Physical Communication 28 (2018) 19–27

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Secrecy energy efficiency optimization for MISO SWIPT systems

Xiaobo Zhou [a,b], Wenlong Cai [c], Riqing Chen [d], Linqing Gui [a,*], Feng Shu [a], Jinyong Lin [c], Shuo Zhang [c], Yijin Zhang [a]

[a] School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, 210094, China
[b] Fuyang normal university, Fuyang, 236037, China
[c] National Key Laboratory of Science and Technology on Aerospace Intelligence Control, Beijing Aerospace Automatic Control Institute, Beijing, 100854, China
[d] College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China

ARTICLE INFO

Article history:
Received 31 December 2017
Received in revised form 9 February 2018
Accepted 2 March 2018
Available online 14 March 2018

Keywords:
Secrecy energy efficiency
SWIPT
Energy harvesting
Physical layer security
Beamforming

ABSTRACT

In this paper, we investigate the secrecy energy efficiency (SEE) optimization of the multiple-input single-output (MISO) system. First, transmission beamforming vector is designed to achieve the SEE maximization subject to the constraints of transmission power, minimum secrecy rate threshold and harvested energy threshold. The optimization problem belongs to the category of fractional optimization, which is non-convex and is very difficult to tackle. In order to solve the optimization problem, we propose an algorithm that can obtain a near-optimal solution, which consists of outer-tier and inner-tier iterations. For the outer-tier iteration, we first employ the Dinkelbach method to convert the fractional objective function into a polynomial form, and then transform the optimization problem into a difference of concave (DC) programming. For the inner-tier iteration, we employ the first-order Taylor expansion and successive convex approximation (SCA) method to solve the DC optimization problem. Then, we analyze the computational complexity of the proposed algorithm. In addition,we prove that the rank relaxation is tight. The simulation results show that the SEE performance of our proposed algorithm is obviously superior to that of secrecy rate maximization scheme and zero-forcing scheme.

1. Introduction

Recently, the world has witnessed tremendous increase of new wireless applications. To meet the requirement of elevated quality of service (QoS), those new applications always demand wireless devices to support higher data rate transmission [1]. Evidently, wireless devices have to consume much more energy. However, conventionally wireless devices are equipped with small batteries which can only provide limited energy. Moreover, it is always neither convenient nor economic to replace or recharge the batteries especially when the devices are deployed somewhere hard to reach. To overcome this problem, wireless power transfer (WPT) and energy harvesting (EH) have emerged as promising solutions, because they can turn ambient radio frequency (RF) signals to economic energy sources. Particularly, combining power transfer with traditional information transmission has generated an attractive research area, i.e., simultaneous wireless information and power transfer (SWIPT).

SWIPT has been studied in various communication systems [2–4]. In [2], the capacity-energy bound for a single-input single-output (SISO) SWIPT system was investigated. In [3], as for multi ple-input multiple-output (MIMO) SWIPT system, the authors not only investigated the beamforming design, but also proposed two information/energy receiving strategies, i.e., time-switching (TS) and power-splitting (PS). In order to maximize the throughput, the authors in [4] proposed a PS-based relaying scheme. However, the design with the sole goal of throughput maximization will inevitably increase the energy consumption. A balance between them should be achieved. Therefore, energy efficiency (EE) has been regarded as an important metric for SWIPT systems [5–7].

Secure communication is also an important issue for wireless communication systems due to the broadcast nature of wireless channel [8,9]. Different from traditional encryption performed at higher layers of communication systems, physical-layer security techniques aim to prevent eavesdroppers from capturing secure information, leaving no chance for them to do decryption [10,11]. In recent years, many physical-layer security techniques have been proposed for SWIPT systems [12–14]. Secure SWIPT systems can be applied in various scenarios, e.g. some wireless-powered sensor networks require secure transmission of the sensitive information gathered from local private environment [15]. In secure SWIPT

* Corresponding author.
E-mail addresses: zxb@njust.edu.cn (X. Zhou), caiwenlon@buaa.edu.cn (W. Cai), riqing.chen@fafu.edu.cn (R. Chen), guilinqing@163.com (L. Gui), shufeng0101@163.com (F. Shu), ljiny3771@sina.com (J. Lin), gcshuo@163.com (S. Zhang), yijin.zhang@gmail.com (Y. Zhang).

https://doi.org/10.1016/j.phycom.2018.03.001
1874-4907/

systems, to fulfill both secure transmission and power transfer, one common method is to design beamforming matrix and/or artificial noise (AN) matrix at the transmitter side [14].

When designing secure SWIPT systems, researchers usually consider four objective metrics, i.e., secrecy rate maximization [12,13], transmission power minimization [16], harvested energy maximization and secrecy energy efficiency (SEE) maximization [17–19]. Compared to the former three metrics which conflict with each other, SEE is supposed to make a good tradeoff, which is essentially important in green and sustainable networks. Thus, the optimization of SEE has attracted a lot of research attentions recently. For example, in [17], in order to obtain an optimal SEE subject to transmission power and QoS constraints, the authors designed the beamforming for MISO channel. The SEE was defined as the ratio of secrecy rate over the transmission power. With the same definition of SEE, in [18], the authors investigated the SEE maximization with AN and observed that although AN could bring higher secrecy rates, it also increased power consumption due to the augmented complexity. In [19], dedicated for MIMO channel, the authors aimed to maximize SEE by optimizing the transmission covariance under the constraint of transmission power consumption. They proposed an optimization method which can guarantee the convergence to the Karush–Kuhn–Tucker point.

Although these works all aim to optimize SEE, they were proposed not for SWIPT systems but merely for physical layer security. In fact, until very recently, researchers found out the traditional SEE design should be modified to fit SWIPT systems. For example, in [20], compared to secrecy rate, the authors emphasized more on energy harvesting. Thus instead of traditional SEE, they completely changed the objective and proposed a new metric namely harvested power efficiency, which is defined as the ratio of the total harvested power at the receiver to the transmission power. The secrecy rate was also taken into consideration, but only as a constraint. On the contrary, without any bias to harvested energy, the authors in another most-recent paper [19] redesigned SEE by considering the overall energy consumption of the system. Thus, the new SEE was defined as the ratio of secrecy rate to the sum of power consumption at both transmitter and receiver. However, it did not consider the effect of energy harvesting. Due to SWIPT, part of transmission energy is actually harvested by the receiver, and then the harvested energy will become part of energy source for the receiver. Therefore, the harvested energy should be taken into account when calculating the energy consumption at the receiver.

The main contributions of this paper are illustrated as follows.

(1) We consider SEE as the ratio of secrecy rate to the real power consumption of the system. Joining the effect of energy harvesting, the real power consumption is the sum of power consumption at both transmitter and receiver but with harvested energy deducted.

(2) We have formulated and solved the SEE optimization problem. Although the optimization problem is difficult to solve, we have made critical transformation and obtained the near-optimal solution. First, using Dinkelbach-based iterative algorithm, the original objective function in the form of fraction is transformed into a polynomial function which becomes a difference of concave (DC) programming. Then, after rank-one relaxation, successive convex approximation (SCA) method is used to further transform the objective to concave function, whose near-optimal solution can be obtained by common CVX tools. More importantly, we have proved that the near-optimal solution actually satisfies the rank-one constraint, which means the previous relaxation is tight.

(3) We have evaluated and analyzed the performance of our SEE maximization scheme in detail. First, we derived the exact complexity of our proposed algorithm. Then through simulations we demonstrated that our proposed algorithm has better SEE performance than zero-forcing algorithm and secrecy rate maximization algorithm.

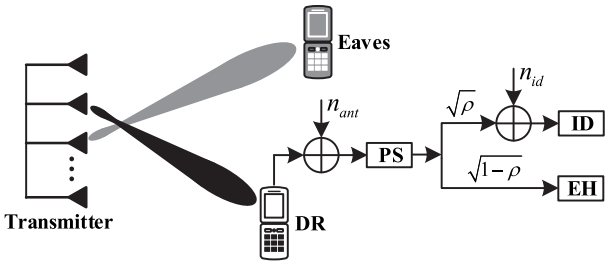

Fig. 1. An illustration of MISO secure SWIPT system.

The rest of this paper is organized as follows. Section 2 introduces the system model and formulates the SEE maximization problem. In Section 3, we propose a two-tier iterative algorithm to solve the optimization problem and then analyze the complexity of the proposed algorithm. Simulation results are given in Section 4. Finally, Section 5 concludes the paper.

Notation: Boldface lowercase denote the vectors and uppercase letters denote matrices. $\mathbf{A}^H$, $\mathrm{Tr}(\mathbf{A})$, $\mathrm{rank}(\mathbf{A})$ and $\mathbf{A} \succeq \mathbf{0}$ denote conjugate transpose, trace, rank, semi-definite of matrix $\mathbf{A}$, respectively, $[x]^+ = \max\{x, 0\}$.

2. System model and problem formulation

In this section, we first describe the MISO secure SWIPT system model and the total power consumption model, and then we formulate the SEE optimization problem.

2.1. System model

We consider a secure SWIPT system as shown in Fig. 1. The system consists of a transmitter, a desired receiver (DR), and an eavesdropper (Eaves), where the transmitter is equipped with N antennas, DR and the eavesdropper are both equipped with one antenna. DR divides the received signals into two parts by using PS, one part is used for information decoding (ID), and the other is used for energy harvesting (EH).

In order to ensure secure communication between transmitter and DR, we need to design the transmission signal $\mathbf{s}$ which can be expressed as

$$\mathbf{s} = \mathbf{w}x, \tag{1}$$

where $\mathbf{w}$ represents the transmission beamforming vector, x is the confidential message intended for DR with $\mathbb{E}\{xx^*\} = 1$. The received signal at the DR and the eavesdropper are given by

$$y_d = \mathbf{h}^H\mathbf{w}x + n_{ant}, \tag{2}$$

and

$$\mathbf{y}_e = \mathbf{g}^H\mathbf{w}x + n_e, \tag{3}$$

respectively, $\mathbf{h} \in \mathbb{C}^{N\times 1}$ and $\mathbf{g} \in \mathbb{C}^{N\times 1}$ denote the channel responses between the transmitter and the DR, the eavesdropper, respectively. $n_{ant} \sim \mathcal{CN}(0, \sigma_{nat}^2)$ and $n_e \sim \mathcal{CN}(0, \sigma_e^2)$ respectively denote the complex Gaussian noise at DR and the eavesdropper. DR divides the received signal into two parts for ID and EH, respectively. The signal for ID can be expressed as

$$\tilde{y}_d = \sqrt{\rho}\mathbf{h}^H\mathbf{w}x + \sqrt{\rho}n_{ant} + n_{id}, \tag{4}$$

where $0 < \rho \leq 1$ denotes the PS ratio, and $n_{id} \sim \mathcal{CN}(0, \sigma_{id}^2)$ is the additive Gaussian noise. In this paper, we assume that the transmitter knows the perfect CSI of DR and the eavesdropper.