Game Theory-Based Resource Allocation for Secure WPCN Multiantenna Multicasting Systems

Zheng Chu, *Member, IEEE*, Huan X. Nguyen, *Senior Member, IEEE*
Giuseppe Caire, *Fellow, IEEE*

Abstract

This paper investigates a secure wireless-powered multiantenna multicasting system, where multiple power beacons (PBs) supply power to a transmitter in order to establish a reliable communication link with multiple legitimate users in the presence of multiple eavesdroppers. The transmitter has to harvest radio frequency (RF) energy from multiple PBs due to the shortage of embedded power supply before establishing its secure communication. We exploit a novel and practical scenario that the PBs and the transmitter may belong to different operators and a hierarchical energy interaction between the PBs and the transmitter is considered. Specifically, the monetary incentives are required for the PBs to assist the transmitter for secure communications. This leads to the formulation of a *Stackelberg* game for the secure wireless-powered multiantenna multicasting system, where the transmitter and the PB are modelled as leader and follower, respectively, each maximizing their own utility function. The closed-form *Stackelberg* equilibrium of the formulated game is then derived where we study various scenarios of eavesdroppers and legitimate users that can have impact on the optimality of the derived solutions. Finally, numerical results are provided to validate our proposed schemes.

Index Terms

Wireless powered communication networks (WPCN), Physical layer security, SWIPT, Multicasting, *Stackelberg* game

I. Introduction

Wireless multicast media streaming is anticipated to be a significant component of the forthcoming 5G systems, motivated by the consumers' desire to take advantage of high quality multimedia wireless

Z. Chu and H. Nguyen are with the School of Science and Technology, Middlesex University, The Burroughs, London NW4 4BT, U.K. (Email: z.chu@mdx.ac.uk; h.nguyen@mdx.ac.uk)

Giuseppe Caire is with the Communications and Information Theory Group, Technical University of Berlin, 10587 Berlin, Germany, and also with the Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089 USA. (Email: caire@tu-berlin.de)

devices (e.g., 4k hand-held devices, 3D augmented reality) [1]–[3]. Energy efficiency and security are major critical issues that must be addressed in the design of such systems.

Radio frequency (RF) energy harvesting and transfer techniques have recently been considered as a promising solution to the energy-constrained wireless networks [4]–[6]. As a recent application of RF energy harvesting and transfer techniques, wireless powered communication networks (WPCNs) have become a novel technology in wireless networking and attracted more and more attention [7]. A "*harvest-then-transmit*" protocol was proposed for WPCNs in [8], where the wireless users harvest power from the RF signals broadcast by an access point in the downlink (DL), and then send information to the AP in the uplink (UL) by employing the harvested energy. Cooperative protocols for WPCNs were developed based on different models [9]–[11]. In [12], an intermediate self-sustainable relay was employed to enable cooperation between a wireless energy transfer (WET) network and a wireless information transfer (WIT) network to guarantee secure communications subject to outage probability constraints. A different approach consists of deploying a dedicated WET network with multiple power beacons (PBs) to provide wireless charging services to the wireless terminals via the RF energy transfer technique [13], [14]. Since the PBs do not require any *backhaul link*, the associated cost of PBs deployment is much lower, hence, it is feasible to deploy the PBs densely to guarantee network coverage for a wide range of mobile devices [15].

Security in data transmission can be addressed either by traditional crypto methods, or more fundamentally, in terms of information theoretic secure rates. The latter approach, commonly referred to as "physical-layer security," was initially developed for the wiretap channel [16], [17], i.e., a broadcast channel with one transmitter and two sets of receivers: legitimate users and eavesdroppers. Multiantenna wiretap channels have been widely investigated in terms of secure rate region [18]–[22]. Some state-of-art techniques, such as artificial noise (AN) and cooperative jammer (CJ), have been designed for multiantenna transceivers, in order to introduce more interference at the eavesdroppers [23]–[30]. In [23], rank-one solution properties were exploited with semidefinite programming (SDP) relaxation for secure transmit beamforming. AN-assisted transmit optimization has been presented in [24], where the spatially selective AN embedded with secure transmit beamforming was designed to obtain the optimal power allocation. In [25], CJ from an external node is exploited in order to create interference at the eavesdroppers and achieve the desired target secure rate. However, it is not always possible to have an own CJ to improve the secrecy rates. Another option could be to employ a private CJ by paying a price for the jamming services. This strategy was investigated in [25], [26], where a CJ releases its jamming service depending interference caused to the eavesdropper, while the transmitter pays a certain amount to guarantee its secure communication. In this strategy, a *Stackelberg* game can be formulated to obtain the optimal power allocation. In addition, cooperative cognitive radio (CR) combined with secure communications could also be modelled as a *Stackelberg* game to determine the optimal resource allocations [27]. In [28]–[30], the secrecy rate optimization problem was posed in terms of outage secrecy rates, due to the fact that the channels are not perfectly known and are subject to random fading with known statistics. Physical-layer security techniques have also been recently developed in radio frequency identification (RFID). The design of RFID systems is a challenge due to the broadcast nature of backscatter communication, which is vulnerable to eavesdropping [31]. Simultaneous wireless information and power transfer (SWIPT) has emerged as one of most promising approaches to provide power for communication devices. SWIPT has been considered in combination with physical-layer security in a number of recent works (e.g., [32]–[35]). It is worth pointing out that the transmit power is constant in the above secure communication systems. However, the use of WET effectively makes the available transmit power a system variable in order to achieve secure communications. Thus, this research gap motivates the work in this paper.

We investigate a WPCN-assisted multiantenna secure multicasting system, in which a multicast service provider (i.e., the transmitter) guarantees secure communication with legitimate users in the presence of multiple eavesdroppers by utilizing the harvested energy from the PBs that are deployed by different service operators. We exploit this energy interaction between the PBs and transmitter and formulate this for the considered PB-assisted secure WPCN as a game theory framework. The contributions of this paper are highlighted as follows:

1) *Game theory based WPCN-aided multiantenna secure multicasting system*: We investigate a scenario where the PBs and the transmitter belong to different service operators, both of which want to maximize their own benefit. Thus, incentives are required for the PBs to assist the transmitter to guarantee the secure multicasting communications, which is known as 'energy trading'. Particularly, an energy price must be paid by the transmitter in order to induce the PBs to provide sufficient energy. We develop an energy trading framework for the wireless powered secure multiantenna multicasting systems, where the strategic behavior of the transmitter and the PBs is modeled as a Stackelberg game. The transmitter acts as a leader that buys energy service from the PBs, which optimizes the energy price and the energy transfer time to maximize its utility function, defined as the weighted difference between revenues (proportional to the achievable secrecy rate) and costs of the purchased energy. The PBs are the followers that determine their optimal transmit powers based on the energy price offered by the transmitter to maximize their own profits, defined as the difference between the payment received from the transmitter and their energy production cost. We derive a closed-form solution for the Stackelberg equilibrium, in which both the PBs and the transmitter come to an agreement on the energy price, transmit power and energy time allocation.

2) *Conic Convex Reformulation*: In the formulated Stackelberg game, the multicasting transmit beamforming vector leads to the nonconvexity of the leader game. To circumvent this issue, we propose a conic convex reformulation to solve the optimal multicasting transmit beamforming vector directly. We first propose a novel reformulation based on matrix transformations and convex conic optimization techniques, yielding a second-order cone programming (SOCP) solution which is optimal when the SDP relaxed solution satisfies the rank-one conditions. In addition, a special case with single legitimate user and eavesdropper is investigated, where we derive a closed-form optimal solution based on the dual problem and Karush-Kuhn-Tucker (KKT) conditions. Then, we propose a successive convex approximation (SCA) based SOCP scheme, which is performed iteratively to obtain the optimal transmit beamformer directly for any general case. Numerical results confirm that our proposed SCA based SOCP scheme outperforms the SDP randomization scheme.

This paper differs from the related works in [8], [14], [23], [36]–[39] in terms of problem formulation and mathematical solutions as follows:

- *Problem formulation*: This paper investigates a secure WPCN multicasting system, while [36] considered a secure WPCN system with one legitimate user and one eavesdropper. Note that in the existing literatures (e.g., [14], [36]), it was assumed that the dedicated PBs are deployed by the same service operator with the existing WIT network. In this case, the network can provide both wireless access and wireless charging services [8], [14], or support the secrecy communication by utilizing the harvested energy [36]. However, in this paper, we take into account a practical and novel scenario that both PBs and the communication transmitter belong to different service providers, each aims to maximize their own utility. For this scenario, the conventional approaches addressing the security by maximizing the secrecy rate [36] or secrecy outage probability [37] subject to transmit power budget cannot be applied. In fact, in the proposed approach we use hierarchical energy interaction (i.e., *energy trading*) framework through Stackeberg game to address the security when multiple providers operate in a competitive manner. This approach is novel and has not been treated in previous literature.
- *Mathematical solutions*: In [23], [36], semidefinite programming (SDP) relaxation was employed to relax both power minimization and secrecy rate maximization problems for the case of single legitimate user only. However, this approach will not always guarantee a rank-one solution when extending to the case of multiple legitimate users. Therefore, the rank-one feasible solution for the original beamforming problem can only be achieved via the rank reduction methods (i.e., randomization techniques [1]), with no optimality guarantee (see, e.g., [38], [39]). In this paper, we study a more comprehensive scheme than its counterparts in [23], [38], [39] by covering both scenarios of when the rank-one condition is satisfied and when it is not. In particular, we employ an SCA

based method which can be applied to the general case when the rank-one condition is not satisfied. In this way, the transmit beamforming vector can be solved directly by using the SOCP, in which the conventional SDP randomization solution would not be able to provide the optimal solution. In addition, the proposed SOCP approach allows a closed-form solution to be achieved for the special case of single legitimate user and single eavesdropper.

The rest of the paper is organized as follows. Section II presents our system model. Section III investigates the game theory based secure WPCN multiantenna multicasting system. Section IV provides simulation results to validate the theoretical derivations. Finally, Section V concludes the paper.

A. Notations

We use the upper case boldface letters for matrices and lower case boldface letters for vectors. $(\cdot)^T$ and $(\cdot)^H$ denote the transpose and conjugate transpose respectively. $\mathrm{Tr}(\cdot)$ and $\mathbb{E}\{\cdot\}$ stand for trace of a matrix and the statistical expectation for random variables. $\varrho_{max}(*)$ represents the maximum eigenvalue, whereas $\upsilon_{\max}(*)$ denotes the eigenvector associated with the maximum eigenvalue. $\mathbf{A} \succeq 0$ indicates that $\mathbf{A}$ is a positive semidefinite matrix. $\| * \|$ denotes the Euclidean norm of a vector. $\mathbf{I}$ and $(\cdot)^{-1}$ denote the identity matrix with appropriate size and the inverse of a matrix respectively. $[x]^+$ represents $\max\{x, 0\}$. The notation $\succeq_{K_n}$ denotes the following generalized inequality:

$$\begin{bmatrix} a \\ \mathbf{b} \end{bmatrix} \succeq_{K_n} \mathbf{0} \Leftrightarrow \|\mathbf{b}\| \leq a,$$

where $a \in \mathbb{R}_+,\ \mathbf{b} \in \mathbb{C}^{n-1}$ and $K_n \subseteq \mathbb{R}^n$ is a *proper cone* [41].

II. System Model

In this section, we consider the secure wireless powered multiantenna multicasting system as shown in Fig. 1, where a transmitter broadcasts the same information to all legitimate users in the presence of multiple eavesdroppers. It is assumed that the transmitter has not an exogenous energy source and must harvest energy from a WET network, formed by multiple PBs. This system consists M single antenna PBs, one multiantenna transmitter equipped with N_T transmit antennas, K single antenna legitimate users and L single antenna eavesdroppers. This secrecy model has some potential applications, such as wireless sensor networks, device to device (D2D) communication systems, and on-demand video broadcasting. For example, in recent works of femtocaching, D2D caching networks [42], [43], it is advocated that "helper" nodes are densely disseminated in a coverage area and serve users' demands using their own large cached information. Cache memory at the helpers alleviates the need for a backhaul connection such that these helper nodes can be placed arbitrarily, even if there is no high-speed data connection. In this case, we always wish to make such helper nodes truly free from any wired connection, including power. Thus, they need to harvest energy somewhere, for example, from a WET network. However, there arises a need for secrecy projection as on-demand broadcasting normally requires a subscription, which means illegitimate users will not be able to access the content that they do not pay for. In our paper, a *harvest-then-transmit* protocol is considered. Specifically, time is divided in periods of duration T. Each period is split into a WET phase of duration θT, and a WIT phase of duration $(1-\theta)T$, where $\theta \in (0,1)$ is a system parameter that must be optimized. Let $\mathbf{h}_{s,k} \in \mathbb{C}^{N_T \times 1}$ denote the channel coefficients between the transmitter and the k-th legitimate user, while $\mathbf{h}_{e,l} \in \mathbb{C}^{N_T \times 1}$ denotes the channel coefficients between the transmitter and the l-th eavesdropper. Also, $\mathbf{g}_m \in \mathbb{C}^{1 \times N_T}$ denotes the channel coefficients between the m-th PB and the

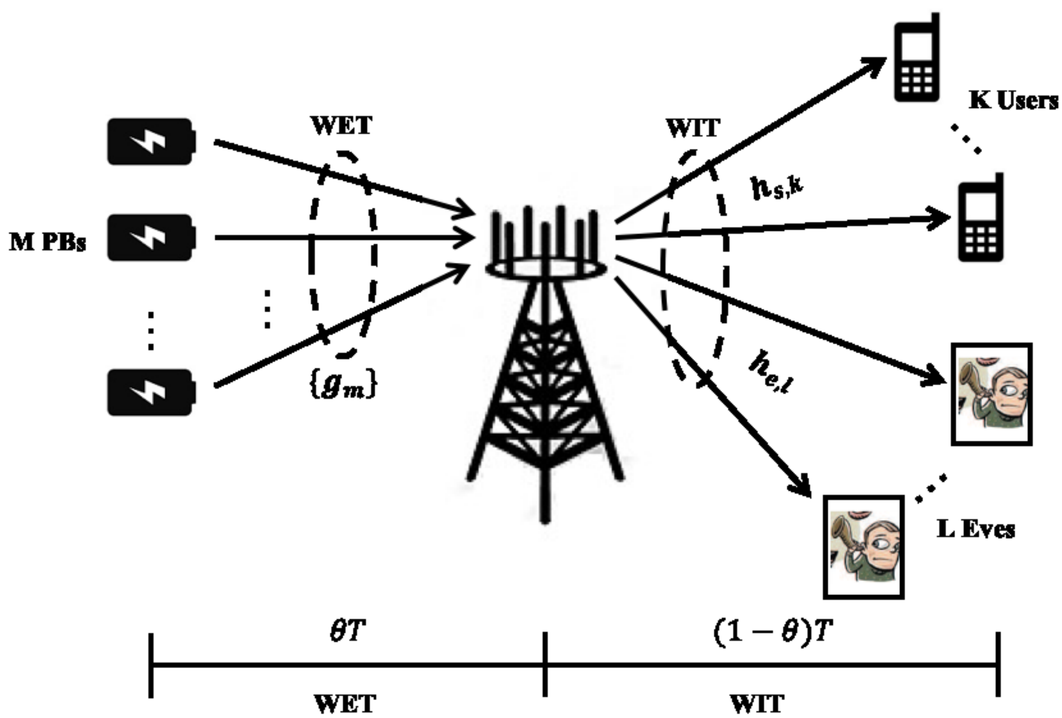

Fig. 1: WPCN for multiantenna secure multicasting system.

transmitter. First, each PB transfers the energy to the transmitter, the harvested energy during the WET phase of θT at the transmitter can be written as

$$E_B = \xi \sum_{m=1}^{M} p_m \|\mathbf{g}_m\|^2 \theta T, \tag{1}$$

where p_m denotes the transmit power of the m-th PB, and $0 < \xi \leq 1$ is the efficiency for converting the harvested energy to the electrical energy to be stored, which is assumed to be $\xi = 1$ in this paper. During the WIT phase of $(1-\theta)T$, the received signal at the k-th legitimate user and the l-th eavesdropper are given by

$$\mathbf{y}_{s,k} = \sqrt{\frac{E_B}{(1-\theta)T}}\mathbf{h}_{s,k}^H\mathbf{v}s + n_{s,k},\ k = 1, ..., K,$$

$$\mathbf{y}_{e,l} = \sqrt{\frac{E_B}{(1-\theta)T}}\mathbf{h}_{e,l}^H\mathbf{v}s + n_{e,l},\ l = 1, ..., L,$$

where s denotes the Gaussian distributed transmit signal with unit norm, $\mathbf{v} \in \mathbb{C}^{N_T \times 1}$ is the normalized transmit beamformer with $\mathbb{E}\{\|\mathbf{v}\|^2\} = 1$, $n_{s,k}$ and $n_{e,l}$ are additive white Gaussian noises (AWGNs) at the k-th legitimate user and the l-th eavesdropper with variance σ_s^2 and σ_e^2. Hence, the channel capacity of the k-th legitimate user and the l-th eavesdropper can be expressed as [36]

$$R_{s,k} = (1-\theta)\log\left(1 + \frac{\theta\sum_{m=1}^M p_m\|\mathbf{g}_m\|^2|\mathbf{h}_{s,k}^H\mathbf{v}|^2}{(1-\theta)\sigma_s^2}\right),\ \forall k, \tag{2}$$

and

$$R_{e,l} = (1-\theta)\log\left(1 + \frac{\theta\sum_{m=1}^M p_m\|\mathbf{g}_m\|^2|\mathbf{h}_{e,l}^H\mathbf{v}|^2}{(1-\theta)\sigma_e^2}\right),\ \forall l, \tag{3}$$

respectively. For this secure multicasting system, we have the following definition:

Definition 1: Multicast secrecy rate of a multicasting system with K users is defined as [39]

$$R_K = \min_{k\in[1,K]}[R_{s,k} - \max_{l\in[1,L]} R_{e,l}]^+ = \min_{k\in[1,K]}(1-\theta)\Bigg[\log\left(1 + \frac{\theta\sum_{m=1}^M p_m\|\mathbf{g}_m\|^2|\mathbf{h}_{s,k}^H\mathbf{v}|^2}{(1-\theta)\sigma_s^2}\right) - \max_{l\in[1,L]}\log\left(1 + \frac{\theta\sum_{m=1}^M p_m\|\mathbf{g}_m\|^2|\mathbf{h}_{e,l}^H\mathbf{v}|^2}{(1-\theta)\sigma_e^2}\right)\Bigg]^+. \tag{4}$$

III. Game theory based Secure WPCN Multiantenna Multicasting System

In this section, we consider the scenario where the transmitter and the PBs are from two different service providers. Both parties want to maximize their own benefit. To model this scenario, we assume that the transmitter will have to pay for the energy services from the PBs, whereas the PBs will consider this payment as incentives to provide wireless energy transfer service. Obviously, being able to decide what price to pay for the energy service, the transmitter can take a leading role in dictating the energy trading interaction. This fits very well the model of a *Stackelberg* game, which motivates us to use this game theory to optimize both parties' benefit. We assume that the channel state information (CSI) between the transmitter and k-th user as well as l-th eavesdropper (i.e., $\mathbf{h}_{s,k},\ \forall k$ and $\mathbf{h}_{e,l},\ \forall l$) is available at the transmitter. This can be achieved through different methods such as the local oscillator power leakage from the eavesdropper receivers' RF frontend [44] or even the CSI feedback method [45]. For example, in a video broadcasting system there may be legitimate users that are entitled to receive the content and other users who have not subscribed to this content, but are still part of the system. These users obey the basic physical-layer protocol rules, which includes feeding back CSI to enable beamforming. Hence, in this case, it is practical to assume that the CSI of the eavesdroppers is known at the transmitter. In this game model, the transmitter (leader) first pays for the harvested energy with an energy price to maximize its utility function. Then, the PBs (followers) optimize their transmit powers based on their released energy price to maximize their individual utility function.

A. Stackelberg Game Formulation

Let λ denote the energy price that the transmitter will pay to the PBs. The total payment of the transmitter to the M PBs, donoted by Q_M, is written as

$$Q_M = \lambda\theta T \sum_{m=1}^{M} p_m \|\mathbf{g}_m\|^2, \tag{5}$$

where p_m denotes the transmit power of the mth PB. Without loss of generality, we can assume $T = 1$. We now define the utility function of the transmitter as follows:

$$U_M = \mu R_K - Q_M, \tag{6}$$

where $\mu > 0$ is the weight per a unit of secrecy throughput, by which the transmitter uses to convert the achievable secrecy rate R_K into the equivalent revenue. Therefore, the leader game for the transmitter can be formulated as

$$\max_{\lambda,\theta,\mathbf{v}} \ U_M, \ \ s.t. \ 0 < \theta < 1, \ \lambda \geq 0. \tag{7}$$

At the same time, each PB can be modelled as a follower that wants to maximize its own revenue function, which is defined as follows:

$$U_{PB,m} = \theta(\lambda p_m \|\mathbf{g}_m\|^2 - \mathcal{F}_m(p_m)), \tag{8}$$

where $\mathcal{F}_m(p_m)$ is used to model the cost of the m-th PB per unit time for wirelessly charging the transmitter with the transmit power p_m. In this paper, we consider the following quadratic model[1] for the cost function of the PBs:

$$\mathcal{F}_m(x) = A_m x^2 + B_m x \tag{9}$$

where $A_m > 0$ and $B_m > 0$ are the constants that can be different for each PB. Thus, the follower game of m-th PB is given by

$$\max_{p_m} \ U_{PB,m}, \ \ s.t. \ p_m \geq 0. \tag{10}$$

Both (7) and (10) form a *Stackelberg* game for this secure WPCN multiantenna multicasting system, where the transmitter (leader) announces an energy price, and then the PBs (followers) optimize the transmit

[1]The quadratic model has been commonly used in the energy market to model the energy cost [46].

power based on the released energy price to maximize their individual revenue functions. The solution of this *Stackelberg* game can be obtained by investigating the *Stackelberg* equilibrium, where the transmitter and the PBs come to an agreement on the energy price, the transmit power of each PB and the time fraction of energy transfer duration. Note that the deviation of either the transmitter or the PBs from the *Stackelberg* equilibrium will introduce a loss in their revenue functions.

B. Stackelberg Equilibrium

In order to derive the solution of this game, the well-known *Stackelberg* equilibrium concept can be defined as follows:

Definition 2: Let $(\theta^{\text{opt}}, \lambda^{\text{opt}})$ denote the solutions of problem (7) while $\{p_m^{\text{opt}}\}$ represents the solution of problem (10) (here, the brackets $\{\}$ indicate a vector that include all p_m's with $\forall m$). Then, the triple-variable set $(\theta^{\text{opt}}, \lambda^{\text{opt}}, p_m^{\text{opt}})$ is a *Stackelberg* equilibrium of the formulated game provided that the following conditions are satisfied

$$U_M(\theta^{\text{opt}}, \lambda^{\text{opt}}, \{p_m^{\text{opt}}\}) \geq U_M(\theta, \lambda, \{p_m^{\text{opt}}\}), \tag{11}$$

$$U_{PB,m}(\theta^{\text{opt}}, \lambda^{\text{opt}}, p_m^{\text{opt}}) \geq U_{PB,m}(\theta^{\text{opt}}, \lambda^{\text{opt}}, p_m), \ \forall m. \tag{12}$$

for $0 < \theta < 1$, $\lambda \geq 0$, and $p_m \geq 0$, $\forall m$.

C. Solution of The Follower Game

First, it can be observed that problem (10) is convex with respect with p_m for given values of λ and θ. Thus, the solution of (10) is immediately obtained by setting the derivative w.r.t. p_m to zero as follows:

$$p_m^{\text{opt}} = \begin{cases} \frac{\lambda\|\mathbf{g}_m\|^2 - B_m}{2A_m}, & \lambda > \frac{B_m}{\|\mathbf{g}_m\|^2} \\ 0, & \lambda \leq \frac{B_m}{\|\mathbf{g}_m\|^2}. \end{cases} \tag{13}$$

Based on (13), we can deduce the following remark:

Remark 1: From (13), it is observed that the optimal power allocation p_m^{opt} can only be obtained (i.e., solution p_m is positive) under the condition that the energy price λ is greater than threshold $\frac{B_m}{\|\mathbf{g}_m\|^2}$. Thus, in order to guarantee the sufficient energy harvested by the transmitter, we divide these PBs into two sets, namely, the active PB set and the non-active PB set. The PBs who can transfer the energy to the transmitter and help determine the achievable secrecy rate by using the harvested energy are called the active PB set, who satisfies the first equation in (13). The remaining ones are the non-active PB set (i.e., their power p_m^{opt} is zero). In our paper, we assume that from M available PBs there are $\bar{M}$ active PBs ($\bar{M} \leq M$). Hereafter, we consider this set of active PBs only and re-index the mth PB to be one of this set (i.e., $m = 1, 2, \cdots, \bar{M}$).

D. Solution of The Leader Game

By exploiting *Remark* 1, we replace p_m in (7) with (13), so that problem (7) becomes

$$\max_{\lambda,\theta,\mathbf{v}} \mu(1-\theta)\left[\min_k \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{s,k}^H\mathbf{v}|^2}{(1-\theta)\sigma_s^2}\right] - \max_l \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{e,l}^H\mathbf{v}|^2}{(1-\theta)\sigma_e^2}\right]\right] - \lambda\theta\sum_{m=1}^{\bar{M}} p_m\|\mathbf{g}_m\|^2$$
$$s.t.\ 0<\theta<1,\ \lambda\geq 0. \tag{14}$$

The problem is not convex in terms of normalized transmit beamfoming vector $\mathbf{v}$, the energy transfer price λ, and the energy time allocation θ, which cannot be solved directly.

1) Solution for Transmit Beamforming Vector: Thus, for given λ and θ, we first achieve the optimal solution for $\mathbf{v}$ by solving the following optimization problem:

$$\max_{\mathbf{v}} \ \min_k \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{s,k}^H\mathbf{v}|^2}{(1-\theta)\sigma_s^2}\right] - \max_l \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{e,l}^H\mathbf{v}|^2}{(1-\theta)\sigma_e^2}\right],$$
$$s.t.\ \|\mathbf{v}\|^2\leq 1. \tag{15}$$

Problem (15) is not convex due to its objective function. In order to circumvent this issue, we relax this problem as

$$\max_{\mathbf{w},R}\ R,$$
$$s.t.\ \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{s,k}^H\mathbf{w}|^2}{(1-\theta)\sigma_s^2}\right] - \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{e,l}^H\mathbf{w}|^2}{(1-\theta)\sigma_e^2}\right]\geq R,\ \ \forall\ (k,l),$$
$$\|\mathbf{w}\|^2\leq P, \tag{16}$$

where $\mathbf{w}=\sqrt{P}\mathbf{v}$, $P=\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2$. Problem (16) is still non-convex and, thus, is not likely to be solved efficiently. To make the problem tractable, we first decompose (16) into a sequence of following minimization problems, one for each target rate $R>0$:

$$\min_{\mathbf{w}}\ \|\mathbf{w}\|^2,$$
$$s.t.\ \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{s,k}^H\mathbf{w}|^2}{(1-\theta)\sigma_s^2}\right] - \log\left[1+\frac{\theta(\sum_{m=1}^{\bar{M}} p_m^{\text{opt}}\|\mathbf{g}_m\|^2)|\mathbf{h}_{e,l}^H\mathbf{w}|^2}{(1-\theta)\sigma_e^2}\right]\geq R,\ \ \forall\ (k,l). \tag{17}$$

Problem (17) can be reformulated as

$$\min_{\mathbf{w}}\ \|\mathbf{w}\|^2$$
$$s.t.\ \log\left(1+\frac{|\mathbf{h}_{s,k}^H\mathbf{w}|^2}{\bar{\sigma}_s^2}\right) - \log\left(1+\frac{|\mathbf{h}_{e,l}^H\mathbf{w}|^2}{\bar{\sigma}_e^2}\right)\geq R,\ \ \forall\ (k,l), \tag{18}$$

where $\bar{\sigma}_s^2 = \frac{(1-\theta)\sigma_s^2}{\theta}$, $\bar{\sigma}_e^2 = \frac{(1-\theta)\sigma_e^2}{\theta}$.

Algorithm 1: Bisection method

1) Choose $\varepsilon > 0$ (termination parameter), R_{lb} and R_{ub} such that R^{opt} lies in $[R_{lb}, R_{ub}]$;
2) $R = (R_{lb} + R_{ub})/2$;
3) Check the feasibility of problem (18) with R. If infeasible, let $R_{ub} = R$, and go to step 4; otherwise, go to step 5.
4) Check $\|\mathbf{w}\|^2 \leq P$. If it is satisfied, set $R_{lb} = R$; otherwise, $R_{ub} = R$;
5) Until $R_{ub} - R_{lb} \leq \varepsilon$; else go to step 2.

Obviously, the optimal objective value of the problem (17) is monotonically increasing with respect to R. Thus, by solving problem (17) with different R and using a bisection search over R as described in Algorithm 1, the optimal secrecy rate R and the associated normalized transmit beamforming vector $\mathbf{v}$ can be obtained. Therefore, we will focus on solving (17) in the following.

The problem (18) is not convex in terms of $\mathbf{w}$, and still cannot be solved efficiently. In order to circumvent this non-convex issue, we introduce a new rank-one semidefinite matrix $\mathbf{Q}_s = \mathbf{w}\mathbf{w}^H$. By relaxing the rank-one constraint, we can arrive at the following convex relaxation:

$$\begin{aligned} &\min_{\mathbf{Q}_s \succeq \mathbf{0}} \ \text{Tr}(\mathbf{Q}_s), \\ &s.t. \ \frac{1}{\sigma_s^2}\text{Tr}(\mathbf{h}_{s,k}\mathbf{h}_{s,k}^H\mathbf{Q}_s) - \frac{2^R}{\sigma_e^2}\text{Tr}(\mathbf{h}_{e,l}\mathbf{h}_{e,l}^H\mathbf{Q}_s) \geq 2^R - 1, \ \forall (k,l). \end{aligned} \tag{19}$$

The above problem is convex by dropping the non-convex constraint $\text{rank}(\mathbf{Q}_s) = 1$ and can be solved by using interior-point methods [41]. It is not always possible to expect that the optimal solution of (19) attains the optimum of the original problem (18). However, the SDP relaxation is tight if the optimal solution of (19) has rank one. The rank of the solution of (19) is characterized by the following result:

Proposition 1: [38, Theorem 1] Provided the problem (19) is feasible, the optimal solution of (19) must satisfy the following rank inequality:

$$\text{rank}(\mathbf{Q}_s) \leq \min(K, \sqrt{KL}) \tag{20}$$

With *Proposition* 1, we are able to identify the tightness of SDP relaxed solution via the following *lemma*

Lemma 1: [38, Corollary 1] Provided the problem (19) feasible, it is guaranteed that (19) can yield a rank-one solution which exactly solves the problem (18) when either one of the two following conditions is satisfied:

1) $K = 1$ and $L \geq 1$.
2) $1 < K \leq 3$, and $L = 1$.

By exploiting *Proposition* 1 and *Lemma* 1, if $\text{rank}(\mathbf{Q}_s)$ satisfies the rank-one condition in *Lemma* 1, we can employ the eigen-decomposition for $\mathbf{Q}_s$ to obtain the optimal transmit beamformer $\mathbf{w}$. Otherwise, we need to use a rank reduction algorithm to tackle this problem [47]. However, when the rank-one condition in *Lemma* 1 is satisfied, we can also consider the following *theorem* to directly solve the problem (18).

Theorem 1: The problem (18) can be reformulated as the following convex optimization when the rank-one condition in *Lemma* 1 is satisfied.

$$\begin{aligned} &\min_{t\geq 0,\mathbf{w}} \quad t, \\ &s.t. \quad \begin{bmatrix} t \\ \mathbf{w} \end{bmatrix} \succeq_{K_{(N_T+1)}} \mathbf{0}, \quad \begin{bmatrix} \frac{1}{\bar{\sigma}_s}\mathbf{w}^H\mathbf{h}_{s,k} \\ \frac{2^{\frac{R}{2}}}{\bar{\sigma}_e}\mathbf{w}^H\mathbf{h}_{e,l} \\ (2^R-1)^{\frac{1}{2}} \end{bmatrix} \succeq_{K_3} \mathbf{0}, \quad \forall \ (k,l). \end{aligned} \tag{21}$$

Proof: The proof can be obtained by using the generalized cone inequality $\begin{bmatrix} a \\ \mathbf{b} \end{bmatrix} \succeq_{K_n} \mathbf{0} \Leftrightarrow \|\mathbf{b}\| \leq a.$ ■

By exploiting *Theorem* 1, it is verified that (21) is a convex optimization problem, which can be solved by using interior-point methods [41]. Thus, the optimal normalized transmit beamforming vector $\mathbf{v}^{\text{opt}}$ can be easily achieved. Now, we consider the computation complexity of solving problem (21). According to the analysis of the basic complexity elements in [48], problem (21) includes one second-order cone (SOC) constraint with dimension N_T+1, KL SOC constraints with dimension N_T, and one linear constraint. Thus, its computation complexity can be given by $\mathcal{O}\left(\sqrt{2KL+3}n[KLN_T^2+(N_T+1)^2+1+n^2]\right)\ln(\frac{1}{\epsilon})$, where $n=\mathcal{O}(N_T+1)$, and $\epsilon>0$ denotes the accuracy requirement.

A special case: Consider the case with a single legitimate user and a single eavesdropper only. The closed-form solution can be derived by exploiting Lagrange dual problem and Karush-Kuhn-Tucker (KKT) conditions[2]. For notational convenience, we replace the channel notations $\mathbf{h}_{s,k}$ and $\mathbf{h}_{e,l}$ by $\mathbf{h}_s$ and $\mathbf{h}_e$, respectively. The following *lemma* is introduced:

Lemma 2: The optimal solution to (18) with only single legitimate user and single eavesdropper is given by

$$\begin{aligned} &\mathbf{w}^{\text{opt}} = \sqrt{P^{\text{opt}}}\mathbf{v}^{\text{opt}}, \ \mathbf{v}^{\text{opt}} = \frac{\bar{\mathbf{w}}}{\|\bar{\mathbf{w}}\|_2}, \ \bar{\mathbf{w}} = v_{\max}(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H), \\ &P^{\text{opt}} = \alpha^{\text{opt}}(2^R-1), \ \alpha^{\text{opt}} = \frac{1}{\varrho_{\max}(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H)}. \end{aligned} \tag{22}$$

Proof: See Appendix A. ■

[2]For this special case, a related work in [49] aimed at maximizing the secrecy rate subject to a transmit power constraint, in which the optimal beamforming vector is obtained based on Rayleigh quotient approach. Our work obtained a closed-form solution of the joint design of the optimal time allocation and the optimal transmit beamforming vector via the dual problem and the KKT condition. Note that our work can also be extended to the problem of minimization of the transmitter's transmit power.

Now, a natural question is how to tackle problem (18) when the rank-one condition of *Lemma* 1 is not satisfied. For this scenario, SDP relaxed method may result in poor performance or even fail to obtain the optimal beamforming vector when SDP relaxed method returns high-rank solutions. This phenomenon is very common in multicast scenario even without security constraint [1]. For this purpose, we consider an SCA based scheme to reformulate the problem (18) for any general case, yielding an SOCP. We equivalently rewrite the problem (18) by introducing a new set of variables $(x_{s,k}, y_{s,k}, b_{s,k}),\ \forall k$ as

$$\min_{\mathbf{w}, b_{s,k}} \ \|\mathbf{w}\|^2,$$

$$s.t.\ x_{s,k}^2 + y_{s,k}^2 \geq b_{s,k}, \tag{23a}$$

$$(2^R-1)\bar{\sigma}_s^2 + \frac{2^R\bar{\sigma}_s^2}{\bar{\sigma}_e^2}|\mathbf{w}^H\mathbf{h}_{e,l}|^2 \leq b_{s,k}, \tag{23b}$$

$$x_{s,k} = \Re\left\{\mathbf{w}^H\mathbf{h}_{s,k}\right\},\ y_{s,k} = \Im\left\{\mathbf{w}^H\mathbf{h}_{s,k}\right\}, \tag{23c}$$

where $(x_{s,k}, y_{s,k}, b_{s,k}) \in \mathbb{R}$, $\forall k$ In the above reformulation, it is observed that both constraint (23a) and (23b) are still not convex while (23c) are linear constraints. In order to further process these non-convex constraints, we first introduce iterative successive approximation methods to tackle (23a). Specifically, set $\mathbf{q}_{s,k} = [x_{s,k}\ y_{s,k}]^T$, and denote the value of this vector at the n-th iteration as $\mathbf{q}_{s,k}^{(n)}$. We consider the first-order Taylor series to approximate the left hand side of (23a) as

$$x_{s,k}^2 + y_{s,k}^2 = \mathbf{q}_{s,k}^T\mathbf{q}_{s,k} \approx \|\mathbf{u}_{s,k}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}_{s,k}^{(n)}(i)[\mathbf{q}_{s,k}(i) - \mathbf{u}_{s,k}^{(n)}(i)], \tag{24}$$

where the parameter vector $\mathbf{u}_{s,k}^{(n)}(i)$ can be updated $\mathbf{u}_{s,k}^{(n+1)} = \mathbf{q}_{s,k}^{(n)},\ \forall k$ at the $(n+1)$-th iteration, and $\mathbf{q}_{s,k}(i)$ denotes the ith element of $\mathbf{q}_{s,k}$. It depends on the optimization variables obtained as a solution to (23) at n-th iteration. Thus, (24) can be given by

$$\|\mathbf{u}_{s,k}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}_{s,k}^{(n)}(i)[\mathbf{q}_{s,k}(i) - \mathbf{u}_{s,k}^{(n)}(i)] \geq b_{s,k}. \tag{25}$$

To proceed, the constraint (23b) can be equivalently reformulated into the following SOC constraint

$$\left\|\begin{bmatrix}(2^R-1)^{\frac{1}{2}}\bar{\sigma}_s \\ \frac{2^{\frac{R}{2}}\bar{\sigma}_s}{\bar{\sigma}_e}\mathbf{w}^H\mathbf{h}_{e,l}\end{bmatrix}\right\|^2 \leq b_{s,k} \Rightarrow \left\|\begin{bmatrix}(2^R-1)^{\frac{1}{2}}\bar{\sigma}_s \\ \frac{2^{\frac{R}{2}}\bar{\sigma}_s}{\bar{\sigma}_e}\mathbf{w}^H\mathbf{h}_{e,l} \\ \frac{(b_{s,k}-1)}{2}\end{bmatrix}\right\| \leq \frac{(b_{s,k}+1)}{2}. \tag{26}$$

Remark 2: The convexity of the term $\mathbf{q}_{s,k}^T\mathbf{q}_{s,k}$ and the first-order Taylor approximation ensures that the right hand side in (24) bounds the left side in each iterative procedure. In other words, the optimal solution of the problem with the approximated constraint in (24) definitely belongs to the feasible set of the original optimization problem at each iteration. Also, due to the above update, the approximation in (24) holds with equality at the $(n+1)$-th iteration. In addition, the gradients of both sides in (24) (i.e., left hand side $x_{s,k}^2 + y_{s,k}^2$ or $\mathbf{q}_{s,k}^T\mathbf{q}_{s,k}$, and right hand side $\|\mathbf{u}_{s,k}^{(n)}\|^2 + 2\sum_{i=1}^{2}\mathbf{u}_{s,k}^{(n)}(i)[\mathbf{q}_{s,k}(i) - \mathbf{u}_{s,k}^{(n)}(i)]$) with respect to $\mathbf{q}_{s,k}$ are the same at the $(n+1)$-th iteration, which shows that this approximation algorithm converges to a KKT point, and the solution of the iterative procedure satisfies the KKT conditions [50, Theorem 1].

By exploiting *Remark* 2, the problem (18) takes the following form at the n-th iteration

$$\begin{aligned} &\min_{\mathbf{w}, b_{s,k}} \ \|\mathbf{w}\|^2, \\ &s.t. \ (25), (26), (23\text{c}), \ \forall (k,l). \end{aligned} \tag{27}$$

Based on the above discussion, an iterative algorithm to solve the problem in (18) is summarized in **Algorithm** 2.

Algorithm 2: Successive convex approximation to solve (18)

---

1) **Initialization**: Randomly generate $\mathbf{u}_{s,k}^{(0)}, \ \forall k$ to make (27) feasible
2) **Repeat**
   a) **Solve** (27).
   b) **Set** $\mathbf{u}_{s,k}^{(n+1)} = \mathbf{q}_{s,k}^{(n)}, \forall k$.
   c) **Set** $n := n + 1$.
3) **Until** required accuracy is achieved or the maximum number of iterations is reached.

From **Algorithm** 2, the initialized vector $\mathbf{u}_{s,k}$ is given by random generation to guarantee the feasibility of (27), which can be updated at each iteration until $\mathbf{u}_{s,k}^{(n+1)} = \mathbf{q}_{s,k}^{(n)}$ holds when the algorithm converges. Now, we claim that **Algorithm** 2 is guaranteed to converge. The optimization variables $\mathbf{w}$, $x_{s,k}$ and $y_{s,k}$, for all k belong to both $\mathcal{S}^{(n)}$ and $\mathcal{S}^{(n+1)}$, where $\mathcal{S}^{(n)}$ is the feasible set of optimization problem at n-th iteration. Therefore, $f_{\mathcal{S}}^{(n)} \geq f_{\mathcal{S}}^{(n+1)}$, where $f_{\mathcal{S}}^{(n)}$ is the objective function at n-th iteration. Since the feasible set of (27) is convex and compact, this iterative procedure converges to a locally optimum solution [40].

2) Solution for The Energy Price and Energy Time Allocation: In previous subsection, we exploit the optimal solution for the transmit beamforming vector $\mathbf{v}$. In this subsection, we solve for the optimal solution to the energy price λ and the energy transfer time allocation θ only in leader level game (14) for given $\mathbf{v}$, which is written as

$$\max_{\lambda,\theta}\ \mu(1-\theta)\left[\min_{k}\log\left[1+\left(\lambda\sum_{m=1}^{\bar{M}}\frac{\|\mathbf{g}_m\|^4}{2A_m}-\sum_{m=1}^{\bar{M}}\frac{B_m\|\mathbf{g}_m\|^2}{2A_m}\right)t_s\right]\right.$$
$$\left.-\min_{l}\log\left[1+\left(\lambda\sum_{m=1}^{\bar{M}}\frac{\|\mathbf{g}_m\|^4}{2A_m}-\sum_{m=1}^{\bar{M}}\frac{B_m\|\mathbf{g}_m\|^2}{2A_m}\right)t_e\right]\right]$$
$$-\theta\lambda^2\sum_{m=1}^{\bar{M}}\frac{\|\mathbf{g}_m\|^4}{2A_m}+\theta\lambda\sum_{m=1}^{\bar{M}}\frac{B_m\|\mathbf{g}_m\|^2}{2A_m}$$
$$s.t.\ 0<\theta<1,\ \lambda\geq 0 \tag{28}$$

where

$$t_s=\min_{k}t_{s,k}=\min_{k}\frac{\theta|\mathbf{h}_{s,k}^H\mathbf{v}|^2}{(1-\theta)\sigma_s^2},\ \forall k,\ t_e=\max_{l}t_{e,l}=\min_{l}\frac{\theta|\mathbf{h}_{e,l}^H\mathbf{v}|^2}{(1-\theta)\sigma_e^2},\ \forall l.$$

The problem (28) is not jointly convex in terms of θ and λ. It is extremely hard to find their optimal solutions simultaneously due to the complexity of the objective function in (28). In order to address this issue, we first derive the closed-form solution for the optimal λ with a given value θ. Then, the optimal value for θ can be achieved through numerical analysis. In order to derive the closed-form solution of λ, we set $C_M=\sum_{m=1}^{\bar{M}}\frac{\|\mathbf{g}_m\|^4}{2A_m}$, $D_M=\sum_{m=1}^{\bar{M}}\frac{B_m\|\mathbf{g}_m\|^2}{4A_m}$, and the objective function to (14) can be expressed as

$$U_M(\theta,\lambda)=\mu(1-\theta)\left[\log\left[1+\left(\lambda C_M-2D_M\right)t_s\right]-\log\left[1+\left(\lambda C_M-2D_M\right)t_e\right]\right]$$
$$-\theta\lambda^2C_M+2\theta\lambda D_M. \tag{29}$$

Lemma 3: (29) is a concave function with respect to λ.

Proof: See Appendix B. ■

By exploiting *Lemma* 3, we can claim that (14) is a convex problem. Now, we derive the closed-form solution of λ. In order to obtain the optimal solution to λ, let the first order derivative of (29) equate to zero, we have

$$\frac{\mu(1-\theta)t_sC_M}{1+(\lambda C_M-D_M)t_s-D_Mt_s}-\frac{\mu(1-\theta)t_eC_M}{1+(\lambda C_M-D_M)t_e-D_Mt_e}-2\theta C_M\lambda+2\theta D_M=0. \tag{30}$$

Set $x=\lambda C_M-D_M$, and after a few of mathematical simplifications, we arrive at

$$x^3+ax^2+bx+c=0, \tag{31}$$

where

$$a=\frac{(t_s+t_e)-2D_Mt_st_e}{t_st_e},\ b=\frac{(D_Mt_s-1)(D_Mt_e-1)}{t_st_e},\ c=-\mu(1-\theta)C_M(t_s-t_e).$$

It is easily observed that (31) is a cubic equation, which can be solved in terms of closed-form solution of x by using Cardano's formula [51],

$$x^{\text{opt}} = e^{j\angle x_1}\sqrt[3]{|x_1|} + e^{j\angle x_2}\sqrt[3]{|x_2|} - a/3, \tag{32}$$

where $\angle$ denotes the phase angle of an complex random variable, and

$$x_1 = -\frac{q}{2} + \sqrt{\Delta},\ x_2 = -\frac{q}{2} - \sqrt{\Delta},$$
$$\Delta = \frac{p^3}{27} + \frac{q^2}{4},\ p = -\frac{a^2}{3} + b,\ q = \frac{2a^3}{27} - \frac{ab}{3} + c.$$

Thus, we obtain the optimal energy price as

$$\lambda^{\text{opt}} = \frac{x^{\text{opt}} + D_M}{C_M}. \tag{33}$$

We have already obtained the optimal energy price of the transmitter for a given θ. Now, the optimal energy transfer time allocation is derived in the following. We substitute the closed-form expression (33) into (29), thus, the following optimization problem can be written with respect to θ,

$$\max_{\theta}\ U_M(\theta, \lambda^{\text{opt}}) = \mu(1-\theta)\left[\log\left(1 + \frac{\theta}{1-\theta}\bar{t}_s\right) - \log\left(1 + \frac{\theta}{1-\theta}\bar{t}_e\right)\right] - \theta\Psi,$$
$$s.t.\ 0 < \theta < 1, \tag{34}$$

where

$$\bar{t}_s = \frac{\Phi \min_k |\mathbf{h}_{s,k}^H \mathbf{v}|^2}{\sigma_s^2},\ \bar{t}_e = \frac{\Phi \max_l |\mathbf{h}_{e,l}^H \mathbf{v}|^2}{\sigma_e^2},$$
$$\Phi = \lambda^{\text{opt}} \sum_{m=1}^{\bar{M}} \frac{\|\mathbf{g}_m\|^4}{2A_m} - \sum_{m=1}^{\bar{M}} \frac{B_m \|\mathbf{g}_m\|^2}{2A_m},\ \Psi = (\lambda^{\text{opt}})^2 \sum_{m=1}^{\bar{M}} \frac{\|\mathbf{g}_m\|^4}{2A_m} - \lambda^{\text{opt}} \sum_{m=1}^{\bar{M}} \frac{B_m \|\mathbf{g}_m\|^2}{2A_m}. \tag{35}$$

Now, we show that the problem (34) is a convex optimization problem with respect to θ for given $\mathbf{v}$ and λ^{opt} via the following *lemma*:

Lemma 4: (34) is a convex problem with respect to θ.

Proof: See Appendix C. ■

By exploiting *Lemma* 4, the problem (34) can be efficiently handled by using 1D search to obtain the optimal energy transfer time solution θ^{opt} as follows:

$$\theta^{\text{opt}} = \arg \max_{\theta \in (0,1)} U_M(\theta, \lambda^{\text{opt}}). \tag{36}$$

We have completed the derivation of the *Stackelberg* equilibrium $(p_m^{\text{opt}}, \lambda^{\text{opt}}, \theta^{\text{opt}})$ for the formulated *Stackelberg* game, which are shown in (13), (32) and (36).

IV. Numerical Results

In this section, we provide the simulation results to validate the proposed schemes. We consider the secure multiantenna multicasting system that consists of three legitimate receivers (i.e., $K = 3$) and two eavesdroppers ($L = 5$), where the transmitter is wirelessly powered by five PBs ($M = 5$). It is assumed that the transmitter is equipped with eight transmit antennas (i.e., $N_T = 8$), whereas the others consist of single antenna. We employ the path loss channel model $\sqrt{Ad_x^{-\alpha}}$ [52], [53], where $A = 10^{-3}$. The path loss exponent is set to $\alpha = 3$. Distance variable d_x can be replaced with d_s, d_e, and d_{PB} according to different channel coefficients, representing the distance between the transmitter and the legitimate users, the eavesdroppers as well as the PBs, respectively. In our simulation, we choose $d_s = d_e = 2$ m, and $d_{PB} = 5$ m unless specified. The target secrecy rate is set to be $R = 2$ bps/Hz. The noise powers at the legitimate users and the eavesdroppers are set as $\sigma_s^2 = \sigma_e^2 = 10^{-8}$ mW.

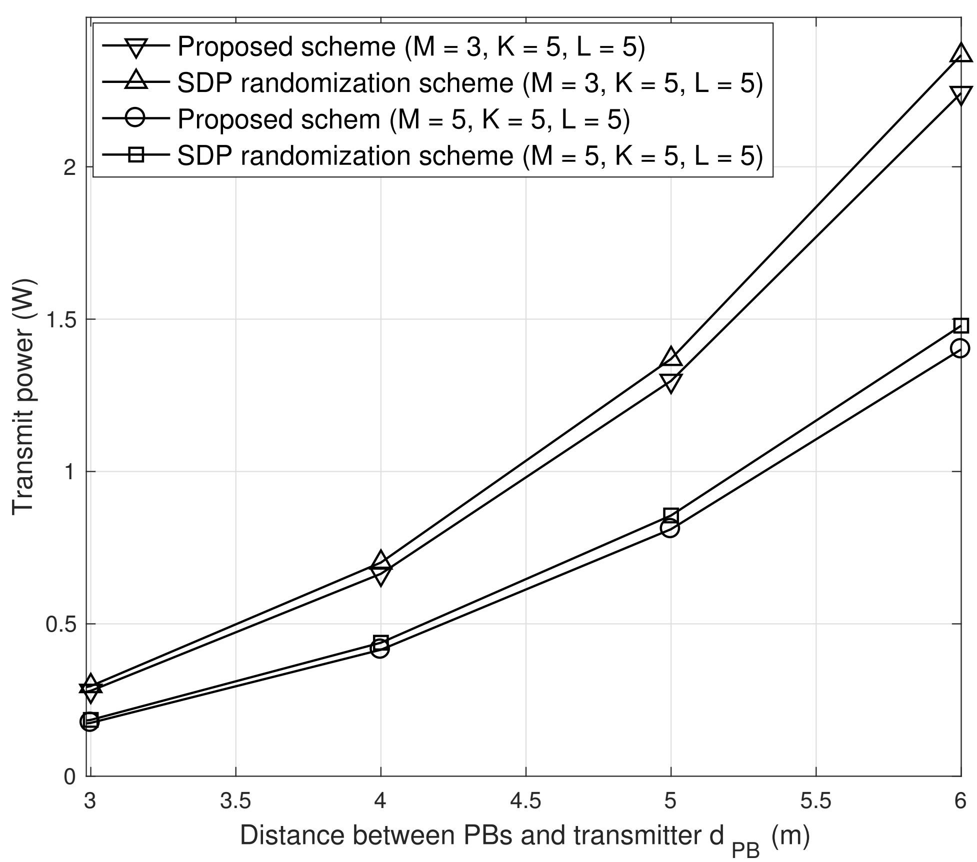

Fig. 2: Comparison of transmit power between the proposed scheme and SDP scheme versus distance between PBs and transmitter.

First, we evaluate the leader game and particularly problem (17) where we can achieve the minimized transmit power against the distance between PBs and the transmitter (i.e., d_{PB}). Fig. 2 shows the result in

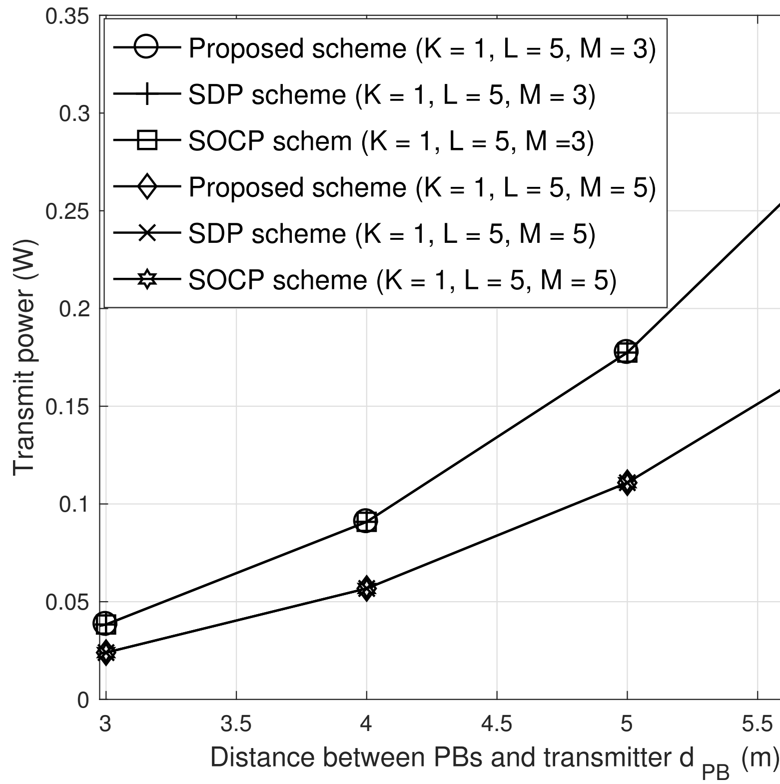

Fig. 3: Comparison of transmit power between the SOCP and SDP schemes versus distance between PBs and transmitter.

general case where the rank-one condition in *Lemma* 1 is not satisfied. One can observe that our proposed SCA scheme slightly performs better than the SDP randomization scheme[3] in [39]. This is owing to the fact that our proposed scheme can achieve an optimal solution via **Algorithm** 2, whereas the relaxed solution for the SDP randomization scheme may not achieve the optimality, which highlights the advantage of our proposed SCA scheme. However, in the case of the rank-one condition being satisfied, Fig. 3 shows that the SOCP yields the same performance as that of the proposed SCA scheme and the SDP scheme, which validates the correctness of *Theorem* 1. Fig. 4 shows the impact of the energy time allocation. From this figure, we observe that the proposed SOCP scheme with the fixed time allocation (i.e., $\theta = 0.5$) obviously requires more transmit power than the proposed SOCP scheme with optimal energy time allocation. This is owing to a fact that our proposed scheme can achieve an optimal energy time allocation by numerical search (i.e., $\theta = \theta^{\rm opt}$). Similar behaviors are observed in Fig. 5 which is obtained for the special case of single user and single eavesdropper. This figure shows that the derived closed-form solution in *Lemma* 2 matches well with the numerical results obtained from a convex optimization tool, which validates the accuracy of this closed-form solution.

[3]Randomization techniques can be used to construct a rank-one solution to tackle the non rank-one SDP relaxed solution [1], which is a feasible solution.

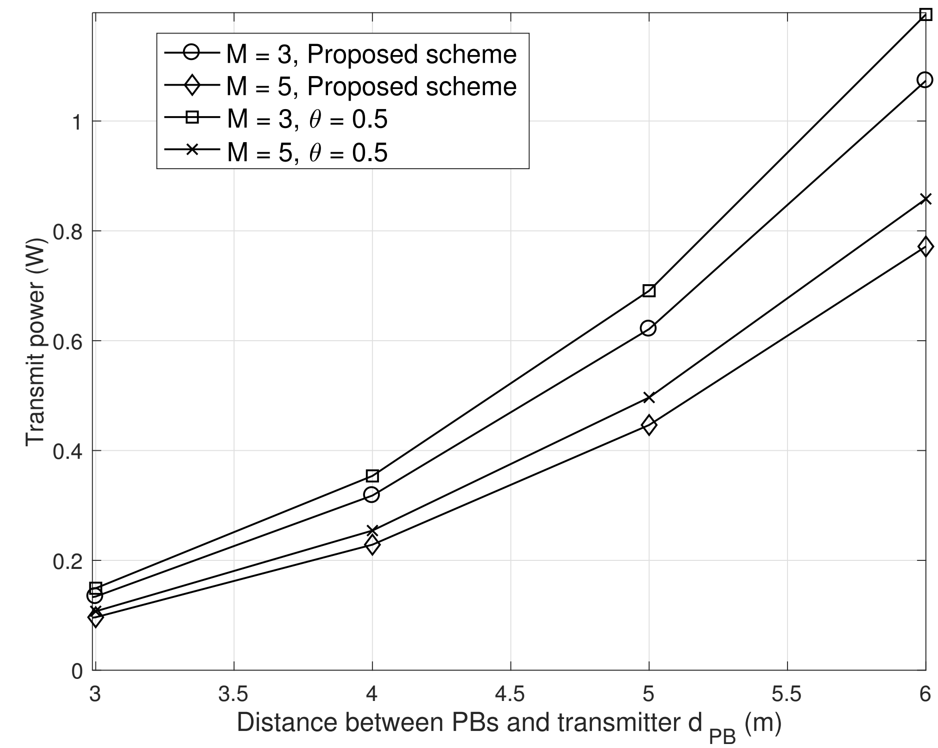

Fig. 4: Comparison of transmit power between the proposed scheme with optimal θ and fixed θ versus distance between PBs and transmitter.

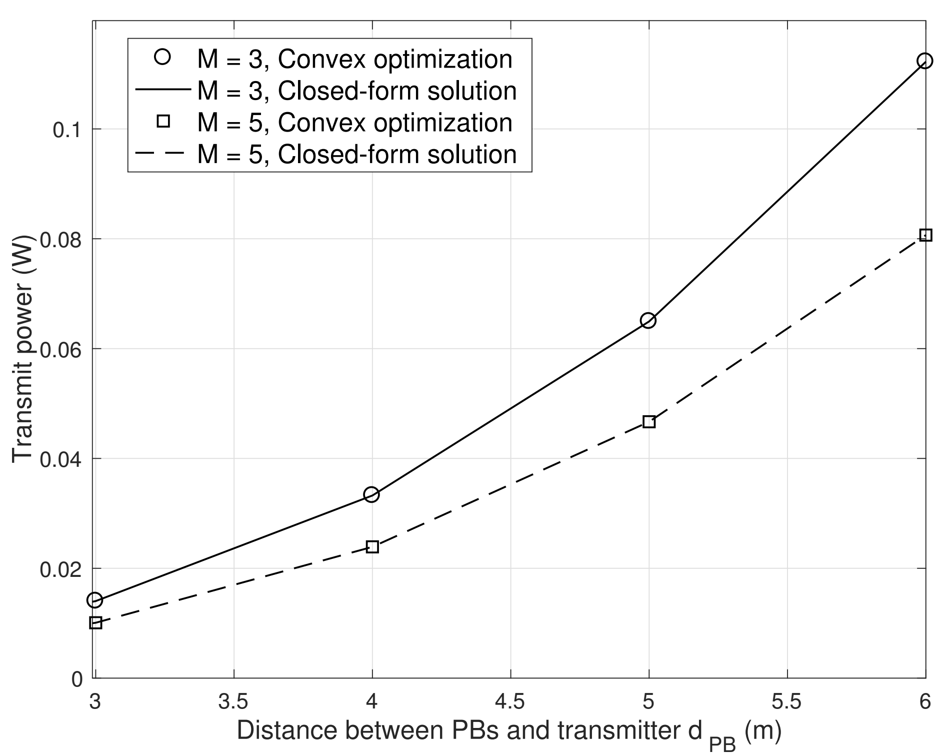

Fig. 5: Transmit power versus distance between PBs and transmitter with special case.

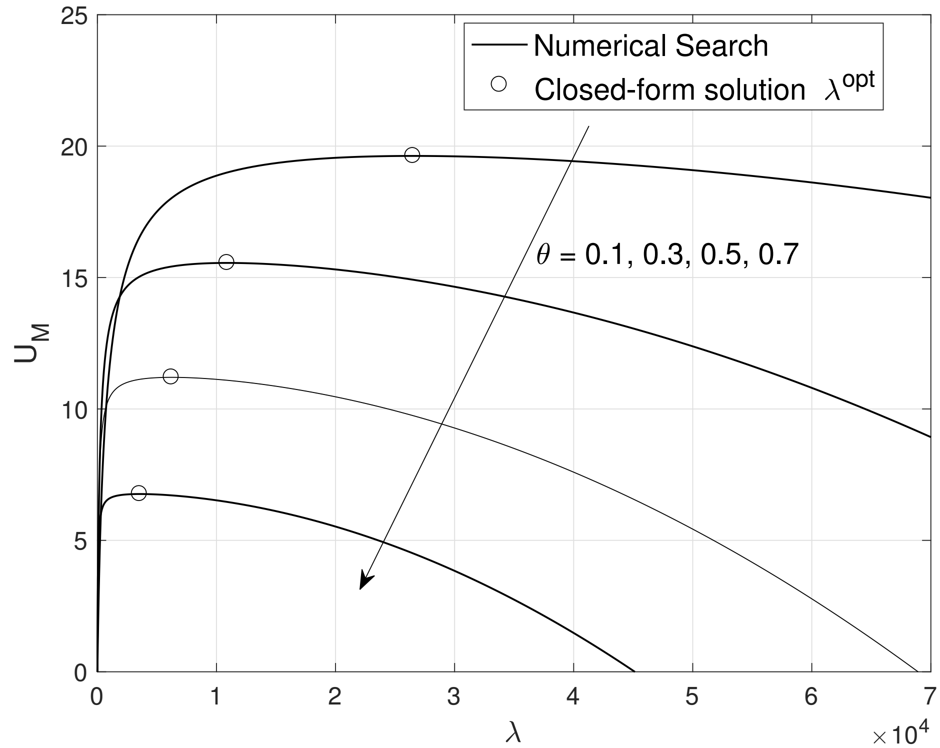

Fig. 6: The utility function of transmitter U_M versus energy transfer price λ

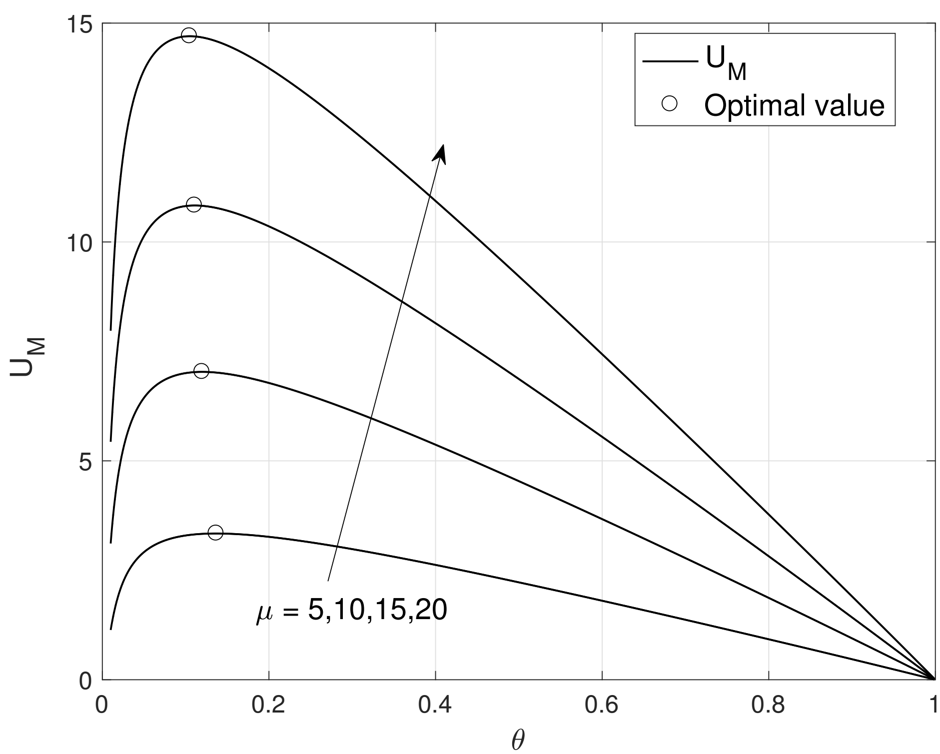

Fig. 7: The utility function of transmitter U_M versus energy transfer time allocation θ

Next, we validate the equilibrium of the proposed *Stackelberg* game. In order to support the derived *Stackelberg* equilibrium, we first evaluate the utility function of the transmitter versus the energy transfer price λ with a fixed energy transfer time allocation θ in Fig. 6. From this figure, it is observed that the revenue function is concave, which validates the proof of convexity shown in *Lemma* 3. In this figure, it also can be shown that the optimal utility function of the transmitter can be obtained via optimal energy transfer price λ^{opt} in (33) and it matches the numerical search with different given θ, which confirms the optimal closed-form solution of the energy transfer price λ. Also, as θ increases, the utility function of the legitimate transmitter is decreasing, and the optimal value λ shifts to the left. In addition, the revenue function of the transmitter versus energy transfer time allocation (i.e., θ) with optimal energy price λ^{opt} is shown in Fig. 7. From this figure, it is shown that the revenue function is concave with respect to θ, which validates (36). Moreover, there exists a optimal utility transfer time (i.e., θ^{opt}) via numerical search with the optimal energy price. As μ increases, the optimal value slightly shifts to the left.

Then, we evaluate the transmitter revenue function performance of the proposed *Stackelberg* game. Fig. 8 and Fig. 9 show the revenue function of the transmitter versus the number of PBs. From both figures, we can observe that this utility is improved with increasing of the number of PBs and μ. From

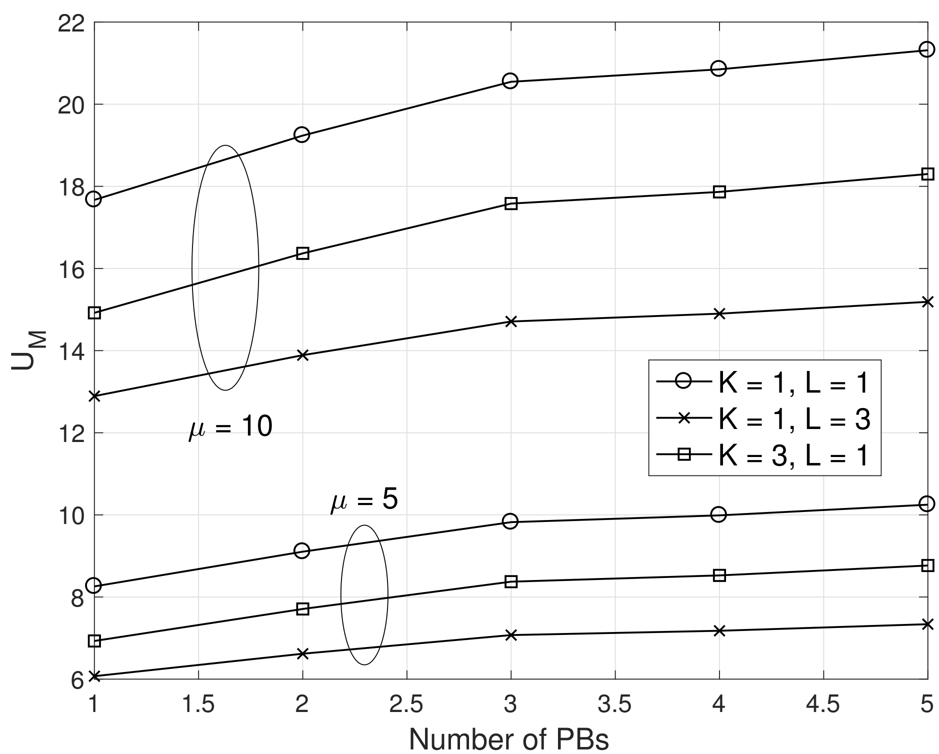

Fig. 8: The utility function of transmitter U_M versus No. of PBs with different number of legitimate users and eavesdroppers

Fig. 8, increasing the number of the eavesdroppers can have more significant impact on the revenue than increasing the number of the legitimate users. In Fig. 9, the revenue is decreased when the distance between the source and PBs is increased from 5m to 6.5m. This is because the nearer the PBs to the transmitter, the higher the transferred energy efficiency between them, which reduces the transmitter's payments to the PBs for their wireless energy services. Fig. 10 shows the optimal energy transfer time θ

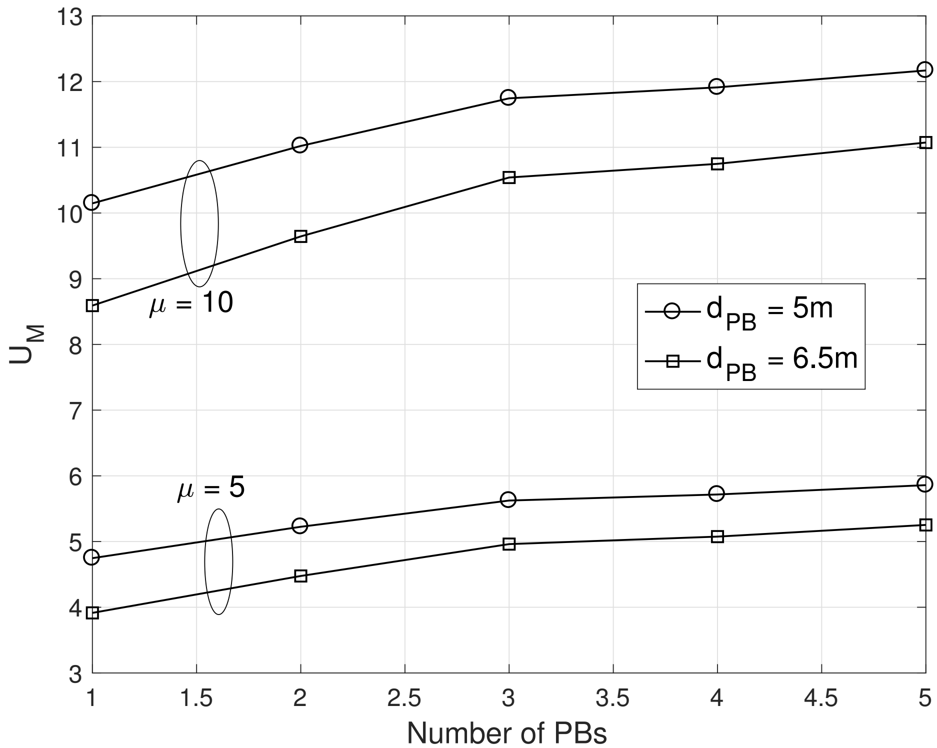

Fig. 9: The utility function of transmitter U_M versus No. of PBs with different d_{PB}

versus the number of PBs. It is observed that θ decreases as either the number of the PBs or μ increase. The same behavior is observed when the distance between the source and PBs (i.e., d_{PB}) decreases. Fig. 11 shows the optimal energy price versus the number of PBs. The price decreases as the number of PBs increases. Besides, the larger μ, the higher optimal energy price needs to be paid. It can also be seen from this figure that the decrease of the distance between the transmitter and PBs can also reduce the optimal energy price. This is because the shorter the distance between the source and PBs, the more energy harvested by the transmitter for the same power transmitted by the PBs, such that a lower energy price can be paid by the transmitter.

V. Conclusion and Future Work

In this paper, we developed an energy interaction framework for the PBs-assisted secure wireless-powered multiantenna multicasting system. Considering the strategic behaviours of the transmitter and

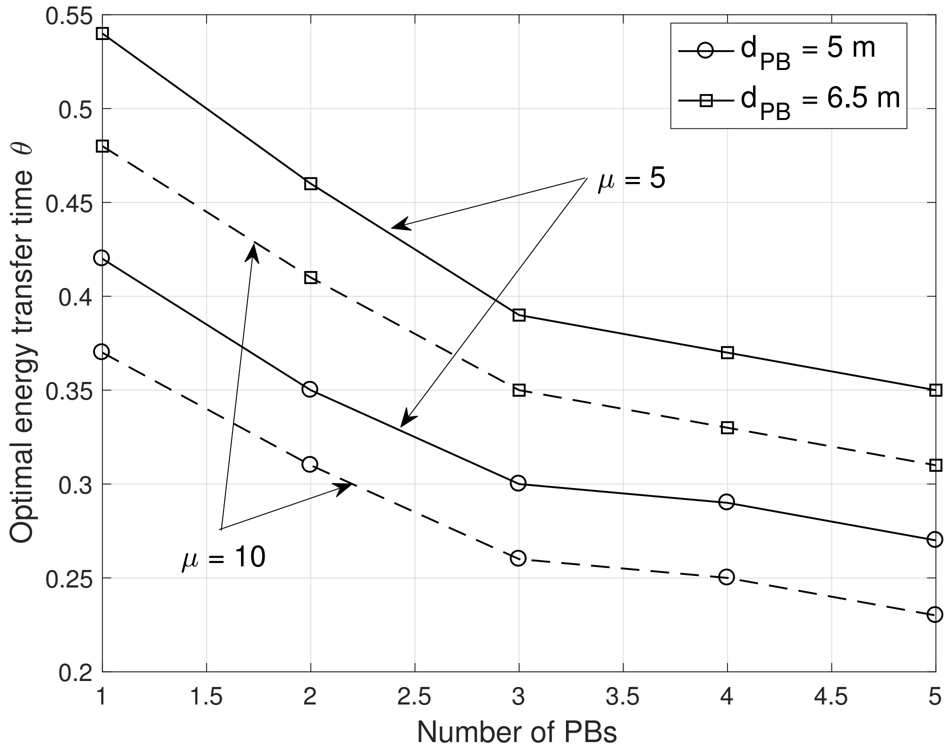

Fig. 10: Optimal energy transfer time allocation θ versus No. of PBs

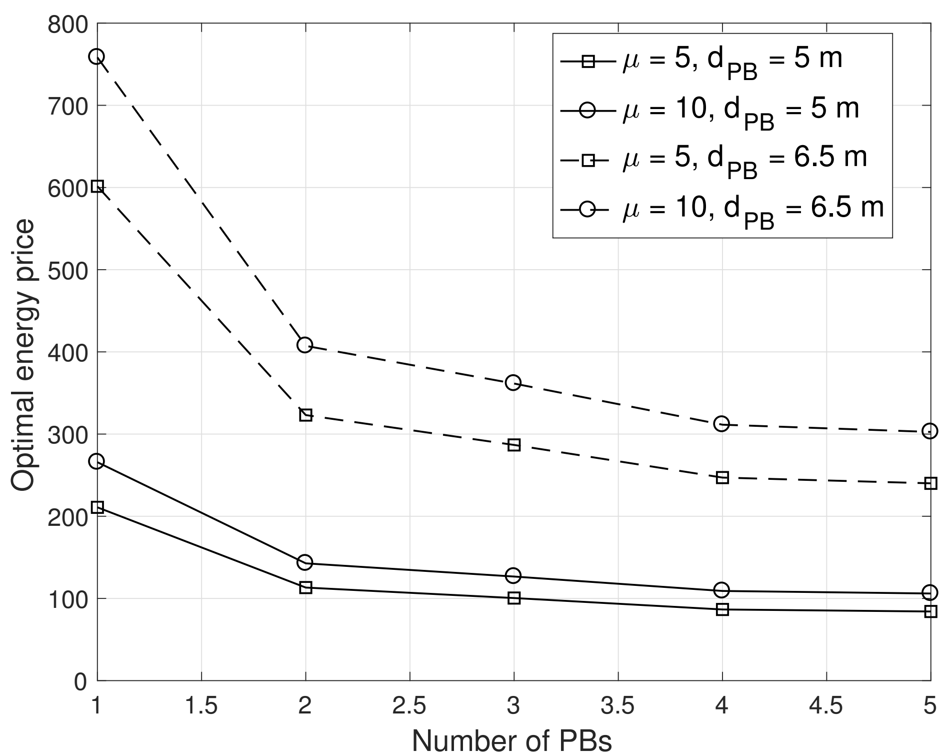

Fig. 11: The optimal energy price versus No. of PBs.

the PBs, we formulated this energy interaction as a *Stackelberg* game for the considered network, where the transmitter plays a leader role and pays a price for the energy services from the PBs to guarantee the required security, and optimizes the energy price and the energy transfer time to maximize its utility function. Meanwhile, the PBs are modelled as the followers that determine their optimal transmit powers based on the released energy price to maximize their own utility function. In addition, conic convex reformulation was proposed to achieve the optimal transmit beamforming vector for the leader game. The *Stackelberg* equilibrium have been derived in terms of closed-form solution, where both the transmitter and the PBs come to an agreement on the energy price, PB's transmit power and energy transfer time. Simulation results have been provided to validate the proposed schemes. For future works, we can consider a more challenging scenario such that the PBs will not stay silent during the wireless information transfer phase but rather transmit artificial noise to interfere with the eavesdroppers. This would change the dynamic of the optimization problems and may require different design/solutions.

APPENDIX

A. *Proof of* Lemma *2*

The power minimization problem (18) with only single legitimate user and eavesdropper can be rewritten as

$$\begin{aligned}&\min_{\mathbf{w}}\ \mathbf{w}^H\mathbf{w}\\ &s.t.\ \log\left(1+\frac{|\mathbf{h}_s^H\mathbf{w}|^2}{\bar{\sigma}_s^2}\right)-\log\left(1+\frac{|\mathbf{h}_e^H\mathbf{w}|^2}{\bar{\sigma}_e^2}\right)\geq R.\end{aligned} \tag{37}$$

Now we equivalently modify (37) as

$$\begin{aligned}&\min_{\mathbf{v},P}\ P\mathbf{v}^H\mathbf{v}\\ &s.t.\ \frac{\mathbf{v}^H(\mathbf{I}+\frac{P}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H)\mathbf{v}}{\mathbf{v}^H(\mathbf{I}+\frac{P}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H)\mathbf{v}}\geq 2^R,\ \mathbf{v}^H\mathbf{v}=1,\ P\geq 0.\end{aligned} \tag{38}$$

In order to achieve the optimal solution $(P^{\rm opt},\mathbf{v}^{\rm opt})$, we consider the Lagrange dual problem to (37), which can be expressed as

$$\mathcal{L}(\mathbf{w},\alpha)=\mathbf{w}^H\mathbf{w}+\alpha\left[2^R\left(1+\frac{1}{\bar{\sigma}_s^2}\mathbf{w}^H\mathbf{h}_e\mathbf{h}_e^H\mathbf{w}\right)-\left(1+\frac{1}{\bar{\sigma}_e^2}\mathbf{w}^H\mathbf{h}_s\mathbf{h}_s^H\mathbf{w}\right)\right], \tag{39}$$

where $\alpha\geq 0$ is the Lagrange multiplier associated with the secrecy rate constraint. The corresponding dual problem can be given by

$$\max_{\alpha\geq 0}\ \alpha(2^R-1),\ s.t.\ \mathbf{Y}=\mathbf{I}-\alpha\left(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H-\frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H\right)\succeq\mathbf{0}. \tag{40}$$

To proceed, we consider the following problem:

$$\min_{\mathbf{Q}_s} \; \text{Tr}(\mathbf{Q}_s),$$
$$s.t. \; \frac{1}{\sigma_s^2}\text{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{Q}_s) - \frac{2^R}{\sigma_e^2}\text{Tr}(\mathbf{h}_e\mathbf{h}_e^H\mathbf{Q}_s) \geq 2^R - 1, \tag{41a}$$
$$\mathbf{Q}_s \succeq \mathbf{0}. \tag{41b}$$

We investigate the Lagrangian function of the problem (41) as follows:

$$\begin{aligned}\mathcal{L}(\mathbf{Q}_s, \alpha_1, \mathbf{Z}) &= \text{Tr}(\mathbf{Q}_s) + \alpha_1\left[\frac{2^R}{\sigma_e^2}\text{Tr}(\mathbf{h}_e\mathbf{h}_e^H\mathbf{Q}_s) - \frac{1}{\sigma_s^2}\text{Tr}(\mathbf{h}_s\mathbf{h}_s^H\mathbf{Q}_s) + 2^R - 1\right] - \text{Tr}(\mathbf{Q}_s\mathbf{Z}) \\ &= \text{Tr}\left[\left(\mathbf{I} + \frac{2^R\alpha_1}{\sigma_e^2}\mathbf{h}_e\mathbf{h}_e^H - \frac{\alpha_1}{\sigma_s^2}\mathbf{h}_s\mathbf{h}_s^H - \mathbf{Z}\right)\mathbf{Q}_s\right] + \alpha_1(2^R - 1),\end{aligned} \tag{42}$$

where $\alpha_1 \geq 0$ and $\mathbf{Z} \succeq \mathbf{0}$ are the dual variables associated with the constraints (41a) and (41b), respectively. Thus, the dual problem can be expressed as

$$\max_{\alpha_1 \geq 0} \; \alpha_1(2^R - 1),$$
$$s.t. \; \mathbf{Z} = \mathbf{I} - \alpha_1\left(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H\right) \succeq \mathbf{0}. \tag{43}$$

It can be easily observed that the dual problems of (40) and (43) are the same. Thus, we can claim that these two problems have the same solution. Now, we need to prove that $\mathbf{Z}$ in problem (43) has at least one zero eigenvalue, which means that $\mathbf{Y}$ in (40) has at least one zero eigenvalue as well. By exploiting the following matrix rank property [54]:

$$\text{rank}(\mathbf{A} - \mathbf{B}) \geq \text{rank}(\mathbf{A}) - \text{rank}(\mathbf{B}), \tag{44}$$

we have

$$\text{rank}(\mathbf{Z}) = \text{rank}\left(\mathbf{B} - \frac{\alpha_1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H\right) \geq \text{rank}(\mathbf{B}) - \text{rank}\left(\frac{\alpha_1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H\right), \tag{45}$$

where

$$\mathbf{B} = \mathbf{I} + \frac{\alpha_1 2^R}{\sigma_e^2}\mathbf{h}_e\mathbf{h}_e^H \tag{46}$$

From (45), one can observe that $\text{rank}(\mathbf{Z})$ is either N_T or $N_T - 1$. If $\text{rank}(\mathbf{Z}) = N_T$, it leads to $\mathbf{Q}_s = \mathbf{0}$, which violates $R > 0$. Thus, we can claim $\text{rank}(\mathbf{Z}) = N_T - 1$, which means that $\mathbf{Z}$ has at least one zero eigenvalue. Similarly, $\mathbf{Y}$ has at least one zero eigenvalue as well. On the other hand, the solution of α can be the maximum value that satisfies the positive semidefinite constraint in (40), which leads to

$$\alpha^{\text{opt}} = \frac{1}{\varrho_{\max}\left(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H\right)}. \tag{47}$$

The problem (37) can be formulated as a convex optimization problem. Hence, the strong duality holds between the original problem (37) and the corresponding dual problem (40). The required minimum power to achieve the secrecy rate constraint is

$$P^{\text{opt}} = \alpha^{\text{opt}}(2^R - 1). \tag{48}$$

On the other hand, it is easily verified that the optimal $\mathbf{w}$ lies in the null space of $\mathbf{Y}$

$$\bar{\mathbf{w}} = v_{\max}\left(\frac{1}{\bar{\sigma}_s^2}\mathbf{h}_s\mathbf{h}_s^H - \frac{2^R}{\bar{\sigma}_e^2}\mathbf{h}_e\mathbf{h}_e^H\right),\ \mathbf{v}^{\text{opt}} = \frac{\bar{\mathbf{w}}}{\|\bar{\mathbf{w}}\|_2}. \tag{49}$$

Hence, the optimal solution to (37) can be expressed as

$$\mathbf{w}^{\text{opt}} = \sqrt{P^{\text{opt}}}\mathbf{v}^{\text{opt}}. \tag{50}$$

B. *Proof of* Lemma *3*

We first derive the first-order derivatives of (29), which is written as

$$\frac{\partial U_M(\lambda)}{\partial \lambda} = \frac{1}{\ln 2}\left[\frac{\mu(1-\theta)t_sC_M}{1+(\lambda C_M - 2D_M)t_s} - \frac{\mu(1-\theta)t_eC_M}{1+(\lambda C_M - 2D_M)t_e}\right] - 2C_M\lambda + 2D_M. \tag{51}$$

Then, the second-order derivatives of (29) is given by

$$\frac{\partial^2 U_M(\lambda)}{\partial^2 \lambda} = \frac{1}{\ln 2}\left[\frac{\mu(1-\theta)C_M^2(t_e^2 - t_s^2)}{[1-(\lambda C_M - 2D_M)t_s]^2[1-(\lambda C_M - 2D_M)t_e]^2}\right] - 2C_M < 0. \tag{52}$$

The above inequality holds since $t_s - t_e > 0$ to guarantee the minimum achievable secrecy rate is greater than zero. Thus, (29) is a concave function.

C. *Proof of* Lemma *4*

In order to show that (34) is a convex problem, which means that we only need to show U_M is a concave function with respect to θ. First, we rewrite U_M as follows:

$$U_M = \mu(1-\theta)\log\left(\frac{1-\theta+\theta\bar{t}_s}{1-\theta+\theta\bar{t}_e}\right) - \theta\Psi. \tag{53}$$

It is easily observed that the concavity of (53) is only dependent on its first term due to the linear form of its second term. Thus, let us define

$$\begin{aligned} f_M &= \mu(1-\theta)\log\left(\frac{\frac{1-\theta+\theta\bar{t}_s}{1-\theta}}{\frac{1-\theta+\theta\bar{t}_e}{1-\theta}}\right) = \mu(1-\theta)\log\left(\frac{\frac{\theta(\bar{t}_s-1)+(1-\bar{t}_s)+\bar{t}_s}{1-\theta}}{\frac{\theta(\bar{t}_e-1)+(1-\bar{t}_e)+\bar{t}_e}{1-\theta}}\right) \\ &= \mu(1-\theta)\log\left(\frac{\frac{(1-\bar{t}_s)(1-\theta)+\bar{t}_s}{1-\theta}}{\frac{(1-\bar{t}_e)(1-\theta)+\bar{t}_e}{1-\theta}}\right). \end{aligned} \tag{54}$$

The remaining part is to focus on the concavity of f_M. Let $z = 1-\theta$, ($0 < \theta < 1$), f_M can be rewritten as

$$f_M(z) = \mu z\log\frac{(1-\bar{t}_s)z+\bar{t}_s}{z} - \mu z\log\frac{(1-\bar{t}_e)z+\bar{t}_e}{z}. \tag{55}$$

Then, we consider the first derivative of f_M,

$$\frac{\partial f_M}{\partial z} = \frac{\mu}{\ln 2}\left[\left(\ln\frac{(1-\bar{t}_s)z+\bar{t}_s}{z} + \frac{-\bar{t}_s}{(1-\bar{t}_s)z+\bar{t}_s}\right) - \left(\ln\frac{(1-\bar{t}_e)z+\bar{t}_e}{z} + \frac{-\bar{t}_e}{(1-\bar{t}_e)z+\bar{t}_e}\right)\right]. \tag{56}$$

Furthermore, the second derivative of f_M is given by

$$\frac{\partial^2 f_M}{\partial z^2} = \frac{\mu}{\ln 2}\left[\frac{-\bar{t}_s^2}{[(1-\bar{t}_s)z+\bar{t}_s]^2 z} - \frac{-\bar{t}_e^2}{[(1-\bar{t}_e)z+\bar{t}_e]^2 z}\right]. \tag{57}$$

Let $g(t) = \frac{-t^2}{[(1-t)z+t]^2 z}$, $t > 0$ the first derivative of $g(t)$ is given by

$$\frac{\partial g(t)}{\partial t} = \frac{-2t[(1-t)z+t] + 2(1-z)t^2}{[(1-t)z+t]^3 z} = \frac{-2t}{[z+(1-z)t]^3} < 0. \tag{58}$$

It is easily verified that (58) holds since $z = 1-\theta \in (0,1)$. Thus, $g(t)$ is a monotonically decreasing function of t. Due to $\bar{t}_s > \bar{t}_e > 0$, it is easily obtained that $\frac{\partial^2 f_M(z)}{\partial z^2} < 0$. In other words, $f_M(\theta)$ is a concave function with respect to θ. Thus, U_M is also a concave function with respect to θ.

REFERENCES

[1] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.

[2] Z. Xiang, M. Tao, and X. Wang, "Coordinated multicast beamforming in multicell networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 12–21, Jan. 2013.

[3] Z. Xiang, M. Tao, and X. Wang, "Massive MIMO multicasting in noncooperative cellular networks," *IEEE J. Sel. Area. Comm.*, vol. 32, no. 6, pp. 1180–1193, Jun. 2014.

[4] L. Varshney, "Transporting information and energy simultaneously," in *Proc. 2008 IEEE Int. Symp. Inf. Theory*, pp. 1612–1616, July, 2008.

[5] P. Grover and A. Sahai, "Shannon meets tesla: Wireless information and power transfer," in *Proc. 2010 IEEE Int. Symp. Inf. Theory*, pp. 2363–2367, Jun., 2010.

[6] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, pp. 1989–2001, May 2013.

[7] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: an overview," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 10–18, Apr. 2016.

[8] H. Ju and R. Zhang, "Throughput maximization in wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 1, pp. 418–428, Jan. 2014.

[9] H. Ju and R. Zhang, "User cooperation in wireless powered communication networks," in *Proc. IEEE GLOBECOM*, pp. 1430–1435, Dec. 2014.

[10] H. Chen, X. Zhou, Y. Li, P. Wang, and B. Vucetic, "Wireless-powered cooperative communications via a hybrid relay," in *Proc. IEEE Information Theory Workshop (ITW)*, pp. 666–670, Nov. 2014.

[11] H. Chen, Y. Li, J. L. Rebelatto, B. F. Ucha-Filho, and B. Vucetic, "Harvest-then-cooperate: Wireless-powered cooperative communications," *IEEE Trans. Signal Process.*, vol. 63, no. 7, pp. 1700–1711, Apr. 2015.

[12] H. Gao, T. Lv, W. Wang, and N. C. Beaulieu, "Energy-efficient and secure beamforming for self-sustainable relay-aided multicast networks," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1509–1513, Nov. 2016.

[13] K. Huang and X. Zhou, "Cutting the last wires for mobile communications by microwave power transfer," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 86–93, Jun. 2015.

[14] K. Huang and V. K. N. Lau, “Enabling wireless power transfer in cellular networks: Architecture, modeling and deployment,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 902–912, Feb. 2014.

[15] C. Zhong, G. Zheng, Z. Zhang, and G. K. Karagiannidis, “Optimum wirelessly powered relaying,” *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1728–1732, Oct. 2015.

[16] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. Journ.*, vol. 54, pp. 1355–1387, Jan. 1975.

[17] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, May 1978.

[18] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[19] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[20] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas II: The MIMOME wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[21] J. Li and A. P. Petropulu, “On ergodic secrecy rate for gaussian MISO wiretap channels,” *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, April Apr. 2011.

[22] S. A. A. Fakoorian and A. L. Swindlehurst, “Full rank solutions for the MIMO gaussian wiretap channel with an average power constraint,” *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May. 2013.

[23] Q. Li and W.-K. Ma, “Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming,” *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[24] Q. Li and W.-K. Ma, “Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization,” *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[25] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, “Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer,” *IEEE Trans. Vehicular Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[26] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. L. Goff, “Secrecy rate optimization for a MIMO secrecy channel based on stackelberg game,” in *Proc. EUSIPCO, Lisbon, Portugal*, pp. 126–130, Sept. 2014.

[27] A. Al-Talabani, Y. Deng, A. Nallanathan, and H. X. Nguyen, “Enhancing secrecy rate in cognitive radio networks via stackelberg game,” *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4764–4775, Nov. 2016.

[28] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, “Robust outage secrecy rate optimizations for a MIMO secrecy channel,” *IEEE, Wireless Commun. Lett.*, vol. 4, no. 1, pp. 86–89, Feb. 2015.

[29] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, “Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers,” *IEEE Trans. Wireles Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[30] Z. Zhu, Z. Chu, Z. Wang, and I. Lee, “Outage constrained robust beamforming for secure broadcasting systems with energy harvesting,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7610–7620, Nov. 2016.

[31] Q. Yang, H. M. Wang, Y. Zhang, and Z. Han, “Physical layer security in MIMO backscatter wireless systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547–7560, Nov. 2016.

[32] L. Liu, R. Zhang, and K.-C. Chua, “Secrecy wireless information and power transfer with MISO beamforming,” *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850–1863, Apr. 2014.

[33] D. W. K. Ng, E. S. Lo, and R. Schober, “Robust beamforming for secure communication in systems with wireless information and power transfer,” *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[34] M. Khandaker and K. Wong, “Masked beamforming in the presence of energy-harvesting eavesdroppers,” *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 40–54, Jan 2015.

[35] Z. Chu, Z. Zhu, M. Johnston, and S. Y. L. Goff, “Simultaneous wireless information power transfer for MISO secrecy channel,” *IEEE Trans. Vehicular Technol.*, vol. 65, no. 9, pp. 6913–6925, Sept. 2016.

[36] Y. Wu, X. Chen, C. Yuen, and C. Zhong, "Robust resource allocation for secrecy wireless powered communication networks," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2430–2433, Dec. 2016.

[37] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commun.*, vol. 64, pp. 3858–3871, Sept 2016.

[38] Q. Li and W. K. Ma, "Multicast secrecy rate maximization for MISO channels with multiple multi-antenna eavesdroppers," in *Proc. IEEE, ICC, Tokyo, Japan*, pp. 1–5, Jun. 2011.

[39] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.

[40] L. N. Tran, M. F. Hanif, and M. Juntti, "A conic quadratic programming approach to physical layer multicasting for large-scale antenna arrays," *IEEE Signal Process. Lett.*, vol. 21, no. 1, pp. 114–117, Jan. 2014.

[41] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, UK: Cambridge University Press, 2004.

[42] D. Bethanabhotla, G. Caire, and M. J. Neely, "Adaptive video streaming for wireless networks with multiple users and helpers," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 268–285, Jan. 2015.

[43] J. Kim, G. Caire, and A. F. Molisch, "Quality-aware streaming and scheduling for device-to-device video delivery," *IEEE/ACM Trans. Networking*, vol. 24, no. 4, pp. 2319–2331, Aug. 2016.

[44] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *IEEE ICASSP, Tokyo, Japan*, Mar. 2012.

[45] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[46] A. H. Mohsenian-Rad, V. W. S. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia, "Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid," *IEEE Trans. Smart Grid*, vol. 1, no. 3, pp. 320–331, Dec. 2010.

[47] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.

[48] K. Y. Wang, A. M. C. So, T. H. Chang, W. K. Ma, and C. Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2014.

[49] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE ISIT, Nice, France*, pp. 2466–2470, Jun. 2007.

[50] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper Res.*, vol. 26, no. 4, pp. 681–683, 1978.

[51] X. Huang, J. He, Q. Li, Q. Zhang, and J. Qin, "Optimal power allocation for multicarrier secure communications in full-duplex decode-and-forward relay networks," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2169–2172, Dec. 2014.

[52] Y. Yuan and Z. Ding, "The application of non-orthogonal multiple access in wireless powered communication networks," in *Proc. IEEE SPAWC, Edinburgh, United Kindom*, pp. 1–5, Jul. 2016.

[53] Z. Chu, F. Zhou, Z. Zhu, M. Sun, and N. Al-Dhahir, "Energy beamforming design and user cooperation for wireless powered communication networks," *to appear in IEEE Wireless Commun. Lett.*, 2017.

[54] R. A. Horn and C. R. Johnson, *Matrix Analysis*. New York, NY, USA: Cambridge University Press, 2012.