OPTIMAL POWER ALLOCATION AND SECRECY CAPACITY OF THE
FULL-DUPELEX AMPLIFY-AND-FORWARD WIRE-TAP RELAY CHANNEL
UNDER RESIDUAL SELF-INTERFERENCE

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

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

Cuong Dang
December, 2015
OPTIMAL POWER ALLOCATION AND SECRECY CAPACITY OF THE
FULL-DUPEX AMPLIFY-AND-FORWARD WIRE-TAP RELAY CHANNEL
UNDER RESIDUAL SELF-INTERFERENCE

Cuong Dang

Thesis

Approved:  
Advisor  
Dr. Nghi H. Tran

Interim Department Chair  
Dr. Joan Carletta

Committee Member  
Dr. Shivakumar Sastry

Interim Dean of the College  
Dr. Mario Garzia

Committee Member  
Dr. Forrest Sheng Bao

Dean of the Graduate School  
Dr. Chand Midha

Date
ABSTRACT

Due to the broadcast nature of wireless channels, security and privacy are of utmost concern for future wireless technologies. However, securely transferring confidential information over a wireless network in the presence of adversaries still remains a challenging task. As one of the most important aspects of wireless communication security, Physical Layer (PHY) security has started gaining research attention in the past few years. In wireless PHY security, the breakthrough idea is to exploit the characteristics of wireless channels such as fading or noise to transmit a message from a source to an intended destination while trying to keep this message confidential from passive eavesdroppers. Unlike cryptographic methods, no computational constraints are placed on the eavesdroppers. Benefiting from information-theoretic studies in cooperative relaying communications, relaying strategies have also recently received considerable attention in the context of PHY security over wireless networks. Specifically, 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. This thesis studies a wireless relay network in which a source node wants to communicate securely to a destination node in the presence of an eavesdropper under the aid of an amplify-and-forward (AF) relay operating in full-duplex (FD)
mode for further security enhancement. The focus is on the optimal power allocation (PA) schemes to maximize the secrecy rate in different wireless environments.

The first part of the thesis considers the problem of optimizing the PA at the source node and the relay node to achieve the secrecy capacity for slowly varying fading channels. Under this consideration, the optimal PA problem is shown to be quasi-concave. As such, the globally optimal power allocation solution exists, and it is unique. A simple bisection method for root finding can then be used to obtain the optimal PA scheme. To further provide an insight on the solutions, the method of dominant balance is applied to analyze the secrecy capacity and PA schemes in different high power regions. It is then demonstrated that full PA at the relay is only needed when the power at the relay is sufficiently small compared to the power at the source. Comparison with half-duplex (HD) relaying also shows that FD relaying can achieve a significantly higher secrecy capacity.

In the second part of the thesis, the study is extended to ergodic fading channels where the channel gains are assumed to be available at the receivers but not the transmitters. Due to the presence of fading, analysis on secrecy rate are normally very challenging because of the lack of an insightful method to calculate secrecy rate in closed-form. To this end, a novel method to calculate the expectation of an exponentially distributed random variable is first proposed. By exploiting this calculation, the ergodic secrecy rate of the system can be then established in closed-form. The optimal PA scheme and the corresponding secrecy capacity are then studied. Numerical results also reveal the superiority of FD over HD relaying in ergodic fading.
ACKNOWLEDGMENTS

This thesis would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them.

Foremost, I am deeply indebted to my supervisor, Dr. Nghi Tran, for supporting and guiding me during my studies at the University of Akron. His stimulating motivation and valuable ideas in accordance with his way of doing research tremendously inspired me. Helping me achieve the best with my M.Sc. studies is always of his interest. Without his constant support, encouragement and availability, this thesis would not have been finished.

My sincere appreciation and gratitude also go to my colleague Dr. Leonardo J. Rodríguez for his guidance and many useful research discussions. His advices and suggestions have helped me on many aspects of my research. Also, I am very honored to have Dr. Forrest Bao and Prof. Shiva Sastry as members of the thesis examination committee. Their constructive comments and suggestions are very valuable for me.

It has also been a pleasure to work with Duc-Anh, Hung, Tuyen, Mohhamad, and Lubna, my labmates and friends in the Coding and Communications Research Group at the University of Akron. Without discussions and encouragement from them, my study would not be so enjoyable.
Last but not least, I am very grateful for the unconditional love and support from my parents and sister. This thesis is a dedication to them.
TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>LIST OF FIGURES</th>
<th>ix</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF ACRONYMS</td>
<td>x</td>
</tr>
<tr>
<td>CHAPTER</td>
<td></td>
</tr>
<tr>
<td>I. INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 Motivation</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Contributions</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Thesis Outline</td>
<td>6</td>
</tr>
<tr>
<td>II. BACKGROUND</td>
<td>8</td>
</tr>
<tr>
<td>2.1 Physical Layer Security</td>
<td>8</td>
</tr>
<tr>
<td>2.2 Wireless channels</td>
<td>15</td>
</tr>
<tr>
<td>2.3 Amplify-and-Forward Relay Comm.</td>
<td>17</td>
</tr>
<tr>
<td>2.4 Full-Duplex Comm.</td>
<td>19</td>
</tr>
<tr>
<td>III. OPTIMAL POWER ALLOC. AND SEC.</td>
<td>22</td>
</tr>
<tr>
<td>OF AF FD RELAY WIRETAP CHANNELS</td>
<td></td>
</tr>
<tr>
<td>3.1 System Model</td>
<td>23</td>
</tr>
<tr>
<td>3.2 Optimal Power Alloc. and Sec.</td>
<td>26</td>
</tr>
<tr>
<td>3.3 Asymptotic Analysis and Comp.</td>
<td>33</td>
</tr>
</tbody>
</table>
### LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Wiretap channel.</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>FD Relay protocols.</td>
<td>20</td>
</tr>
<tr>
<td>3.1</td>
<td>FD AF wire-tap channel.</td>
<td>23</td>
</tr>
<tr>
<td>3.2</td>
<td>Secrecy Rate vs. $P_s/N_0$ for static channels ($\lambda = [0, 0.5, 1], P_r/N_0 = 5dB$).</td>
<td>39</td>
</tr>
<tr>
<td>3.3</td>
<td>Secrecy Rate vs. $P_r/N_0$ for static channels ($\lambda = [0, 0.5, 1], P_s/N_0 = 5dB$).</td>
<td>40</td>
</tr>
<tr>
<td>3.4</td>
<td>Secrecy Rate vs. $P/N_0$ for static channels ($\lambda = [0, 0.5, 1]$).</td>
<td>41</td>
</tr>
<tr>
<td>3.5</td>
<td>Secrecy Rate vs. $P_t/N_0$ for static channels ($\lambda = [0, 0.5, 1]$).</td>
<td>42</td>
</tr>
<tr>
<td>4.1</td>
<td>Secrecy rates: Closed-form expression vs Monte Carlo simulations.</td>
<td>53</td>
</tr>
<tr>
<td>4.2</td>
<td>Secrecy Rate vs. $P_s/N_0$ for fading channels ($\lambda = [0, 0.5, 1], P_r/N_0 = 5dB$).</td>
<td>55</td>
</tr>
<tr>
<td>4.3</td>
<td>Secrecy Rate vs. $P_r/N_0$ for fading channels ($\lambda = [0, 0.5, 1], P_s/N_0 = 5dB$).</td>
<td>56</td>
</tr>
<tr>
<td>4.4</td>
<td>Secrecy Rate vs. $P/N_0$ for fading channels ($\lambda = [0, 0.5, 1]$).</td>
<td>57</td>
</tr>
<tr>
<td>4.5</td>
<td>Secrecy Rate vs. $P_t/N_0$ for fading channels ($\lambda = [0, 0.5, 1]$).</td>
<td>58</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>AF</td>
<td>Amplify-and-Forward</td>
<td></td>
</tr>
<tr>
<td>CDI</td>
<td>Channel Distribution Information</td>
<td></td>
</tr>
<tr>
<td>CF</td>
<td>Compress-and-Forward</td>
<td></td>
</tr>
<tr>
<td>CI</td>
<td>Channel Inversion</td>
<td></td>
</tr>
<tr>
<td>CSI</td>
<td>Channel State Information</td>
<td></td>
</tr>
<tr>
<td>DF</td>
<td>Decode-and-Forward</td>
<td></td>
</tr>
<tr>
<td>DH</td>
<td>dual-hop</td>
<td></td>
</tr>
<tr>
<td>FD</td>
<td>Full-Duplex</td>
<td></td>
</tr>
<tr>
<td>HD</td>
<td>Half-Duplex</td>
<td></td>
</tr>
<tr>
<td>i.i.d</td>
<td>independent identically distributed</td>
<td></td>
</tr>
<tr>
<td>PA</td>
<td>Power Allocation</td>
<td></td>
</tr>
<tr>
<td>PDF</td>
<td>Probability Density Function</td>
<td></td>
</tr>
<tr>
<td>PMF</td>
<td>Probability Mass Function</td>
<td></td>
</tr>
<tr>
<td>PHY</td>
<td>Physical layer</td>
<td></td>
</tr>
<tr>
<td>SNR</td>
<td>Signal-to-noise ratio</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER I

INTRODUCTION

1.1 Motivation

Wireless communications has grown explosively and played an important role in daily activities of human beings. While the popularity of wireless transmission allows ubiquitous access to communication networks, the broadcast nature of wireless channels makes wireless transmission very susceptible to eavesdropping. Given the increased dependency on network services, the interception and illegal uses of data might result in a tremendous cost. As a result, there is an increasing need for secure communication solutions in wireless environments.

The problems of information security have been investigated during the last few decades with many state-of-art techniques being proposed to address four fundamental security problems: confidentiality, integrity, authentication, and availability. Out of these four factors, confidentiality, which is defined as protecting the information from disclosure to unauthorized parties, is considered as one of the the most important aspects. While information such as bank account statements, personal information, credit card numbers, government documents is critically important, especially in today’s world, protecting such information from unauthorized parties is a major part of information security. Although confidentiality was originally considered
as high-layer problem to be solved using cryptographic methods such as encryption, PHY security metrics based on information theory such as secrecy rate and secrecy capacity [1, 2] have been gaining increasing research attention. In PHY security, the source takes advantage of the channel characteristics to transmit a message to the intended receiver while trying to keep a perfect secrecy against passive eavesdroppers. One advantage of this approach over traditional cryptographic methods is that no assumption about computational limitation of eavesdroppers is made [3].

In another context, relaying techniques in which a relay node assists a source node to communicate to a destination node have received considerable attention from both industry and academia. In particular, the deployment of relays has been shown to increase the range and reliability of wireless networks in a cost-effective manner (see for example [4, 5] and reference within). In general, relaying strategies can be categorized as decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF). In AF relaying, the relay simply needs to transmit a scaled version of the received signal. As such, the AF technique is transparent to the modulation/coding used by the source nodes, and requires lower implementation complexity [6]. AF relaying then can be further classified according to the availability of channel knowledge. Specifically, when the relay has only channel distribution information (CDI) of the incoming link, the fixed-gain CDI amplification coefficient [7] can be used to maintain an average power constraint at the relay. On the other hand, when the relay has instantaneous knowledge of the incoming link, the received signal can be normalized with such knowledge to the desired power level similar to channel in-
version (CI) techniques [8, 9]. The latter variable-gain method is therefore referred to as the CI coefficient.

Although relaying strategies in wireless networks have been well investigated, most previous studies on relaying are carried out under the assumption that the relay operates in HD mode. This is because the transmitted signal power in wireless systems is usually in order of magnitudes larger than the received signal power, thus, makes rendering simultaneous transmission and reception over the same frequency band infeasible. Such HD constraint results in an inefficient use of resources as a dedicated bandwidth or time slot is required for relay transmissions. Given the limitation of HD transmission, considerable research effort has been devoted to FD transmission in which sending and receiving can be performed simultaneously. Although FD wireless operation was considered impractical in the past, recent prototypes have demonstrated the feasibility of FD through novel combinations of antenna, analog, and digital cancellations (e.g., [10, 11, 12, 13, 14]). As one important aspect of FD transmission, FD relaying has since started to gain significant interest in the literature [15, 16, 17, 18, 19, 20, 21, 22]. However, the advent of FD relaying brings an inevitable trade-off. Although FD relaying allows better utilization of the spectrum, it still suffers from residual self-interference as the power leakage between the transmitter and receiver at the relay cannot be completely mitigated in practice. However, a number of research works have shown that with proper control of the residual self-interference, FD relaying can provide significant advantages over HD in terms of achievable rate [16, 17, 18, 21] and error performance [19, 20, 22].
Recently, relaying has also been shown to be a very attractive solution to enhance the secrecy rate of wireless networks [23, 24, 25, 26, 27, 28, 29, 30, 31]. For instance, relays can be used to apply distributed beamforming and steer the information vector away from the eavesdropper and in the direction of the intended destination (e.g., [26, 27, 30, 31]). Alternatively, relays can also be used as jammers to degrade the signal-to-noise ratio (SNR) at the eavesdropper without degrading the SNR at the destination (e.g., [23, 24, 25, 26, 27, 28, 29]). All of the above strategies have assumed that the relay operates in HD mode. While the potential benefits of FD relaying to enhance the secrecy are undoubted, analyzing and optimizing the secrecy rate of wireless FD relay networks still remains a challenging task as compared to the HD counterpart. Besides secrecy constraints, the residual self-interference of FD operation must be taken into account. In addition, the presence of fading and various relaying strategies makes it difficult to calculate the secrecy rate in an effective manner. To our knowledge, such calculation usually relies on lengthy Monte Carlo simulations. All of these challenges make the related optimization problems much more complicated.

Motivated by above observations, this thesis investigates the secrecy rate and respective optimal PA schemes to achieve secrecy capacity of a AF relay wire-tap channel in which the relay operates in FD mode. The residual self-interference of FD relaying shall be explicitly taken into account.
1.2 Contributions

The first part of the thesis studies the AF relay wire-tap channel which a source node wants to communicate securely to a destination node in the presence of an eavesdropper under the aid of an AF relay operating in FD in slowly varying wireless fading environments. The focus is on the optimal PA schemes between the source and the relay to maximize the secrecy rate in different wireless environments. Both individual (i.e., per-node) and joint (i.e., sum) power constraints at the source and relay are considered. At first, the related power optimization problems are shown to be quasi-concave. As such, the globally optimal solution exists and it is unique. Due to the non-linearity of the derivative, a closed-form expression for the optimal solution is not always feasible. For such cases, we apply a simple bisection method for root finding and obtain an approximate solution for the optimal PA scheme. To further provide some insight on the solutions, the method of dominant balance is applied to analyze the capacity and PAs in different high power regions. It is then demonstrated that full PA at the relay is only needed when the power at the relay is sufficiently small compared to the power at the source. In other high power regions, full PA becomes suboptimal compared to the proposed optimal PA. Also, comparison with HD relaying also reveals that FD relaying can achieve a significantly higher secrecy capacity than HD relaying.

In the second part of the thesis, the considered problem is extended to the case of ergodic fading channels where the time-varying channel gains are assumed to
be available at the receivers but not the transmitters. To this end, a novel method to
calculate the expectation of an exponentially distributed random variable using the
exponential integral function is first proposed. By exploiting this calculation, we then
establish the ergodic secrecy rate of the considered AF relay system in closed-form.
The bisection method can then be applied to find the optimal PA scheme. Numerical
results also reveal the superiority of FD over HD relaying in ergodic fading. Similar
to the static channels, it is also demonstrated that full PA at the relay is only optimal
when the power at the relay is sufficiently small compared to the power at the source.

1.3 Thesis Outline

The remainder of the thesis is organized as follows. Chapter 2 presents some basic
background that is related to the problems investigated in this thesis. The chapter
starts with some fundamental information-theoretic concepts such as Entropy,
Conditional Entropy and Mutual Information. Based on these concepts, a brief in-
troduction about the wiretap channel and related concepts in PHY security such as
secrecy rate and secrecy capacity is then presented. Also, in this chapter, the topics
of wireless channels, relay communications, and FD communication are provided.

Chapter 3 studies the optimal PA and the secrecy rate for the considered AF
system in slow fading environment. The optimal PA for the system is first derived.
Then the asymptotic analyses for different PA schemes and corresponding secrecy
rate in different high power regions are provided to gain an insight about the optimal
solutions. Simulation results are finally provided to confirm the optimality of the proposed solution and the accuracy of analytical results.

Chapter 4 extends the investigation to the fast fading environment. A closed-form formula for ergodic secrecy capacity is first provided. The optimal PA schemes and the corresponding secrecy capacity are then addressed. Simulations are also carried out to verify the correctness of the derived formula and the advantage of the proposed PA solutions.

Finally, Chapter 5 concludes the thesis and outlines some important future research directions.
CHAPTER II
BACKGROUND

This chapter provides the background material required for the development of subsequent chapters in this thesis. An introduction on PHY security and its fundamental concepts is first provided. Then wireless channels and its characteristics are discussed in details. An overview on AF relay communications is also presented. Finally, the chapter is concluded with some background information on FD transmission.

2.1 Physical Layer Security

Along with the traditional cryptography security, PHY security has recently emerged as an important technique to improve wireless communication security. Different from cryptographic approaches, which assumes computational constrains of adversaries, PHY security achieves secrecy by exploiting the PHY properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels. By this motivation, to understand the notion of PHY Security, one should first be familiar with fundamental information theoretic concepts such as mutual information or capacity. This section first provides some basic concepts in information theory from [32] such as entropy, conditional entropy, and mutual infor-
mation. Given these notions, secrecy rate and secrecy capacity, two primary concepts of PHY Security are then presented under the model of wiretap channel.

2.1.1 Entropy, Conditional Entropy and Mutual Information

**Entropy:** The concept of entropy starts with the definition of self-information. Let $X$ be a discrete Random Variable (RV) with probability mass function (PMF) $P(X = x)$, denoted as $p(x)$. Self-information of an event $X = x$ is defined as:

$$I(x) = \log \frac{1}{p(x)} = -\log p(x)$$

(2.1)

where log is based 2 $^1$ and the entropy is measured in bits. It can be seen that high probability events convey less information than low-probability ones.

Simply speaking, entropy is an average of self-information, or it can be understood as a measure of the uncertainty of a RV. The entropy $H(X)$ of a discrete RV $X$ with PMF $p(x)$ is given by

$$H(X) = -\sum_x p(x) \log p(x).$$

(2.2)

While many processes and phenomena in real life involve continuous RV, the concept of entropy for discrete RV does not apply for continuous RV and we need a new definition for this idea. Unlike discrete RVs that are characterized by their PMF, when $X$ is continuous, the distribution of $X$ will be represented by probability distribution

$^1$Throughout this thesis, log refers to the logarithm to base 2
The entropy in this case is called *differential entropy* and calculated as:

\[
h(x) = - \int f_x(x) \log f_x(x) \, dx.
\]  

(2.3)

**Conditional Entropy:** When two RVs are considered, the conditional entropy is the entropy of one RV given the knowledge of another. It is calculated as the expected value of the entropies of the conditional distribution, averaged over the conditioning random variable. For example, let \((X; Y)\) be a pair of discrete RVs with a joint PMF \(p(x; y) = Pr(X = x; Y = y)\) and a conditional probability \(p(y|x) = Pr(Y = y|X = x)\), the conditional entropy \(H(Y|X)\) can be calculated as:

\[
H(Y|X) = \sum_{x \in X} p(x) H(Y|X = x)
\]

\[
= - \sum_{x \in X} p(x) \sum_{y \in Y} p(y|x) \log p(y|x)
\]

(2.4)

\[
= - \sum_{x \in X} \sum_{y \in Y} p(x, y) \log p(y|x)
\]

When \(X\) and \(Y\) are both continuous with a join PDF \(f_{x,y}(x, y)\) and a conditional PDF \(f_{y|x}(y|x)\), the conditional entropy \(h(X|Y)\) is calculated as:

\[
h(y|x) = - \int_X \int_Y f_{X,Y}(x, y) \log f_{Y|X}(y|x) \, dy \, dx
\]

\[
= - \int_X \int_Y f_X(x) f_{Y|X}(y|x) \log f_{Y|X}(y|x) \, dy \, dx
\]

(2.5)
**Mutual Information**: Mutual information is the reduction of the uncertainty of a RV, let say $X$, due to the knowledge of another RV, for example $Y$. Mutual information $I(X, Y)$ between $X$ and $Y$ is given as:

$$I(X, Y) = H(Y) - H(Y|X) = H(X) - H(X|Y)$$  \hspace{1cm} (2.6)

In case $X$ and $Y$ are discrete RVs, from (2.2) and (2.4), the mutual information $I(X, Y)$ can be expressed as:

$$I(X, Y) = H(Y) - H(Y|X) = \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{p(y|x)}{p(x)}$$  \hspace{1cm} (2.7)

When $X$ and $Y$ are continuous, the mutual information will be written from (2.3) and (2.5) as:

$$I(x, y) = h(y) - h(y|x) = \int_X \int_Y f_X(x)f_{Y|X}(y|x)\log \frac{f_{Y|X}(y|x)}{f_Y(y)}dydx$$  \hspace{1cm} (2.8)

Because of its direct connection to the capacity of communication systems, which is defined as maximum rate at which we can send information over the channel and recover the information at the output with a vanishingly low probability of error, mutual information is considered as the heart of information theory. Similarly, as can be seen in the following, the concept of mutual information is also utilized to define secrecy rate and secrecy capacity, which are fundamental concepts of PHY Security.
2.1.2 Wiretap Channel

The quantified definitions of PHY security are formulated under the classical model of wiretap channel. The wiretap channel model was initially introduced by Wyner in [1] and later refined by Csiszr and Korner for broadcast channels [33]. Figure 2.1 illustrates the first model with the following components:

- The *source* sequence $S^K = \{S_k\}_{1}^{\infty}$, where $S_k$ are independent, identically distributed (i.i.d) RV with values from the finite set $S$. It is assumed that the source distribution, and thus, the entropy of $\{S_k\}$ is known. Let the entropy $H(S_k) = H_S$.

- The *main channel* with finite input alphabet $X$, finite output alphabet $Y$, transition probability $Q_M(y|x), x \in X, y \in Y$ and the capacity $C_M$. The channel is assumed to be discrete memoryless, so the transition probability for $N$ vectors is given as: $Q_M^{(N)}(y|x) = \prod_{n=1}^{N} Q_M(y_n|x_n)$.

- The *wire-tap channel* is also a discrete memoryless channel with input alphabet $Y$, finite output alphabet $Z$, and transition probability $Q_W(z|y), y \in Y, z \in Z$.

Figure 2.1: Wiretap channel.
The cascade channel $Q_{MW}$ of the main channel and the wire-tap channel $Q_{W}$ is another memoryless channel with capacity $C_{MW}$ and transition probability given by

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

It is stated in [1] that with given channels $Q_{M}$ and $Q_{W}$, an encoder and decoder are defined as following:

- **An encoder** $(K, N)$ takes an input $S^{K} = (S_{1}, ..., S_{K})$ and produce an output $X^{N}$ with transition probability $q_{E}(x|s), s \in S^{K}, x \in X^{N}$. Therefore, $X^{N}$ becomes input of the main channel. Assume the output of the main channel $Q^{(N)}_{M}$ and cascade channel $Q^{(N)}_{MW}$ to be $Y^{N}$ and $Z^{N}$ respectively. The equivocation of the source at the output of the wire-tap channel is defined as

$$\Delta \triangleq \frac{1}{K} H(S^{K}|Z^{N}).$$

It can be seen that $\Delta$ represents the wire-tapper’s confusion about the source information. Thus, from the system designer’s point of view, it is desirable to make $\Delta$ as large as possible.

- **The decoder** is a mapping $f_{D} : Y^{N} \rightarrow S^{K}$. Assume that $f_{D}(Y) = \tilde{S} = (\tilde{S}_{1}, ..., \tilde{S}_{K})$, then the error-rate corresponding to the encoder and decoder is

$$P_{e} = \frac{1}{K} \sum_{k=1}^{N} Pr(S_{k} \neq \tilde{S}_{k}).$$
The above encoder-decoder is denoted as \((K, N, \Delta, P_e)\). A pair \((R, d)\) \((R, d > 0)\) is said to be \textit{achievable} if, for all \(\varepsilon > 0\), there exists an encoder-decoder \((N, K, \Delta, P_e)\) for which the following conditions are satisfied:

\[
\frac{(H_SK)}{N} \geq R - \varepsilon, \Delta \geq d - \varepsilon, P_e \leq \varepsilon.
\]

Let \(\Omega(R)\) be the set of \(p_x\) such that \(I(X;Y) \geq R\). For \(0 \leq R \leq C_M\), define

\[
\Gamma(R) \overset{\Delta}{=} \sup_{p_x \in \Omega(R)} I(X;Y|Z).
\]

(2.10)

Note that for any distribution \(p_x\) on \(X\), the corresponding \(X, Y, Z\) forms a Markov chain, so that the definition of mutual information yields:

\[
I(X;Y|Z) = H(X|Z) - H(X|Y, Z)
\]

\[
= H(X|Z) - H(X|Y) = I(X|Y) - I(X|Z)
\]

(2.11)

Thus, (2.10) can be written as:

\[
\Gamma(R) \overset{\Delta}{=} \sup_{p_x \in \Omega(R)} I(X;Y|Z) = \sup_{p_x \in \Omega(R)} [I(X|Y) - I(X|Z)].
\]

(2.12)

It is proven in Theorem 3 of [1] that if \(C_M > C_{MW}\), there exist a unique solution \(C_S\) of \(C_S = \Gamma(C_S)\) in which \(C_S\) satisfies 0 < \(C_M - C_{MW}\) \(\leq \Gamma(C_M) \leq C_S \leq C_M\).

In other words, for a degraded discrete-memoryless channel, a non-zero rate can be
achieved in approximately perfect secrecy. Such a rate is defined as the secrecy rate and calculated as the subtraction of the rate between the sender and the receiver and the rate between the sender and the eavesdropper. The maximum secrecy rate is called the secrecy capacity.

2.2 Wireless channels

Wireless communication makes use of electromagnetic wave propagation through atmosphere to transmit information from a source to a destination. Thus, not only the wireless channel suffers from many kinds of impairments such as noise, interference, physical obstacles but also these impairments change over time in unpredictable ways due to user movement and environment dynamic. The variation in received signal power may be caused by the propagation of signal over distance. In this scenario, signals may suffer from effects such as path loss and shadowing. Path loss is caused by attenuation of the power radiated by the transmitter as well as by the effects of the propagation channel. Shadowing is caused by obstacles between the transmitter and receiver that attenuate signal power through absorption, reflection, scattering, and diffraction. The variations in received power caused by path loss and shadowing occur over large distance, and thus, are called large-scale fading. Another kind of fading happens due to the constructive and destructive addition of multipath signal components and is referred to as small-scale fading. The name comes from the fact that these variations occur over very short distances, on the order of the signal wave-
length. In general, the transmission of signal experiences the combined effects of both large-scale and small-scale fading.

For this thesis, the effect of small-scale fading is taken into account. The channel is assumed to be narrow-band which is also referred to as frequency non-selective or flat fading channel. The channels can be considered as narrow-band when the delay spread, which is the time delay between the arrival of the first signal component and the last received signal component, is relatively small compared to the inverse of the signal bandwidth. In such conditions, the discrete-time baseband-equivalent model of the received signal at time $t$ is expressed as:

$$y_t = h_t x_t + n_t,$$

in which $x_t$ is the transmitted signal, $h_t$ is the channel gains, and $n_t$ is the noise sample.

This thesis considered thermal noise, a prevailing noise in reality. Thermal noise is caused by the random movement of electron in electrical devices, and thus, by central limit theorem, modeled as a zero-mean circularly symmetric complex Gaussian random variable with covariance $N_0$, which can be denoted as $n_t \sim \mathcal{CN}(0, N_0)$. Regarding the channels gain $h_t$, its form depends on the dynamic feature of the surrounding environment or how fast the channel is changing, which can be characterized by coherence time. If the coherence time is larger than the signal pulse duration or within a given time range, the channel does not change much, it is called slow fading.
channel or static channel. Otherwise, if the coherence bandwidth smaller than the signal pulse duration or the channel dynamically change during a considered time range, the channel is fast fading channel.

In this thesis, the first part will consider the system under slow fading environment in which the channel gains can be assumed as constants. In the second part, fast fading channels are addressed. In this environment, it is common to assume that the number of paths is large, hence the channel gain can also be modeled as a zero-mean circularly symmetric complex Gaussian random variables, i.e., \( h_t \sim \mathcal{CN}(0, \sigma) \), where \( \sigma \) is the channel variance. This channel gain has Rayleigh distributed magnitude and uniformly distributed phase in \([0, 2\pi]\), and it is called Rayleigh fading channel.

2.3 Amplify-and-Forward Relay Communication

Relay communications were first proposed in [34, 35] and have received considerable research attention since due to the advantages in increasing range and reliability in wireless networks. In general, relaying strategies can be categorized as decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF), depending on the signal processing techniques at the relay. While DF and CF relaying requires high decoding complexity, AF relaying is simple to implement because the relay simply needs to transmit a scaled version of the received signal. As such, the AF technique is transparent to the modulation/coding used by the source nodes, and requires lower implementation complexity. Beside the advantage of low complexity,
the fact that the intermediate nodes in AF relaying only transmit an amplified version of the transmitted signal without decoding makes it less vulnerable to security thread. In particular, even if intruders have control over a relay node, it is still difficult for them to access the source information.

Regarding the knowledge of the relay nodes about channel state information (CSI) of links between different nodes, relay communications can be considered in three possible cases:

- **Full CSI**: Relay nodes have complete instantaneous knowledge of all the links in the system, include the relay - eavesdropper links. This can be achieved by using feedback channel from a receiver to a sender.

- **Channel Distribution Information (CDI)**: Relay nodes only know the distribution of the corresponding source - relay links.

- **Source-Relay CSI**: Relay nodes have CSI of only the source - relay nodes.

Depending on what type of CSI is available, different techniques can be applied at the relay to amplify the noisy version of the received signal using a suitable amplification coefficient. For example, by assuming that a relay can only obtain the CDI of the source-relay channel, the received signal at the relay is scaled by a constant-gain coefficient before being transmitted to the destination. When the relay has an instantaneous knowledge of the source-relay channel, the Channel Inversion (CI)
technique can be used to amplify the received signal at a desired power level [8]. In this thesis, the first part focuses on the case of static channels in which full CSI is available at all nodes. In the second part, it assumed that all channels CSI is only available at receivers side. Note that because the relay has instantaneous knowledge of the incoming link in both cases, CI technique can be applied.

2.4 Full-Duplex Communication

In modern communication system, most of devices (e.g., base stations, relays, or mobiles) functions as both transmitters and receivers. Conventionally, these terminals operate in HD mode in which they transmit and receive either at different times, or over different frequency bands. Recently, great research effort has been devoted to enable FD capability on those terminals because of its many fold advantage. An obvious benefit is that transmitting and receiving simultaneously over the same frequency band can double the spectral efficiency. Moreover, FD concepts can also be utilized at higher layer. For example, from the access-layer point of view, terminals with the capability of reliably receiving an incoming frame while simultaneously transmitting an outgoing frame could detect collisions or receive instantaneous feedback from other terminals while transmitting in a contention-based network. Furthermore, FD techniques has been shown to be an effective solution to tackle many problems in cognitive radio. In particular, FD radios equipped users in a cognitive radio system can simultaneously sense and access the vacant spectrum, and thus, significantly improve sensing performances and meanwhile increase data transmission efficiency.
Despite its potential benefits, until now, FD communications have not been widely used. The key challenge in implementing a FD wireless communication on a node is the large self-interference from its own transmissions in comparison to the signal received from the distant transmitting antenna. The large self-interference spans most of the dynamic range of the analog-to-digital converter in the receiving chain, which in turn dramatically increases the quantization noise for the signal of interest. However, recent experimental results for indoor scenarios have shown that it is possible to implement self-interference cancellation mechanisms that can sufficiently attenuate the self-interference and thus, demonstrated that FD systems are a feasible option for future indoor wireless communications [10, 11, 12, 13, 14].

As the FD transmission has been becoming practical, FD relaying has started gaining significant research attention. Depending whether the direct source-destination
link is used for transmission, FD relaying can be categorized as dual-hop (DH) or cooperative relaying. As depicted in the Fig. 2.2, in cooperative FD relaying, the source transmits to the relay and the destination, while the relay simultaneously receives the signal from the source and transmits to the destination. On the other hand, in DH relaying, the link between the source and the destination is not used. An obvious advantage of DH FD relay compared to HD relay is that by utilizing FD transmission at the relay, the source is allowed to transmit continuously. A trade-off is that the self-interference from FD operation at the relay may degrade the rate between the source and the destination. Because of its simplicity and potential benefits for security enhancement compared to cooperative relaying, the model of FD DH relay is considered in this thesis.
CHAPTER III

OPTIMAL POWER ALLOCATION AND SECRECY CAPACITY OF AF FD RELAY WIRETAP CHANNELS IN SLOW FADING

In this chapter, a relay wiretap channel in which a source node wants to communicate securely to a destination node in the presence of an eavesdropper under the aid of an AF relay operating in FD mode is studied in a slowly varying fading environment. To take into account the practical aspects of FD operation, the empirical residual self-interference model proposed in [12] is adopted for the FD operation at the relay. This practical model has been shown to fit well to a variety of FD prototypes [12, 13].

Similar to previous works, the residual self-interference is commonly assumed to be Gaussian in which the variance is modeled based on the experimental results. In particular, depending on cancellation techniques, this variance can be modelled as a function of the transmitting power.

As discussed earlier, while the potential benefits of FD relaying to enhance the secrecy are undoubted, analyzing and optimizing the secrecy capacity of wireless FD relay networks still remains a challenging task as compared to the HD counterpart. It is because besides secrecy constraints, the above residual self-interference of FD operation makes the PA problems much more complicated, even for the case of static channels.
This chapter is therefore concerned with the development of an optimal PA scheme between the source and the relay to further improve the secrecy rate of the considered AF channel. Toward this end, it is first demonstrated that the related optimization problem is quasi-concave and a simple bisection method can be used to obtain the globally optimal solution. Both analytical and numerical analysis are then provided to show the superiority of the proposed solutions and the advantage of FD relaying over HD relaying for security enhancement.

3.1 System Model

As shown in Fig. 3.1, the considered FD system consists of four nodes: a HD source node $S$, a FD relay node $R$, a HD destination node $D$, and a HD eavesdropper node $E$. Applying the FD DH relaying operation, $R$ receives a signal from $S$ and at the same time, forwards it to $D$. Transmission protocol is presented in detailed as follows.
At a given frame $i$, $S$ continuously transmits the signal $x_i$ to the relay $R$. The signal received at $R$ then can be written as

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

where $P_s$ is a positive constant related to the power transmitted at $S$ that shall be explained shortly; $h_1^{(i)}$ is the $S$-$R$ channel gain at frame $i$; $n_{r,i}$ is the zero-mean circularly Gaussian noise at $R$, denoted as $n_{r,i} \sim \mathcal{CN}(0, N_r)$; and $v_i$ is the residual self-interference term due to FD operation. While receiving $x_i$, $R$ amplifies and forwards the signal received at $i-1$ using an amplification coefficient $b$. Thus, the signal transmitted by $R$ at the frame $i$ is given by $t_i = br_{i-1}$. Then, the signal received at $D$ and overheard at $E$ can be written respectively as

$$y_{d,i} = \sqrt{P_r}h_3^{(i)}t_i + n_{d,i} = \sqrt{P_sP_r}h_3^{(i)}h_1^{(i-1)}bx_{i-1} + \sqrt{P_r}h_3^{(i)}b(n_{r,i-1} + v_{i-1}) + n_{d,i},$$

$$y_{e,i} = \sqrt{P_r}h_4^{(i)}t_i + n_{e,i} = \sqrt{P_sP_r}h_4^{(i)}h_1^{(i-1)}bx_{i-1} + \sqrt{P_r}h_4^{(i)}b(n_{r,i-1} + v_{i-1}) + n_{e,i},$$

(3.1)

where $P_r$ is a positive constant related to the power transmitted at $R$ that shall be explained shortly; $h_3^{(i)}$ and $h_4^{(i)}$ are respectively the $R$-$D$ and $R$-$E$ channel gains at the frame $i$; and $n_{d,i} \sim \mathcal{CN}(0, N_d)$ and $n_{e,i} \sim \mathcal{CN}(0, N_e)$ are the noise samples at $D$ and $E$. Without loss of generality, it is assumed that the noise variances at all nodes are the same, i.e., $N_r = N_e = N_d = N_0$. 

24
Let $\mathbb{E}[|x_i|^2] = q_1$ so that $S$ spends an average power of $q_1 P_s$. To keep a power constraint of $q_2 P_r$ at $R$ and to prevent oscillation [36], $\mathbb{E}[|t_i|^2] = \mathbb{E}[|br_{i-1}|^2] = q_2$. We also assume that the relay has instantaneous knowledge of the $S - R$ link, so the CI technique can be used and the variable gain amplification coefficient is given as

$$b = \frac{q_2}{\sqrt{|h_1^{(i-1)}|^2 q_1 P_s + N_0 + V}},$$

where $V = \mathbb{E}[|v_i|^2]$. Here, similar to previous works, we assume that the residual self-interference is Gaussian as $v_i \sim \mathcal{CN}(0, V)$. In addition, the variance of the residual self-interference is modeled based on the experimental results in [12] as $V = \beta(q_2 P_r)^\lambda$, where $\beta$ and $\lambda$ ($0 \leq \lambda \leq 1$) are constants that depend on the cancellation technique [12, 13]. For the static channels, the channel gains $h_i = [h_1^{(i)}, h_3^{(i)}, h_4^{(i)}] = [h_1, h_3, h_4] = \mathbf{h}$ can be considered as constants. Similar to [23, 25, 26, 27, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50], the constant channel gains are assumed to be available at all nodes. This assumption holds true for many practical systems where the eavesdropper is a lower-level user belonging to the legitimate network and therefore has restricted access to confidential information [27]. Assuming Gaussian codebooks at $S$, the achievable rate at $D$ and $E$ can now be written (in b/s/Hz) from (3.1) as

$$I_d|\mathbf{h} = \log \left(1 + \frac{q_1 q_2 \gamma_1 \gamma_3}{q_1 \gamma_1 + q_2 \gamma_3 + q_2^\lambda \gamma_2 + q_2^{1+\lambda} \gamma_2 \gamma_3 + 1}\right),$$

$$I_e|\mathbf{h} = \log \left(1 + \frac{q_1 q_2 \gamma_1 \gamma_4}{q_1 \gamma_1 + q_2 \gamma_4 + q_2^\lambda \gamma_2 + q_2^{1+\lambda} \gamma_2 \gamma_4 + 1}\right),$$

(3.2)
where \( \gamma_1 = |h_1|^2 P_s/N_0, \gamma_2 = \beta P^\lambda_r/N_0, \gamma_3 = |h_3|^2 P_r/N_0, \) and \( \gamma_4 = |h_4|^2 P_r/N_0. \) The achievable secrecy rate is then given by

\[
R_s = [I_d|h - I_e|h]^+
\]  

(3.3)

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

In this chapter, the main objective is to obtain the optimal PA \( q = [q_1^*, q_2^*] \) on \( S \) and \( R \) to maximize the secrecy rate in (3.3) under individual and global power constraints. For the individual constraints scenario, we assume that \( q_1 \leq q_s \) and \( q_2 \leq q_r \) so that the power constraints at \( S \) and \( R \) are \( q_s P_s \) and \( q_r P_r \). In the global constraints scenario, we assume \( P_s = P_r = P_t \) and \( q_1 + q_2 \leq q_t \). The global power is then constrained to \( q_t P_t \).

3.2 Optimal Power Allocation and Secrecy Capacity

In this section, we first show that the optimization problem is quasi-concave and obtain the optimal PA solution using a simple bisection method. To further obtain an insight on the solutions, an asymptotic analysis in different high power regions is then provided. Comparisons to HD relaying are also made to evaluate the efficiency of our FD solutions.

3.2.1 Optimal Power Allocation

For convenience, let \( \alpha_j = |h_j|^2 \). It means that \( \gamma_1 = \alpha_1 P_s/N_0, \gamma_3 = \alpha_3 P_r/N_0, \) and \( \gamma_4 = \alpha_4 P_r/N_0 \), which are constant. From (3.3), the secrecy capacity for the cases
of individual and joint power constrains can be obtained by solving the following optimization problem:

\[
C_s = \max_{q_1,q_2 \geq 0} [I_d|h - I_e|h]^+, \text{ s.t. } \begin{cases} q_1 \leq q_s, q_2 \leq q_r \quad \text{(indiv.)} \\ q_1 + q_2 \leq q_t \quad \text{(joint).} \end{cases} \tag{3.4}
\]

First, it can be verified that the secrecy rate in (3.3) is positive when \( I_d|h > I_e|h \).

Equivalently, from (3.2) we have:

\[
\left( \frac{q_1 q_2 \gamma_1 \gamma_3}{q_1 \gamma_1 + q_2 \gamma_4 + q_2 \gamma_2 + q_2^{1+\lambda} \gamma_2 \gamma_4 + 1} \right) - 1 = \frac{(\gamma_3 - \gamma_4)(q_1 \gamma_1 + q_2 \gamma_2 + 1)}{\gamma_4 (q_2 \gamma_3 + q_2^{1+\lambda} \gamma_2 \gamma_4 + 1)} > 0.
\]

This condition is simply equivalent to \( \gamma_3 > \gamma_4 \), or \( \alpha_3 > \alpha_4 \).

Given that a strictly positive secrecy rate is achievable if and only if \( \alpha_3 > \alpha_4 \), we now proceed further to find the solutions for (3.4) under individual and global power constraints, respectively. Since \( \log(\cdot) \) is a monotonically increasing function, the problem in (3.4) is equivalent to the following optimization problem:

\[
\max_{q_1 \geq 0, q_2 \geq 0} g(q_1,q_2) = \left( \frac{1}{1 + \frac{q_1 q_2 \gamma_1 \gamma_3}{q_1 \gamma_1 + q_2 \gamma_4 + q_2^{1+\lambda} \gamma_2 \gamma_4 + 1}} \right) \tag{3.5}
\]

with the constrains \( q_1 \leq q_s, q_2 \leq q_r, \) and \( q_1 + q_2 \leq q_t \) respectively for individual and joint power cases and where \( g(q_1,q_2) \) can be simplified to

\[
g(q_1,q_2) = \frac{(q_2 \gamma_3 + 1)(q_1 \gamma_1 + q_2 \gamma_4 + q_2^{1+\lambda} \gamma_2 \gamma_4 + 1)}{(q_2 \gamma_4 + 1)(q_1 \gamma_1 + q_2 \gamma_3 + q_2^{1+\lambda} \gamma_2 \gamma_3 + 1)}. \tag{3.6}
\]
In the following, we first address the individual constraint scenario before looking into the global constraint one. In both cases, it is assumed that $\alpha_3 > \alpha_4$ so that a positive secrecy rate is achieved.

1) Individual Constraints

In the individual scenario, it can be seen that

$$\frac{\partial g(q_1, q_2)}{\partial q_1} = \frac{\gamma_1 q_2 (\gamma_2 q_2^\lambda + 1)(\gamma_3 q_2 + 1)(\gamma_3 - \gamma_4)}{\gamma_4 q_2 + 1)(q_1 \gamma_1 + q_2 \gamma_3 + q_2^\lambda \gamma_2 + q_2^{1+\lambda} \gamma_2 \gamma_3 + 1)^2} > 0,$$

so $g(q_1, q_2)$ is an increasing function of $q_1$. Thus, the optimal power at $S$ is $q_1^* = q_s$.

The optimal power at $R$ then can be found by taking the derivatives of $g(q_s, q_2)$ along $q_2$:

$$\frac{\partial g(q_s, q_2)}{\partial q_2} = \frac{q_s \gamma_1 (\gamma_3 - \gamma_4) P_1(q_2, \lambda)}{(q_2 \gamma_4 + 1)^2(\gamma_3 \gamma_2 q_2^{\lambda+1} + \gamma_2 q_2^\lambda + \gamma_3 q_2 + \gamma_1 q_s + 1)^2}$$

where

$$P_1(q_2, \lambda) = A q_2^{\lambda+2} + B q_2^{\lambda+1} + C q_2^\lambda + D q_2^2 + E \quad (3.7)$$

with $A = -(\lambda + 1) \gamma_2 \gamma_3 \gamma_4 < 0$, $B = -\lambda \gamma_2 (\gamma_3 + \gamma_4) < 0$, $C = (1 - \lambda) \gamma_2 > 0$, $D = -\gamma_3 \gamma_4 < 0$, and $E = \gamma_1 q_s + 1 > 0$.

Consider the following cases according to the value of $\lambda$.

(i) When $\lambda = 0$: We have

$$P_1(q_2, 0) = (A + D) q_2^2 + C + E$$
with $A + D = -\gamma_2 \gamma_3 \gamma_4 - \gamma_3 \gamma_4 \leq 0$, $C + E = \gamma_2 + \gamma_1 q_s + 1 > 0$. If $A + D = 0$ (or $\alpha_4 = 0$), then $P_1(q_2, 0) = C + E > 0$. Therefore, $\partial g(q_s, q_2)/\partial q_2 > 0$, and $g(q_s, q_2)$ is increasing regarding $q_2$, so the optimal value is $q_2^* = q_r$. Otherwise, the quadratic polynomial $P_1(q_2, 0)$ has two roots

$$x_{1,2} = \pm \sqrt{-\frac{C + E}{A + D} + \frac{1}{\gamma_2 \gamma_3 \gamma_4 + \gamma_3 \gamma_4}} (x_1 > x_2)$$

in which $x_2$ is negative and cannot be a solution. Consider the following subcases:

- If $x_1 < q_r$: $P_1(q_2, 0) \geq 0$ when $0 \leq q_2 \leq x_1$ and $P_1(q_2, 0) < 0$ when $x_1 < q_2 \leq q_r$. Therefore, $g(q_s, q_2)$ is a quasi-concave function with the optimal value $q_2^* = x_1$.

- If $x_1 \geq q_r$: $P_1(q_2, 0) \geq 0$ when $0 \leq q_2 \leq q_r$, so $g(q_s, q_2)$ is increasing and the optimal value is $q_2^* = q_r$.

**(ii)** When $0 < \lambda \leq 1$: Calculate the first derivative of $P(q_2, \lambda)$, we have

$$\frac{\partial P_1(q_2, \lambda)}{\partial q_2} = q_2 \left[ (\lambda + 2)Aq_2^\lambda + (\lambda + 1)Bq_2^{\lambda-1} + \lambda Cq_2^{\lambda-2} + 2D \right].$$

It can be seen that $\partial P_1(q_2, \lambda)/\partial q_2$ can be either positive or negative. Therefore, for a better evaluation of $P_1(q_2, \lambda)$, we consider its second derivative as follows:

$$\frac{\partial^2 P_1(q_2, \lambda)}{\partial q_2^2} = (\lambda + 2)(\lambda + 1)Aq_2^\lambda + \lambda(\lambda + 1)Bq_2^{\lambda-1} + \lambda(\lambda - 1)Cq_2^{\lambda-2} + 2D.$$
Observe that \( \partial P_1^2(q_2, \lambda)/\partial q_2 < 0 \) when \( 0 \leq q_2 \leq q_r \) and \( 0 < \lambda \leq 1 \), so \( \partial P_1(q_2, \lambda)/\partial q_2 \) is decreasing within \([0, q_r]\). Then because \( \partial P_1(0, \lambda)/\partial q_2 = 0 \), it can be concluded that \( \partial P_1(q_2, \lambda)/\partial q_2 \leq 0 \) or \( P_1(q_2, \lambda) \) is decreasing when \( 0 \leq q_2 \leq q_r \). Furthermore, given that \( P_1(0, \lambda) > 0 \) and \( \lim_{q_2 \to +\infty} P_1(q_2, \lambda) = -\infty \), \( P_1(q_2, \lambda) \) has a single strictly positive root (if feasible). Assume this root is \( \rho \), consider the following subcases:

- If \( \rho < q_r \): \( P_1(q_2, \lambda) > 0 \) when \( 0 \leq q_2 < \rho \) and \( P_1(q_2, \lambda) \leq 0 \) when \( \rho \leq q_2 \leq q_r \), so \( g(q_1, q_2) \) is again a quasi-concave function with the optimal value \( q_2^* = \rho \).

- If \( \rho \geq q_r \): \( P_1(q_2, \lambda) \geq 0 \) when \( 0 \leq q_2 \leq q_r \), so \( g(q_1, q_2) \) is increasing in this interval and the optimal value \( q_2^* = q_r \).

Given that \( P_1(q_2, \lambda) \) is non-linear when \( 0 < \lambda < 1 \) and cubic when \( \lambda = 1 \), a closed-form solution for \( \rho \) cannot be obtained. A root finding method such as bisection method is thus needed to calculate this root. From the sub-cases, the optimal PA is given as:

\[
q_1^* = q_s, \\
q_2^* = \begin{cases} 
q_r & (\lambda = 0, \alpha_4 = 0) \\
\min(\sqrt{\frac{(\gamma_2 + \gamma_1 q_s + 1)}{(\gamma_2 \gamma_4 + \gamma_3 \gamma_4)}}, q_r), & (\lambda = 0, \alpha_4 \neq 0) \\
\min(\rho, q_r), & (0 < \lambda \leq 1)
\end{cases}
\] (3.8)
2) Joint Power Constraints

In the joint constraints scenario, we need to find the optimal PA under the constraint \( q_1 + q_2 \leq q_t \). Since \( \partial g(q_1, q_2) / \partial q_1 > 0 \), the optimal power is achieved when \( q_1 + q_2 = q_t \). Taking the derivative along the line \( q_1 + q_2 = q_t \), we have

\[
\frac{\partial g(q_1, q_t - q_1)}{\partial q_1} = \frac{\gamma_1 (\gamma_3 - \gamma_4) P_2(q_1, \lambda)}{[(q_t - q_1)\gamma_4 + 1]^2[q_1 \gamma_1 + (q_t - q_1)\gamma_3 + (q_t - q_1)\lambda \gamma_2 + (q_t - q_1)^{1+\lambda} \gamma_2 \gamma_3 + 1]^2}
\]

where

\[
P_2(q_1, \lambda) = \gamma_2 (q_t - q_1)\lambda \left\{ \gamma_3 \gamma_4 (q_t - q_1)^3 + [(\lambda + 1)q_1 \gamma_3 \gamma_4 + \gamma_3 + \gamma_4] (q_t - q_1)^2 + \lambda (\gamma_3 + \gamma_4) q_1 + 1 \right\} (q_t - q_1) + \gamma_3 \gamma_4 (q_t - q_1)^3 + (\gamma_3 \gamma_4 q_1 + \gamma_3 + \gamma_4)(q_t - q_1)^2 + (q_t - q_1) - q_1 (q_1 \gamma_1 + 1)
\]

Now, consider the following cases:

(i) When \( \lambda = 0 \): We have \( P_2(q_1, 0) = A_0 q_1^2 + B_0 q_1 + C_0 \) with

\[
A_0 = [(\gamma_2 + 1)\gamma_3 \gamma_4 q_t + (\gamma_2 + 1)(\gamma_3 + \gamma_4) - \gamma_1], B_0 = -2(\gamma_2 + 1) [\gamma_3 \gamma_4 q_t^2 + (\gamma_3 + \gamma_4) q_t + 1], C_0 = (\gamma_2 + 1) q_t [\gamma_3 \gamma_4 q_t^2 + (\gamma_3 + \gamma_4) q_t + 1].
\]

If \( A_0 = 0 \), then \( g(q_1, q_2) \) is quasi-concave with the optimal value \( q_1^* = -C_0 / B_0 = q_t / 2 \). Otherwise, observe that \( P_2(0, 0) > 0 \) and \( P_2(q_t, 0) = -q_1 (q_1 \gamma_1 + 1) < 0 \), so \( P_2(q_1, 0) \) has two roots of which one is in the range \([0, q_t]\). Assume the two roots are \( z_1 \) and \( z_2 \) and \( z_1 < z_2 \). We consider the following sub-cases:
• If $A_0 > 0$: $z_1$ is in $[0, q_t]$, so $P_2(q_1, 0) \geq 0$ when $0 \leq q_1 \leq z_1$ and $P_2(q_1, 0) < 0$ when $z_1 < q_1 \leq q_t$, so $g(q_1, q_2)$ is quasi-concave with the optimal value $q_1^* = z_1$.

• If $A_0 < 0$: Similarly, $g(q_1, q_2)$ is quasi-concave with the optimal value $q_1^* = z_2$

(ii) When $0 < \lambda \leq 1$: Observe that $P_2(0, \lambda) > 0$, and $P_2(q_t, \lambda) < 0$ so $P_2(q_1, \lambda) = 0$ has roots within $[0, q_t]$. Moreover, we know from the individual constraint case that $g(q_1, q_2)$ is quasi-concave with respect to both $q_1$ and $q_2$ (i.e., it is increasing in $q_1$ and quasi-concave in $q_2$). Thus, it must also be quasi-concave along any convex subset of the feasible region. This includes the line $q_1 + q_2 = q_t$, i.e., the global constraint scenario. Therefore, $P_2(q_1, \lambda) = 0$ has exactly one root within $[0, q_t]$. Assume this root is $z$. Then, $\partial g(q_1, q_t - q_1) / \partial q_1 \geq 0$ when $0 \leq q_1 \leq z$ and $\partial g(q_1, q_t - q_1) / \partial q_1 < 0$ when $z < q_1 < q_t$. Thus, $g(q_1, q_2)$ is quasi-concave with the optimal value $q_1^* = z$.

Similar to the case of individual constraints, it is not possible to find a closed-form expression for $z$ and bisection is needed to find the solution. From these sub-cases, the optimal PA is given by

$$q_1^* = \begin{cases} 
  q_t/2, & (\lambda = 0, A_0 = 0) \\
  z_1, & (\lambda = 0, A_0 > 0) \\
  z_2, & (\lambda = 0, A_0 < 0) \\
  z, & (0 < \lambda \leq 1), 
\end{cases}$$

$$q_2^* = q_t - q_1^*.$$  

(3.9)
3.3 Asymptotic Analysis and Comparison to Half-Duplex Relaying

In the previous section, the optimal PA schemes that achieve the secrecy capacity under individual and joint power constraints were derived. In the following, an asymptotic analysis is provided to shed further light on the derived solutions in different high power regions. Comparisons to HD relaying are also made to evaluate the efficiency of our solutions. Note that the optimal PA for the same system where the relay operates in HD mode was derived in [51]. Note that for the HD system, the secrecy rates can be obtained by setting $\gamma_2 = 0$ in (3.2) and pre-multiplying $R_s$ in (3.3) by a factor of $1/2$. Also, for a fair comparison, the same average power constraints between HD and FD are used, i.e., $q_s,_{HD} = 2q_s,_{FD}$, $q_r,_{HD} = 2q_r,_{FD}$, and $q_t,_{HD} = 2q_t,_{FD}$ for the HD system. In the following, different high power regions under individual and joint power constraints are considered.

3.3.1 Individual Constraints

1) Large $P_s/N_0$

First, consider the individual constraint scenario where $P_s$ are sufficiently higher than $P_r$. When $\lambda = 0$,

$$q^*,_{2,FD} = \min \left( \sqrt{\frac{\gamma_2 + \gamma_1 q_s + 1}{\gamma_2 \gamma_3 \gamma_4 + \gamma_3 \gamma_4}} , q_r \right) = \min \left( O \left( \left( \frac{P_s}{N_0} \right)^{1/2} \right), q_r \right) = q_r.$$
When $0 < \lambda \leq 1$, applying the method of dominant balance [52] to the equation $P_1(q_2, \lambda) = 0$, we have $O(q_2^{\lambda+2}) = O(P_s/N_0)$, so

$$q_{2,FD}^* = \min(\rho, q_r) = \min(O((P_s/N_0)^{1/(\lambda+2)}), q_r) = q_r.$$ 

Therefore, when the power at the source node outweighs the power at relay node, full PA at both source and relay is asymptotically optimal for every $\lambda \in [0, 1]$. In this case, the secrecy capacity approaches a constant as $C_{s,FD} \to \log[(q_r \gamma_3 + 1)/(q_r \gamma_4 + 1)]$.

Regarding HD system in high source power region, the optimal PA is $q_{1,HD}^* = 2q_s$,

$$q_{2,FD}^* = \min\left(\sqrt{\frac{2\gamma q_s + 1}{\gamma_3 \gamma_4}}, 2q_r\right) = \min\left(O\left(\left(\frac{P_s}{N_0}\right)^{1/2}\right), 2q_r\right) = 2q_r$$

and the upper bound of secrecy capacity is $C_{s,HD} \to 1/2 \log[(2q_r \gamma_3 + 1)/(2q_r \gamma_4 + 1)]$.

By comparing FD and HD modes, it is straightforward to show that

$$\log \frac{\gamma_3 q_r + 1}{\gamma_4 q_r + 1} > \frac{1}{2} \log \frac{2\gamma_3 q_r + 1}{2\gamma_4 q_r + 1} \quad \text{when} \quad \gamma_3 > \gamma_4,$$

As such, in this case, FD relaying is more helpful than HD relaying in terms of secrecy capacity.
2) Large $P_r/N_0$

Now consider the individual constraint case where $P_r$ are sufficiently higher than $P_s$.

When $\lambda = 0$, 

$$q_{2,FD}^* = \min \left( \frac{\gamma_2 + \gamma_1 q_s + 1}{\gamma_2 \gamma_3 \gamma_4 + \gamma_3 \gamma_4}, q_r \right) = \min \left( \sqrt{\frac{O(1)}{O\left(\left(\frac{P_r}{N_0}\right)^2\right)}}, q_r \right)$$

$$= \min \left( O\left(\left(\frac{P_r}{N_0}\right)^{-1}\right), q_r \right) = O\left(\left(\frac{P_r}{N_0}\right)^{-1}\right).$$

When $0 < \lambda \leq 1$, applying the method of dominant balance to the equation $P_1(q_2, \lambda) = 0$, we have $O((P_r/N_0)^{\lambda+2})q_2^{\lambda+2} = O(1)$, so $q_{2,FD}^* = \min(\rho, q_r) = \min(O((P_r/N_0)^{-1}), q_r) = O((P_r/N_0)^{-1})$. Therefore, when the power at the source is sufficiently small compared to relay, the power transmitted by the relay $q_{2,FD}^* P_r = O(1)$ eventually saturates to a constant to control the self-interference. The secrecy capacity also approaches a constant for a given value of $\lambda$. However, given the dependence of the secrecy capacity on $\lambda$, it is not straightforward to make a direct comparison between FD and HD relaying. As we demonstrate shortly by simulation results, this secrecy capacity is indeed higher than that achieved by using HD relaying for various $\lambda$. 

35
3) Large $P_s/N_0$ and $P_r/N_0$

Consider the individual constrained system where $P_s/N_0 = P_r/N_0 = P/N_0$ is large.

When $\lambda = 0$,

$$q_{2,FD}^* = \min \left( \sqrt{\frac{\gamma_2 + \gamma_1 q_s + 1}{\gamma_2 \gamma_3 \gamma_4 + \gamma_3 \gamma_4}}, q_r \right) = \min \left( O \left( \left( \frac{P}{N_0} \right)^{-1/2} \right), q_r \right) = O \left( \left( \frac{P}{N_0} \right)^{-1/2} \right).$$

When $0 < \lambda \leq 1$, applying the method of dominant balance to the equation $P_1(q_2, \lambda) = 0$, we have $O((P/N_0)^{\lambda+2}) q_2^{\lambda+2} = O(P/N_0)$, so $O(q_2) = O((P/N_0)^{-\frac{\lambda+1}{\lambda+2}})$. Then,

$$q_{2,FD}^* = \min(\rho, q_r) = \min(O((P/N_0)^{-\frac{\lambda+1}{\lambda+2}}), q_r) = O((P/N_0)^{-\frac{\lambda+1}{\lambda+2}}).$$

In both cases, the secrecy capacity $C_{s,FD} \rightarrow \log(\alpha_3/\alpha_4)$ approaches a constant. Now for HD mode, in this high power region,

$$q_{2,HD}^* = \min \left( \sqrt{\frac{\gamma_1 q_s + 1}{\gamma_3 \gamma_4}}, 2q_r \right) = \min \left( O \left( \left( \frac{P}{N_0} \right)^{-1/2} \right), 2q_r \right) = O \left( \left( \frac{P}{N_0} \right)^{-1/2} \right).$$

and the secrecy capacity $C_{s,FD} \rightarrow 1/2 \log(\alpha_3/\alpha_4)$ also approaches a constant. However, this upper bound value of secrecy capacity in HD mode is only as half as it is achieved in FD mode, or, in other words, in case the power at both source and relay become sufficiently large, FD mode enhances the secrecy capacity as twice as HD mode does.
3.3.2 Joint Constraint

Finally, consider the global constraint case where $P_s/N_0 = P_r/N_0 = P_t/N_0$ is large. When $\lambda = 0$,

$$q^*_{2,FD} = q_t - q^*_1 = q_t - \frac{-B_0 \pm \sqrt{B_0^2 - 4A_0C_0}}{2A_0} = O\left(\left(\frac{P_t}{N_0}\right)^{-1/2}\right)$$

and $q^*_{1,FD} = q_t - O\left((P_t/N_0)^{-1/2}\right)$. When $0 < \lambda \leq 1$, using again the method of dominant balance into the equation $P_2(q_t - q_2, \lambda) = 0$, we have $O((P_t/N_0)^{\lambda+2})q_2^{\lambda+2} = O(P_t/N_0)$, so $q^*_{2,FD} = O((P_t/N_0)^{-\frac{\lambda+1}{2}})$ and $q^*_{1,FD} = q_t - O((P_t/N_0)^{-\frac{\lambda+1}{2}})$. In both cases, the power at the relay scales as $q^*_{2,FD}P_t = O(P_t^{1/2+\lambda})$ and the secrecy capacity $C_{s,FD} \rightarrow \log(\alpha_3/\alpha_4)$ approaches a constant. For the HD mode, the similar results are obtain: $q^*_{2,HD} = O((P_t/N_0)^{-1/2})$ and $q^*_{1,HD} = q_t - O((P_t/N_0)^{-1/2})$. Furthermore, like the previous case of individual constraints when both $P_s$ and $P_r$ are large, in this case, HD mode only achieves half of the secrecy capacity as FD mode does because $C_{s,HD} \rightarrow 1/2 \log[\alpha_3/\alpha_4]$.

From the above analysis, the following important observations can be drawn about the optimal PA in FD mode for the considered system under static channels. First, full PA is optimal only when the power at the relay is sufficiently small compare to the power at the source. When the power at the relay is considerably larger than the power at the source, the power transmitted at the relay always saturates to a constant to control the self-interference. When power at both nodes are large, the power transmitted at the relay scales lower than its power constraint. Compared to HD mode, FD mode provides higher secrecy capacity in all cases.
3.4 Illustrative Examples

In this section, simulation results are provided to confirm the optimality of our solutions for the case of static channels. In all simulations, unless otherwise stated, 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 (3.8) and (3.9), we also consider the full PA scheme in FD with $(q_1 = q_s, q_2 = q_r)$ under the individual constraints and the uniform PA scheme with $(q_1 = q_2 = q_t/2)$ under the joint power constraint. The same dual hop model for HD systems with $q_{s,HD} = q_{r,HD} = q_{t,HD} = 2$ and its optimal PA schemes derived in section IV. B of [51] are also used as the system benchmarks.

3.4.1 Individual Constraints

Under the individual power constraints, Fig. 3.2 first shows the secrecy rates of the system versus $P_s/N_0$ when $P_r/N_0$ is fixed at 5dB and three values of $\lambda$ ($\lambda = 0, 0.5, 1$). First, observe from Fig. 3.2 the secrecy rates in the FD mode asymptotically approach $\log[(q_r\gamma_3 + 1)/(q_r\gamma_4 + 1)] = 0.815$ for both the full and the optimal PA. This reinforces the analysis in Sec. 3.3, where we showed that full power is asymptotically optimal for this case. Second, note that the FD system provides better secrecy rate than the HD system in this power region. As reflected in this example, when $P_s/N_0$ is sufficiently large, $C_{s,FD} \to \log(\frac{q_r\gamma_3 + 1}{q_r\gamma_4 + 1}) = 0.815 > C_{s,HD} \to 1/2 \log(\frac{2q_r\gamma_3 + 1}{2q_r\gamma_4 + 1}) = 0.449$

Fig. 3.3 shows the secrecy rates using the same PA schemes but the rates are drawn versus $P_r/N_0$ when $P_s/N_0$ is set at 5dB ($\lambda = 0, 0.5, 1$). Observe that in this case, secrecy rates in the FD mode mostly remains constant when the optimal PA
Figure 3.2: Secrecy Rate vs. $P_s/N_0$ for static channels ($\lambda = [0, 0.5, 1], P_r/N_0 = 5dB$).
Figure 3.3: Secrecy Rate vs. $P_r/N_0$ for static channels ($\lambda = [0, 0.5, 1], P_s/N_0 = 5dB$).
Figure 3.4: Secrecy Rate vs. $P/N_0$ for static channels ($\lambda = [0, 0.5, 1]$).

is applied. However, if full PA is used, the secrecy capacity approaches zero. This is because with full PA, $C_{s,FD} \rightarrow \log \frac{q_{\alpha_3}(q_{\lambda+1}\alpha_3)}{q_{\alpha_4}(q_{\lambda+1}\alpha_4)} = 0$ when $P_r/N_0$ is large. Similar to the previous result, the FD mode outperforms HD in high relay power regions for all values of $\lambda$. This is because although the secrecy in HD mode also approaches a constant $C_{s,HD} \rightarrow 1/2 \log \frac{(q_2\gamma_1+1)(q_4\gamma_1+q_3\gamma_4+1)}{(q_2\gamma_4+1)(q_4\gamma_1+q_3\gamma_3+1)} = 0.228$, this value is still smaller than the rate achieved in the worst-case of FD, which is $C_{s,FD} \rightarrow 0.319$ when $\lambda = 1$.

For the case when both $P_s/N_0$ and $P_r/N_0$ are large, the secrecy rates is depicted in Fig. 3.4. Note from Fig. 3.4 that in FD mode with full PA, the secrecy rates goes down to 0 when $0 < \lambda \leq 1$ because $C_{s,FD} \rightarrow \log[\alpha_3\alpha_4O(P^{\lambda+2})/\alpha_3\alpha_4O(P^{\lambda+2})] = \ldots
0, and it peaks when \( \lambda = 0 \), \( C_{s,FD} \rightarrow \log \frac{\alpha_3(\alpha_1 q_s + (1+\beta)q_r)}{\alpha_4(\alpha_1 q_s + (1+\beta)q_r)} = 0.392 \). However, this is still far less efficient compared to optimal PA scheme in which the secrecy capacity approaches \( C_{s,FD} \rightarrow \log(\alpha_3/\alpha_4) = 1 \) for all values of \( \lambda \). As expected from Sec. 3.3, this FD system with the optimal PA scheme is also twice more efficient than the HD system with its respective optimal PA, i.e., \( C_{s,HD} \rightarrow 1/2 \log(\alpha_3/\alpha_4) = 0.5 \).

3.4.2 Joint Power Constraint

The joint constraints case is illustrated in Fig. 3.5 where the secrecy rates is plotted against \( P_t/N_0 \). The secrecy capacity of the FD system with the optimal PA
approaches $C_{s,FD} \rightarrow \log(\alpha_3/\alpha_4) = 1$. With uniform PA, the secrecy rates peaks in the case when $\lambda = 0$ to $C_{s,FD} \rightarrow \log\frac{\alpha_3(\alpha_1 + (\beta+1)\alpha_4)}{\alpha_4(\alpha_1 + (\beta+1)\alpha_3)} = 0.392$, which is still far worse than the optimal scheme. In other cases when $0 < \lambda \leq 1$, the uniform PA brings the secrecy capacity down to zero. When compared to the HD mode, the FD system using the optimal PA is still superior. This is because the HD mode using optimal PA makes the secrecy capacity approach $C_{s,HD} \rightarrow 1/2 \log(\alpha_3/\alpha_4) = 0.5$, which is just half of that achieved by FD. This, again, confirms the analytical result from Sec. 3.3.
CHAPTER IV

OPTIMAL POWER ALLOCATION AND SECRECY CAPACITY OF AF FD RELAY WIRETAP CHANNELS IN ERGODIC FADING

In the previous chapter, the optimal PA and the secrecy capacity were addressed for the AF system under the assumption of static channels i.e., where all channel gains remain constant. In a more practical scenario, the wireless channel can be dynamic, which results in time-varying fading channels. In this part of the thesis, the investigation on optimal PA and secrecy capacity shall be extended to this scenario. The focus is on ergodic fading where the channel gains change randomly over time and they are available at the receivers but not the transmitters.

Due to the presence of fading, the problems of interest become more involved. Specifically, fading makes it more difficult to calculate the average secrecy rate. As a result, the optimization PA problem is more challenging. The calculation of secrecy rate under fading usually relies on lengthy Monte Carlo simulations [53, 54]. Therefore, in this chapter, the first focus is on the proposal of an effective way to calculate the secrecy rate for a given PA scheme. Specifically, it is shown that the average secrecy rate involving a triple integral can be expressed in a simple closed-form. By exploiting this closed-form expression, the optimal PA and the corresponding secrecy capacity are then addressed.
4.1 Ergodic Fading Channels

Under ergodic fading environments, the channel gains are time-varying and they are assumed to be independent zero-mean complex circular Gaussian as $h_1^{(i)} \sim \mathcal{CN}(0, \phi_1)$, $h_3^{(i)} \sim \mathcal{CN}(0, \phi_3)$, $h_4^{(i)} \sim \mathcal{CN}(0, \phi_4)$. Furthermore, it is assumed that the source $S$ only has the statical knowledge of the channels, while the destination $D$ and eavesdropper $E$ have instantaneous knowledge of all the channels, i.e., the channel knowledge is available at the receivers but not the transmitters. For a given channel vector $\mathbf{h}$, the achievable rate at $D$ and $E$ can be written respectively as $I_d|\mathbf{h}$ and $I_e|\mathbf{h}$ in the static case in (3.2). The ergodic secrecy rate can then be obtained by averaging these instantaneous rates over $\mathbf{h}$ as

$$R_s = E_{\mathbf{h}}[I(x_i, y_{d,i}|\mathbf{h}_i) - I(x_i, y_{e,i}|\mathbf{h}_i)]^+ = \int\int\int_{h_1, h_3, h_4} [I_d|\mathbf{h} - I_e|\mathbf{h}] p(h_1)p(h_3)p(h_4) dh_1 dh_3 dh_4. \quad (4.1)$$

Here, $E_{\mathbf{h}}$ denotes the expectation over the time-varying channel gains of $S$-$R$, $R$-$D$, and $R$-$E$ links, and $p(h_1), p(h_3), p(h_4)$ are pdf functions of fading channel gains.

Similar to the previous chapter, the main objective of this chapter is to obtain the optimal PA $\mathbf{q} = [q_1^*, q_2^*]$ on $S$ and $R$ to maximize the secrecy rate in (4.1) for both cases of individual and global power constraints. However, as can be seen from (4.1), the average secrecy rate involves a triple-integral due to the presence of fading, and numerically calculating it with high accuracy is very cumbersome. In the following, we first demonstrate that a closed-form expression of the secrecy rate can be established.
4.2 Closed-form Expression of the Average Secrecy Rate

The average secrecy rate $R_s$ in (4.1) can be expressed as:

$$R_s = f(q_1, q_2) = [E_{h_3} \log(1 + q_2 \gamma_3)] + E_{h_1,n_4} \log((1 + q_2^2 \gamma_2) + q_1 \gamma_1 + (q_2 + q_2^{1+\lambda} \gamma_2) \gamma_4)]$$

$$- E_{h_4} [\log(1 + q_2 \gamma_4)] - E_{h_1,n_4} [\log((1 + q_2^2 \gamma_2) + q_1 \gamma_1 + (q_2 + q_2^{1+\lambda} \gamma_2) \gamma_3)]^+. \tag{4.2}$$

Recall that for the ergodic channel, $\gamma_1 = |h_1^{(i)}|^2 P_s / N_0$, $\gamma_2 = \beta P_s / N_0$, $\gamma_3 = |h_3^{(i)}|^2 P_r / N_0$, and $\gamma_4 = |h_4^{(i)}|^2 P_r / N_0$. To further examine the expectations in (4.2), we first have the following lemma with regards to the exponential integral.

**Lemma 1.** Let $\omega_1$ and $\omega_2$ be independent exponentially distributed random variables with means $\phi_1$ and $\phi_2$, respectively. Define

$$J(x) = \exp(x) E_1(x),$$

where $E_1(.)$ is the exponential integral

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

and $\gamma$ is the Euler constant. Then, for $a_0 > 0$, one has

$$E_{\omega_1} [\ln(a_0 + \omega_1)] = J(a_0 / \phi_1), \tag{4.3a}$$

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

$$\begin{cases} 
1 + \ln(a_0) + \left(1 - \frac{a_0}{\phi_1}\right) J\left(\frac{a_0}{\phi_1}\right), & \phi_1 = \phi_2 \\
\ln(a_0) + \frac{\phi_1 J(1/\phi_1) - \phi_2 J(1/\phi_2)}{\phi_1 - \phi_2} - \gamma, & \phi_1 \neq \phi_2 
\end{cases} \tag{4.3b}$$
Proof. (4.3a) can be written as the rate (in nats/s/Hz) of a single-input-single-output system with instantaneous SNR $\omega_1$, which is given by [55, eq. (15.26)]. Moreover, (4.3b) can be written as the rate of a two-branch MRC combiner with SNRs $\omega_1$ and $\omega_1$. This rate is given by [55, eq. (15.33)] when the average SNRs are equal ($\phi_1 = \phi_2$) and by [56] for unequal average SNRs ($\phi_1 \neq \phi_2$).

Now, let $\gamma_1 = E\{\gamma_1\} = P_s\phi_1/N_0$, $\gamma_3 = E\{\gamma_3\} = P_r\phi_3/N_0$, $\gamma_4 = E\{\gamma_4\} = P_r\phi_4/N_0$, from (4.3a) and (4.3b) in Lemma 1, the expectations in (4.2) can be expressed as:

$$E[\log(1 + q_2\gamma_3)] = \frac{1}{\ln 2} J\left(\frac{1}{q_2\gamma_3}\right),$$

$$E[\log(1 + q_2\gamma_4)] = \frac{1}{\ln 2} J\left(\frac{1}{q_2\gamma_4}\right),$$

$$E[\log((1 + q_2^2\gamma_2) + q_1\gamma_1 + q_2\gamma_4(1 + q_2^2\gamma_2))] =$$

$$\begin{cases} \frac{1}{\ln 2} \left[1 + \log\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right) J\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right)\right], & \text{if } q_1\gamma_1 = q_2\gamma_4(1 + q_2^2\gamma_2) \\
\frac{1}{\ln 2} \left[\log\left(1 + q_2^2\gamma_2\right) + \frac{q_1\gamma_1 J\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right) - q_2\gamma_4 J\left(\frac{1}{q_2\gamma_4}\right)}{q_1\gamma_1 - q_2\gamma_4(1 + q_2^2\gamma_2)}\right], & \text{if } q_1\gamma_1 \neq q_2\gamma_4(1 + q_2^2\gamma_2), \end{cases}$$

$$E[\log((1 + q_2^2\gamma_2) + q_1\gamma_1 + q_2\gamma_3(1 + q_2^2\gamma_2))] =$$

$$\begin{cases} \frac{1}{\ln 2} \left[1 + \log\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right) J\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right)\right], & \text{if } q_1\gamma_1 = q_2\gamma_3(1 + q_2^2\gamma_2) \\
\frac{1}{\ln 2} \left[\log\left(1 + q_2^2\gamma_2\right) + \frac{q_1\gamma_1 J\left(\frac{1 + q_2^2\gamma_2}{q_1\gamma_1}\right) - q_2\gamma_3 J\left(\frac{1}{q_2\gamma_3}\right)}{q_1\gamma_1 - q_2\gamma_3(1 + q_2^2\gamma_2)}\right], & \text{if } q_1\gamma_1 \neq q_2\gamma_3(1 + q_2^2\gamma_2), \end{cases}$$
By combining these results, the average secrecy rate can be expressed in closed-form as:

$$R_s = f(q_1, q_2) = \frac{1}{\ln 2} \times$$

$$\begin{cases}
q_1 \gamma_1 \left( J \left( \frac{1}{q_2 \gamma_2} \right) - J \left( \frac{1+q_2 \gamma_2}{q_1 \gamma_1} \right) - \frac{J \left( 1+q_2 \gamma_2 \right)}{q_1 \gamma_1 - q_2 \gamma_2(1+q_2 \gamma_2)} \right) +, & \text{if } q_1 \gamma_1 \neq q_2 \gamma_3(1+q_2 \gamma_2) \\
1 - \frac{1}{q_2 \gamma_3} J \left( \frac{1}{q_2 \gamma_3} \right) + \frac{q_1 \gamma_1 J \left( \frac{1+q_2 \gamma_2}{q_1 \gamma_1} \right)}{q_1 \gamma_1 - q_2 \gamma_3(1+q_2 \gamma_2)} +, & \text{if } q_1 \gamma_1 \neq q_2 \gamma_3(1+q_2 \gamma_2) \\
-1 + \frac{1}{q_2 \gamma_3} J \left( \frac{1}{q_2 \gamma_3} \right) - \frac{q_1 \gamma_1 J \left( \frac{1+q_2 \gamma_2}{q_1 \gamma_1} \right)}{q_1 \gamma_1 - q_2 \gamma_3(1+q_2 \gamma_2)} +, & \text{if } q_1 \gamma_1 = q_2 \gamma_3(1+q_2 \gamma_2)
\end{cases}$$

The average secrecy rate can be easily calculated for given $q_1$ and $q_2$, since it involves only the well-known exponential integrals. In the next section, we shall address the optimal PA to maximize this rate under individual and joint power constraints.

4.3 Optimal Power Allocation

Given the closed-form expression of the secrecy rate in (4.1) above, the objective of this section is to find the optimal PA scheme and establish the secrecy capacity. We first have the following lemma regarding the positiveness of average secrecy rate $R_s$ in (4.1):

**Lemma 2.** To achieve positive average secrecy rate $R_s$, the relay-destination channel must be stronger than the relay-eavesdropper channel, i.e., $\gamma_3 > \gamma_4$. 

48
Proof. The average secrecy rate in (4.1) can be re-written as:

\[ R_s = E_h[I(x_i, y_{d,i}|h_i) - I(x_i, y_{e,i}|h_i)]^+ = (E_h[I(x_i, y_{d,i}|h_i)] - E_h[I(x_i, y_{e,i}|h_i)])^+ \]  

(4.5)

in which \( I(x_i, y_{d,i}|h_i) \) and \( I(x_i, y_{e,i}|h_i) \) are given in (3.2). For convenience, let \( I_d = E_h[I(x_i, y_{d,i}|h_i)] \) and \( I_e = E_h[I(x_i, y_{e,i}|h_i)] \). First, let consider \( I_d \). Let \( \gamma_3 = \gamma_3 \times x \) with \( x \) being an exponential random variable with unit variance. From (3.2), we can write

\[ I_d = E_h[\log(k(\gamma_3))] \]

where

\[ k(\gamma_3) = 1 + \frac{q_1 q_2 \gamma_1 x \gamma_3}{q_1 \gamma_1 + q_2 x \gamma_3 + q_2^1 \gamma_2 + q_2^1 + \lambda \gamma_2 x \gamma_3 + 1} \]  

(4.6)

By taking the first derivative of \( k(\gamma_3) \) with respect to \( \gamma_3 \), we have

\[ \frac{\partial k(\gamma_3)}{\partial \gamma_3} = \frac{q_1 q_2 x \gamma_1 (q^1 \gamma_2 + q_1 \gamma_1 + 1)}{(q_1 \gamma_1 + q_2 x \gamma_3 + q_2^1 \gamma_2 + q_2^1 + \lambda \gamma_2 x \gamma_3 + 1)^2} > 0, \]  

(4.7)

Clearly, \( k(\gamma_3) \) is an increasing function of \( \gamma_3 \). Since logarithm is an monotonically increasing function, \( I_d|\gamma_3 = \log(k(\gamma_3)) \) is also an increasing function of \( \gamma_3 \). Therefore, \( I_d = E[I_d|\gamma_3 = E[\log(k(\gamma_3))] \) is also an increasing function of \( \gamma_3 \).

In a similar manner, we can also show that \( I_e \) is also an increasing function of \( \gamma_4 \). Therefore, (4.5) can be written as

\[ R_s = (E[\log(k(\gamma_3))] - E[\log(k(\gamma_4))])^+, \]  

(4.8)
Thus, we can conclude that the average secrecy rate $R_s$ is positive if and only if $\gamma_3 > \gamma_4$.

Now, focusing on the case $\gamma_3 > \gamma_4$ so that a positive secrecy rate is achieved.

For convenience, let express $R_s$ in (4.4) as a function of $q_1$ and $q_2$ as $R_s = f(q_1, q_2) = \frac{1}{\ln 2} \times [r(q_1, q_2)]^+$. Since $\gamma_3 > \gamma_4$, we can re-write $R_s$ in (4.4) without using the "+" operation, i.e., $R_s = f(q_1, q_2) = \frac{1}{\ln 2} \times r(q_1, q_2)$. The optimization problem in (3.4) can then be re-written as follows:

$$\max_{q_1 \geq 0, q_2 \geq 0} f(q_1, q_2) \text{ s.t. } \begin{cases} q_1 \leq q_s, q_2 \leq q_r \quad \text{(indiv.)} \\ q_1 + q_2 \leq q_t \quad \text{(joint)}, \end{cases}$$

(4.9)

First, let evaluate the rate $R_s = f(q_1, q_2)$ as a function of $q_1$. As we have shown in Sec. 3.2, the instantaneous rate for a given channel realization is an increasing function of $q_1$. Since the logarithm function is an increasing function, we can conclude that $f(q_1, q_2)$ is also an increasing function of $q_1$. This fact can also be easily verified by taking the first derivative of (4.4) with respect to $q_1$. Having this result, in the following, we shall address the optimal values of $q_1$ and $q_2$ that maximize $f(q_1, q_2)$ for both cases of individual and global constrains.

4.3.1 Individual Constraints

Now, let start with the individual constraint. Because $f(q_1, q_2)$ is an increasing function of $q_1$, the optimal PA at $S$ is $q_1^* = q_s$. Therefore, for this case, we need to examine the property of the average secrecy rate versus $q_2$ via the analysis of $f(q_s, q_2)$. By
taking the first derivative of \( f(q_s, q_2) \) and applying the bisection method, we obtain

the optimal \( q_2^* \), which is the root of:

\[
\frac{\partial f(q_s, q_2)}{\partial q_2} = \frac{D_1}{\ln 2} \left[ \frac{(A_1' - C_1')}{(D_1 - \gamma_3 E_1)} + \frac{E_1' \gamma_3 (A_1 - C_1)}{(D_1 - \gamma_3 E_1)^2} - \frac{(B_1' - C_1')}{(D_1 - \gamma_4 E_1)} - \frac{E_1' \gamma_4 (B_1 - C_1)}{(D_1 - \gamma_4 E_1)^2} \right]
\]

(4.10)

Here, \( A_1 = J \left( 1/q_2 \gamma_3 \right) \), \( B_1 = J \left( 1/q_2 \gamma_4 \right) \), \( C_1 = J \left( \left( 1 + q_2^\lambda \gamma_2 / q_1 \gamma_1 \right) / q_2 \gamma_1 \right) \), \( D_1 = q_2 \gamma_1 \), \( E_1 = q_2^* \), \( q_2^*(1 + q_2^\lambda \gamma_2) \), and,

\[
A_1' = \frac{\partial A}{\partial q_2} = \frac{-A}{q_2^2 \gamma_3} + \frac{1}{q_2}, \quad B_1' = \frac{\partial B}{\partial q_2} = \frac{-B}{q_2^2 \gamma_4} + \frac{1}{q_2},
\]

\[
C_1' = \frac{\partial C_1}{\partial q_2} = \frac{\lambda \gamma_2 q_2^\lambda - 1}{D_1} C_1 - \frac{\lambda \gamma_2 q_2^\lambda - 1}{1 + q_2^\gamma_2}, \quad E_1' = \frac{\partial E_1}{\partial q_2} = 1 + (\lambda + 1) q_2^\lambda \gamma_2
\]

(4.11)

In general, the solution \( q_2^* \) only gives a local maxima. It is because different from the static case, it is not possible to analytically verify the quasi-concavity of \( f(q_1, q_2) \) in (4.4). However, via extensive simulation results, we have observed that the quasi-concavity of the secrecy rate in the case of static channels still holds true and the solution \( q_2^* \) is indeed the same with the globally optimal solution obtained by performing a brute-force search.

### 4.3.2 Global Constraint

Under the joint power constraint, we need to find the optimal PA scheme under \( q_1 + q_2 \leq q_t \). Since \( f(q_1, q_2) \) is an increasing function of \( q_1 \), the power is optimal when \( q_1 + q_2 = q_t \). As a result, the optimal solution \( q_1^* \) can be easily found by performing
bisection on $\frac{\partial}{\partial q_1} f(q_1, q_t - q_1) = 0$, and then we obtain $q^*_2 = q_t - q^*_1$. Specifically, we have:

$$f(q_1, q_t - q_1) = \frac{q_1 \gamma_1}{\ln 2} \times \frac{J \left( \frac{1}{(q_t - q_1) \gamma_3} \right) - J \left( \frac{1+(q_t - q_1) \gamma_2}{q_1 \gamma_3} \right) - J \left( \frac{1+q_t-q_1}{q_1 \gamma_3} \right)}{q_1 \gamma_1 - (q_t - q_1) \gamma_3 (1 + (q_t - q_1) \gamma_2)}$$

(4.12)

For convenience, let $A_2 = J \left( \frac{1}{(q_t - q_1) \gamma_3} \right), B_2 = J \left( \frac{1}{q_1 \gamma_3} \right), C_2 = J \left( \frac{1+(q_t - q_1) \gamma_2}{q_1 \gamma_3} \right), E_2 = (q_t - q_1) (1 + (q_t - q_1) \gamma_2)$. The optimal solution $q^*_1$ is therefore the root of the following:

$$\frac{\partial f(q_1, q_t - q_1)}{\partial q_1} = \frac{1}{\ln 2} \frac{\partial \left( \frac{T_1}{M_1} - \frac{T_2}{M_2} \right)}{\partial q_1}$$

(4.13)

where $T_1 = D_1 A_2 - D_1 C_2, T_2 = D_1 B_2 - D_1 C_2, M_1 = D_1 - \gamma_3 E_2, M_2 = D_1 - \gamma_4 E_2$.

This solution can be obtained using bisection method.

4.4 Illustrative Examples

In this section, numerical examples are provided to confirm the analysis and the advantage of the proposed solutions. Unless otherwise stated, we use the following channel parameters: $\beta = 0.1, \phi_1 = 2, \phi_3 = 2.5, \phi_4 = 1, \text{and } q_s = q_r = q_t = 1$. It should be noted that the proposed solutions can apply to any set of channel parameters.
4.4.1 Accuracy of the Closed-Form Secrecy Rate

At first, to demonstrate the usefulness of the closed-form expression in (4.4), Fig. 4.1 compares the secrecy rate using this closed-form and that obtained by Monte Carlo simulations for different values of $\lambda$ ($\lambda = 0, 0.5, 1$). For the considered systems, it is assumed that $q_1 = q_s$ and $q_2 = q_r$. Furthermore, $P_s = P_r = P$ and the rate curves versus SNR = $P/N_0$ are provided. Observe from Fig. 4.1 that the results obtained by the proposed closed-form match very well with the Monte Carlo simulations. Given that, in the following, we will present the secrecy rate calculated using (4.4) with...
different PA schemes as in the case of the static channels. For comparison, we also consider the use of HD mode of operation at the relay. With HD relaying, the optimal PA is obtained as in the case of FD relaying, where the average secrecy rate is calculated by setting \( \gamma_2 = 0 \) in (4.4) and pre-multiplying by a factor of 1/2.

4.4.2 Individual Constraints

Under the individual power constraints, Fig. 4.2 shows the average secrecy rates versus \( P_s/N_0 \) for the proposed optimal PA FD scheme and the full PA FD scheme when \( P_r/N_0 \) is fixed at 5dB and \( \lambda \) is set at 0, 0.5, and 1. The secrecy rate attained by the optimal PA HD scheme is also provided. It can be seen from Fig. 4.2 that the secrecy rates achieved by using full and optimal PA schemes look very similar and they approach 0.9222. This shows that full PA is asymptotically optimal under this scenario. It can also be seen that FD system outperforms the HD system in this power region; as reflected in this example, \( C_{s,FD} \to 0.9222 > C_{s,HD} \to 0.5253. \)

Fig. 4.3 shows the secrecy rates using the same PA schemes but the rates are drawn versus \( P_r/N_0 \), and \( P_s/N_0 \) is set at 5dB. Similar to the case of static channels, secrecy rates in the FD mode mostly remain constant when the optimal PA is applied. In contrast, when full PA is used, the secrecy rate asymptotically approaches zero. This demonstrates the advantage of using optimal PA over full PA for this case. Finally, it can also be seen that FD relaying with optimal PA performs much better than HD relaying in high relay power regions for all values of \( \lambda \). Although the secrecy secrecy in HD mode also remains constant \( C_{s,HD} \to 0.2558 \), this value is still smaller.
Figure 4.2: Secrecy Rate vs. $P_s/N_0$ for fading channels ($\lambda = [0, 0.5, 1], P_r/N_0 = 5dB$).
Figure 4.3: Secrecy Rate vs. $P_r/N_0$ for fading channels ($\lambda = [0, 0.5, 1], P_s/N_0 = 5dB$).
than the rate achieved in the worst-case scenario of FD relaying, which is $C_{s,\text{FD}} \rightarrow 0.3685$ when $\lambda = 1$.

The behavior of secrecy rates when $P_s/N_0 = P_r/N_0 = P/N_0$ are large is depicted in Fig. 4.4. In this case, full PA scheme is again suboptimal and the secrecy rates approach 0 when $0 < \lambda \leq 1$. When $\lambda = 0$, the rate is positive. However, it is much smaller than the secrecy capacity obtained using the optimal PA scheme, which asymptotically approaches $C_{s,\text{FD}} \rightarrow 1.2389$. Clearly, FD mode with the optimal PA also greatly outperforms its HD counterpart.
Figure 4.5: Secrecy Rate vs. $P_t/N_0$ for fading channels ($\lambda = [0, 0.5, 1]$).
4.4.3 Joint Power Constraint

Finally, Fig. 4.5 illustrates the case under joint power constraint where the secrecy rates are plotted against $P_t/N_0$. Besides the proposed solution in Sec. 4.3.2, the uniform PA scheme is also considered. It can be observed from Fig. 4.5 that secrecy capacity of the FD system approaches $C_{s,FD} \rightarrow 1.2386$. With the uniform PA, the secrecy rates approaches $C_{s,FD} \rightarrow 0.6901$ when $\lambda = 0$, i.e., perfect self-interference cancellation. The performance of uniform PA becomes even worse when $0 < \lambda \leq 1$. In fact, in this case, the secrecy rate asymptotically goes to zero. It can also be observed from Fig. 4.5 that compared to HD relaying, FD relaying with the optimal PA is much more efficient.

Several important observations can be made from the simulation results above. First of all, the numerical results for both scenarios of static channels and fading channels show the optimality of the proposed PA solutions over other PA schemes and optimal PA HD scheme. Moreover, the behaviors of the secrecy rates in different power regions are similar for both static and fading channels.
CHAPTER V
CONCLUSIONS AND SUGGESTIONS FOR FURTHER RESEARCH

5.1 Conclusions

This thesis studied the secrecy rate of a FD relay wiretap channel under practical self-residual interference. The optimal PA schemes at the source and the relay and the corresponding secrecy capacity were addressed for both cases of slow and fast fading channels respectively. The main contributions of the thesis are summarized as follow.

For the case of static channels, the related optimization problem has been shown to be quasi-concave. This condition ensures the uniqueness of the optimal solution. As a result, a simple root-finding method, such as bisection, can be applied and the algorithm will converge to a globally optimal solution. Moreover, further analyses on the capacity and PA schemes in different high power regions produce some important conclusions, which constitutes the second contribution of the first part. It is demonstrated that full PA at the relay is only needed when the power at the relay is sufficiently small compared to the power at the source. Then comparison with HD relaying also shows that FD relaying can achieve a significantly higher secrecy capacity.
The problem was also extended to ergodic fading channels in the second part of the thesis where the channel gains are assumed available at the receivers but not the transmitters. The main contribution here is by proposing a method to calculate the ergodic secrecy rate of the system in closed-form, the thesis has addressed the challenging problem of analyzing secrecy rate in fading environment due to the lack of an insightful method to calculate this metric. Given the formula for ergodic secrecy rate, the bisection method can be applied again to find the optimal PA scheme. Finally, various simulations were carried out for this case to verify the accuracy of the derived formula and the optimality of the PA scheme. Also, numerical results reveal that the conclusions obtained from the case of static channels hold true in the presence of fading, e.g. FD relaying is also superior over HD relaying in ergodic fading environments, and full PA at the relay is optimal only when the power at the relay is significant smaller than power at the source.

5.2 Future Works

Although this thesis has been able to thoroughly address the optimal PA problem in the case of static channels and propose a method to calculate the ergodic secrecy rate in the case of fading channel, several open problems still remain to be answered. In the following, I would like to present some potential research problems that are worth investigating.
• For the optimal PA problem discussed in Chapter 4 for the case of fading channels, although extensive simulations have been carried out to verify the global optimality of the solution, rigorous mathematical proof was not provided to guarantee the uniqueness of the solution obtained by bisection method. To my best knowledge, when it comes to finding the optimal PA to maximize ergodic secrecy rate, there is no globally convergence proof available on literature. Further research on this class of optimization problem to yield the globally optimal solution is certainly very challenging yet interesting.

• Although this thesis considered the relay in FD mode of operation, the use of FD transmission at relay is still limited to transmitting and forwarding at the same time. Further research effort can be invested to exploit the actual benefit of FD transmission in PHY security context. For example, new transmission protocols that enable relay nodes to use FD capability to receive the information and at the same time send jamming signal to degrade the signal-to-noise ratio at eavesdroppers should be proposed. That approach can eventually improve the overall secrecy rate of the system.

• Given that the relay was assumed to implement AF technique in this thesis, further investigation on FD relaying can be conducted by considering other relaying techniques such as DF and CF. For example, studying a similar model in which the relay implements DF technique may obtain some interesting results. The approach to tackle this new problem is also similar. In particular,
PA problem can be first addressed for the case of static channels by considering the quasi-concavity of the secrecy rate. Then when fading channels are taken into account, a closed-form formula could be proposed to calculate the ergodic secrecy capacity. Finally, PA for fading scenarios can be addressed by utilizing this closed-form formula.


