Secure And Efficient Wireless Communications in SWIPT-enabled Cooperative Networks

by

Maymoona Ahmad Yaseen Hayajneh
B.Sc., Jordan University of Science and Technology, 2010
M.Sc., Jordan University of Science and Technology, 2013

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Electrical and Computer Engineering

Secure And Efficient Wireless Communications in SWIPT-enabled Cooperative Networks

by

Maymoona Ahmad Yaseen Hayajneh
B.Sc., Jordan University of Science and Technology, 2010
M.Sc., Jordan University of Science and Technology, 2013

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor
(Department of Electrical and Computer Engineering)

Dr. Wu-Sheng Lu, Departmental member
(Department of Electrical and Computer Engineering)

Dr. Boualem Khouider, Outside Member
(Department of Mathematics and Statistics)

ACKNOWLEDGEMENTS

I am extremely grateful to my supervisor, Prof. Gulliver, for his invaluable advice, persistent support, encouragement, and patience during the last few years. His great knowledge and constant encouragement were critical to keeping me on the right track while trying to synchronize academic research with daily life. I would also like to express my sincere gratitude to the Schlumberger Foundation for their generous funding as part of believing in me and to spread knowledge around the world. My ultimate thanks and gratitude to my husband. His love, support, and sacrifice were there in good and bad times. The presence of my children around me was always great motivation to keep going. Moreover, I would like to express my gratitude to my mother, the soul of my father, my sister, and my brothers for their tremendous understanding and encouragement. Finally, special thanks to all friends, family members, and colleagues for their continuous help and support.

ABSTRACT

Wireless communications has gone through tremendous growth in the past decades. There has been a shift in wireless network research from spectral efficiency and quality of service (QoS) constraints to energy efficiency and green communications to reduce power consumption. Green energy resources such as solar, wind, thermal and mechanical vibrations can be employed to increase the energy efficiency of energy-constrained networks such as wireless sensor networks. Converting the available energy in the surrounding area into electricity, energy harvesting (EH), has been the subject of recent research. EH from radio frequency (RF) signals can be utilized to prolong the lifetime of devices in energy-constrained systems. Wireless power transmission (WPT) for EH is a promising solution to provide a reliable source of energy for devices which are difficult to service due to mobility and/or hard to reach locations.

The integration of relaying into conventional wireless networks is promising to increase the coverage area and reduce power consumption. However, the extra power consumed to relay signals may be a problem that can be mitigated by WPT. WPT has made it possible for relays to power themselves by capturing ambient energy wirelessly. The received signal at the relay can be utilized to both forward information and harvest energy.

This dissertation focuses on practical energy harvesting schemes in wireless communication networks. Further, the broadcast nature of wireless systems makes wireless transmissions more vulnerable to eavesdropping compared to wired signals. The goal of this work is to develop EH schemes that are capable of supplying sustainable energy to the relays and overcoming the secrecy hazards from potential eavesdroppers. Power splitting (PS) and time switching (TS) are studied in communication networks to prolong the lifetime of an energy-constrained relay. First, a dual hop system with an amplify and forward (AF) relay employing wireless information and power transfer (WIPT) via power splitting is studied. Optimal transmit antenna selection that maximizes the end-to-end signal to noise ratio (SNR) at the destination is considered and the outage probability is derived. It is shown that the outage probability increases with the number of transmit antennas but this also increases the system complexity.

Since the spectral efficiency with two-way relaying is higher than with one-way relaying, a two-way EH-based relay network with an eavesdropper is investigated. The secrecy capacity at the users is derived for two diversity combining cases at the eavesdropper, selection combining (SC) and maximal ratio combining (MRC).

A friendly jammer is introduced to increase the secrecy capacity of the users by reducing the received signal to noise ratio at the eavesdropper since the signal of the jammer is considered as noise at the eavesdropper. The corresponding optimization problem is reformulated using the single condensation method (SCM) and geometric programming (GP) into a convex optimization problem. Then, GP is used to jointly optimize the power splitting factor of the relay and transmit powers of the two users and jammer to maximize the secrecy capacity of the system. Imperfect cancellation of the jamming signal at the relay is assumed. It is shown that increasing the power allocated to the jammer decreases the secrecy capacity at the users. However, when perfect jamming signal cancellation is assumed, increasing the power allocated to the jammer increases the secrecy capacity at the users. The secrecy capacity is also shown to be greater with a jammer than without a jammer. Channel state information uncertainty at the eavesdropper is also considered as an extra noise source.

TS at the relay of a two-way EH-based relay network was also considered. GP is used to jointly optimize the time switching ratio of the relay and transmit powers of the two users and jammer to maximize the secrecy capacity of the system. It is shown that PS two-way relaying achieves a better secrecy capacity than TS two-way relaying.

Contents

List of Tables

List of Figures

List of Algorithms

List of Acronyms

AF	Amplify and Forward
AWGN	Additive White Gaussian Noise
BS	Base Station
CDF	Cumulative Distribution Function
CSI	Channel State Information
DF	Decode and Forward
DL	Direct Link
EH	Energy Harvesting
FJ	Friendly Jamming
GNJ	Gaussian Noise Jamming
GP	Geometric Programming
ID	Information Decoding
IoT	Internet of Things
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
MMSE	Minimum Mean Squared Error
MRC	Maximal Ratio Combining
OASEH	Optimal Antenna Selection with Energy Harvesting
OP	Outage Probability
PDF	Probability Density Function
PS	Power Splitting

RF Radio Frequency

SC Secrecy Capacity

SC Selection Combining

SCM Single Condensation Method

SNR Signal to Noise Ratio

SWIPT Simultaneous Wireless Information and Power Transfer

TS Time Switching

WIPT Wireless Information and Power Transfer

Chapter 1

Introduction

1.1 Background and Motivation of Wireless Power Transfer

Wireless communication networks have experienced exponential growth due to smart electronic devices and internet of things (IoT) applications. However, the increased power consumption of wireless communication systems puts a burden on service providers and also has a harmful impact on the environment, e.g. greenhouse effect [1]. Thus, careful wireless system design is a must for these increasing demands. To address this challenge, industry and academia have to develop energy efficient systems. One approach is to employ cooperative communications which allows nodes within a network to collaborate for information transmission. This leads to improved network connectivity, enhanced energy efficiency and increased reliability. Hence, cooperative communications can be used to improve the performance of wireless networks with constrained resources [2]–[4].

Energy harvesting (EH) from ambient energy sources such as sunlight can be used to enable green communications to significantly reduce the pressure on battery power or grid energy. In particular, the harvested energy can be used to reduce the need to recharge the batteries of wireless nodes as accessing these batteries can be costly, impractical or undesirable. With renewable energy sources such as solar and thermo-electric [5], the randomness of energy availability is a main problem [6]. Therefore, it is important to use this energy to maximize system utility while minimizing energy outage. Among other energy sources such as thermal, wind, and piezoelectric, radio frequency (RF) signals are promising for EH [7]. Since RF signals carry both energy and information, energy-constrained nodes can harvest energy and process information simultaneously [8]. However, a careful design at the receiver is required to reliably decode information and harvest energy successfully [8] [9]. Recently, RF EH has been studied as a promising candidate to extend the lifetime of energy-constrained wireless networks [10].

Ensuring secure communications between nodes is another motivation of this work. As a result of the massive number of devices in wireless communication networks, a network coordinator or controller may not be available or it is not practical to enable encrypted transmission by distributing security keys [11]. Further, keys can be intercepted by eavesdroppers as a result of the broadcast nature of wireless transmissions. Simple and low complexity security methods are required for energy-constrained wireless communication networks. Conventional cryptography may not be suitable because of the computational and key management costs which result in high complexity and resource consumption [12]. Therefore, it is a challenge to secure energy-constrained networks. Physical layer security is an emerging technique to improve the security of wireless networks. Compared to conventional cryptographic schemes, physical layer security is a very different paradigm. In physical layer security, secrecy is achieved by exploiting the characteristics of the wireless system such as the time-varying nature of fading channels [13]. The main challenge is to provide secure communications while minimizing the energy consumption at EH nodes.

Most of the research in information processing and wireless energy harvesting has considered point-to-point communications and the rate-energy tradeoff for various system configurations. These include single-input single-output (SISO) [14], [15], [16], multiple-input single-output (MISO) [17], single-input multiple-output (SIMO) [18], and multiple-input multiple-output (MIMO) [19]. EH relies on two switching techniques to receive information and perform EH, opportunistic time switching (TS) and dynamic power splitting (PS) [20]. For TS, the receive antenna switches between an EH receiver and an information decoding (ID) receiver periodically. For PS, the received signal is split into two portions, one sent to an EH receiver and the other to an ID receiver. Wireless energy harvesting has also been considered for orthogonal frequency division multiplexing (OFDM) [21] and cognitive radio [22] systems. Energy beamforming for a multi-antenna wireless broadcasting system with wireless energy harvesting was studied in [23]. Furthermore, multiuser scheduling was considered in [24] with wireless energy harvesting.

Recently, wireless relaying networks which employ energy harvesting from RF signals have been considered [25]–[27]. In [28], the optimal source and relay precoding in a MIMO relay system was studied for different rate-energy tradeoffs. The outage performance of cooperative communication systems was studied in [27]. The relay in [27] and [28] was assumed to have its own energy and so does not need to charge from external sources. Simultaneous information and power transfer for multiuser and multihop communications was investigated in [29]. It was assumed that the relay is capable of processing information and harvesting energy simultaneously, but the analysis in [14] showed that this assumption does not hold in practice. In [30], dual hop full-duplex relaying with energy harvesting using time switching was proposed and the outage probability and ergodic capacity of the system were derived. A greedy switching policy was introduced in [25] to minimize the outage probability at the destination of a three node cooperative system employing EH. In [26], the impact of the power splitting factor was evaluated for a two-way amplify and forward (AF) relay with SWIPT.

Physical layer security [31], [32] is a promising approach to secure wireless communications. Two-way relay networks were considered in [33]–[36] as relays are vulnerable to eavesdropping and can be trusted or untrusted. In [34], the tradeoff between secrecy and system complexity was studied for a two-way trusted relay network with three different antenna selection schemes. The effect of a friendly jammer on the physical layer security was studied in [33] for two-way untrusted relays. EH was considered in [37]–[39] to deal with the energy shortage of a two-way relay and maintain secure communications. In [37], an untrusted power splitting relay as an active eavesdropper or passive eavesdropper with one-way and two-way relaying. The secrecy outage probability was derived in [38] for an AF two-way untrusted relay employing energy harvesting. In [39], two-way communications via a wireless powered untrusted relay was considered for confidential communications using a friendly jammer.

1.2 Geometric Programming and the Single Condensation Method

In this section, a brief description of geometric programming (GP) and the single condensation method (SCM) is given. GP is used to obtain a nonlinear but convex optimization problem with convex objective and inequality constraint functions and linear equality constraints. This is achieved via a logarithmic change of variables and a logarithmic transformation of the objective function and constraints. The resulting convex problem can be solved efficiently using CVX solvers [40].

A GP problem has the form [40]

$$\text{minimize} \quad f_0(x) \tag{1.1a}$$

$$\text{subject to} \quad f_i(x) \leq 0, \quad i = 1, \ldots, m, \tag{1.1b}$$

$$g_i(x) = 1, \quad i = 1, \ldots, p \tag{1.1c}$$

where the f_i are polynomial functions, g_i are monomials, and x_i are the optimization variables. A real valued function f of the form $f(x) = cx_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ where $c > 0$ and $a_i \in \mathbf{R}$ is a monomial function. The sum of two or more monomials is a polynomial function such that $f(x) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} x_2^{a_{2k}} \ldots x_n^{a_{nk}}$ where $c_k > 0$.

The objective function in (1.1a) is a ratio of two posynomials, so it cannot be transformed into GP form. To solve this issue, the denominator is approximated as a monomial function using SCM [41]. SCM provides an upper bound on the ratio of posynomials. This ratio can be put into GP form by approximating the denominator of the ratio of posynomials with a monomial, but leaving the numerator as a posynomial. For example, $w(\mathbf{x}) = \sum_i u_i(\mathbf{x})$ is the denominator of a ratio of posynomials, where $\mathbf{x}$ is a vector of the optimization variables. $w(\mathbf{x})$ is the sum of i monomials, so it is a posynomial by definition, and the monomial approximation of $w(\mathbf{x})$ using SCM is

$$\overline{w}(\mathbf{x}) = \prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i}\right)^{\alpha_i}, \tag{1.2}$$

such that $w(\mathbf{x}) \geq \overline{w}(\mathbf{x})$. For a given $\mathbf{x}$, the α_i are obtained such that

$$\alpha_i = \frac{u_i(\mathbf{x})}{w(\mathbf{x})}, \tag{1.3}$$

and $\overline{w}(\mathbf{x})$ is substituted for $w(\mathbf{x})$ in the optimization problem. The objective function after SCM approximation is a posynomial. GP is used to obtain a nonlinear but convex optimization problem with convex objective function and inequality constraint functions and linear equality constraints. A logarithmic change of variables and a logarithmic transformation of the objective function and constraints are used to obtain a GP form. The resulting convex problem can be solved efficiently using CVX solvers [40]. As the optimal solution can be far from the initial guess $\mathbf{x}_0$ used in the SCM approximation, an iterative approach is used to solve this problem.

1.3 Research Objectives and Organization

Chapter 2 In this chapter, a dual hop, half-duplex amplify and forward (AF) relay is considered to forward the information signal from a source equipped with multiple transmit antennas to the destination. The relay does not have a fixed power supply, so it depends on the energy harvested from the source signal to amplify and forward the information signal to the destination node. The transmit antenna at the source is selected to maximize the end-to-end signal to noise ratio (SNR). The outage probability for a given transmission rate is derived as a function of the power splitting factor at the relay. It is shown that the proposed energy harvesting (EH)-based scheme outperforms the direct link model (without a relay). Further, there exists an optimal power splitting factor at which the outage probability is minimized. The impact of the relay placement on the outage performance is studied. The best performance is achieved when the relay is closer to the source node. The contributions of this chapter were published in [94].

Chapter 3 In this chapter, two users exchange information through a wireless powered two-way relay in the presence of an eavesdropper and cooperative jammer. The jammer transmits artificial noise to prevent the eavesdropper from overhearing the information signals. In this network, the relay relies solely on harvesting energy from the sources and jammer signals. Perfect self-interference cancellation is assumed for both sources so each source is capable of recovering the information signal of the other source assuming perfect channel state information (CSI) [35], [36], and [42]. The goal is to optimize the power allocated to the users and jammer and the power splitting to maximize the secrecy capacity [43]. The single condensation method (SCM) is used to convert the objective function to a standard geometric programming (GP) form. Then, GP is employed to transform the optimization problem into a convex problem. The contributions of this chapter were published in [109].

Chapter 4 The system model in Chapter 3 is modified assuming imperfect estimation of the channels connecting the eavesdropper to the other nodes in the system. Further, imperfect cancellation of the jamming signal at the relay is studied. Two combining techniques are employed at the eavesdropper, selection combining (SC) and maximal ratio combining (MRC). SCM is used to convert the objective function to a standard GP form. Then, GP is employed to transform the optimization problem into a convex problem.

Chapter 5 In this chapter, the secrecy capacity of the system model in Chapter 3 is studied with a relay that employs time switching to harvest energy and decode information. The effect of imperfect estimation of the channels connecting the eavesdropper to the other nodes in the system is studied. In addition, the jamming signal is not perfectly canceled at the relay which reduces the received signal to noise ratio at the users. The time switching ratio and the transmit power allocated to the users and jammer are jointly optimized to maximize the secrecy capacity. The eavesdropper employs selection combining and maximal ratio combining for the wiretapped signals to maximize the received signal to noise ratio.

Chapter 6 Some conclusions are given as well as suggestions for future work.

In the next chapters, the reader will notice some repetition. This is because the chapters are taken from the corresponding published and submitted journal papers.

Chapter 2

Optimal Transmit Antenna Selection with Wireless Information and Power Transfer

In this chapter, a dual hop system with an amplify and forward (AF) relay employing wireless information and power transfer (WIPT) via power splitting (PS) is studied. Optimal transmit antenna selection that maximizes the end-to-end signal to noise ratio (SNR) at the destination is considered. It is assumed that a direct link between the source and destination also exists. The exact outage probability is derived and numerical results are presented.

The main contributions of this chapter are as follows.

1. Upper bounds on the cumulative distribution function (CDF) of the end-to-end SNR are derived.

2. The outage probability (OP) is derived and the number of transmit antennas

at the source is varied to study the effect on the outage probability.

3. An optimal antenna selection scheme is proposed to maximize the signal to noise ratio at the destination. The performance was compared to the case with direct link.

2.1 System Model and Signal Representation

The wireless cooperative system considered is shown in Fig. 2.1. A source S with S_t transmit antennas communicates with a destination D utilizing both a direct link and a relay link, while the relay R and D are equipped with single antennas [30]. This model describes a downlink mobile communications system. The mobile nodes have only one antenna because their size is limited while the basestation has more than one antenna. The system employs AF relaying at the relay with PS factor θ, $0 \leq \theta \leq 1$, such that a fraction θ of the received signal is dedicated to energy harvesting. It is assumed that the channels between the ith source antenna, $i = 1, \ldots, S_t$, and D, $h_{S_i,D}$, the ith source antenna and R, $h_{S_i,R}$, and R and D, $h_{R,D}$, are subject to independent Rayleigh fading and modelled as mutually independent and identically distributed complex Gaussian random variables with zero mean and average power λ_{SD}, λ_{SR}, and λ_{RD}, respectively. The distances between S and D, S and R, and R and D are d_{SD}, d_{SR}, and d_{RD}, respectively. The transmit antenna that maximizes the signal to noise ratio (SNR) at the destination is selected.

A summary of the notation employed is given in Table 2.1.

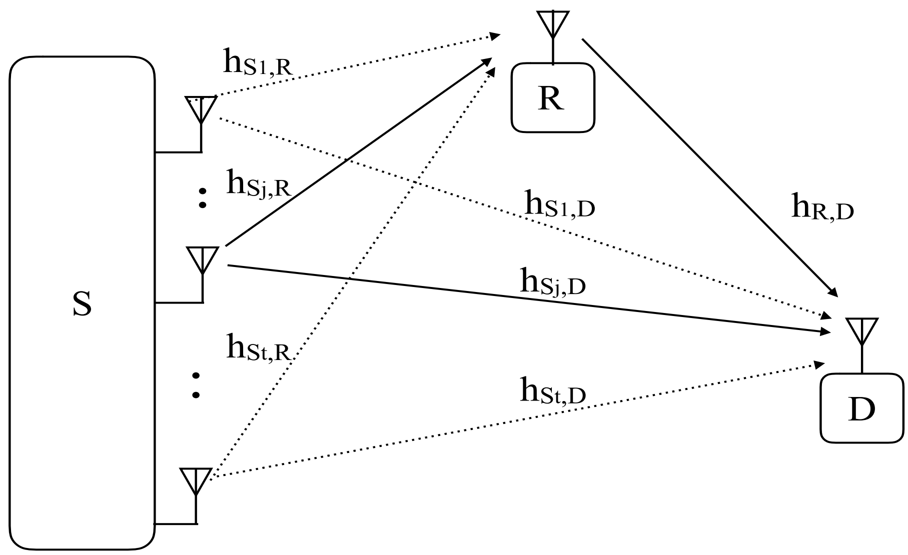

Figure 2.1: The system model with source antenna j selected for transmission.

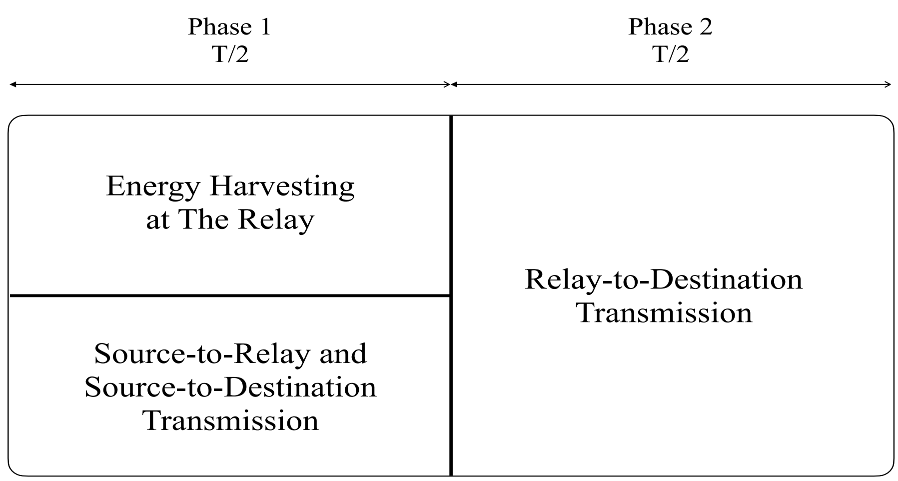

Figure 2.2: The data transmission time frame.

Table 2.1: Notation

Symbol	**Description**
S	Source
D	Destination
S_t	Number of transmit antennas at the source
R	Relay
θ	Power splitting factor
$h_{S_i,D}$	Channels between the ith source antenna and D
$h_{S_i,R}$	Channel between the ith source antenna and R
$h_{R,D}$	Channel between R and D
λ_{ij}	Average power of the channel link between node i and node j
d_{SD}	Distance between node i and node j
x_i	Signal transmitted by node i
P_i	Transmit power of node i
y_R	Signal received at node R
y_{D_i}	Signal received at node D in transmission phase i
n_{ai}	Baseband AWGN at node i
$\sigma^2_{n_{a_i}}$	Variance of the baseband AWGN at node i
n_{c_i}	Noise due to RF to baseband signal conversion at node i
$\sigma^2_{n_{c_i}}$	Variance of the additive noise due to RF to baseband conversion at node i

Continued on next page

Table 2.1 – *Continued from previous page*

Symbol	**Description**
n_i	Overall AWGN at i
σ_i^2	Overall noise variance at node i
y_{Re}	Energy harvesting signal at the relay
y_{Ri}	Information retrieval signal at the relay
E_H	Harvested energy
ζ	Energy conversion efficiency
G_R	Amplifier gain of the relay
$K_n(.)$	The nth order modified Bessel function of the second kind
m	Path loss exponent
R_T	Required transmission rate

In the proposed system, there are two data transmission phases as shown in Fig. 2.2. In the first phase, S sends a signal x_S to both R and D with fixed power P_S. The narrow band signals received at R and D in this phase are

$$y_R = \frac{\sqrt{P_S}}{\sqrt{d_{SR}^m}} h_{S_i,R} x_S + n_{a_R} \tag{2.1}$$

$$y_{D_1} = \frac{\sqrt{P_S}}{\sqrt{d_{SD}^m}} h_{S_i,D} x_S + n_{a_D} + n_{c_D}, \tag{2.2}$$

respectively, where n_{aR} and n_{aD} are the baseband additive white Gaussian noise (AWGN) at the receive antennas of R and D with zero mean and variances $\sigma^2_{n_{a_R}}$ and $\sigma^2_{n_{a_D}}$, respectively. The receiver at the destination down-converts the radio frequency, (RF), signal to baseband and processes the baseband signal, where n_{c_D} is the additive noise due to RF to baseband signal conversion with zero mean and variance $\sigma^2_{n_{c_D}}$. The overall AWGN at D is $n_D = n_{a_D} + n_{c_D}$ with variance $\sigma^2_D = \sigma^2_{n_{a_D}} + \sigma^2_{n_{c_D}}$. A block diagram of the relay receiver is given in Fig. 2.3. The received signal at R, y_R, is split with PS factor θ such that a fraction

$$y_{Re} = \sqrt{\theta} y_R = \frac{\sqrt{\theta P_S}}{\sqrt{d^m_{SR}}} h_{S_i,R} x_S + \sqrt{\theta} n_{a_R} \tag{2.3}$$

is forwarded to the EH receiver. The remaining fraction

$$y_{Ri} = \sqrt{1-\theta} y_R + n_{c_R} \tag{2.4}$$

$$= \frac{\sqrt{(1-\theta) P_S}}{\sqrt{d^m_{SR}}} h_{S_i,R} x_S + \sqrt{1-\theta} n_{a_R} + n_{c_R}, \tag{2.5}$$

is forwarded to the information receiver where n_{c_R} is the AWGN of the RF to baseband signal conversion circuit at R with zero mean and variance $\sigma^2_{n_{c_R}}$. In (2.5), the overall AWGN at R is $n_R = \sqrt{1-\theta} n_{a_R} + n_{c_R}$ with variance $\sigma^2_R = (1-\theta)\sigma^2_{n_{a_R}} + \sigma^2_{n_{c_R}}$. The energy harvested in the first phase is

$$E_H = \frac{\zeta \theta P_S |h_{S_i,R}|^2}{d^m_{SR}} \frac{T}{2}, \tag{2.6}$$

where ζ is the energy conversion efficiency, $0 < \zeta < 1$, which depends on the EH receiver design. The time portion used to receive and harvest energy at the relay is $T/2$. Since the noise term in (2.3) is much smaller than the signal term, only the energy from the transmitted signal is harvested as given in (2.6). In the second phase, the relay amplifies y_{Ri} and forwards it to D using the harvested energy in the first

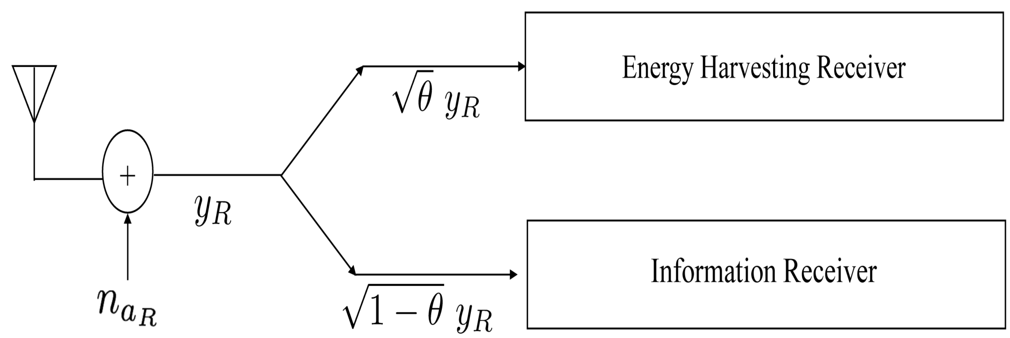

Figure 2.3: The relay receiver block diagram.

phase. The relay transmit power can then be expressed as

$$P_R = \frac{E_H}{T/2} = \frac{\zeta \theta P_S |h_{S_i,R}|^2}{d_{SR}^m}, \tag{2.7}$$

so the transmitted signal is

$$x_R = G_R y_{Ri}, \tag{2.8}$$

where G_R is the relay gain as defined in [44]

$$G_R = \sqrt{\frac{P_R}{(1-\theta) P_S |h_{S_i,R}|^2 d_{SR}^{-m} + \sigma_R^2}}. \tag{2.9}$$

The received signal at D from the relay in the second phase is

$$y_{D_2} = x_R h_{R,D} + n_D. \tag{2.10}$$

2.2 Outage Probability Analysis

The destination receives two observations of x_S given by (2.2) and (2.10). It is assumed that the destination employs a minimum mean squared error (MMSE) receiver. The instantaneous post-processing SNR at the destination can be expressed as [45]

$$\gamma_i = \gamma_{S_i,D} + \frac{\gamma_{S_i,R}\gamma_{R,D}}{1 + \gamma_{S_i,R} + \gamma_{R,D}}, \tag{2.11}$$

where $\gamma_{S_i,D} = \frac{P_S|h_{S_i,D}|^2}{\sigma_D^2 d_{SD}^m}$ is the SNR between the ith transmit antenna of the source and the destination. The SNR between the ith source antenna and the relay is $\gamma_{S_i,R} = \frac{(1-\theta)P_S|h_{S_i,R}|^2}{\sigma_R^2 d_{SR}^m}$, and $\gamma_{R,D} = \frac{\zeta\theta P_S|h_{S_i,R}|^2|h_{R,D}|^2}{\sigma_D^2 d_{SR}^m d_{RD}^m}$ is the SNR between the relay and destination. MIMO training methods can be used to estimate $h_{S_i,R}$, $h_{S_i,D}$, and $h_{R,D}$ for antenna selection. A short narrowband signal as in [45] can be used to estimate (2.11). Then the destination feeds back to the source the index of the antenna corresponding to the largest γ_i. The optimal transmit antenna is

$$j = \arg\max_i \{\gamma_i\}. \tag{2.12}$$

Unfortunately, a closed form expression for the cumulative distribution function (CDF) or probability density function (PDF) of γ_i cannot be obtained, but an upper bound is given by [46] and [47]

$$\gamma_i \leq \gamma_{S_i,D} + \min\{\gamma_{S_i,R}, \gamma_{R,D}\}. \tag{2.13}$$

The upper bound on the SNR at D when the jth transmit antenna is selected is

$$\gamma_{upper} = \gamma_{S_j,D} + \min\{\gamma_{S_j,R}, \gamma_{R,D}\}. \tag{2.14}$$

A system outage implies that the mutual information I is below the required transmission rate R_T, i.e.

$$P_{out} = P_r\left\{I < R_T\right\} = P_r\left\{1/2\log_2(1+\gamma) < R_T\right\}, \tag{2.15}$$

where γ is the SNR at the destination. The factor 1/2 reflects the two time phases required for data transmission from the source to destination. The PDFs of $\gamma_{S_i,D}$ and $\gamma_{S_i,R}$ are $f_{\gamma_{S_i,D}}(x) = \frac{1}{\alpha_{SD}}e^{-\frac{x}{\alpha_{SD}}}$ and $f_{\gamma_{Si,R}}(x) = \frac{1}{\alpha_{SR}}e^{-\frac{x}{\alpha_{SR}}}$, respectively, where $\alpha_{SD} = \frac{P_S\lambda_{S,D}}{\sigma_D^2 d_{SD}^m}$ and $\alpha_{SR} = \frac{(1-\theta)P_S\lambda_{SR}}{\sigma_R^2 d_{SR}^m}$. The CDF of the R-D link is then

$$\begin{aligned} F_{\gamma_{RD}}(x) &= P_r\left\{\gamma_{R,D} < x\right\} && (2.16)\\ &= P_r\left\{|h_{RD}|^2 < \frac{x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S|h_{S_i,R}|^2}\right\} && (2.17)\\ &= 1 - \frac{1}{\lambda_{RD}}e^{-\frac{x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S\lambda_{RD}|h_{S_i,R}|^2}}. && (2.18) \end{aligned}$$

Substituting $Y = |h_{S_i,R}|^2$ in (2.18) gives

$$F_{\gamma_{RD}}(x) = 1 - \frac{1}{\lambda_{RD}}e^{-\frac{x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S\lambda_{RD}Y}}. \tag{2.19}$$

Since $|h_{S_i,R}|^2$ is an exponential random variable with mean value λ_{SR}, $f_{|h_{S_i,R}|^2}(y) = \frac{1}{\lambda_{SR}} e^{-\frac{y}{\lambda_{SR}}}$. Conditioning (2.19) over Y and taking the expected value gives

$$\begin{aligned} F_{\gamma_{RD}}(x) &= \int_0^\infty (1 - \frac{1}{\lambda_{RD}} e^{-\frac{x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S \lambda_{RD} y}}) f_y(y) dy & (2.20) \\ &= 1 - \frac{1}{\lambda_{RD}\lambda_{SR}} \int_0^\infty e^{-\frac{x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S \lambda_{RD} y}} e^{-\frac{y}{\lambda_{SR}}} dy & (2.21) \\ &= 1 - \frac{1}{\lambda_{RD}\lambda_{SR}} \int_0^\infty e^{-\frac{4x\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S \lambda_{RD}} \frac{1}{4y}} e^{-\frac{1}{\lambda_{SR}} y} dy. & (2.22) \end{aligned}$$

Using [48, §3.324.1], we obtain

$$F_{\gamma_{RD}}(x) = 1 - \Xi\sqrt{x} K_1(\Xi\sqrt{x}), \tag{2.23}$$

where $\Xi = \sqrt{\frac{4\sigma_D^2 d_{SR}^m d_{RD}^m}{\zeta\theta P_S \lambda_{SR}\lambda_{RD}}}$ and $K_n(.)$ is the nth order modified Bessel function of the second kind. Given $f_{\gamma_{RD}}(x) = \frac{\partial F_{\gamma_{RD}}(x)}{\partial x}$ and using [48, §8.486.18], the PDF of the R-D link is $f_{\gamma_{RD}}(x) = \frac{\Xi^2}{2} K_0(\Xi\sqrt{x})$. The CDF of the upper bound on the SNR is

$$F_{upper}(c) = \int_0^c A(c,x)^{S_t} \frac{\Xi^2}{2} K_0(\Xi\sqrt{x}) dx + \int_c^\infty B(c)^{S_t} \frac{\Xi^2}{2} K_0(\Xi\sqrt{x}) dx \tag{2.24}$$

where

$$A(c,x) = 1 - \frac{\alpha_{SD}}{\alpha_{SD}-\alpha_{SR}} e^{-\frac{c}{\alpha_{SD}}} + \frac{\alpha_{SR}}{\alpha_{SD}-\alpha_{SR}} e^{-\frac{c}{\alpha_{SD}}} e^{-xg}, \quad (2.25)$$

$$= a + be^{-xg}, \quad (2.26)$$

$$a = 1 - \frac{\alpha_{SD}}{\alpha_{SD}-\alpha_{SR}} e^{-\frac{c}{\alpha_{SD}}}, \quad (2.27)$$

$$b = \frac{\alpha_{SR}}{\alpha_{SD}-\alpha_{SR}} e^{-\frac{c}{\alpha_{SD}}}, \quad (2.28)$$

$$g = \frac{\alpha_{SD}-\alpha_{SR}}{\alpha_{SD}\alpha_{SR}}, \quad (2.29)$$

$$B(c) = 1 - e^{-\frac{c}{\alpha_{SR}}} - \frac{\alpha_{SD}}{\alpha_{SD}-\alpha_{SR}} (e^{-\frac{c}{\alpha_{SD}}} - e^{-\frac{c}{\alpha_{SR}}}). \quad (2.30)$$

See Appendix for the derivation of $A(c,x)$ and $B(c)$. Substituting the binomial expansion of $(a+be^{-xg})^{S_t}$ for $A(c,u)^{S_t}$ in (2.24), where $(y+z)^n = \sum_{k=0}^{n} \binom{n}{k} y^{n-k} z^k$, and observing that $B(c)$ is independent of the integration variable x, $F_{upper}(c)$ can be rewritten as

$$F_{upper}(c) = \frac{\Xi^2}{2} \sum_{i=0}^{S_t} \binom{S_t}{i} a^{S_t-i} b^i \int_0^c e^{-gxi} K_0(\Xi\sqrt{x}) dx + \frac{\Xi^2}{2} B(c)^{S_t} \int_c^{\infty} K_0(\Xi\sqrt{x}) dx. \quad (2.31)$$

An upper bound on the outage probability (OP) is then obtained by substituting $c = 2^{2R_T} - 1$ in (2.31).

2.3 Numerical Results

In this section, the system OP is evaluated numerically. Unless otherwise stated, the energy conversion efficiency is $\zeta = 0.7$, the noise variances at the relay and destination are $\sigma^2_{n_{a_D}} = \sigma^2_{n_{c_D}} = \sigma^2_{n_{a_R}} = \sigma^2_{n_{c_R}} = 0.01$, and $R_T = 1$ bit/sec/Hz. The values of λ_{SD},

λ_{SR}, and λ_{RD} are set to 1, $d_{SD} = 5$, and the path loss exponent is $m = 2$. Fig.

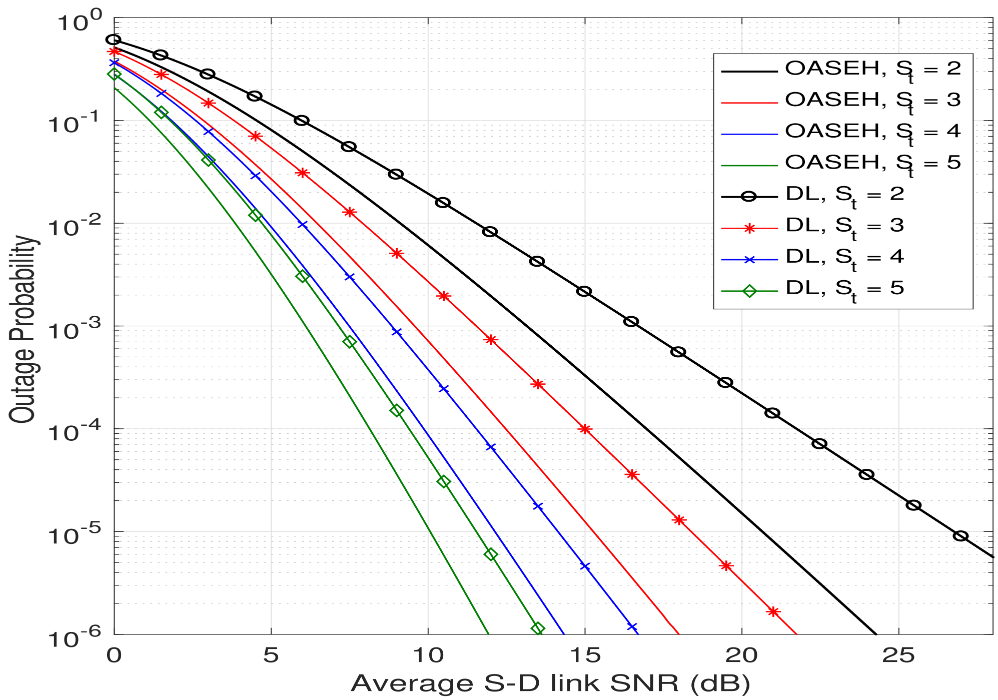

Figure 2.4: Outage probability versus the average S-D link SNR for $S_t = 2$ to 5, $\theta = 0.6$, $\zeta = 0.7$, and $m = 2$.

2.4 presents the outage probability for the direct link without a relay (DL) and the optimal antenna selection with an energy harvesting relay (OASEH) for $S_t = 2$ to 5. It is assumed that both sources in OASEH and DL transmit with equal transmit power P_S. The power splitting factor is $\theta = 0.6$, and the relay is assumed to be equidistant on the straight line between the source and the destination. Fig. 2.4 shows that the outage performance of OASEH improves as the number of transmit antennas increases from $S_t = 2$ to 5. It is also observed that the EH relay significantly improves the outage probability performance without additional power at the source node. For an OP of 10^{-6}, the improvement in OASEH relay performance is 9.3, 3.6, and 2.3 dB for $S_t = 2$ to 3, 3 to 4, and 4 to 5, respectively, so it decreases as the number of transmit antennas increases. Adding antennas increases the system cost, so there is a tradeoff between cost and performance. Fig. 2.4 shows that OASEH improves the outage performance by 7.5 dB at $S_t = 2$ to 1.7 dB at $S_t = 5$ compared to DL performance for an OP of 10^{-6}. In the low SNR region, the performance is similar, but the difference increases as the SNR increases. This is because at higher SNRs, the EH relay harvests more energy, and hence the transmit power at the relay is larger during the second phase.

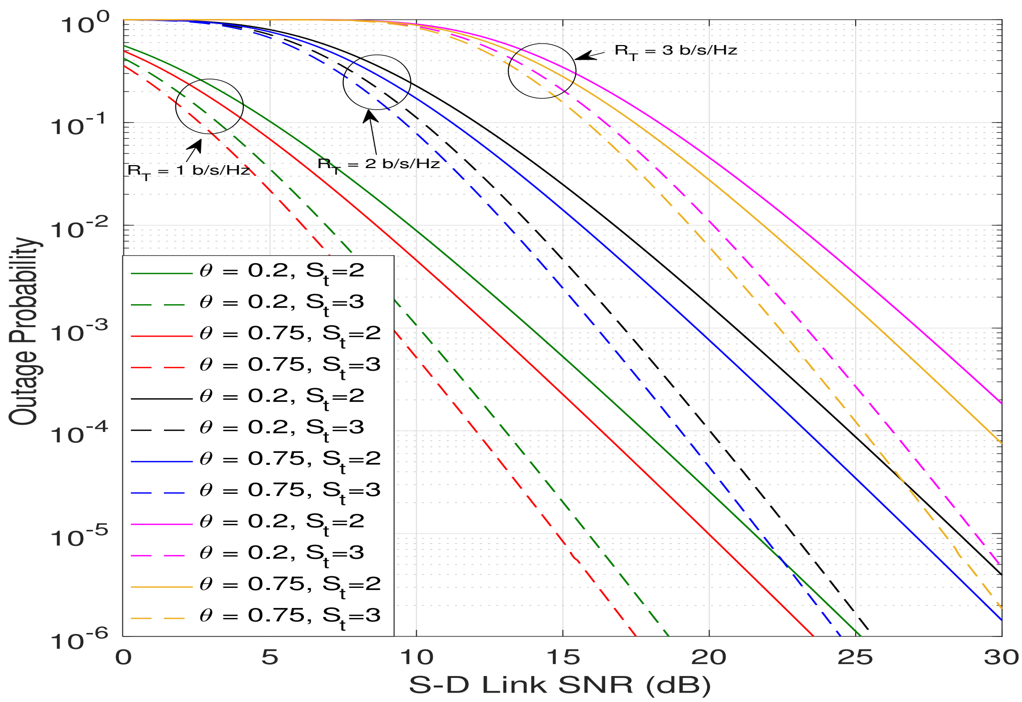

Figure 2.5: Outage probability versus the average S-D link SNR for $S_t = 2$ and 3, $\theta = 0.2$ and 0.75, $\zeta = 0.7$, $m = 2$, and $R_T = 1$, 2, and 3 bits/sec/Hz.

Fig. 2.5 presents the outage probability for different values of θ and R_T. This shows that the outage probability (OP) increases with the transmission rate. Further, increasing θ from 0.2 to 0.75 reduces the OP for both $S_t = 2$ and $S_t = 3$.

Fig. 2.6 shows the effect of the power splitting factor θ on the OP of OASEH for

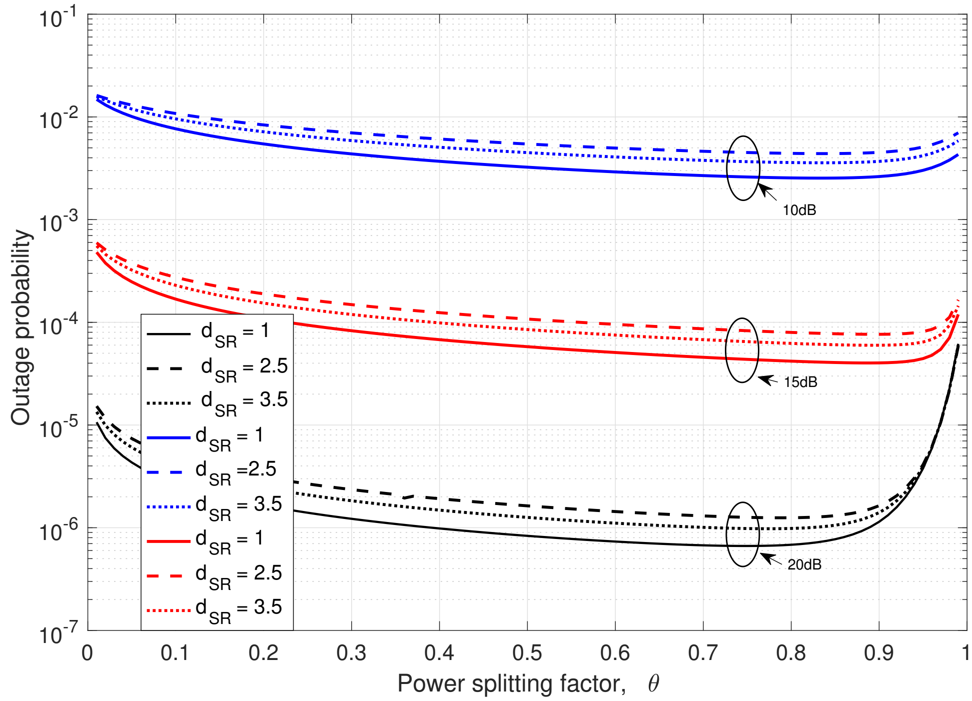

Figure 2.6: OASEH and DL outage probability versus the power splitting factor θ for different relay locations, $S_t = 3$, average S-D link SNR 10, 15, and 20 dB, and $R_T = 1$ bit/sec/Hz.

three different relay locations with respect to the source and three different average S-D link SNRs. The number of transmit antennas is $S_t = 3$ and $d_{SD} = 5$ so that $d_{RD} = 5 - d_{SR}$, and the transmission rate is $R_T = 1$ bit/sec/Hz. This figure shows that the OP initially decreases as θ increases from 0 to an optimal value, θ_{opt}, and then increases for θ beyond the optimal value and approaches 1. At smaller values of θ, there is less power available at the relay for energy harvesting. Hence less power, P_R, is available for the relay to forward the received signal to the destination. On the other hand, as θ increases beyond θ_{opt}, there is sufficient harvested power, but the signal received at the relay is poor. When this noisy signal is amplified and forwarded to the destination node, the OP at D is high. For the relay placements shown, the optimal value of θ increases as the average S-D link SNR decreases. For example, at $d_{SR} = 1$, θ_{opt} is 0.75, 0.81, and 0.84 for S-D average link SNRs of 20 dB, 15 dB, and 10 dB, respectively. This can be explained by the fact that when the EH relay is not receiving significant power, a large portion of the received signal power is needed for EH to maximize the end-to-end SNR.

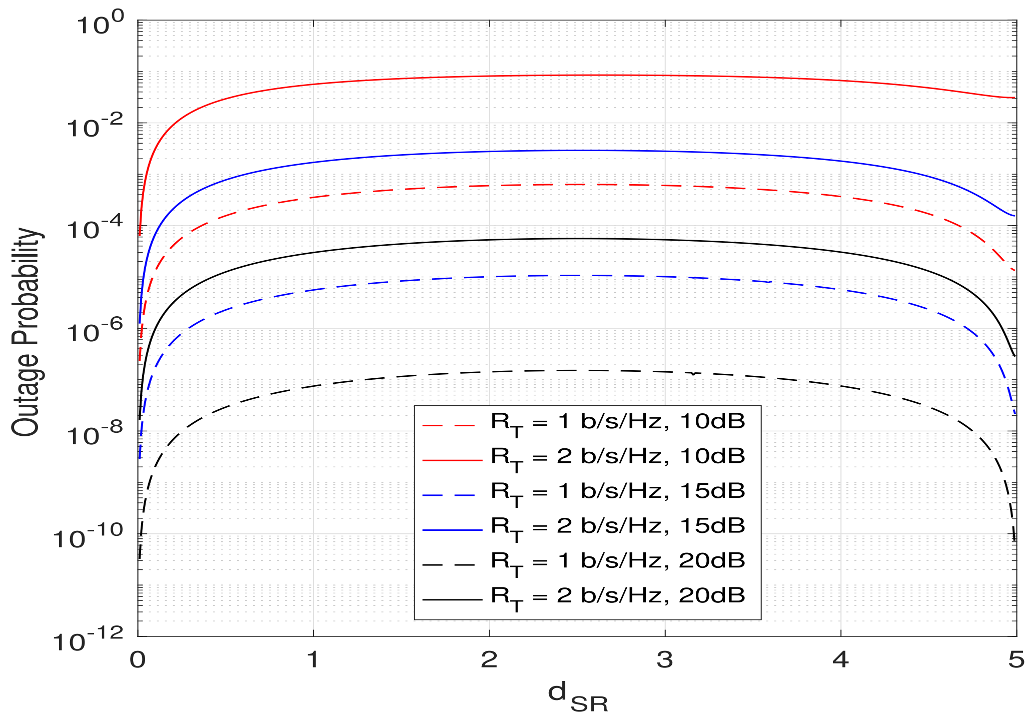

Figure 2.7: OASEH outage probability versus the S-R distance, d_{SR}, for $R_T = 1$ and 2 bits/sec/Hz, $S_t = 3$, and average S-D link SNR of 15 dB.

Fig. 2.7 presents the OP with OASEH as a function of the distance between the source and relay, d_{SR}, for $R_T = 1$ and 2 bits/sec/Hz at different average S-D link SNRs. For both values of R_T the outage probability increases as the relay moves further from the source and the maximum outage occurs near the midpoint. Further, the lowest OP occurs when the relay is closer to the source. When the relay is close to the source, it can harvest more energy from the transmitted signal. The received signal strength at the relay, y_R in (2.5), is better due to the smaller path loss ${d_{SR}}^{-m}$. When the relay is close to the destination, the signal from the source is poor, but less transmit power is required to support reliable communication from R to D. In Fig. 2.7, as the transmission rate increases, the outage probability increases because it is affected by the SNR at the destination. The results are not symmetric around the midpoint $d_{SR} = 2.5$ as may appear from the figure. For example, at $R_T = 1$ b/s/Hz, the maximum OP occurs at a distance 2.52 at 10 dB, 2.505 at 15 dB, and 2.50 at 20. For $R_T = 2$ b/s/Hz, the maximum OP occurs at a distance 2.625 at 10 dB, 2.535 at 15 dB, and 2.515 at 20 dB. Thus, the optimum relay location can be approximated as equidistant between the source and destination.

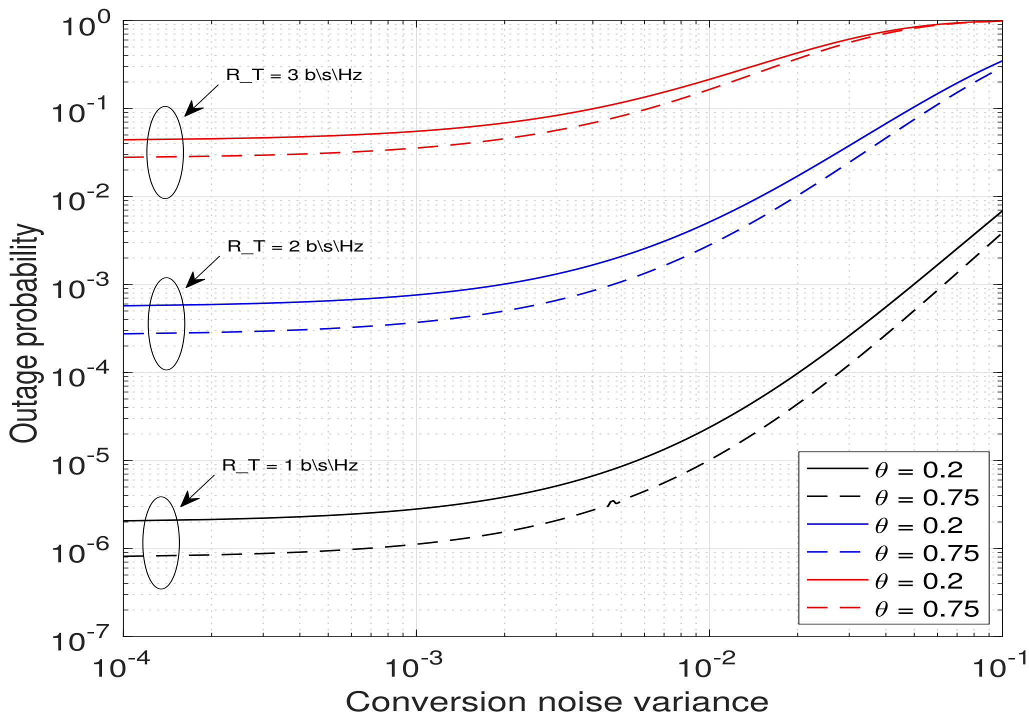

Figure 2.8: OASEH outage probability versus $\sigma^2_{n_c}$ for different values of θ, $S_t = 3$, $d_{SR} = 3$, average S-D link SNR 15 dB, and $\sigma^2_{n_{a_D}} = \sigma^2_{n_{a_R}} = 0.01$.

Fig. 2.8 gives the OP as a function of the RF-to-baseband conversion noise variance, $\sigma^2_{n_c} = \sigma^2_{n_{c_D}} = \sigma^2_{n_{c_R}}$. Two values of θ are considered, $\theta = 0.2$ and $\theta = 0.75$, for transmission rates $R_T = 1$, 2, and 3 bits/sec/Hz. The OP performance for $\theta = 0.75$ is better than with $\theta = 0.2$. This is due to the fact that at a splitting factor of $\theta = 0.2$, a larger portion of the noisy received signal is passed to the information receiver. The noise is amplified and forwarded to the destination which increases the OP at the destination. Further, increasing the transmission rate degrades the performance as the noise variance increases. Fig. 2.9 presents the OP performance as a function of θ for different average S-D link SNR values. The relay is assumed to be equidistant on the straight line between the source and destination. This shows that there exists an optimal splitting factor, θ_{opt}, which is a function of the average S-D link SNR. As the SNR increases, θ_{opt} decreases since the received signal strength improves. This allows the relay to amplify and forward a larger portion, $(1 - \theta)$, of the received signal to the destination, resulting in improved OP performance.

2.4 Conclusion

In this chapter, a dual hop, half-duplex, amplify and forward (AF) relaying system with energy harvesting (EH) and optimal transmit antenna selection was investigated. Upper bounds on the CDF of the end-to-end SNR and the outage probability (OP) were derived. The effect of various system parameters on the performance with wireless energy harvesting using an AF relay was provided. The optimal power splitting factor was considered. The OP as a function of the distance between the source and relay was examined for different transmission rates. It was shown that increasing the number of transmit antennas improves the OP, but this also increases the system complexity.

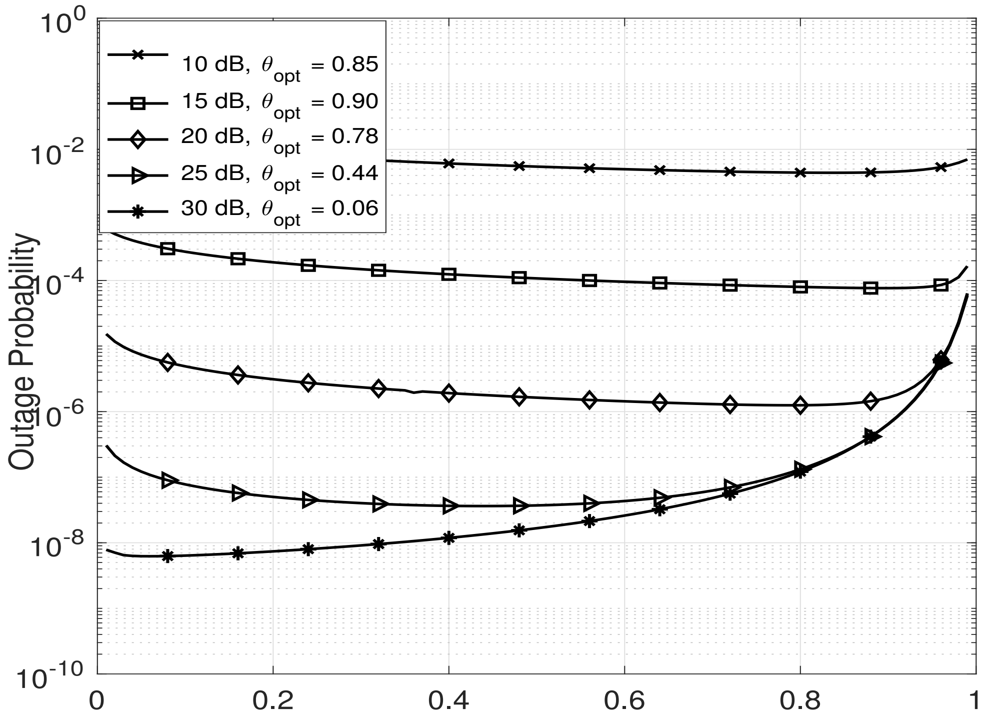

Figure 2.9: OASEH outage probability versus the power splitting factor θ for different average S-D link SNR values, $S_t = 3$, and $d_{SR} = 2.5$.

Chapter 3

Optimal Power Allocation and Secrecy Capacity in a Wireless-Powered Two-Way Relay Network

This chapter considers secure two-way relay communications in the presence of an eavesdropper. Two users without a direct link between them communicate via an energy harvesting two-way relay. A friendly jammer is employed to reduce information leakage to the eavesdropper. The relay relies on the signals received to harvest energy and forward signals to the users. The power splitting factor and transmit power at the users and jammer are jointly optimized using geometric programming (GP) to maximize the secrecy capacity of the system. The imperfect cancellation of the jamming signal is interpreted as noise at the users which decreases the secrecy capacity. Further, it is shown that the secrecy capacity with a jammer is greater than without a jammer. The effect of the relay, jammer, and eavesdropper locations on the performance is studied. It is shown that the secrecy capacity is greater when the relay is equidistant from the users. In addition, having the jammer closer to the eavesdropper results in a higher secrecy capacity.

3.1 Introduction

Energy harvesting (EH) from radio frequency (RF) signals in wireless communication systems can be employed to extend the lifetime of energy-constrained devices [60]. Simultaneous wireless information and power transfer (SWIPT) is possible as RF signals carry information and energy simultaneously [61]–[15]. The energy harvesting (EH) and information retrieval differ so two separate circuits are typically employed [95]. Two practical EH relaying protocols for communication systems are power splitting (PS) and time switching (TS) [49]. With TS, the receiver switches between the information retrieval circuit and the EH circuit while with PS, a portion of the received signal is directed to the information retrieval circuit and the remainder to the EH circuit. In [63] and [64], the transmission rate was maximized using optimal PS and TS relaying, respectively.

In [63], the outage probability was derived for a decode and forward (DF) network and the optimum PS and TS coefficients were obtained to maximize the transmission rate. In [64], a SWIPT-enabled relay was studied for three scenarios, ideal (information extraction and EH are done simultaneously), PS, and TS. The achievable rate was optimized for each of the these scenarios at the relay. PS and TS can be used separately or combined as in [65] where a hybrid EH protocol was proposed. This protocol is more general because the relay can switch between PS and TS. The optimal

EH TS and PS ratios were derived to maximizing the throughput and it was shown that a hybrid circuit outperforms separate circuits. Joint PS and TS schemes for amplify and forward (AF) and decode and forward (DF) relay systems were proposed in [66] and [67], respectively, and the outage probability was shown to be better than with the hybrid protocol in [65]. In [66], the outage probability, network throughput and energy efficiency were derived as a function of the PS and TS ratios, and the network throughput was maximized. Two joint optimization problems were formulated in [67] to maximize the channel capacity and minimize the outage probability. An optimal offline joint relay selection and power allocation scheme was proposed in [68] to maximize the system throughput in a cognitive two-way relaying network. This scheme outperforms random relay selection when the transmit power is limited.

The broadcast nature of wireless relay networks makes it vulnerable to eavesdropping [73]. Thus, maintaining the secrecy of the transmitted information in the presence of an eavesdropper is important [69]. The secrecy capacity is defined as the difference between the capacity of the link from the source to destination and the capacity of the wiretap link from the source to the eavesdropper. Cryptographic techniques can be used in the application layer to improve the security of wireless communications [70]. Physical layer security which exploits the physical characteristics of the wireless channel can also be employed [71].

In [72], the impact of fading on the secrecy capacity of a two user network with a potential eavesdropper was considered. It was shown that information security is achievable even when the average signal to noise ratio of the eavesdropper links is better than that of the user links. Physical layer security in an untrusted relay network was first investigated in [74] where the relay was treated as a potential eavesdropper.

A jamming signal was used to achieve a non zero secrecy capacity. In [75], the secrecy performance of one-way communications for decode and forward (DF) and amplify and forward (AF) EH relays was studied. It was shown that DF provides better secrecy than AF. The secrecy capacity of a one-way untrusted relaying network was analyzed in [76] for PS and TS at the relay and it was shown that PS outperforms TS.

Two-way relaying can provide a higher spectral efficiency than one-way relaying. The secrecy performance of a two-way EH-based relay network in the presence of an eavesdropper was studied in [77]. The optimal TS and PS ratios were derived for a high signal to noise ratio using an iterative method. The ratios were adjusted adaptively according to the instantaneous channel state information. It was shown that the proposed approach provides near optimal secrecy capacity in the case of unknown wiretap channels. In [78], secrecy capacity and energy efficiency were jointly considered in a two-way untrusted relay network. The probability of successful eavesdropping was derived in [79] for a two-way three-step EH DF relay network with independent κ-μ shadowed fading on all links. The results obtained show that the secrecy capacity can be improved by allocating more power for information decoding over a small reception time. In [80], the intercept probability was derived for multiple eavesdroppers in a two-way DF EH relay network. The impact of the relay activation power threshold and power splitting factor on the secrecy capacity was also studied. Antenna selection considering the harvested energy was employed in [81] to maximize the secrecy capacity of a two-way communication network. The users communicate through two multi-antenna time-switching relays in the presence of an eavesdropper. It was shown that the secrecy performance can be improved with equal user transmit power.

The secrecy capacity can be significantly improved with cooperative jamming. Two types of jamming signals have been considered in the literature to improve the physical layer security of wireless communication networks. The first is friendly jamming (FJ) where the jamming signal is known at the users [82]. The second is Gaussian noise jamming (GNJ) where the users have no a priori information about the jamming signal and so it is considered as interference [83]. FJ and GNJ can improve the secrecy capacity, but FJ provides better secrecy performance because the jamming signal can be cancelled by the users. Two secure SWIPT relaying strategies were presented in [78] for two-way untrusted AF EH relay networks to maximize the secrecy capacity and energy efficiency. In both strategies, the source transmits a jamming signal to charge the relay and maintain information security. In [84], communications in the presence of two eavesdroppers was examined. A friendly jammer is employed that harvests energy from the user signals. One eavesdropper is located near the transmitting user while the other is located near the jammer. The eavesdroppers cooperate to detect user signals and reduce the effects of jamming. The jamming signal power was optimized to maximize the secrecy capacity and energy efficiency of the network.

A separate jammer was employed in [85] to secure two-way communications in an EH-based relay network. A lower bound on the secrecy capacity in the high signal-to-noise ratio regime was derived. It was shown that one-way and the two-way communications outperforms GNJ and no jamming. In [86], the secrecy capacity of one-way untrusted relay communications was maximized by jointly optimizing the power allocation at the transmitter and jammer with an EH threshold at the relay.

In [87], destination-aided jamming was employed to prevent untrusted EH relays from eavesdropping. An energy-aware distributed beamforming scheme was proposed and shown to improve secrecy performance. The secrecy capacity was improved in [88] with a strategy that selects the jammer and relay nodes from multiple friendly but selfish intermediate nodes where the jammer broadcasts Gaussian noise. Power allocation to the intermediate nodes was determined based on price competition. The secrecy capacity of the network was maximized while optimizing the profit of intermediate nodes.

Multiple friendly jammers were considered in [33] for a two-way untrusted relay system. The secrecy capacity was improved by optimizing the jamming power allocated to friendly jammers. In [89], a network with multiple relay-user pairs communicating in the presence of multiple eavesdroppers was examined. A joint relay-user pair and friendly jammer selection scheme was proposed to improve the secrecy capacity. Round-robin and conventional relay-user pair selection schemes were considered as benchmarks. The secrecy capacity of the proposed approach was shown to outperform these schemes as the number of relay-user pairs and number of eavesdroppers increase. Adaptive cooperative jamming was proposed in [90] for an EH relay network in the presence of multiple eavesdroppers. The power allocation factor was adjusted to maximize the secrecy capacity. Optimal PS and TS ratios were derived in [91] to maximize the secrecy capacity in a two-way EH relay network in the presence of multiple eavesdroppers and a friendly jammer. It was shown that PS at the relay provides better protection against eavesdropping than TS. In [92], hybrid PS and TS was employed in the intermediate nodes of a two-way relay network with partial relay selection. A jammer was located near the eavesdropper to improve the secrecy capacity. Reliable secure communications was shown to be guaranteed with an appropriate choice of parameters.

In this chapter, the physical layer security of a two-way communication system with an EH relay is investigated. An eavesdropper is present so a friendly jammer is employed to improve the secrecy. Joint optimization of the power allocated to two users, a relay, and a jammer in the presence of an eavesdropper is presented. This has not been considered in the literature. In addition, the effect of imperfect jamming power cancellation is investigated. The main contributions of this chapter are as follows.

1. The power splitting factor and transmit powers of the two users and jammer are jointly optimized to maximize the secrecy capacity.

2. The optimization problem is not convex so it is transformed into a convex problem using geometric programming (GP). The single condensation method is employed to convert the objective function into GP format.

3. The effect of the jamming signal on the two users and Imperfect cancellation of the jamming signal is considered. This has not been examined previously in the literature.

4. The secrecy capacity of the system is compared to the case without a jammer, and results are presented for different relay, jammer, and eavesdropper positions.

The remainder of this chapter is organized as follows. The system model is presented in Section 3.2. The secrecy capacity for the two-way relay network is derived in Section 3.3 and the optimization problem is converted to a convex form. Section

3.4 presents the simulation results and finally, some concluding remarks are given in Section 3.5.

3.2 System Model

Fig. 3.1 presents the system model of a two-way relay network connecting two users A and B. This model includes a trusted relay R, a friendly jammer J, and an eavesdropper E. Each node operates in half-duplex mode and has a single antenna. The eavesdropper is randomly located near the relay to listen to the signals transmitted from and received by the relay. The A-R, E-R, A-E, B-E, R-E, J-R, and J-E channel links are denoted by h_{AR}, h_{BR}, h_{AE}, h_{BE}, h_{RE}, h_{JR}, and h_{JE}, respectively. Rayleigh fading is assumed so all channel coefficients are Rayleigh random variables. Further, channel reciprocity is assumed so that $h_{ij} = h_{ji}$. The channel gains, $|h_{ij}|^2$, $\{i,j\} \in \{A,B,R,J,E\}, i \neq j$, are then exponentially distributed random variables with mean λ. The additive white Gaussian noise (AWGN) at A, B, R, and E, denoted n_A, n_B,n_R, and n_E, respectively, has zero mean and variance σ^2. The notation used in this chapter is given in Table 3.1.

Table 3.1: Notation

Symbol	**Description**
A and B	Users
R	Relay

Continued on next page

Table 3.1 – *Continued from previous page*

Symbol	**Description**
J	Jammer
E	Eavesdropper
h_{ij}	Channel between node i and node j
$\lvert h_{ij}\rvert^2$	Channel gain between node i and node j
n_i	Additive white Gaussian noise at node i
σ^2	Noise variance
x_i	Signal transmitted by node i
y_i	Signal received at node i
P_A	Transmit power of node A
P_B	Transmit power of node B
P_R	Transmit power of node R
P_J	Transmit power of node J
P_T	Total power constraint
$\mathbf{E}[.]$	Expected value
y_{Re}	Energy harvesting signal at the relay
y_{Ri}	Information retrieval signal at the relay
θ	Power splitting factor
E_H	Harvested energy
ζ	Energy conversion efficiency
T	Total transmission time
m	Path loss exponent

Continued on next page

Table 3.1 – *Continued from previous page*

Symbol	**Description**
Φ	Jamming signal cancellation factor
y_R	Information retrieval signal at the relay after jamming cancellation
$y_E^{(1)}$	Received signal at E in the first phase
$y_E^{(2)}$	Received signal at E in the second phase
$SNR_{E,A}^{(1)}$	SNR at E for x_B sent to A in the first phase
$SNR_{E,B}^{(1)}$	SNR at E for x_A sent to B in the first phase
$SNR_{E,A}^{(2)}$	SNR at E for x_B sent to A in the second phase
$SNR_{E,B}^{(2)}$	SNR at E for x_A sent to B in the second phase
SNR_A	SNR at A
SNR_B	SNR at B
R_A	Achievable rate at A
R_B	Achievable rate at B
$R_E^{(1)}$	Achievable rate at E in the first phase
$R_E^{(2)}$	Achievable rate at E in the second phase
R_E	Achievable rate at E for both phases
C_A	Secrecy capacity at A
C_B	Secrecy capacity at B
C_S	Secrecy capacity

The relay network requires two phases to complete the transmission between A

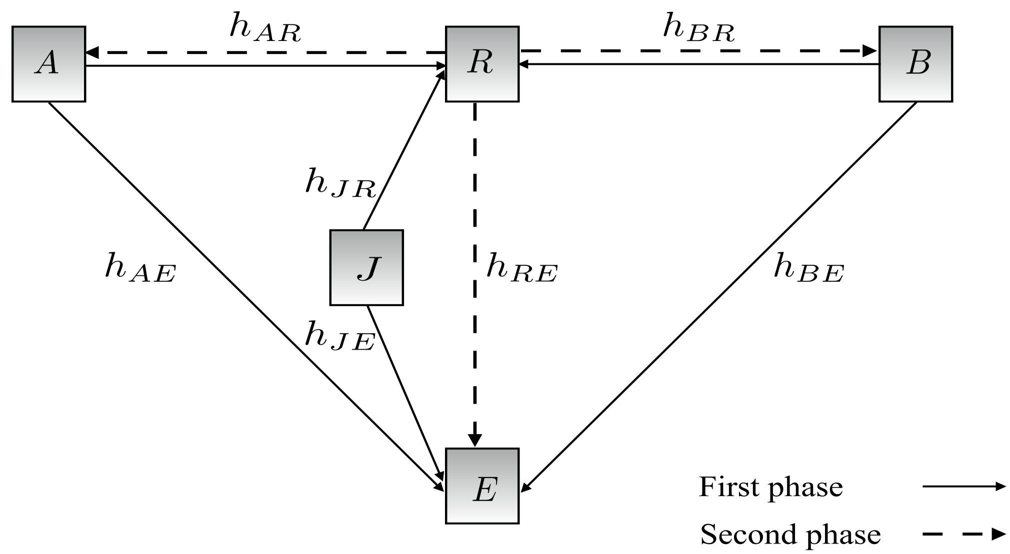

Figure 3.1: System model of the two-way wireless relay network with a jammer and eavesdropper.

and B as shown in Fig. 3.2. In the first phase, A and B send their signals x_A and x_B with $\mathbf{E}[|x_A|^2] = \mathbf{E}[|x_B|^2] = 1$ and transmission powers P_A and P_B, respectively, to R. At the same time, the jammer broadcasts a jamming signal, x_J with $\mathbf{E}[|x_J|^2] = 1$, to make it more difficult for the eavesdropper to overhearing the signals from A and B.

The relay does not have a fixed power supply and relies on PS to harvest energy from the user and jamming signals. The received signal at the relay has two parts corresponding to energy harvesting and information retrieval. The energy harvesting part is

$$y_{Re} = \sqrt{\theta P_A} h_{AR} x_A + \sqrt{\theta P_B} h_{BR} x_B + \sqrt{\theta P_J} h_{JR} x_J, \tag{3.1}$$

where the power splitting factor is $\theta, 0 \leq \theta \leq 1$, and the additive noise at the relay,

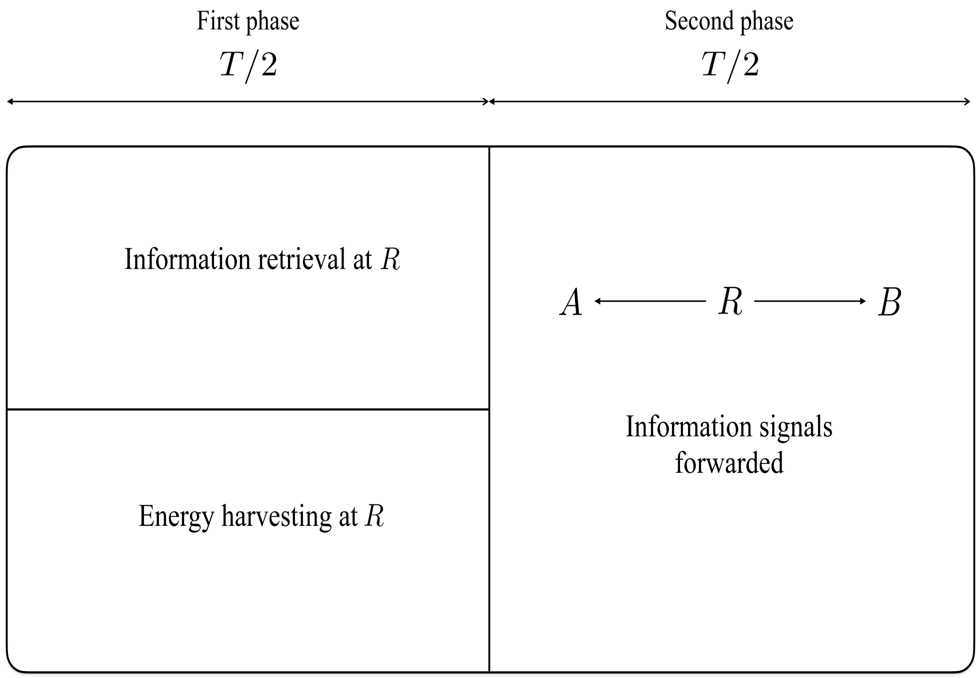

Figure 3.2: Transmission time frame for power splitting in the two-way relay network.

n_R, is assumed to be much less than the other terms in (3.1) and so can be neglected [49]. The harvested energy is

$$E_H = \frac{T}{2}\zeta\theta\left(P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2\right), \tag{3.2}$$

where $\zeta, 0 < \zeta \leq 1$, is the energy conversion efficiency. The transmit power of the relay in the second phase is then

$$P_R = \frac{E_H}{T/2} = \zeta\theta E_R, \tag{3.3}$$

where $E_R = P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2$. The information retrieval part of the received signal is

$$y_{Ri} = \sqrt{(1-\theta)P_A}h_{AR}x_A + \sqrt{(1-\theta)P_B}h_{BR}x_B + \sqrt{(1-\theta)P_J}h_{JR}x_J + n_R. \tag{3.4}$$

The signal from the jammer can be assumed to be known at A and B as in [33] so that the term $\sqrt{(1-\theta)P_J}h_{JR}x_J$ in (3.4) can be canceled from y_{Ri} at the relay [50, 51]. However, in this chapter imperfect cancellation of this signal at the relay is assumed. A cancellation factor Φ, $0 \leq \Phi \leq 1$, is used to indicate the fraction of the jamming signal that remains. This fraction is amplified and forwarded to the users A and B by the relay. If $\Phi = 0$, then the jamming signal is perfectly canceled and if $0 < \Phi$, a fraction of the jamming signal, $\Phi \times P_J$, is not canceled. The value of Φ depends on the ability of the relay receiver circuitry to cancel the jamming signal and the CSI of the link between R and J. The information retrieval signal after jamming cancellation is then

$$y_R = \sqrt{(1-\theta)P_A}h_{AR}x_A + \sqrt{(1-\theta)P_B}h_{BR}x_B + \Phi\sqrt{(1-\theta)P_J}h_{JR}x_J + n_R. \tag{3.5}$$

The received signal at E during the first phase is

$$y_E^{(1)} = \sqrt{P_A}h_{AE} + \sqrt{P_B}h_{BE} + \sqrt{P_J}h_{JE} + n_E \tag{3.6}$$

The SNR at E for x_B sent to A during the first phase is

$$SNR_{E,A}^{(1)} = \frac{P_B|h_{BE}|^2}{P_A|h_{AE}|^2 + P_J|h_{JE}|^2 + \sigma^2} \tag{3.7}$$

and the SNR at E for x_A sent to B during this phase is

$$SNR_{E,B}^{(1)} = \frac{P_A|h_{AE}|^2}{P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2} \tag{3.8}$$

Since the eavesdropper does not know the jamming signal, x_J is additional noise which reduces the SNR at E. In the second phase, the relay uses the harvested energy to amplify and forward the received signal to the users. The transmitted signal at the relay is

$$\begin{aligned} x_R &= \frac{\sqrt{P_R}}{\sqrt{\widetilde{\theta}\,[P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2] + \sigma^2}} \quad y_R & (3.9) \\ &= \sqrt{\frac{P_R}{\widetilde{\theta}E_R + \sigma^2}} \quad y_R, & (3.10) \end{aligned}$$

where $\sqrt{\frac{P_R}{\widetilde{\theta}E_R + \sigma^2}}$ is the amplifier gain of the relay and $\widetilde{\theta} = 1 - \theta$. The received signal at A in the second phase is

$$\begin{aligned}
y_A &= h_{AR}x_R + n_A && (3.11)\\
&= \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_B}h_{AR}h_{BR}}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}x_B}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_A}|h_{AR}|^2}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}x_A}_{\text{information signal}}\\
&+ \underbrace{\Phi\frac{\sqrt{\widetilde{\theta}P_R P_J}h_{AR}h_{JR}}{\sqrt{\widetilde{\theta}E_R + \sigma^2}} + \frac{\sqrt{P_R}h_{AR}n_R}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}}_{\text{noise}} + n_A, && (3.12)
\end{aligned}$$

and the received signal at B in the second phase is

$$\begin{aligned}
y_B &= h_{BR}x_R + n_B && (3.13)\\
&= \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_A}h_{AR}h_{BR}}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_B}|h_{BR}|^2}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}x_B}_{\text{information signal}}\\
&+ \underbrace{\Phi\frac{\sqrt{\widetilde{\theta}P_R P_J}h_{BR}h_{JR}}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}x_J + \frac{\sqrt{P_R}h_{BR}n_R}{\sqrt{\widetilde{\theta}E_R + \sigma^2}}}_{\text{noise}} + n_B\,. && (3.14)
\end{aligned}$$

Self interference cancellation at A and B is assumed so they can cancel their own signals [35, 36]. Let

$$\gamma_A = \frac{P_A|h_{AR}|^2}{\sigma^2}, \tag{3.15}$$

$$\gamma_B = \frac{P_B|h_{BR}|^2}{\sigma^2}, \tag{3.16}$$

$$\gamma_J = \frac{P_J|h_{JR}|^2}{\sigma^2}, \tag{3.17}$$

$$\overline{\gamma} = \gamma_A + \gamma_B + \gamma_J = \frac{E_R}{\sigma^2}. \tag{3.18}$$

The SNR at A is then

$$\begin{aligned} SNR_A &= \frac{\dfrac{\widetilde{\theta} P_B P_R |h_{BR}|^2 |h_{AR}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{P_R|h_{AR}|^2\sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{\Phi^2 \widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{AR}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2} \\ &= \frac{\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B}{\left(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta}\right)\overline{\gamma} + 1}, \end{aligned} \tag{3.19}$$

and the achievable rate at A is [43]

$$R_A = \frac{T}{2}\log_2\left(1 + SNR_A\right). \tag{3.20}$$

The corresponding SNR at B is

$$\begin{aligned} SNR_B &= \frac{\dfrac{\widetilde{\theta} P_A P_R |h_{AR}|^2 |h_{BR}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{P_R|h_{BR}|^2\sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{\Phi^2 \widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{BR}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2} \\ &= \frac{\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A}{\left(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta}\right)\overline{\gamma} + 1}, \end{aligned} \tag{3.21}$$

and the achievable rate is

$$R_B = \frac{T}{2}\log_2\left(1 + SNR_B\right). \tag{3.22}$$

The signal received at E during the second phase is

$$y_E^{(2)} = h_{RE}x_R + n_E, \tag{3.23}$$

$$= \underbrace{\frac{\sqrt{\widetilde{\theta} P_R P_A} h_{AR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta} P_R P_B} h_{BR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_B}_{\text{information signal}}$$

$$\underbrace{+ \Phi \frac{\sqrt{\widetilde{\theta} P_R P_J} h_{JR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_J + \frac{\sqrt{P_R} h_{RE} n_R}{\sqrt{\widetilde{\theta} E_R + \sigma^2}}}_{\text{noise}} + n_E\,. \tag{3.24}$$

The SNR at E for x_A sent to B during the second phase through the main link $A \to R \to B$ is

$$SNR_{E,B}^{(2)} \tag{3.25}$$

$$= \frac{\dfrac{\widetilde{\theta} P_R P_A |h_{AR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{\widetilde{\theta} P_R P_B |h_{BR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{P_R |h_{RE}|^2 \sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \Phi^2 \dfrac{\widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2}$$

$$= \frac{\zeta \theta \widetilde{\theta} \overline{\gamma} \gamma_A |h_{RE}|^2}{\overline{\gamma}\left[\zeta \theta |h_{RE}|^2 (\widetilde{\theta} \gamma_B + \widetilde{\theta} \gamma_J \Phi^2 + 1) + \widetilde{\theta}\right] + 1}. \tag{3.26}$$

The SNR at E when x_B is sent to A in the second phase through the link $B \to R \to A$

is

$$
\begin{aligned}
&SNR_{E,A}^{(2)} \\
&= \frac{\dfrac{\widetilde{\theta} P_R P_B |h_{BR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{\widetilde{\theta} P_R P_A |h_{AR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{P_R |h_{RE}|^2 \sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \Phi^2 \dfrac{\widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{RE}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2} \\
&= \frac{\zeta \theta \widetilde{\theta} \overline{\gamma} \gamma_B |h_{RE}|^2}{\overline{\gamma} \left[\zeta \theta |h_{RE}|^2 (\widetilde{\theta} \gamma_A + \widetilde{\theta} \gamma_J \Phi^2 + 1) + \widetilde{\theta} \right] + 1}. \qquad (3.27)
\end{aligned}
$$

The achievable rate at E for both phases is $R_E = R_E^{(1)} + R_E^{(2)}$. The first term $R_E^{(1)} = \frac{T}{2} \log_2 \left(1 + SNR_{E,i}^{(1)}\right)$ is the achievable rate during the first phase and $R_E^{(2)} = \frac{T}{2} \log_2 \left(1 + SNR_{E,i}^{(2)}\right)$ is the achievable rate during the second phase for $i \in \{A, B\}$.

3.3 Optimization Problem Formulation

The secrecy capacity with an eavesdropper is defined as the difference between the secrecy capacity of the main link and that of the wiretap link [43]. In the network, the total transmit power is restricted by a power constraint P such that $P_A + P_B + P_J \leq P_T$. Under this constraint, the optimal power allocation to A and B and the optimal power splitting factor are found to maximize the sum of the secrecy capacities at A and B. The secrecy capacity at A and B is $C_{S,A} = [R_A - R_{E,A}]^+$ and $C_{S,B} = [R_B - R_{E,B}]^+$ [93], respectively, where $[x]^+ = \max(0, x)$. The secrecy capacity is

$$
\begin{aligned}
C_S &= C_{S,A} + C_{S,B}, \qquad (3.28) \\
&= [R_A - R_{E,A}]^+ + [R_B - R_{E,B}]^+ . \qquad (3.29)
\end{aligned}
$$

The optimization problem can be formulated as

$$\max_{\theta,\widetilde{\theta},P_A,P_B,P_J} \quad C_S$$

$$P_A + P_B + P_J \leq P_T$$

$$\theta + \widetilde{\theta} \leq 1$$

$$\theta, \widetilde{\theta}, P_A, P_B, P_J \geq 0$$

From (3.29), there are four cases to consider to maximize the secrecy capacity.

3.3.1 Case I: $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$

In this case, the secrecy capacity at A is [43]

$$\begin{aligned} C_{S,A} &= R_A - R_{E,A}, \\ &= \frac{T}{2} \log_2 \left[\frac{1 + SNR_A}{\left(1 + SNR_{E,A}^{(1)}\right)\left(1 + SNR_{E,A}^{(2)}\right)} \right], \end{aligned} \tag{3.30}$$

where

$$1 + SNR_A =$$
$$\frac{\overline{\gamma}\zeta\theta|h_{AR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_B\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1}{\overline{\gamma}(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta}) + 1}, \tag{3.31}$$
$$1 + SNR_{E,A}^{(1)} =$$
$$\frac{P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}{P_A|h_{AE}|^2 + P_J|h_{JE}|^2 + \sigma^2}, \tag{3.32}$$
$$1 + SNR_{E,A}^{(2)} =$$
$$\frac{\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1}{\overline{\gamma}\left[\zeta\theta|h_{RE}|^2(\widetilde{\theta}\gamma_A + \Phi^2\widetilde{\theta}\gamma_J + 1) + \widetilde{\theta}\right] + 1}. \tag{3.33}$$

and the secrecy capacity at B is

$$\begin{aligned} C_{S,B} &= R_B - R_{E,B}, \\ &= \frac{T}{2}\log_2\left[\frac{1 + SNR_B}{\left(1 + SNR_{E,B}^{(1)}\right)\left(1 + SNR_{E,B}^{(2)}\right)}\right], \end{aligned} \tag{3.34}$$

where

$$1 + SNR_B = \frac{\zeta\theta\overline{\gamma}|h_{BR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_A\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1}{\overline{\gamma}(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta}) + 1}, \tag{3.35}$$

$$1 + SNR_{E,B}^{(1)} = \frac{P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}{P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}, \tag{3.36}$$

$$1 + SNR_{E,B}^{(2)} = \frac{\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1}{\overline{\gamma}\left[\theta\zeta|h_{RE}|^2\left(\widetilde{\theta}\gamma_B + \Phi^2\widetilde{\theta}\gamma_J + 1\right) + \widetilde{\theta}\right] + 1}. \tag{3.37}$$

Then

$$\begin{aligned} C_S &= C_{S,A} + C_{S,B}, \\ &= \frac{T}{2}\log_2 \frac{w\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}{z\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}, \end{aligned} \tag{3.38}$$

where

$$\begin{aligned} w(\theta,\widetilde{\theta}, P_A, P_B, P_J) = &\left(\overline{\gamma}\zeta\theta|h_{AR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_B\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1\right) \\ &\left(P_A|h_{AE}|^2 + P_J|h_{JE}|^2 + \sigma^2\right)\left(P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2\right) \\ &\left(\zeta\theta\overline{\gamma}|h_{BR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_A\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1\right) \\ &\left(\overline{\gamma}\left[\theta\zeta|h_{RE}|^2\left(\widetilde{\theta}\gamma_B + \Phi^2\widetilde{\theta}\gamma_J + 1\right) + \widetilde{\theta}\right] + 1\right) \\ &\left(\overline{\gamma}\left[\zeta\theta|h_{RE}|^2(\widetilde{\theta}\gamma_A + \Phi^2\widetilde{\theta}\gamma_J + 1) + \widetilde{\theta}\right] + 1\right) \end{aligned} \tag{3.39}$$

and

$$z(\theta,\widetilde{\theta},P_A,P_B,P_J) = \left(P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2\right)^2$$
$$\left(\overline{\gamma}(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta}) + 1\right)$$
$$\left(\overline{\gamma}(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta}) + 1\right)$$
$$\left(\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1\right)^2. \tag{3.40}$$

The corresponding optimization problem is

$$\underset{\theta,\widetilde{\theta},P_A,P_B,P_J}{\text{minimize}} \quad \frac{z}{w} \tag{3.41a}$$
$$\text{subject to} \quad P_A + P_B + P_J \leq P_T, \tag{3.41b}$$
$$\theta + \widetilde{\theta} \leq 1, \tag{3.41c}$$
$$\theta, \widetilde{\theta}, P_A, P_B, P_J \geq 0 \tag{3.41d}$$

A Geometric programming (GP) problem has the form [40]

$$\text{minimize} \quad f_0(x) \tag{3.42a}$$
$$\text{subject to} \quad f_i(x) \leq 0, \quad i = 1, \ldots, m, \tag{3.42b}$$
$$g_i(x) = 1, \quad i = 1, \ldots, p \tag{3.42c}$$

where the f_i are polynomial functions, g_i are monomials, and x_i are the optimization variables. A real valued function f of the form $f(x) = cx_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ where $c > 0$ and $a_i \in \mathbf{R}$ is a monomial function. The sum of two or more monomials is a polynomial function such that $f(x) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} x_2^{a_{2k}} \ldots x_n^{a_{nk}}$ where $c_k > 0$.

The constraints in (3.41b) and (3.41c) are polynomials. When the objective function and the constraints are polynomials, the problem can be converted into a convex problem by transforming it into GP form. However, the objective function is not a polynomial since it is a ratio of two polynomials. To overcome this issue, a monomial approximation of $w(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ is obtained using the single condensation method (SCM) for GP [41]. This method approximates the denominator of the ratio of polynomials with a monomial function. The numerator of the ratio is left unchanged (a polynomial), hence the term single. In the above optimization problem, $w(\mathbf{x}) = \sum_i u_i(\mathbf{x})$ is the sum of i monomials which is a polynomial by definition. Then, the monomial approximation of $w(\mathbf{x})$, where $\mathbf{x} = \left[\theta, \widetilde{\theta}, P_A, P_B, P_J\right]^T$, using SCM is

$$\overline{w}(\mathbf{x}) = \prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i}\right)^{\alpha_i}, \tag{3.43}$$

such that $w(\mathbf{x}) \geq \overline{w}(\mathbf{x})$. For a given $\mathbf{x}$, the α_i in $w(\mathbf{x})$ are obtained such that

$$\alpha_i = \frac{u_i(\mathbf{x})}{w(\mathbf{x})}, \tag{3.44}$$

and $\overline{w}(\mathbf{x})$ is substituted for $w(\mathbf{x})$ in (3.41a). The resulting objective function after the approximation is a polynomial (posynomial) function. The accuracy of the approximation was determined by calculating the difference between the value of $w(\mathbf{x})$ and $\overline{w}(\mathbf{x})$ at the solution point $\mathbf{x}$. The maximum difference is 0.0000724. GP is used to obtain a nonlinear but convex optimization problem with convex objective and inequality constraint functions and linear equality constraints. This is achieved via a logarithmic change of variables and a logarithmic transformation of the objective function and constraints. The resulting convex problem can be solved efficiently using CVX solvers [40].

Since the optimal solution may be far from the initial guess $\mathbf{x}_0$ used in the above approximation, an iterative approach is employed to solve this problem. If the current optimal solution, $\mathbf{x}_{k+1}$, agrees with the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then use $\mathbf{x}_{k+1}$ to calculate $\overline{w}(\mathbf{x}_{k+1})$ and solve the GP problem again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, proceed to the next case.

3.3.2 Case II: $C_{S,A} \geq 0$ and $C_{S,B} \leq 0$

In this case

$$\begin{aligned} C_S &= C_{S,A}, && (3.45)\\ &= R_A - R_{E,A}, && (3.46)\\ &= \frac{T}{2}\log_2\left[\frac{1+SNR_A}{\left(1+SNR_{E,A}^{(1)}\right)\left(1+SNR_{E,A}^{(2)}\right)}\right], && (3.47)\end{aligned}$$

and

$$1 + SNR_A = \frac{\overline{\gamma}\zeta\theta|h_{AR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_B\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1}{\overline{\gamma}(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta}) + 1}, \tag{3.48}$$

$$1 + SNR_{E,A}^{(1)} = \frac{P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}{P_A|h_{AE}|^2 + P_J|h_{JE}|^2 + \sigma^2}, \tag{3.49}$$

$$1 + SNR_{E,A}^{(2)} = \frac{\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1}{\overline{\gamma}\left[\zeta\theta|h_{RE}|^2(\widetilde{\theta}\gamma_A + \Phi^2\widetilde{\theta}\gamma_J + 1) + \widetilde{\theta}\right] + 1} \tag{3.50}$$

are substituted in (3.47) to get

$$C_S = \frac{T}{2}\log_2\frac{w\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}{z\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}, \tag{3.51}$$

such that

$$\begin{aligned} w(\theta, \widetilde{\theta}, P_A, P_B, P_J) = &\left(\overline{\gamma}\zeta\theta|h_{AR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_B\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1\right) \\ &\left(P_A|h_{AE}|^2 + P_J|h_{JE}|^2 + \sigma^2\right) \\ &\left(\overline{\gamma}\left[\zeta\theta|h_{RE}|^2(\widetilde{\theta}\gamma_A + \Phi^2\widetilde{\theta}\gamma_J + 1) + \widetilde{\theta}\right] + 1\right), \end{aligned} \tag{3.52}$$

and

$$z(\theta, \widetilde{\theta}, P_A, P_B, P_J) = \left(\overline{\gamma}(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta}) + 1\right)$$
$$(P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2) \tag{3.53}$$
$$\left(\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1\right).$$

The optimization problem is the same as in Case I using $w(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ and $z(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ in (3.52) and (3.53), respectively. The monomial approximation $\overline{w}(\mathbf{x})$ is updated every iteration using the solution from the previous iteration as long as $C_{S,A} \geq 0$ and $C_{S,B} \leq 0$ hold. If not, proceed to the next case.

3.3.3 Case III: $C_{S,A} \leq 0$ and $C_{S,B} \geq 0$

In this case

$$C_S = C_{S,B}, \tag{3.54}$$
$$= R_B - R_{E,B}, \tag{3.55}$$
$$= \frac{T}{2}\log_2\left[\frac{1 + SNR_B}{\left(1 + SNR_{E,B}^{(1)}\right)\left(1 + SNR_{E,B}^{(2)}\right)}\right], \tag{3.56}$$

and

$$1 + SNR_B = \frac{\zeta\theta\overline{\gamma}|h_{BR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_A\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1}{\overline{\gamma}(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta}) + 1}, \tag{3.57}$$

$$1 + SNR_{E,B}^{(1)} = \frac{P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}{P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2}, \tag{3.58}$$

$$1 + SNR_{E,B}^{(2)} = \frac{\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1}{\overline{\gamma}\left[\theta\zeta|h_{RE}|^2\left(\widetilde{\theta}\gamma_B + \Phi^2\widetilde{\theta}\gamma_J + 1\right) + \widetilde{\theta}\right] + 1}. \tag{3.59}$$

are substituted in (3.56) to get

$$C_S = \frac{T}{2}\log_2\frac{w\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}{z\left(\theta, \widetilde{\theta}, P_A, P_B, P_J\right)}, \tag{3.60}$$

such that

$$\begin{aligned} w(\theta, \widetilde{\theta}, P_A, P_B, P_J) = &\left(\zeta\theta\overline{\gamma}|h_{BR}|^2\left(1 + \Phi^2\widetilde{\theta}\gamma_J + \gamma_A\widetilde{\theta}\right) + \overline{\gamma}\widetilde{\theta} + 1\right) \\ &\left(P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2\right) \\ &\left(\overline{\gamma}\left[\theta\zeta|h_{RE}|^2\left(\widetilde{\theta}\gamma_B + \Phi^2\widetilde{\theta}\gamma_J + 1\right) + \widetilde{\theta}\right] + 1\right) \end{aligned} \tag{3.61}$$

and

$$\begin{aligned} z(\theta, \widetilde{\theta}, P_A, P_B, P_J) = &\left(\overline{\gamma}(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta}) + 1\right) \\ &(P_A|h_{AE}|^2 + P_B|h_{BE}|^2 + P_J|h_{JE}|^2 + \sigma^2) \\ &\left(\zeta\theta\widetilde{\theta}\overline{\gamma}|h_{RE}|^2(\gamma_A + \gamma_B + \Phi^2\gamma_J) + \overline{\gamma}(\zeta\theta|h_{RE}|^2 + \widetilde{\theta}) + 1\right) \end{aligned} \tag{3.62}$$

The optimization problem is the same as in Case I using $w(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ and $z(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ in (3.61) and (3.62), respectively. The monomial approximation $\overline{w}(\mathbf{x})$ is updated every iteration using the solution from the previous iteration as long as $C_{S,A} \leq 0$ and $C_{S,B} \geq 0$ hold. If not, proceed to the next case.

3.3.4 Case IV: $C_{S,A} \leq 0$ and $C_{S,B} \leq 0$

In this case, the secrecy capacity is $C_S = 0$ because the secrecy capacity of the wiretapped links A to E and B to E is higher than the secrecy capacity at A and B.

The algorithm to solve the optimization problem and obtain the optimal values $\left[\theta^*, \widetilde{\theta}^*, P_A^*, P_B^*, P_J^*\right]^T$ is summarized in Algorithm 1.

Algorithm 1 Optimization of the Secrecy Capacity C_S

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, $k = 1$

1: **while** $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**
2: Calculate the monomial approximation $\overline{w}$ for w using the single condensation method (SCM) at $\mathbf{x} = \left[\theta_k, \widetilde{\theta}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$
3: $k = k + 1$
4: Solve the optimization problem in (3.41) using $\overline{w}$ to find $\left[\theta_{k+1}, \widetilde{\theta}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}\right]$
5: Using the solution in step 4, calculate $C_{S,A}$ and $C_{S,B}$
6: **if** $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**
7: Go to step 1
8: **else**
9: Continue to Cases II, III, and IV in turn
10: **end if**
11: Find the optimal $\left[\theta_k, \widetilde{\theta}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]$
12: **end while**
13: Assign $C_S = C_{S,k}$

3.4 Results and Discussion

In this section, the secrecy capacity of a two-way relay network with a jammer to reduce the SNR at the eavesdropper is evaluated. There is no line of sight between A and B so they rely on R to communicate. The simulation parameters are as follows unless noted otherwise. The noise variance is $\sigma^2 = 10^{-3}$, the energy conversion efficiency is $\zeta = 0.5$, $T = 1$, $\Phi = 0$, and the optimization tolerance is $\epsilon = 0.001$. The channel gains $|h_{AR}|^2$, $|h_{BR}|^2$, $|h_{JR}|^2$, and $|h_{JE}|^2$ are exponential random variables with mean $\lambda = 1$, $|h_{RE}|^2$ and $|h_{BE}|^2$ are exponential random variables with mean λ_{Eve}, and $|h_{AE}|^2$ is an exponential random variable with mean $\frac{1}{\lambda_{Eve}}$, $\lambda_{Eve} \in \{1, 2, 3\}$. All locations are normalized to the distance between A and B. The positions of A and B are $(0, 0)$ and $(1, 0)$, respectively. R is assumed to be at the midpoint, (0.5, 0), J at (0.5, -0.5), $P_T = 10$ dB, and $P_J = 0.1P_T$ unless noted otherwise.

Fig. 3.3 presents the secrecy capacity as a function of the total transmit power for three values of λ_{Eve}. This shows that the secrecy capacity increases as the total transmit power increases for all values of λ_{Eve}. With a total transmit power of 15 dB, the difference in secrecy capacity between $\lambda_{Eve} = 1$ and 3 is 1.53 bits per channel use. Fig. 3.4 presents the secrecy capacity as a function of the power splitting factor, θ, for $P_T = 10$ and 20 dB and three values of λ_{Eve}. As the transmit power increases, the secrecy capacity improves and the optimal value of θ decreases. At smaller values of θ, there is less power available at the relay for EH. Hence, less power is available for the relay to forward the received signals to the users. On the other hand, as θ increases beyond the optimal value, there is sufficient harvested energy, but the signal received at the relay is poor. When this noisy signal is amplified and forwarded, the secrecy capacity is low. For the same value of λ_{Eve}, as P_T increases, the optimal value

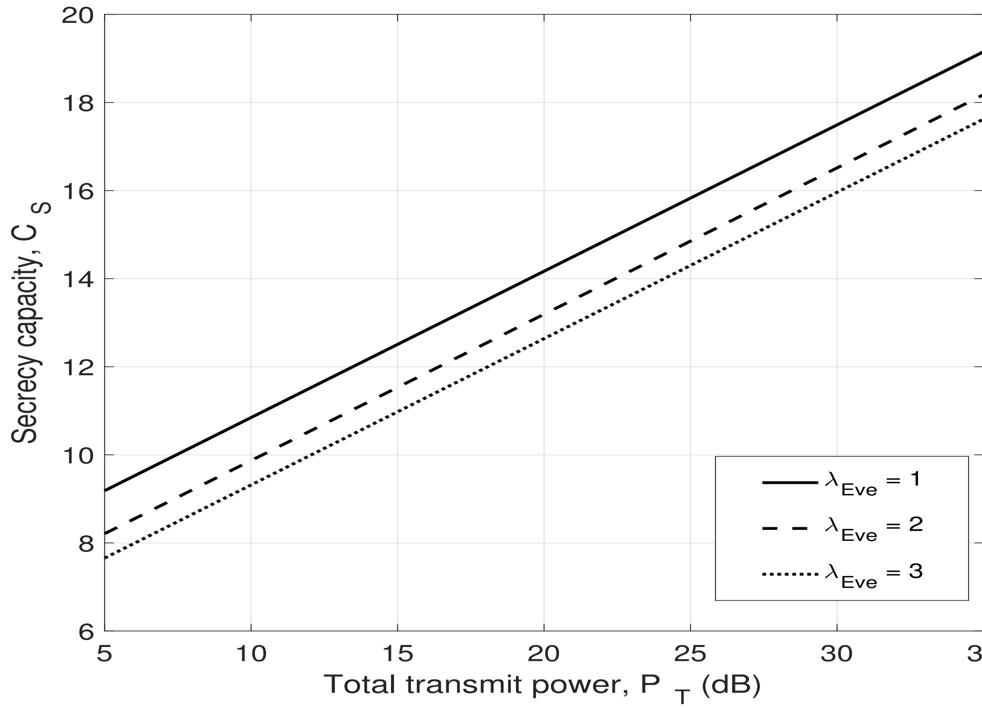

Figure 3.3: Secrecy capacity versus the total transmit power for three values of λ_{Eve}.

of the power splitting factor, θ_{opt}, decreases so a smaller portion of the received signal is required to harvest energy at the relay. For $\lambda_{Eve} = 1$, $\theta_{opt} = 0.73$ and 0.71 for $P_T = 10$ and 20 dB, respectively.

The harvested energy, E_H, at the relay as a function of the total transmit power is shown in Fig. 3.5 for different values of θ and jamming power P_J as a fraction of P_T. This indicates that the harvested energy increases as the total transmit power increases in all cases. As θ increases, a larger portion of the received signal is used for energy harvesting so more energy is available at the relay. Increasing the jamming power for a given value of θ will increase the harvested energy but not the secrecy capacity as will be shown later for the values of θ considered. The optimal jamming power allocation is shown in Fig. 3.6 as a function of the total transmit power for

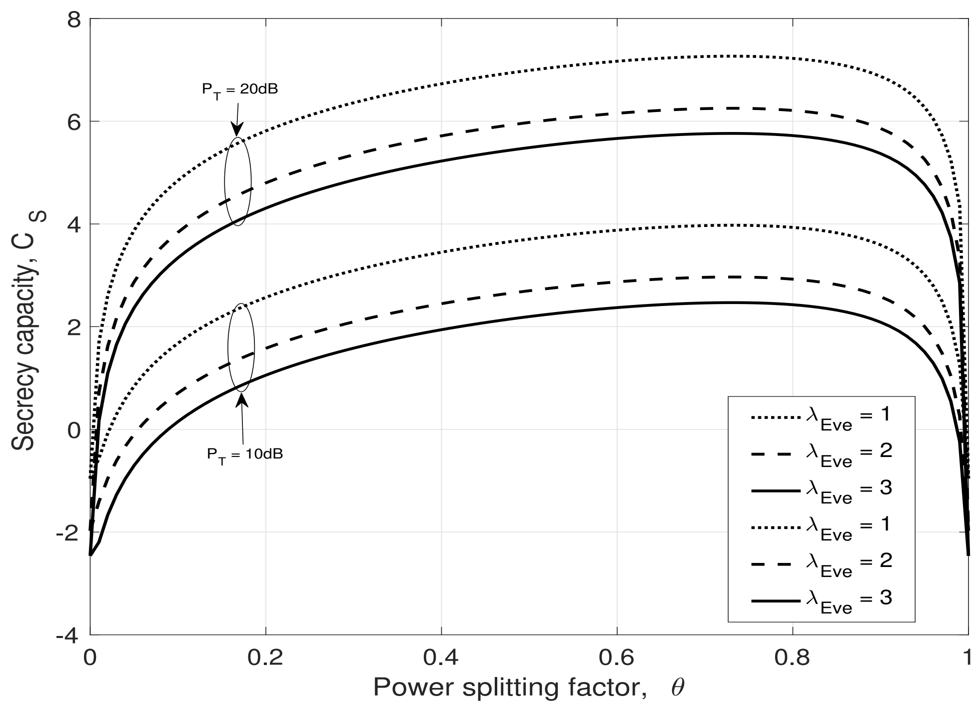

Figure 3.4: Secrecy capacity versus the power splitting factor for three values of λ_{Eve}.

$\lambda_{Eve} = 1$, 2, and 3. As λ_{Eve} increases, the corresponding channels improve so the eavesdropper is better able to intercept the transmitted signals. Thus, more jamming power is required to decrease the eavesdropper capacity. Although increasing this power has a positive effect on the harvested energy as shown in Fig. 3.5, the secrecy capacity suffers. Fig. 3.7 shows that as the jamming signal power increases from $0.1P_T$ to $0.3P_T$, the secrecy capacity decreases for the same value of λ_{Eve}. This is because increasing P_J results in less power allocated to A and B to transmit so the signals received at the relay from A and B are weaker.

Figs. 3.8 and 3.9 present the secrecy capacity for different locations of the relay and eavesdropper. The channel links between the nodes can be expressed as $h_{ij} = \frac{f_{ij}}{d_{ij}^m}$ where f_{ij} is an exponential random variable with mean 1, d_{ij} is the distance between i

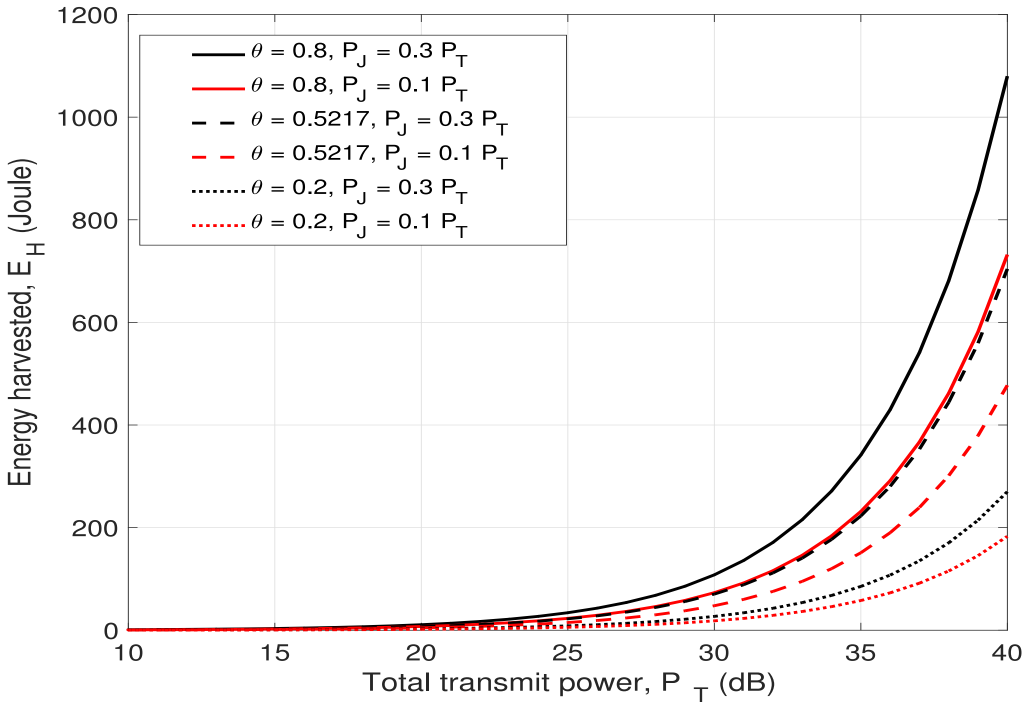

Figure 3.5: The harvested energy, E_H, at the relay versus the total transmit power for different values of θ and P_J.

and j, and m is the path loss exponent which here is $m = 2.7$. In Fig. 3.8, the relay is at (0.5, 0) and the jammer at (0.5, −0.5). Two eavesdropper locations are considered, (0.2, −0.2) and (0.5, −1), with $d_{AE} = 0.282$ and 1.118, respectively, where d_{AE} is the distance between A and E. As the distance increases from 0.282 to 1.118, the secrecy capacity increases. When $d_{AE} = 1.118$, the gap between the curves for $P_J = 0.1P_T$ and $0.3P_T$ is smaller than that for $d_{AE} = 0.282$. The reason is that as this distance increases, less jamming power is required to achieve the same secrecy capacity. The effect of the relay position on secrecy capacity is shown in Fig. 3.9 for $P_T = 10$ and 20 dB. As the relay gets closer to A or B, the secrecy capacity decreases and the highest secrecy capacity is achieved when the relay is equidistant between the two users as was the case in [94].

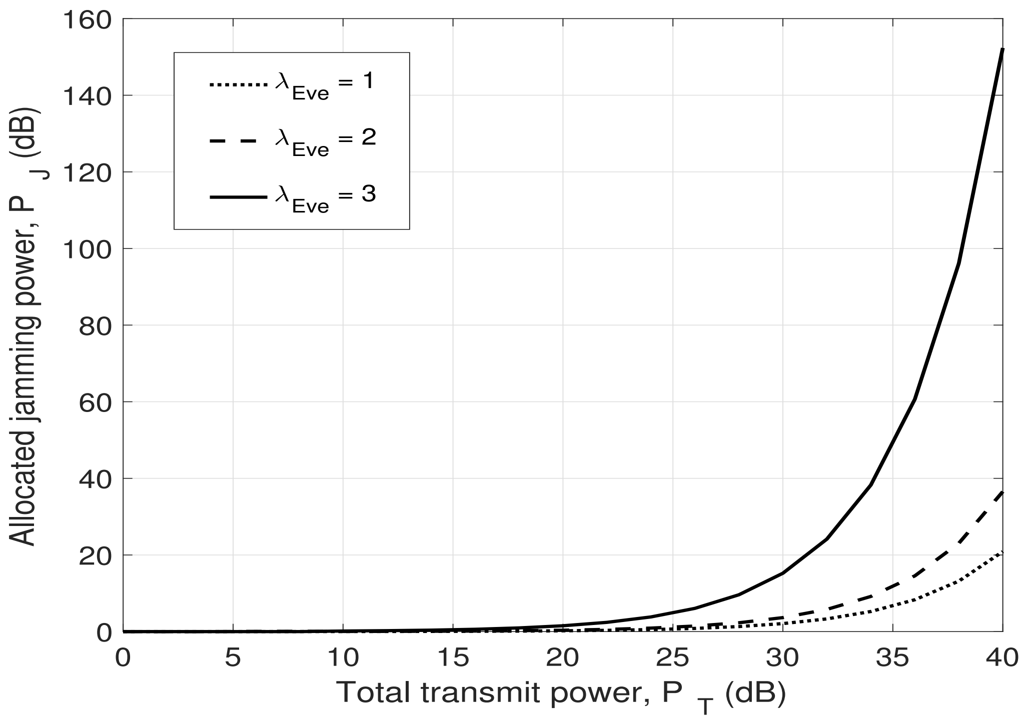

Figure 3.6: The optimal jamming power allocation versus the total transmit power for $\lambda_{Eve} = 1$, 2, and 3.

The effect of the eavesdropper and jammer locations on the secrecy capacity is shown in Figs. 3.10 and 3.11. The location of the eavesdropper in Fig. 3.10 changes from $(0, -0.7)$ to $(1, -0.7)$ and the location of the eavesdropper in Fig. 3.11 changes from $(0, -0.2)$ to $(1, -0.2)$. The locations of the jammer are $(0.5, -0.5)$, $(0.5, -1)$, $(0.2, -0.5)$, $(0.2, -1)$, $(0.7, -0.5)$, and $(0.7, -1)$. In all cases, the secrecy capacity is a minimum when the eavesdropper is at $x = 0$ or $x = 1$, i.e. closest to A or B, respectively. As the eavesdropper moves from $x = 0$ to 1, the jamming signal power at the eavesdropper increases and the secrecy capacity increases. The secrecy capacity decreases when the eavesdropper moves farther from the jammer after it reaches the maximum secrecy capacity. The maximum secrecy capacity depends on the location of the jammer. The minimum secrecy capacity in Fig. 3.11 is lower than

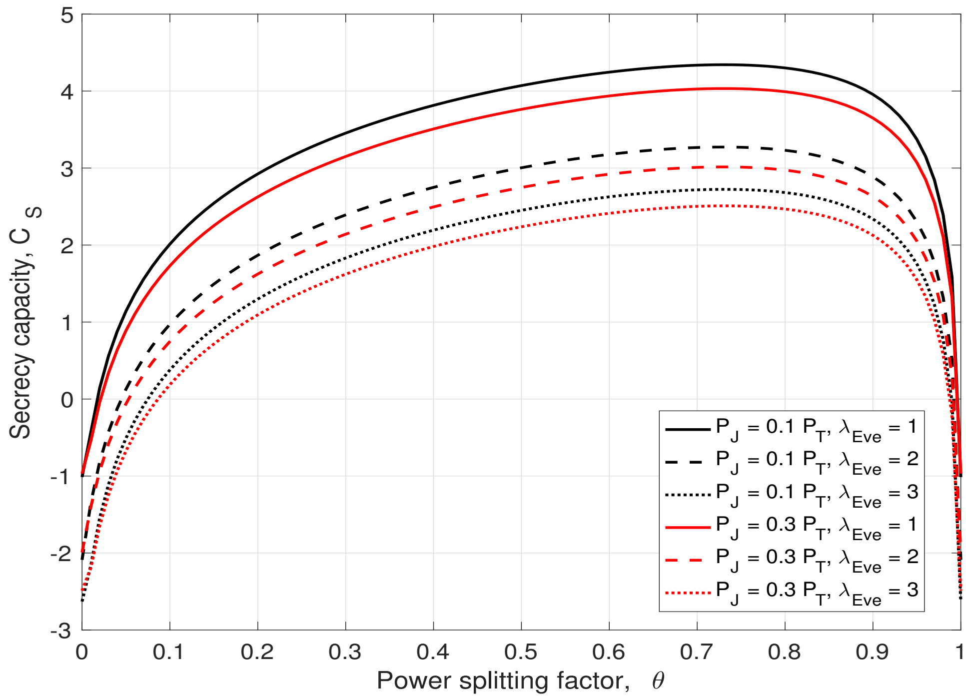

Figure 3.7: Secrecy capacity versus the power splitting factor for three values of λ_{Eve} and P_J.

the minimum secrecy capacity in Fig. 3.10 because the eavesdropper is closer to the links between A, B, and R. When the jammer is at $y = -1$ in Fig. 3.11, there is less variation in the secrecy capacity compared to $y = -0.5$ because the jammer is further from the relay.

3.4.1 Imperfect Jamming Signal Cancellation

The effect of imperfect jamming signal cancellation on the secrecy capacity is now investigated. Fig. 3.12 presents the secrecy capacity for three values of λ_{Eve} and the following two cases, $\Phi = 0$ so the jamming signal is perfectly canceled and $\Phi = 0.1$ so 10% of this signal is not canceled. These results show that imperfect cancellation decreases the secrecy capacity because a fraction of the jamming signal is amplified

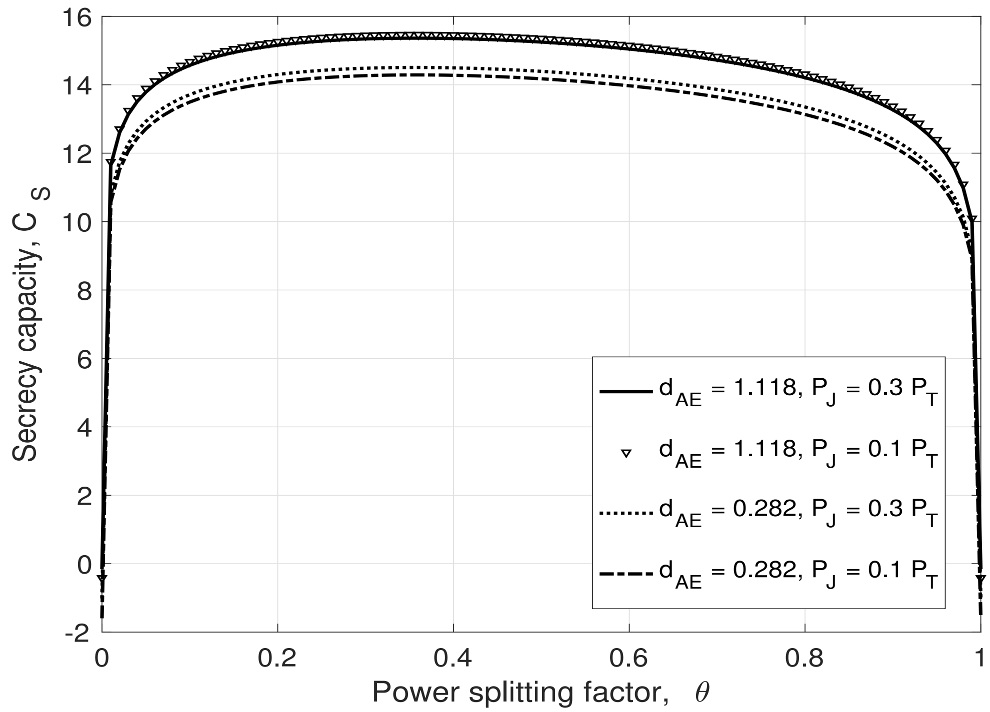

Figure 3.8: Secrecy capacity versus the power splitting factor for $d_{AE} = 0.282$ and 1.118 and $P_T = 10$ dB.

and forwarded by the relay which decreases the received SNR at A and B. For $P_T = 15$ dB, the secrecy capacity is 12.51 and 2.65 b/sec/Hz for $\Phi = 0$ and 0.1, respectively, for $\lambda_{Eve} = 1$. The secrecy capacity is zero when λ_{Eve} is 2 and 3 and $P_T \geq 10$ dB.

Fig. 3.13 presents the secrecy capacity for $P_J = 0.1P_T$ and $0.3P_T$, and $\lambda_{Eve} = 1$ and 3. This shows that the secrecy capacity decreases as Φ increases from 0 to 1 for all cases considered. When $\Phi = 0$, the jamming signal is cancelled completely at the relay, so the capacity is highest. As Φ increases, more jamming power is amplified and forwarded to A and B. This increases the noise at A and B which degrades their SNRs, thus decreasing the secrecy capacity. Further, the secrecy capacity with $P_J = 0.1P_T$ is better than for $P_J = 0.3P_T$ because increasing the fraction of power

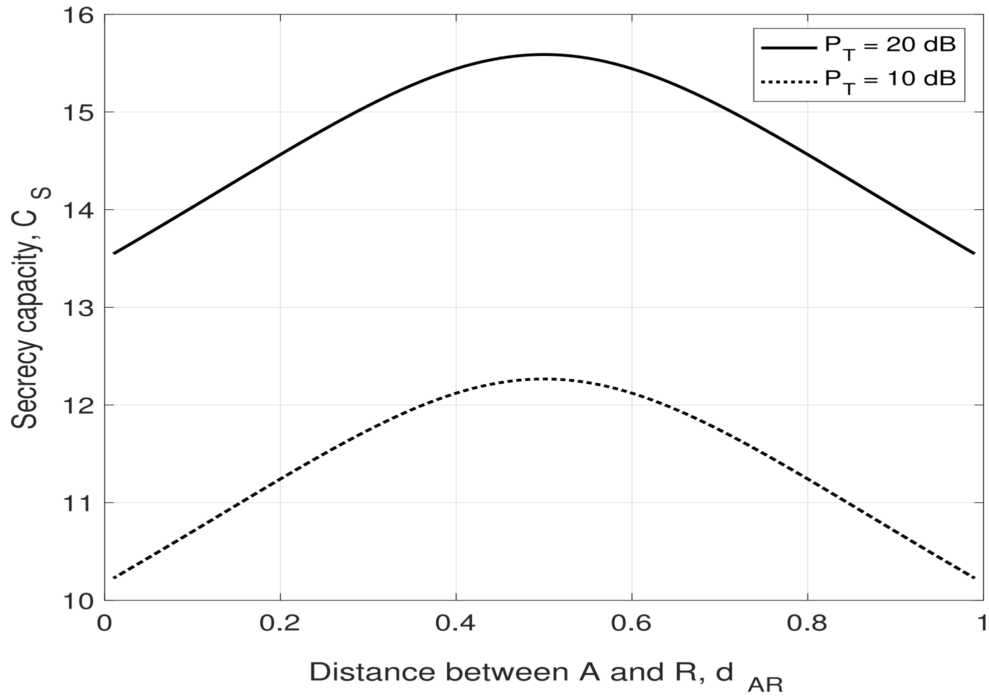

Figure 3.9: The secrecy capacity versus the distance between A and R, d_{AR}.

allocated to the jammer increases the jamming power not canceled which degrades the capacity.

Fig. 3.14 presents the effect of the cancellation factor, Φ, on the secrecy capacity as a function of the power splitting factor for $P_J = 0.1P_T$ and $0.3P_T$. This shows that as the jamming power increases, the secrecy capacity decreases for all values of Φ, but the difference varies with Φ. For $P_J = 0.1P_T$ and $\theta = 0.6$, the secrecy capacity is 4.246, 3.442, and 0.4054 for $\Phi = 0$, 0.1, and 0.5, respectively. The decrease in secrecy capacity is 0.804 from $\Phi = 0$ to 0.1 and 3.0366 from $\Phi = 0.1$ to 0.5. This decrease is because more jamming power is transmitted to A and B after being amplified by the relay which reduces the SNR at A and B.

The effect of changing the jammer location on the secrecy capacity for $\Phi = 0$,

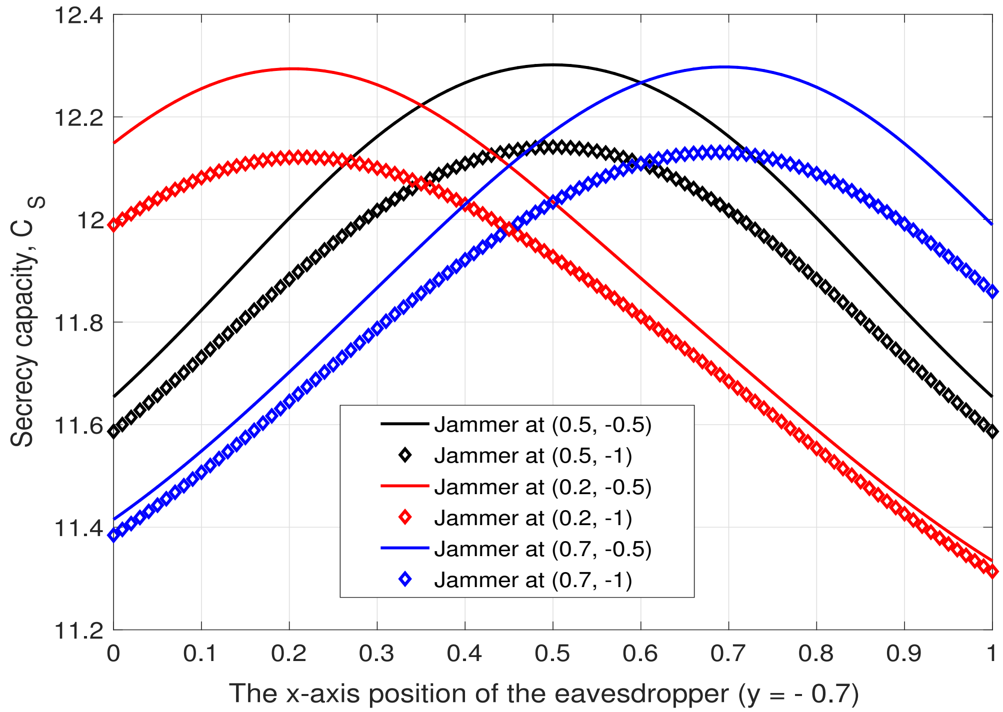

Figure 3.10: Secrecy capacity versus the x-axis location of the eavesdropper (y-axis location -0.7), for different locations of the jammer.

0.1, 0.5, and 1 is shown in Fig. 3.15. The red lines represent the jammer location $(0.5, -0.1)$ and the black lines $(0.5, -1)$. For $\Phi = 0, 0.1$, 0.5, and 1, the secrecy capacity is reduced when the jammer moves closer to the relay from $(0.5, -1)$ to $(0.5, -0.1)$. This is because the received jamming signal at the relay is stronger when the jammer is at $(0.5, -0.1)$ which means more noise which reduces the SNR at A and B. The difference in secrecy capacity for $\Phi = 0$ is minimal since the jamming signal is only an energy source and not a noise source.

3.4.2 Performance Without a Jammer

The effect of not having a jammer is now examined. Fig. 3.16 presents the secrecy capacity as a function of the transmit power with and without a jammer. The secrecy

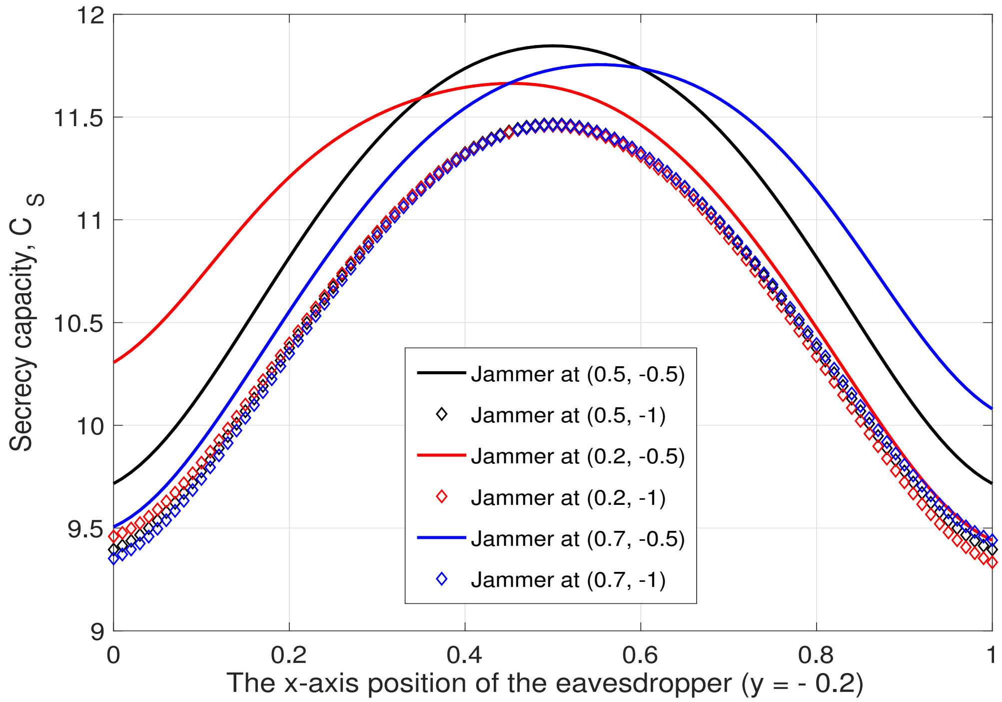

Figure 3.11: Secrecy capacity versus the x-axis location of the eavesdropper (y-axis location -0.2), for different locations of the jammer.

capacity with no jammer and $P_T = 15$ dB is 6.36 b/sec/Hz lower than with a jammer for $\lambda_{Eve} = 1$, 11.732 b/sec/Hz lower for $\lambda_{Eve} = 2$, and 10.98 b/sec/Hz lower for $\lambda_{Eve} = 3$. The presence of a jammer increases the secrecy capacity because the jamming signal reduces the SNR at the eavesdropper. The secrecy capacity with no jammer is near zero for $\lambda_{Eve} = 2$ and 3. Further, the difference in secrecy capacity with and without a jammer is smaller when $\lambda_{Eve} = 1$.

Fig. 3.17 shows the effect of the jammer on the energy harvested at the relay. The relay harvests energy from A, B, and the jammer in the first transmission phase. The amount of harvested energy with no jammer is less than that with a jamming signal of $0.3P_T$ for both values of θ. When there is no jammer, more transmit power is allocated to the users A and B, but the path loss due to the distances d_{AR} and d_{BR}

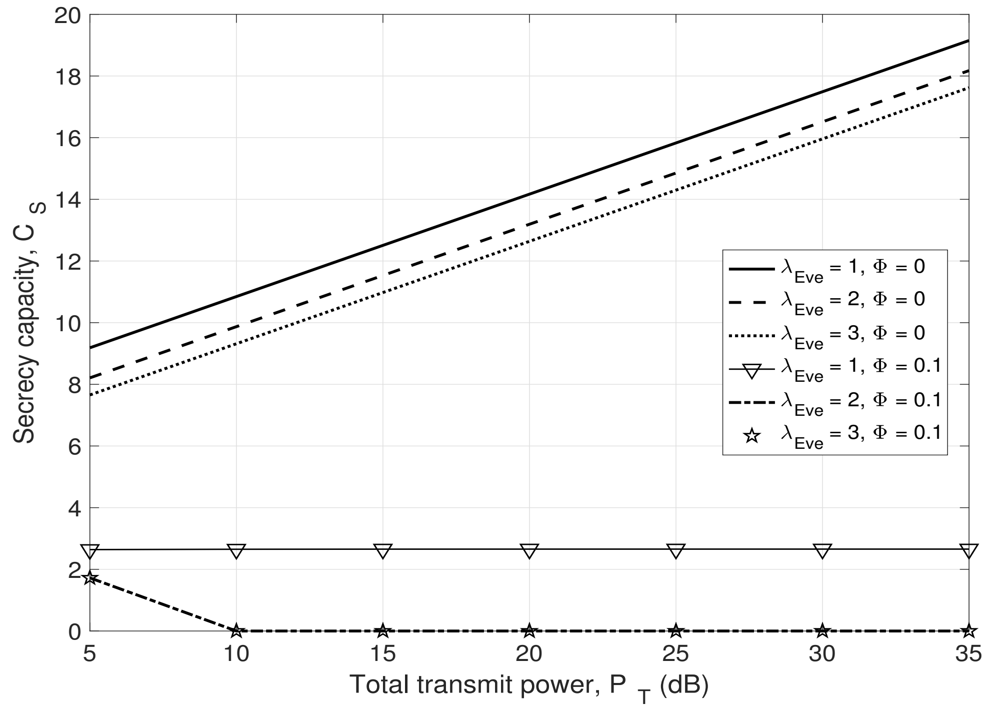

Figure 3.12: Secrecy capacity versus the total transmit power for $\Phi = 0$ and 0.1.

limits the energy harvested at the relay. Although the use of a jammer reduces the power allocated to A and B, the distance d_{JR} is smaller than d_{AR} and d_{BR}. Thus, a strong jamming signal is received for energy harvesting at the relay.

The secrecy capacity as a function of the x-axis position of the eavesdropper, E_x, is shown in Fig. 3.18 with and without a jammer located at $(0.5, -0.5)$. The y-axis position of the eavesdropper is -0.2, -0.5, and -0.8. The best secrecy capacity is obtained when the eavesdropper is at $E_x = 0.5$ which is the midpoint between A and B. Further, the secrecy capacity is better with a jammer because the jamming signal reduces the eavesdropper SNR. The secrecy capacity in both cases is lowest when E_x is 0 and 1 because the eavesdropper SNR from A and B, respectively, is highest.

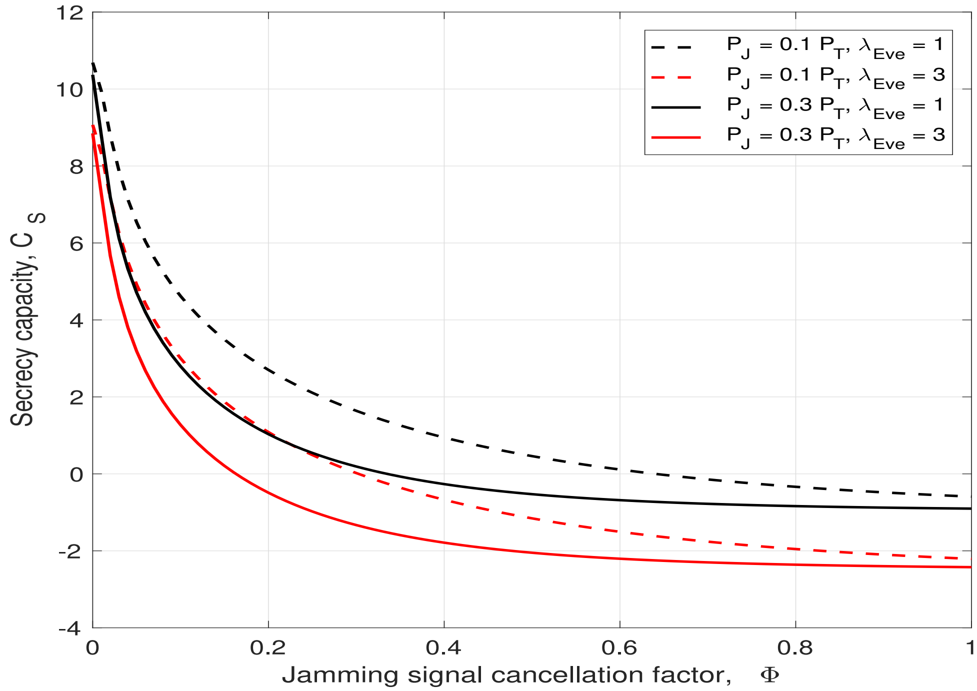

Figure 3.13: Secrecy capacity versus the jamming signal cancellation factor, Φ, for $\lambda_{Eve} = 1$ and 3.

3.4.3 Time Complexity

The simulations were conducted using Matlab R2017a on a MacBook Pro laptop with an Intel Core i5 processor. The average time required to run Algorithm 1 is 15.42 s with a jammer and 23.49 s without a jammer. Determining the optimal secrecy capacity is more difficult without a jammer so more time is required.

3.5 Conclusion

The secrecy capacity of a two-way relay network was investigated. The effect of an eavesdropper E was mitigated using a friendly jammer J. The power splitting factor and transmit power at the two users A and B, and J were jointly optimized

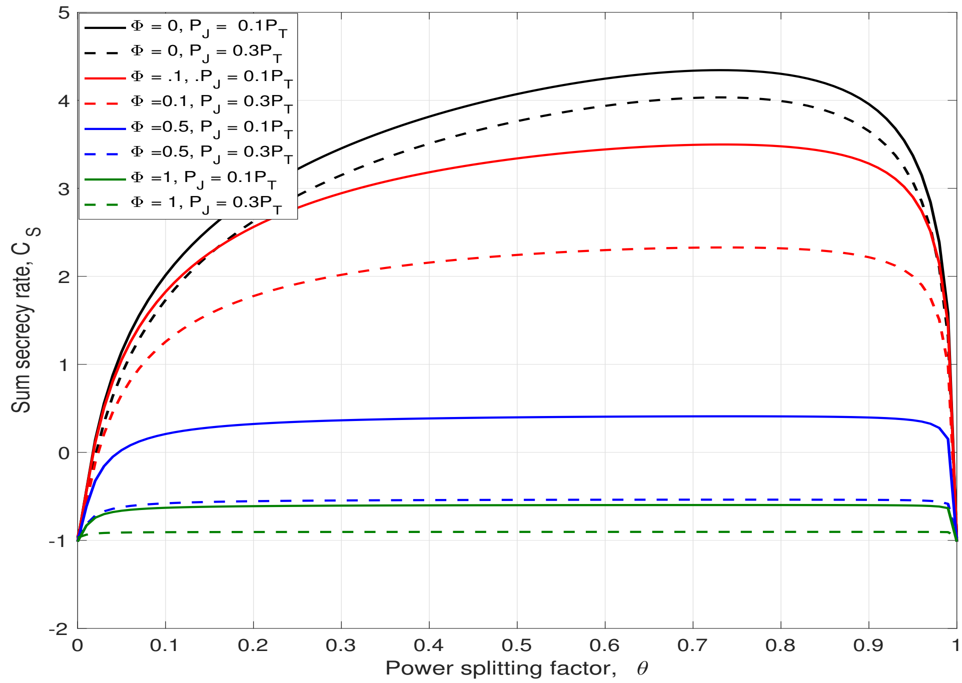

Figure 3.14: Secrecy capacity versus the power splitting factor for different values of P_J and Φ for $P_T = 10$ dB and $\lambda_{Eve} = 1$.

to maximize the secrecy capacity. The single condensation method (SCM) was used to convert the objective function into geometric programming (GP) form to obtain a convex optimization problem. The results presented show that using a jammer improves the secrecy performance and the amount of harvested energy at the relay. Further, the allocated jamming power increases as the eavesdropper channel links improve so as to reduce the information obtained by the eavesdropper. The secrecy capacity without a jammer was examined and compared to that with a jammer. The effect of the locations of the eavesdropper and jammer on the secrecy capacity was also investigated. It was determined that the best secrecy capacity is achieved when the relay is equidistant between A and B. The effect of the relative locations of the relay and jammer with respect to the eavesdropper on the secrecy capacity was

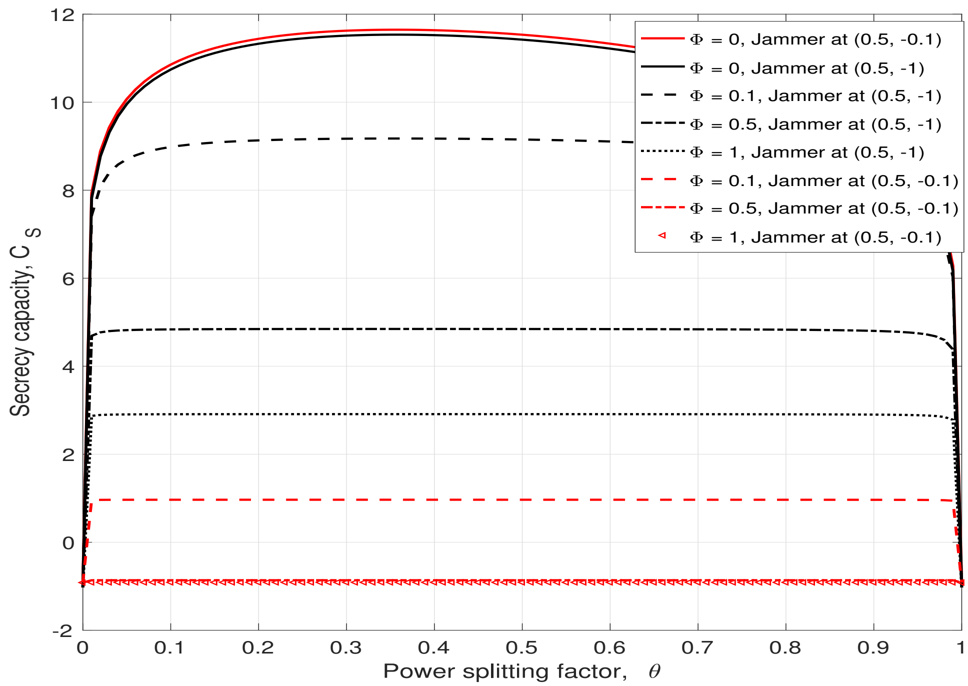

Figure 3.15: Secrecy capacity versus the power splitting factor for different values of P_J and Φ, $\lambda_{Eve} = 1$, $P_J = 0.1P_T$, $P_T = 10$ dB, and the eavesdropper at $(0.2, -0.5)$.

examined. Finally, it was shown that imperfect cancellation of the jamming signal at the relay degrades the secrecy capacity.

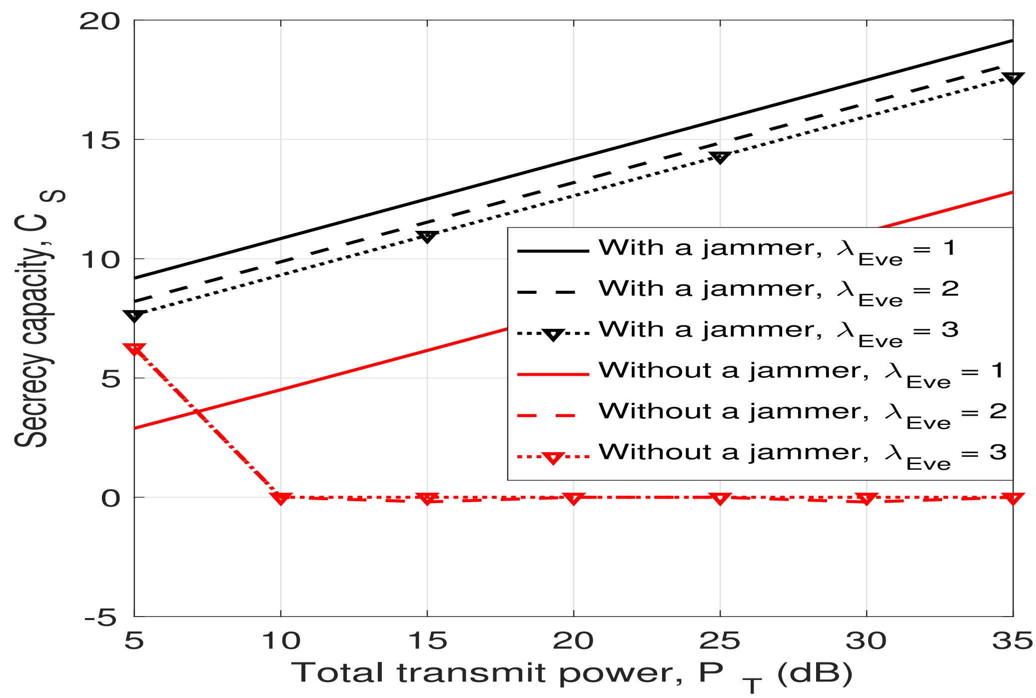

Figure 3.16: Secrecy capacity versus the transmit power with and without a jammer for $\lambda_{Eve} = 1$, 2, and 3.

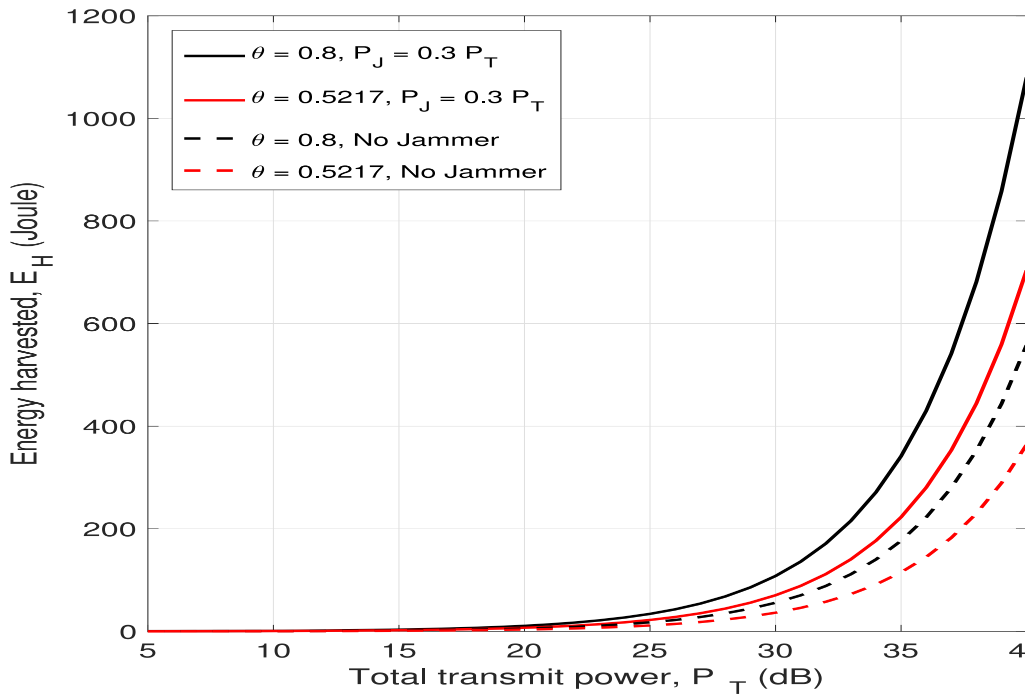

Figure 3.17: The energy harvested at the relay with and without a jammer for $\theta = 0.8$ and 0.5217 and $\lambda_{Eve} = 1$.

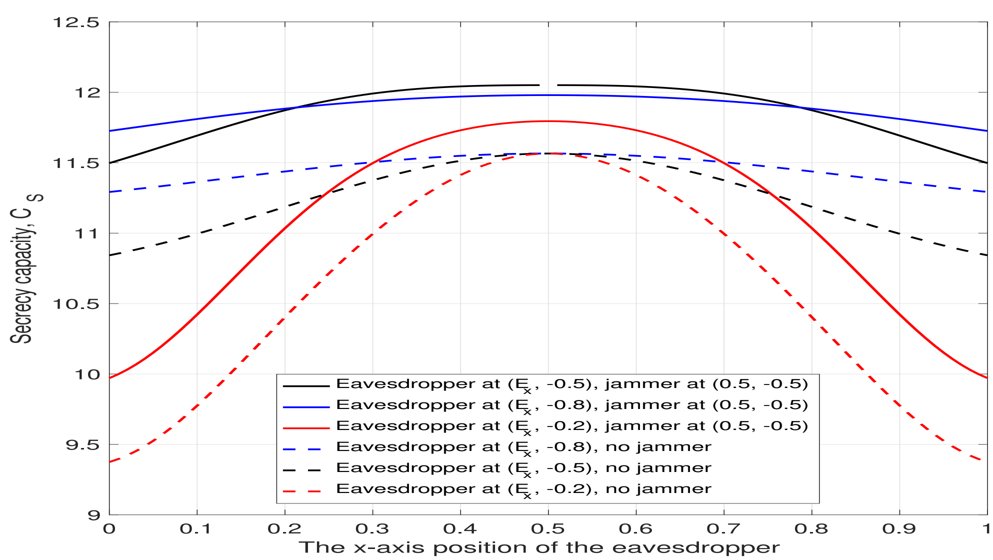

Figure 3.18: Secrecy capacity versus the x-axis location of the eavesdropper for different jammer locations and without a jammer.

Chapter 4

Secrecy Capacity in Two-Way Energy Harvesting Relay Networks with a Friendly Jammer and Imperfect CSI

This chapter investigates the security of two-way relay communications in the presence of an eavesdropper. In Chapter 3, perfect cancellation of the jamming signal at the relay was assumed and the eavesdropper was capable of estimating the CSI perfectly which is not the case in this chapter. The system includes two users that communicate via an energy harvesting relay. A friendly jammer is utilized to increase the secrecy capacity of the users by reducing the received signal to noise ratio at the eavesdropper. Imperfect channel state information for the links between the eavesdropper and other nodes is assumed. The eavesdropper employs maximal ratio combining (MRC) and selection combining (SC) to maximize the received signal to noise ratio of the wiretapped signals. Geometric programming (GP) is used to jointly optimize the power splitting factor of the relay and transmit powers of the two users and jammer to maximize the secrecy capacity of the system. The impact of channel estimation errors on the wiretap channel is studied. Further, the effect of imperfect cancellation of the jamming signal at the relay is examined. This signal is considered as a noise source at the users which decreases the secrecy capacity. The secrecy capacity is also studied for the case without a friendly jammer. This capacity is shown to be greater with a jammer than without a jammer. The locations of the relay, jammer, and eavesdropper have an effect on the secrecy capacity. It is shown that the secrecy capacity is greatest when the relay is at the midpoint between the users, and the closer the jammer is to the eavesdropper, the higher the secrecy capacity.

4.1 Introduction

Energy harvesting (EH) from radio frequency (RF) signals can be employed in wireless communications systems to prolong the lifetime of devices in energy-constrained systems [60]. Since RF signals carry information and energy simultaneously [61], simultaneous wireless information and power transfer (SWIPT) is possible. Separate circuits are usually employed to harvest energy and retrieve information [14]. Power splitting (PS) and time switching (TS) are EH relaying protocols that have been developed for SWIPT [49]. In time switching, the receiver switches between the two circuits while with power splitting, a fraction of the signal is directed to the EH circuit and the remaining is sent to the information retrieval circuit. The maximum transmission rate with optimal PS and TS relaying was derived in [63] and [64], respectively. In [63], the outage probability was obtained for a decode and forward (DF) relay network, and the optimal transmission rates with PS and TS were determined.

A SWIPT-enabled relay was considered in [64] for three scenarios, ideal (simultaneous EH and information retrieval), PS, and TS, and the maximum rate for each scenario was obtained. PS and TS can be used separately or combined as in the hybrid protocol proposed in [65] where the relay can switch between PS and TS. The optimal TS and PS ratios were derived for an EH relay to maximize the throughput, and the hybrid circuit was shown to perform better than separate circuits. In [66] and [67], joint PS and TS schemes were considered for amplify and forward (AF) and DF relay networks, respectively. The outage probability was shown to be better than with the hybrid protocol in [65]. In [66], the outage probability, energy efficiency, and network throughput were derived as a function of the PS and TS ratios, and the network throughput maximized. In [67], two optimization problems were jointly formulated to minimize the outage probability. The system throughput of a cognitive two-way relaying network was maximized in [68] using an optimal offline joint relay selection and power allocation scheme which outperforms random relay selection when the transmit power is limited.

Wireless transmissions are more vulnerable to eavesdropping than wired given the broadcast nature of wireless systems. The physical layer security of a wiretap channel was introduced in [73] and is defined as the difference between the capacity of the link between the source and destination and the capacity of the wiretap link between the source and eavesdropper. This can be used to assist upper-layer cryptographic techniques [96]–[97]. Physical layer security exploits the physical properties of wireless channels such as fading and interference, to secure transmissions between users in the presence of an eavesdropper [98]–[99]. However, the wireless channel conditions have a significant effect on these solutions [100]. Physical layer security with cooperative relaying can be employed to mitigate this issue [101]. This was first studied in [74] for an untrusted relay network which was considered as a possible eavesdropper. One-way communications was investigated in [75] for DF and AF EH relays and DF was shown to outperform AF in terms of secrecy performance. The secrecy capacity with PS and TS relaying protocols in a one-way untrusted relay network was analyzed in [76] and the performance of PS was better.

The spectral efficiency provided by two-way relaying is higher than with one-way relaying. In [77], a two-way EH-based relay network in the presence of an eavesdropper was studied. The secrecy capacity was maximized and the optimal TS and PS ratios were derived for high signal to noise ratios (SNRs) based on the instantaneous channel state information. It was shown that near optimal secrecy capacity is achievable with the proposed approach even when the wiretap channels are unknown. The secrecy capacity and energy efficiency were considered jointly in [78] for a two-way untrusted relay network. The likelihood of successful eavesdropping for a two-way three-step DF EH relay network was derived in [79] assuming independent κ-μ shadowing. It was shown that allocating additional power for information decoding over a small reception time improves the secrecy capacity. In [80], a closed-form expression for the intercept probability was obtained for a two-way DF EH relay network in the presence of multiple eavesdroppers. The effect of the power splitting factor on the secrecy capacity was studied. The secrecy capacity of a two-way communication network with multi-antenna time-switching relays in the presence of an eavesdropper was maximized in [81]. The secrecy capacity with equal transmit power allocated to the users was shown to be better than with an unequal transmit power allocation.

Cooperative jamming can be used to improve the secrecy capacity of wireless communication networks [102, 103, 104]. Both friendly jamming (FJ) and Gaussian noise jamming (GNJ) have been proposed. The jamming signal is known at the receiver with FJ [82], but GNJ cannot be recreated at the receiver so this is treated as noise [83]. While both FJ and GNJ can improve the secrecy capacity, the performance provided by FJ is better because the users can cancel the jamming signal. In [84], a system with two eavesdroppers and an energy harvesting friendly jammer was considered. One eavesdropper is near the user and the other is near the jammer, and they cooperate to obtain user signals and mitigate the effects of jamming. The secrecy capacity and energy efficiency of the network were maximized by optimizing the jamming signal power. The secrecy capacity with FJ was examined in [105] for a one-way untrusted relay network without a line-of-sight transmission link. In [85], a jammer was employed in an EH-based relay network to secure two-way communications. A lower bound was derived for the secrecy capacity with high SNRs. It was shown that FJ with two-way communications outperforms one-way and the two-way communications without jamming and with GNJ. In [86], the secrecy capacity of one-way untrusted relay communications was maximized by jointly optimizing the transmit and jamming powers with an EH threshold at the relay.

In [87], the secrecy performance with untrusted EH relays was improved using energy-aware distributed beamforming. The secrecy capacity was improved in [88] by selecting GNJ and relay nodes from multiple friendly but selfish intermediate nodes. Price competition was used to allocate power to the intermediate nodes and their profit was optimized to maximize the secrecy capacity. A two-way untrusted relay network with multiple friendly jammers was considered in [33] and the jamming power optimized to maximize the secrecy capacity. In [89], a network with multiple relay-user pairs was examined in the presence of multiple eavesdroppers. A joint relay-user pair and friendly jammer selection scheme was proposed to maximize the secrecy capacity. In [33], the secrecy capacity was optimized using a Stackelberg game for power allocation between users and friendly jammers.

In [90], adaptive cooperative jamming in the presence of multiple eavesdroppers with an EH relay was considered. The secrecy capacity was maximized by adjusting the power allocation factor. A two-way EH relay network with multiple eavesdroppers and a friendly jammer was investigated in [91]. The relay PS and TS ratios were optimized to maximize the secrecy capacity, and PS was shown to be more robust to eavesdropping. A two-way relay network was studied in [92] with partial relay selection and hybrid PS and TS at the intermediate nodes. It was shown that secure communications is possible with an appropriate selection of parameters.

The above results assume perfect knowledge of the CSI at the eavesdropper for the user and relay signals. However, this assumption is not valid in practical systems due to the presence of delays and channel estimation errors. In two-way relay networks, imperfect CSI results in imperfect self-interference cancellation [106]. In [107], a transmission scheme for multiple input single output (MISO) channels was presented with imperfect CSI for the user and eavesdropper channels with cooperative jamming. In [108], the CSI for the jammer to eavesdropper link was assumed to be unknown and imperfect CSI assumed for the jammer to user link. The impact of imperfect CSI on the secrecy outage capacity with cooperative jamming was analyzed. Although imperfect CSI has received some research attention, the impact of imperfect CSI on the security of a SWIPT two-way relay network has not yet been studied.

This chapter considers the physical layer security of a two-way communication system with an EH relay and a friendly jammer under the assumption of imperfect CSI at the eavesdropper. The eavesdropper employs maximal ratio combining (MRC) and selection combining (SC). The power allocated to the two users, relay, and jammer are jointly optimized in the presence of an eavesdropper with imperfect CSI. This has not been previously considered in the literature. Further, the effect of imperfect cancellation of the jamming power at the relay is studied. The main contributions of this chapter are as follows.

1. The effect of channel estimation errors on the secrecy capacity is investigated when the eavesdropper employs MRC and SC. Imperfect CSI at the eavesdropper has not been previously considered.

2. The secrecy capacity is maximized by jointly optimizing the power splitting factor and transmit powers of the two users and jammer.

3. The single condensation method (SCM) is used to convert the objective function to a standard GP form. Then, geometric programming (GP) is employed to transform the optimization problem into a convex problem.

4. Imperfect cancellation of the jamming signal at the relay and the effect on the users is studied. This has not been considered previously in the literature.

5. The secrecy capacity is evaluated with and without a jammer. In addition, results are given for different eavesdropper and jammer locations.

The remainder of this chapter is organized as follows. The system model is presented in Section 4.2. The secrecy capacity for the two-way relay network is derived in Section 4.3 for MRC and SC at the eavesdropper. In Section 4.4, the optimization problem is formulated and converted to a convex problem. Section 4.5 presents some simulation results and some concluding remarks are given in Section 4.6.

4.2 System Model

The system model of a two-way relay network is presented in Fig. 4.1. It includes two users A and B, a trusted relay R, a friendly jammer J, and an eavesdropper E. Each node has a single antenna and operates in half-duplex mode. The eavesdropper is located randomly near the relay to listen to the signals received by and transmitted from the relay. The A-R, B-R, A-E, B-E, R-E, J-R, and J-E channels are denoted by h_{AR}, h_{BR}, h_{AE}, h_{BE}, h_{RE}, h_{JR}, and h_{JE}, respectively. The channels are assumed to be reciprocal so that $h_{ij} = h_{ji}$, $\{i, j\} \in \{A, B, R, J, E\}, i \neq j$. With Rayleigh fading, the channel gains, $|h_{ij}|^2$, are exponentially distributed random variables with mean λ. n_A, n_B,n_R, and n_E denote the additive white Gaussian noise (AWGN) at A, B, R, and E, respectively, with zero mean and variance σ^2.

In this chapter, the practical case is considered where the channels at A, B, R, and J can be estimated accurately given that they are trusted nodes, while there are channel estimation errors at the eavesdropper [107]. The estimated channel gain from the eavesdropper to node i, $i \in \{A, B, R, J\}, i \neq E$, is given by [106]

$$h_{iE} = \widehat{h}_{iE} + e_{iE}, \tag{4.1}$$

where $\widehat{h}_{iE}$ is the estimated channel gain and e_{iE} is the channel estimation error. For simplicity, the e_{iE} are denoted by e_E which is a Gaussian distributed random variable with zero mean and variance σ_e^2. A summary of the notation employed is given in Table 4.1.

Table 4.1: Notation

Symbol	**Description**
A, B	Users
R	Relay
J	Jammer
E	Eavesdropper
h_{ij}	Channel between node i and node j
$\|h_{ij}\|^2$	Channel gain between node i and node j
$\widehat{h}_{iE}$	Estimated channel between E and node i
$\|\widehat{h}_{iE}\|^2$	Estimated channel gain between E and node i
e_{iE}	Channel estimation error between E and node i
σ_e^2	Channel estimation error variance
n_i	Additive white Gaussian noise (AWGN) at node i
σ^2	AWGN variance
x_i	Signal transmitted by node i
y_i	Signal received at node i
P_A	Transmit power of node A
P_B	Transmit power of node B

Continued on next page

Table 4.1 – *Continued from previous page*

Symbol	**Description**
P_R	Transmit power of node R
P_J	Transmit power of node J
P_T	Total power constraint
$\mathbf{E}[.]$	Expected value
y_{Re}	Energy harvesting signal at the relay
y_{Ri}	Information retrieval signal at the relay
θ	Power splitting factor
E_H	Harvested energy
ζ	Energy conversion efficiency
T	Total transmission time
m	Path loss exponent
Φ	Jamming signal cancellation factor
y_R	Information retrieval signal at the relay after jamming cancellation
$y_E^{(1)}$	Received signal at E in the first phase
$y_E^{(2)}$	Received signal at E in the second phase
$SNR_{E,A}^{(1)}$	SNR at E for x_B sent to A in the first phase
$SNR_{E,B}^{(1)}$	SNR at E for x_A sent to B in the first phase
$SNR_{E,A}^{(2)}$	SNR at E for x_B sent to A in the second phase
$SNR_{E,B}^{(2)}$	SNR at E for x_A sent to B in the second phase
SNR_A	SNR at A
SNR_B	SNR at B

Continued on next page

Table 4.1 – *Continued from previous page*

Symbol	**Description**
R_A	Achievable rate at A
R_B	Achievable rate at B
$R_E^{(1)}$	Achievable rate at E in the first phase
$R_E^{(2)}$	Achievable rate at E in the second phase
R_E	Achievable rate at E for both phases
C_A	Secrecy capacity at A
C_B	Secrecy capacity at B
C_S	Secrecy capacity

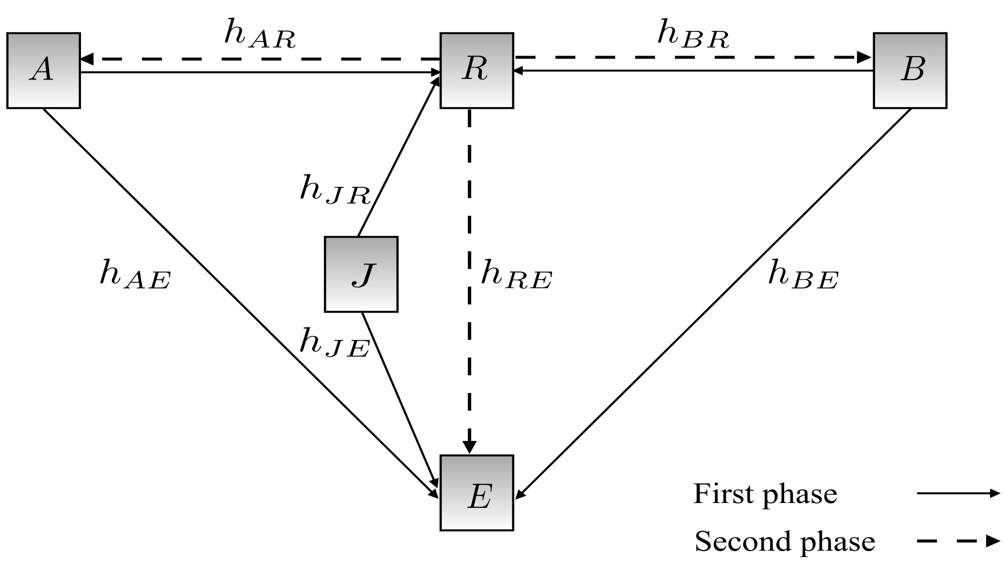

Figure 4.1: System model of the two-way wireless relay network with a jammer and eavesdropper.

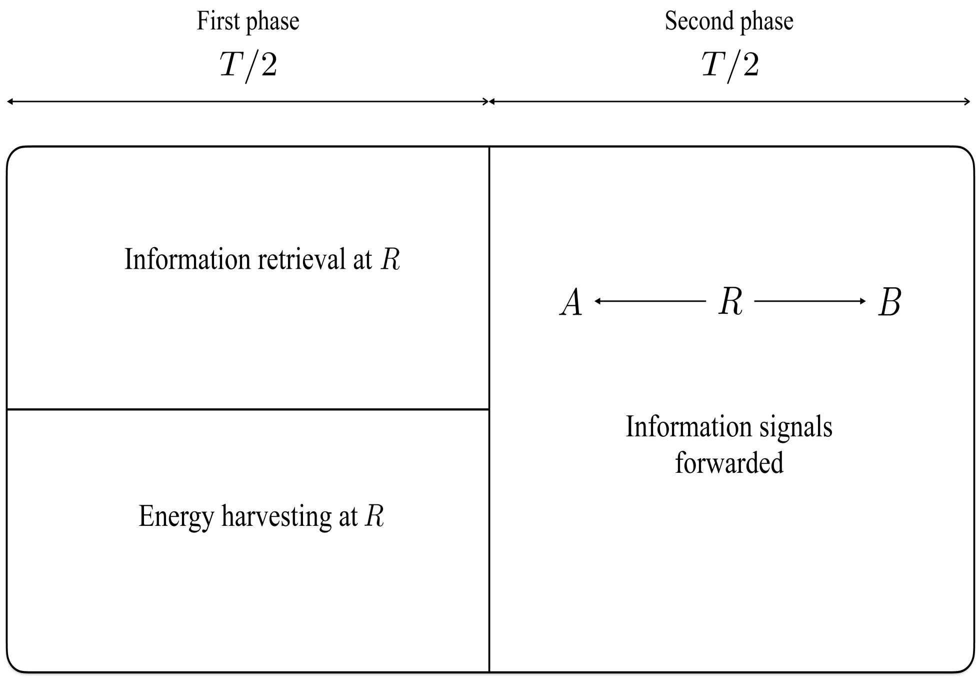

Figure 4.2: Transmission time frame for power splitting in the two-way relay network.

Fig. 4.2 shows the two phases required to forward the signals between A and B in the relay network. In the first phase, A and B send their signals x_A and x_B with $\mathbf{E}[|x_A|^2] = \mathbf{E}[|x_B|^2] = 1$ and transmit powers P_A and P_B, respectively, to R. During this phase, the jammer broadcasts a jamming signal, x_J with $\mathbf{E}[|x_J|^2] = 1$, so to make it more difficult for the eavesdropper to recover x_A and x_B. The relay depends solely on energy harvested from the user and jamming signals for power. The signal at the relay is divided into two parts for information retrieval and energy harvesting. The energy harvesting part is

$$y_{Re} = \sqrt{\theta P_A} h_{AR} x_A + \sqrt{\theta P_B} h_{BR} x_B + \sqrt{\theta P_J} h_{JR} x_J, \tag{4.2}$$

where θ is the power splitting factor, $0 \leq \theta \leq 1$. The additive noise at the relay, n_R, is neglected because it can be assumed to be much less than the other terms in (4.2) [49]. The harvested energy is

$$E_H = \frac{T}{2}\zeta\theta\left(P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2\right), \tag{4.3}$$

where $\zeta, 0 < \zeta \leq 1$, is the energy conversion efficiency. In the second phase, the relay transmit power is

$$P_R = \frac{E_H}{T/2} = \zeta\theta E_R, \tag{4.4}$$

where $E_R = P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2$. The information retrieval part of the received signal is

$$y_{Ri} = \sqrt{(1-\theta)P_A}h_{AR}x_A + \sqrt{(1-\theta)P_B}h_{BR}x_B + \sqrt{(1-\theta)P_J}h_{JR}x_J + n_R. \tag{4.5}$$

The jamming signal term $\sqrt{(1-\theta)P_J}h_{JR}x_J$ at the relay can be cancelled from y_{Ri} if R has knowledge of the jammer signal [50, 51]. The jammer is located close to the relay and farther from A and B, so the jamming signal at A and B can be neglected. Information regarding the jamming signal is securely shared between the jammer, relay and users before cooperative jamming begins. However, the jamming signal may not be perfectly canceled at the relay and this case is considered here. A cancellation factor Φ, $0 \leq \Phi \leq 1$, is used to indicate the fraction of this signal that is not cancelled. This fraction, $\Phi \times P_J$, is amplified and forwarded to A and B by the relay. The jamming signal is perfectly cancelled if $\Phi = 0$, and there is no cancellation if $\Phi = 1$. The value of Φ depends on the relay receiver circuitry and the CSI at R.

The information retrieval signal assuming imperfect jamming cancellation is then

$$y_R = \sqrt{(1-\theta)P_A} h_{AR} x_A + \sqrt{(1-\theta)P_B} h_{BR} x_B + \Phi\sqrt{(1-\theta)P_J} h_{JR} x_J + n_R. \quad (4.6)$$

During the first phase, the signal received at E is

$$y_E^{(1)} = \sqrt{P_A}(\widehat{h}_{AE} + e_E)x_A + \sqrt{P_B}(\widehat{h}_{BE} + e_E)x_B + \sqrt{P_J}(\widehat{h}_{JE} + e_E)x_J + n_E. \quad (4.7)$$

The SNR at E for x_B sent to A is

$$SNR_{E,A}^{(1)} = \frac{P_B|\widehat{h}_{BE}|^2}{P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2} \quad (4.8)$$

and the SNR at E for x_A sent to B is

$$SNR_{E,B}^{(1)} = \frac{P_A|\widehat{h}_{AE}|^2}{P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2} \quad (4.9)$$

The eavesdropper does not have knowledge of the jamming signal. Therefore, x_J is treated as additional noise that reduces the received SNR at E.

During the second phase, the relay amplifies the received signal and forwards it to the users using the energy harvested. The signal transmitted by the relay is then

$$x_R = \frac{\sqrt{P_R}}{\sqrt{\widetilde{\theta}\left[P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2\right] + \sigma^2}} \quad y_R = \sqrt{\frac{P_R}{\widetilde{\theta}E_R + \sigma^2}} \quad y_R, \quad (4.10)$$

where $\widetilde{\theta} = 1 - \theta$ and $\sqrt{\frac{P_R}{\widetilde{\theta}E_R + \sigma^2}}$ is the relay amplifier gain. The received signal at

A in this phase is

$$
\begin{aligned}
y_A &= h_{AR}x_R + n_A \\
&= \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_B}h_{AR}h_{BR}}{\sqrt{\widetilde{\theta}E_R+\sigma^2}}x_B}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_A}|h_{AR}|^2}{\sqrt{\widetilde{\theta}E_R+\sigma^2}}x_A}_{\text{information signal}} + \underbrace{\Phi\frac{\sqrt{\widetilde{\theta}P_R P_J}h_{AR}h_{JR}}{\sqrt{\widetilde{\theta}E_R+\sigma^2}} + \frac{\sqrt{P_R}h_{AR}n_R}{\sqrt{\widetilde{\theta}E_R+\sigma^2}} + n_A}_{\text{noise}},
\end{aligned}
\tag{4.11}
$$

and the corresponding signal at B is

$$
\begin{aligned}
y_B &= h_{BR}x_R + n_B \\
&= \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_A}h_{AR}h_{BR}}{\sqrt{\widetilde{\theta}E_R+\sigma^2}}x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta}P_R P_B}|h_{BR}|^2}{\sqrt{\widetilde{\theta}E_R+\sigma^2}}x_B}_{\text{information signal}} + \underbrace{\Phi\frac{\sqrt{\widetilde{\theta}P_R P_J}h_{BR}h_{JR}}{\sqrt{\widetilde{\theta}E_R+\sigma^2}}x_J + \frac{\sqrt{P_R}h_{BR}n_R}{\sqrt{\widetilde{\theta}E_R+\sigma^2}} + n_B}_{\text{noise}}\,.
\end{aligned}
\tag{4.12}
$$

A and B cancel their own signals since self-interference cancellation can be assumed [35, 36]. Let

$$\gamma_A = \frac{P_A|h_{AR}|^2}{\sigma^2}, \tag{4.13}$$

$$\gamma_B = \frac{P_B|h_{BR}|^2}{\sigma^2}, \tag{4.14}$$

$$\gamma_J = \frac{P_J|h_{JR}|^2}{\sigma^2}, \tag{4.15}$$

$$\overline{\gamma} = \gamma_A + \gamma_B + \gamma_J = \frac{E_R}{\sigma^2}. \tag{4.16}$$

The SNR at A is then

$$
\begin{aligned}
SNR_A &= \frac{\dfrac{\widetilde{\theta} P_B P_R |h_{BR}|^2 |h_{AR}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{P_R |h_{AR}|^2 \sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{\Phi^2 \widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{AR}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2} \\
&= \frac{\zeta \theta \widetilde{\theta} |h_{AR}|^2 \overline{\gamma} \gamma_B}{\left(\zeta \theta |h_{AR}|^2 + \Phi^2 \zeta \theta \widetilde{\theta} |h_{AR}|^2 \gamma_J + \widetilde{\theta}\right) \overline{\gamma} + 1},
\end{aligned}
\tag{4.17}
$$

and the corresponding achievable rate is [43]

$$
R_A = \frac{T}{2} \log_2 \left(1 + SNR_A\right). \tag{4.18}
$$

The SNR at B is

$$
\begin{aligned}
SNR_B &= \frac{\dfrac{\widetilde{\theta} P_A P_R |h_{AR}|^2 |h_{BR}|^2}{\widetilde{\theta} E_R + \sigma^2}}{\dfrac{P_R |h_{BR}|^2 \sigma^2}{\widetilde{\theta} E_R + \sigma^2} + \dfrac{\Phi^2 \widetilde{\theta} P_R P_J |h_{JR}|^2 |h_{BR}|^2}{\widetilde{\theta} E_R + \sigma^2} + \sigma^2} \\
&= \frac{\zeta \theta \widetilde{\theta} |h_{BR}|^2 \overline{\gamma} \gamma_A}{\left(\zeta \theta |h_{BR}|^2 + \Phi^2 \zeta \theta \widetilde{\theta} |h_{BR}|^2 \gamma_J + \widetilde{\theta}\right) \overline{\gamma} + 1},
\end{aligned}
\tag{4.19}
$$

and the corresponding achievable rate is

$$
R_B = \frac{T}{2} \log_2 \left(1 + SNR_B\right). \tag{4.20}
$$

The signal received at E during the second phase is

$$y_E^{(2)} = h_{RE} x_R + n_E, \tag{4.21}$$

$$= \underbrace{\frac{\sqrt{\widetilde{\theta} P_R P_A} h_{AR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{\widetilde{\theta} P_R P_B} h_{BR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_B}_{\text{information signal}} + \underbrace{\Phi \frac{\sqrt{\widetilde{\theta} P_R P_J} h_{JR} h_{RE}}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} x_J + \frac{\sqrt{P_R} h_{RE} n_R}{\sqrt{\widetilde{\theta} E_R + \sigma^2}} + n_E}_{\text{noise}}, \tag{4.22}$$

where $h_{RE} = \widehat{h}_{RE} + e_E$. The SNR at E for x_B sent to A during the second phase is

$$SNR_{E,A}^{(2)} = \frac{\zeta \theta \widetilde{\theta} \overline{\gamma} \gamma_B |\widehat{h}_{RE}|^2}{\overline{\gamma} \left[\zeta \theta |\widehat{h}_{RE}|^2 (\widetilde{\theta} \gamma_A + \widetilde{\theta} \gamma_J \Phi^2 + 1) + \widetilde{\theta} \right] + \sigma_e^2 \zeta \theta \overline{\gamma} \left[\widetilde{\theta} (\gamma_A + \gamma_B + \Phi^2 \gamma_J) + 1 \right] + 1}. \tag{4.23}$$

and the SNR at E for x_A sent to B during the second phase is

$$SNR_{E,B}^{(2)} = \frac{\zeta \theta \widetilde{\theta} \overline{\gamma} \gamma_A |\widehat{h}_{RE}|^2}{\overline{\gamma} \left[\zeta \theta |\widehat{h}_{RE}|^2 (\widetilde{\theta} \gamma_B + \widetilde{\theta} \gamma_J \Phi^2 + 1) + \widetilde{\theta} \right] + \sigma_e^2 \zeta \theta \overline{\gamma} \left[\widetilde{\theta} (\gamma_A + \gamma_B + \Phi^2 \gamma_J) + 1 \right] + 1}. \tag{4.24}$$

The achievable rate at E during both phases is then

$$R_{E,i} = \begin{cases} \frac{T}{2} \log_2 \left(1 + SNR_{E,i}^{(1)} + SNR_{E,i}^{(2)} \right), & \text{MRC at } E \\ \\ \frac{T}{2} \log_2 \left(1 + \max(SNR_{E,i}^{(1)}, SNR_{E,i}^{(2)}) \right), & \text{SC at } E. \end{cases} \tag{4.25}$$

4.3 Secrecy Capacity Analysis

The secrecy capacity in the presence of an eavesdropper is the difference between the secrecy capacity of the main link and the secrecy capacity of the wiretap link [43].

The power transmitted in the network is limited by the total power constraint P_T where $P_A+P_B+P_J \leq P_T$. The power splitting factor and transmit power of A, B, and J are allocated to maximize the secrecy capacity at A and B under this constraint. The secrecy capacity at A is $C_{S,A} = [R_A - R_{E,A}]^+$ and at B is $C_{S,B} = [R_B - R_{E,B}]^+$ [93], where $[x]^+ = \max(0, x)$. The secrecy capacity at user i, $i \in \{A, B\}$, is then

$$C_{S,i} = \begin{cases} \frac{T}{2}\log_2\left(\frac{1+SNR_i}{1+SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)}}\right), & \text{MRC at } E \\ \\ \frac{T}{2}\log_2\left(\frac{1+SNR_i}{1+\max(SNR_{E,i}^{(1)}, SNR_{E,i}^{(2)})}\right), & \text{SC at } E. \end{cases} \tag{4.26}$$

The secrecy capacity is

$$C_S = C_{S,A} + C_{S,B}, \tag{4.27}$$

$$= [R_A - R_{E,A}]^+ + [R_B - R_{E,B}]^+. \tag{4.28}$$

and the corresponding optimization problem can be formulated as

$$\begin{aligned} \max_{\theta,\widetilde{\theta},P_A,P_B,P_J} \quad & C_S \\ P_A + P_B + P_J \leq P_T& \\ \theta + \widetilde{\theta} \leq 1& \\ \theta, \widetilde{\theta}, P_A, P_B, P_J \geq 0& \end{aligned}$$

4.3.1 MRC at the Eavesdropper

In this subsection, the secrecy capacity of the network is derived considering imperfect channel estimation at the eavesdropper. The eavesdropper employs MRC to combine the signals from the direct and relay links in both transmission phases. The achievable rates at E for x_B sent to A and x_A sent to B, $R_{E,A}$ and $R_{E,B}$, respectively, are defined in (4.25). $C_{S,A}$ is obtained by substituting SNR_A, $SNR_{E,A}^{(1)}$, and $SNR_{E,A}^{(2)}$ given by (4.17), (4.8), and (4.23), respectively, in (4.26) with $i = A$, and $C_{S,B}$ is obtained by substituting SNR_B, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (4.19), (4.9), and (4.24), respectively, in (4.26) with $i = B$. From (4.28), there are four cases to consider to maximize the secrecy capacity as given below.

Case I: $C_{S,A} \geq 0$ **and** $C_{S,B} \geq 0$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& (R_A - R_{E,A}) + (R_B - R_{E,B}) \\ =& \frac{T}{2} \log_2 \left(\frac{w_I^{MRC}}{z_I^{MRC}} \right), \end{aligned} \tag{4.29}$$

where $(.)_I^{MRC}$ denotes the first case with MRC at the eavesdropper

$$
\begin{aligned}
& w_I^{MRC} = \\
& [(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
& [P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2] \\
& [\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] \\
& \qquad\qquad + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1] \\
& [(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
& [P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2] \\
& [\overline{\gamma}(\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}) + \sigma_e^2\zeta\theta\overline{\gamma}(\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1) + 1]
\end{aligned}
\tag{4.30}
$$

and

$$
\begin{aligned}
&z_I^{MRC} = \\
&[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)) \\
&\quad \times (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}]1) + \widetilde{\theta}] \\
&\qquad + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1)) \\
&\qquad + [(P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)1) + \widetilde{\theta}] \\
&\qquad \times (\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2)]] \\
&[(((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 1) + \widetilde{\theta}] \\
&\qquad + \sigma_e^2(P_A + P_B + P_J) + \sigma^2))\times \\
&\qquad\quad (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}]1) + \widetilde{\theta}] \\
&\qquad + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1) \\
&\qquad + [(P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 1) + \widetilde{\theta}] \\
&\qquad + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \times (\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]].
\end{aligned}
\tag{4.31}
$$

Case II: $C_{S,A} \geq 0$ **and** $C_{S,B} \leq 0$

In this case, $C_{S,B} = 0$ since the SNR at the eavesdropper is higher than that at B. The secrecy capacity is then

$$\begin{aligned} C_S =& (R_A - R_{E,A}) \\ =& \frac{T}{2} \log_2 \left(\frac{w_{II}^{MRC}}{z_{II}^{MRC}} \right), \end{aligned} \tag{4.32}$$

where $(.)_{II}^{MRC}$ denotes the second case with MRC at the eavesdropper

$$\begin{aligned} & w_{II}^{MRC} = \\ & [(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\ & [P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 1) + \widetilde{\theta}] + \sigma_e^2(P_A + P_B + P_J) + \sigma^2] \\ & [\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}]1) + \widetilde{\theta}] \\ & \qquad + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1] \end{aligned} \tag{4.33}$$

and

$$
\begin{aligned}
&z_{II}^{MRC} = \\
&[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 \\
&\qquad + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)) \\
&\quad \times (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] + \\
&\qquad \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1)) \\
&\quad + [(P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&\qquad \times (\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2)]].
\end{aligned}
\tag{4.34}
$$

Case III: $C_{S,A} \leq 0$ **and** $C_{S,B} \geq 0$

In this case, $C_{S,A} = 0$ since the SNR at the eavesdropper is higher than that at A. The secrecy capacity is then

$$
\begin{aligned}
C_S =& (R_B - R_{E,B}) \\
=& \frac{T}{2}\log_2\left(\frac{w_{III}^{MRC}}{z_{III}^{MRC}}\right),
\end{aligned}
\tag{4.35}
$$

where $(.)_{III}^{MRC}$ denotes the third case with MRC at the eavesdropper

$$
\begin{aligned}
w_{III}^{MRC} = \\
&[(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
&[P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2] \\
&[\overline{\gamma}(\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}) \\
&\quad + \sigma_e^2\zeta\theta\overline{\gamma}(\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1) + 1]
\end{aligned}
\tag{4.36}
$$

and

$$
\begin{aligned}
&z_{III}^{MRC} = \\
&[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)) \\
&\times (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1) \\
&\quad + [(P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&\quad\quad \times (\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]].
\end{aligned}
\tag{4.37}
$$

Case IV: $C_{S,A} \leq 0$ **and** $C_{S,B} \leq 0$

In this case, the secrecy capacity is $C_S = 0$ because the secrecy capacity of the wiretap links is higher than the secrecy capacity at A and B.

4.3.2 SC at the Eavesdropper

In this subsection, the secrecy capacity of the network with imperfect channel estimation at the eavesdropper is derived when the eavesdropper employs SC so the link (direct or relay) with the maximum SNR is selected. Based on $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (4.8), (4.23), (4.9), and (4.24), respectively, the following four cases can be considered.

Case I: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(1)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(1)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{I,A}^{SC}}{z_{I,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{I,B}^{SC}}{z_{I,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{I}^{SC}}{z_{I}^{SC}}\right), \end{aligned} \tag{4.38}$$

where

$$w_{I,A}^{SC} =$$

$$[(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma}$$

$$+ 1)]$$

$$[P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2], \tag{4.39}$$

$$w_{I,B}^{SC} =$$

$$[(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)]$$

$$[P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2], \tag{4.40}$$

$$z_{I,A}^{SC} =$$

$$[(((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J)$$

$$+ \sigma^2))]$$

$$[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1], \tag{4.41}$$

$$z_{I,B}^{SC} =$$

$$[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1]$$

$$[(((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J)$$

$$+ \sigma^2))], \tag{4.42}$$

$$\tag{4.43}$$

$$\frac{w_I^{SC}}{z_I^{SC}} = \begin{cases} \frac{w_{I,A}^{SC} w_{I,B}^{SC}}{z_{I,A}^{SC} z_{I,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \\ \frac{w_{I,A}^{SC}}{z_{I,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \\ \frac{w_{I,B}^{SC}}{z_{I,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{4.44}$$

and $(.)_I^{SC}$ denotes the first case with SC at the eavesdropper.

Case II: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(1)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(2)}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{II,A}^{SC}}{z_{II,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{II,B}^{SC}}{z_{II,B}^{SC}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{II}^{SC}}{z_{II}^{SC}} \right), \end{aligned} \tag{4.45}$$

where

$$
\begin{aligned}
&w_{II,A}^{SC} = \\
&[(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
&[P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2], \qquad (4.46) \\
&w_{II,B}^{SC} = \\
&[(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
&[\overline{\gamma}(\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}) + \sigma_e^2\zeta\theta\overline{\gamma}(\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1) + 1], \qquad (4.47) \\
&z_{II,A}^{SC} = \\
&[(((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2))] \\
&[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1], \qquad (4.48) \\
&z_{II,B}^{SC} = \\
&[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(\overline{\gamma}\left[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}\right] + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] \\
&\qquad + 1) + [(\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]], \qquad (4.49) \\
&\qquad (4.50)
\end{aligned}
$$

$$\frac{w_{II}^{SC}}{z_{II}^{SC}} = \begin{cases} \frac{w_{II,A}^{SC} w_{II,B}^{SC}}{z_{II,A}^{SC} z_{II,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \frac{w_{II,A}^{SC}}{z_{II,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \frac{w_{II,B}^{SC}}{z_{II,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{4.51}$$

and $(.)_{II}^{SC}$ denotes the second case with SC at the eavesdropper.

Case III: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2}\log_2\left(\frac{1+SNR_A}{1+SNR_{E,A}^{(2)}}\right) + \frac{T}{2}\log_2\left(\frac{1+SNR_B}{1+SNR_{E,B}^{(1)}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{III,A}^{SC}}{z_{III,A}^{SC}}\right) + \frac{T}{2}\log_2\left(\frac{w_{III,B}^{SC}}{z_{III,B}^{SC}}\right), \\ =& \frac{T}{2}\log_2\left(\frac{w_{III}^{SC}}{z_{III}^{SC}}\right), \end{aligned} \tag{4.52}$$

where

$$
\begin{aligned}
&w_{III,A}^{SC} = \\
&[(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
&[\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) \\
&\qquad + 1] + 1], \qquad (4.53)\\
&w_{III,B}^{SC} = \\
&[(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)] \\
&[P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2], \qquad (4.54)\\
&z_{III,A}^{SC} = \\
&[(\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] \\
&\qquad + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1)] \\
&[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1], \qquad (4.55)\\
&z_{III,B}^{SC} = \\
&[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1] \\
&[(((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 \\
&\qquad + \sigma_e^2(P_A + P_B + P_J) + \sigma^2))], \qquad (4.56)\\
&\qquad (4.57)
\end{aligned}
$$

$$\frac{w_{III}^{SC}}{z_{III}^{SC}} = \begin{cases} \frac{w_{III,A}^{SC} w_{III,B}^{SC}}{z_{III,A}^{SC} z_{III,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \\ \frac{w_{III,A}^{SC}}{z_{III,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \\ \frac{w_{III,B}^{SC}}{z_{III,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{4.58}$$

and $(.)_{III}^{SC}$ denotes the third case with SC at the eavesdropper.

Case IV: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(2)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(2)}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{IV}^{SC}}{z_{IV}^{SC}} \right), \end{aligned} \tag{4.59}$$

where

$$w_{IV,A}^{SC} =$$

$$[(\zeta\theta\widetilde{\theta}|h_{AR}|^2\overline{\gamma}\gamma_B) + ((\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)]$$

$$[\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}] + \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1], \tag{4.60}$$

$$w_{IV,B}^{SC} =$$

$$[(\zeta\theta\widetilde{\theta}|h_{BR}|^2\overline{\gamma}\gamma_A) + ((\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1)]$$

$$[\overline{\gamma}(\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta})$$

$$+ \sigma_e^2\zeta\theta\overline{\gamma}(\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1) + 1], \tag{4.61}$$

$$z_{IV,A}^{SC} =$$

$$[(\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_A + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}]$$

$$+ \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1)]$$

$$[(\zeta\theta|h_{AR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{AR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1], \tag{4.62}$$

$$z_{IV,B}^{SC} =$$

$$[(\zeta\theta|h_{BR}|^2 + \Phi^2\zeta\theta\widetilde{\theta}|h_{BR}|^2\gamma_J + \widetilde{\theta})\overline{\gamma} + 1]$$

$$\Bigg[(\overline{\gamma}[\zeta\theta|\widehat{h}_{RE}|^2(\widetilde{\theta}\gamma_B + \widetilde{\theta}\gamma_J\Phi^2 + 1) + \widetilde{\theta}]$$

$$+ \sigma_e^2\zeta\theta\overline{\gamma}[\widetilde{\theta}(\gamma_A + \gamma_B + \Phi^2\gamma_J) + 1] + 1) + [(\zeta\theta\widetilde{\theta}\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]\Bigg], \tag{4.63}$$

$$\tag{4.64}$$

$$\frac{w_{IV}^{SC}}{z_{IV}^{SC}} = \begin{cases} \dfrac{w_{IV,A}^{SC} w_{IV,B}^{SC}}{z_{IV,A}^{SC} z_{IV,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\[2em] \dfrac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\[2em] \dfrac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\[2em] 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{4.65}$$

and $(.)_{IV}^{SC}$ denotes the fourth case with SC at the eavesdropper.

4.4 Optimization Problem Formulation

The secrecy capacity optimization problem for MRC and SC at the eavesdropper is

$$\underset{\theta, \widetilde{\theta}, P_A, P_B, P_J}{\text{minimize}} \quad \frac{z}{w} \tag{4.66a}$$

$$\text{subject to} \quad P_A + P_B + P_J \leq P_T, \tag{4.66b}$$

$$\theta + \widetilde{\theta} \leq 1, \tag{4.66c}$$

$$\theta, \widetilde{\theta}, P_A, P_B, P_J \geq 0 \tag{4.66d}$$

where w and z are defined below for each diversity scheme.

The standard form of a Geometric Programming (GP) problem is [40]

$$\text{minimize} \quad f_0(x) \tag{4.67a}$$

$$\text{subject to} \quad f_i(x) \leq 0, \quad i = 1, \ldots, m, \tag{4.67b}$$

$$g_i(x) = 1, \quad i = 1, \ldots, p \tag{4.67c}$$

where $f_i(x)$ is a posynomial function, $g_i(x)$ is a monomial function, and x is the optimization variable. A monomial function g of x is a real valued function of the form $g(x) = cx_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}$ where $c > 0$, $a_i \in \mathbf{R}$, and n is the number of optimization variables. A posynomial function is the sum of two or more monomials such that $f(x) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} x_2^{a_{2k}} \ldots x_n^{a_{nk}}$ where $c_k > 0$ and K is the number of monomial functions.

The constraints in (4.66b) and (4.66c) are posynomials. This problem can be transformed into GP form and then into a convex problem because the constraints and the objective function are posynomials. However, the objective function is a ratio of two posynomials, so it cannot be transformed into GP form. To solve this issue, $w(\theta, \widetilde{\theta}, P_A, P_B, P_J)$ is approximated as a monomial function using the single condensation method (SCM) [41]. In SCM, the denominator of the ratio of posynomials is approximated with a monomial function. The numerator (a posynomial) is not approximated, hence the term single. In the optimization problem, $w(\mathbf{x}) = \sum_i u_i(\mathbf{x})$, $\mathbf{x} = \left[\theta, \widetilde{\theta}, P_A, P_B, P_J\right]^T$, is the sum of i monomials, so it is a posynomial by definition, and the monomial approximation of $w(\mathbf{x})$ using SCM is

$$\overline{w}(\mathbf{x}) = \prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i}\right)^{\alpha_i}, \tag{4.68}$$

such that $w(\mathbf{x}) \geq \overline{w}(\mathbf{x})$. For a given $\mathbf{x}$, the α_i are obtained such that

$$\alpha_i = \frac{u_i(\mathbf{x})}{w(\mathbf{x})}, \tag{4.69}$$

and $\overline{w}(\mathbf{x})$ is substituted for $w(\mathbf{x})$ in (4.66a). The objective function after SCM approximation is a polynomial (posynomial). The accuracy of the approximation was determined by calculating the difference between the value of $w(\mathbf{x})$ and $\overline{w}(\mathbf{x})$ at the solution point $\mathbf{x}$. The maximum difference is 0.00107. GP is used to obtain a nonlinear but convex optimization problem with convex objective and inequality constraint functions and linear equality constraints. A logarithmic change of variables and a logarithmic transformation of the objective function and constraints is used to obtain a GP form. The resulting convex problem can be solved efficiently using CVX solvers [40]. As the optimal solution can be far from the initial guess $\mathbf{x}_0$ used in the SCM approximation, an iterative approach is used to solve this problem.

For MRC at the eavesdropper, the initial guess is used to calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (4.8), (4.23), (4.9), and (4.24), respectively. $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ are then substituted in (4.26) along with SNR_A from (4.17) and SNR_B from (4.19) to calculate $C_{S,A}$ and $C_{S,B}$, respectively. Then $C_{S,A}$ and $C_{S,B}$ are compared and the 4 MRC cases are employed to maximize the secrecy capacity. If the current optimal solution, $\mathbf{x}_{k+1}$, satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$ and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $\left[\theta^*, \widetilde{\theta}^*, P_A^*, P_B^*, P_J^*\right]^T$ is summarized in Algorithm 1.

For SC at the eavesdropper, the initial guess is used to calculate $SNR^{(1)}_{E,A}$, $SNR^{(2)}_{E,A}$, $SNR^{(1)}_{E,B}$, and $SNR^{(2)}_{E,B}$ given by (4.8), (4.23), (4.9), and (4.24), respectively. The values of $SNR^{(1)}_{E,A}$ and $SNR^{(2)}_{E,A}$ are compared to determine which expression for $C_{S,A}$ to consider, and the values of $SNR^{(1)}_{E,B}$ and $SNR^{(2)}_{E,B}$ are compared to determine which expression for $C_{S,B}$ to consider. The results of these comparisons determine which case in Subsection 4.3.2 to employ. $\mathbf{x}_0$ is then used to calculate values of $C_{S,A}$ and $C_{S,B}$. Next, $w^{SC}_{(.)}$ is approximated using the SCM method and the resulting $\overline{w}^{SC}_{(.)}(\mathbf{x})$ is used in (4.66a) to solve the optimization problem. If the current optimal solution, $\mathbf{x}_{k+1}$, satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$ and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $\left[\theta^*, \widetilde{\theta}^*, P_A^*, P_B^*, P_J^*\right]^T$ is summarized in Algorithm 2.

4.5 Results and Discussion

In this section, the secrecy capacity is evaluated for a two-way relay network with a friendly jammer in the presence of an eavesdropper. Users A and B can only communicate through R since there is no direct link between them. The simulation parameters are as follows unless noted otherwise. The noise variance is $\sigma^2 = 10^{-3}$, $\sigma_e^2 = 0.1$, $T = 1$, the optimization tolerance is $\epsilon = 0.001$, $\Phi = 0$, and the energy conversion efficiency is $\zeta = 0.5$. The channel gains $|h_{AR}|^2$, $|h_{JR}|^2$, $|h_{JE}|^2$, and $|h_{BR}|^2$ are exponential random variables with mean $\lambda = 1$, $|h_{RE}|^2$ and $|h_{BE}|^2$ are exponential random variables with mean λ_{Eve}, and $|h_{AE}|^2$ is an exponential random variable with mean $\frac{1}{\lambda_{Eve}}$, $\lambda_{Eve} \in \{1, 2, 3\}$. The node locations are normalized to the distance

Algorithm 2 Optimization of the Secrecy Capacity, C_S, for MRC at the Eavesdropper

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$

```
1: while |C_{S,k} − C_{S,k−1}| > ε do
2:     Calculate the monomial approximation \overline{w} for w using the single condensation method at x = [θ_k, \tilde{θ}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T
3:     k = k + 1
4:     Solve the optimization problem in (4.66) using \overline{w} to find [θ_{k+1}, \tilde{θ}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}]
5:     Using the solution in step 4, calculate C_{S,A} and C_{S,B}
6:     if C_{S,A} ≥ 0 and C_{S,B} ≥ 0 then
7:         Go to step 1
8:     else
9:         Continue to the next case of C_{S,A} and C_{S,B}
10:    end if
11:    Solve the optimization problem in (4.29) to obtain [θ_k, \tilde{θ}_k, P_{A,k}, P_{B,k}, P_{J,k}]
12: end while
13: Assign [θ^*, \tilde{θ}^*, P_A^*, P_B^*, P_J^*]^T = [θ_k, \tilde{θ}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T and C_S = C_{S,k}
```

between A and B so that A and B are at (0, 0) and (1, 0), respectively. R is at the midpoint, (0.5, 0), J is at (0.5, −0.5), $P_T = 10$ dB, and $P_J = 0.1P_T$.

Fig. 4.3 presents the secrecy capacity versus the total transmit power, P_T, for $\lambda_{Eve} = 1$ with SC and MRC at the eavesdropper, and the corresponding secrecy capacity from [109]. This shows that the secrecy capacity increases in all cases as the total transmit power increases. In [109], the secrecy capacity at A and B is defined as $C_i = \frac{T}{2}\log_2\left(\frac{1+SNR_i}{(1+SNR_{E,i}^{(1)})(1+SNR_{E.i}^{(2)})}\right)$, $i \in \{A, B\}$, i.e. diversity combining was not employed by the eavesdropper. However, in this chapter, the received SNR at the eavesdropper is either the combination of $SNR_{E,i}^{(1)}$ and $SNR_{E,i}^{(2)}$ using MRC, or the maximum is selected using SC as given in (4.26). At $P_T = 15$ dB, the difference in secrecy capacity between SC and [109] is 1.01 bit/sec/channel use and the difference between MRC and [109] is 0.21 bits/sec/channel use. The reason is that SC selects

Algorithm 3 Optimization of the Secrecy Capacity, C_S, for SC at the Eavesdropper

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$

while $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**

2: Calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$

if $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$ **then**

4: Calculate the monomial approximation $\overline{w}$ for w using the single condensation method at $\mathbf{x} = \left[\theta_k, \widetilde{\theta}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$

$k = k + 1$

6: Solve the optimization problem in (4.66) using $\overline{w}$ to find $\left[\theta_{k+1}, \widetilde{\theta}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}\right]$

Using the solution in step 6, calculate $C_{S,A}$ and $C_{S,B}$

8: **if** $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**

Go to step 1

10: **else**

Continue to the next case of $C_{S,A}$ and $C_{S,B}$

12: **end if**

else

14: Continue to the next case of $SNR_{E,A}^{(1)} \gtreqless SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \gtreqless SNR_{E,B}^{(2)}$

end if

16: Solve the optimization problem in (4.29) to obtain $\left[\theta_k, \widetilde{\theta}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]$

end while

18: Assign $\left[\theta^*, \widetilde{\theta}^*, P_A^*, P_B^*, P_J^*\right]^T = \left[\theta_k, \widetilde{\theta}_k, P_{A,k}, P_{B,k}, P_{J,k}\right]^T$ and $C_S = C_{S,k}$

only one wiretap link which reduces the SNR at the eavesdropper. As a result, the secrecy capacity of the network with SC at the eavesdropper is higher than that with MRC.

Fig. 4.4 presents the secrecy capacity versus the power splitting factor, θ, with SC and MRC for $\sigma_e^2 = 0$ and 0.1. This shows that SC outperforms MRC for the given values of σ_e^2 and λ_{Eve}, and the secrecy capacity for imperfect CSI, $\sigma_e^2 = 0.1$, is better than that for perfect CSI, $\sigma_e^2 = 0$, for all values of θ. Considering the SNR expressions of the eavesdropper links, the denominators of (4.8), (4.23), (4.9), and (4.24) contain σ_e^2, so increasing this term reduces the SNR at E.

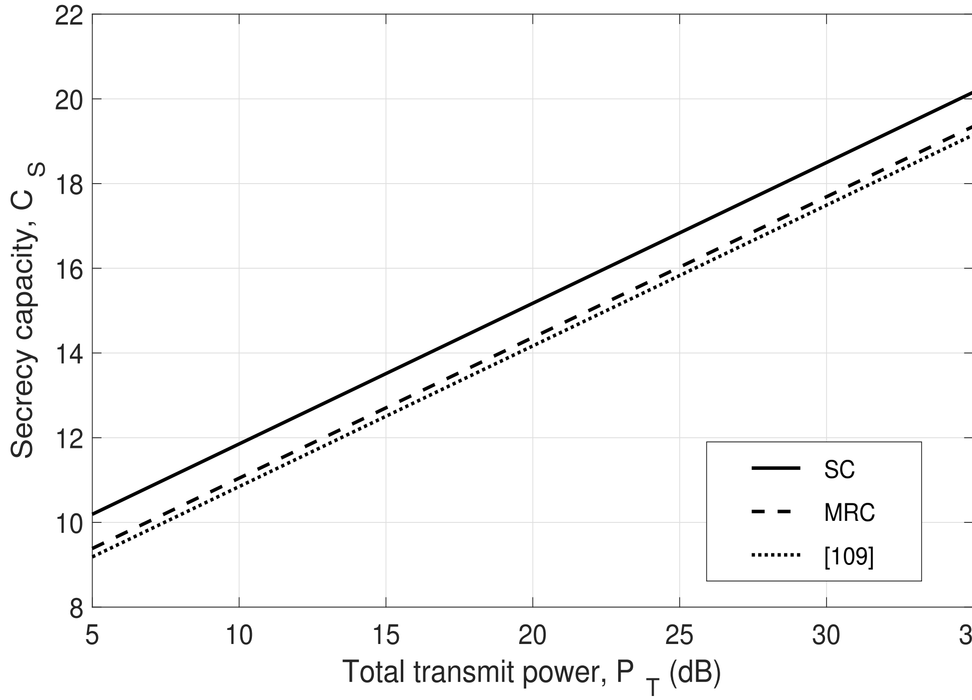

Figure 4.3: The secrecy capacity versus the total transmit power, P_T, with $\lambda_{Eve} = 1$ and $\sigma_e^2 = 0$.

4.5.1 Channel Estimation Error

Figs. 4.5 and 4.6 present the effect of the channel estimation error variance, σ_e^2, on the secrecy capacity. Fig. 4.5 shows the secrecy capacity for $\lambda_{Eve} = 1, 2$, and 3. A higher value of σ_e^2 means that the eavesdropper is less able to estimate the wiretap links so the secrecy capacity improves. The difference in secrecy capacity between SC and MRC is 0.283, 0.033, and 0.031 bits/sec/channel use for $\lambda_{Eve} = 1, 2$, and 3, respectively, at $\sigma_e^2 = 0.1$. Thus, increasing λ_{Eve} decreases the gap between SC and MRC. This is because a larger λ_{Eve} improves the corresponding link of the eavesdropper and degrades the other eavesdropper link. Fig. 4.6 shows the secrecy capacity versu the channel estimation error variance for $\theta = 0.8$ and 0.2 at $\lambda_{Eve} = 1$. At $\sigma_e^2 = 0.01$, SC outperforms MRC with a difference of 0.287 at $\theta = 0.8$ and 0.285

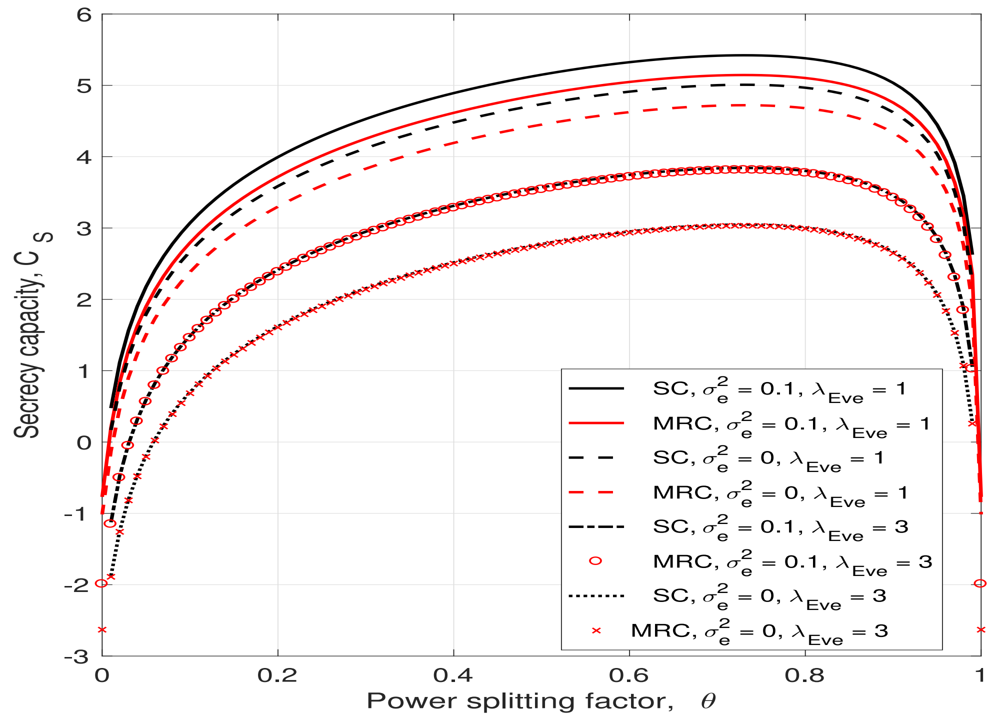

Figure 4.4: The secrecy capacity versus the power splitting factor, θ, for different values of λ_{Eve} and σ_e^2 with $P_J = 0.1P_T$ and $P_T = 10$ dB.

at $\theta = 0.2$. Thus, increasing θ improves the performance of SC and MRC but has little effect on the difference between them.

4.5.2 Jammer, Cancellation Factor, and Locations

The secrecy capacity versus the jamming signal cancellation factor, Φ, is presented in Fig. 4.7 for $\sigma_e^2 = 0$ and 0.5. This shows that SC outperforms MRC for both values of σ_e^2. When $\Phi = 0$, the secrecy capacity is highest because the jamming signal at the relay is completely cancelled. As Φ increases, more jamming power is amplified and forwarded to A and B. Thus, the noise at A and B increases which degrades their SNRs and thus decreases the secrecy capacity. The difference in secrecy capacity with SC is 0.933 bits/sec/channel use at $\Phi = 0.1$ but decreases to 0.744 bits/sec/channel

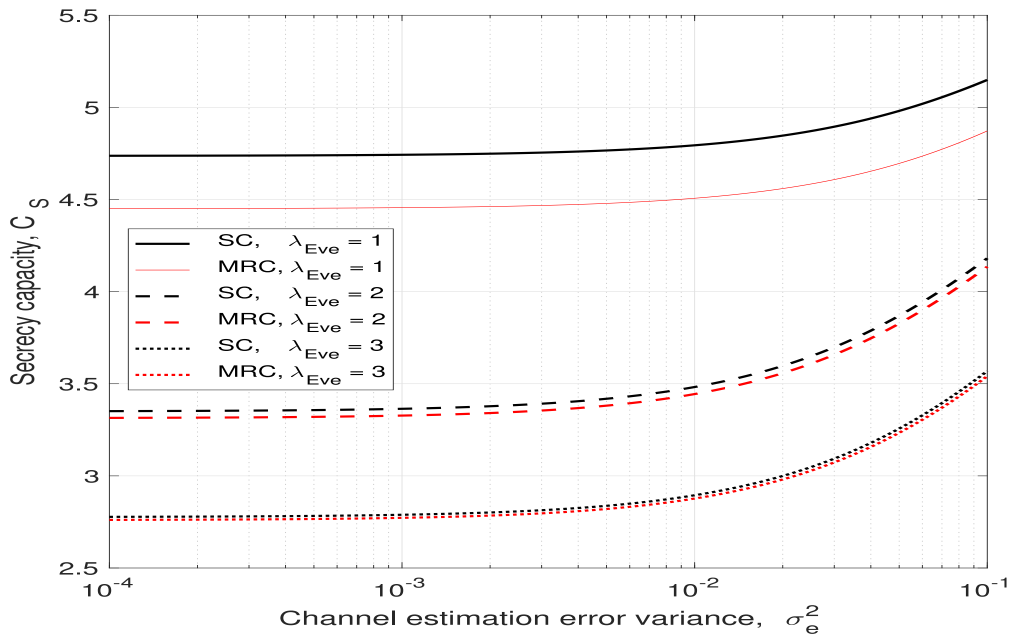

Figure 4.5: The secrecy capacity versus the channel estimation error variance, σ_e^2, for three values of λ_{Eve} with $\theta = 0.5$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

use at $\Phi = 0.8$. The results in [109] show that the secrecy capacity without SC is more sensitive to Φ, and the secrecy capacity decreases at a faster rate as Φ increases.

In the following figures, the secrecy capacity is considered for different locations of the eavesdropper and jammer. The channel links can be expressed as $h_{ij} = \frac{f_{ij}}{d_{ij}^m}$ where f_{ij} is an exponential random variable with mean $= 1$, $m = 2.7$ is the path loss exponent, and d_{ij} is the distance between i and j. Figs. 4.8 and 4.9 present the secrecy capacity versus Φ for SC and MRC at the eavesdropper, respectively. The jammer is at (0.5, -0.5) and the location of the eavesdropper is (0.5, -1) and (0.2, -0.2) with $d_{AE} = 1.118$ and 0.282, respectively. These results show that secrecy capacity increases as d_{AE} increases from 0.282 to 1.118 for both values of σ_e^2. The

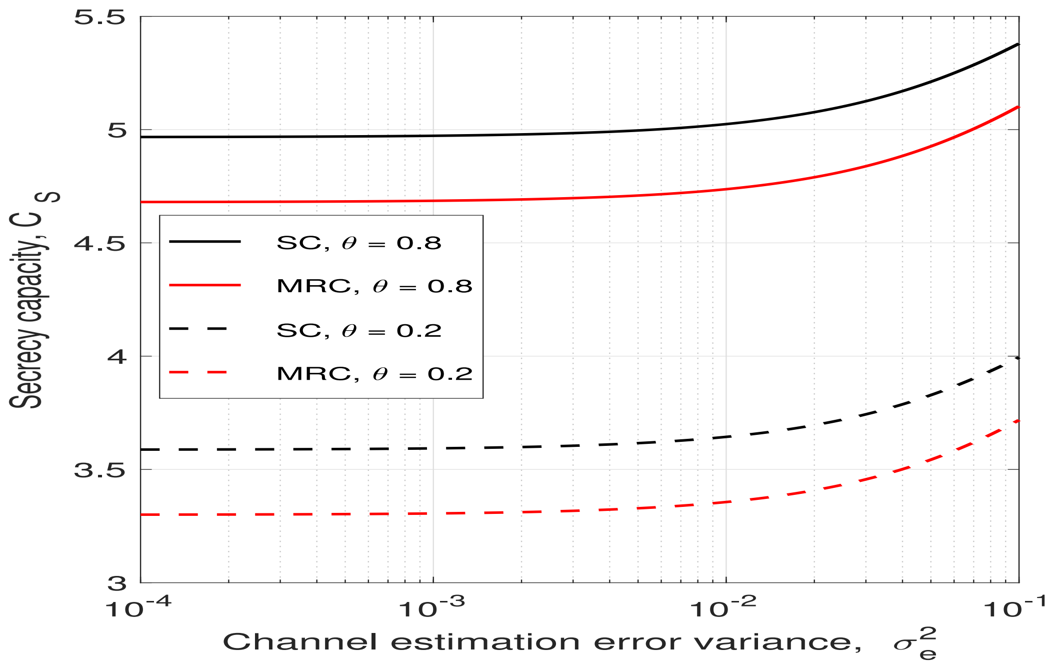

Figure 4.6: The secrecy capacity versus the channel estimation error variance, σ_e^2 with $\theta = 0.8$ and 0.2, $\lambda_{Eve} = 1$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

reason is that as d_{AE} increases, less power is required to be allocated to the jammer. Hence, more power is allocated to A and B, and more energy is harvested at R. Fig. 4.8 shows that when $\sigma_e^2 = 0$, the difference in SC secrecy capacity for $d_{AE} = 1.118$ and 0.282 is 1.06 bit/sec/channel use, and this increases to 1.14 bit/sec/channel use for $\sigma_e^2 = 0.1$. Fig. 4.9 shows that when $\sigma_e^2 = 0$, the difference in MRC secrecy capacity for $d_{AE} = 1.118$ and 0.282 is 0.93 bit/sec/channel use, and this increases to 1.02 bit/sec/channel use for $\sigma_e^2 = 0.1$.

Fig. 4.10 presents the effect of Φ on the secrecy capacity when the jammer is close to the relay. In this case, E is at $(0.2, -1)$ and J is at $(0.5, -0.1)$, so significant jamming power is received by the relay. These results show that a small increase in Φ causes a significant drop in secrecy capacity for both SC and MRC. For example,

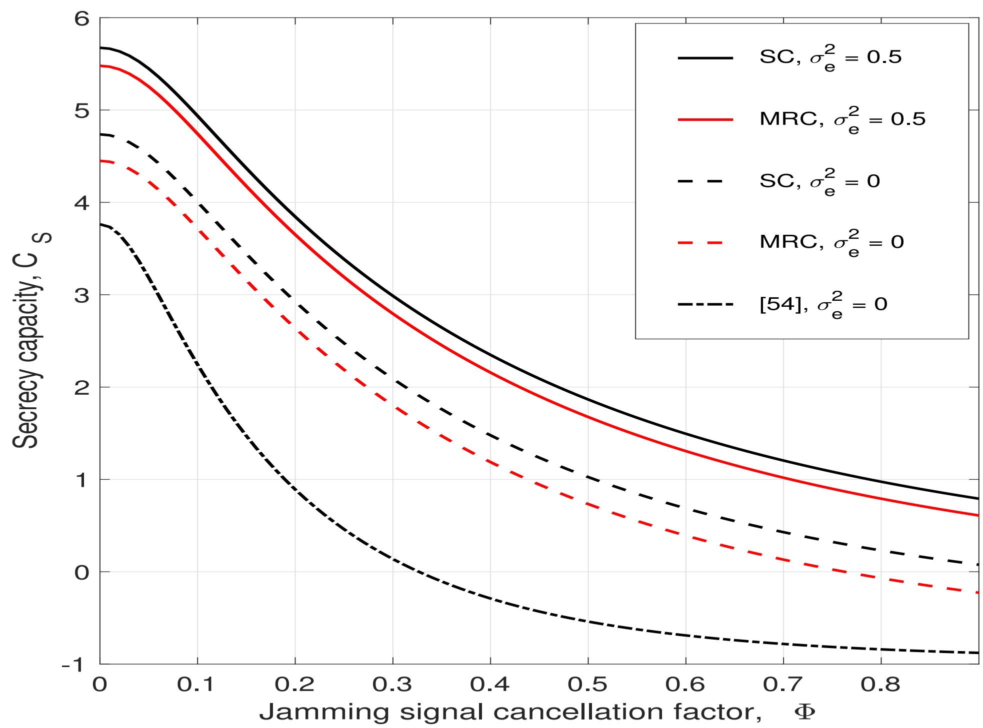

Figure 4.7: The secrecy capacity versus the jamming signal cancellation factor, Φ with $\lambda_{Eve} = 1$, $\theta = 0.5$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

with SC and $\theta = 0.5$, the secrecy capacity drops by 4.331 bit/sec/channel use when Φ increases from 0 to 0.01 and by 6.291 bit/sec/channel use when Φ increases from 0.01 to 0.1. This is because the jamming signal at the relay is stronger since the jammer is closer to the relay.

Fig. 4.11 shows the secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), when the jammer is located at $(0.5, -0.5)$ and without a jammer. Results are given for y-axis eavesdropper positions -0.2, -0.5, and -0.8 and MRC at the eavesdropper. The solid lines are for the case with a jammer at $(0.5, -0.5)$ and the other lines correspond to no jammer. When the eavesdropper is at $x = 0.5$, i.e. midway between A and B, the secrecy capacity is the highest. Further, the secrecy capacity is better with a jammer since the jamming signal reduces the SNR at the

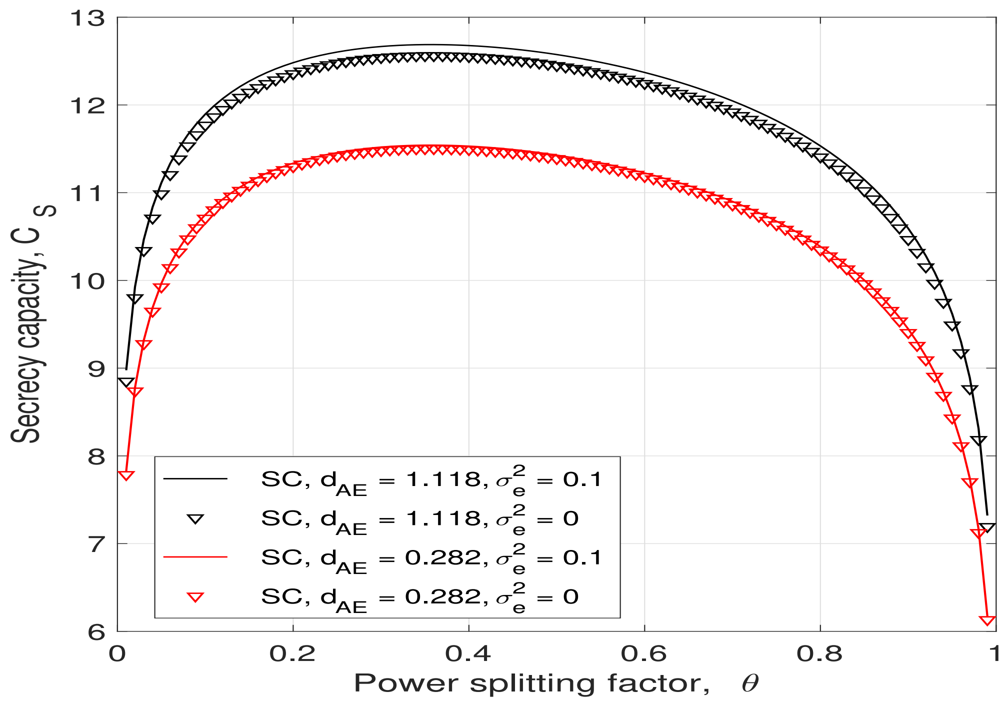

Figure 4.8: The secrecy capacity for SC at the eavesdropper with $d_{AE} = 0.282$ and 1.118, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

eavesdropper regardless of their y-axis position. The lowest secrecy capacity in both cases (with and without a jammer), is when the eavesdropper is at $x = 0$ or $x = 1$ since the SNR at the eavesdropper from A and B, respectively, is highest.

Fig. 4.12 shows the secrecy capacity versus the x-axis location of the eavesdropper (employing SC), when the jammer is located at $(0.5, -0.5)$ and without a jammer. Again, results are given for y-axis eavesdropper positions -0.2, -0.5, and -0.8. Similar to Fig. 4.11, the secrecy capacity is highest when the eavesdropper is at $x = 0.5$ and the lowest secrecy capacity is when the eavesdropper is at $x = 0$ or $x = 1$. Further, the secrecy capacity is better with a jammer since the jamming signal reduces the SNR at the eavesdropper regardless of their y-axis position. A higher secrecy capacity is achieved when the eavesdropper employs SC rather than

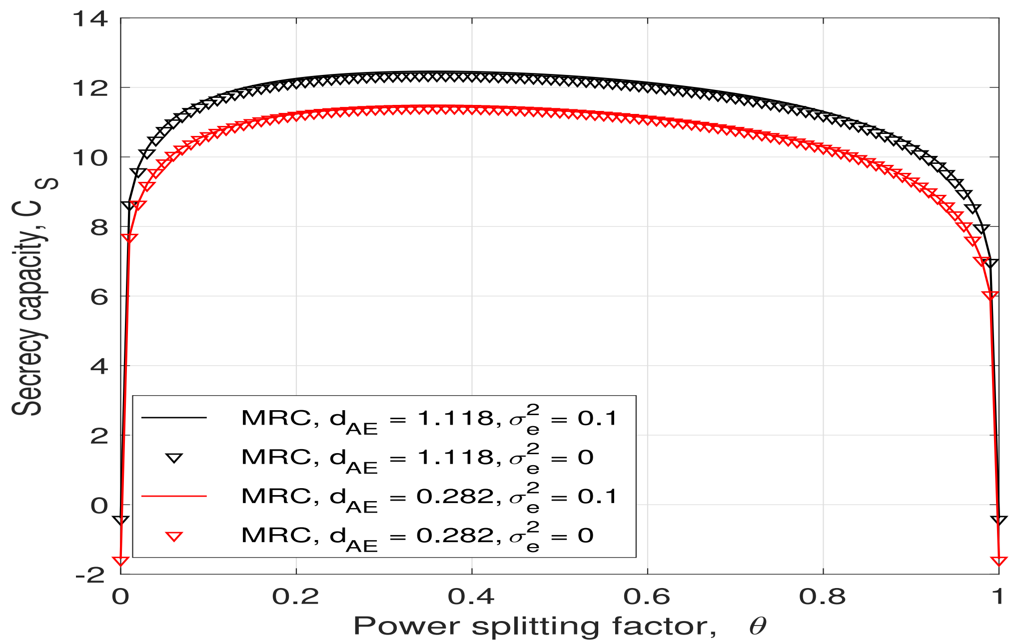

Figure 4.9: The secrecy capacity for MRC at the eavesdropper with $d_{AE} = 0.282$ and 1.118, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

MRC.

Fig. 4.13 presents the secrecy capacity versus the x-axis position of the eavesdropper (employing MRC), with the jammer located at $(0.5, -0.5)$, $(0.5, -1)$, $(0.2, -0.5)$, $(0.2, -1)$, $(0.7, -0.5)$, and $(0.7, -1)$. The location of the eavesdropper changes from $(0, -0.7)$ to $(1, -0.7)$. In all cases, the secrecy capacity is a minimum when the eavesdropper is at $x = 0$ or $x = 1$, which is closest to A or B, respectively. As the eavesdropper moves from $x = 0$ to 1, the jamming signal power at the eavesdropper increases so the secrecy capacity increases. The secrecy capacity decreases as the eavesdropper moves farther from the jammer after the maximum secrecy capacity has been reached.

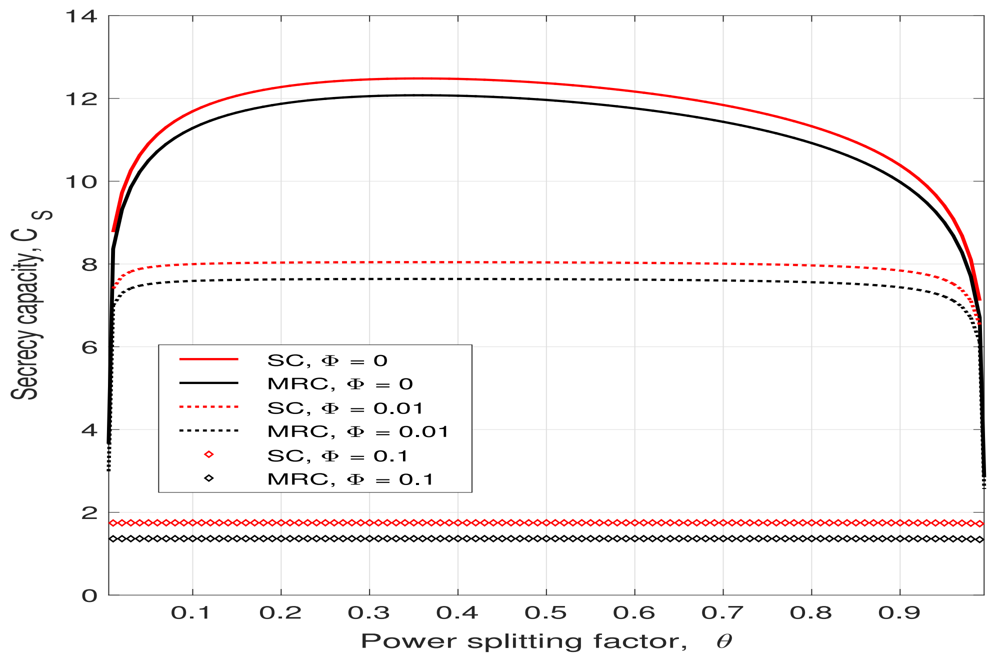

Figure 4.10: The secrecy capacity for different values of Φ with the jammer at $(0.5, -0.1)$, the eavesdropper at $(0.2, -1)$, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

4.5.3 Time Complexity

Matlab R2017a was used to conduct all simulations on a MacBook Pro laptop with an Intel Core i5 processor. An average time of 84.01 s was required to run Algorithm 1 (MRC) and 4.65 s to run Algorithm 2 (SC). SC selects the maximum of $SNR_{E,i}^{(1)}$ and $SNR_{E,i}^{(2)}$ while MRC combines $SNR_{E,i}^{(1)}$ and $SNR_{E,i}^{(2)}$ to obtain the achievable rate at the eavesdropper. The average number of iterations required to solve the optimization problem for a given total transmit power was approximately 2 for both MRC and SC at the eavesdropper. However, Algorithm 2 was faster because the number of monomial terms to be approximated with SC is 64 while with MRC it is 250.

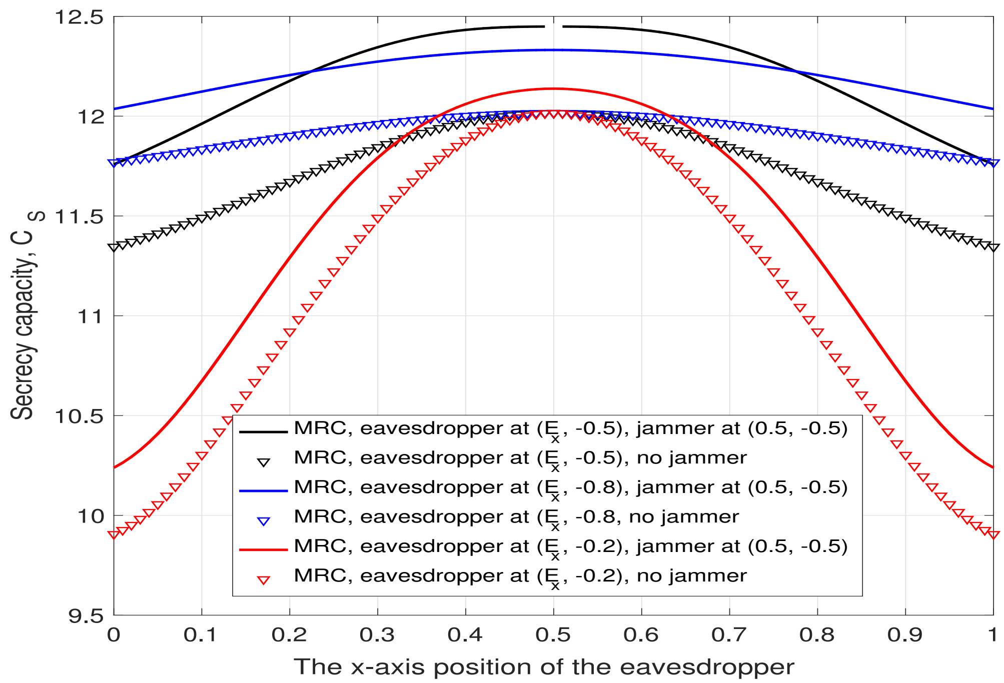

Figure 4.11: The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), with a jammer at a fixed location and without a jammer.

4.6 Conclusion

In this chapter, the secrecy capacity was investigated for a two-way energy-constrained relay network in the presence of an eavesdropper. A friendly jammer was used to reduce the ability of the eavesdropper to intercept the user signals. The secrecy capacity was maximized by jointly optimizing the power splitting factor, θ, and the transmit power of the two users, A and B, and the jammer J. The single condensation method (SCM) was employed to convert the objective function of the corresponding optimization problem into a posynomial form suitable for geometric programming (GP). Then, GP was used to transform the non-convex objective function to obtain a convex optimization problem. Two diversity combining techniques, MRC and SC, were employed

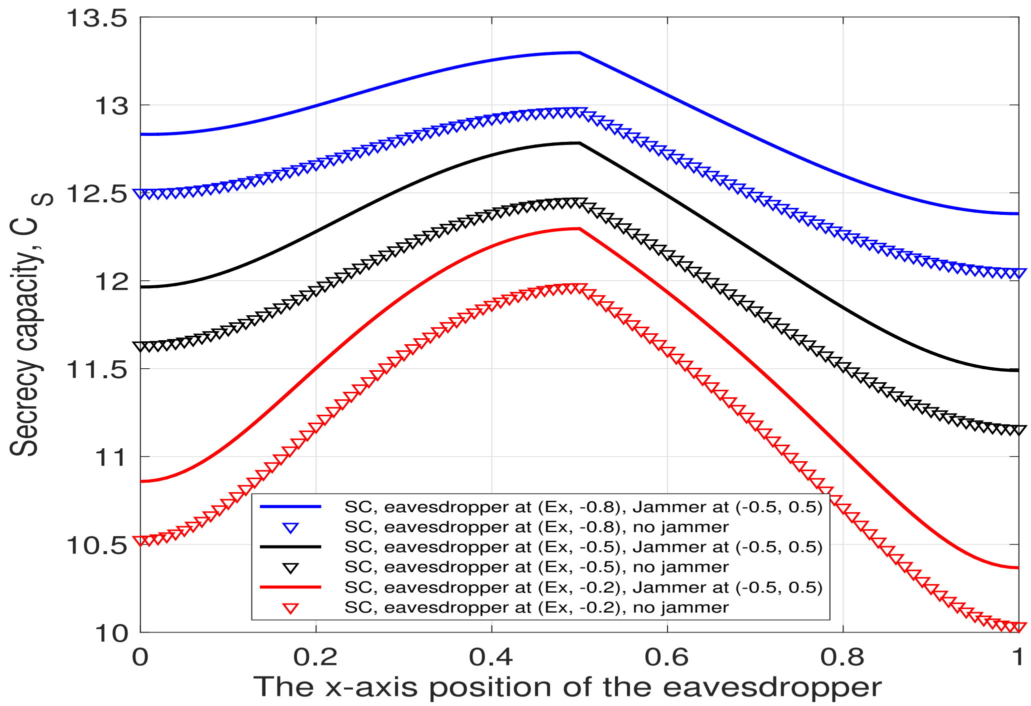

Figure 4.12: The secrecy capacity versus the x-axis location of the eavesdropper (employing SC), with a jammer at a fixed location and without a jammer.

at the eavesdropper. Imperfect cancellation of the jamming signal at the relay was also considered. Results were presented which show that imperfect jamming signal cancellation at the relay degrades the secrecy capacity. In addition, utilizing a jammer improves the secrecy capacity and increases the amount of harvested energy at the relay. Further, the secrecy capacity is higher if the jammer is located closer to the eavesdropper.

Imperfect channel estimation at the eavesdropper was considered. It was shown that as the estimation error increases, the secrecy capacity improves. MRC has shown to provide a lower secrecy capacity than SC. Thus, to achieve the SC secrecy capacity with MRC at the eavesdropper, a higher SNR is required at A and B.

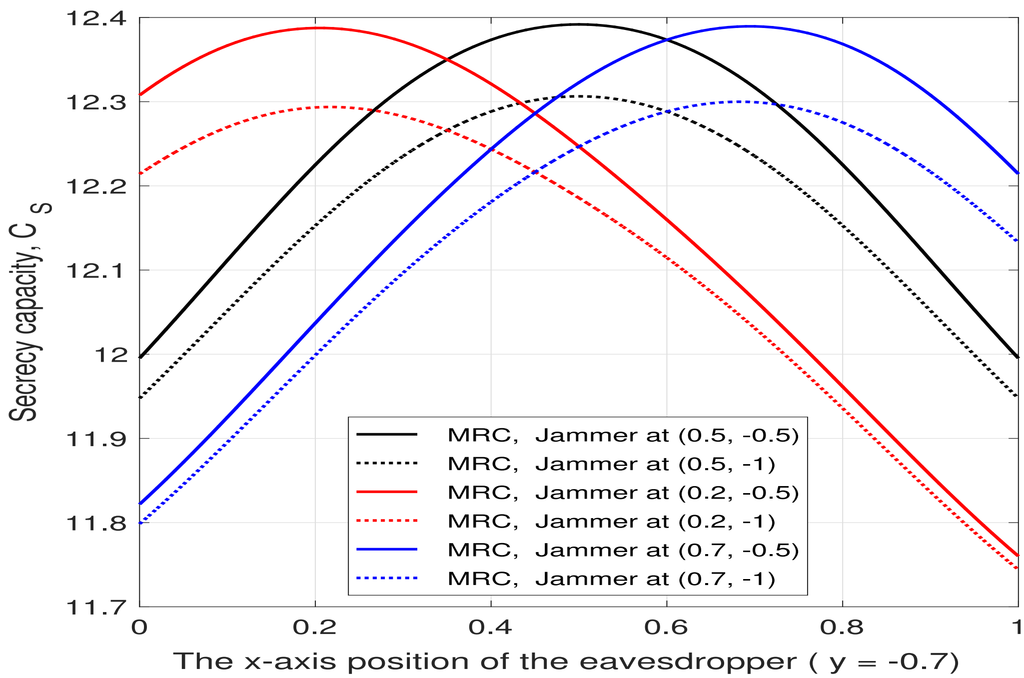

Figure 4.13: The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), for different jammer locations with $\sigma_e^2 = 0$, $\Phi = 0$, and $P_T = 10$ dB.

Chapter 5

Optimization of Physical Layer Security in Two-Way SWIPT Relay Networks with Imperfect CSI and a Friendly Jammer

In this chapter, the security of two-way relay communications in the presence of an eavesdropper is investigated. Two users communicate via a relay that depends solely on energy harvesting to amplify and forward the received signals. Time switching is employed at the relay to harvest energy and obtain user information. A friendly jammer is utilized to hinder the eavesdropping from wiretapping the information signal. The eavesdropper employs maximal ratio combining and selection combining to improve the signal to noise ratio of the wiretapped signals. Geometric programming (GP) is used to maximize the secrecy capacity of the system by jointly optimizing the time switching ratio of the relay and transmit power of the two users and jammer.

The impact of imperfect channel state information at the eavesdropper for the links between the eavesdropper and the other nodes is determined. Further, the secrecy capacity when the jamming signal is not perfectly canceled at the relay is examined. The secrecy capacity is shown to be greater with a jammer compared to the case without a jammer. The effect of the relay, jammer, and eavesdropper locations on the secrecy capacity is also studied. It is shown that the secrecy capacity is greatest when the relay is at the midpoint between the users. The closer the jammer is to the eavesdropper, the higher the secrecy capacity.

5.1 Introduction

There has also been a shift in wireless network research from spectral efficiency and quality of service (QoS) constraints to energy efficiency and green communication [111] to reduce the power consumption [112]. Green energy resources such as solar, wind, thermal and mechanical vibrations can be employed to improve the energy efficiency of energy-constrained devices such as in wireless sensor networks. Energy harvesting (EH) to convert the available energy in the surrounding area into electricity has been the subject of recent research [110]. Energy harvesting (EH) from radio frequency (RF) signals has employed in wireless communication systems to prolong the lifetime of devices in energy-constrained systems [60]. Wireless power transmission (WPT) for EH is a promising solution to sustainable energy for wireless devices [113, 114, 115]. It can provide a reliable source of energy for devices which are difficult to service due to mobility and location [20, 116, 117].

RF signals can carry both information and energy, so WPT in wireless communication systems is known as simultaneous wireless information and power transfer

(SWIPT) [114],[20], [61], [62], and [15]. Two circuits are usually employed to harvest energy and retrieve information [95]. Two SWIPT protocols have been developed, power splitting (PS) and time switching (TS) [49]. With TS, the receiver switches between the two circuits while in PS, a fraction of the signal is directed to the EH circuit and the remaining part is sent to the information retrieval circuit. The maximum transmission rate using optimal PS and TS was derived in [63] and [64], respectively. In [63], the outage probability was obtained for a decode and forward (DF) relay network, and the optimal transmission rates with PS and TS were determined. A SWIPT-enabled relay was considered in [64] for three scenarios, ideal (simultaneous EH and information retrieval), PS, and TS, and the maximum rates for each were obtained. PS and TS can be used separately or combined as a hybrid protocol where the relay switches between PS and TS [65] . The optimal TS and PS ratios were derived to maximize the throughput with an EH relay and the hybrid protocol was shown to provide the best performance. In [66] and [67], joint PS and TS schemes were considered for amplify and forward (AF) and DF relay networks, respectively. In [66], the outage probability, energy efficiency, and network throughput were derived as a function of the PS and TS ratios, and the network throughput maximized. In [67], two optimization problems were jointly formulated to minimize the outage probability. These outage probabilities were shown to be better than that with the hybrid protocol in [65]. The system throughput of a cognitive two-way relaying network was maximized in [68] using an optimal offline joint relay selection and power allocation scheme.

Wireless transmissions are more vulnerable to eavesdropping compared to wired signals given the broadcast nature of wireless systems. The physical layer security of the wiretap channel was introduced in [73] and is defined as the difference between the capacity of the link between the source and destination and the capacity of the wiretap link between the source and eavesdropper. This can be used to assist upper-layer cryptographic techniques [96], [82], and [97]. Physical layer security-based solutions exploit the physical properties of wireless channels, such as fading and interference, to secure transmissions between users in the presence of eavesdroppers [98], [99].

Physical layer security has been considered for relay networks [118], cellular networks [119], [120], cognitive radio networks [121], internet of things (IoT) networks [122], and massive multiple-input multiple-output (MIMO) networks [123]. However, wireless channel conditions have a significant effect on the solutions [100]. Physical layer security with cooperative relaying has been employed to overcome this issue [101]. This was first studied in [74] for an untrusted relay network which was considered as a possible eavesdropper. One-way communications was examined in [75] for DF and AF EH relays and it was shown that DF outperforms AF in terms of secrecy performance. The secrecy capacity was analyzed in [76] for PS and TS relaying protocols in a one-way untrusted relay network, and PS outperformed TS.

Two-way relay channels in which two users simultaneously exchange messages were first considered in [124] and more recently in [125]. The spectral efficiency with two-way relaying is higher than with one-way relaying. In [77], a two-way EH-based relay network with an eavesdropper was investigated. The secrecy capacity was maximized and an iterative method employed to obtain the optimal TS and PS ratios for high signal to noise ratios (SNRs) based on the instantaneous channel state information (CSI). It was shown that near optimal secrecy capacity is achievable with proposed approach even when the wiretap channels are unknown. Joint secrecy capacity and energy efficiency were considered in [78] for a two-way untrusted relay network. The probability of successful eavesdropping in a two-way EH DF relay network was derived in [79] assuming independent κ-μ shadowed fading. It was shown that allocating extra power for information decoding over a small reception time improves the secrecy capacity. In [80], the intercept probability was derived for a two-way DF EH relay network in the presence of multiple eavesdroppers. The effect of the PS factor on the secrecy capacity was studied. The secrecy capacity of a two-way communication network with multi-antenna time-switching relays in the presence of an eavesdropper was maximized in [81] . It this case, the secrecy capacity with equal transmit power is better than with unequal transmit power.

Cooperative jamming can improve the secrecy capacity [102, 103, 42]. Friendly jamming (FJ) and Gaussian noise jamming (GNJ) have been considered to improve the secrecy capacity of wireless communication networks. The jamming signal is known at the receiver when FJ is used [82], while with GNJ the jamming signal is considered to be noise at the receiver [83]. While both of FJ and GNJ can improve the secrecy capacity, the performance with FJ is better because the users can cancel this signal. In [84], a system with two eavesdroppers and an EH friendly jammer was considered. One eavesdropper is near the user while the other is near the jammer, and they cooperate to obtain user signals and mitigate the effects of jamming. The secrecy capacity and energy efficiency of the network were maximized by optimizing the jamming signal power. In [105], the secrecy capacity with a friendly jammer was investigated for a one-way untrusted relay network with non line-of-sight transmissions. A jammer was employed in [85] for an EH-based relay network to secure two-way communications, and a lower bound was derived for the secrecy capacity at high SNRs. It was shown that FJ with two-way communications outperforms one-way and the two-way communications without jamming and with GNJ. In [86], the secrecy capacity of one-way untrusted relay communications was jointly optimizing considering the transmit and jamming powers with an EH relay threshold. The secrecy performance with untrusted EH relays and energy-aware distributed beamforming was investigated in [87]. The secrecy capacity was increased in [88] by choosing GNJ and relay nodes from multiple friendly but selfish intermediate nodes. Price competition was used for power allocating to these nodes and their profit to maximize the secrecy capacity was determined. A two-way untrusted relay system with multiple friendly jammers was considered in [33] and the jamming power was optimized to improve the secrecy capacity. In [89], a network with multiple relay-user pairs was investigated in the presence of multiple eavesdroppers. Joint relay-user pairs and friendly jammer selection were determined to maximize the secrecy capacity. The secrecy capacity was optimized in [33] using a Stackelberg game for power allocation between users and friendly jammers.

In [90], adaptive cooperative jamming in the presence of multiple eavesdroppers was investigated for an EH relay. The secrecy capacity was maximized by optimizing the power allocation factor. A two-way EH relay network with an eavesdroppers and a friendly jammer was considered in [91]. The optimal PS and TS factors were derived to maximize the secrecy capacity and PS was shown to be better than TS. A two-way relay network with partial relay selection and hybrid PS and TS at the intermediate nodes was investigated in [92]. It was shown that secure communications is possible with an appropriate selection of parameters.

In the results given above, perfect knowledge of the CSI for the user and relay signals at the eavesdropper was assumed. However, this is not a practical assumption considering unknown delays and channel estimation errors. In two-way relay networks, imperfect CSI results in imperfect self-interference cancellation [106]. In [107], a transmission scheme was proposed for multiple input single output (MISO) channels with imperfect CSI for the user and eavesdropper channels with cooperative jamming. In [108], the CSI for the channel between the jammer and eavesdropper was assumed to be unknown and imperfect CSI assumed between the jammer and user. The impact of imperfect CSI on the secrecy outage capacity with cooperative jamming was analyzed. Although imperfect CSI has received some research attention, the impact of imperfect CSI on the security of a SWIPT two-way relay network has not yet been studied.

In this chapter, the physical layer security of a two-way communication system with a relay employing TS to harvest energy and a friendly jammer, and imperfect CSI at the eavesdropper is studied. The eavesdropper employs maximal ratio combining (MRC) and selection combining (SC) to degrade the secrecy capacity. The power allocated to two users, a relay, and a jammer are jointly optimized in the presence of an eavesdropper with imperfect CSI. This system has not been previously considered in the literature for a TS EH relay. Further, the effect of imperfect cancellation of the jamming power at the relay is studied. The main contributions of this chapter are as follows.

1. The effect of channel estimation errors on the secrecy capacity is investigated when the eavesdropper employs MRC and SC. Imperfect CSI at the eavesdropper has not been previously considered.

2. The secrecy capacity is maximized by jointly optimizing the TS ratio and trans-

mit powers of the two users and jammer.

3. The single condensation method (SCM) is used to convert the objective function into a standard GP form. Then, geometric programming (GP) is employed to transform the optimization problem into a convex form.

4. The effect of imperfect cancellation of the jamming signal at the relay is examined. This has not been considered previously in the literature.

5. The effect of the TS ratio on the secrecy capacity is investigated.

6. The secrecy capacity is evaluated with and without a jammer. In addition, results are given for different eavesdropper and jammer locations.

The remainder of this chapter is organized as follows. The system model is given in Section 5.2. The secrecy capacity for the two-way relay network is presented in Section 5.3 for MRC and SC. In Section 5.4, the optimization problem is formulated and converted to a convex form. Section 5.5 presents the simulation results and finally, some concluding remarks are given in Section 5.6.

5.2 System Model

The two-way relay network considered here is shown in Fig. 5.1. It consists of two users A and B, a trusted relay R, a friendly jammer J, and an eavesdropper E. Each of these nodes has a single antenna and operates in half-duplex mode. The eavesdropper is randomly located near the relay to listen to the signals received by and transmitted from the relay. The A-R, B-R, A-E, B-E, R-E, J-R, and J-E

channel links are denoted by h_{AR}, h_{BR}, h_{AE}, h_{BE}, h_{RE}, h_{JR}, and h_{JE}, respectively. Rayleigh fading is assumed so the channel coefficients are Rayleigh random variables. Then, the channel gains, $|h_{ij}|^2$ are exponentially distributed random variables with mean λ. The channels are assumed to be reciprocal such that $h_{ij} = h_{ji}$, $\{i,j\} \in \{A, B, R, J, E\}, i \neq j$. The parameters n_A, n_B,n_R, and n_E denote the additive white Gaussian noise (AWGN) at A, B, R, and E, respectively, with zero mean and variance σ^2.

In this chapter, the practical case is considered where the channels at A, B, R, and J can be estimated accurately given that they are trusted nodes, but there are channel estimation errors at the eavesdropper [107]. The estimated channel gain from the eavesdropper to node i, $i \in \{A, B, R, J\}, i \neq E$, is given by [106]

$$h_{iE} = \widehat{h}_{iE} + e_{iE}, \tag{5.1}$$

where $\widehat{h}_{iE}$ is the estimated channel gain and e_{iE} is the channel estimation error. For simplicity, denote e_{iE} by e_E which is a Gaussian distributed random variable with zero mean and variance σ_e^2. A summary of the notation used in this chapter is given in Table 5.1.

Table 5.1: Notation

Symbol	**Description**
A, B	Users

Continued on next page

Table 5.1 – *Continued from previous page*

Symbol	Description
R	Relay
J	Jammer
E	Eavesdropper
h_{ij}	Channel between node i and node j
$\|h_{ij}\|^2$	Channel gain between node i and node j
$\widehat{h}_{iE}$	Estimated channel between E and node i
$\|\widehat{h}_{iE}\|^2$	Estimated channel gain between E and node i
e_{iE}	Channel estimation error between E and node i
σ_e^2	Channel estimation error variance
n_i	Additive white Gaussian noise (AWGN) at node i
σ^2	AWGN variance
x_i	Signal transmitted by node i
y_i	Signal received at node i
P_A	Transmit power of node A
P_B	Transmit power of node B
P_R	Transmit power of node R
P_J	Transmit power of node J
P_T	Total power constraint
$\mathbf{E}[.]$	Expected value
y_{Re}	Energy harvesting signal at the relay
y_{Ri}	Information retrieval signal at the relay

Continued on next page

Table 5.1 – *Continued from previous page*

Symbol	**Description**
ρ	Time switching (TS) ratio
E_H	Harvested energy
ζ	Energy conversion efficiency
T	Total transmission time
m	Path loss exponent
Φ	Jamming signal cancellation factor
y_R	Information retrieval signal after jamming cancellation
$y_E^{(1)}$	Received signal at E in the first phase
$y_E^{(2)}$	Received signal at E in the second phase
$SNR_{E,A}^{(1)}$	SNR at E for x_B sent to A in the first phase
$SNR_{E,B}^{(1)}$	SNR at E for x_A sent to B in the first phase
$SNR_{E,A}^{(2)}$	SNR at E for x_B sent to A in the second phase
$SNR_{E,B}^{(2)}$	SNR at E for x_A sent to B in the second phase
SNR_A	SNR at A
SNR_B	SNR at B
R_A	Achievable rate at A
R_B	Achievable rate at B
$R_E^{(1)}$	Achievable rate at E in the first phase
$R_E^{(2)}$	Achievable rate at E in the second phase
R_E	Achievable rate at E for both phases
C_A	Secrecy capacity at A

Continued on next page

Table 5.1 – *Continued from previous page*

Symbol	**Description**
C_B	Secrecy capacity at B
C_S	Secrecy capacity

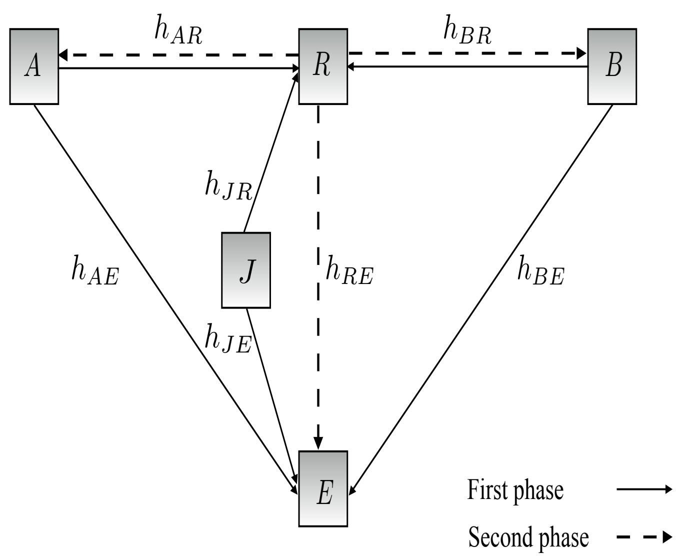

Figure 5.1: System model of a two-way wireless relay network with two users, a jammer, and eavesdropper.

Fig. 5.2 illustrates the two phases required to forward signals between A and B in the relay network. The first phase is dedicated to signal reception and energy harvesting at the relay and is divided into two subphases. As in [49], in the first subphase, all the received signal power is used for energy harvesting. This subphase has durationρT where ρ is the TS ratio, $0 \leq \rho \leq 1$. In the second subphase, all the received signal power is used for information decoding and the duration is $(1-\rho)\frac{T}{2}$.

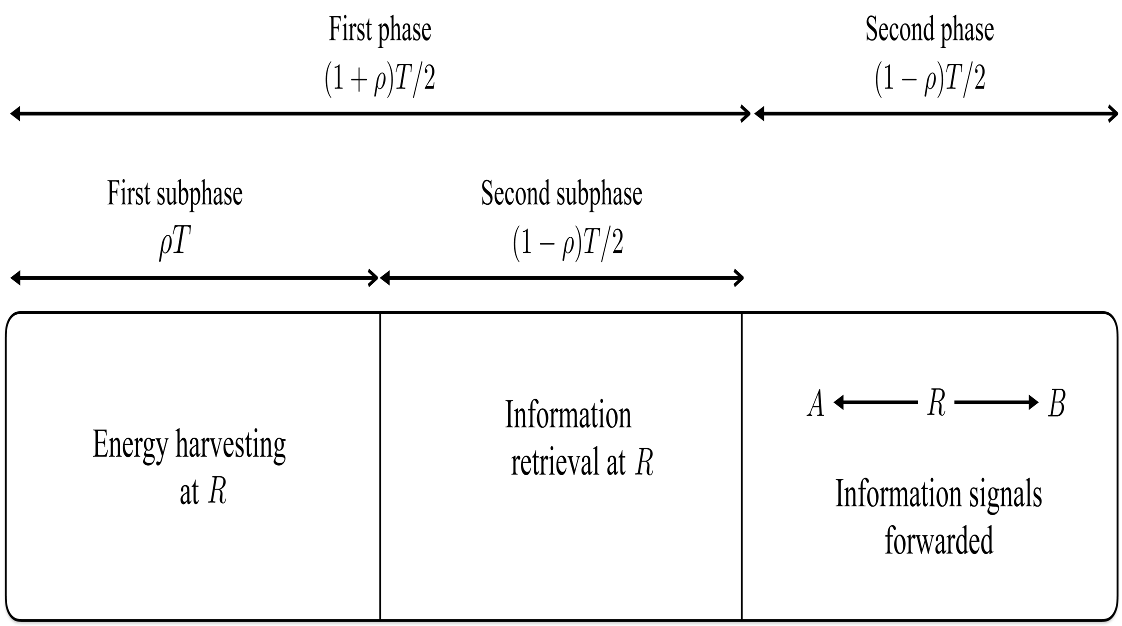

Figure 5.2: Transmission time frame for time switching (TS) in the two-way relay network.

A, B, and J send their signals x_A, x_B, and x_J with $\mathbf{E}[|x_A|^2] = \mathbf{E}[|x_B|^2] = \mathbf{E}[|x_J|^2 = 1$ and transmit powers P_A, P_B, and P_J, respectively, to R. The relay depends solely on energy harvested from the user and jamming signals in the first subphase to amplify and forward the signals received from the users in the second subphase. The EH signal during the first subphase is

$$y_{Re} = \sqrt{P_A}h_{AR}x_A + \sqrt{P_B}h_{BR}x_B + \sqrt{P_J}h_{JR}x_J. \tag{5.2}$$

The noise at the relay, n_R, is neglected because it is much less than the other terms in (5.2) [49]. The harvested energy is

$$E_H = \rho T \zeta \left(P_A |h_{AR}|^2 + P_B |h_{BR}|^2 + P_J |h_{JR}|^2 \right), \tag{5.3}$$

where $\zeta, 0 < \zeta \leq 1$, is the energy conversion efficiency. In the second phase, the relay transmit power is

$$P_R = \frac{E_H}{(1-\rho)T/2} = \frac{2\rho\zeta E_R}{1-\rho}, \tag{5.4}$$

where $E_R = P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2$. The information retrieval part of the received signal during the second subphase is

$$\begin{aligned} y_{Ri} &= \sqrt{P_A} h_{AR} x_A + \sqrt{P_B} h_{BR} x_B \\ &\quad + \sqrt{P_J} h_{JR} x_J + n_R. \end{aligned} \tag{5.5}$$

The jamming signal term $\sqrt{P_J} h_{JR} x_J$ at the relay can be cancelled from y_{Ri} as in [50, 51] as A and B are assumed to have a prior information of the jammer signal. Further, the jammer is located close to the relay and farther from A and B, so the jamming signal at A and B is negligible. Information regarding the jamming signal is securely shared between the jammer, relay and users before cooperative jamming begins. However, the jamming signal may not be perfectly canceled at the relay which is the assumption here. A cancellation factor Φ, $0 \leq \Phi \leq 1$, is used to indicate the fraction of the jamming signal that is not cancelled. This fraction, $\Phi \times P_J$, is amplified and forwarded to A and B by the relay. The jamming signal is perfectly cancelled if $\Phi = 0$, and there is no cancellation if $\Phi = 1$. The value of Φ depends on the circuitry of the relay receiver and the CSI at R.

The information retrieval signal with imperfect jamming cancellation is

$$\begin{aligned} y_R = \sqrt{P_A} h_{AR} x_A + \sqrt{P_B} h_{BR} x_B \\ + \Phi \sqrt{P_J} h_{JR} x_J + n_R. \end{aligned} \tag{5.6}$$

During the first phase, the signal received at E is

$$\begin{aligned} y_E^{(1)} =& \sqrt{P_A}(\widehat{h}_{AE} + e_E) x_A + \sqrt{P_B}(\widehat{h}_{BE} + e_E) x_B \\ &+ \sqrt{P_J}(\widehat{h}_{JE} + e_E) x_J + n_E. \end{aligned} \tag{5.7}$$

The SNR at E for x_B sent to A in this phase is

$$\begin{aligned} &SNR_{E,A}^{(1)} \\ &= \frac{P_B |\widehat{h}_{BE}|^2}{P_A |\widehat{h}_{AE}|^2 + P_J |\widehat{h}_{JE}|^2 + \sigma_e^2 (P_A + P_B + P_J) + \sigma^2} \end{aligned} \tag{5.8}$$

and the SNR at E for x_A sent to B is

$$\begin{aligned} &SNR_{E,B}^{(1)} \\ &= \frac{P_A |\widehat{h}_{AE}|^2}{P_B |\widehat{h}_{BE}|^2 + P_J |\widehat{h}_{JE}|^2 + \sigma_e^2 (P_A + P_B + P_J) + \sigma^2} \end{aligned} \tag{5.9}$$

The eavesdropper does not have knowledge of the jamming signal. Therefore, x_J is treated as additional noise that reduces the received SNR at E.

During the second phase, the relay amplifies the received signal and forwards this to the users using the harvested energy. Thus, the relay transmits the signal

$$
\begin{aligned}
x_R &= \frac{\sqrt{P_R}}{\sqrt{P_A|h_{AR}|^2 + P_B|h_{BR}|^2 + P_J|h_{JR}|^2 + \sigma^2}} \quad y_R && (5.10)\\
&= \sqrt{\frac{P_R}{E_R + \sigma^2}} \quad y_R, && (5.11)
\end{aligned}
$$

where $\sqrt{\frac{P_R}{E_R + \sigma^2}}$ is the relay amplifier gain. The received signal at A in this phase is

$$
\begin{aligned}
y_A &= h_{AR} x_R + n_A \\
&= \underbrace{\frac{\sqrt{P_R P_B} h_{AR} h_{BR}}{\sqrt{E_R + \sigma^2}} x_B}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_A} |h_{AR}|^2}{\sqrt{E_R + \sigma^2}} x_A}_{\text{information signal}} \\
&\quad \underbrace{+ \Phi \frac{\sqrt{P_R P_J} h_{AR} h_{JR}}{\sqrt{E_R + \sigma^2}} x_J + \frac{\sqrt{P_R} h_{AR} n_R}{\sqrt{E_R + \sigma^2}} + n_A}_{\text{noise}}, && (5.12)
\end{aligned}
$$

and the received signal at B is

$$
\begin{aligned}
y_B &= h_{BR} x_R + n_B \\
&= \underbrace{\frac{\sqrt{P_R P_A} h_{AR} h_{BR}}{\sqrt{E_R + \sigma^2}} x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_B} |h_{BR}|^2}{\sqrt{E_R + \sigma^2}} x_B}_{\text{information signal}} \\
&\quad \underbrace{+ \Phi \frac{\sqrt{P_R P_J} h_{BR} h_{JR}}{\sqrt{E_R + \sigma^2}} x_J + \frac{\sqrt{P_R} h_{BR} n_R}{\sqrt{E_R + \sigma^2}} + n_B}_{\text{noise}}. && (5.13)
\end{aligned}
$$

A and B cancel their own signals since self-interference cancellation can be assumed

[35, 36]. Let

$$\gamma_A = \frac{P_A|h_{AR}|^2}{\sigma^2}, \tag{5.14}$$

$$\gamma_B = \frac{P_B|h_{BR}|^2}{\sigma^2}, \tag{5.15}$$

$$\gamma_J = \frac{P_J|h_{JR}|^2}{\sigma^2}, \tag{5.16}$$

$$\overline{\gamma} = \gamma_A + \gamma_B + \gamma_J = \frac{E_R}{\sigma^2}. \tag{5.17}$$

The SNR at A is then

$$SNR_A = \frac{2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2}{2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)}, \tag{5.18}$$

where $\widetilde{\rho} = 1 - \rho$ and the achievable rate at A is [43]

$$R_A = (1-\rho)\frac{T}{2}\log_2\left(1 + SNR_A\right). \tag{5.19}$$

The SNR at B is

$$SNR_B = \frac{2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2}{2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)}, \tag{5.20}$$

and the achievable rate at B is

$$R_B = (1-\rho)\frac{T}{2}\log_2\left(1 + SNR_B\right). \tag{5.21}$$

The signal received at E during the second phase is

$$
\begin{aligned}
y_E^{(2)} &= h_{RE} x_R + n_E, && (5.22)\\
&= \underbrace{\frac{\sqrt{P_R P_A} h_{AR} h_{RE}}{\sqrt{E_R + \sigma^2}} x_A}_{\text{information signal}} + \underbrace{\frac{\sqrt{P_R P_B} h_{BR} h_{RE}}{\sqrt{E_R + \sigma^2}} x_B}_{\text{information signal}}\\
&\quad \underbrace{+ \Phi \frac{\sqrt{P_R P_J} h_{JR} h_{RE}}{\sqrt{E_R + \sigma^2}} x_J + \frac{\sqrt{P_R} h_{RE} n_R}{\sqrt{E_R + \sigma^2}} + n_E}_{\text{noise}}, && (5.23)
\end{aligned}
$$

where $h_{RE} = \widehat{h}_{RE} + e_E$. The SNR at E for x_B sent to A during the second phase is

$$
SNR_{E,A}^{(2)} = \frac{2\rho\zeta\overline{\gamma}\gamma_B |\widehat{h}_{RE}|^2}{\begin{array}{l} 2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) \\ \quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1) \end{array}} \tag{5.24}
$$

and the SNR at E for x_A sent to B during the second phase is

$$
SNR_{E,B}^{(2)} = \frac{2\rho\zeta\overline{\gamma}\gamma_A |\widehat{h}_{RE}|^2}{\begin{array}{l} 2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) \\ \quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1) \end{array}}. \tag{5.25}
$$

The achievable rate at E during both phases is

$$
R_{E,i} = \begin{cases} (1-\rho)\frac{T}{2}\log_2\left(1 + SNR_{E,i}^{(1)} + SNR_{E,i}^{(2)}\right), & \text{MRC at } E \\ \\ (1-\rho)\frac{T}{2}\log_2\left(1 + \max(SNR_{E,i}^{(1)}, SNR_{E,i}^{(2)})\right), & \text{SC at } E. \end{cases} \tag{5.26}
$$

5.3 Secrecy Capacity Analysis

The secrecy capacity in the presence of an eavesdropper is the difference between the secrecy capacity of the link between the users and the secrecy capacity of the wiretap link [43]. The total transmit power in this network is limited by the total power constraint P_T where $P_A + P_B + P_J \leq P_T$. The goal is to determine the time switching ratio and transmit power of A, B, and J to maximize the secrecy capacity at A and B under this constraint. The secrecy capacity at A is $C_{S,A} = [R_A - R_{E,A}]^+$ and at B is $C_{S,B} = [R_B - R_{E,B}]^+$ [93], where $[x]^+ = \max(0, x)$. The secrecy capacity at user i, $i \in \{A, B\}$, is then

$$C_{S,i} = \begin{cases} (1-\rho)\frac{T}{2}\log_2\left(\dfrac{1+SNR_i}{1+SNR_{E,i}^{(1)}+SNR_{E,i}^{(2)}}\right), & \text{MRC at } E \\ \\ (1-\rho)\frac{T}{2}\log_2\left(\dfrac{1+SNR_i}{1+\max(SNR_{E,i}^{(1)}, SNR_{E,i}^{(2)})}\right), & \text{SC at } E. \end{cases} \tag{5.27}$$

The secrecy capacity is

$$C_S = C_{S,A} + C_{S,B}, \tag{5.28}$$

$$= [R_A - R_{E,A}]^+ + [R_B - R_{E,B}]^+ . \tag{5.29}$$

and the corresponding optimization problem is formulated as

$$\max_{\rho,\widetilde{\rho},P_A,P_B,P_J} \quad C_S$$
$$P_A + P_B + P_J \leq P_T$$
$$\rho + \widetilde{\rho} \leq 1$$
$$\rho, \widetilde{\rho}, P_A, P_B, P_J \geq 0$$

5.3.1 MRC at the Eavesdropper

In this subsection, the secrecy capacity of the communication system is investigated with imperfect channel estimation at the eavesdropper. The eavesdropper employs MRC to combine the signals from the direct and relay links in both transmission phases. The achievable rates at E for x_B sent to A and x_A sent to B, $R_{E,A}$ and $R_{E,B}$, respectively, are defined in (5.26). $C_{S,A}$ is obtained by substituting SNR_A, $SNR_{E,A}^{(1)}$, and $SNR_{E,A}^{(2)}$ given by (5.18), (5.8), and (5.24), respectively, in (5.27) with $i = A$. $C_{S,B}$ is obtained by substituting SNR_B, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (5.20), (5.9), and (5.25), respectively, in (5.27) with $i = B$. From (5.29), there are four cases to consider to maximize the secrecy capacity as given below.

Case I: $C_{S,A} \geq 0$ **and** $C_{S,B} \geq 0$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& (R_A - R_{E,A}) + (R_B - R_{E,B}) \\ =& \frac{T}{2} \log_2 \left(\frac{w_I^{MRC}}{z_I^{MRC}} \right), \end{aligned} \tag{5.30}$$

where $(.)_I^{MRC}$ denotes the first case with MRC at the eavesdropper

$$
\begin{aligned}
&w_I^{MRC} = \\
&(2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2 + 2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1)) \\
&(P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \\
&\quad \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma}+1))
\end{aligned} \tag{5.31}
$$

$$
\begin{aligned}
&(2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1)) \\
&(P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
&\quad + \widetilde{\rho}(\overline{\gamma}+1))
\end{aligned} \tag{5.32}
$$

and

$$
\begin{aligned}
&z_I^{MRC} = \\
&(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1)) \\
&(2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J+1\right)+\widetilde{\rho}(\overline{\gamma}+1)) \\
&[((P_B|\widehat{h}_{BE}|^2)+(P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J)+\sigma^2)) \\
&\quad(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A+\Phi^2\gamma_J+1)+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\
&\quad+\widetilde{\rho}(\overline{\gamma}+1))+(P_A|\widehat{h}_{AE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J)+\sigma^2) \\
&\quad(2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2)] \\
&[((P_A|\widehat{h}_{AE}|^2)+(P_B|\widehat{h}_{BE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J)+\sigma^2)) \\
&\quad(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B+\Phi^2\gamma_J+1)+\sigma_e^2(\gamma_A+\gamma_B+\Phi^2\gamma_J+1)] \\
&\quad+\widetilde{\rho}(\overline{\gamma}+1))+(P_B|\widehat{h}_{BE}|^2+P_J|\widehat{h}_{JE}|^2+\sigma_e^2(P_A+P_B+P_J)+\sigma^2) \\
&\quad(2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)]
\end{aligned}
\tag{5.33}
$$

Case II: $C_{S,A} \geq 0$ **and** $C_{S,B} \leq 0$

In this case, $C_{S,B} = 0$ since the SNR at the eavesdropper is higher than that at B. The secrecy capacity is then

$$
\begin{aligned}
C_S =&(R_A - R_{E,A}) \\
=&\frac{T}{2}\log_2\left(\frac{w_{II}^{MRC}}{z_{II}^{MRC}}\right),
\end{aligned}
\tag{5.34}
$$

where $(.)_{II}^{MRC}$ denotes the second case with MRC at the eavesdropper

$$
\begin{aligned}
&w_{II}^{MRC} = \\
&((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\
&(P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma}+1))
\end{aligned} \tag{5.35}
$$

and

$$
\begin{aligned}
&z_{II}^{MRC} = \\
&(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1)) \\
&[((P_B|\widehat{h}_{BE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)) \\
&\qquad (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
&\quad + \widetilde{\rho}(\overline{\gamma}+1)) + ((P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
&\quad (2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2)].
\end{aligned} \tag{5.36}
$$

Case III: $C_{S,A} \leq 0$ **and** $C_{S,B} \geq 0$

In this case, $C_{S,A} = 0$ since the SNR at the eavesdropper is higher than that at A. The secrecy capacity is then

$$
\begin{aligned}
C_S =& (R_B - R_{E,B}) \\
=& \frac{T}{2}\log_2\left(\frac{w_{III}^{MRC}}{z_{III}^{MRC}}\right),
\end{aligned} \tag{5.37}
$$

where $(.)_{III}^{MRC}$ denotes the third case with MRC at the eavesdropper

$$
\begin{aligned}
& w_{III}^{MRC} = \\
& ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1))) \\
& (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2) \\
& (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
& \quad + \widetilde{\rho}(\overline{\gamma}+1))
\end{aligned} \tag{5.38}
$$

and

$$
\begin{aligned}
& z_{III}^{MRC} = \\
& (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma}+1)) \\
& [((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) \\
& \quad + \sigma^2))(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) \\
& \quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma}+1))(P_B|\widehat{h}_{BE}|^2 \\
& \quad + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)(2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2)].
\end{aligned} \tag{5.39}
$$

Case IV: $C_{S,A} \leq 0$ **and** $C_{S,B} \leq 0$

In this case, the secrecy capacity is $C_S = 0$ because the secrecy capacity of the wiretap links is higher than the secrecy capacity at A and B.

5.3.2 SC at the Eavesdropper

In this subsection, the secrecy capacity of the communication system is investigated with imperfect channel estimation at the eavesdropper. The eavesdropper employs SC so the link (direct or relay) with the maximum SNR is selected. Based on $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (5.8), (5.24), (5.9), and (5.25), respectively, the following four cases can be considered.

Case I: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned}
C_S =& C_{S,A} + C_{S,B} \\
=& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(1)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(1)}} \right), \\
=& \frac{T}{2} \log_2 \left(\frac{w_{I,A}^{SC}}{z_{I,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{I,B}^{SC}}{z_{I,B}^{SC}} \right), \\
=& \frac{T}{2} \log_2 \left(\frac{w_{I}^{SC}}{z_{I}^{SC}} \right),
\end{aligned} \tag{5.40}$$

where

$$w_{I,A}^{SC} =$$

$$((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)))$$

$$(P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2), \tag{5.41}$$

$$w_{I,B}^{SC} =$$

$$((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)))$$

$$(P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2), \tag{5.42}$$

$$z_{I,A}^{SC} =$$

$$((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2)$$

$$(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \tag{5.43}$$

$$z_{I,B}^{SC} =$$

$$((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2))$$

$$(2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \tag{5.44}$$

$$\frac{w_I^{SC}}{z_I^{SC}} = \begin{cases} \frac{w_{I,A}^{SC} w_{I,B}^{SC}}{z_{I,A}^{SC} z_{I,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \\ \frac{w_{I,A}^{SC}}{z_{I,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \\ \frac{w_{I,B}^{SC}}{z_{I,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{5.45}$$

and $(.)_I^{SC}$ denotes the first case with SC at the eavesdropper.

Case II: $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(1)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(2)}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{II,A}^{SC}}{z_{II,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{II,B}^{SC}}{z_{II,B}^{SC}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{II}^{SC}}{z_{II}^{SC}} \right), \end{aligned} \tag{5.46}$$

where

$$
\begin{aligned}
& w_{II,A}^{SC} = \\
& ((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1))) \\
& (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2), && (5.47) \\
& w_{II,B}^{SC} = \\
& ((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1))) \\
& (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
& \quad + \widetilde{\rho}(\overline{\gamma} + 1)), && (5.48) \\
& z_{II,A}^{SC} = \\
& ((P_B|\widehat{h}_{BE}|^2) + (P_A|\widehat{h}_{AE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) \\
& \quad + \sigma^2)(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), && (5.49) \\
& z_{II,B}^{SC} = \\
& ((2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) \\
& \quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1))) \\
& \quad (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), && (5.50)
\end{aligned}
$$

$$\frac{w_{II}^{SC}}{z_{II}^{SC}} = \begin{cases} \frac{w_{II,A}^{SC} w_{II,B}^{SC}}{z_{II,A}^{SC} z_{II,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \\ \frac{w_{II,A}^{SC}}{z_{II,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \\ \frac{w_{II,B}^{SC}}{z_{II,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{5.51}$$

and $(.)_{II}^{SC}$ denotes the second case with SC at the eavesdropper.

Case III: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(2)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(1)}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{III,A}^{SC}}{z_{III,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{III,B}^{SC}}{z_{III,B}^{SC}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{III}^{SC}}{z_{III}^{SC}} \right), \end{aligned} \tag{5.52}$$

where

$$w^{SC}_{III,A} =$$

$$((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)))$$

$$(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)]$$

$$+ \widetilde{\rho}(\overline{\gamma} + 1)), \tag{5.53}$$

$$w^{SC}_{III,B} =$$

$$((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)))$$

$$(P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2), \tag{5.54}$$

$$z^{SC}_{III,A} =$$

$$((2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1)$$

$$+ \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1)))$$

$$(2\rho\zeta\overline{\gamma}|h_{AR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \tag{5.55}$$

$$z^{SC}_{III,B} =$$

$$((P_A|\widehat{h}_{AE}|^2) + (P_B|\widehat{h}_{BE}|^2 + P_J|\widehat{h}_{JE}|^2 + \sigma_e^2(P_A + P_B + P_J) + \sigma^2))$$

$$(2\rho\zeta\overline{\gamma}|h_{BR}|^2\left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \tag{5.56}$$

$$\tag{5.57}$$

$$\frac{w_{III}^{SC}}{z_{III}^{SC}} = \begin{cases} \frac{w_{III,A}^{SC} w_{III,B}^{SC}}{z_{III,A}^{SC} z_{III,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \frac{w_{III,A}^{SC}}{z_{III,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \frac{w_{III,B}^{SC}}{z_{III,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{5.58}$$

and $(.)_{III}^{SC}$ denotes the third case with SC at the eavesdropper.

Case IV: $SNR_{E,A}^{(1)} \leq SNR_{E,A}^{(2)}$ **and** $SNR_{E,B}^{(1)} \leq SNR_{E,B}^{(2)}$

In this case, the secrecy capacity is

$$\begin{aligned} C_S =& C_{S,A} + C_{S,B} \\ =& \frac{T}{2} \log_2 \left(\frac{1 + SNR_A}{1 + SNR_{E,A}^{(2)}} \right) + \frac{T}{2} \log_2 \left(\frac{1 + SNR_B}{1 + SNR_{E,B}^{(2)}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}} \right) + \frac{T}{2} \log_2 \left(\frac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}} \right), \\ =& \frac{T}{2} \log_2 \left(\frac{w_{IV}^{SC}}{z_{IV}^{SC}} \right), \end{aligned} \tag{5.59}$$

where

$$
\begin{aligned}
&w_{IV,A}^{SC} = \\
&((2\rho\zeta\overline{\gamma}\gamma_B|h_{AR}|^2) + (2\rho\zeta\overline{\gamma}|h_{AR}|^2 \left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1))) \\
&(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
&\quad + \widetilde{\rho}(\overline{\gamma} + 1)), \qquad (5.60) \\
&w_{IV,B}^{SC} = \\
&((2\rho\zeta\overline{\gamma}\gamma_A|h_{BR}|^2) + (2\rho\zeta\overline{\gamma}|h_{BR}|^2 \left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1))) \\
&(2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] \\
&\quad + \widetilde{\rho}(\overline{\gamma} + 1)), \qquad (5.61) \\
&z_{IV,A}^{SC} = \\
&((2\rho\zeta\overline{\gamma}\gamma_B|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_A + \Phi^2\gamma_J + 1) \\
&\quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1))) \\
&\quad (2\rho\zeta\overline{\gamma}|h_{AR}|^2 \left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \qquad (5.62) \\
&z_{IV,B}^{SC} = \\
&((2\rho\zeta\overline{\gamma}\gamma_A|\widehat{h}_{RE}|^2) + (2\rho\zeta\overline{\gamma}[|\widehat{h}_{RE}|^2(\gamma_B + \Phi^2\gamma_J + 1) \\
&\quad + \sigma_e^2(\gamma_A + \gamma_B + \Phi^2\gamma_J + 1)] + \widetilde{\rho}(\overline{\gamma} + 1))) \\
&\quad (2\rho\zeta\overline{\gamma}|h_{BR}|^2 \left(\Phi^2\gamma_J + 1\right) + \widetilde{\rho}(\overline{\gamma} + 1)), \qquad (5.63) \\
&\qquad (5.64)
\end{aligned}
$$

$$\frac{w_{IV}^{SC}}{z_{IV}^{SC}} = \begin{cases} \frac{w_{IV,A}^{SC} w_{IV,B}^{SC}}{z_{IV,A}^{SC} z_{IV,B}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} \geq 0 \\ \frac{w_{IV,A}^{SC}}{z_{IV,A}^{SC}}, & C_{S,A} \geq 0 \text{ and } C_{S,B} < 0 \\ \frac{w_{IV,B}^{SC}}{z_{IV,B}^{SC}}, & C_{S,A} < 0 \text{ and } C_{S,B} \geq 0 \\ 0, & C_{S,A} < 0 \text{ and } C_{S,B} < 0, \end{cases} \tag{5.65}$$

and $(.)_{IV}^{SC}$ denotes the fourth case with SC at the eavesdropper.

5.4 Optimization Problem Formulation

The secrecy capacity optimization problem for MRC and SC at the eavesdropper is

$$\underset{\rho, \widetilde{\rho}, P_A, P_B, P_J}{\text{minimize}} \quad \frac{z}{w} \tag{5.66a}$$

$$\text{subject to} \quad P_A + P_B + P_J \leq P_T, \tag{5.66b}$$

$$\rho + \widetilde{\rho} \leq 1, \tag{5.66c}$$

$$\rho, \widetilde{\rho}, P_A, P_B, P_J \geq 0 \tag{5.66d}$$

where w and z are defined below for each diversity scheme.

The standard form of a Geometric Programming (GP) problem is [40]

$$\text{minimize} \quad f_0(x) \tag{5.67a}$$

$$\text{subject to} \quad f_i(x) \leq 0, \quad i = 1, \ldots, m, \tag{5.67b}$$

$$g_i(x) = 1, \quad i = 1, \ldots, p \tag{5.67c}$$

where $f_i(x)$ is a posynomial function, $g_i(x)$ is a monomial function, and x is the optimization variable. A monomial function g of x is a real valued function of the form $g(x) = cx_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ where $c > 0$, $a_i \in \mathbf{R}$, and n is the number of optimization variables. A posynomial function is the sum of two or more monomials such that $f(x) = \sum_{k=1}^{K} c_k x_1^{a_{1k}} x_2^{a_{2k}} \ldots x_n^{a_{nk}}$ where $c_k > 0$ and K is the number of monomial functions.

The constraints in (5.66b) and (5.66c) are posynomials. This problem can be transformed into GP form then into a convex problem because the constraints and the objective function are posynomials. However, the objective function is a ratio of two posynomials, so it cannot be transformed into GP form. To solve this problem, $w(\rho, \widetilde{\rho}, P_A, P_B, P_J)$ is approximated as a monomial function using the single condensation method (SCM) [41]. In SCM, the denominater of the ratio of posynomials is approximated with a monomial function. The numerator (a posynomial) is not approximated, hence the term single. In the optimization problem, $w(\mathbf{x}) = \sum_i u_i(\mathbf{x})$ where $\mathbf{x} = [\rho, \widetilde{\rho}, P_A, P_B, P_J]^T$, is the sum of i monomials, so it is a posynomial by definition. The monomial approximation of $w(\mathbf{x})$ using SCM is

$$\overline{w}(\mathbf{x}) = \prod_i \left(\frac{u_i(\mathbf{x})}{\alpha_i} \right)^{\alpha_i}, \tag{5.68}$$

such that $w(\mathbf{x}) \geq \overline{w}(\mathbf{x})$. For a given $\mathbf{x}$, α_i $\forall i$ are obtained in $w(\mathbf{x})$ so that

$$\alpha_i = \frac{u_i(\mathbf{x})}{w(\mathbf{x})}, \tag{5.69}$$

and $\overline{w}(\mathbf{x})$ is substituted for $w(\mathbf{x})$ in (5.66a). The objective function after SCM approximation is a polynomial (posynomial). The accuracy of the approximation was determined by calculating the difference between the value of $w(\mathbf{x})$ and $\overline{w}(\mathbf{x})$ at the solution point $\mathbf{x}$. The maximum difference is 0.00232. GP is used to obtain a nonlinear but convex optimization problem with convex objective and inequality constraint functions and linear equality constraints. A logarithmic change of variables and a logarithmic transformation of the objective function and constraints is used to obtain a GP form. The resulting convex problem can be solved efficiently using CVX [40]. As the optimal solution may be far from the initial guess $\mathbf{x}_0$ used in the SCM approximation, an iterative approach is used to solve this problem.

For MRC at the eavesdropper, the initial guess is used to calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (5.8), (5.24), (5.9), and (5.25), respectively. $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ are then substituted in (5.27) along with SNR_A from (5.18) and SNR_B from (5.20) to calculate $C_{S,A}$ and $C_{S,B}$, respectively. Then $C_{S,A}$ and $C_{S,B}$ are compared to determine which case in Subsection 5.3.1 to employ, and $\mathbf{x}_0$ is used to obtain $C_{S,A}$ and $C_{S,B}$. Next, $w_{(.)}^{MRC}$ is approximated using the SCM method and the resulting $\overline{w}_{(.)}^{MRC}(\mathbf{x})$ is used in (5.66a) to solve the optimization problem. If the current optimal solution, $\mathbf{x}_{k+1}$, satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$ and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*]^T$ is summarized in Algorithm 1.

For SC at the eavesdropper, the initial guess is used to calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$ given by (5.8), (5.24), (5.9), and (5.25), respectively. The values of $SNR_{E,A}^{(1)}$ and $SNR_{E,A}^{(2)}$ are compared to determine which expression for $C_{S,A}$ to consider, and the values of $SNR_{E,B}^{(1)}$ and $SNR_{E,B}^{(2)}$ are compared to determine which expression for $C_{S,B}$ to consider. These results determine which case in Subsection 5.3.2 to employ. $\mathbf{x}_0$ is then used to calculate values of $C_{S,A}$ and $C_{S,B}$. Next, $w_{(.)}^{SC}$ is approximated using the SCM method and the resulting $\overline{w}_{(.)}^{SC}(\mathbf{x})$ is used in (5.66a) to solve the optimization problem. If the current optimal solution, $\mathbf{x}_{k+1}$, satisfies the initial assumption $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then $\mathbf{x}_{k+1}$ is used to calculate $\overline{w}(\mathbf{x}_{k+1})$ and the optimization problem is solved again. If $\mathbf{x}_{k+1}$ violates $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$, then proceed to the next case. The algorithm to obtain the optimal values $[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*]^T$ is summarized in Algorithm 2.

5.5 Results and Discussion

In this section, the secrecy capacity is evaluated for a two-way relay network with a friendly jammer in the presence of an eavesdropper. Users A and B can only communicate through R since there is no direct link between them. The simulation parameters are as follows unless noted otherwise. The noise variance is $\sigma^2 = 10^{-3}$, $\sigma_e^2 = 0.1$, $T = 1$, the optimization tolerance is $\epsilon = 0.001$, $\Phi = 0$, and the energy conversion efficiency is $\zeta = 0.5$. The channel gains $|h_{AR}|^2$, $|h_{JR}|^2$, $|h_{JE}|^2$, and $|h_{BR}|^2$ are exponential random variables with mean $\lambda = 1$, $|h_{RE}|^2$ and $|h_{BE}|^2$ are exponential random variables with mean λ_{Eve}, and $|h_{AE}|^2$ is an exponential random variable with

Algorithm 4 Optimization of the Secrecy Capacity, C_S, for MRC at the Eavesdropper

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$

1: **while** $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**
2:   Calculate the monomial approximation $\overline{w}$ for w using the single condensation method at $\mathbf{x} = [\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T$
3:   $k = k + 1$
4:   Solve the optimization problem in (5.66) using $\overline{w}$ to find $[\rho_{k+1}, \widetilde{\rho}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}]$
5:   Using the solution in step 4, calculate $C_{S,A}$ and $C_{S,B}$
6:   **if** $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**
7:     Go to step 1
8:   **else**
9:     Continue to the next case of $C_{S,A}$ and $C_{S,B}$
10:   **end if**
11:   Solve the optimization problem in (5.30) to obtain $[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]$
12: **end while**
13: Assign $[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*]^T = [\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T$ and $C_S = C_{S,k}$

mean $\frac{1}{\lambda_{Eve}}$, $\lambda_{Eve} \in \{1, 2, 3\}$. The node locations are normalized to the distance between A and B so that A and B are at (0, 0) and (1, 0), respectively. R is at the midpoint, (0.5, 0), J is at (0.5, −0.5), $P_T = 10$ dB, and $P_J = 0.1P_T$.

Fig. 5.3 presents the secrecy capacity versus the total transmit power, P_T, for $\lambda_{Eve} = 1$, 2, and 3 with SC and MRC at the eavesdropper. The secrecy capacity increases in all cases as the total transmit power increases. The secrecy capacity of SC outperforms MRC for all values of λ_{Eve}. The reason is that SC selects only one wiretap link which reduces the SNR at the eavesdropper. As a result, the secrecy capacity of the network with SC at the eavesdropper is higher than that with MRC. The effect of increasing λ_{Eve} on the secrecy capacity of SC and MRC is negligible except for MRC with $P_T \leq 8$ dB. The reason is that as λ_{Eve} increases from 1 to 2 and 3, the corresponding channel links of the eavesdropper improve and so does the SNR at the relay which reduces the secrecy capacity. However, once the total transmit

Algorithm 5 Optimization of the Secrecy Capacity, C_S, for SC at the Eavesdropper

Require: Channel coefficients, power constraint P_T, energy conversion efficiency ζ, noise variance σ^2, tolerance ϵ, estimation error variance σ_e^2, $k = 1$

    while $|C_{S,k} - C_{S,k-1}| > \epsilon$ **do**

2:         Calculate $SNR_{E,A}^{(1)}$, $SNR_{E,A}^{(2)}$, $SNR_{E,B}^{(1)}$, and $SNR_{E,B}^{(2)}$

        if $SNR_{E,A}^{(1)} \geq SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \geq SNR_{E,B}^{(2)}$ **then**

4:             Calculate the monomial approximation $\overline{w}$ for w using the single condensation method at $\mathbf{x} = [\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T$

            $k = k + 1$

6:             Solve the optimization problem in (5.66) using $\overline{w}$ to find $[\rho_{k+1}, \widetilde{\rho}_{k+1}, P_{A,k+1}, P_{B,k+1}, P_{J,k+1}]$

            Using the solution in step 6, calculate $C_{S,A}$ and $C_{S,B}$

8:             **if** $C_{S,A} \geq 0$ and $C_{S,B} \geq 0$ **then**

                Go to step 1

10:            **else**

                Continue to the next case of $C_{S,A}$ and $C_{S,B}$

12:            **end if**

        else

14:            Continue to the next case of $SNR_{E,A}^{(1)} \gtrless SNR_{E,A}^{(2)}$ and $SNR_{E,B}^{(1)} \gtrless SNR_{E,B}^{(2)}$

        end if

16:        Solve the optimization problem in (5.30) to obtain $[\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]$

    end while

18: Assign $[\rho^*, \widetilde{\rho}^*, P_A^*, P_B^*, P_J^*]^T = [\rho_k, \widetilde{\rho}_k, P_{A,k}, P_{B,k}, P_{J,k}]^T$ and $C_S = C_{S,k}$

power exceeds 8 dB, the effect of increasing λ_{Eve} on the secrecy capacity is negligible.

Fig. 5.4 presents the secrecy capacity versus the time switching ratio, ρ, with SC and MRC for $\sigma_e^2 = 0$ and 0.1. This shows that SC outperforms MRC for the given values of σ_e^2 and λ_{Eve}, and the secrecy capacity for imperfect CSI, $\sigma_e^2 = 0.1$, is better than that for perfect CSI, $\sigma_e^2 = 0$, for all values of ρ. Considering the SNR expressions of the eavesdropper links, the denominators of (5.8), (5.24), (5.9), and (5.25) contain σ_e^2, so increasing this term reduces the SNR at E. These results also show that the secrecy capacity increases as ρ increases until it reaches an optimal value, and then the secrecy capacity decreases. As the time switching ratio increases,

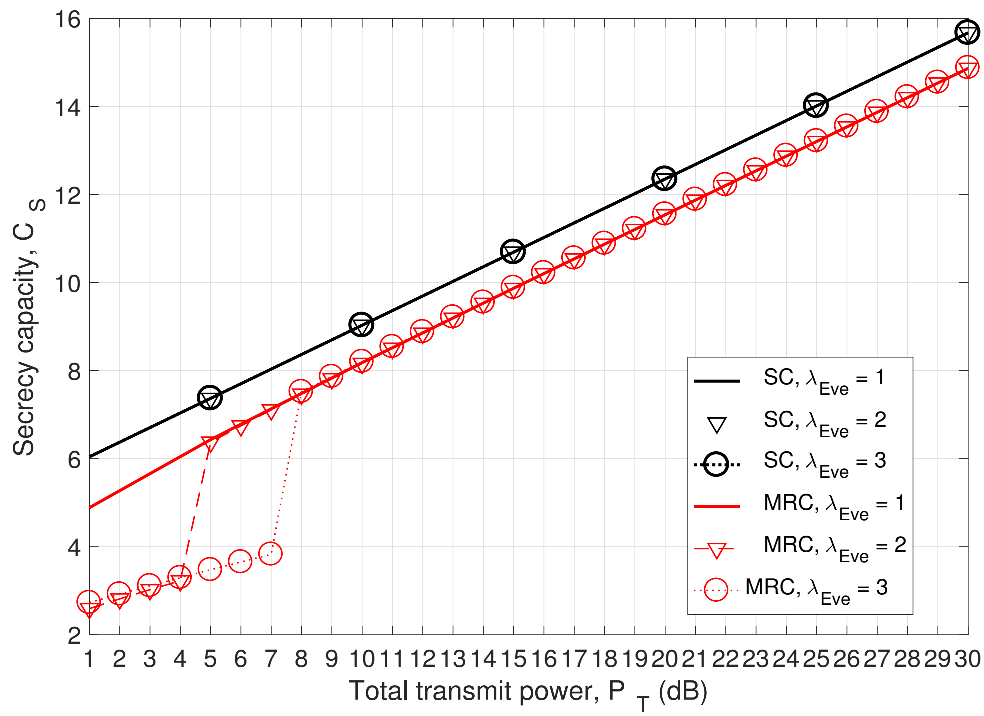

Figure 5.3: The secrecy capacity versus the total transmit power, P_T, with $\lambda_{Eve} = 1$ and $\sigma_e^2 = 0$.

the relay harvests more energy for signal forwarding in the second phase. However, a larger ρ means the eavesdropper has more time to overhear the transmitted signals, so there is a tradeoff.

5.5.1 Channel Estimation Error

Figs. 5.5 and 5.6 present the effect of the channel estimation error variance, σ_e^2, on the secrecy capacity. Fig. 5.5 shows the secrecy capacity for $\lambda_{Eve} = 1, 2$, and 3. A higher value of σ_e^2 means that the eavesdropper is less able to estimate the wiretap links so the secrecy capacity improves. The differences in secrecy capacity between SC and MRC are 0.14, 0.023, and 0.014 bits/sec/channel use for $\lambda_{Eve} = 1, 2$, and 3, respectively, at $\sigma_e^2 = 0.1$. Thus, increasing λ_{Eve} decreases the gap between SC and MRC. This

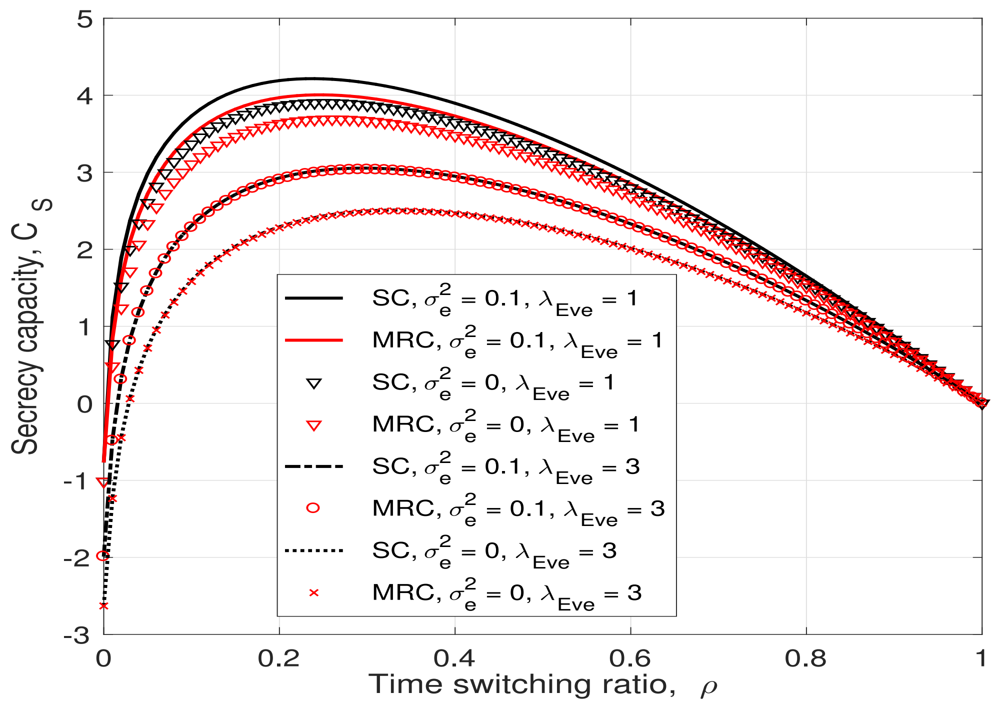

Figure 5.4: The secrecy capacity versus the time switching ratio, ρ, for different values of λ_{Eve} and σ_e^2 with $P_J = 0.1P_T$ and $P_T = 10$ dB.

is because a larger λ_{Eve} improves the corresponding link of the eavesdropper but degrades the other eavesdropper link. Fig. 5.6 shows the secrecy capacity versus the channel estimation error variance for $\rho = 0.8$ and 0.2 with $\lambda_{Eve} = 1$. At $\sigma_e^2 = 0.01$, SC outperforms MRC with a difference of 0.057 at $\rho = 0.8$ and 0.23 at $\rho = 0.2$. Thus, decreasing ρ improves the performance of SC and MRC but does not have a significant effect on the difference between them. As ρ increases, the relay harvests more energy, so there is more higher transmit power at the relay. This improves the received SNR at the users.

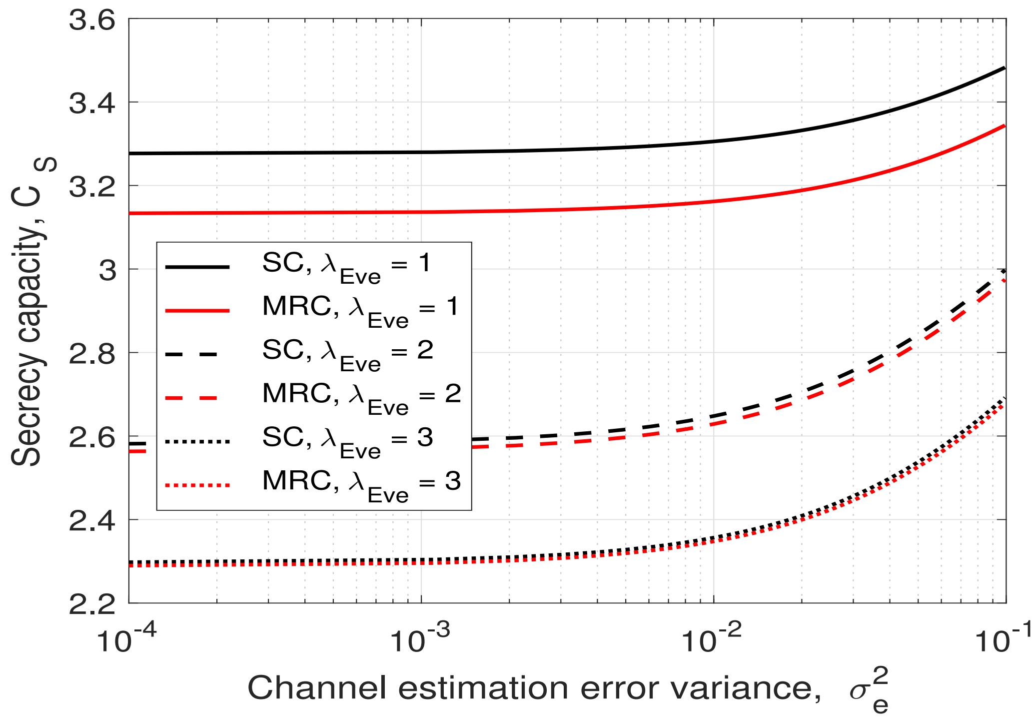

Figure 5.5: The secrecy capacity versus the channel estimation error variance, σ_e^2, for three values of λ_{Eve} with $\rho = 0.5$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

5.5.2 Jammer, Cancellation Factor, and Locations

The secrecy capacity versus the jamming signal cancellation factor, Φ, is given in Fig. 5.7 for $\sigma_e^2 = 0$ and 0.5. This shows that SC outperforms MRC for both values of σ_e^2. When $\Phi = 0$, the secrecy capacity is highest because the jamming signal at the relay is completely cancelled. As Φ increases, more jamming power is amplified and forwarded to A and B. Thus, the noise at A and B increases which degrades their SNRs and so decreases the secrecy capacity. The difference in secrecy capacity with SC is 0.93 bits/sec/channel use at $\Phi = 0.1$ and this decreases to 0.74 bits/sec/channel use at $\Phi = 0.8$.

In the following figures, the secrecy capacity is considered for different locations of the eavesdropper and jammer. The channel links can be expressed as $h_{ij} = \frac{f_{ij}}{d_{ij}^m}$

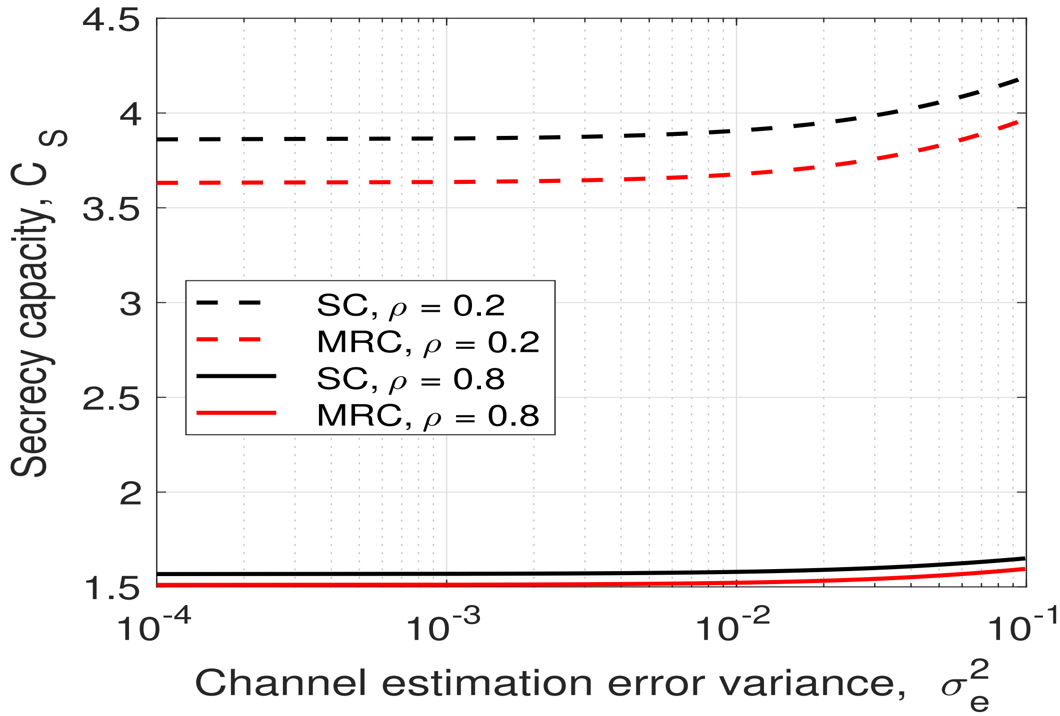

Figure 5.6: The secrecy capacity versus the channel estimation error variance, σ_e^2, with $\rho = 0.8$ and 0.2, $\lambda_{Eve} = 1$, $P_J = 0.1P_T$, and $P_T = 10$ dB.

where f_{ij} is an exponential random variable with mean = 1, $m = 2.7$ is the path loss exponent, and d_{ij} is the distance between i and j. Figs. 5.8 and 5.9 present the secrecy capacity versus Φ for SC and MRC at the eavesdropper, respectively. The jammer is at (0.5, -0.5) and the location of the eavesdropper is (0.5, -1) and (0.2, -0.2) with $d_{AE} = 1.12$ and 0.28, respectively. These results show that the secrecy capacity increases as d_{AE} increases from 0.28 to 1.12 for both values of σ_e^2. The reason is that as d_{AE} increases, less power is required to be allocated to the jammer. Hence, more power is allocated to A and B, and more energy is harvested at R. Fig. 5.8 shows that when $\sigma_e^2 = 0$, the difference in SC secrecy capacity for $d_{AE} = 1.12$ and 0.28 is 0.53 bit/sec/channel use, and this increases to 0.57 bit/sec/channel use for $\sigma_e^2 = 0.1$. Fig. 5.9 shows that when $\sigma_e^2 = 0$, the difference in MRC secrecy

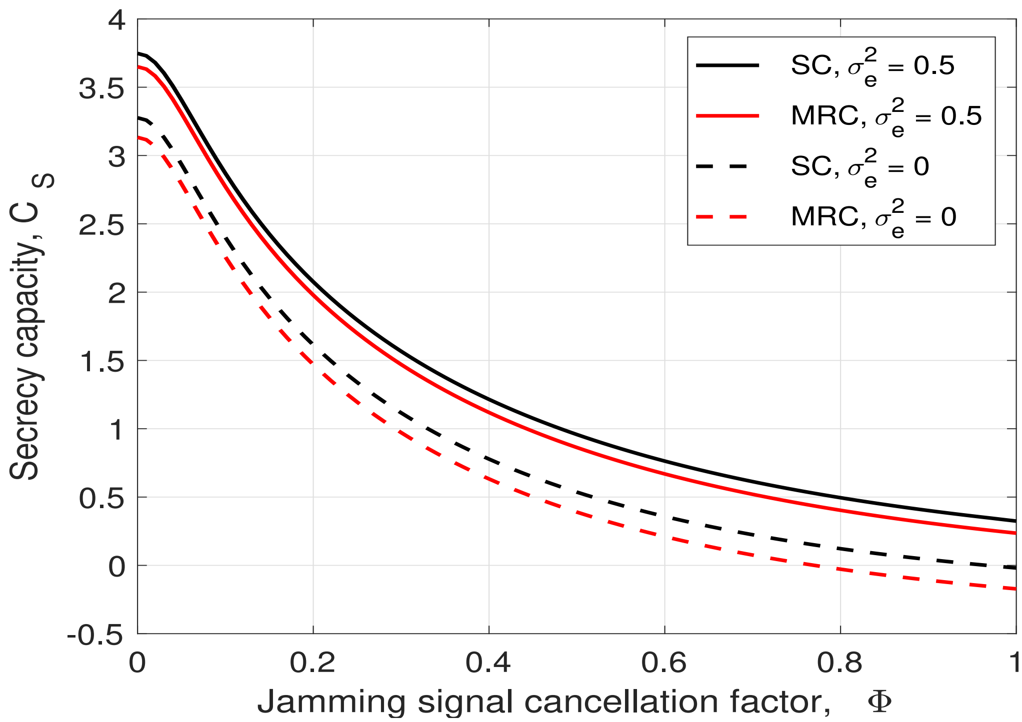

Figure 5.7: The secrecy capacity versus the jamming signal cancellation factor, Φ, with $\lambda_{Eve} = 1$, $\theta = 0.5$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

capacity for $d_{AE} = 1.12$ and 0.28 is 0.51 bit/sec/channel use, and this increases to 0.62 bit/sec/channel use for $\sigma_e^2 = 0.1$.

Fig. 5.10 presents the effect of Φ on the secrecy capacity when the jammer is close to the relay. In this case, E is at $(0.2, -1)$ and J is at $(0.5, -0.1)$, so significant jamming power is received by the relay. These results show that a small increase in Φ causes a significant drop in secrecy capacity for both SC and MRC. For example, with SC and $\rho = 0.5$, the secrecy capacity for SC drops by 2.74 bit/sec/channel use when Φ increases from 0 to 0.01 and by 3.17 bit/sec/channel use when Φ increases from 0.01 to 0.1. This is because the jamming signal at the relay is larger because the jammer is closer to the relay.

Fig. 5.11 shows the secrecy capacity versus the x-axis location of the eavesdropper

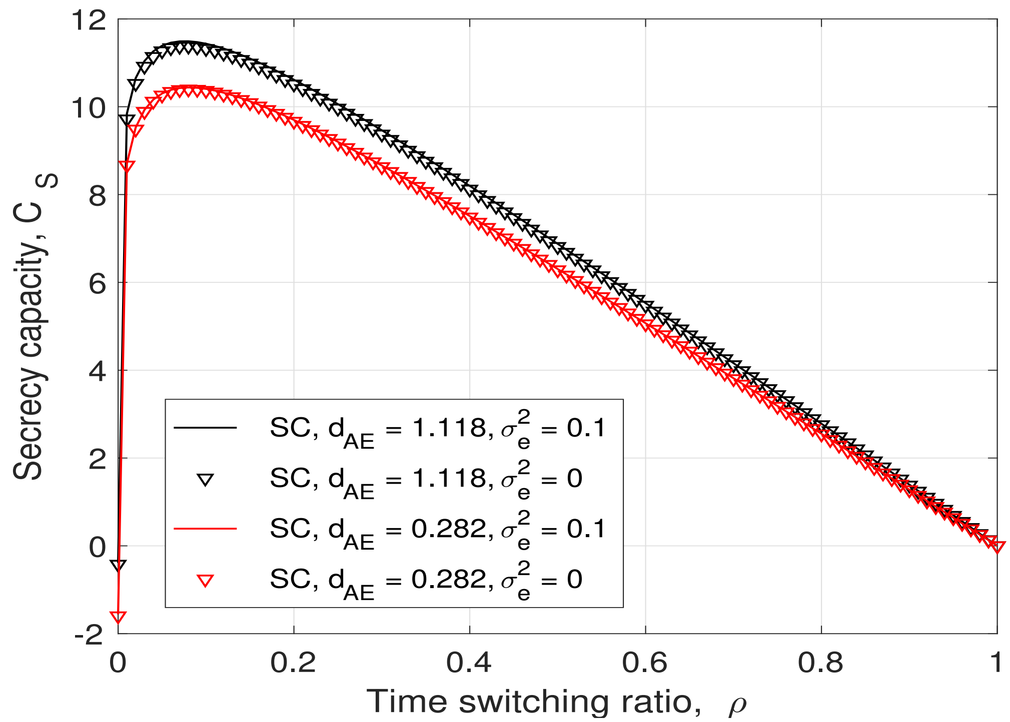

Figure 5.8: The secrecy capacity for SC at the eavesdropper with $d_{AE} = 0.28$ and 1.12, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

(employing MRC), when the jammer is located at $(0.5, -0.5)$ and without a jammer. Results are given for y-axis eavesdropper positions -0.2, -0.5, and -0.8 and MRC at the eavesdropper. The solid lines are for the case with a jammer at $(0.5, -0.5)$ and the other lines correspond to no jammer. When the eavesdropper is at $x = 0.5$, i.e. midway between A and B, the secrecy capacity is the highest. Further, the secrecy capacity is better with a jammer since the jamming signal reduces the SNR at the eavesdropper regardless of their y-axis position. The lowest secrecy capacity in both cases (with and without a jammer), is when the eavesdropper is at $x = 0$ and $x = 1$ since the SNR at the eavesdropper from A and B, respectively, is highest.

Fig. 5.12 presents the secrecy capacity versus the x-axis position of the eavesdropper (employing MRC), with the jammer located at $(0.5, -0.5)$, $(0.5, -1)$, $(0.2, -0.5)$,

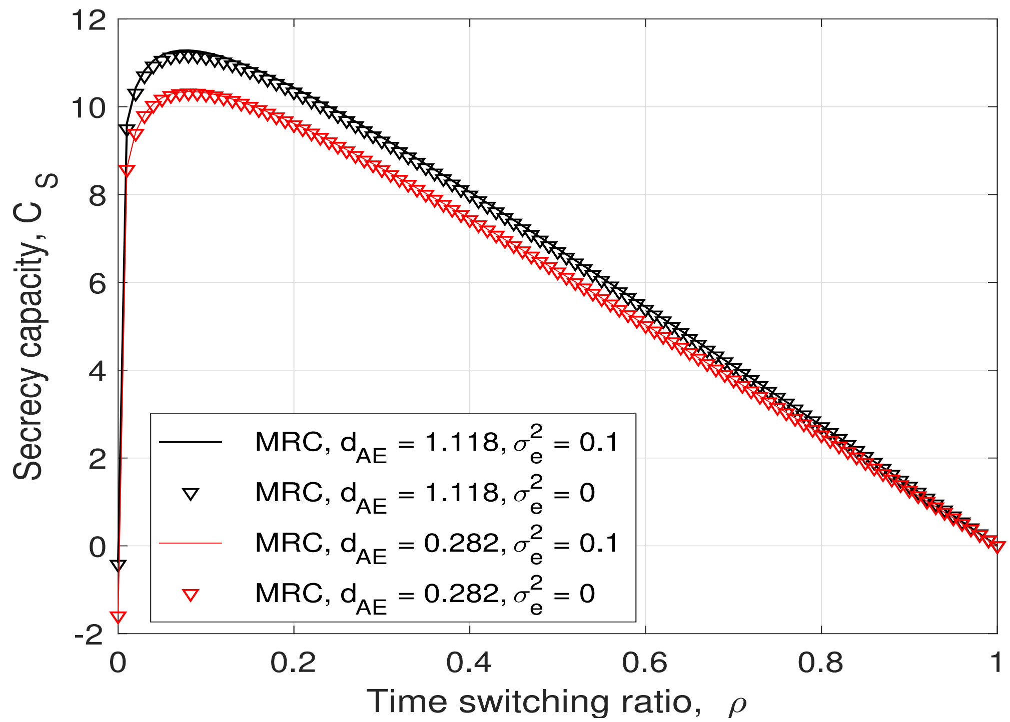

Figure 5.9: The secrecy capacity for MRC at the eavesdropper with $d_{AE} = 0.28$ and 1.12, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

$(0.2, -1)$, $(0.7, -0.5)$, and $(0.7, -1)$. The location of the eavesdropper changes from $(0, -0.7)$ to $(1, -0.7)$. In all cases, the secrecy capacity is a minimum when the eavesdropper is at $x = 0$ or $x = 1$ which is closest to A or B, respectively. As the eavesdropper moves from $x = 0$ to 1, the jamming signal power at the eavesdropper increases and the secrecy capacity increases. Then, the secrecy capacity decreases as the eavesdropper moves farther from the jammer after the maximum secrecy capacity has been reached.

5.5.3 Time Complexity

Matlab R2017a on a MacBook Pro laptop with an Intel Core i5 processor was used to obtain the simulation results. An average time of 7.89 s was required to run Al-

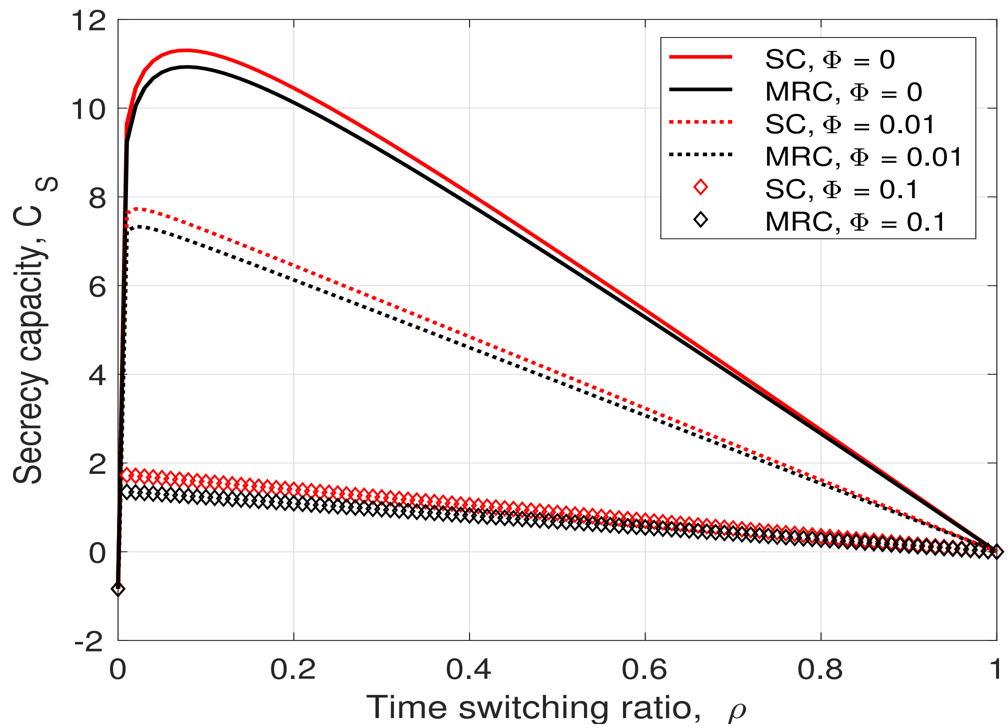

Figure 5.10: The secrecy capacity for different values of Φ with the jammer at $(0.5, -0.1)$, the eavesdropper at $(0.2, -1)$, $\lambda_{Eve} = 1$, $P_T = 10$ dB, and $P_J = 0.1P_T$.

gorithm 1 (MRC) and 1.56 s to run Algorithm 2 (SC). SC selects the maximum of $SNR_{E,i}^{(1)}$ and $SNR_{E,i}^{(2)}$ and MRC combines $SNR_{E,i}^{(1)}$ and $SNR_{E,i}^{(2)}$ to obtain the achievable rate at the eavesdropper. The average number of iterations required to solve the optimization problem for a given total transmit power was approximately 3 for SC at the eavesdropper and 2 for MRC. However, Algorithm 2 was faster because the number of monomial terms to be approximated with SC is 12 while with MRC it is 40.

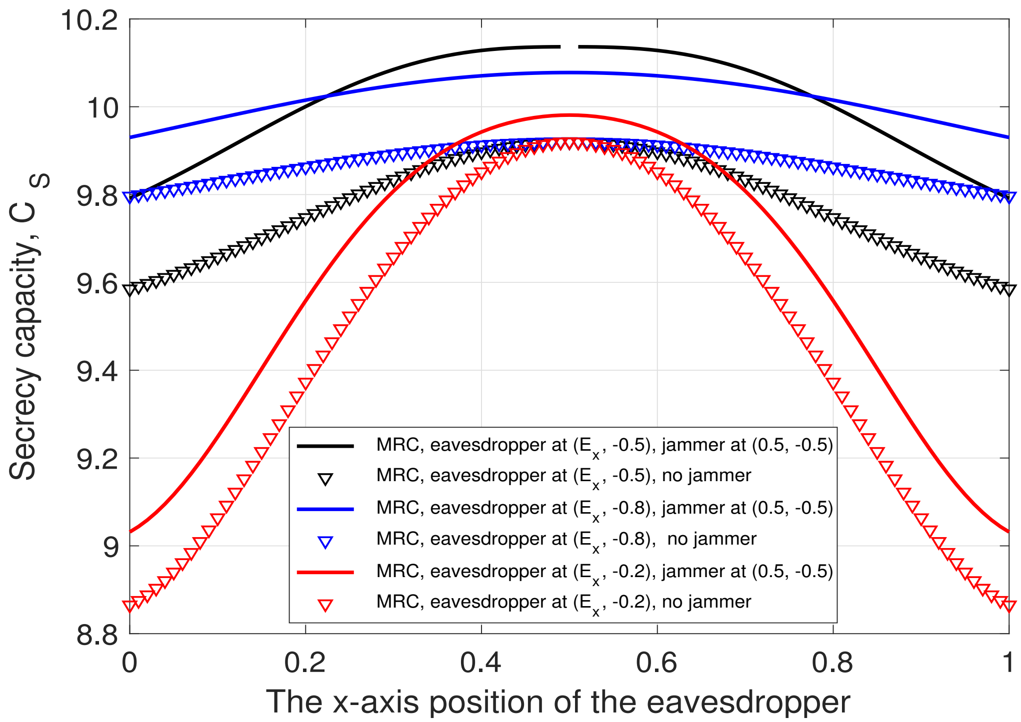

Figure 5.11: The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), with a jammer at a fixed location and without a jammer.

5.5.4 Comparison of PS and TS Two-Way Relaying Protocols

In this subsection, the two proposed protocols are compared to understand the advantages and disadvantages of each protocol. Fig. 5.13 compares the optimal secrecy capacity for PS and TS in each case of SC and MRC at the eavesdropper at $\lambda_{Eve} = 1$ and using the same parameters stated at the beginning of Section 5.5. It shows that PS two-way relaying protocol achieves a better secrecy capacity than TS two-way relaying protocol. Since TS has a longer time for eavesdropping ($\frac{(1+\rho)T}{2}$) than PS ($\frac{T}{2}$), the eavesdropper can overhear the users for longer time.

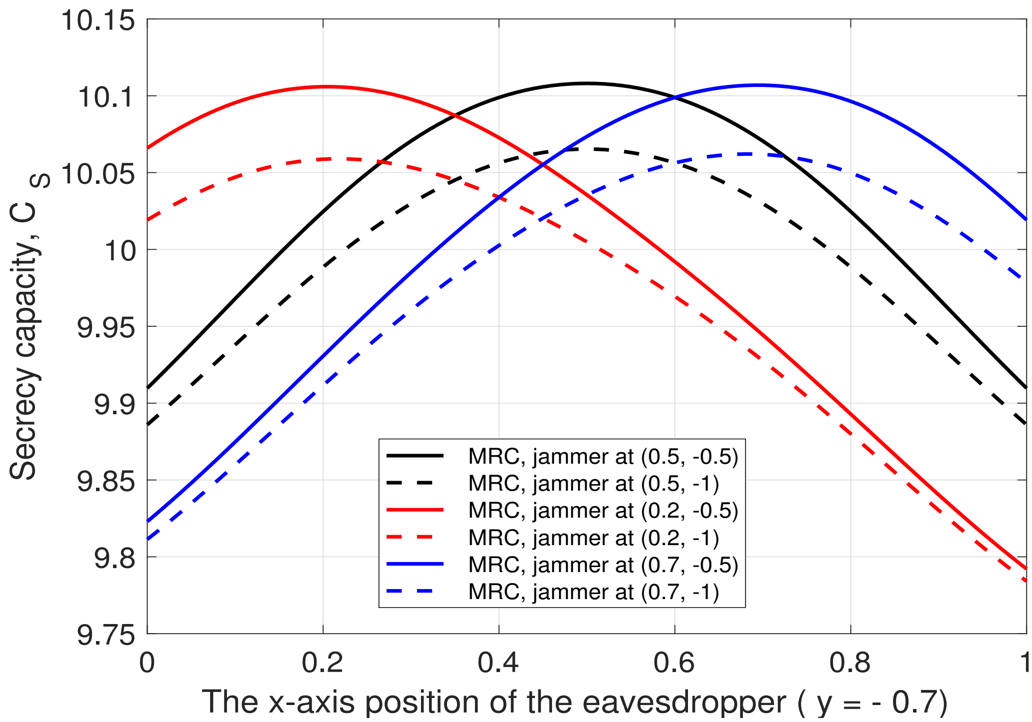

Figure 5.12: The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), for different jammer locations with $\sigma_e^2 = 0$, $\Phi = 0$, and $P_T = 10$ dB.

5.6 Conclusion

In this chapter, the secrecy capacity was investigated for a two-way energy-constrained time-switching relay network in the presence of an eavesdropper. A friendly jammer was used to reduce the ability of the eavesdropper to intercept the user signals. The secrecy capacity was maximized by jointly optimizing the time switching ratio, ρ, and the transmit power of the two users, A and B, and the jammer J. The single condensation method (SCM) was employed to convert the objective function of the corresponding optimization problem into a posynomial form suitable for geometric programming (GP). Then, GP was used to transform the non-convex objective function to obtain a convex optimization problem. Two diversity combining techniques,

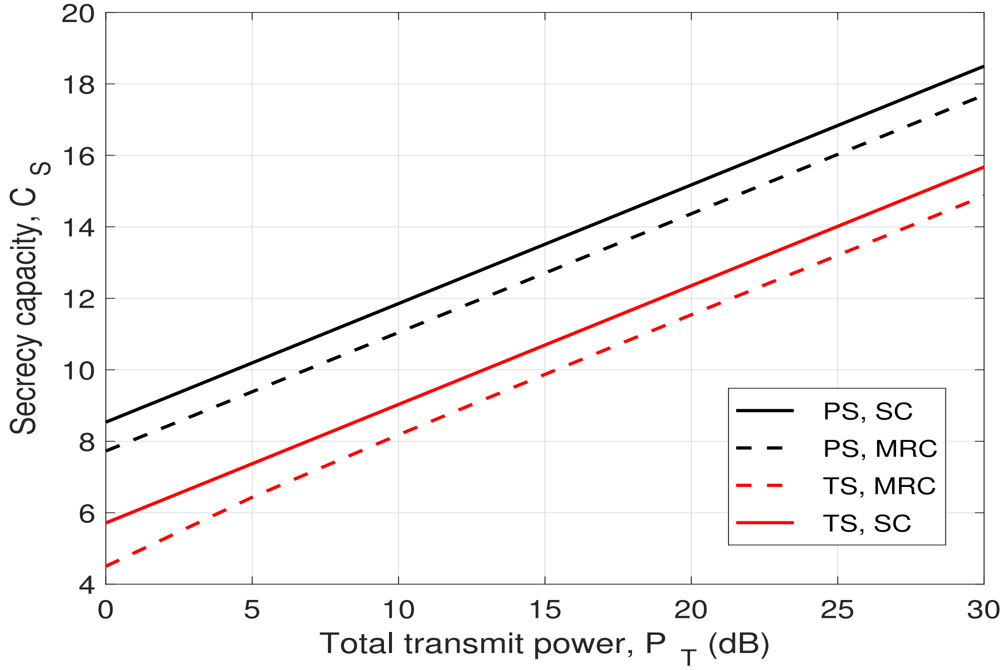

Figure 5.13: The secrecy capacity versus the x-axis location of the eavesdropper (employing MRC), with a jammer at a fixed location and without a jammer.

MRC and SC, were employed at the eavesdropper. Imperfect cancellation of the jamming signal at the relay was also considered. Results were presented which show that imperfect jamming signal cancellation at the relay degrades the secrecy capacity. In addition, utilizing a jammer improves the secrecy capacity and increases the amount of harvested energy at the relay. Further, the secrecy capacity is higher if the jammer is located closer to the eavesdropper. Imperfect channel estimation at the eavesdropper was also investigated. It was shown that as the estimation error increases, the secrecy capacity improves. MRC has shown to provide a lower secrecy capacity than SC. Thus, to achieve the SC secrecy capacity with MRC at the eavesdropper, a higher SNR is required at A and B.

Chapter 6

Conclusion and Future Work

6.1 Conclusions

In this work, the performance of simultaneous wireless information and power transfer via energy harvesting in a cooperative network was investigated. The performance was studied in terms of outage probability, secrecy capacity, and optimal power allocation. An EH structure was proposed which provides a foundation for further research. The results are summarized below and suggestions for future work are presented in Section 6.2.

In Chapter 2, a dual hop, half-duplex AF relay was considered to forward the information signal from a source equipped with multiple transmit antennas to the destination. The transmit antenna at the source was selected to maximize the end-to-end SNR. The outage probability for a given transmission rate was derived as a function of the power splitting factor at the relay. It was shown that the harvested energy at the relay increased when the number of transmit antennas increased which decreased the outage probability.

In Chapter 3, two-way relaying was introduced to provide a higher spectral efficiency than the one-way relaying studied in Chapter 2. Two users employed a two-way EH relay to exchange information in the presence of an eavesdropper and a cooperative friendly jammer. The effect of the eavesdropper was mitigated using the friendly jammer. Furthermore, the jamming signal was utilized by the relay for energy harvesting. SCM was used to convert the objective function into GP form to obtain a convex optimization problem. In this optimization problem, the power splitting factor and transmit power at the two users A and B, and J were jointly optimized to maximize the secrecy capacity. Using the jammer improved the secrecy capacity compared to the case without a jammer. It was shown that the secrecy capacity is degraded when the relay is not capable of cancelling the jamming signal perfectly. The effect of the locations of the eavesdropper and jammer on the secrecy capacity was also investigated. The best secrecy capacity was achieved when the relay was equidistant between the two users.

In Chapter 4, the system model in Chapter 3 was modified to have imperfect estimation of the channels connecting the eavesdropper to the other nodes in the system. Further, SC and MRC were employed at the eavesdropper. SCM and GP were employed to obtain a convex optimization problem and the power splitting factor and transmit power at the two users A and B, and J were jointly optimized. It was shown that an increase in channel estimation error improved the secrecy capacity as the estimation error is considered as noise at the eavesdropper. It was observed that MRC provided a lower secrecy capacity than SC. Further, the secrecy capacity was lower if the jammer was located farther from the eavesdropper.

In Chapter 5, time switching was employed at the relay and the secrecy capacity was maximized by jointly optimizing the time switching ratio and transmit power allocated to the users and jammer. It was shown that the PS two-way relaying protocol achieves a better secrecy capacity than the TS two-way relaying protocol. This is because with TS the eavesdropper can overhear the users for a longer time. It was shown that imperfect channel estimation at the eavesdropper and imperfect jamming signal cancellation at the relay resulted in a lower secrecy capacity. MRC provided a lower secrecy capacity than SC. A higher SNR was required at A and B to achieve the SC secrecy capacity with MRC at the eavesdropper.

6.2 Future Work

Three research directions for further work are described below.

6.2.1 Self-Interference Energy Recycling

Although secrecy is achievable in half-duplex transmission, full-duplex (FD) transmission could be implemented to provide spectral efficiency where the relay receives and transmits at the same time on the same channel. However, FD suffers from self-interference between the transmit and receive antennas [53]. To take advantage of this, self-interference recycling with full-duplexing was studied to extend battery lifetime via energy harvesting [54]. In [55], an energy recycling FD relay was designed to improve spectral efficiency and energy consumption. An FD AF multiple-antenna relay system employing time switching energy harvesting can be considered. An energy constrained relay harvests energy and receives information in the first phase and forwards the received signals while harvesting energy from the self-interference and transmitted signal in the second phase. The beamforming vector of the relay antenna can be optimized to maximize the achievable secrecy rate at both users in the presence of an eavesdropper. The greedy antenna switching algorithm in [56] can be employed to maximize the transmit power of the source, spectral efficiency of the system, and beamforming matrix at the relay.

6.2.2 Energy Cooperation

In previous models, relays harvest energy from the transmitted signals during communications. When a user has an abundance of harvested energy in its batteries it can transmit a portion of this energy to other users with energy harvesting capabilities. This is called energy cooperation [57]. It can be used to manage the energy at wireless nodes and prolong the network lifetime [58]. In [57], energy cooperation was introduced to allow an EH source to share energy with an EH relay. In this model, energy cooperation between multiple relays in a two-way communications network was considered. The relay with the best channel is selected to amplify (or decode) and forward the information signal. If the available transmit power is not sufficient for reliable transmission, other relay(s) can transmit power to the intended relay. The goal is to maximize the end-to-end SNR at both users through energy cooperation.

6.2.3 Multiple Relay Selection

In this dissertation, a single relay was employed to forward information signals. Multiple EH relays can be used to increase network lifetime, improving energy-efficiency, and decrease energy consumption and operational costs [126]. The best relay is selected to forward the information signals in the presence of multiple eavesdroppers.

This decision is based on variables such as the relay location and the current energy available at the relay. The goal is to select the best relay to maximize the secrecy capacity.

In [20], the performance of an EH system with best relay selection (BRS) was investigated. It was shown that spectral efficiency degradation occurs with EH relaying compared with conventional relaying. On the other hand, EH relaying has been shown to provide increased network lifetime, improved energy-efficiency, and lower energy consumption and operational costs.

Chapter 7

Appendix: Derivation of $A(c, x)$ and $B(c)$ in (2.24)

The end-to-end SNR at the destination of the proposed AF relay network in Chapter 2 is

$$\gamma_k = \gamma_{S_k,D} + \frac{\gamma_{S_k,R}\gamma_{R,D}}{1 + \gamma_{S_k,R} + \gamma_{R,D}}. \tag{7.1}$$

The CDF of (7.1) is

$$F_\gamma(c) = \Pr\left(\gamma_{S_k,D} + \frac{\gamma_{S_k,R}\gamma_{R,D}}{1 + \gamma_{S_k,R} + \gamma_{R,D}} < c\right). \tag{7.2}$$

Substituting $\gamma_{R,D}$ with x and taking the expected value of $F_\gamma(c)$ over x results in

$$F_\gamma(c) = E_x\left\{\Pr\left(\gamma_{S_k,D} + \frac{\gamma_{S_k,R}x}{1 + \gamma_{S_k,R} + x} < c\right)\right\}, \tag{7.3}$$

where E_x is the expected value with respect to x. Now using the upper bound in (2.14) to rewrite (7.3) gives

$$
\begin{aligned}
F_{\gamma_{upper}}(c) = \quad & E_x \left\{ \Pr\left(\gamma_{S_k,D} + \min(\gamma_{S_k,R}, x) < c \right) \right\} && (7.4)\\
= \quad & E_x \left\{ \Pr\left(\gamma_{S_i,D} + \min(\gamma_{S_i,R}, x) < c \right)^{S_t} \right\} && (7.5)
\end{aligned}
$$

Define $Y = \gamma_{SR}$, $W = \gamma_{SD}$, and $C = W + \min(Y, x)$, so then

$$
\begin{aligned}
F_C(c) &= \Pr\left(W + \min(Y, x) < c \right) && (7.6)\\
&= \Pr\left(W < c - \min(Y, x) \right) && (7.7)\\
&= \frac{1}{\alpha_{SR}} \int_0^\infty \Pr\left(W < c - \min(y, x) \right) e^{-\frac{y}{\alpha_{SR}}} dy. && (7.8)
\end{aligned}
$$

There are two domains for $\min(y, x)$.

1. $G_1 \in \{\min(y, x) > c\}$, then $x > c$ and $y > c$.

2. $G_2 \in \{\min(y, x) < c\}$, then $x < c$ and $y < c$.

If $x > c$ then $G_1 = \{y > c\}$ and $G_2 = \{y < c\}$, and if $x < c$ then $G_1 = \{\phi\}$ and $G_2 = \{y > 0\}$. For the case $x < c$, $F_C(c)$ can be rewritten as

$$
\begin{aligned}
F_C(c) &= \frac{1}{\alpha_{SR}} \int_0^\infty \left(1 - e^{-\frac{c - \min(y,x)}{\alpha_{SD}}} \right) e^{-\frac{y}{\alpha_{SR}}} dy && (7.9)\\
&= 1 - \frac{1}{\alpha_{SR}} \int_0^x e^{-\frac{c-y}{\alpha_{SD}}} e^{-\frac{y}{\alpha_{SR}}} dy - \frac{1}{\alpha_{SR}} \int_x^\infty e^{-\frac{c-x}{\alpha_{SD}}} e^{-\frac{y}{\alpha_{SR}}} dy && (7.10)\\
&= 1 - \frac{\alpha_{SD} e^{-\frac{c}{alpha_{SD}}}}{\alpha_{SD} - \alpha_{SR}} + \frac{\alpha_{SR}}{\alpha_{SD} - \alpha_{SR}} e^{-\frac{c}{\alpha_{SD}}} e^{-xg} && (7.11)\\
&= a + b e^{-xg} && (7.12)\\
&= A(c, x), && (7.13)
\end{aligned}
$$

where $g = \frac{\alpha_{SD}-\alpha_{SR}}{\alpha_{SD}\alpha_{SR}}$. For the case $x > c$, $\min(y, x) = y$ so $F_C(c)$ can be rewritten as

$$
\begin{aligned}
F_C(c) &= \frac{1}{\alpha_{SR}} \int_0^c \left(1 - e^{-\frac{c-y}{\alpha_{SD}}}\right) e^{-\frac{y}{\alpha_{SR}}} dy && (7.14)\\
&= 1 - e^{-\frac{c}{\alpha_{SR}}} - \frac{\alpha_{SD}}{\alpha_{SD} - \alpha_{SR}} (e^{-\frac{c}{\alpha_{SD}}} - e^{-\frac{c}{\alpha_{SR}}}) && (7.15)\\
&= B(c). && (7.16)
\end{aligned}
$$

Chapter 8

Bibiolography

Bibliography

[1] M. A. Khan, M. Z. Khan, K. Zaman, and L. Naz, "Global estimates of energy consumption and greenhouse gas emissions." *Renewable and Sustainable Energy Reviews*, vol. 29, pp. 336–344, 2014.

[2] Q. C. Li, R. Q. Hu, Y. Qian, and G. Wu, "Cooperative communications for wireless networks: techniques and applications in LTE-advanced systems," *IEEE Wireless Commun. Mag.*, vol. 19, no. 2, pp. 22–29, Apr. 2012.

[3] Y.W. Hong,W. J. Huang, F. H. Chiu, and C. C. J. Kuo, "Cooperative communications in resource-constrained wireless networks," *IEEE Signal Process. Mag.*, vol. 24, no. 3, pp. 47–57. May 2007.

[4] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 74–80, Oct. 2004.

[5] O. Ozel, K. Tutuncuoglu, J. Yang, S. Ulukus, and A. Yener, "Transmission with energy harvesting nodes in fading wireless channels: Optimal policies," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1732–1743, Sep. 2011.

[6] O. Ozel, K. Tutuncuoglu, S. Ulukus, and A. Yener, "Fundamental limits of energy harvesting communications," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 126–132, Apr. 2015.

[7] S. Kim, V. Rushi, B. Jo, N. Kyriaki, C. Ana, G. Apostolos, and T. Manos, "Ambient RF energy-harvesting technologies for self-sustainable standalone wireless sensor platforms," *Proc. IEEE*, vol. 102, no. 11, pp. 1649–1666, Nov. 2014.

[8] T. Zhu, Z. Zhong, Y. Gu, T. He, and Z. L. Zhang, "Leakage-aware energy synchronization for wireless sensor networks," *Proc. Int. Conf. Mobile Systems, Applications, and Services*, Wroclaw, Poland, Jun. 2009, pp. 319–332.

[9] H. Wang and N. B. Mandayam, "A simple packet-transmission scheme for wireless data over fading channels, *IEEE Trans. Commun.*, vol. 52, no. 7, pp. 1055–1059, Jul. 2004.

[10] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: principles and requirements," *Proc. IEEE*, vol. 101, no. 6, pp. 1410–1423, Jun. 2013.

[11] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Syngress, 2017.

[12] W. Stallings, Cryptography and Network Security: Principles and Practice, New York, NY, USA: Pearson, 2011.

[13] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*, 1st ed., Boca Raton, FL, USA: CRC Press, 2016.

[14] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4757–4767, Nov. 2013.

[15] L. Liu, R. Zhang, and K.-C. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288–300, Jan. 2013.

[16] J. Xu and R. Zhang, "Throughput optimal policies for energy harvesting wireless transmitters with non-ideal circuit power," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 2, pp. 322–332, Feb. 2014.

[17] C. Shen, W.-C. Li, and T.-H. Chang, "Wireless information and energy transfer in multi-antenna interference channel," *IEEE Trans. Signal Process.*, vol. 62, no. 23, pp. 6249–6264, Dec. 2014.

[18] L. Liu, R. Zhang, and K. C. Chua, "Wireless information and power transfer: A dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, Sep. 2013.

[19] J. Park and B. Clerckx, "Joint wireless information and energy transfer in a two-user MIMO interference channel," *IEEE Trans. Commun.*, vol. 12, no. 8, pp. 4210–4221, Aug. 2013.

[20] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[21] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in multiuser OFDM systems with wireless information and power transfer," in *Proc. IEEE Wireless Communications and Networking Conf.*, Shanghai, China, Apr. 2013, pp. 3823–3828.

[22] S. H. Lee, R. Zhang, and K. B. Huang, "Opportunistic wireless energy harvesting in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 9, pp. 4788–4799, Sep. 2013.

[23] Q. Shi, L. Liu, W. Xu, and R. Zhang, "Joint transmit beamforming and receive power splitting for MISO SWIPT systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, pp. 3269–3280, Jun. 2014.

[24] H. Ju and R. Zhang, "Throughput maximization information wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[25] I. Krikidis, S. Timotheou, and S. Sasaki, "RF energy transfer for cooperative networks: Data relaying or energy harvesting?," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1772–1775, Nov. 2012.

[26] Z. Chen, B. Xia, and H. Liu, "Wireless information and power transfer in two-way amplify-and-forward relaying channels," in *Proc. IEEE Global Conf. Signal and Information Processing*, Atlanta, GA, USA, Dec. 2014, pp. 168–172.

[27] K. Ishibashi, H. Ochiai, and V. Tarokh, "Energy harvesting cooperative communications," in *Proc. IEEE Int. Symposium on Personal, Indoor and Mobile Radio Communications*, Sydney, Australia, Sep. 2012, pp. 1819–1823.

[28] B. K. Chalise, Y. D. Zhang, and M. G. Amin, "Energy harvesting in an OSTBC based amplify-and-forward MIMO relay system," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Kyoto, Japan, Mar. 2012, pp. 3201–3204.

[29] A. M. Fouladgar and O. Simeone, "On the transfer of information and energy in multi-user systems," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1733–1737, Nov. 2012.

[30] C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3447–3461, Sep. 2014.

[31] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Qtr. 2016.

[32] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[33] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[34] Z. Ding, Z. Ma, and P. Fan, "Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[35] H. Long, W. Xiang, and Y. Li, "Precoding and cooperative jamming in multi-antenna two-way relaying wiretap systems without eavesdropper's channel state information," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1309–1318, Jun. 2017.

[36] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[37] L. Xiao, T. Zhang, X. Shen, D. Yang, and L. Cuthbert, "Secrecy in wireless information and power transfer for one-way and two-way untrusted relaying with friendly jamming," *Mob. Inf. Syst.*, vol. 2017, no. 10, art. no. 2192606, Aug. 2017.

[38] S. Sharma, A. Kumar, S. D. Roy, and S. Kundu, "Secrecy outage probability of a two-way cooperative network with an energy harvesting untrusted AF relay," *CSI Trans. ICT*, vol. 6, no. 2, pp. 129–136, Jun. 2018.

[39] M. T. Mamaghani, A. Mohammadi, P. L. Yeoh, and A. Kuhestani, "Secure two-way communication via a wireless powered untrusted relay and friendly jammer," in *IEEE Global Communications Conf.*, Singapore, Dec. 2017.

[40] S. Boyd, S.-J. Kim, L. Vandenberghe, and A. Hassibi, "A tutorial on geometric programming," *Optim. Eng.*, vol. 8, no. 1, pp. 67–127, Apr. 2007.

[41] M. Chiang, C. W. Tan, D. P. Palomar, D. O'neill, and D. Julian, "Power control by geometric programming," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2640–2651, Jul. 2007.

[42] J. Huang and A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," in *Asilomar Conf. Signals, Systems and Computers*, Pacific Grove, CA, USA, Nov. 2013, pp. 1555–1559.

[43] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[44] J. N. Laneman, D. N. C. Tse, G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behaviour," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[45] W. Peters and R. W. Heath, Jr., "Nonregenerative MIMO relaying with optimal transmit antenna selection," *IEEE Signal Process. Lett.*, vol. 15, pp. 421–424, Jan. 2008.

[46] T. Nechiporenko, P. Kalansuriya, and C. Tellambura, "Performance of optimum switching adaptive M-QAM for amplify-and-forward relays," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2258–2268, Jun. 2009.

[47] M. Ashraf, J. W. Jang, and K.-G. Lee, "Outage probability analysis for energy harvesting cooperative relays in a clustered environment," *Mobile Netw. Appl.*, vol. 23, no. 5, pp. 1208–1219, Oct. 2018.

[48] S. Gradshteyn and M. Ryzhik, Table of Integrals, Series, and Products, New York, NY, USA: Academic Press, 1980.

[49] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Relaying protocols for wireless energy harvesting and information processing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3622–3636, Jul. 2013.

[50] J. Xu, L. Liu, and R. Zhang, “Multiuser MISO beamforming for simultaneous wireless information and power transfer,” *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4798–4810, Sep. 2014.

[51] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, “Wireless powered cooperative jamming for secure OFDM system,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[52] Z. Chang, X. Hou, X. Guo, T. Ristaniemi, and Z. Han, “Secure and energy-efficient resource allocation for wireless power enabled full-/half-duplex multiple-antenna relay systems,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 11208–11219, Dec. 2017.

[53] T. Riihonen, S. Werner, and R. Wichman, “Mitigation of loopback self-interference in full-duplex MIMO relays,” *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[54] J. J. Park, J. H. Moon, and D. I. Kim, “Time-switching based in-band full duplex wireless powered two-way relay,” in *URSI Asia-Pacific Radio Science Conf.*, Seoul, Korea, Aug. 2016, pp. 438–441.

[55] M. Maso, C. Liu, C. Lee, T. Q. S. Quek, and L. S. Cardoso, “Energy-recycling full-duplex radios for next-generation networks,” *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2948-2962, Dec. 2015.

[56] C. Li, W. Wen, P. Wu, and M. Xia, “Wirelessly-powered full-duplex AF MIMO relay systems based on antenna switching,” *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1640–1643, Sept. 2019.

[57] B. Gurakan, O. Ozel, J. Yang, and S. Ulukus, "Energy cooperation in energy harvesting communications," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4884–4898, Dec. 2013.

[58] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity- part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[59] X. Huang and N. Ansari, "Energy sharing within EH-enabled wireless communication networks," *IEEE Wireless Commun.*, vol. 22, no. 3, pp. 144–149, Jun. 2015.

[60] L. R. Varshney, "Transporting information and energy simultaneously," in *Proc. IEEE Int. Symposium on Information Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1612–1616.

[61] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," in *Proc. IEEE Int. Symposium on Information Theory*, Austin, TX, USA, Jun. 2010, pp. 2363–2367.

[62] M. A. Hossain, R. Md Noor, K. A. Yau, I. Ahmedy, and S. S. Anjum, "A survey on simultaneous wireless information and power transfer with cooperative relay and future challenges," *IEEE Access*, vol. 7, pp. 19166–19198, Jan. 2019.

[63] M. Ju, K. Kang, K. Hwang, and C. Jeong, "Maximum transmission rate of PSR/TSR protocols in wireless energy harvesting DF-based relay networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 12, pp. 2701–2717, Dec. 2015.

[64] X. Di, K. Xiong, P. Fan, and H. Yang, "Simultaneous wireless information and power transfer in cooperative relay networks with rateless codes," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 2981–2996, Apr. 2017.

[65] S. Atapattu and J. Evans, "Optimal energy harvesting protocols for wireless relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5789–5803, Aug. 2016.

[66] S. Huang, Y. Yao, and Z. Feng, "Simultaneous wireless information and power transfer for relay assisted energy harvesting network," *Wireless Netw.*, vol. 24, no. 2, pp. 453–462, Feb. 2018.

[67] Y. Ye, Y. Li, D. Wang, F. Zhou, R. Q. Hu, and H. Zhang, "Optimal transmission schemes for DF relaying networks using SWIPT," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7062–7072, Aug. 2018.

[68] D. Jiang, H. Zheng, D. Tang, and Y. Tang, "Relay selection and power allocation for cognitive energy harvesting two-way relaying networks," in *Proc. IEEE Int. Conf. on Electronics Information and Emergency Commun.*, Beijing, China, May 2015, pp. 163–166.

[69] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Netw.*, vol. 25, no. 3, pp. 35–40, May 2011.

[70] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, 2nd ed., Berlin, Germany: Springer-Verlag, 2007.

[71] Y.-P. Hong, P. Lan, and C.-J. Kuo, "Enhancing physical-layer secrecy in multi-antenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[72] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symposium on Information Theory*, Seattle, WA, USA, Dec. 2006, pp. 356–360.

[73] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[74] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep. 2001, pp. 87–89.

[75] P. N. Son and H. Y. Kong, "Cooperative communication with energy harvesting relays under physical layer security," *IET Commun.*, vol. 9, no. 17, pp. 2131–2139, Nov. 2015.

[76] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi-antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[77] Y. Zhang, X. Zhao, and Y. Xie, "Secure communications in SWIPT-enabled two way relay networks," *IEEE Access*, vol. 7, pp. 111890–111896, Aug. 2019.

[78] J. Zhang, X. Tao, H. Wu, and X. Zhang, "Secure transmission in SWIPT-powered two-way untrusted relay networks," *IEEE Access*, vol. 6, pp. 10508–10519, Feb. 2018.

[79] F. Jameel, S. Wyne, and Z. Ding, "Secure communications in three-step two-way energy harvesting DF relaying," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 308–311, Feb. 2018.

[80] F. Jameel, F. Khan, M. A. A. Haider, and A. U. Haq, "On physical layer security of two way energy harvesting relays," in *Proc. Int. Conf. Frontiers of Information Technology*, Islamabad, Pakistan, Dec. 2017, pp. 35–40.

[81] C. Thakur and S. Chattopadhyay, "Secrecy performance of an improved interference-aided RF energy harvesting scheme in two-way multi-antenna relay network," in *Proc. IEEE Applied Signal Processing Conf.*, Kolkata, India, Oct. 2020, pp. 123–127.

[82] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[83] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259–6274, Aug. 2016.

[84] A. Rajaram, D. N. K. Jayakody, R. Dinis, and M. Beko, "Energy efficient secure communication model against cooperative eavesdropper," *Appl. Sci.*, vol. 11, no. 4, art. no. 1563, Feb. 2021.

[85] M. T. Mamaghani, A. Kuhestani, and K.-K. Wong, "Secure two-way transmission via wireless-powered untrusted relay and external jammer," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8451–8465, Sep. 2018.

[86] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353–1356, Jun. 2017.

[87] Y. Wang, T. Zhang, W. Yang, H. Yin, Y. Shen, and H. Zhu, "Secure communication via multiple RF-EH untrusted relays with finite energy storage," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1476–1487, Feb. 2020.

[88] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic antieavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 10, pp. 9448–9457, Oct. 2017.

[89] X. Jiang, P. Li, B. Li, Y. Zou, and R. Wang, "Security-reliability tradeoff for friendly jammer aided multiuser scheduling in energy harvesting communications," *Secur. Commun. Netw.*, vol. 2021, art. no. 5599334, Apr. 2021.

[90] K. Cao, B. Wang, H. Ding, and J. Tian, "Adaptive cooperative jamming for secure communication in energy harvesting relay networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1316–1319, Oct. 2019.

[91] K. Lee, J. Hong, H. Choi, and T. Q. S. Quek, "Wireless-powered two-way relaying protocols for optimizing physical layer security," *IEEE Trans. Inf. Forens. Security*, vol. 14, no. 1, pp. 162–174, Jan. 2019.

[92] D.-H. Ha, T. N. Nguyen, M. H. Q. Tran, X. Li, P. T. Tran, and M. Voznak, "Security and reliability analysis of a two-way half-duplex wireless relaying network using partial relay selection and hybrid TPSR energy harvesting at relay nodes," *IEEE Access*, vol. 8, pp. 187165–187181, Oct. 2020.

[93] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1878–1911, 2nd Qtr. 2018.

[94] M. Hayajneh and T. A. Gulliver, "Wireless information and power transfer with optimal transmit antenna selection," *IET Commun.*, vol. 13, no. 19, pp. 3217–3221, Dec. 2019.

[95] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4754–4767, Nov. 2013.

[96] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[97] A. Yenner and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct. 2015.

[98] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Qtr. 2014.

[99] K. Cumanan, G. C. Alexandropoulos, Z. Ding, and G. K. Karagiannidis, "Secure communications with cooperative jamming: Optimal power allocation and secrecy outage analysis," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 7495–7505, Aug. 2017.

[100] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[101] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[102] G. Zheng, L. Choo, and K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[103] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, Jun. 2011.

[104] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[105] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," in *Proc. IEEE Conf. and Exhibition on Global Telecommunications*, New Orleans, LA, USA, Dec. 2008, pp. 1–5.

[106] C. Y. Wang, T. C. K. Liu, and X. D. Dong, "Impact of channel estimation error on the performance of amplify-and-forward two-way relaying," *IEEE Trans. Veh. Technol.*, vol. 61, no. 3, pp. 1197–1207, Mar. 2012.

[107] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[108] X. Chen, J. Chen, H. Zhang, Y. Zhang, and C. Yuen, "On secrecy performance of multiantenna-jammer-aided secure communications with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8014–8024, Oct. 2016.

[109] M. Hayajneh and T. A. Gulliver, "Secrecy capacity in two-way energy harvesting relay networks with a friendly jammer," *Wireless Netw.*, vol. 27, pp. 4551–4566, Aug. 2021.

[110] A. A. Babayo, M. H. Anisi, and I. Ali, "A review on energy management schemes in energy harvesting wireless sensor networks," *Renew. Sustain. Energy Rev.*, vol. 76, pp. 1176–1184, Sep. 2017.

[111] I. Ahmed, M. M. Butt, C. Psomas, A. Mohamed, I. Krikidis, and M. Guizani, "Survey on energy harvesting wireless communications: Challenges and opportunities for radio resource allocation," *Comput. Netw.*, vol. 88, pp. 234–248, Sep. 2015.

[112] L. D. Nguyen, "Resource allocation for energy efficiency in 5G wireless networks," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 5, no. 14, Jun. 2018.

[113] S. A. A. Kazmi and S. Coleri, "Optimization of full-duplex relaying system with non-linear energy harvester," *IEEE Access*, vol. 8, pp. 201566–201576, Oct. 2020.

[114] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, C. Symeon, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): recent advances and future challenges," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 264–302, Dec. 2018.

[115] D. N. Hanh, H. V. Khuong, and D. D. Thiem, "Secrecy analysis of overlay mechanism in radio frequency energy harvesting networks with jamming under Nakagami-m fading," *Wirel. Pers. Commun.*, vol. 120, no. 1, pp. 1–33, Sep. 2021.

[116] H. H. Jang, K. W. Choi, and D. I. Kim, "Novel frequency splitting SWIPT for overcoming amplifier nonlinearity," *IEEE Wireless Commun. Lett.*, vol. 6, no. 9, pp. 826–829, Jun. 2020.

[117] P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Security in energy harvesting networks: a survey of current solutions and research challenges," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2658–2693, 4th Qtr. 2020.

[118] W. Wang, K. C. Teh, and K. H. Li, "Generalized relay selection for improved security in cooperative DF relay networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 1, pp. 28–31, Feb. 2016.

[119] A. Pandey and S. Yadav, "Physical layer security for cellular multiuser two-way relaying networks with single and multiple decode and- forward relays," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 12, pp. 3639–3662, Dec. 2019.

[120] M. K. Shukla, A. Pandey, S. Yadav, and N. Purohit, "Secrecy outage analysis of full duplex cellular multiuser two-way AF relay networks," in *Proc. Int. Conf. on Wireless Communications Signal Processing and Networking*, Kalavakkam, India, Oct. 2019, pp. 458–463.

[121] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[122] X. Li, M. Zhao, X.-C. Gao, L. Li, D.-T. Do, K. M. Rabie, and R. Kharel, "Physical layer security of cooperative NOMA for IoT networks under I/Q imbalance," *IEEE Access*, vol. 8, pp. 51189–51199, 2020.

[123] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.

[124] C. E. Shannon, "Two-way communication channels," in *Proc. Berkeley Symposium on Mathematical Statistics and Probability*, Berkeley, CA, USA., Jun.–Jul. 1960, vol. 4.1, pp. 611–644.

[125] B. Rankov and A. Wittneben, "Achievable rate regions for the two way relay channel," in *Proc. IEEE Int. Symposium on Information Theory*, Seattle, WA, USA, Jul. 2006, pp. 1668–1672.

[126] A. Andrawes, R. Nordin, and M. Ismail, "Wireless energy harvesting with co-operative relaying under the best relay selection scheme", *Energies*, vol. 12, no. 5, pp. 892–914, Mar. 2019.