Secure full-duplex two-way relaying for SWIPT

This item was submitted to Loughborough University's Institutional Repository by the/an author.


Additional Information:

- This is an Open Access Article. It is published by IEEE under the Creative Commons Attribution 3.0 Unported Licence (CC BY). Full details of this licence are available at: http://creativecommons.org/licenses/by/3.0/

Metadata Record: https://dspace.lboro.ac.uk/2134/28149

Version: Published

Publisher: IEEE

Rights: This work is made available according to the conditions of the Creative Commons Attribution 3.0 Unported (CC BY 3.0) licence. Full details of this licence are available at: http://creativecommons.org/licenses/by/3.0/

Please cite the published version.
Secure Full-Duplex Two-Way Relaying for SWIPT

Alexander A. Okandeji, Muhammad R. A. Khandaker, and Kai-Kit Wong

Abstract—This letter studies bi-directional secure information exchange in a simultaneous wireless information and power transfer system enabled by a full-duplex multiple-input multiple-output amplify-and-forward (AF) relay. The AF relay injects artificial noise (AN) in order to confuse the eavesdropper. Specifically, we assume a zeroforcing (ZF) solution constraint to eliminate the residual self-interference. As a consequence, we address the optimal joint design of the ZF matrix and the AN covariance matrix at the relay node as well as the transmit power at the sources. We propose an alternating algorithm utilizing semi-definite programming technique and 1-D searching to achieve the optimal solution. Simulation results are provided to demonstrate the effectiveness of the proposed algorithm.

Index Terms—Full-duplex, energy harvesting, relay, secrecy, physical layer security.

I. INTRODUCTION

WIRELESS communication networks are inherently susceptible to sophisticated eavesdropping attacks; however, full-duplex wireless operation is even more prone to overhearing due to continuous transmission and reception by the full-duplex nodes. Guaranteeing security in full-duplex communications is therefore a critical issue that needs to be addressed.

Recently, simultaneous wireless information and power transfer (SWIPT) [1], full-duplex (FD) enabled bi-directional wireless communications [2] as well as physical-layer (PHY) security [3] have each been a major research area and also led to efforts investigating the combination of these technologies. To name a few, for example, FD SWIPT has been considered in [4]. Also, PHY security in FD systems was addressed in [5] and [6]. In contrast to existing works, our main contribution is the study of the integration of all three and the joint optimization of the transmit power, the artificial noise (AN) covariance and the two-way relay beamforming matrix to maximize the secrecy sum-rate for SWIPT with a FD multiple-input multiple-output (MIMO) amplify-and-forward (AF) relay employing power splitter (PS). Specifically, the total transmit power is minimized while guaranteeing the signal to interference and noise ratio (SINR) constraints at the two legitimate users as well as the eavesdropper and the energy harvesting constraint at the relay.

Notations: We use $\mathbf{X} \in \mathbb{C}^{M \times N}$ to represent a complex $M \times N$ matrix. Also, $(\cdot)^\dagger$ denotes the conjugate transpose, $\text{trace}(\cdot)$ is the trace operation, and $\| \cdot \|$ denotes the Frobenius norm. In addition, $| \cdot |$ returns the absolute value of a scalar, and $\mathbf{X} \succeq 0$ denotes that the Hermitian matrix $\mathbf{X}$ is positive semidefinite. The expectation operator is denoted by $\mathbb{E} \{\cdot\}$.

II. SYSTEM MODEL

We consider SWIPT in a three-node MIMO relay network with nodes $\text{SA}$ and $\text{SB}$, equipped with one transmit and one receive antennas for information transmission and reception, respectively, exchanging confidential information with the aid of a multi-antenna AF relay $\text{R}$, in the presence of a single antenna eavesdropper $\text{E}$. We assume that: i) $\text{SA}$, $\text{SB}$ and $\text{R}$ all operate in FD mode, ii) there is no direct link between $\text{SA}$ and $\text{SB}$, iii) the harvested energy at the relay is used to complete the bi-directional information exchange [7], and iv) $\text{SA}$ and $\text{SB}$ are not aware of any eavesdropper thus, no direct link exist between $\text{SA}$ and $\text{SB}$ and the eavesdropper, as in [8]. The inclusion of the source-eavesdropper links can be handled in a similar manner. The relay, however, is aware of the eavesdropper. As a result, the relay injects AN signals to confuse the eavesdropper.

In the first phase, the relay receives confidential information from $\text{SA}$ and $\text{SB}$, while in the next phase, $\text{R}$ amplifies and forwards the processed information to both nodes with the AN signal being superimposed to jam the eavesdropper [8]. Using the transmit power $P_{\text{A}}$ and $P_{\text{R}}$, respectively, $\text{SA}$ and $\text{SB}$ transmit their confidential messages simultaneously to $\text{R}$. On the other hand, $\text{R}$ employs linear processing with amplification matrix $\mathbf{W}$ to process the received signal and broadcasts the processed signal to the nodes with harvested power $U$.

The antennas at $\text{R}$ are separated for transmission and reception with $M_{\text{T}}$ transmit antennas and $M_{\text{R}}$ receive antennas. Also, we denote $\mathbf{h}_{\text{RX}} \in \mathbb{C}^{M_{\text{R}} \times 1}$ and $\mathbf{h}_{\text{RR}} \in \mathbb{C}^{M_{\text{T}} \times 1}$ to, respectively, represent the directional channel vectors between the node $\mathbf{X} \in \{A, B\}$ and $\text{R}$. Similarly, we use $\mathbf{h}_{\text{RE}}$ to denote the channel between $\text{E}$ and $\text{R}$.

To achieve FD communication, self-interference (SI) must be significantly suppressed, as total cancellation is not possible as a result of imperfect channel estimation [4]. Therefore, we adopt the use of existing SI cancellation mechanisms (e.g., antenna isolation, digital and analog cancellation, etc.), to reduce the effect of SI. For convenience, we denote $h_{\text{AA}}$, $h_{\text{BB}}$, and $\mathbf{H}_{\text{RR}} \in \mathbb{C}^{M_{\text{T}} \times M_{\text{T}}}$ as the residual SI (RSI) channels at the respective nodes [4]. Also, the RSI channel is represented as a Gaussian distribution random variable with zero mean and variance $\sigma_X^2$, for $X \in \{A, B, R\}$ [4]. Furthermore, the relay,
assumed to be equipped with a PS device, coordinates information decoding and energy harvesting. Specifically, the relay splits the received signal power such that a $\rho \in (0, 1)$ portion of the received signal power is fed to the information receiver (IR) and the remaining $(1 - \rho)$ portion of the power is fed to the energy receiver (ER) at the relay.

A. Signal Model

The received signal $y_i[n]$ and the transmit signal $x_R[n]$ at $R$ at time instant $n$, can be written, respectively, as

$$y_i[n] = h_{ARS_A}[n] + h_{BRS_B}[n] + h_{RR}[n] + n[R][n],$$

$$x_R[n] = W[y_R] = [n] + [n][],$$

where $\tau$ is the processing delay to implement FD operation and assumed short enough to be neglected as far as the achievable rate computation is concerned, $n[R] \sim \mathcal{CN}(0, \sigma^2_n)$ is the additive white Gaussian noise (AWGN) at $R$, $z[n] \sim \mathcal{CN}(0, Q)$, with $Q \geq 0$, is the AN used for interfering $E$, and $y_E[n]$ is the signal split to the IR at $R$ given by

$$y_E[n] = \sqrt{\rho}(h_{ARS_A}[n] + h_{BRS_B}[n] + h_{RR}[n] + n[R][n]).$$

Thus, the signal transmitted by $R$ can then be expressed as

$$x_R[n] = \sqrt{\rho}W(h_{ARS_A}[n - \tau] + h_{BRS_B}[n - \tau]$$

$$+ h_{RR}[n - \tau] + n[R][n - \tau]) + z[n - \tau].$$

As shown in [9], the relay output can be further written as

$$x_R[n] = W[\sum_{j=0}^{\infty} (h_{RR}[j]W[j][h_{ARS_A}[n - j\tau] - \tau]$$

$$+ h_{BRS_B}[n - j\tau - \tau] + n[R][n - j\tau - \tau])$$

$$+ z[n - j\tau - \tau].$$

where $j$ denotes the index of the delayed symbols. We define the covariance matrix of (5) as

$$\mathbb{E}[x_R^t x_R] = \rho[PAW[\sum_{j=0}^{\infty} (h_{RR}[j]W[j])h_{ARS_A}^t[(h_{RR}[j]W[j])^tW^t$$

$$+ P_bw[\sum_{j=0}^{\infty} (h_{RR}[j]W[j])h_{BRS_B}^t[(h_{RR}[j]W[j])^tW^t$$

$$+ W[\sum_{j=0}^{\infty} (h_{RR}[j]W[j])h_{RR}^t[(h_{RR}[j]W[j])^tW^t + Q].$$

Clearly, the relay’s transmit covariance is indeed a complicated function of $W$. In this letter, we adopt the zero-forcing (ZF) solution constraint to cancel the RSI from the relay output to the relay input via the optimization of $W$ [4]. In particular, the ZF constraints may take the following forms [8]

$$WH_{RR} = 0, \quad \text{if } M_R > M_T,$$

$$H_{RR}W = 0, \quad \text{if } M_T > M_R.$$

For convenience, we only consider the case $M_T > M_R$ as the other case can be handled similarly. Thus, (5) becomes

$$x_R[n] = \sqrt{\rho}W(h_{ARS_A}[n - \tau] + h_{BRS_B}[n - \tau] + n[R][n - \tau]$$

$$+ z[n].$$

with the relay output power expressed as

$$P_R = \text{trace}(\mathbb{E}[x_R^t x_R])$$

$$= \rho[PA\|h_{ARS_A}\|^2 + P_B\|h_{BRS_B}\|^2 + \text{trace}(W^tW)]$$

$$+ \text{trace}(Q).$$

In the second time slot after cancelling the SI signal $s_A[n - \tau]$, the received signal at $S_A$ is given as

$$y_{SA}[n] = \sqrt{\rho}(h_{RA}^t \cdot h_{BRS_B} [n - \tau] + h_{RA}^t \cdot n[R][n])$$

$$+ h_{RA}^t \cdot z[n] + h_{ARS_A}[n] + n[R][n].$$

where $n[R][n]$ is the AWGN at node $S_A$. From this, we can work out the rates at $S_A$ and $S_B$ as

$$R_X = \log_2(1 + \Gamma_X), \quad \text{for } X \in \{A, B\},$$

where

$$\Gamma_A = \frac{\rho P_B||h_{RA}||^2}{\rho^2||h_{RA}||^2 + P_A||h_{AA}||^2 + h_{RA}^t \cdot Qh_{RA} + 1},$$

$$\Gamma_B = \frac{\rho P_A||h_{BB}||^2}{\rho^2||h_{BB}||^2 + P_B||h_{RR}||^2 + h_{RR}^t \cdot Qh_{RB} + 1}.$$

The achievable secrecy sum-rate is then defined as [8]

$$R_{sec} = [R_A + R_B - R_E]^t,$$

where $[x]^t$ represents max($x, 0$). The eavesdropper is a legitimate user for another service, hence perfect CSI is available. Meanwhile, the signal split to the ER at $R$ is given by

$$y_E[n] = \sqrt{\rho}(h_{ARS_A}[n] + h_{BRS_B}[n] + h_{RR}[n] + n[R][n]).$$

The harvested energy at the relay is thus given as [4]

$$U = \beta(1 - \rho)(\rho^2 \cdot P_A + \rho \cdot P_B + \bar{E} + \sigma^2_R M_R),$$

in which $\bar{E} = \mathbb{E}[x_R^t x_R]$ and $\beta$ denotes the energy conversion efficiency of the ER at the relay which is assumed unity.

B. Problem Statement

Due to the inherent SI at each FD node, the nodes may not use the maximum available transmit power in order not to increase the level of SI. Thus, there is a need to transmit at optimal values. Furthermore, it is known that optimal values of system parameters guarantees that the secrecy rate is as large as possible [8]. Thus, in this letter, our aim is to maximize the secrecy sum-rate for SWIPT by ensuring that system parameters are optimal. We achieve this by jointly optimizing the transmit power $(P_A, P_B)$ at nodes $S_A$ and $S_B$, the
relaying matrix \((W)\) and the AN covariance matrix \((Q)\) at the relay. Thus, we have

\[
\min_{\rho \in \mathbb{C}, W \in \mathbb{C}^{M_T \times M_T}} P_A + P_B + P_R \quad \text{s.t.} \quad \Gamma_A \geq \gamma_A, \quad \Gamma_B \geq \gamma_B, \quad \Gamma_E \leq \gamma_E, \\
(1 - \rho) \left( |h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} + \sigma_R^2 M_R \right) \geq \hat{U},
\]

where \(\gamma_A, \gamma_B, \gamma_E\) and \(\hat{U}\) are respective QoS threshold. Note that the second constraint guarantees that the energy receiver circuit can harvest sufficient energy such that the relay can successfully forward the received signals.

### III. PROPOSED SCHEME

#### A. Optimization of \(W\) and \(Q\) at the Relay

Here, we study the optimal beamforming matrix and the AN covariance matrix assuming the transmit power \((P_A, P_B)\) and the PS ratio \((\rho)\) all being fixed. For convenience, we define \(W = N_W V\), where \(N_W \in \mathbb{C}^{M_T \times M_T}\) represents the null space of \(H_{RR}\), and \(V \in \mathbb{C}^{M_T \times M_T}\) is the new optimization variable. As a consequence, the optimization of \(W\) reduces to optimizing \(V\). Hence, we remove the ZF constraint in (18) and obtain the equivalent optimization problem:

\[
\min_{V, Q \geq 0} P_R \quad \text{s.t.} \quad \left\{ \begin{array}{l}
\Gamma_A \geq \gamma_A, \quad \Gamma_B \geq \gamma_B, \quad \Gamma_E \leq \gamma_E, \\
(1 - \rho)(|h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} + \sigma_R^2 M_R) \geq \hat{U}.
\end{array} \right.
\]

Problem (19) is a nonconvex problem due to the coupled optimization variables in the constraints. However, by rearranging the terms in the constraints, (19) can be re-expressed as

\[
\min_{V, Q \geq 0} P_R
\]

\[
\begin{align*}
&\frac{1}{\gamma_A} P_B C_{RB} h_{BR}^\dagger \Sigma h_{BB} - \sigma_R^2 C_N h_{RA}^\dagger \Sigma h_{RA} \\
&\quad \geq \frac{1}{\rho} (P_A |h_{AA}|^2 + h_{RA}^\dagger Q h_{RA} + 1), \\
&\frac{1}{\gamma_B} P_A C_{RB} h_{AR}^\dagger \Sigma h_{AR} - \sigma_R^2 C_N h_{RB}^\dagger \Sigma h_{RB} \\
&\quad \geq \frac{1}{\rho} (P_B |h_{BB}|^2 + h_{RB}^\dagger Q h_{RB} + 1), \\
&\frac{1}{\gamma_E} \left[ P_A C_{EE} h_{AR}^\dagger \Sigma h_{AR} + P_B C_{EE} h_{BR}^\dagger \Sigma h_{BB} \right] - \sigma_R^2 C_N h_{RE}^\dagger \Sigma h_{RE} \\
&\quad \leq \frac{1}{\rho} (h_{RE}^\dagger Q h_{RE} + 1), \\
|h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} &\geq \frac{U}{1 - \rho} - \sigma_R^2 M_R.
\end{align*}
\]

where \(\Sigma = V V^\dagger, C_A = |N_W h_{RA}|^2, C_N = \text{trace}(N_W N_W^\dagger), C_B = |N_W h_{RB}|^2\) and \(C_{EE} = |N_W h_{RE}|^2\). Problem (20) can be efficiently solved by existing solvers such as CVX. Once the optimal \(\Sigma\) is obtained, optimal \(V\) can be constructed through matrix decomposition.

#### B. Optimization of the PS Coefficient \((\rho)\)

For fixed values of the relay beamforming matrix \((W)\), AN covariance \((Q)\) and for given values of the transmit power \((P_A, P_B)\), (18) can be reformulated as

\[
\min_{\rho \in \mathbb{C}, \rho \geq 0} P_A + P_B + P_R \quad \text{s.t.} \quad \begin{align*}
\rho P_B |h_{RA}^\dagger W h_{BR}|^2 &\geq \gamma_A, \\
\rho |h_{RA}^\dagger W|^2 + P_A |h_{AA}|^2 + h_{RA}^\dagger Q h_{RA} + 1 &\geq \gamma_B, \\
\rho P_A |h_{RB}^\dagger W h_{BR}|^2 &\geq \gamma_B, \\
\rho |h_{RB}^\dagger W|^2 + P_B |h_{BB}|^2 + h_{RB}^\dagger Q h_{RB} + 1 &\leq \gamma_B, \\
(1 - \rho)(|h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} + \sigma_R^2 M_R) &\geq \hat{U},
\end{align*}
\]

which can be expressed in a form solvable by existing solvers by rearranging the terms in the constraints as

\[
\begin{align*}
\min_{\rho \in \mathbb{C}, \rho \geq 0} P_A + P_B + P_R &\quad \text{s.t.} \quad \begin{align*}
\rho P_B |h_{RA}^\dagger W h_{BR}|^2 &\geq \gamma_A, \\
\rho |h_{RA}^\dagger W|^2 + P_A |h_{AA}|^2 + h_{RA}^\dagger Q h_{RA} + 1 &\geq \gamma_B, \\
\rho P_A |h_{RB}^\dagger W h_{BR}|^2 &\geq \gamma_B, \\
\rho |h_{RB}^\dagger W|^2 + P_B |h_{BB}|^2 + h_{RB}^\dagger Q h_{RB} + 1 &\leq \gamma_B, \\
(1 - \rho)(|h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} + \sigma_R^2 M_R) &\geq \hat{U}.
\end{align*}
\end{align*}
\]

#### C. Optimization of the Source Power \((P_A, P_B)\)

For given values of the relay beamforming matrix \((W)\), AN covariance matrix \((Q)\) and the PS ratio, problem (18) can be written as

\[
\min_{P_A, P_B} P_A + P_B + P_R \quad \text{s.t.} \quad \begin{align*}
\rho P_B |h_{RA}^\dagger W h_{BR}|^2 &\geq \gamma_A, \\
\rho |h_{RA}^\dagger W|^2 + P_A |h_{AA}|^2 + h_{RA}^\dagger Q h_{RA} + 1 &\geq \gamma_B, \\
\rho P_A |h_{RB}^\dagger W h_{BR}|^2 &\geq \gamma_B, \\
\rho |h_{RB}^\dagger W|^2 + P_B |h_{BB}|^2 + h_{RB}^\dagger Q h_{RB} + 1 &\leq \gamma_B, \\
q |h_{AR}|^2 P_A + |h_{BR}|^2 P_B + \bar{E} + \sigma_R^2 M_R &\leq \hat{U}.
\end{align*}
\]

It is worth noting that full-duplexity in communication systems is preceded by successful SI cancellation. In our model, both \(S_A\) and \(S_B\) are equipped with a single transmitter-receiver pair for signal transmission and reception, respectively. As a result, it is impossible to cancel the SI in the spatial domain [4]. The relay, in contrast, equipped with at least two transmitter-receiver pairs, can cancel the generated SI in the spatial domain. We proceed to investigate the optimal power solution \((P_A, P_B)\) assuming \(W, Q\) and \(\rho\) all being fixed. Evidently, it is easy to check that at the optimum, either \(S_A\) or \(S_B\) will be transmitting with maximum power [4], i.e., \(P_A = P_{\text{max}}\) or \(P_B = P_{\text{max}}\). As a consequence, we can relax (23) into two subproblems with: (i) \(P_A = P_{\text{max}}\), (ii) \(P_B = P_{\text{max}}\). Considering the symmetric nature of case (i) and case (ii), we study case (i) as
is thus reformulated as

\[ \min_{P_B} P_B + \bar{P}_R \quad \text{s.t.} \]

\[ \rho P_B |h_{RA}^T W h_{BR}|^2 \geq \gamma_A, \quad (24a) \]

\[ \rho P_{max} |h_{RR}^T W h_{AR}|^2 \geq \gamma_B, \quad (24b) \]

\[ \rho P_{max} |h_{RE}^T W h_{AR}|^2 \geq \gamma_E, \quad (24c) \]

\[ (1 - \rho)|h_{AR}|^2 P_{max} + |h_{BR}|^2 P_B + |h_{RE}|^2 \rho h_{RB} Q_{hR} + 1 \geq \tilde{U}, \quad (24d) \]

0 < P_B \leq P_{max}, \quad (24e)

where \( P_R = \rho P_{max} |W h_{BR}|^2 + P_B |W h_{AB}|^2 + \text{trace}(W W^*) + \text{trace}(Q) \). Since 0 < \( P_B \leq P_{max} \), we can obtain the feasible range \( P_{min} \leq P_{max} \) for \( P_B \). Also, the constraints in (24) can be analyzed with respect to \( P_R \):

1) A continuous increase in \( P_R \) is required to guarantee that (24b) remains satisfied. As a consequence, we can set the minimum of \( P_B \) as \( P_{min} \).

2) Constraint (24c) is a decreasing function of \( P_B \). Therefore, the minimum \( P_B \) satisfying (24c) to equality is defined as \( P_{max} \).

3) An upper bound of the eavesdropping constraint in (24d) is satisfied when \( P_B \leq P_{min} \).

4) A lower bound of the energy harvesting constraint in (24e) is guaranteed to be satisfied when \( P_B \geq P_{min} \).

The optimal \( P_B \) is chosen between \( P_{min} \) and \( P_{max} \) which satisfies (24b)-24e). Accordingly, to obtain the optimal \( P_B \), we perform a 1-D search over \( P_B \) starting from \( P_{min} \) until \( P_{max} \) is reached to find a feasible solution to problem (24). Clearly, if \( P_{min} > P_{max} \) then (24) becomes infeasible.

Thus problem (18) is solved in an alternating manner.

IV. SIMULATION RESULTS

In this section, we consider Rayleigh flat fading channels for computer simulations. The results are averaged over 1000 channel realizations with \( \gamma_A = -5 \) (dB), \( \gamma_B = -5 \) (dB), \( \gamma_E = -15 \) (dB). We also assume that 60% of the SI at node A and node B has been eliminated through digital cancellation [4].

In Fig. 1, we investigate the secrecy sum-rate for SWIPT in FD systems versus the transmit power budget \( P_{max} \) (dB) for different values of the harvested power constraint. We study the performance of the proposed scheme (denoted ‘Joint Opt.’ in the figure) in comparison with the relay-only optimization scheme (denoted ‘Relay Only Opt.’). We see that the proposed scheme yields a higher secrecy sum-rate than the relay-only optimization scheme. Also, it can be observed that the secrecy sum-rate increases with \( P_{max} \) to a certain level after which it begins to experience a decrease with a continuous increase in \( P_{max} \), due to the increase of RSI [10].

In Fig. 2, we further study the secrecy sum-rate performance against the RSI for different values of the harvested power constraints. Evidently, as RSI increases, a corresponding decrease in the secrecy sum-rate is observed. However, the proposed scheme yields higher secrecy sum-rate compared to the secrecy sum-rate of the relay-only optimization scheme for different values of the harvested energy constraint. Hence, the need for joint optimization is justified.

Note from Fig. 1 and 2, as the harvested energy threshold increases, more power is directed to the ER of the relay. The result is a corresponding decline in the achievable secrecy rate.

V. CONCLUSION

This letter investigated the joint optimization of the transmit power, AN covariance matrix, and the relay beamforming matrix for SWIPT in FD AF relay systems in the presence of an eavesdropper. Specifically, using SDP and 1-D searching, we proposed an algorithm that minimizes the total transmit power for secure SWIPT in a FD MIMO AF relay system.

REFERENCES


