Physical Communication 26 (2018) 1–8

Contents lists available at ScienceDirect

Physical Communication

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

Full length article

Optimal transceiver design for SWIPT system with full-duplex receiver and energy-harvesting eavesdropper

Zhixiang Deng *, Yuan Gao, Changchun Cai, Wei Li

College of Internet of Things Engineering, Hohai University, Changzhou, 213022, China

ARTICLE INFO

Article history:
Received 4 June 2017
Received in revised form 24 September 2017
Accepted 30 October 2017
Available online 10 November 2017

Keywords:
Simultaneous wireless information and power transfer (SWIPT)
Physical-layer security
Full-duplex (FD)
Semidefinite relaxation (SDR)

ABSTRACT

In this paper, we consider simultaneous wireless information and power transfer (SWIPT) in a multiple-input-single-output (MISO) channel with a full-duplex (FD) receiver and an energy-harvesting (EH) receiver which is a potential eavesdropper, where the receivers adopt the power splitting approach to decode information and harvest energy simultaneously. The FD receiver decodes the information that should be kept secret from the EH receiver and sends jamming signals to degrade the eavesdropper simultaneously using the energy it harvests from the source. Taking into account the eavesdropper channel uncertainties, we attempt to maximize the worst-case secrecy rate (WCSR) at the receiver by jointly optimizing the information beamforming and energy covariance at the transmitter and the artificial noise (AN) covariance at the FD receiver, subject to the power constraint at the transmitter and the minimum energy required at the EH receiver. In order to solve this non-convex optimization problem, semidefinite relaxation (SDR) approach and extended S-procedure are explored to convert the original non-convex optimization problem to a convex one which can be solved efficiently. Numerical results are given to show the superiority of our proposed scheme.

1. Introduction

Radio signal enabled SWIPT has drawn a great interest due to its potential in meeting the rapidly escalated energy consumption of 5G communications [1,2]. Full-duplex (FD) wireless communication, another potential technique for 5G communications, has also gained an upsurge attention since it doubles the spectral efficiency by enabling simultaneous transmission and reception over the same frequency band. However, due to the open nature of the wireless medium, communication security arises to be an essential problem in SWIPT or FD systems. To address this problem, physical layer security, which achieves secure transmissions by exploiting the randomness in the physical layer, has drawn considerable attentions [3,4].

For the security problems in the SWIPT systems, the literatures tried to maximize the secrecy rate under the constraints of minimum required energy harvested at the energy-harvesting receivers (ER) [5] or to maximize the energy harvested at the ERs under the secrecy rate constraints of the legitimate receivers [6–8]. In [5], a wireless MISO secure communication system with SWIPT overheard by multiple multi-antenna eavesdroppers was considered. The achievable secrecy rate was maximized under the transmit power and energy harvesting constraints by jointly design AN-aided transmission and power splitting scheme. Wu et al. [6] studied an energy-harvesting maximization problem under the constraints of transmit power and secrecy rate at the legitimate receiver for a MIMO wiretap channel with SWIPT. They adopted Taylor series expansion to convert the original non-convex problem into a convex one. In [8], Zhang et al. studied a SWIPT MISO broadcast channel with confidential messages with the goal to minimize the total transmit power while guaranteeing the secrecy rate and the harvested energy constraints at each receiver. The authors in [9] also aimed to minimize the transmit power such that the target secrecy rate of the co-located receiver (CR) and the energy harvesting constraints for the CR and ERs which are potential eavesdroppers. Both the two problems: to maximize the secrecy rate subject to harvested energy constraints of ERs, or to maximize the harvested energy of the ERs subject to secrecy rate constraint of legitimate receivers, are investigated in [10].

Because of the potential in increasing the spectrum efficiency, FD wireless communication which allows simultaneous transmission and reception over the same frequency band has gained an upsurge attention. In the context of physical layer security, the FD relaying technology also shows its potential benefits by allowing the legitimate receiver to generate AN to degrade the eavesdropper channel simultaneously while receiving data [11,12]. For the SWIPT systems with FD nodes, the AN generated by the FD nodes not only degrades the eavesdropper channel, but also charges the

* Corresponding author.
E-mail address: dengzhixiang@hhuc.edu.cn (Z. Deng).

https://doi.org/10.1016/j.phycom.2017.10.017
1874-4907/

ERs. In [13], the authors considered a wireless-powered cooperative jamming to secure communication where a FD jammer harvests energy from the information signal and transmits jamming signal at the same time to confound eavesdropper and to charge the ER. A secrecy wireless powered communication network is also studied in [14] and [15], where the FD information source transmits secrecy information to the legitimate receiver using the energy it harvests from the energy source node. In [16], a two-hop FD wireless-powered relaying system where the relay assists the transmission of confidential information while simultaneously harvesting energy. In [17], a FD capable base station transmits data to one downlink user and concurrently receives data from one uplink user. The FD base station also exploits AN to degrade the channel of the idle user, as well as to provide energy to the idle user. As known, interference is often considered as one of the performance limiting factors for communication rate in traditional communication systems, and hence needs to be suppressed or managed. Interference alignment is a promising solution for interference management. Actually, for the novel SWIPT systems, interference signals may be re-utilized for energy harvesting. Wireless energy harvesting and interference alignment can be performed simultaneously in the wireless communication networks. The authors [18–20] presented an unified framework to jointly study wireless energy harvesting and interference alignment. Valuable schemes and algorithms were proposed to optimize both information transmission and wireless energy harvesting performance simultaneously in interference networks. In addition, the self-interference caused by the signal leakage from the transmit antennas to the receive antennas at the FD nodes can now be harvested and reused by the energy harvester. Wireless-powered systems with full-duplexing and self-energy recycling have been studied in many works [21,22]. In [21], the authors considered the beamforming optimization problem in an amplify-and-forward relaying network where the FD relay node harvested energy from RF signal with self-energy recycling protocol. This work mainly focused on the design of self-energy recycling relaying protocol and the optimization design of the relay beamforming vector. If secrecy performance was considered in the considered system, more system parameters such as relay beamforming, wireless energy and confidential information transmission trade-off, relaying protocols, etc. would be involved in the optimization. Further, if CSI uncertainty was considered, the optimization became more complicated. The authors in [22] considered robust transceiver optimization for a downlink MISO SWIPT system and relaxed the optimization problem as a semi-definite program through a linear matrix inequality representation for infinitely many quadratic matrix inequality constraints taking into account CSI uncertainty.

In this paper, we consider a SWIPT system with a FD receiver and an energy-harvesting (EH) eavesdropper. The EH eavesdropper not only harvests energy from the RF signal but also attempts to decode the confidential information of the legitimate users. The source node intends to send confidential information to the legitimate FD receiver which concurrently transmits AN to degrade the EH eavesdropper using the energy it harvests from the source node such that the confidential message is as secret as possible to the eavesdropper. The potential applications of such a system could be wireless sensor networks where some access points are responsible for energy and information transmission while some others have dual functions of information transmission and energy reception. However, some energy-harvesting points may be curious of the information of the other communication pairs. Thus, the information should be kept as secret as possible to the curious points. It is necessary to maximize the achievable secrecy rate while guaranteeing the minimum required energy harvested at the energy-harvesting points.

In order to address the challenging problems in the SWIPT system considered in this paper, including wireless energy transfer efficiency, wireless information and energy transmission trade-off and secrecy SWPT, it is necessary to jointly optimize the system parameters. As known, the accuracy of channel state information (CSI) has a significant effect on the design of joint optimization. Especially, if the energy-harvesting nodes are more willing to eavesdrop information rather than to harvest energy, it will be more difficult to estimate the CSI of the eavesdropping channel precisely. In order to capture the effect of inaccurate CSI on the system performance, it is assumed that CSI of the channel between the source node and the legitimate receiver is perfectly known, while the CSI of the eavesdropping channels is imperfectly known. Taking into account the eavesdropper channel uncertainties, we attempt to maximize the worst-case secrecy rate (WCSR) at the receiver by jointly optimizing the information beamforming and energy covariance at the transmitter and the AN covariance at the FD receiver, subject to the power constraint at the transmitter and the minimum energy required at the EH eavesdropper. For the formulated non-convex worst-case secrecy rate maximization problem, the SDR-based optimization method [23] is introduced to solve it effectively. Extended S-procedure [24] and Charnes–Cooper [25] transformation are used to convert the original non-convex problem to a convex one which can be handled by solving a sequence of semidefinite problems (SDPs). Further, we prove the tightness of the SDR of the original worst-case secrecy rate maximization problem by showing the existence of rank-one optimal solutions.

Notations: Scalars, vectors and matrices are denoted by lower-case, boldface lower-case and boldface upper-case letters, respectively. $Tr(\mathbf{X})$, $\mathbf{X}^H$ and $Rank(\mathbf{X})$ denote trace, Hermitian transpose and rank of a matrix $\mathbf{X}$. $|\cdot|$ denotes the absolute value of a complex scalar. $E(\cdot)$ represents statistical expectation. $\mathbb{C}^{m\times n}$ denotes the space of $m \times n$ complex matrices. $\mathbf{I}_N$ represents N-dimensional identity matrix. $\mathbf{x} \sim \mathcal{CN}(\mu, \Sigma)$ means that the random vector $\mathbf{x}$ follows a circularly symmetric complex Gaussian distribution with mean μ and covariance Σ. $\mathbf{X} \succeq 0$ ($\mathbf{X} \succ 0$) means that the matrix $\mathbf{X}$ is semidefinite positive (positive).

2. System model and problem formulation

2.1. System model

We consider a SWIPT system with a FD receiver and an EH eavesdropper, as shown in Fig. 1. The source node S with N_t antennas, transmits information signals and transfers energy simultaneously. The legitimate node D, operating in FD mode, is equipped with one antenna for receiving and N_d antennas for transmitting. The node E with one antenna harvests energy from node S and is a potential eavesdropper. Note that for simplicity, we consider the multi-input single-output (MISO) setup with only one antenna for information or energy receiving. This simplicity may be of practical interest in many scenarios due to its low hardware cost, e.g. for the MISO system with only one antenna used for energy harvesting, only one rectifier is needed.

The FD legitimate receiver D receives confidential messages from the source node S and transmits jamming signal to degrade the potential eavesdropper E simultaneously, using the energy it harvests. Note that the receiver D receives information and energy signals from the same antenna. In order to achieve simultaneous wireless information and power transfer, the received signal at D has to be split into two distinct parts, one for information decoding and one for energy harvesting. Some techniques have been proposed to achieve this signal splitting, such as time switching, power splitting, antenna switching, etc. In this paper, the receiver D adopts the power splitting approach to split the received signal into two streams of different power for decoding information and harvesting energy separately. Specifically, in order to obtain the inputs