Secure beamforming design of SWIPT relay network with multiple users and eavesdroppers

Lu He¹, Taoshen Li¹,², Baber¹, Zhe Wang¹,³, Mingyu Lu¹, Anni Shi¹, Qing Zhu¹

¹College of Computer Electronic and Information, Guangxi University, Nanning 530004
²School of Information Engineering, Nanning University, Nanning 530004
³School of Artificial Intelligence, Guangxi University for Nationalities, Nanning 530004

*Corresponding author: tshli@gxu.edu.cn

Abstract. This paper studies the secure beamforming design for simultaneous wireless information and power transfer (SWIPT) in an amplify-and-forward (AF) relay networks with multiple users and eavesdroppers. Each user node adopts the power splitting (PS) scheme to decode information and harvest energy simultaneously. Our objective is to minimize the total relay transmit power under the constraints of secure transmission rate and energy harvesting requirements by jointly optimizing the beamforming matrix, artificial noise covariance matrix and PS ratios. For this non-convex problem, we propose a two-stage optimization approach to convert the original problem into two sub-problems. The first subproblem uses semidefinite relaxation (SDR) technique to transform the original problem into a convex problem, and then finds the optimal solution of the second subproblem through k-dimensional exhaustive search algorithm. Furthermore, we also propose a low complexity suboptimal solution scheme based on particle swarm optimization (PSO) algorithm. Simulation results show that the proposed scheme saves transmitting power and achieves better performance than other schemes.

1. Introduction

The life span of traditional wireless devices is limited by the power supply capacity, simultaneous wireless information and power transfer (SWIPT) technology can solve the energy scarcity problem in energy-constrained wireless networks by harvesting the energy of radio frequency (RF) signals into wireless devices, which is widely regarded as a promising technology [1]-[4]. Compared with 4G networks, 5G energy consumption will increase exponentially, and energy efficiency has become one of its key indicators, therefore, SWIPT technology is of great significance for 5G [5]. In recent years, this technology has attracted widespread attention and intense research [6]. In general, SWIPT has two primary energy harvesting schemes, namely, time switching (TS) and power splitting (PS) [7]-[9]. For the TS, the user node switches between information decoding (ID) and energy harvesting (EH) while with PS, the user node splits the received signal into two parts for ID and EH. It has been shown in [8] that the TS scheme switches between the two modes instantaneously, which can be regarded as a special case of the PS scheme. So, the performance of the PS scheme is usually better than the TS scheme. In this paper, we focus on the PS scheme.

The wireless information in SWIPT systems is more vulnerable to eavesdropping than other wireless networks due to the inherent characteristics of SWIPT and the open nature of wireless channel.
Therefore, how to achieve secure communication in the SWIPT wireless network is a crucial issue. Although the cryptographic technology guarantees the communication security of the application layer to a certain extent, it might not be suitable in the SWIPT system because the SWIPT system requires sophisticated encryption, decryption algorithms and critical distribution protocols [10]. Fortunately, this problem can be solved at the physical layer by using the physical characteristics of wireless channels, such as channel fading [11] and interference [12], especially the design of beamforming and artificial noise (AN) [13] has become two key technologies to ensure the secure transmission of wireless communication.

In recent years, security of SWIPT network physical layer has attracted wide attention of researchers. In [14]-[15], the authors proposed a secure transmission scheme based on zero forcing (ZF) technology. A problem of maximizing the secrecy rate in a multi-input single-output (MISO) SWIPT system is described in [14], and the author in [15] considered the secure transmission scheme of two-user SWIPT cooperative zero forcing interference. However, the research models are all in simple scenes, and in the face of complex comprehensive network, zero-forcing interference cannot play its role significantly. Besides, in [16], a amplify-and-forward (AF) beamforming was designed to maximize the secrecy rate in full duplex wireless-powered relay network. But the model only considers simple scenarios, without the general scenario with multiple eavesdroppers. Therefore, we consider a more general model with multiple eavesdropping nodes and multiple user nodes in this paper.

In addition, in [17], the author studies the physical security in more complex MISO-SWIPT relay model by considering the dual-function nodes capable of information decoding and energy collection. The signal sent by the base station is forwarded to the user node through multiple single-antenna relay nodes. Although multiple user nodes and multiple eavesdropping nodes are considered, the author’s relay system is composed of multiple single-antenna relays. However, as one of the key technologies of LTE, multi-antenna technology can greatly improve system capacity and link reliability, and it has been widely used [18].

Based on the above research, in this paper, we consider the secure beamforming design of SWIPT multi-antenna AF relay system with multiple eavesdropping nodes and multiple user nodes. Each user node adopts the PS scheme to decode information and harvest energy simultaneously. At the same time, AN is also added in the relay to confuse these eavesdropping nodes. We study the joint design of beamforming matrix, AN covariance and PS ratios to minimize the relay transmission power under the constraints of secure transmission rate and energy harvesting requirements. The main contributions of this paper are summarized as follows:

1) We study the physical layer security of SWIPT relay networks with multiple eavesdropping nodes and multi-users, and propose a joint AF beamforming and AN scheme to interfere with the eavesdropping nodes to ensure secure transmission;

2) Unlike traditional networks, user nodes use PS schemes for information decoding and energy collection, and by jointly optimizing beamforming, AN, and PS ratios, the total transmission power of the relay network is saved;

3) We propose a robust secure beamforming design, use a two-stage optimization method and semidefinite relaxation technique to solve the original non-convex problem. Moreover, we also propose a low complexity suboptimal solution scheme based on particle swarm optimization (PSO) algorithm to provide secure transmission and promote effective energy harvesting.

2. System Model and Problem Formulations
As illustrated in figure 1, we consider a SWIPT relay system with a source $S$, an AF relay $R$, K user nodes $U$, and L eavesdropping nodes $E$, where the AF relay is equipped with M receive antennas and M transmit antennas. Let $f \in \mathbb{C}^{M \times 1}$, $h_u \in \mathbb{C}^{M \times 1}$, $g_e \in \mathbb{C}^{M \times 1}$ denote the channel vector from the $S$ to the $R$, from the $R$ to the $k$th $U$ and the $l$th $E$, respectively. Each user node adopts the PS scheme to ID and EH. The signal attenuation from the relay to the user, and the eavesdropping node is the same, and the line-of-sight (LOS) is dominant for this short-distance attenuation case [10], hence we assume that the channel is an independent Rician fading channel, and channel coefficients will not change until next
time slot. Similar to the design in [17], we assume that the eavesdropping nodes are closer to the user nodes, and there is no direct link from the source node to the user nodes and the eavesdropping nodes, which requires long-distance forwarding through the relay. Hence, information leakage occurs in the relay forwarding stage. Since the AF relay works in half-duplex mode, one transmission cycle consists of two phases.

\[
y_r = fs + n_r
\]

where \( s \in \mathbb{C} \) is the confidential message sent by the source node, \( E(|s|^2) = P_s \), \( E(\cdot) \) means mathematical expectation; \( n_r \sim CN(0, \sigma_n^2 I_{m}) \) represents the additive white Gaussian noise introduced by the relay.

In the second phase, the relay employs the beamforming matrix \( \mathbf{W} \in \mathbb{C}^{M \times M} \) to forward the information. In the meantime, the relay emits artificial noise \( \mathbf{v} \in \mathbb{C}^{M \times 1} \) obeying \( \mathbf{v} \sim CN(0, \Sigma_v) \) with \( \Sigma_v = \mathbf{v} \mathbf{v}^H \succeq 0 \) [19] to confuse the \( E_s \) as well as improve energy harvesting at the \( U_s \). Therefore, the transmission signal of the relay can be expressed as

\[
x_r = \mathbf{y}_r + \mathbf{v}
\]

Since the relay processing information delay is minimal, it can be ignored. The power transmitted by the relay node can be expressed as

\[
E_r = P_s Tr(\mathbf{W}f f^H) + \sigma_v^2 Tr(\mathbf{W} \mathbf{W}^H) + Tr(\Sigma_v)
\]

In the remainder of this paper, we use index \( k = \{1, \ldots, K\} \), \( l = \{1, \ldots, L\} \) to denote the index set of \( U_s \) and \( E_s \). Thus, the signals received by the \( k \)th user and the \( l \)th eavesdropper are expressed as

\[
y_{uk} = h_k^H \mathbf{W}(fs + n_r) + h_k^H \mathbf{v} + n_{uk}, \forall k
\]

\[
y_{el} = g_l^H \mathbf{W}(fs + n_r) + g_l^H \mathbf{v} + n_{el}, \forall l
\]

Where \( n_{uk} \sim CN(0, \sigma_{uk}^2 I_{m}), n_{el} \sim CN(0, \sigma_{el}^2 I_{m}) \) denote the additive white Gaussian noise introduced by the \( k \)th user and the \( l \)th eavesdropping node, respectively.

We assume that each user node is equipped with a power splitter to decode information and harvest energy. Specifically, at the \( k \)th user node, \( \rho_k \in (0,1) \) portion signal is used for information decoding, and \((1-\rho_k) \) portion of the signal is used for energy harvesting [8]-[9]. Thus, after PS, the equivalent received signals of the \( k \)th user for information decoding and energy harvesting are expressed as

\[
y_{uk}^{ID} = \sqrt{\rho_k}(h_k^H \mathbf{W}(fs + n_r) + h_k^H \mathbf{v} + n_{uk}) + n_{uk}, \forall k
\]
\[ y_{sk}^{HH} = \sqrt{(1-\rho_s)}(h_k^s W(f s + n_k) + h_k^s v + n_{sk}), \forall k \]

Where \( n_k \sim CN(0, \sigma_k^2) \) denote the noise added by the kth user node during signal processing. Therefore, the signal-interference to noise (SINR) of the kth user node is expressed as

\[ \text{SINR}_{sk} = \frac{P_k \rho_k^2 \sigma_k^2}{\rho_k^2 \sigma_k^2 + \rho_k^2 \text{Tr}(h_k^s h_k^s V) + \rho_k^2 \sigma_k^2 + \sigma_k^2}, \forall k \]

On the other hand, the energy harvested by kth user node is expressed as

\[ E_k = \eta (1 - \rho_k) (P_k h_k^H W f W h_k^H + \sigma_k^2 h_k^H W W h_k^H + \text{Tr}(h_k^H h_k^H V) + \sigma_k^2), \forall k \]

Where \( \eta \in (0,1) \) denotes the energy harvesting efficiency. In addition, the SINR of the lth eavesdropping node is expressed as

\[ \text{SINR}_{el} = \frac{P_k g_k^H W f W g_k^H}{\sigma_k^2 g_k^H W W g_k^H + \text{Tr}(g_k^H g_k^H V) + \sigma_k^2} \]

we consider communication security from the perspective of individual confidentiality. According to [20]-[21], an individual achievable security rate of the kth user can be expressed as

\[ R_k = \left[ \log_2 (1 + \text{SINR}_{sk}) - \log_2 (1 + \max_{\mu_k} \{\text{SINR}_{sk}\}) \right]^+ \]

Where \( [x]^+ = \max(0, x) \)

Our objective is to minimize the total power consumption at the AF relay while maintaining the achievable secrecy rate and energy harvesting constraints at each user node. Specifically, the power minimization problem can be formulated as

\[ \min_{P_k, \rho_k} P_k \text{Tr}(W f W h_k^H) + \sigma_k^2 \text{Tr}(W W h_k^H) + \text{Tr}(V) \]

\[ \text{s.t. } R_k \geq r_k, E_k \geq e_k, 0 < \rho_k < 1, \forall k \in K \]

\[ V \succeq 0 \]

Where \( r_k \) and \( e_k \) are the secure transmission rate and energy harvesting of the kth user, respectively. Since the optimization variables \( V, W, \rho_k \) are coupled in the optimization problem formula, and the constraints involve quadratic terms, the problem (12) is non-convex, making it difficult to solve.

3. Secure Beamforming Design

In this section, we propose a two-stage optimization method to transform the original problem into two sub-problems to solve the global optimization of problem (12). The first non-convex sub-problem is solved by semidefinite relaxation (SDR) technique, and then the optimal solution of the second sub-problem is sought by K-dimensional exhaustive search. Furthermore, facing the extremely high complexity of K-dimensional exhaustive search algorithm, we propose a PSO-based low-complexity algorithm to solve the original problem.

3.1. Two-stage optimization method

In this subsection, we develop a two-stage optimization method to deal with the problem (12). First, denote \( \bar{s} = \{W, V, \overline{\rho_k}\} \) as the optimal solution of problem (12), and define

\[ \bar{\mu}_k = \frac{P_k \rho_k h_k^H W f W h_k}{\rho_k^2 \sigma_k^2 h_k^H W W h_k + \rho_k^2 \text{Tr}(h_k^H h_k^H V) + \rho_k^2 \sigma_k^2 + \sigma_k^2}, \forall k \]

Then \( \bar{s} \) is also the optimal set to the following problem (13) with \( \mu_k = \bar{\mu}_k, \forall k \)
\[
\min_{W,V,\rho} P_{\Delta}\text{Tr}(W^{\mu}W^H) + \sigma_i^2\text{Tr}(WW^H) + \text{Tr}(V)
\]

\[
\text{s.t.} \quad \frac{P_{\Delta}g^H(W^{\mu}W^H)g_i}{\sigma_i^2g^HWW^Hg_i + \text{Tr}(g^Hg_i)V} \leq \mu^l_i, \forall l
\]

\[
\frac{P_{\Delta}\rho_k h^H(W^{\mu}W^H)h_k}{\rho_k\sigma_i^2h^HWW^Hh_i + \rho_k\text{Tr}(h^HH^HV)} + \frac{\rho_k\sigma_i^2 + \sigma_i^2}{\mu_k} \geq \mu_k, \forall k
\]

\[
\eta(1-\rho_k)(P_{\Delta}h^H(W^{\mu}W^H)h_k + \sigma_i^2h^HWW^Hh_i + \text{Tr}(h^HH^HV) + \sigma_i^2) \geq e_i, \forall k
\]

\[
V \succeq 0, 0 < \rho_k < 1, \forall k
\]

where \(\mu^l_i = \frac{\mu_k}{2^{\rho_k}} - 1\).

For a given set of \(\mu_i\), denote the optimal objective function value of problem (13) as \(f(\mu_1, \ldots, \mu_k)\). Then, problem (12) is equivalent to the following problem (14)

\[
\min_{(\mu_1, \ldots, \mu_k) \in \{1, \ldots, \mu_k\}} f(\mu_1, \ldots, \mu_k)
\]

Let \(\mu^*\) denote the optimal solution of problem (14), problem (12) and problem (13) have the same solution with \(\mu_k = \mu^*, \forall k\). Hence, the problem (12) can be solved equivalently in the following two stage: first, for a given \(\mu_k\), solve the problem (13) to obtain the optimal objective function value \(f(\mu_1, \ldots, \mu_k)\), then, through K-dimensional exhaustive search all possible combinations of \(\mu_k\) to find the optimal \(\mu^*\), thereby solving the problem (14). Therefore, we will solve problem (13) for a fixed set of \(\mu_k\) at first in the following.

### 3.2. SDR-based optimal solution for problems (13)

For a given \(\mu_k\), problem (13) is also a non-convex problem. In this paper, SDR technology will be used to deal with this non-convex problem. First, according to the identity formula \(\text{Tr}(B^H(CDE)) = \text{vec}(B^H(E^T \otimes C) \text{vec}(D))\) and the formula \(\text{Tr}(BC) = \text{Tr}(CB)\), convert equation (12) to the following equation (15)

\[
\min_{a, V, \rho} a^H Ba + \text{Tr}(V)
\]

\[
\text{s.t.} \quad \frac{a^H C_{1,k} a}{\sigma_i^2a^H C_{2,k} a + g^H V g + \sigma_i^2} \leq \mu^l_i, \forall l
\]

\[
\frac{\rho_k a^H D_{2,k} a}{\rho_k \sigma_i^2 a^H D_{2,k} a + \rho_k h^H V h + \rho_k \sigma_i^2 + \sigma_i^2} \geq \mu_k, \forall k
\]

\[
\eta(1-\rho_k)(a^H D_{1,k} a + \sigma_i^2 a^H D_{2,k} a + h^H V h + \sigma_i^2) \geq e_i, \forall k
\]

\[
V \succeq 0, 0 < \rho_k < 1, \forall k
\]

Where \(a = \text{vec}(W)\); \(\text{vec}(\bullet)\) denote the column vectorization operation of a matrix \(B = (P_{\Delta}f^T + \sigma_i^2I_N) \otimes I_N\); \(C_{1,k} = P_{\Delta}(f^T \otimes (g_i^H))\); \(C_{2,k} = I_N \otimes (g_i^H)\); \(D_{1,k} = P_{\Delta}(f^T \otimes (h_i^H))\); \(D_{2,k} = I_N \otimes (h_i^H)\).

According to the idea of SDR technology in [19], we define \(A = aa^H\) with \(\text{rank}(A) = 1\). As a standard routine of SDR, we drop the rank-one constraint and recast problem (15) as
Problem (16) is a convex semidefinite programming problem that can be solved using standard optimization software packages, such as CVX [22]. Notably, though, the problem (14) can be solved directly by k-dimensional exhaustive search for all possible combinations of $\mu_k$, $\forall k$, but the complexity of k-dimensional exhaustive search is too high to be implemented in practice. Therefore, in the next section, we propose a low complexity heuristic algorithm based on PSO to solve this problem (14).

3.3. SDR-based optimal solution for problem (14)

The PSO algorithm has been widely used in the field of wireless communication due to its advantages of simple implementation, high solution quality, and fast convergence speed [23]. In this paper, PSO algorithm first randomly generates a group of particles $\{x[i][n]\}$ in $U_4$, where $S$ is the swarm size and $n$ is the iterations index. The algorithm solves the problem (16) to calculate the fitness value corresponding to each particle $x[i][n]$. Then, find the position of the particle $x[i][n]$ corresponding to the best fitness value (global optimal) of the entire population in each iteration, expressed as $\mathbf{G}_i x[i][n]$. In addition, remember the best position of each previous particle (previous optimal), expressed as $\mathbf{P}_i x[i][n]$. After finding these two optimal values, the algorithm updates the velocity and position of the $i$th particle in each iteration according to following equation

$$v[i]^{(n+1)} = \omega v[i]^{(n)} + c_1 \varphi_1 (\mathbf{P}_i x[i][n] - x[i][n]) + c_2 \varphi_2 (\mathbf{G}_i x[i][n] - x[i][n])$$

(17)

$$x[i]^{(n+1)} = x[i][n] + v[i]^{(n+1)}$$

(18)

Where $\omega$ is the inertia weight, $c_1$ and $c_2$ are two constant accelerations, $\varphi_1$ and $\varphi_2$ are random numbers uniformly distributed in [0, 1]. This process is repeated until the termination condition is satisfied or the maximum number of iterations is reached. The details are summarized in Algorithm 1.

Algorithm 1 PSO-Based Algorithm with Python for Problem (14)

1. Initialize: $n=0, N, \{x[i][n]\}, \{v[i][n]\}, \omega, c_1, c_2$
2. while $n \leq N$ or the particle swarm does not converge:
3. for i in range (S):
4. temp = the optimal value of problem (15)
5. if temp $< P_{fit}^{(n)}$
6. $P_{fit}^{(n)} = temp$ : $\mathbf{P}_i x[i][n] = x[i][n]$
7. if $P_{fit}^{(n)} < G_{fit}^{(n)}$
8. $G_{fit}^{(n)} = x[i][n]$ : $G_{fit}^{(n)} = P_{fit}^{(n)}$
9. for i in range (S):
10. Update the $v[i][n]$ and $x[i][n]$ according to formula (17) and (18)
11. return $G_{fit}^{(n)}, G_{fit}^{(n)}$
The computational complexity of Algorithm 1 is mainly based on the swarm size $S$, the maximum number of iterations $N$, and the complexity in evaluating the fitness value in problem (16), which has the computational complexity of $O(\sqrt{KM^3M^6} + \sqrt{KM^2L^4M^4})$. Therefore, the complexity of Algorithm 1 is $O(S(\sqrt{KM^3M^6} + \sqrt{LM^2L^4M^4}))$, while compared with K-dimensional exhaustive search, this algorithm greatly reduces the complexity significantly.

4. Simulation Results
In this section, numerical simulation is presented to evaluate the performance of the proposed scheme in SWIPT multi-antenna relay system. The simulation experiment parameters are set as follows: $P_d = 10dB, M = 3, \eta = 0.8, \sigma_r^2 = \sigma_{ak}^2 = \sigma_{il}^2 = -50dB, \sigma_{ak}^2 = -70dB, r_k = r_l, e_k = e_l, \forall k, \forall l$. Moreover, we set PSO parameters $\omega = c_1 = c_2 = 2, U_k = U = \left[2^{(u)} - 1, 2^{(u+1)}\right]$. In addition, to highlight the superiority of the proposed scheme, we compare with three baseline methods: 1) No-AN scheme: $V = 0$ by only optimizes $W$ and $\rho_l$; 2) zero forcing (ZF)-based scheme in [14]-[15]: choosing the beamforming vector $W$ to lie in the null space of a matrix composed by eavesdropping nodes; 3) fixed $\rho_l$ scheme: fixed power split ratio, e.g., $\rho_l = 0.5$ by only optimizes $W$ and $V$ in (15).

![Figure 2. PSO algorithm convergence](image)

![Figure 3. The relay transmit power versus the secrecy rate $r_0$](image)

Figure 2 demonstrates the convergence behavior of the proposed algorithm on several random channels. Where $K = 3, L = 2, e_o = -10dBm, r_0 = 5b/s/Hz$. It can be observed that the algorithm only needs about four iterations to achieve convergence, which shows that the algorithm has fast convergence and therefore has low computational complexity.

Figure 3 depicts the relay transmit power of four different schemes versus the minimum secrecy rate requirement of each user node with $K = 3, L = 2, e_o = -10dBm$. It is clear to see that the relay transmit power increases as the secrecy rate requirement increases. Our proposed method is superior to other schemes while the No-AN scheme is the worst design. This phenomenon indicates that AN is conducive to a SWIPT system. Besides, it can be seen from the figure that when the security rate is small, the relay transmit power increases slowly, whereas when the security rate is large, the relay total transmission power rises quickly.
Figure 4 illustrates relay transmit power versus the harvested energy threshold of each user node with $K = 3, L = 2, r_s = 5b/s/HZ$. It is observed from the figure that the relay transmit power increases with the increase of $e_0$, and the scheme proposed in this paper achieves better performance than other schemes.

Figure 5 shows the relay transmit power versus the number of eavesdropping node $L$. It is clear to see that the relay transmission power consumption of all schemes increases with the increase of the number of eavesdropping nodes $L$, and our proposed design has a better performance gain than other schemes. Moreover, it can be seen from the figure that when $K \geq 5$, the zero-forcing scheme is significantly increased, which further indicates that the number of eavesdropping nodes $L$ has a significant influence on the performance of the zero-forcing system.

5. CONCLUSION

In this paper, the security of multiple user nodes and multiple eavesdropping nodes in a multi-antenna AF relay network based on SWIPT is studied. This paper proposed an artificial noise-assisted secure beamforming design. Under the constraints of secrecy rate and energy harvesting, the goal of minimizing the total transmission power of the relay system is achieved by jointly optimizing the beamforming matrix, AN covariance and PS ratios. The two-stage optimization method and semidefinite relaxation technique are used to solve the optimal solution of the original problem. In this paper, it shows that a $k$-dimensional exhaustive search is difficult to achieve. Hence, a low complexity suboptimal solution based on the PSO algorithm is proposed. Simulation results show that the proposed scheme saves transmission power and has better performance than other scheme while ensuring a secure transmission rate.

References

[1] Zhang R and Ho C K 2013 MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer IEEE Trans. Wirel. Commun. 12 1989-2001
[2] Jameel F, Khan F, Ali H M A, Butt A 2018 A technical review of simultaneous wireless information and power transfer (SWIPT) Int. Symp.RAEE (Islamabad; IEEE) p 1-6
[3] Lu X, Wang P, Niyato D, Kim D I 2015 Wireless Networks with RF Energy Harvesting: A Contemporary Survey IEEE Commun. Surv. Tutor. 17 757-789
[4] Guo K, Guo D and Zhang B 2018 Analysis of hardware impairments on the energy harvesting hybrid relay networks J. Phys.: Conf. Ser. 960 012003
[5] Mukhlif F , Bin N K A , Mansoor A M and Kasirun Z 2019 Green transmission for C-RAN based on SWIPT in 5G: a review Wirel. Netw. 25 2621-49
[6] Clerckx B, Zhang R, Schober R, Ng D W, Kim D I and Poor H V 2018 Fundamentals of Wireless Information and Power Transfer: From RF Energy Harvester Models to Signal and System
Designs IEEE J. Sel. Areas. Commun. 37 4-13

[7] Zhou X, Zhang R and Ho C K 2013 Wireless Information and Power Transfer: Architecture Design and Rate-Energy Tradeoff IEEE Trans. Commun. 61 4754-67

[8] Shi Q, Xu W, Chang T H, Wang Y and Song E 2014 Joint Beamforming and Power Splitting for MISO Interference Channel With SWIPT: An SOCP Relaxation and Decentralized Algorithm IEEE Trans. Signal Process. 62 6194-6208

[9] Wang D, Zhang R, Cheng X and Yang L 2016 Capacity-Enhancing Full-Duplex Relay Networks based on Power Splitting (PS-)SWIPT IEEE T. VEH. TECHNOL. 2016 66 5445-50

[10] Liu L, Zhang R, Chua K and Chua 2014 Secrecy Wireless Information and Power Transfer with MISO Beamforming IEEE Trans. Signal Process 62 1850-63

[11] Liao W C, Chang T H, Ma W K and Chi C Y 2011 QoS-Based Transmit Beamforming in the Presence of Eavesdroppers: An Optimized Artificial-Noise-Aided Approach IEEE Trans. Signal Process. 59 1202-16

[12] Zhu J, Schober R and Bhargava V K 2014 Secure Transmission in Multicell Massive MIMO Systems IEEE Wirel. Commun. 13 4766-81

[13] Li Q and Han D 2014 Sum secrecy rate maximization for full-duplex two-way relay networks IEEE Int. Conf. Acoust. (Shanghai:IEEE) pp 3641-45

[14] Liu L, Zhang R, Chua K and Chua 2014 Secrecy Wireless Information and Power Transfer with MISO Beamforming IEEE Trans. Signal Process. 62 1850-63

[15] Tang X, Cai Y, Yang W, chen D and Hu 2018 Secure Transmission of Cooperative Zero-Forcing Jamming for Two-User SWIPT Sensor Networks Sensors 18 331-343

[16] Chen P, Li T, Wang Z and Xiao N 2019 Secure Beamforming for Simultaneous Wireless Information and Power Transfer in Wireless-Powered Full-Duplex Relay Networks 14nd Int. Conf. on Computer Science & Education (ICCSE) (Toronto:IEEE) pp 789-794

[17] Hehao N, Zhang B, Guo D and Huang Y 2017 Joint Robust Design for Secure AF relay Networks with SWIPT IEEE Access 5 9369-77

[18] Kim Y, Choi O, Kim Y and Park J 2016 Performance analysis of LTE multi-antenna technology in live network. 2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC) (Seoul:IEEE) pp 1302-05

[19] Feng Y, Yang Z, Zhu W P, Li Q and Lv B 2017 Robust Cooperative Secure Beamforming for Simultaneous Wireless Information and Power Transfer in Amplify-and-Forward Relay Networks IEEE T. VEH. TECHNOL. 66 2354-66

[20] Lei J, Han Z, Vazquez-Castro, Maria ángeles and Hjorungners 2011 Secure Satellite Communication Systems Design With Individual Secrecy Rate Constraints IEEE Trans. Inf. Forensics Secur. 6 661-671

[21] Mansour A S, Schaefer R F and Boche H 2015 The individual secrecy capacity of the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap channel Mansour, A. S. , Schaefer, R. F. , & Boche, H. . (2015). The individual secrecy capacity of the Gaussian SISO and degraded Gaussian MIMO multi-receiver wiretap channel. 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). (Stockholm:IEEE) pp 365-369

[22] Grant M 2010 Cvx : matlab software for disciplined convex programming, version 1.21. http://cvxr.com/cvx

[23] Jain N K, Nangia U and Jain J 2018 A review of particle swarm optimization J.Inst. Eng. 99 407-411