wire-tap channel are investigated in [55] under realistic residual self-interference. A detailed comparison with HD relaying shows that FD relaying is superior than HD relaying in terms of secrecy rates and capacity. While the work in [55] provides important insights on the benefits of FD relaying in increasing secrecy rates, the results are only applicable to AF relaying. Due to their operations, there exist fundamental differences between AF and DF relaying strategies [56]. As a consequence, the consideration of DF relaying under the framework of PHY security and FD poses new challenges, especially under the presence of realistic residual self-interference.

Encouraged by the above discussions, this thesis develops a new PHY security framework for a FD relay wiretap channel where a FD relay is assumed to operate in DF mode to support a secured communication from a source to a destination under the presence of an eavesdropper. Specifically, this thesis investigates the secrecy rate and respective optimal power allocation schemes to maximize the secrecy rate of a FD DF relay wire-tap channel. We shall consider both slowly varying fading channels and ergodic fading channels are considered where the channel gains are assumed to be available at the receivers but not the transmitters.
1.2 Contributions

There are two main contributions. First, closed-form expressions for the secrecy rates are derived for slowly varying and ergodic fading channels. In particular, by first considering a slowly varying fading environment, the channel conditions for which a positive secrecy rate is attained are identified. The residual self-interference due to FD transmission is explicitly taken into account in formulating the secrecy rate. For the case of ergodic fading, we first propose an effective method to calculate the expectation of an exponentially distributed random variable using the exponential integral function. Using this result, the ergodic secrecy rates of the considered FD relay channel are then established in closed-form. Numerical results show that the proposed method provides a simple yet effective way to compute the secrecy rates without the need of lengthy Monte Carlo simulations.

In the second part of the contributions, we investigate the problem of power allocation between the source and the relay to improve the secrecy rate. Specifically, for the slowly varying fading channel, Lagrange multipliers are first used to establish the optimal power allocation schemes between the source and relay nodes under both individual and joint power constraints. It is then demonstrated that full power at the relay is not necessary optimal. An asymptotic analysis is then provided to provide important insights on the derived power allocation solutions. Specifically, by using the method of dominant balance, it is demonstrated that full power at the relay is only optimal when the power at relay is sufficiently smaller compared to that of
the source. When the power at the relay is larger than the power at the source, increasing the power consumed at the relay yields a very slow increase in the secrecy rate, i.e., the secrecy rate is insensitive to the power at the relay. In fact, the secrecy rate approaches to a constant for an effective control of the self-interference. Similar results are also obtained over ergodic fading channels. Numerical results also reveal that DF relaying provides significantly higher secrecy rate over AF relaying.

1.3 Thesis Outline

The remainder of the thesis is organized as follows. Chapter 2 introduces essential background that is necessary for the development of the subsequent chapters. This includes several basic concepts in information theory, such as entropy, mutual information, and capacity. In this chapter, we also discuss a basis of physical layer security and wire-tap channels. After establishing these concepts, a brief insight on about wireless communication channel is then presented. Finally, several relaying technologies including AF and DF, and the attractions of FD radio are introduced and discussed.

Chapter 3 addresses the secrecy rate of the considered FD DF relay network. We will start with slowly fading channels before extending the results to ergodic fading channels.

In Chapter 4, the optimal power allocation schemes for a slowly fading FD DF wiretap relay channel are first developed under individual and joint power constraints between the source and relay. An asymptotic analysis is then given to provide impor-
tant insights on the derived power allocation solutions. The results are then extended to ergodic fading channels.

Finally, conclusions are drawn in Chapter 5. In this chapter, interesting research directions in PHY security are also outlined and discussed for future studies.
This chapter sets essential background necessary for the development of subsequent chapters. The first mean of doing so is through the introduction of several fundamental concepts in information theory. An overview of wiretap channels and basic ideas of physical layer security are then provided. This chapter also presents key characteristics of wireless fading channels. A discussion about cooperative relaying with DF and AF is then given. Finally, a brief overview of FD radio and its recent developments are provided.

2.1 Basis of Information Theory

Information theory addresses two fundamental problems in communication theory: What is the maximum data compression and what is maximum transmission rate. The answers to these questions lie in two important quantities, entropy and mutual information.

2.1.1 Entropy

Entropy is a measure of the uncertainty of a random variable (RV). Let $X$ be a discrete RV with probability mass function (PMF) $p(x)$. Then the entropy of $X$ can be
expressed as

$$H(X) = - \sum_{x \in X} p(x) \log p(x). \quad (2.1)$$

The log is either to base 2 or $e$, which gives a measurement in bits or nats, respectively. Throughout this thesis, unless otherwise stated, base 2 is used.

For a continuous RV $X$ with the probability density function $f(x)$ over a support set $S$, its entropy is defined through the concept of differential entropy, which is given as:

$$h(X) = - \int_S f(x) \log f(x) dx. \quad (2.2)$$

2.1.2 Joint and Conditional Entropy

The concept of joint entropy is an extension of entropy when two or more RVs are involved. In particular, consider two discrete RVs $X$ and $Y$ having a joint distribution $p(x, y)$, the joint entropy of $X$ and $Y$ is defined as:

$$H(X, Y) = - \sum_{x \in X} \sum_{y \in Y} p(x, y) \log p(x, y) = -E \log p(x, y). \quad (2.3)$$

Furthermore, the conditional entropy of a RV $Y$ given the knowledge of another RV $X$ denoted as $H(Y|X)$ is defined as:

$$H(Y|X) = - \sum_{x \in X} p(x)H(Y|X = x) = - \sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log p(y|x)$$
\[ - \sum_{x \in X} \sum_{y \in Y} p(x, y) \log p(y|x) = -E \log p(y|x) \quad (2.4) \]

It can then be verified that

\[ H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y). \quad (2.5) \]

For two continuous RVs \(X\) and \(Y\) with the joint density function \(f(x, y)\), the conditional differential entropy is defined as:

\[ h(X \mid Y) = - \int \int f(x, y) \log f(x \mid y) dxdy. \quad (2.6) \]

In a similar manner, we have the following relationship between the conditional and joint differential entropy:

\[ h(X, Y) = h(X) + h(Y|X) = h(Y) + h(X|Y). \quad (2.7) \]

2.1.3 Relative Entropy and Mutual Information

The relative entropy is a metric used to measure the distance between two distributions. Specifically, the relative entropy between two probability mass functions \(p(x)\) and \(q(x)\) is defined as:

\[ D(p \parallel q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)}. \quad (2.8) \]
For continuous RVs, the relative entropy between two density functions $f$ and $g$ is defined as:

$$D(f \parallel g) = \int f \log \frac{f}{g},$$

(2.9)

Finally, mutual information between two RVs $X$ and $Y$ provides the reduction in uncertainty of a RVs due to the knowledge of the other RV, and it can be defined as:

$$I(X; Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X).$$

(2.10)

For a communication system with an input $X$ and an output $Y$, the channel capacity, which can be understood as the maximum transmission rate from the input to the output, can be obtained via the mutual information $I(X, Y)$ as:

$$C = \max_{p(x)} I(X, Y),$$

where the maximum is taken over all possible input distributions $p(x)$.

### 2.2 Physical Layer Security and Wire-Tap Channels

Physical layer (PHY) security based on information theory has been gaining significant research attention recently. Different from traditional cryptography, the key idea of PHY security is to exploit the physical characteristics of communication channels to transmit a confidential message from a source to an intended destination.
In this thesis, the focus is on PHY security over wiretap fading channels. The main objective is to provide information-theoretic privacy of transmitted data based solely on the hypothesis that the channel from the transmitter to the illegitimate eavesdropper is noisier than the channel from the transmitter to the legitimate receiver. This framework has been the subject of decades of work in the information and coding community. The wire-tap channel model, which is shown in Fig. 2.1, was first proposed by Wyner in [57] and further polished in 1978 by Csiszr and Korner for broadcast channels with confidential messages in [58]. Essentially, the wiretap channel includes the following components:

1. The source transmits a sequence of independent, identically distributed (i.i.d) random variables $S^K = \{S_k\}_1^\infty$ assuming that the source distribution and its entropy are known.

2. The encoder converts information from one format or code $(S^K) = (S_1....S_K)$ to another format $(X^N) = (X_1....X_N)$ with transition probability $q_E(x|s), s \in S^K, x \in X^N$.  

![Figure 2.1: Wire-tap channel](image_url)
• The **main channel** $Q_M$—which is assumed to be a discrete memoryless channel—
inputs finite sequences $X^N$ and outputs finite sequences $Y^N$ with transition probability $Q_M(y|x)$, where $x \in X^N$ and $y \in Y^N$.

• The output sequences $Y^N$ from the main channel become the input to the
**wiretap channel** $Q_W$ which is also a discrete memoryless channel that outputs
finite sequences $Z^N$ with a transition probability $Q_W(z|y)$, where $y \in Y^N$ and $z \in Z^N$. Combining these two sequential discrete memoryless channels results
in another discrete memoryless channel $Q_{MW}$ with a transition probability:

$$Q_{MW}(z|x) = \sum_{y \in Y} Q_W(z|y)Q_M(y|x).$$

• The **decoder** maps the sequences $Z^N$ back to an estimated version of $S^K$ with
an error probability:

$$P_e = \frac{1}{K} \sum_{K=1}^{N} Pr(S_k \neq \hat{S}_k).$$

The concept of secrecy rate in information theory, which is the information rate
that can be transmitted confidentially from a source to a destination without any
knowledge leaked to eavesdroppers, is fundamental for the wiretap channel. The
maximum achievable secrecy rate is referred to as the secrecy capacity.

2.3 Wireless Fading Channels

Wireless communication refers to communication of information between devices that
are not physically connected. In wireless communications, channel quality can change
over time, which can be categorized into the following two phenomenons:
• Large-scale fading: This happens due to the path loss of the signal as a function of distance, and shadowing by large obstacles.

• Small-scale fading: This occurs as a result of the constructive and destructive addition of multiple copies of the transmitted signals at the receiver. Due to small-scale fading, channel variations happen over short distance. This phenomenon has been considered as one of the most challenging problems that affects the reliability and efficiency of wireless communications systems. In this thesis, only small-scale fading is considered.

To demonstrate further the effect of small-scale fading, let us consider a simple wireless fading channel as follows. Assume that at a given time \( i \), a signal \( x_i \) is transmitted from a source to a destination. The signal received at the destination is given as:

\[
y_i = h_i x_i + n_i.
\]

Here, \( n_i \) is thermal noise, while \( h_i \) represents the fading gain resulting from small-scale fading. In a richly scattered environment where the number of independently reflected and scattered paths is large, \( h_i \) can be modeled as a zero-mean circularly symmetric complex Gaussian random variable. This results in a so-called Rayleigh fading channel, since the magnitude of \( h_i \) follows a Rayleigh distribution.

Depending on the dynamic feature of the environment, \( h_i \) might change slowly over time. This is usually referred to as slow fading. Under this condition, we can assume that \( h_i \) can be perfectly estimated at both the receiver and the transmitter.
On the other hand, if $h_i$ varies fast over time, we have a so-called fast or ergodic fading channel. In fast fading, it makes it more challenging to obtain an accurate $h_i$, especially at the transmitter side. In this thesis, we consider both slow and fast fading channels.

2.4 Cooperative Relaying

It has been widely recognized that the reliability and efficiency of a wireless transmission from a source to a destination can be significantly enhanced by dedicated nodes that perform relaying function to assist the source and destination [59]. Among different relaying strategies, amplify-and-forward (AF) and decode-and-forward (DF) relaying have been considered as the two most effective relaying schemes [60, 56]. In AF relaying, the relay only amplifies the received message and retransmits it to the intended destination. On the other hand, in DF relaying, a more sophisticated mechanism is performed at the relay. Specifically, the relay can decode and then re-encode the received signal from the source before retransmitting this signal to the destination.

2.5 Full-Duplex Radio

Current wireless communication systems operate in half-duplex mode, i.e., current wireless radios cannot transmit and receive at the same time and on the same frequency. FD wireless operation was generally assumed to be impossible due to the
great difference in transmit and receive signal power levels. However, recent advances have shown that FD operation is feasible by applying and combining different self-interference mitigation techniques [21, 22, 23, 24, 25]. In particular, to avoid saturating the receiver front end, several mitigation techniques prior to the analog-to-digital converter (ADC) have been proposed. For instance, basic analog cancellation methods include antenna separation [61, 62, 63, 23], orientation [62, 64] and directionality [65, 66]. More sophisticated methods have been proposed recently to further eliminate the self-interference [21]. For example, by using two transmit antennas around a single receive antenna, an impressive isolation of about 40dBm can be achieved [21]. Jain et al. in [67] considered the use of only two antennas, combined with passive analog cancelation based on variable attenuators and delay lines, which prevents out-of-band signal leakage and reduces power consumption. The authors in [68] have further modified the architecture to one antenna, which transmits and receives simultaneously by incorporating a circulator. Khojastepour et al. in [22] have recently proposed an architecture, which eliminates the use of programmable attenuators and delay lines utilizing a symmetric antenna configuration, and at the same time providing wideband antenna cancellation. In [69], improved self-interference suppression has been demonstrated for WiFi networks. The proposed FD system achieves 85 dB of cancellation by utilizing passive, analog, and digital methods.

The feasibility in building a practical full-duplex radio using off-the-self hardware and software radios therefore alleviates many problems in wireless network designs, and as a consequence, might change the way to build wireless networks. For
instance, the ability of a full-duplex relay in transmitting and receiving data concurrently allows more flexibility in utilizing limited radio resource, and consequently improving the reliability and security of the wireless transmission.
As reviewed earlier, FD has been recently exploited to improve the security of single- and multi-hop relaying systems [53, 54, 55]. For example, reference [55] has demonstrated the advantage of using a FD relay that can transmit and receive data simultaneously in AF mode. In this chapter, the results in [55] are extended by investigating the secrecy rate of a FD single-hop wiretap relay channel where the relay is assumed to operate in DF mode. In addition to slowly fading channels as in [55], ergodic Rayleigh fading channels are also considered. These ergodic channel models are more realistic. Because wireless environments are dynamic, with time-varying fading channels. As demonstrated in this chapter, the presence of fading in addition to secrecy constraints and the residual self-interference of FD operation certainly makes it more challenging to study the benefits of FD over HD relaying. To our knowledge, the calculation of secrecy rate under fading usually relies on lengthy Monte Carlo simulations and the results here are the first analytical results to determine the secrecy rate. It is important to note that these analytical results represent the best rate that can be achieved under idealized conditions.
This chapter starts with the introduction of the considered FD relay channel and describes the DF operation in detail. The secrecy rate and the conditions with which a positive rate is achieved are then established for the case of slow fading. To deal with ergodic fading, a closed-form expression for the expectation of an exponentially distributed random variable is established via exponential integral functions. By exploiting this result, it is demonstrated that the ergodic secrecy rates of the considered relay channels that involve triple integrals can be expressed in a closed-form. Numerical results demonstrate that the proposed methods provide a simple yet accurate way to calculate the secrecy rate.

3.1 System Model

![Figure 3.1: The FD DF relay wiretap channel.](image)

The considered relay wiretap model is shown in Fig. 3.1. In this model, we have a HD source node, a HD destination, a HD eavesdropper and the transmission from
the source to the destination is aided by a FD relay that uses decode-and-forward (DF). In the following, we first describe the transmission under slow fading before extending it further to the case of ergodic fading.

### 3.1.1 Slow Fading Channels

In this case, at a given frame $i$, $S$ transmits the signal $x_i$ to the relay $R$. At the relay, the received signal is given as

$$ r_i = \sqrt{P_s} h_1 x_i + n_{r,i} + v_i. $$

In (3.1), $P_s$ is a constant associated with the power transmitted at $S$, and $h_1$ is the channel gain of the S-R link. In addition, $n_{r,i}$ is the zero-mean circularly Gaussian noise at $R$, which is denoted as $n_{r,i} \sim CN(0, N_r)$, while $v_i$ is the residual self-interference resulting from the FD operation at the relay. While receiving $x_i$, the relay can decode a signal it receives at time $i - 1$ before extracting the data and retransmitting this information to the destination. Let $\hat{x}_{i-1}$ be the forwarded signal at $R$. The signals received at $D$ and overheard at $E$ can then be written respectively as:

$$ y_{d,i} = \sqrt{P_r} h_3 \hat{x}_{i-1} + n_{r,i}, $$

$$ y_{e,i} = \sqrt{P_r} h_4 \hat{x}_{i-1} + n_{d,i}. $$
Here, that $P_r$ is a constant related to the power consumed at $R$. Furthermore, $h_3$ and $h_4$ are channel gains of the links $R-D$ and $R-E$, respectively, and $n_{d,i} \sim \mathcal{CN}(0, N_d)$ and $n_{e,i} \sim \mathcal{CN}(0, N_e)$ are the thermal noises at $D$ and $E$. For the slow fading channel, it is assumed that the gains $\mathbf{h} = [h_1, h_3, h_4]$ change slowly and can be considered as constants. Furthermore, as in [70, 71, 72, 73, 74], we assume that these gains are available at all nodes. This assumption can be realistic where the eavesdropper is a lower-level user belonging to the same legitimate network. Without loss of generality, we also assume that the thermal noise levels are the same at all nodes, i.e., $N_r = N_e = N_d = N_0$. Now, let $\mathbb{E}[|x_i|^2] = q_1$ and $\mathbb{E}[|\hat{x}_i|^2] = q_2$, i.e., $S$ and $R$ use an average power $q_1 P_s$ and $q_2 P_r$, respectively. We also assume that the source has the power constraint of $q_s P_s$, while we have a power constraint $q_r P_r$ at the relay. It means that $q_1 \leq q_s$ and $q_2 \leq q_r$. Note that in general, the relay might not need to use full power. For FD operation, we adopt the model in [75, 76] where the residual self-interference has been shown to follow a Gaussian distribution with $v_i \sim \mathcal{CN}(0, V)$. The variance $V$ is given as $V = \beta (q_2 P_r)^\lambda$, where $\beta$ and $\lambda$ ($0 \leq \lambda \leq 1$) are constants that depend on the cancellation techniques [75, 76].

3.1.2 Ergodic Fading Channels

For ergodic fading, it is assumed that all the channel gains change independently from frame to frame. Specifically, in (3.1), the channel gain $h_1$ is replaced by a fading gain $h_1^{(i)}$, which is a complex Gaussian random variable with variance $\phi_1$, i.e., $h_1^{(i)} \sim \mathcal{CN}(0, \phi_1)$. In a similar manner, the channel gains $h_3$ and $h_4$ in (3.2) become
$h_3^{(i)}$ and $h_4^{(i)}$, respectively, and they are the complex Gaussian variables with variances $\phi_3$ and $\phi_4$, respectively, i.e., $h_3^{(i)} \sim \mathcal{CN}(0, \phi_3)$, $h_4^{(i)} \sim \mathcal{CN}(0, \phi_4)$. Furthermore, we assume that the channel state information (CSI) is available at the receivers but not the transmitter, i.e, $D$ and $E$ have full knowledge of channel gains $\mathbf{h}_i = [h_1^{(i)}, h_3^{(i)}, h_4^{(i)}]$, while $R$ can estimate $h_1^{(i)}$ perfectly.

3.2 Secrecy Rates

In this section, we first establish the secrecy rate for slow fading channels. The closed-form expression for the secrecy rate in ergodic fading is then investigated.

3.2.1 Slow Fading

With DF relaying, the achievable rate at a destination is bounded by the capacities of the two links so that a reliable decoding at $R$ and $D$ can be guaranteed: from the source to relay and relay to destination [77], [78]. The end-to-end achievable rate at $E$ can also be obtained in a similar manner. The maximum end-to-end achievable rates at $D$ and $E$, respectively, can be written as:

$$I_d = \log \left( 1 + \min \left( \frac{q_1 \gamma_1}{1 + q_2 \gamma_2}, q_2 \gamma_3 \right) \right),$$

$$I_e = \log \left( 1 + \min \left( \frac{q_1 \gamma_1}{1 + q_2 \gamma_2}, q_2 \gamma_4 \right) \right),$$

(3.4)

where

$$\gamma_1 = \alpha_1 P_s/N_0,$$

(3.5)
Table 3.1: The secrecy rate under different channel conditions and self-interference performance in slow fading.

<table>
<thead>
<tr>
<th>Case</th>
<th>Channel conditions</th>
<th>$R_s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Case 1</td>
<td>$\gamma_r \leq \gamma_d \leq \gamma_e$</td>
<td>$R_s = \log \left( \frac{1+\gamma_r}{1+\gamma_d} \right) = 0$</td>
</tr>
<tr>
<td>Case 2</td>
<td>$\gamma_r \leq \gamma_e \leq \gamma_d$</td>
<td>$R_s = \log \left( \frac{1+\gamma_r}{1+\gamma_e} \right) = 0$</td>
</tr>
<tr>
<td>Case 3</td>
<td>$\gamma_d \leq \gamma_r \leq \gamma_e$</td>
<td>$R_s = \log \left( \frac{1+\gamma_d}{1+\gamma_r} \right) = 0$</td>
</tr>
<tr>
<td>Case 4</td>
<td>$\gamma_d \leq \gamma_e \leq \gamma_r$</td>
<td>$R_s = \log \left( \frac{1+\gamma_d}{1+\gamma_e} \right) = 0$</td>
</tr>
<tr>
<td>Case 5</td>
<td>$\gamma_e \leq \gamma_r \leq \gamma_d$</td>
<td>$R_s = \log \left( \frac{1+\gamma_e}{1+\gamma_r} \right) \geq 0$</td>
</tr>
<tr>
<td>Case 6</td>
<td>$\gamma_e \leq \gamma_d \leq \gamma_r$</td>
<td>$R_s = \log \left( \frac{1+\gamma_e}{1+\gamma_d} \right) \geq 0$</td>
</tr>
</tbody>
</table>

\[
\gamma_2 = \beta P_r^\lambda / N_0, \quad (3.6)
\]

\[
\gamma_3 = \alpha_3 P_r / N_0, \quad (3.7)
\]

and

\[
\gamma_4 = \alpha_4 P_r / N_0, \quad (3.8)
\]

with $\alpha_j = |h_j|^2$. The achievable secrecy rate for a given power allocation $q_1$ and $q_2$ can then be expressed as:

\[
R_s = [I_d - I_e]^+ \quad (3.9)
\]

where $[x]^+ = \max\{0, x\}$.

To proceed further, let examine the positivity of the secrecy rate in (3.9). To this end, let $\gamma_r = q_1 \gamma_1 / (1 + q_2^\lambda \gamma_2)$, $\gamma_d = q_2 \gamma_3$ and $\gamma_e = q_2 \gamma_4$. Depending on how $\gamma_r$, $\gamma_d$ and $\gamma_e$ are related, Table 3.1 shows six possible cases of the secrecy rate. Note that a positive secrecy rate is achieved only in cases 5 and 6. These two cases
correspond to the situation where $\gamma_d > \gamma_e$ or, equivalently $\gamma_3 > \gamma_4$. This means that the relay-destination channel must be stronger than the relay-eavesdropper channel for the system to achieve a positive secrecy rate. Under this condition, the rate $R_s$ can be expressed as:

$$R_s = \log \left( \frac{1 + \min (\gamma_r, \gamma_d)}{1 + \gamma_e} \right).$$  \hspace{1cm} (3.10)

3.2.2 Ergodic Fading

In this case, the instantaneous end-to-end rates at $D$ and $E$, respectively, for a given channel realization $\mathbf{h}_i = [h_1^{(i)}, h_3^{(i)}, h_4^{(i)}]$ can then be expressed as:

$$I_{d|h_i} = \log \left( 1 + \min \left( \frac{q_1 \gamma_1}{1 + q_2 \gamma_2}, q_2 \gamma_3 \right) \right).$$

$$I_{e|h_i} = \log \left( 1 + \min \left( \frac{q_1 \gamma_1}{1 + q_2 \gamma_2}, q_2 \gamma_4 \right) \right).$$  \hspace{1cm} (3.11)

Note that difference from (3.4), the parameters $\gamma_1$, $\gamma_3$, $\gamma_4$ in (3.11) depends on the instantaneous channels, i.e., $\gamma_1 = |h_1^{(i)}|^2 P_s/N_0$, $\gamma_3 = |h_3^{(i)}|^2 P_r/N_0$, and $\gamma_4 = |h_4^{(i)}|^2 P_r/N_0$, while we still have $\gamma_2 = \beta P_r^\lambda/N_0$. The ergodic secrecy rate for DF relaying can then be obtained by averaging the difference between the two instantaneous rates over three channel gains as follows:

$$R_s = \mathbb{E}_h [I_{d|h_i} - I_{e|h_i}]^+. \hspace{1cm} (3.12)$$
It can be observed from (3.12) that the average secrecy rates involve triple-integrals. As a consequence, calculating them with high accuracy is very cumbersome. Monte Carlo simulations can be used as an alternative to calculate these rates. However, it is a time consuming process and does not give an insight on the behavior of the secrecy rate. In the following, we propose a simple method to establish $R_s$ in (3.12) in closed-form. To this end, the following lemma first states an important result related to an exponential integral, which is an extension of the result in [79].

**Lemma 1.** Consider two independent exponentially distributed random variables $\omega_1$ and $\omega_2$. Assume that their means are $\phi_1$ and $\phi_2$, respectively. Let $\mathcal{J}(x) = \exp(x)E_1(x)$, with $E_1(.)$ being the well-known the exponential integral given as:

$$E_1(x) = \int_{x}^{\infty} \frac{e^{-u}}{u} du = - \left( \gamma + \ln(x) + \sum_{n=1}^{\infty} \frac{(-1)^n x^n}{n! n} \right),$$

and $\gamma$ is the Euler number. For any positive $a_0$, we have:

$$E_{\omega_1}[\ln(a_0 + \omega_1)] = \mathcal{J}(a_0/\phi_1), \quad (3.13a)$$

$$E_{\omega_1,\omega_2}[\ln(a_0 + \omega_1 + \omega_2)] =$$

$$\begin{cases} 
1 + \ln(a_0) + \left( 1 - \frac{a_0}{\phi_2} \right) \mathcal{J}(\frac{a_0}{\phi_1}), & \phi_1 = \phi_2 \\
\ln(a_0) + \frac{\phi_1 \mathcal{J}(1/\phi_1) - \phi_2 \mathcal{J}(1/\phi_2)}{\phi_1 - \phi_2} - \gamma, & \phi_1 \neq \phi_2.
\end{cases} \quad (3.13b)$$
Proof. By factoring \( a_0 \), the expectation in (3.13a) is expressed as:

\[
E_{\omega_1} \left[ \ln(a_0 + \omega_1) \right] = \ln(a_0) + E_{\omega_1} \left[ \ln(1 + \omega_1/a_0) \right],
\]

(3.14)

The above expectation is similar to the achievable rate achieved in a single-input single-output system with instantaneous SNR \( \omega_1/a_0 \), and average SNR \( \phi_1/a_0 \) in [80, eq. (15.26)]. In a similar manner, the expectation in (3.13b) can be written as

\[
E_{\omega_1,\omega_2} \left[ \ln(a_0 + \omega_1 + \omega_2) \right] = \ln(a_0) + E_{\omega_1,\omega_2} \left[ \ln(1 + (\omega_1/a_0) + (\omega_2/a_0)) \right].
\]

(3.15)

When \( \phi_1 = \phi_2 \), we can use the formula [80, eq. (15.33)] to end up with the first part of (3.13b). When \( \phi_1 \neq \phi_2 \), the above expectation is equivalent to the achievable rate of a general two-branch maximum-ratio combiner provided in [81] and we obtain the second part of (3.13b).

Given the results in Lemma 1, we are now ready to find the closed-form expression of the rate formula in (3.12), which is described in the following.

The average secrecy rate given in (3.12) can be re-written as:

\[
R_S = E_{h_1,h_3} \left[ \log \left( 1 + \min \left( \frac{q_1\gamma_1}{1 + q_2\gamma_2}, q_2\gamma_3 \right) \right) \right] - E_{h_1,h_4} \left[ \log \left( 1 + \min \left( \frac{q_1\gamma_1}{1 + q_2\gamma_2}, q_2\gamma_4 \right) \right) \right].
\]

(3.16)
It has been known that the minimum of two exponential random variables (RV) with the two corresponding expected values $1/\alpha_1$ and $1/\alpha_2$ is also an exponential RV with expected value $1/(\alpha_1 + \alpha_2)$ [82]. Therefore, (3.16) can be rewritten as:

$$R_S = E \left[ \log (1 + \gamma_r) \right] - E \left[ \log (1 + \gamma_e) \right],$$  

(3.17)

where $\gamma_r = \min \left( \frac{q_1 \gamma_1}{1+q_2 \gamma_2}, q_2 \gamma_3 \right)$ and $\gamma_e = \min \left( \frac{q_1 \gamma_1}{1+q_2 \gamma_2}, q_2 \gamma_4 \right)$ are two exponential RVs with the following expected values, respectively:

$$\overline{\gamma}_r = \frac{q_1 \overline{\gamma}_1 \times q_2 \overline{\gamma}_3}{q_1 \overline{\gamma}_1 + q_2^{\lambda + 1} \overline{\gamma}_2 \overline{\gamma}_3 + q_2 \overline{\gamma}_3},$$

$$\overline{\gamma}_e = \frac{q_1 \overline{\gamma}_1 \times q_2 \overline{\gamma}_4}{q_1 \overline{\gamma}_1 + q_2^{\lambda + 1} \overline{\gamma}_2 \overline{\gamma}_4 + q_2 \overline{\gamma}_4}.$$

Here, $\overline{\gamma}_1 = E\{\gamma_1\}=P_s \phi_1/N_0$, $\overline{\gamma}_3 = E\{\gamma_3\}=P_r \phi_3/N_0$, and $\overline{\gamma}_4 = E\{\gamma_4\}=P_r \phi_4/N_0$. Thus, from the results in Lemma 1, the expectation in (3.16) can be obtained in closed-form as:

$$R_S = \frac{1}{\ln(2)} \times$$

$$\left[ J \left( \frac{q_1 \overline{\gamma}_1 + \overline{\gamma}_2 \overline{\gamma}_3 + q_2 \overline{\gamma}_4}{q_1 \overline{\gamma}_1 \times q_2 \overline{\gamma}_3} \right) - J \left( \frac{q_1 \overline{\gamma}_1 + \overline{\gamma}_2 \overline{\gamma}_4 + q_2 \overline{\gamma}_4}{q_1 \overline{\gamma}_1 \times q_2 \overline{\gamma}_4} \right) \right]^+$$

(3.18)

It can be seen from (3.18) the ergodic secrecy rate for DF relaying can be evaluated. Because the expression in (3.18) involves only the well-known exponential integrals.

In the next section, numerical results are presented to confirm the accuracy of the
proposed solution in (3.18).

3.3 Numerical Examples

In the following, numerical results are provided to confirm the accuracy of the proposed secrecy rates in (3.10) for slow fading channels and in (3.18) for ergodic fading channels.

3.3.1 Slow Fading

For slow fading channels, unless otherwise stated, it is assumed that \( \alpha_1 = 1 \), \( \alpha_3 = 2 \), \( \alpha_4 = 1 \). Furthermore, we use \( q_s = q_r = 1 \) and full power allocation is assumed at both the source and relay, i.e., \( q_1 = q_s \) and \( q_2 = q_r \). In all results, we use \( \beta = 0.1 \) and \( \lambda \) can be either 0, 0.5, or 1 to show the effect of self-interference cancellation performance.
Figure 3.2: Secrecy rate versus $P_s/N_0$ while $P_r/N_0$ is fixed at 5dB.

First, Fig. 3.2 shows the secrecy rate $R_s$ versus $P_s/N_0$ when $P_r/N_0$ is fixed at 5dB. It is interesting to observe from Fig. 3.2 the rate $R_s$ approaches a constant at a sufficiently high $P_s/N_0$. Equivalently, when $P_r/N_0$ is fixed, $R_s$ is insensitive to the power used at the source.
In Fig. 3.3, we plot the secrecy rates versus $P_r/N_0$ while the source power is fixed at $P_s/N_0 = 5$dB. It can be seen that at sufficiently high $P_r/N_0$, the secrecy rate approaches zero. It is because when $P_r$ increases, $\gamma_3$ and $\gamma_4$ also increase at the same rate, and the two links $R-D$ and $R-E$ will have a similar SNR.

3.3.2 Ergodic Fading

In the case of ergodic fading, besides the rate obtained by the closed-form expression in (3.18), the results obtained by Monte Carlo simulations will also be used as a benchmark. For the considered channels, the Monte Carlo simulations are performed as follows. For a given set of channel gains $h_i = [h_1^{(i)}, h_3^{(i)}, h_4^{(i)}]$ with respective
Figure 3.4: Secrecy rates with DF relaying over ergodic fading: Closed-form expression vs Monte Carlo simulations.

variances $\Phi = [\phi_1, \phi_3, \phi_4]$, the instantaneous secrecy rates are calculated by using (3.11). To obtain the ergodic secrecy rates in (3.12), we average the instantaneous secrecy rates over $10^7$ samples of the channel gains. As similar to the case of slow fading, in all results, we use $\beta = 0.1$ and $\lambda$ can be either 0, 0.5, or 1. In addition, for the channel variances, we use $\phi_1 = 2, \phi_3 = 2.5$ and $\phi_4 = 1.5$. It should be noted that the proposed solution can apply to any set of channel parameters.

To demonstrate the usefulness of the closed-form expression in (3.18), Fig. 3.4 compares the secrecy rate versus signal-to-noise ratio $\text{SNR} = P/N_0$ using this closed-form and that obtained by Monte Carlo simulations for different values of $\lambda$. Here,
the assumption is that $P_s = P_r = P$ and full power allocation is used at both source and relay nodes, i.e., $q_1 = q_s$ and $q_2 = q_r$. It can be seen from Fig. 3.4 that the results obtained by the proposed closed-form match perfectly with the results from Monte Carlo simulations. This verifies the accuracy of the proposed solution in (3.18).
CHAPTER IV

OPTIMAL POWER ALLOCATION SCHEMES FOR DF FD RELAY WIREFAP CHANNELS

In the previous chapter, close-form expressions of the secrecy rates for both slow fading and ergodic fading have been formulated. These secrecy rates were obtained for a given power allocation scheme at the source and relay, i.e., power allocated at the source and relay is assumed to be fixed. In a more flexible scenario, power allocation at the relay and the source can be further optimized to improve the secrecy rates under some certain constraints.

The focus of this chapter is therefore on finding an optimal power allocation scheme to maximize the secrecy rates. We will investigate both individual and joint power constraints imposed on the source and the relay. In practice, the individual power constraints are due to the power constraint on each individual RF chain. On the other hand, the joint power constraint takes into account the total power allocated to both the source and relay. Although not always being practical, this joint power constraint is a useful criterion to compare different transmission schemes. In addition, a network with such a constraint can serve as a system benchmark to any system under individual power constraints. Finally, it is noted that in several wireless networks where the nodes can be managed directly by the service provider, the joint power
constraint can still be made possible.

This chapter starts with the formulation of the optimization problem of interest under individual and joint power constraints. Focusing on the slow fading channels, we establish the corresponding optimal power allocation for the considered relay wire-tap channel. After that, we perform an asymptotic analysis on the derived optimal power allocation schemes to shed important insights on the solutions. Specifically, using the method of dominant balance, it is shown that full power at the relay is needed only when the power at relay is sufficiently smaller compared to that of the source. When the power at the relay is larger than the power at the source, it is shown that the secrecy rate approaches a constant. Finally, we extend the results to fast fading channels.

4.1 Optimization Problems

As we discussed earlier in Chapter 3, for a given power allocation scheme at the source and relay $q_1$ and $q_2$, respectively, we achieve a secrecy rate $R_s$. Under individual power constraints, it is assumed that $0 \leq q_1 \leq q_s$ and $0 \leq q_2 \leq q_r$ so that the power constraints at the source and the relay are $q_sP_s$ and $q_rP_r$, respectively. The optimization problem of interest is to find the set $\{q_1, q_2\}$ to maximize $R_s$, which is written as:

$$\max_{q_1, q_2} R_s \text{ s.t. } 0 \leq q_1 \leq q_s, 0 \leq q_2 \leq q_r \text{ (individual).}$$ (4.1)
In the case of joint power constraint, the total power budget at both source and relay is $q_t P_t$. Furthermore, it is assumed that $P_s = P_r = P_t$. The optimization problem can then be expressed as:

$$\max_{q_1, q_2} R_s \text{ s.t. } q_1 \geq 0, q_2 \geq 0, q_1 + q_2 \leq q_t \text{ (joint).} \quad (4.2)$$

In the following, the above optimization problems to maximize $R_s$ are shown. We will examine slow fading channels first before considering the ergodic fading cases.

4.2 Optimal Power Allocation Schemes in Slow Fading

In this section, the focus is on slow fading. The optimization problem (4.1) is first studied before we extend the results to the problem in (4.2). Finally, an asymptotic analysis on the derived solutions is provided to shed important insights on the solutions. Recall from Chapter 3 that to achieve a positive $R_S$ in slow fading, the relay-destination channel must be stronger than the relay-eavesdropper channel, i.e., $\gamma_3 > \gamma_4$. Under this condition, the rate $R_S$ can be expressed as:

$$R_s = \log \left( \frac{1 + \min(\gamma_r, \gamma_d)}{1 + \gamma_e} \right). \quad (4.3)$$

where $\gamma_r = q_1 \gamma_1 / (1 + q_2 \gamma_2)$, $\gamma_d = q_2 \gamma_3$, and $\gamma_e = q_2 \gamma_4$. Note that $\gamma_1$, $\gamma_2$, $\gamma_3$, and $\gamma_4$ are calculated as in (3.5), (3.6), (3.7), and (3.8), respectively. Furthermore, since $\gamma_3 > \gamma_4$, we have $\gamma_d > \gamma_e$. Therefore, if $\gamma_r \leq \gamma_e$, $R_s = 0$. As result, we can only achieve a
positive $R_s$ under either of the following conditions: Condition 1: $\gamma_e \leq \gamma_r \leq \gamma_d$; or Condition 2: $\gamma_e \leq \gamma_d \leq \gamma_r$.

4.2.1 Individual Power Constraints

Under the individual power constraints, let us examine the following two cases:

1) **Condition 1 holds**

This happens when $\gamma_e \leq \gamma_r \leq \gamma_d$, or equivalently,

$$q_2^{\lambda+1}\gamma_2\gamma_3 + q_2\gamma_3 \geq q_1\gamma_1 \geq q_2^{\lambda+1}\gamma_2\gamma_4 + q_2\gamma_4.$$  \hfill (4.4)

The rate $R_s$ can then be expressed as:

$$R_s = \log \left( \frac{1 + \gamma_r}{1 + \gamma_e} \right) = \log f_1(q_1, q_2).$$ \hfill (4.5)

The optimization problem in (4.1) then becomes:

$$\max_{q_1, q_2} f_1(q_1, q_2) \text{ s.t.} \begin{cases} 0 \leq q_1 \leq q_s \\ 0 \leq q_2 \leq q_r \\ q_2^{\lambda+1}\gamma_2\gamma_3 + q_2\gamma_3 \\ \geq q_1\gamma_1 \geq q_2^{\lambda+1}\gamma_2\gamma_4 + q_2\gamma_4 \end{cases}$$ \hfill (4.6)

By taking the derivative of $f_1(q_1, q_2)$ w.r.t. $q_1$, we have

$$\frac{\partial f_1(q_1, q_2)}{\partial q_1} = \frac{\gamma_1}{(1 + q_2\gamma_4) \times (1 + q_2^{\lambda}\gamma_2)} > 0.$$ \hfill (4.7)
As a result, \( f_1(q_1, q_2) \) is an increasing function of \( q_1 \). On the other hand, by taking the derivative of \( f_1(q_1, q_2) \) w.r.t. \( q_2 \), we obtain:

\[
\frac{\partial f_1(q_1, q_2)}{\partial q_2} = -\frac{\gamma_4(\frac{\gamma_1 q_1}{\gamma_2 q_2} + 1)}{(\gamma_4 q_2 + 1)^2} - \frac{\lambda \gamma_1 \gamma_2 q_1 q_2^{\lambda - 1}}{(\gamma_4 q_2 + 1)(\gamma_2 q_2^{\lambda} + 1)^2} < 0. \tag{4.8}
\]

Therefore, \( f_1(q_1, q_2) \) is a decreasing function of \( q_2 \). The Lagrangian of (4.6) can be written as

\[
L(q_1, q_2, \mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6) = f_1(q_1, q_2) - \mu_1(\frac{q_1 \gamma_1}{1 + q_2^{\lambda} \gamma_2} - q_2 \gamma_3) - \mu_2(q_2 \gamma_4 - \frac{q_1 \gamma_1}{1 + q_2^{\lambda} \gamma_2}) - \mu_3(q_1 - q_s) - \mu_4(q_2 - q_r) - \mu_5(-q_1) - \mu_6(-q_2), \tag{4.9}
\]

where \( \mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6 \) are the corresponding Lagrange multipliers. We then obtain the following by equating the gradient to zero:

\[
\frac{\partial L}{\partial q_1} = \frac{\gamma_1}{(1 + q_2 \gamma_4)(1 + q_2^{\lambda} \gamma_2)} - \frac{\mu_1 \gamma_1}{1 + q_2^{\lambda} \gamma_2} + \frac{\mu_2 \gamma_1}{1 + q_2^{\lambda} \gamma_2} - \mu_3 + \mu_5 = 0
\]

\[
\frac{\partial L}{\partial q_2} = -\frac{\gamma_4(\frac{\gamma_1 q_1}{1 + \gamma_2 q_2} + 1)}{(\gamma_4 q_2 + 1)^2} - \frac{\lambda \gamma_1 \gamma_2 q_1 q_2^{\lambda - 1}}{(1 + q_2 \gamma_4)(1 + q_2^{\lambda} \gamma_2)^2} + \mu_1(\frac{\lambda \gamma_1 \gamma_2 q_1 q_2^{\lambda - 1}}{(1 + q_2^{\lambda} \gamma_2)^2} + \gamma_3) - \mu_2(\frac{\lambda \gamma_1 \gamma_2 q_1 q_2^{\lambda - 1}}{(1 + q_2^{\lambda} \gamma_2)^2} + \gamma_4) - \mu_4 + \mu_6 = 0
\]

and
\[ \mu_1(q_1\gamma_1 - q_2\gamma_3 - q_2^{\lambda + 1}\gamma_2\gamma_3) = 0, \]
\[ \mu_2(q_2\gamma_4 + q_2^{\lambda + 1}\gamma_2\gamma_4 - q_1\gamma_1) = 0, \]
\[ \mu_3(q_1 - q_s) = 0, \mu_4(q_2 - q_r), \mu_5(q_1) = 0, \text{ and } \mu_6(q_2) = 0. \]

Although not showing here for brevity of the presentation, by examining all possible cases and using (4.7) and (4.8), we obtain the only feasible solution, which is \((\mu_1 > 0, \mu_2 = 0, \mu_3 > 0, \mu_4 = 0, \mu_5 = 0, \mu_6 = 0)\). This leads to the following globally optimal solution of \(q_1\) and \(q_2\):

\[ q_1^* = q_s, q_2^* = \rho_1, \] (4.10)

where \(\rho_1\) is a positive root of

\[ q_2\gamma_3 + q_2^{\lambda + 1}\gamma_2\gamma_3 - q_s\gamma_1 = 0. \] (4.11)

Note that this root can be easily obtained by bisection method. Also, that since Condition 1 holds, it can be verified that \(\rho_1 \leq q_r\).

1) Condition 2 holds: This case corresponds to \(\gamma_e \leq \gamma_d \leq \gamma_r\). Let \(f_2(q_1, q_2) = \frac{1+\gamma_d}{1+\gamma_e}\). Solving (4.1) is equivalent to solving the following problem:

\[
\max_{q_1, q_2} f_2(q_1, q_2) \text{s.t.} \\
\begin{cases}
0 \leq q_1 \leq q_s \\
0 \leq q_2 \leq q_r \\
q_2^{\lambda + 1}\gamma_2\gamma_3 + q_2\gamma_3 \leq q_1\gamma_1
\end{cases}
\] (4.12)

It can be verified that both \(\frac{\partial f_2(q_1, q_2)}{\partial q_2}\) and \(\frac{\partial f_2(q_1, q_2)}{\partial q_1}\) are positive. Furthermore, \(q_2^{\lambda + 1}\gamma_2\gamma_3 + \frac{\partial f_2(q_1, q_2)}{\partial q_1}\)
$q_2 \gamma_3$ is an increasing function of $q_2$. To solve the optimization problem, let again assume that $\rho_1$ is the root of $q_2^{\lambda+1} \gamma_2 \gamma_3 + q_2 \gamma_3 - q_s \gamma_1 = 0$. Consider the following two sub-cases:

i) $\rho_1 \leq q_r$: This happens when $q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3 \geq q_s \gamma_1$. Therefore, the optimal solution is $q_1^* = q_s$ and $q_2^* = \rho_1$.

ii) $\rho_1 > q_r$: This happens when $q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3 < q_s \gamma_1$. It then follows that $q_2^* = q_r$.

For the optimal solution $q_1^*$, it turns out that it can take on any value in the range $\left[\frac{q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3}{\gamma_1}, q_s\right]$.

By combining the results of the problems in (4.6) and in (4.12), the optimal power allocation scheme under individual power constraints can finally be expressed as follows:

\[
\begin{align*}
q_1^* = q_s, q_2^* = \rho_1 & \text{ when } q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3 \geq q_s \gamma_1 \\
q_1^* = \left[\frac{q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3}{\gamma_1}, q_s\right], q_2^* = q_r & \text{ when } q_r^{\lambda+1} \gamma_2 \gamma_3 + q_r \gamma_3 < q_s \gamma_1
\end{align*}
\]

(4.13)

It can be seen from the final solution given in (4.13) that under individual power constraints, full-power at the relay is not always optimal.
4.2.2 Joint Power Constraints

As similar to the case under individual power constraints, let first assume Condition 1 holds, i.e., $\gamma_e \leq \gamma_r \leq \gamma_d$. The optimization problem in (4.2) becomes:

$$\max_{q_1, q_2} f_1(q_1, q_2) \text{ s.t.} \begin{cases} 
q_1 + q_2 \leq q_t \\
n_2^{\lambda+1} \gamma_2 \gamma_3 + q_2 \gamma_3 \\
\geq q_1 \gamma_1 \geq q_2^{\lambda+1} \gamma_2 \gamma_4 + q_2 \gamma_4
\end{cases} \quad (4.14)$$

The Lagrange function can then be expressed as:

$$\mathcal{L}(q_1, q_2, \mu_1, \mu_2, \mu_3) = f_1(q_1, q_2) - \mu_1(q_1 + q_2 - q_t) - \mu_2(q_1 \gamma_1 - q_2 \gamma_3 - q_2^{\lambda+1} \gamma_2 \gamma_3) - \mu_3(q_2 \gamma_4 + q_2^{\lambda+1} \gamma_2 \gamma_4 - q_1 \gamma_1) \quad (4.15)$$

with $\mu_1(q_1 + q_2 - q_t) = 0$, $\mu_2(q_1 \gamma_1 - q_2 \gamma_3 - q_2^{\lambda+1} \gamma_2 \gamma_3) = 0$, and $\mu_3(q_2 \gamma_4 + q_2^{\lambda+1} \gamma_2 \gamma_4 - q_1 \gamma_1) = 0$.

By taking the first derivative of the Lagrange function, we have:

$$\frac{\partial \mathcal{L}}{\partial q_1} = \gamma_1 (1 + q_2 \gamma_4) (1 + q_2^{\lambda} \gamma_2) = 0$$

$$- \mu_1 - \mu_2 \gamma_1 + \mu_3 \gamma_1 = 0$$

$$\frac{\partial \mathcal{L}}{\partial q_2} = -\gamma_4 \left( \frac{\gamma_1 q_1}{1 + q_2 \gamma_4} + 1 \right) - \frac{\lambda \gamma_1 \gamma_2 q_1 q_2^{\lambda - 1}}{(1 + q_2 \gamma_4) (1 + q_2^{\lambda} \gamma_2)^2}$$

$$- \mu_1 - \mu_2 (\gamma_3 (-(\lambda + 1) \gamma_2 q_2^{\lambda} - 1) + \mu_3 (\gamma_4 (-(\lambda + 1) \gamma_2 q_2^{\lambda} - 1) = 0$$

40
By checking these equations, we observe that the only feasible set is \((\mu_1 > 0, \mu_2 > 0, \mu_3 = 0)\), which results in the following solution:

\[ q^*_1 + q^*_2 = q_t, \quad (4.16) \]

\[ q^*_1 = \frac{q_2^*\gamma_3 + (q_2^*)^{\lambda+1}\gamma_2\gamma_3}{\gamma_1}. \quad (4.17) \]

Therefore, the optimal solution under this case is:

\[ q^*_2 = \hat{\rho}_1, q^*_1 = q_t - q^*_2, \quad (4.18) \]

where \(\hat{\rho}_1\) is the positive root of

\[ q_2^{\lambda+1}\gamma_2\gamma_3 + q_2(\gamma_1 + \gamma_3) - q_t\gamma_1 = 0. \quad (4.19) \]

Now, under the assumption that Condition 2 holds, we need to solve the following optimization problem:

\[
\max_{q_1,q_2} f_2(q_1,q_2) \text{ s.t. } \begin{cases} 
q_1 + q_2 \leq q_t \\
q_2^{\lambda+1}\gamma_2\gamma_3 + q_2\gamma_3 \leq q_1\gamma_1
\end{cases}
(4.20)
\]

Using a similar analysis, we obtain the same solution as in (4.18). Therefore, (4.18) is the final solution under the joint power constraint.

Before proceeding to the next subsection, we would like to note that under
the considered relaying protocol, the maximum secrecy rate achieved by the optimal power allocation \( q_1^* \) and \( q_2^* \) can be referred to as the secrecy capacity, denoted as \( C_s \), and this terminology will be used hereafter.

4.2.3 Asymptotic analysis and comparison to HD relaying

Given the solutions in (4.13) and (4.18), this subsection provides an asymptotic analysis to shed important light on the derived solutions in different high power regions. As we will show later, the analysis is helpful to make a direct comparison with traditional HD relaying. Note that for the HD system, the secrecy rates can be obtained by setting \( \gamma_2 = 0 \) in (3.4) and pre-multiplying \( R_s \) by a factor of 1/2. Also, for a fair comparison, the same average power constraints between HD and FD are used, i.e., \( q_{s,HD} = 2q_s \), \( q_r = 2q_r \), and \( q_{t,HD} = 2q_t \) for the HD system. In the following, we will examine different high power regions at the source and relay.

**Individual Constraints:** Under individual power constraints, we consider the following cases:

1) Large \( P_s/N_0 \): Assume that \( P_s \) is sufficiently higher than \( P_r \). When \( \lambda = 0 \), we have \( q_2^* = \frac{q_s \gamma_3}{\gamma_3(1+\beta)} \) if \( \frac{q_s \gamma_3}{\gamma_3(1+\beta)} \leq q_r \). The secrecy capacity \( C_s \) therefore approaches \( \log [(q_s/\alpha_4)] \). On the other hand, if \( \frac{q_s \gamma_3}{\gamma_3(1+\beta)} > q_r \), then \( q_2^* = q_r \), and the secrecy capacity goes to \( \log [(1+q_r \gamma_4)/1+(q_r \gamma_4)] \). When \( 0 < \lambda \leq 1 \), applying the method of dominant balance to the equation \( q_2 \gamma_2 \gamma_3 + q_2 \gamma_3 - \gamma_1 q_s = 0 \), we have \( O(q_2^{\lambda+1}) = O(\frac{P_s}{N_0}) \). As a result, \( q_{2,FD}^* = O(\frac{P_s}{N_0})^{\frac{1}{\lambda+1}} \) if \( O(\frac{P_s}{N_0})^{\frac{1}{\lambda+1}} \leq q_r \), and the secrecy capacity \( C_s \) approaches \( \log [(q_s \alpha_1 P_s)/((q_2 \gamma_4 + 1)(q_2 \gamma_2 + 1))] \). If \( O(\frac{P_s}{N_0})^{\frac{1}{\lambda+1}} > q_r \), \( q_{2,FD}^* = q_r \), and \( C_s \) goes
to $\log\left[\frac{1+q_1^\alpha r_3}{1+q_2 r_4}\right]$. It can be seen that in this case, full power allocation at both source and relay is asymptotically optimal for any $\lambda \in [0,1]$. Regarding the HD system, the optimal power allocation is $q^*_{1,HD} = 2q_s$. For $q^*_{2,HD}$, we have $q^*_{2,HD} = \frac{2q_1^\alpha r_3}{r_3}$ if $\frac{2q_1^\alpha r_3}{r_3} \leq 2q_r$. As a result, $C_{s,HD} \to \frac{1}{2} \log\left[\frac{q_3}{q_4}\right]$. If $\frac{2q_1^\alpha r_3}{r_3} > 2q_r$, we obtain $q^*_{2,HD} = 2q_r$, and $C_{s,HD} \to \frac{1}{2} \log\left[\frac{1+q_1^\alpha r_3}{1+2q_r r_4}\right]$. It is obvious the secrecy capacity of the FD system is twice as much as that of the HD system.

2) Large $P_r/N_0$: When $P_r$ is sufficiently higher than $P_s$. When $\lambda = 0$, we have $q^*_2 = \min\left(q_s, q_r\right) = \min\left(O\left(\frac{P_r}{N_0}\right)^{-1}, q_r\right) = O\left(\frac{P_r}{N_0}\right)^{-1}$. If $0 < \lambda \leq 1$, applying the method of dominant balance to equation (4.11), we have $O\left(\frac{P_r}{N_0}\right)^{\lambda+1} q_2^\lambda = O(1)$. As a result, $q^*_2 = \min\left(\rho_1, q_r\right) = \min\left(O\left(\frac{P_r}{N_0}\right)^{-1}, q_r\right) = O\left(\frac{P_r}{N_0}\right)^{-1}$. Therefore, in this case, the power used by the relay is $q^*_2 P_r = O(1)$. Furthermore, the secrecy capacity approaches $\log\left[\frac{q_3}{q_4}\right]$ regardless of $P_r$ for a given value of $\lambda$. It is clear that full-power allocation at the relay is suboptimal. Regarding the HD system, the optimal power allocation is $q^*_{1,HD} = 2q_s$ and $q^*_{2,HD} = \min(O(P_r/N_0)^{-1}, 2q_r) = O(P_r/N_0)^{-1}$ and the secrecy capacity approaches $1/2 \log\left[\frac{q_3}{q_4}\right]$.

3) Large $P_s/N_0$ and $P_r/N_0$: Finally, let consider the case that both $P_s/N_0$ and $P_r/N_0$ are sufficiently large. For simplicity, assume that they are equal to $P/N_0$. When $\lambda = 0$, we have $q^*_2 = \frac{q_1^\alpha r_3}{r_3(1+\beta)}$ and the secrecy capacity approaches $\log\left[\frac{q_3}{q_4}\right]$. When $0 < \lambda \leq 1$, applying the method of dominant balance again, we obtain $O\left(\frac{P_r}{N_0}\right)^{\lambda+1} q_2^\lambda = O\left(\frac{P_r}{N_0}\right)^{\lambda+1} q_2^\lambda = O\left(\frac{P_r}{N_0}\right)^{-1}$. It means that $O(q_2) = O\left(\frac{P_r}{N_0}\right)^{-1} q_2^\lambda$, or equivalently, $q^*_2 = O\left(\frac{P_r}{N_0}\right)^{\lambda+1}$. The secrecy capacity therefore approaches $\log\left[\frac{q_3}{q_4}\right]$ as well. Note that full power allocation at the relay, the secrecy rate goes to $\log\left[\frac{q_1^\alpha r_3 P^{-\lambda}}{q_r^{\lambda+1} r_4}\right]$ when $0 < \lambda \leq 1$. When
\( \lambda = 0 \), the secrecy rate goes to \( \log \frac{q_1\alpha_1}{(1+\beta)\alpha_3+\alpha_4} \). For HD mode, it is straightforward to see that \( q_{2,FD}^* = (2q_s\alpha_1/\alpha_3) \). The secrecy capacity \( C_{s,HD} \) approaches \( 1/2 \log(\alpha_3/\alpha_4) \), which is half of that of FD relaying.

**Joint Constraints:** Under the joint power constraint, assume that \( P_t/N_0 \) is sufficiently large. When \( \lambda = 0 \), we have \( q_2^* = q_t - q_1^* = O(1), \ q_{1,FD}^* = q_t - O(1) \) and the secrecy capacity \( C_{s,FD} \) approaches \( \log(\alpha_3/\alpha_4) \). When \( 0 < \lambda \leq 1 \), applying the method of dominant balance to (4.19), we have \( q_{2,FD}^{\lambda+1} = O((P_t/N_0)^{-\lambda}) \). Thus \( q_{2,FD}^* = O((P_t/N_0)^{\frac{1}{1+\lambda}}) \).

Note that for the HD mode, one obtains \( q_{2,HD}^* = q_t - q_1^* = O(1), \ q_{1,HD}^* = q_t - O(1) \) and the secrecy capacity \( C_{s,HD} \) approaches \( 1/2 \log(\alpha_3/\alpha_4) \). Therefore, HD relaying only achieves half of the secrecy capacity of FD relaying.

### 4.2.4 Illustrative examples

In this subsection, numerical results are provided to confirm the proposed solutions and the above asymptotic analysis for the case of slow fading. As before, in all simulations, it is assumed that \( \beta = 0.1, \alpha_1 = 1, \alpha_3 = 2, \alpha_4 = 1 \), and \( q_s = q_r = q_t = 1 \).

Besides the optimal allocations in (4.13) and (4.18), full power allocation scheme with \( q_1 = q_s \) and \( q_2 = q_r \) under the individual power constraints and the uniform power allocation with \( q_1 = q_2 = q_t/2 \) under the joint power constraint are also considered.

For comparison, the performance achieved by HD DF relaying is also provided. As an additional benchmark, we also compare the proposed FD DF relaying solution with that using DF AF relaying in [55]. For all FD AF systems, we assume that a perfect self-interference cancellation is achieved, e.g., \( \lambda = 0 \).
Individual Power Constraints: Under the individual power constraints, Fig. 4.1 first shows the secrecy rates versus $P_s/N_0$ for both optimal and full power allocation schemes with $\lambda$ being either 0, 0.5, or 1. Here, $P_r/N_0$ is fixed at 5dB. The secrecy rates obtained by the optimal HD DF scheme as well as the optimal FD AF system are also provided. Observe that the secrecy rates in FD systems asymptotically approach $\log\left[\frac{1+q_2\gamma_3}{1+q_2\gamma_4}\right] = 0.8745$ for both power allocation schemes, which confirms our earlier analysis. It can also be observed that the FD system outperforms the HD
system. Specifically,  
$$C_s \rightarrow \log\left[\frac{1+\frac{\gamma_3}{q}}{1+rac{\gamma_4}{q}}\right] = 0.8745 > C_{s,HD} \rightarrow 1/2 \log\left[\frac{1+2\gamma_3}{1+2\gamma_4}\right] = 0.4664.$$  
Furthermore, it can be seen that FD DF relaying is significantly better than DF AF relaying.

![Figure 4.2: Secrecy rate versus $P_r/N_0$ for different systems.](image)

Fig. 4.2 plot the secrecy rate versus $P_r/N_0$ for the same systems when $P_s/N_0 = 5$dB. Observe from Fig. 4.2 that the secrecy rate achieved by FD DF relaying with the optimal power allocation becomes insensitive to $P_r$ when $P_r$ increases. With full-power allocation, the secrecy rate of the FD DF system goes to zero. Similar to the
previous result, FD DF relaying with optimal power allocation outperforms both HD DF and FD AF relaying.

![Secrecy rate versus $P_s/N_0 = P_r/N_0 = P/N_0$.](image)

Figure 4.3: Secrecy rate versus $P_s/N_0 = P_r/N_0 = P/N_0$.

Finally, under the individual power constraints, Fig. 4.3 presents the secrecy rates achieved by different systems when $P_s/N_0 = P_r/N_0 = P/N_0$. It can be noticed from Fig. 4.3 that in FD mode with full power allocation, the secrecy rates are also below zero. Furthermore, when the optimal power allocation scheme in the FD mode is used, the secrecy rates asymptotically approach $\log_\frac{\alpha_4}{\alpha_4}$. As similar to the previous
results, FD DF relaying provides much better performance than those achieved in
HD DF and FD AF systems.

**Joint Power Constraints:**

![Figure 4.4: Secrecy rate versus $P_t/N_0(\lambda = [0, 0.5, 1])$.](image)

Under the case of joint power constraint, Fig. 4.4 plots the secrecy rate versus
$P_t/N_0$ for the FD systems using the optimal power allocation derived in (4.18) and
the uniform power allocation scheme. The rate achieved by the optimal HD system
under the joint power constraint is also provided for comparison. As expected, the
secrecy capacity of the FD system approaches $\log(\alpha_3/\alpha_4) \to 1$. The uniform power
allocation performs poorly and it does not provide any secrecy. Compared to the HD mode, the FD system is far more superior. It is interesting to see that in this case, while FD DF relaying is much better than DF AF relaying in the low power region, the two systems achieve a similar performance when $P_t/N_0$ increases.

4.3 Optimal Power Allocation Schemes in Ergodic Fading

For ergodic fading channels, given the closed-form expressions of the secrecy rate in (3.18), the power allocation $q_1$ and $q_2$ at the source and relay, respectively, can be further optimized to improve the secrecy rate. Since this rate involves exponential integrals, obtaining a rigorous solution of such an optimization problem is challenging, and it is a subject for future research. However, as an alternative, we can perform an exhaustive search over the two variables $q_1$ and $q_2$ under either the individual power constraint $q_1 \leq q_s$ and $q_2 \leq q_r$, or under the joint power constraint $q_1 + q_2 \leq q_t$, to find the optimal values $q_1^*$ and $q_2^*$.
Figure 4.5: Ergodic secrecy rate versus $P/N_0$ for different power allocation schemes under the individual power constraints.

Under the individual power constraints, via extensive numerical results, we have observed that $q_1^* = q_1$, while $q_2^* < q_2$. It means that full-power allocation at the relay is not an optimal solution to maximize the ergodic secrecy rate. As an illustrative example, Fig. 4.5 shows the ergodic secrecy rates versus SNR for two different power allocation schemes under DF relaying: the full power allocation scheme and the optimal allocation scheme obtained by brute-force search. All channel parameters are the same as the ones we considered earlier in Chapter 3. Furthermore,
it is assumed that $P_s/N_0 = P_r/N_0 = P/N_0$. It can be observed from Fig. 4.5 that full power allocation scheme is suboptimal and the secrecy rates approach 0 when $0 < \lambda \leq 1$. When $\lambda = 0$, the rate is positive. However, it is much smaller that the secrecy capacity obtained using the optimal power allocation scheme.

![Figure 4.6: Ergodic secrecy rate versus $P_t/N_0$ for different power allocation schemes under joint power constraints.](image)

Similar results can also be obtained under the joint power constraint. In particular, Fig. 4.6 plot the secrecy rate versus $P_t/N_0$ when the optimal power allocation
scheme and the uniform power allocation scheme are used. Apparently, a significant gain can be achieved with the optimal solution.
CHAPTER V

CONCLUSIONS

This thesis has investigated the secrecy rates and corresponding optimal power allocation schemes for FD DF relay wiretap channels under both individual and joint power constraints between the source and the relay. The channels under consideration include slowly varying fading channels and ergodic fast fading channels.

The first part of the thesis established the secrecy rates in closed-form. In particular, in slow fading environments, conditions for which a positive rate is achieved have been provided. For the case of ergodic fading where the channel state information is available at the receivers but not the transmitters, closed-form solutions of the ergodic secrecy rates in terms of the well-known exponential integral functions were derived by calculating the expectation of an exponentially distributed random variable. Numerical results show that the closed-form solutions can be used to accurately calculate the ergodic secrecy rates.

In the second part of the thesis, the optimal power allocation scheme to achieve the secrecy capacity was addressed over the considered relay channels. For slow fading channels, the optimal power allocation schemes under both individual and joint power constraints in closed-form were established. By further exploiting these solutions via an asymptotic analysis, important insights on the derived solutions
have been provided to demonstrate the advantage of FD relaying over HD relaying. These results showed that FD DF relaying with suitable power allocation schemes can significantly outperform FD AF relaying.

While successfully addressing an important research topic under the framework of PHY security in wireless relay networks, the research work in this thesis has only scratched a small tip of an iceberg. In the following, several interesting future research problems in PHY security shall be described.

- As a logical extension of this work, a rigorous optimization problem can be formulated to address the optimal power allocation for the same relay channels but in ergodic fading environments. To this end, care must be taken to deal with exponential integrals in the objective function.

- This thesis focused only on a single-relay channel. A more general and also a more practical situation is where multiple relays can be deployed in different locations to support the transmission from the source to the destination. It is certainly interesting to investigate a suitable scheme sharing power among multiple nodes for further security enhancement.

- While PHY security techniques are promising, the security of communication networks has traditionally relied on cryptographic schemes in upper layers, such as the application layer. As such, there has been a call (see e.g., [34]) for the combination of cryptographic schemes and PHY security techniques to guarantee the security of the whole system. Some efforts [83, 84, 85, 34, 86] have
been made to combine cryptographic techniques and PHY security techniques, but many challenges remains unanswered. Therefore, in the long term, it is important to investigate the combination of cryptography and PHY security techniques for a comprehensive security treatment in wireless relay networks.


