저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:

저작자표시. 귀하는 원저작자를 표시하여야 합니다.

비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.

변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리의 내용에 의하여 영향을 받지 않습니다.

이것은 이용허락규약(Legal Code)을 이해하기 쉽게 요약한 것입니다.

Disclaimer
Energy Beamforming for Full-Duplex Wireless Powered Communication in Presence of Eavesdropper

도청자가 존재하는 전이중 무선전력통신에서 에너지 빔 형성

BY

Juhwan Seo

AUGUST 2017

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING COLLEGE OF ENGINEERING SEOUL NATIONAL UNIVERSITY
Abstract

Energy Beamforming for Full-Duplex Wireless Powered Communication in Presence of Eavesdropper

Juhwan Seo

Department of Electrical and Computer Engineering
The Graduate School
Seoul National University

To improve spectrum utilization, full duplex (FD) communication technique is applied to wireless powered communication (WPC). The cochannel interference from energy transmission reduces achievable rate of information transmission. However, when an eavesdropper tries to intercept the information in the FD WPC systems, the energy signal from the power beacon acts as a jamming signal to the eavesdropper. Hence, the secrecy rate of the system is not always degraded by the energy transmission.
In this thesis, to control the energy signal transmitted to the source and eavesdropper, we propose an optimal beamforming scheme for secure communication in a FD WPC system consists of a multi-antenna power beacon, a source, a destination, and an eavesdropper. By using the beamforming scheme, the power beacon transmits an energy signal to a source which acts as a jamming signal to an eavesdropper and the source transmits an information signal by using harvested energy. We consider a scenario that the channel state information of eavesdropper is imperfect. We formulate an optimization problem to find an optimal beamforming for maximizing worst-case secrecy rate assuming that channel state information of the wiretap channel is imperfect. Also, we propose an algorithm to solve the problem. Simulation results show the secrecy performance of FD WPC system with the proposed beamforming scheme.

**Keywords:** Wireless powered communication, secrecy rate, energy beamforming, full-duplex, energy harvesting.

**Student Number:** 2015-20934.
# Contents

Abstract

Contents

List of Figures

Chapter 1 Introduction

Chapter 2 System Model

  2.1 Received SINR and Secrecy Rate
  2.2 Worst-Case Secrecy Rate

Chapter 3 Maximization of Worst-Case Secrecy Rate

Chapter 4 Proposed Energy Beamforming

Chapter 5 Simulation Results

Chapter 6 Conclusion
List of Figures

Figure 2.1 System model of FD WPC system in the presence of eavesdropper. .............................................. 6

Figure 5.1 Average secrecy rate of FD/HD WPC system versus $P_{PB}, N_{PB} = 2$. ............................................. 29

Figure 5.2 Average secrecy rate of FD/HD WPC system versus $P_{PB}, N_{PB} = 3$. ............................................. 30

Figure 5.3 Average secrecy rate of FD/HD WPC system versus $P_{PB}, N_{PB} = 4$. ............................................. 31

Figure 5.4 Average secrecy rate of FD/HD WPC system versus $P_{PB}, N_{PB} = 5$. ............................................. 32

Figure 5.5 Average secrecy rate of FD WPC system versus $\alpha$, $P_{PB} = 10$ dB. ............................................. 33
Figure 5.6 Average secrecy rate of FD WPC system versus $\alpha$,

$P_{PB} = 20$ dB. ............................................. 34

Figure 5.7 Average secrecy rate of FD WPC system versus $\alpha$,

$P_{PB} = 30$ dB ............................................. 35

Figure 5.8 Secrecy outage probability of FD WPC system versus

$P_{PB}$, $N_{PB}$=3, $R_{th}$ = 2 bps/Hz. ......................... 36

Figure 5.9 Secrecy outage probability of FD WPC system versus

$P_{PB}$, $N_{PB}$=5, $R_{th}$ = 2 bps/Hz. ......................... 37
Chapter 1

Introduction

Wireless powered communication (WPC) applies wireless energy transfer to conventional wireless communication systems. In the WPC systems, an energy-constrained source communicates with a destination by using harvested energy from a dedicated energy source, e.g., power beacon, hybrid access point (HAP) [1], [2].

Generally, a HAP transmits an energy signal to users for energy transmission and then users transmits an information signal to the HAP for information transmission by using the harvested energy. However, if a channel
between HAP and user is poor, the user harvests little energy and transmits the information signal to the HAP through the poor channel. This problem is called doubly near-far problem [3], [4]. To avoid the doubly-near-far problem, the concept of power beacon has been considered. the power beacon is not co-located with the information receiver. Hence, the channel for energy transmission is independent to the channel for information transmission.

On the other hand, many previous works focus on a HD WPC systems where energy and information are transmitted over different time/frequency resources. An resource allocation in a multi-user HD WPC system is considered in [4]. An resource allocation and a beamforming are considered to maximize the secrecy performance in [5]. Performances of HD WPC systems in the presence of an interferer is analyzed and an optimal time splitting ratio is obtained in [6].

Full-duplex (FD) WPC systems are recently considered to improve spectrum efficiency [7]-[10]. In the FD WPC systems, energy and information are simultaneously transmitted over the same frequency band so that the energy transmitted from the dedicated energy source acts as an interference to the
destination. To avoid the co-channel interference, beamforming of both en-
gergy transmitter and information transmitter is proposed in [8]. However, the
co-channel interference still remains when optimal beamforming is adopted
in that work.

Physical layer security of wireless communication has drawn much at-
tention due to the fact that it does not need any encryption scheme [11].
In the physical layer security, to ensure perfect secrecy, jamming schemes
have been proposed in the literature. Based on the worst-case secrecy rate,
authors proposed robust transmission schemes for MISO wiretap channels
in [12]. Authors propose beamforming schemes of full-duplex (FD) jamming
receiver in [13]. In the WPC system, wireless powered jammer is considered
to ensure secure communication [14]-[16].

When an eavesdropper tries to intercept the information in the FD WPC
systems, the energy signal from the power beacon acts as a jamming signal
to the eavesdropper. Hence, the secrecy rate of the system is not always
degraded by the energy transmission. Also, it is necessary to properly con-
trol energy transmitted to the source and eavesdropper via beamforming to
achieve desired secrecy rate.

To the best of our knowledge, there exists only one work considering secure communication in the FD WPC system [17]. However, that work neglected the ability of the power beacon as a jammer to an eavesdropper.

In this thesis, we consider a FD WPC system in which the signal of a power beacon acts as a jamming signal at an eavesdropper. We propose an optimal beamforming at the power beacon to maximize the worst-case secrecy rate considering imperfect channel state information (CSI) about the eavesdropper.

The rest of this thesis is organized as follows. Chapter 2 describes the full-duplex wireless powered communication with eavesdropper. Chapter 3, the optimization problem is formulated. Chapter 4, an algorithm to obtain solution of optimization problem is proposed. The simulation results are shown in chapter 5 and the conclusion is given in chapter 6.
Chapter 2

System Model

Consider a full-duplex (FD) wireless powered communication (WPC) system consists of a power beacon $PB$, a source $S$, a destination $D$, and an eavesdropper $E$ as shown in Figure 1. Suppose that the power beacon has $N_{PB}$ transmit antennas, and the source has a transmit antenna for information transmission and a receive antenna for energy harvesting. Suppose that both the destination and eavesdropper have a receive antenna.
Figure 2.1. System model of FD WPC system in the presence of eavesdropper.
2.1 Received SINR and Secrecy Rate

Suppose that transmission takes place in frames of length $T$. In each frame, the power beacon transmits an energy signal $x_{PB} \in \mathbb{C}^{N_{PB} \times 1}$ with power $P_{PB}$ via beamforming. The source harvests energy from the energy signal and simultaneously transmits to the destination an information signal $x_S$ with power $P_S$ while the eavesdropper tries to intercept the transmitted signal from the source. In addition, the source harvests energy from its own transmitted information signal. The transmitted energy signal from the power beacon acts as an interference to both the destination and the eavesdropper.

Assume that all channels remain constant during a frame and vary independently from one frame to another. Assume that all channels have an additive white Gaussian noise (AWGN) with zero mean and variance $\sigma^2$. $h_{PB,X} \in \mathbb{C}^{N_{PB} \times 1}$, $X \in \{S, D, E\}$, is the channel vector from the power beacon to the node $X$, and $h_{S,X}$ is the channel coefficient from the source to the node $X$.

The energy signal $x_{PB}$ is a complex Gaussian random vector with zero
mean and covariance matrix $Q$ \cite{18}- \cite{20}. The amount of harvested energy at the source during a frame is given by

$$E = \eta(P_S|h_{S,S}|^2 + \mathbb{E}(|h_{PB,S}^H x_{PB}|^2))T$$

(2.1)

$$= \eta(P_S|h_{S,S}|^2 + h_{PB,S}^H Qh_{PB,S})T,$$

where $\eta$ is the energy harvesting efficiency, $\mathbb{E}[\cdot]$ stands for expectation, and $(\cdot)^H$ stands for Hermitian transpose.

The source uses the harvested energy to transmit the information signal $x_S$. The transmit power of the source is given by

$$P_S = \frac{E}{T} = \eta(P_S|h_{S,S}|^2 + h_{PB,S}^H Qh_{PB,S}),$$

(2.2)

or equivalently

$$P_S = \frac{\eta h_{PB,S}^H Qh_{PB,S}}{1 - \eta|h_{S,S}|^2}.$$
The received signal at the destination is given by

\[ y_D = h_{S,D} x_S + h_{P,B,D}^H x_{P,B} + n_D, \]  

(2.4)

where \( n_D \) is an AWGN. The received signal at the eavesdropper is given by

\[ y_E = h_{S,E} x_S + h_{P,B,E}^H x_{P,B} + n_E, \]  

(2.5)

where \( n_E \) is an AWGN. From (2.3), (2.4), and (2.5), the received SINRs at the destination and eavesdropper are given by

\[ \gamma_D = \frac{\eta}{1 - \eta |h_{S,S}|^2} \frac{h_{P,B,S}^H Q h_{P,B,S} |h_{S,D}|^2}{\sigma^2 + h_{P,B,D}^H Q h_{P,B,D}} \]  

(2.6)

and

\[ \gamma_E = \frac{\eta}{1 - \eta |h_{S,S}|^2} \frac{h_{P,B,S}^H Q h_{P,B,S} |h_{S,E}|^2}{\sigma^2 + h_{P,B,E}^H Q h_{P,B,E}}, \]  

(2.7)

respectively. From (2.6) and (2.7), the secrecy rate of the system is given
by [21]

\[ R_s = [R_D - R_E]^+, \]

\[ = \left[ \log_2 \left( 1 + \frac{|h_{S,D}|^2}{1 - \eta|h_{S,S}|^2} \cdot \frac{\eta h_{PB,S}^H Q h_{PB,S}}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} \right) \right]^+, \]

\[ = \left[ \log_2 \left( 1 + \frac{|h_{S,E}|^2}{1 - \eta|h_{S,S}|^2} \cdot \frac{\eta h_{PB,S}^H Q h_{PB,S}}{\sigma^2 + h_{PB,E}^H Q h_{PB,E}} \right) \right]^+, \]

where \( R_D = \log_2(1 + \gamma_D) \), \( R_E = \log_2(1 + \gamma_E) \), and \([x]^+ = \max\{0, x\}\).

### 2.2 Worst-Case Secrecy Rate

Assume that the power beacon has imperfect CSI of the channel from the power beacon to the eavesdropper and that from the source to eavesdropper, whereas the power beacon has the perfect CSI of the other channels. Let \( \hat{h}_{PB,E} \) and \( \hat{h}_{S,E} \) denote the imperfect CSI of the channel from the power beacon to the eavesdropper and from the source to that, respectively. Define the errors of the imperfect CSI as

\[ \Delta_{PB} \triangleq h_{PB,E} - \hat{h}_{PB,E} \]
and
\[
\Delta_S \triangleq h_{S,E} - \tilde{h}_{S,E},
\]  
respectively. Assume that \(\Delta_{PB}\) and \(\Delta_S\) are bounded in the following regions [12]:
\[
\mathcal{G}_{PB} = \{ \Delta_{PB} : \| \Delta_{PB} \| \leq \varepsilon_{PB} \}
\]  
and
\[
\mathcal{G}_S = \{ \Delta_S : |\Delta_S| \leq \varepsilon_S \},
\]
respectively, where \(\varepsilon_{PB}\) and \(\varepsilon_S\) are corresponding error bounds which are known at power beacon \(PB\).

The errors due to the imperfect CSI affect \(R_E\) so that it is rewritten as
\[
R_E = \log_2 \left( 1 + k \frac{\mathbf{h}_{PB,S}^H \mathbf{Q} \mathbf{h}_{PB,S} |\hat{h}_{S,E} + \Delta_S|^2}{\sigma^2 + (\mathbf{h}_{PB,E} + \Delta_{PB})^H \mathbf{Q} (\mathbf{h}_{PB,E} + \Delta_{PB})} \right),
\]  

11
where \( k = \eta/(1 - \eta|h_{S,S}|^2) \). The worst-case secrecy rate is defined as

\[
\Delta_{PB,\Delta_S} R_s = \min_{\Delta_{PB,\Delta_S}} \left[ R_D - \max_{\Delta_{PB,\Delta_S}} R_E \right]^+
= \left[ \log_2 \left( 1 + k \frac{h_{PB,S}^H Q h_{PB,S} |h_{S,D}|^2}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} \right) \right] +
- \log_2 \left( 1 + \max_{\Delta_{PB,\Delta_S}} k \frac{h_{PB,S}^H Q h_{PB,S} |\hat{h}_{S,E} + \Delta_S|^2}{\sigma^2 + (\hat{h}_{PB,E} + \Delta_{PB})^H Q (\hat{h}_{PB,E} + \Delta_{PB})} \right) ^+.
\]

(2.14)
Chapter 3

Maximization of Worst-Case Secrecy Rate

To maximize the worst-case secrecy rate in (2.14), the optimization problem to find the optimal covariance matrix $Q$ is formulated as...
\[
\begin{align*}
\max_Q \quad & \log_2 \left( 1 + k \frac{\mathbf{h}_{PB,S}^H \mathbf{Q} \mathbf{h}_{PB,S} |h_{S,D}|^2}{\sigma^2 + \mathbf{h}_{PB,D}^H \mathbf{Q} \mathbf{h}_{PB,D}} \right) \\
- \log_2 \left( 1 + \max_{\Delta_{PB}, \Delta_s} \frac{k}{\sigma^2} \frac{\mathbf{h}_{PB,S}^H \mathbf{Q} \mathbf{h}_{PB,S} |\hat{h}_{S,E} + \Delta_s|^2}{(\mathbf{h}_{PB,E} + \Delta_{PB})^H \mathbf{Q} (\mathbf{h}_{PB,E} + \Delta_{PB})} \right) \quad (3.1a) \\
\text{s. t.} \quad & \text{tr}(\mathbf{Q}) = P_{PB}, \quad (3.1b) \\
& \mathbf{Q} \succeq 0 \quad (3.1c)
\end{align*}
\]

where \( \text{tr} (\cdot) \) is the trace function. The constraint (3.1b) is transmit power constraint at the power beacon and the constraint (3.1c) is the positive semi-definite constraint of covariance matrix \( \mathbf{Q} \).

The objective function (3.1a) is non-concave so that the optimization problem (3.1) is non-convex and difficult to solve directly. We introduce an auxiliary variable \( t \) and reformulate the optimization problem (3.1) as
\[
\max_{Q, t} \log_2 \left( 1 + k \frac{h_{PB,S}^H Q h_{PB,S} |h_{S,D}|^2}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} \right) \\
- \log_2 (1 + kt) \tag{3.2a}
\]
\[
\text{s. t. } \max_{\Delta_{PB}, \Delta_S \sigma^2} \frac{h_{PB,S}^H Q h_{PB,S} |\hat{h}_{S,E} + \Delta_S|^2}{\Delta_{PB}^2 + (h_{PB,E} + \Delta_{PB})^H Q (h_{PB,E} + \Delta_{PB})} \leq t, \tag{3.2b}
\]
\[
\text{tr}(Q) = P_{PB}, \tag{3.2c}
\]
\[
Q \succeq 0. \tag{3.2d}
\]

The optimization problem (3.2) is divided into the following two-level subproblems. The inner problem for finding the optimal covariance matrix given a fixed \(t\) is given by
\[ H(t) = \max_Q \log_2 \left( 1 + k \frac{h^H_{PB,S} Q h_{PB,S} |h_{S,D}|^2}{\sigma^2 + h^H_{PB,D} Q h_{PB,D}} \right) \]

\[- \log_2 (1 + kt) \quad (3.3a)\]

s. t. \[
\max_{\Delta_s} h^H_{PB,S} Q h_{PB,S} |\hat{h}_{S,E} + \Delta_s|^2 \\
\min_{\Delta_{PB}} \left( \sigma^2 + (\hat{h}_{PB,E} + \Delta_{PB})^H Q (\hat{h}_{PB,E} + \Delta_{PB}) \right) \leq t, \quad (3.3b)\]

\[ \text{tr}(Q) = P_{PB}, \quad (3.3c)\]

\[ Q \succeq 0. \quad (3.3d)\]

The outer problem for finding the optimal value of \( t \) is given by

\[ H^* = \max_t H(t). \quad (3.4)\]
Chapter 4

Proposed Energy Beamforming

After some algebraic manipulations, the optimization problem (3.3) is equivalently simplified as

\[
\max_Q \frac{h_{PB,S}^H Q h_{PB,S}}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} \tag{4.1a}
\]

s. t. \[ \frac{1}{\Delta_s} \max_{\Delta_S} h_{PB,S}^H Q h_{PB,S} |\hat{\Delta}_{S,E} + \Delta_S|^2 \leq \min_{\Delta_{PB}} \left( \sigma^2 + (\hat{\Delta}_{PB,E} + \Delta_{PB})^H Q (\hat{\Delta}_{PB,E} + \Delta_{PB}) \right), \tag{4.1b} \]

\[ \text{tr}(Q) = P_{PB}, \tag{4.1c} \]

\[ Q \succeq 0. \tag{4.1d} \]
In the left hand side of (4.1b), we have the following inequality:

\[
\begin{align*}
    h_{PB,S}^H Q h_{PB,S} |\hat{h}_{S,E} + \Delta_S|^2 \\
    \leq h_{PB,S}^H Q h_{PB,S} (|\hat{h}_{S,E}| + |\Delta_S|)^2 \quad (4.2a) \\
    \leq h_{PB,S}^H Q h_{PB,S} (|\hat{h}_{S,E}| + \epsilon)^2, \quad (4.2b)
\end{align*}
\]

where (4.2a) follows from the triangle inequality and (4.2b) follows from (2.12), and both inequalities (4.2a), (4.2b) become equalities when \( \Delta_S = \epsilon \hat{h}_{S,E}/|\hat{h}_{S,E}| \).

Based on the inequality (4.2b), the optimization problem (4.1) is reformulated as

\[
\begin{align*}
    \max_Q & \quad h_{PB,S}^H Q h_{PB,S} \\
    \text{s. t.} & \quad \frac{1}{t} h_{PB,S}^H Q h_{PB,S} \left(|\hat{h}_{S,E}|^2 + \epsilon^2 + 2\epsilon |\hat{h}_{S,E}| \right) \\
    & \leq \min_{\Delta_{PB}} \left( \sigma^2 + (\hat{h}_{PB,E} + \Delta_{PB})^H Q (\hat{h}_{PB,E} + \Delta_{PB}) \right), \quad (4.3b) \\
    & \text{tr}(Q) = P_{PB}, \quad (4.3c) \\
    & Q \succeq 0. \quad (4.3d)
\end{align*}
\]
To tackle the non-convexity of the linear-fractional function (4.3a), we use the Charnes-Cooper transformation which transforms the linear-fractional function (4.3a) to a linear function [23]. Let \( u = 1/(\sigma^2 + h_{PB,D}^H Q h_{PB,D}) \) and \( W = Q/u \). The objective function (4.3a) is rewritten as

\[
\begin{align*}
\frac{h_{PB,S}^H Q h_{PB,S}}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} &= h_{PB,S}^H (u Q) h_{PB,S} \\
&= h_{PB,S}^H W h_{PB,S}.
\end{align*}
\] (4.4)

\( u = 1/(\sigma^2 + h_{PB,D}^H Q h_{PB,D}) \) can be rewritten as

\[
1 = \sigma^2 u + h_{PB,D}^H (u Q) h_{PB,D}
\] (4.5)

Due to the fact that \( u \geq 0 \), the constraint (4.3b) is equivalent to

\[
\frac{1}{\bar{\Delta}_{PB}} h_{PB,S}^H W h_{PB,S} \left( |\hat{h}_{S,E}|^2 + \varepsilon^2 + 2\varepsilon |\hat{h}_{S,E}| \right) \leq \min_{\Delta_{PB}} \left( \sigma^2 + (\hat{h}_{PB,E} + \Delta_{PB})^H Q (\hat{h}_{PB,E} + \Delta_{PB}) \right). \] (4.6)
The constraint (4.3c) and (4.3d) are rewritten as

\[ \text{tr}(W) = P_{PB}u \quad (4.7) \]

and

\[ W \succeq 0 \quad (4.8) \]

, respectively. From (4.5), (4.6), (4.7), and (4.8), the optimization problem (4.3) is reformulated as

\[
\begin{align*}
\text{maximize} \quad & h_{PB,S}^H W h_{PB,S} \\
\text{subject to} \quad & \sigma^2 u + h_{PB,D}^H W h_{PB,D} = 1, \\
& \frac{1}{2} h_{PB,S}^H W h_{PB,S} \left( |\hat{h}_{S,E}|^2 + \varepsilon_S^2 + 2\varepsilon_S |\hat{h}_{S,E}| \right) \\
& \quad \leq \min_{\Delta_{PB}} \left( \sigma^2 u + (\hat{h}_{PB,E} + \Delta_{PB})^H W (\hat{h}_{PB,E} + \Delta_{PB}) \right), \\
& \text{tr}(W) = P_{PB}u, \\
& W \succeq 0.
\end{align*}
\]

The optimization problem (4.9) is still non-convex due to the non-convex
constraint (4.9c) which contains $\Delta_{PB}$. The constraint (4.3b) can be transformed to linear matrix inequality (LMI) by the following lemma 4.0.1.

**Lemma 4.0.1.** *(S-procedure [24]*) Let a function $f_m, m = 1, 2,$ be defined as

$$f_m(x) = x^H A_m x + 2 \text{Re}\{b_m^H x\} + c_m$$  \hspace{1cm} (4.10)

where $A_m$ is symmetric matrix, $b_m$ is vector, and $c_m$ is scalar. Then, there exists a vector $x$ satisfying

$$f_1(x) \geq 0$$ \hspace{1cm} (4.11)

$$f_2(x) \geq 0$$ \hspace{1cm} (4.12)

if and only if there exist $\lambda \geq 0$ such that

$$\begin{bmatrix} A_2 & b_2 \\ b_2^H & c_2 \end{bmatrix} - \lambda \begin{bmatrix} A_1 & b_1 \\ b_1^H & c_1 \end{bmatrix} \succeq 0.$$ \hspace{1cm} (4.13)
The constraint (4.9c) can be rewritten as two constraints, i.e.,

\[
\sigma^2 u + \hat{h}_{PB,E}^H \hat{W}_{PB,E} + 2 \text{Re}(\hat{h}_{PB,E}^H \hat{W} \Delta_{PB}) \\
+ \Delta_{PB}^H \hat{W} \Delta_{PB} - \frac{\hat{h}_{PB,S}^H \hat{W}_{PB,S}(|\hat{h}_{S,E}|^2 + \varepsilon_S^2 + 2 |\hat{h}_{S,E}| \varepsilon_S)}{t} \geq 0
\]

(4.14)

and

\[
\Delta_{PB}^H \Delta_{PB} \leq \varepsilon_{PB}^2.
\]

(4.15)

According to lemma 4.0.1., the constraints (4.14) and (4.15) can be combined as LMI, i.e.,

\[
\begin{bmatrix}
\lambda \mathbf{I} + \mathbf{W} & \mathbf{W}^H \hat{h}_{PB,E} \\
\hat{h}_{PB,E}^H \mathbf{W} & -\lambda \varepsilon_{PB}^2 + \sigma^2 u + \hat{h}_{PB,E}^H \mathbf{W} \hat{h}_{PB,E} \\
\end{bmatrix} \succeq 0.
\]

(4.16)

The optimization problem (4.9) can be reformulated as semidefinite programming problem:
\[
\begin{align*}
\max_{\mathbf{W}, \sigma, \lambda} & \quad \mathbf{h}_{PB,S}^{H} \mathbf{W} \mathbf{h}_{PB,S} \\
\text{s. t.} & \quad \sigma^{2} u + \mathbf{h}_{PB,D}^{H} \mathbf{W} \mathbf{h}_{PB,D} = 1, \\
& \quad \begin{bmatrix}
\lambda \mathbf{I} + \mathbf{W} & \mathbf{W}^{H} \hat{\mathbf{h}}_{PB,E} \\
\hat{\mathbf{h}}_{PB,E}^{H} \mathbf{W} & -\lambda \mathbf{I} + \sigma^{2} u + \hat{\mathbf{h}}_{PB,E}^{H} \mathbf{W} \hat{\mathbf{h}}_{PB,E} \\
- \mathbf{h}_{PB,S}^{H} \mathbf{W} \mathbf{h}_{PB,S} (|\hat{h}_{S,E}|^{2} + \sigma^{2} + 2\sigma |\hat{h}_{S,E}|) 
\end{bmatrix} \succeq 0, \\
\text{tr}(\mathbf{W}) &= P_{PB} u, \\
\mathbf{W} &\succeq 0
\end{align*}
\] (4.17)

where \( \mathbf{I} \) is an identity matrix. The optimization problem (4.17) can be solved by a convex programming tool, e.g., CVX.
The optimization problem (3.4) is a single-variable non-convex problem so that the problem (3.4) is solved by one dimensional exhaustive search over \((0, t_{\text{max}}]\). \(t_{\text{max}}\) is derived as follows:

\[
\begin{align*}
    t &\leq \frac{h_{PB,S}^H Q h_{PB,S} |h_{S,D}|^2}{\sigma^2 + h_{PB,D}^H Q h_{PB,D}} \\
    &\leq \frac{h_{PB,S}^H Q h_{PB,S} |h_{S,D}|^2}{\sigma^2} \\
    &\leq \frac{\text{tr}(Q) \text{tr}(h_{PB,S} h_{PB,S}^H) |h_{S,D}|^2}{\sigma^2} \\
    &= \frac{P_{PB} \| h_{PB,S} \|^2 |h_{S,D}|^2}{\sigma^2} \\
    &= t_{\text{max}},
\end{align*}
\]

where (4.18a) follows from the fact that the secrecy rate should be nonnegative in (3.3a), and (4.18c) follows from the matrix trace inequality in [25].

The overall process for solving the optimization problem (3.1) is described in Algorithm 1.
Algorithm 1: Proposed algorithm for obtaining Q

1. Initialize $i = 0$, $t_0 = 0$, and an iterative step $\Delta t$.

2. repeat
   
3. \hspace{1cm} $i = i + 1$.

4. \hspace{1cm} $t_i = t_{i-1} + \Delta t$.

5. \hspace{1cm} Obtain $Q_i = W_i / u_i$ by solving (4.17).

6. \hspace{1cm} Compute $H(t_i)$ from the objective function of (3.3a).

7. until $t_i < t_{\text{max}}$

8. $i^* = \arg \max_i H(t_i)$.

9. Update $Q = Q_{i^*}$.
Chapter 5

Simulation Results

In this chapter, we simulate average secrecy rate of a full duplex (FD) wireless powered communication (WPC) system where energy and information are simultaneously transmitted over the same frequency band. Suppose that the energy harvesting efficiency \( \eta = 0.8 \) and the noise variance \( \sigma^2 = -70 \text{ dBm} \). As in [7], assume that \( h_{S,S} = 10^{-0.75} \). Assume that the entries of \( h_{PB,S} \) are independent and identically distributed (i.i.d) complex Gaussian random variables with zero mean and variance \( \lambda_1 = -30 \text{ dB} \). Except for both \( h_{S,S} \) and \( h_{PB,S} \), all the channel coefficients and entries of channel vectors are
i.i.d. complex Gaussian random variables with zero mean and variance $\lambda_2 = -50$ dB. Let $\alpha = \varepsilon_{PB}^2/\lambda_2 = \varepsilon_S^2/\lambda_2$.

Figure 5.1, Figure 5.2, Figure 5.3, and Figure 5.4 show the average secrecy rate versus the transmit power $P_{PB}$ with the number of the power beacon’s transmit antennas $N_{PB} = 2$, $N_{PB} = 3$, $N_{PB} = 4$, and $N_{PB} = 5$, respectively.

In Figure 5.1, Figure 5.2, Figure 5.3, and Figure 5.4, the average secrecy rate of the half-duplex (HD) WPC system is also depicted for comparison. In the HD WPC system, the energy and information are simultaneously transmitted over different frequency bands, and the power beacon employs the maximum ratio transmission (MRT) to maximize harvested energy at the source. It is shown that the average secrecy rate increases as $P_{PB}$ increases whereas the average secrecy rate decreases as the normalized error bound $\alpha$ increases. It is shown that the FD WPC system achieves higher average secrecy rate than the HD WPC system for $\alpha = 0$, 0.2, and 0.6.

Figure 5.5, Figure 5.6, and Figure 5.7 show the average secrecy rate versus the normalized error bound $\alpha$ with the transmit power of the power beacon $P_{PB} = 10$ dB, $P_{PB} = 20$ dB, and $P_{PB} = 30$ dB, respectively. It is shown
that the average secrecy rate increases as \( N_{PB} \) increases whereas the average secrecy rate decreases as the \( \alpha \) increases.

Figure 5.8 and Figure 5.9 show the secrecy outage probability versus the transmit power \( P_{PB} \) with power beacon’s transmit antennas \( N_{PB} = 4 \), \( N_{PB} = 5 \), respectively. The secrecy outage probability is defined as \( P_{out} = \Pr(R_s \leq R_{th}) \), where \( R_{th} \) is a predefined threshold secrecy rate. It is shown that the secrecy outage probability decreases as \( P_{PB} \) increases and the secrecy outage probability decreases as the \( N_{PB} \) increases.
Figure 5.1. Average secrecy rate of FD/HD WPC system versus $P_{PB}$. $N_{PB} = 2$. 
Figure 5.2. Average secrecy rate of FD/HD WPC system versus $P_{PB}, N_{PB} = 3$. 
Figure 5.3. Average secrecy rate of FD/HD WPC system versus $P_{PB}$, $N_{PB} = 4$. 

---

31
Figure 5.4. Average secrecy rate of FD/HD WPC system versus $P_{PB}$, $N_{PB} = 5$. 
Figure 5.5. Average secrecy rate of FD WPC system versus $\alpha$, $P_{PB} = 10$ dB.
Figure 5.6. Average secrecy rate of FD WPC system versus $\alpha$, $P_{PB} = 20$ dB.
Figure 5.7. Average secrecy rate of FD WPC system versus $\alpha$, $P_{PB} = 30$ dB
Figure 5.8. Secrecy outage probability of FD WPC system versus $P_{PB}$, $N_{PB}=3$, $R_{th} = 2$ bps/Hz.
Figure 5.9. Secrecy outage probability of FD WPC system versus $P_{PB}$, $N_{PB}=5$, $R_{th}=2$ bps/Hz.
Chapter 6

Conclusion

In this thesis, we consider the full-duplex (FD) wireless powered communication (WPC) system in the presence of an eavesdropper. In chapter 1, we introduce the basic concept and related works of both the WPC and physical layer security. In addition, we describe the outline of this thesis. In chapter 2, we describe the system architecture of FD WPC and obtain the received SINR and the secrecy rate. In addition, we obtain the worst-case secrecy rate. In chapter 3, we formulate an optimization problem to obtain optimal
beamforming when the power beacon has imperfect channel state information (CSI) of the channel from the power beacon to the eavesdropper and that from the source to the eavesdropper. To solve the optimization problem, we divide the problem into two subproblems and solve them separately. In chapter 4, Simulation results show that the FD WPC system with optimal beamforming at the power beacon achieves higher secrecy rate than the half duplex WPC system with maximal ratio transmission at the power beacon. Also, it is shown that the secrecy rate decreases as the error of the imperfect CSI increases whereas the secrecy rate increases as the number of power beacon’s antennas increases.

Our proposed beamforming algorithm is optimal and useful. However, the proposed algorithm contains one-dimensional exhaustive search, which causes high complexity and overheads. To reduce the complexity, suboptimal beamforming scheme can also be developed. The suboptimal beamforming scheme may achieve lower complexity and communication overhead than optimal beamforming algorithm. The suboptimal beamforming scheme is our future work.
Bibliography


본 논문에서는 도청자가 존재하는 전이중 방식으로 작동하는 무선전력 통신에서 보안 통신을 위한 최적의 범 형성 기법을 제안한다. 전력 비콘은 에너지 신호를 범 형성을 통해 정보 송신단에 전송한다. 이때 에너지 신호는 도청자에게 재밍 신호의 역할을 한다. 최적의 범 형성을 설계하기 위한 최적화 문제를 제안하고 그 문제를 풀기 위한 알고리즘을 제시한다. 그리고 모의실험을 통하여 제안된 범 형성 방법을 적용했을 때 전이 중 방식의 무선전력통신의 보안 성능을 확인한다.

주요어: 무선전력통신, 보안 전송률, 에너지 범 형성, 전이중 통신, 에너지 하베스팅.

학번: 2015-20934.