Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems

Meng Zhang, *Student Member, IEEE*, Yuan Liu, *Member, IEEE*, and Rui Zhang, *Senior Member, IEEE*

Abstract—In this paper, we study simultaneous wireless information and power transfer (SWIPT) in orthogonal frequency division multiple access (OFDMA) systems with the coexistence of information receivers (IRs) and energy receivers (ERs). The IRs are served with best-effort secrecy data and the ERs harvest energy with minimum required harvested power. To enhance the physical layer security for IRs and yet satisfy energy harvesting requirements for ERs, we propose a new frequency-domain artificial noise (AN) aided transmission strategy. With the new strategy, we study the optimal resource allocation for the weighted sum secrecy rate maximization for IRs by power and subcarrier allocation at the transmitter. The studied problem is shown to be a mixed integer programming problem and thus non-convex, while we propose an efficient algorithm for solving it based on the Lagrange duality method. To further reduce the computational complexity, we also propose a suboptimal algorithm of lower complexity. The simulation results illustrate the effectiveness of proposed algorithms as compared against other heuristic schemes.

Index Terms—Physical layer security, simultaneous wireless information and power transfer (SWIPT), artificial noise (AN), orthogonal frequency-division multiple access (OFDMA), resource allocation.

I. INTRODUCTION

ORTHOGONAL frequency division multiple access (OFDMA) has many advantages such as flexibility in resource allocation and robustness against multipath channel fading, and therefore has become a well established multiple-access technique for multiuser wireless communications systems.

Recently, simultaneous wireless information and power transfer (SWIPT) provides an appealing solution to prolong the operation time of energy-limited wireless nodes [2]–[9]. SWIPT systems enable the users to harvest energy and decode information from the same received signal, thus making most efficient use of the wireless spectrum for both information and energy transfer. SWIPT has drawn a great amount of research interests. For instance, two practical schemes for SWIPT, namely power splitting (PS) and time switching (TS), were proposed in [2] and [3]. With TS applied at each receiver, the received signal is either processed for energy harvesting or for information decoding. When PS is used at the receiver, the signal is split into two streams, for information decoding and energy harvesting, respectively. The authors in [2] and [3] also investigated the achievable rate-energy tradeoffs for a multiple-input multiple-output (MIMO) SWIPT system and a single-input single-output (SISO) SWIPT system, respectively. SWIPT systems in fading channels were studied by dynamic time switching (DTS) and dynamic power splitting (DPS) in [4] and [5], respectively.
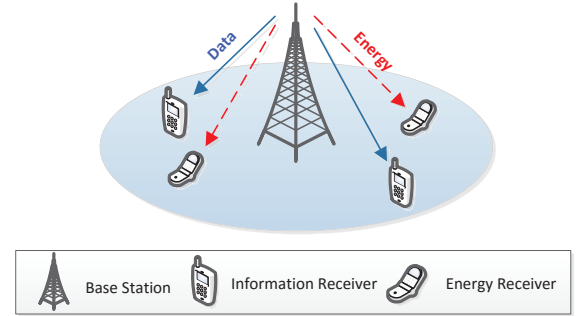

Fig. 1. System model of OFDMA-based SWIPT, where each receiver is a potential eavesdropper to other receivers.

On the other hand, due to the increasing importance of information security, substantial research efforts have been dedicated to information-theoretic physical layer security [10]–[17], as a complementary solution to the traditional cryptography based encryption applied in the upper layers. The authors in [11] considered physical layer security in an OFDMA system, with the goal of maximizing the sum rate of best-effort information users subject to the individual secrecy rate requirements of secure users. In [13], the orthogonal frequency division multiplexing (OFDM) based wiretap channel was considered and the achievable secrecy rate with Gaussian inputs was studied. Artificial noise (AN) is a well-known approach for improving physical layer security by degrading eavesdroppers' channel condition [14], [15]. In [14], in order to assist secrecy information transmission, AN is transmitted into the null space of the channels of legitimate users to interfere with the eavesdroppers. In [15], the authors proposed a time-domain AN design by exploiting temporal degrees of freedom from the cyclic prefix in OFDM modulated signals, even with a single antenna at the transmitter. In [17], the authors studied robust transmission schemes for the multiple-input single-output (MISO) wiretap channels.

A handful of works have been investigated the secure issues in SWIPT systems [18]–[21]. Since the energy receivers (ERs) need to be deployed much closer to the access points than the information receivers (IRs) due to their much higher received power requirement [9], they are inevitably capable of eavesdropping the messages to the IRs. Moreover, AN also plays a role of energy signal, i.e., besides interfering with the eavesdroppers to facilitate secure communication, AN is a new source for wireless power transfer as well. In [18], [19], the authors studied the secrecy communication in SWIPT by properly designing the beamforming vectors at the multi-antenna transmitter. Secrecy communication in
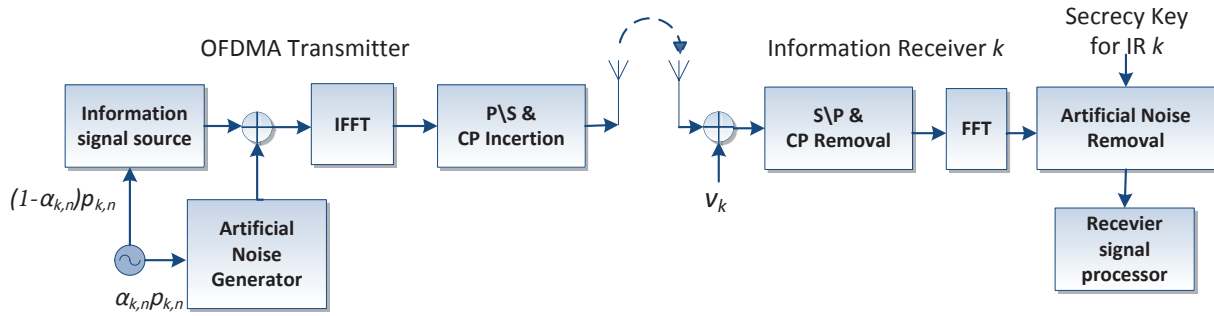
Fig. 2. Block diagram of an OFDMA transmitter and receiver with AN generation and removal procedure.

SWIPT over fading channels was also studied in [20]. In [21], the authors studied the secure OFDMA-based systems with a power splitter applied at each user terminal to coordinate the secure transmission and energy harvesting. However, AN aided OFDMA-based SWIPT systems with secrecy constraints have not yet been investigated in the literature. In a secure OFDMA system without AN, only the user with the largest channel gain over each subcarrier (SC) can receive secure information [11]. Thus, the new method of using AN not only achieves the secrecy information and wireless power transfer at the same time, but also leads to new resource allocation solutions different from the conventional secure OFDMA system without AN.

Motivated by the aforementioned reasons, in this paper, we study the optimal resource allocation in the AN aided secure OFDMA systems with SWIPT as shown in Fig. 1, where two types of receivers are assumed, i.e., IRs and ERs. Our goal is to maximize the weighted sum secrecy rate of the IRs subject to minimum harvested power requirements of individual ERs. We propose a new frequency-domain AN method in OFDMA-based SWIPT to facilitate both secrecy information transmission and energy transfer to IRs and ERs, respectively. Specifically, as shown in Fig. 2, independent AN is added over each SC at the transmitter and only the desired IR is able to cancel it using the corresponding key before decoding the information[1]. The formulated problem is a mixed integer programming problem and thus non-convex. We propose an efficient algorithm based on the Lagrange duality method, which solves the problem asymptotically optimally when the number of SCs becomes large. Moreover, a suboptimal algorithm is also proposed to tradeoff complexity and performance.

The remainder of this paper is organized as follows. In Section II, we introduce the system model of the OFDMA-based SWIPT with secrecy constraints, and present the problem formulation. The problem is solved by the Lagrange duality method in Section III. In Section IV, we propose the suboptimal algorithm of lower complexity. In Section V, we provide the numerical results on the performance of proposed

algorithms. Finally, we conclude the paper in Section VI.

II. SYSTEM MODEL AND PROBLEM FORMULATION

We consider a downlink OFDMA-based SWIPT system with secrecy constraints as shown in Fig. 1. The system consists of one base station (BS) with a single antenna, K single-antenna receivers and N SCs. The set of receivers is denoted by $\mathcal{K} = \{1, ..., K\}$, among which K_1 receivers are IRs given by the set $\mathcal{K}_1$ and the rest K_2 receivers are ERs given by the set $\mathcal{K}_2$, i.e., $\mathcal{K}_1 \cup \mathcal{K}_2 = \mathcal{K}$. Note that the receivers (both IRs and ERs) are considered to be *separated* and can only decode information or harvest energy at a time, unlike the *co-located* receivers considered in [6], [7]. The set of SCs is denoted as $\mathcal{N} = \{1, ..., N\}$. Furthermore, we assume that for each IR, all other receivers (IRs and ERs) are potential eavesdroppers, similar to the case considered in [11]. The BS is assumed to know the channel state information (CSI) of all receivers. This is practically valid since the IRs and ERs need to help the BS in obtaining their individual CSI for receiving required information and energy, respectively. We assume that the OFDM symbols are time slotted so that the length of each time slot is comparable to the channel coherence time, i.e., the channel impulse response can be treated as time invariant during each time slot. As a result, the BS can accurately estimate CSI of all receivers on all SCs.

We propose a frequency-domain AN generation and removal method for OFDMA-based SWIPT, similar to that in [20] over the time domain. The scheme is illustrated in Fig. 2 and described as follows. A large ensemble of sequences used to generate Gaussian distributed AN are pre-stored at the BS[2], and the indices of the sequences are regarded as the keys. After SC allocation to IRs, the BS first randomly picks N sequences (each corresponds to one SC) from the ensemble and transmits each of their indices (keys) to the IR to whom the corresponding SC is assigned. As the random sequence (or AN) is only known to the intended IR but unknown to all the other receivers, any potential eavesdropper cannot have access to the random sequence used at each SC. Moreover, in order to prevent the eavesdropper from decoding the random sequence by long-term observation of the signal, the BS randomly picks new random sequences and transmits the corresponding keys in a secret manner to the desired IRs from time to time, using e.g. the method proposed in [24] by exploiting the channel

---

[1]Note that the key-assisted approach is normally exclusively used for cryptography, while physical-layer methods are traditionally adopted when the shared keys are not available. However, some recent works (e.g. [22], [23]) have considered applying physical-layer security to enhance cryptographic secrecy, showing the potentials to benefit from both types of secrecy approaches. Hence, under such multi-layer security framework, it is also possible to jointly consider the key-assisted physical-layer security and cryptography design, which is left for our future work.

[2]Note that in the literature, the AN is usually assumed to follow Gaussian distribution (e.g. [14]–[16]).

independence and reciprocity. Specifically, the IR sends a pilot signal to the BS, and then the BS sends a random key and modulates it over the phase of the transmitted signal with the received channel phase pre-compensated. In this way, the intended IR is able to decode the key while the channel phases between the BS and other receivers are different from that between the BS and the intended IR. Thus, the key can be confidentially transmitted without being eavesdropped by other receivers.

The transmit signal comprises the transmitted data symbol $s_{k,n}$ from the BS to IR k on SC n and the AN bearing signal $z_{k,n}$ for IR k, $k \in \mathcal{K}_1$ and $n \in \mathcal{N}$. It is assumed that $s_{k,n}$ and $z_{k,n}$ are independent circularly symmetric complex Gaussian (CSCG) random variables with zero mean and unit variance, denoted by $s_{k,n} \sim \mathcal{CN}(0,1)$ and $z_{k,n} \sim \mathcal{CN}(0,1)$, which are also independent over n.

The transmitted signal to IR k at SC n is given by

$$X_{k,n} = \sqrt{(1 - \alpha_{k,n})p_{k,n}}s_{k,n} + \sqrt{\alpha_{k,n}p_{k,n}}z_{k,n}, \quad (1)$$

where $p_{k,n} \geq 0$ is the total power at SC n and $0 \leq \alpha_{k,n} \leq 1$ is the transmit power splitting ratio at the BS-side to generate AN to be added at SC n.

Let $h_{k,n}$ denote the complex channel coefficient from the BS to receiver k at SC n, and $\beta_{k,n}$ denote the eavesdropper's complex channel coefficient. Here, we let $|\beta_{k,n}|^2 = \max_{k' \in \mathcal{K}, k' \neq k} |h_{k',n}|^2$, indicating that the considered eavesdropper of receiver k is the receiver of the largest channel gain among all the other receivers on SC n. The downlink received signal at IR k on SC n and that at a potential eavesdropper who is wiretapping IR k over SC n are respectively given by

$$Y_{k,n} = h_{k,n}X_{k,n} + v_k, \quad (2)$$
$$E_{k,n} = \beta_{k,n}X_{k,n} + e_k, \quad (3)$$

where the noise v_k and e_k are assumed to be independent and identically distributed (i.i.d.) as $\mathcal{CN}(0, \sigma^2)$.

With the aforementioned scheme, the AN can be canceled at the desired IR at each SC but not possibly at any of the potential eavesdroppers. From (1)-(3), the received signals at IR k after AN cancellation and the "best" eavesdropper on SC n are further expressed as

$$Y_{k,n} = h_{k,n}\sqrt{(1 - \alpha_{k,n})p_{k,n}}s_{k,n} + v_k, \quad (4)$$
$$E_{k,n} = \beta_{k,n}\sqrt{(1 - \alpha_{k,n})p_{k,n}}s_{k,n} + \beta_{k,n}\sqrt{\alpha_{k,n}p_{k,n}}z_{k,n} + e_k. \quad (5)$$

Here we can write the achievable information rate of IR k on SC n, which is given by

$$r_{k,n} = \log_2\left(1 + \frac{(1 - \alpha_{k,n})|h_{k,n}|^2 p_{k,n}}{\sigma^2}\right). \quad (6)$$

The decodable information rate of the "best" eavesdropper on SC n is given by

$$r^e_{k,n} = \log_2\left(1 + \frac{(1 - \alpha_{k,n})|\beta_{k,n}|^2 p_{k,n}}{\sigma^2 + \alpha_{k,n}|\beta_{k,n}|^2 p_{k,n}}\right). \quad (7)$$

The achievable secrecy rate for IR k on SC n is thus given by [25]

$$\begin{aligned}
R^s_{k,n} &= [r_{k,n} - r^e_{k,n}]^+ \\
&= \left[\log_2\left(1 + \frac{(1 - \alpha_{k,n})|h_{k,n}|^2 p_{k,n}}{\sigma^2}\right) \right. \\
&\quad \left. - \log_2\left(1 + \frac{(1 - \alpha_{k,n})|\beta_{k,n}|^2 p_{k,n}}{\alpha_{k,n}|\beta_{k,n}|^2 p_{k,n} + \sigma^2}\right)\right]^+, \quad (8)
\end{aligned}$$

for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}$, where $[\cdot]^+ \triangleq \max(0, \cdot)$.

Lemma 1. $R^s_{k,n}$ in (8) can be further expressed as

$$R^s_{k,n} = \begin{cases} 0, & \text{if } 0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+, \\ r_{k,n} - r^e_{k,n} \geq 0, & \text{if } p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+, \end{cases} \quad (9)$$

where

$$\mathcal{X}_{k,n}(\alpha_{k,n}) \triangleq \begin{cases} \frac{\sigma^2}{\alpha_{k,n}}\left(\frac{1}{|h_{k,n}|^2} - \frac{1}{|\beta_{k,n}|^2}\right) & \text{if } \alpha_{k,n} \neq 0 \\ \text{sgn}\left(|\beta_{k,n}|^2 - |h_{k,n}|^2\right) \times \infty & \text{if } \alpha_{k,n} = 0 \end{cases}, \quad (10)$$

and $\text{sgn}(x) = |x|/x$ if $x \neq 0$ and $\text{sgn}(x) = 1$ if $x = 0$.

Proof: Please refer to Appendix A. ∎

Remark 1. *Note that the traditional AN scheme (without AN cancelation, e.g. [14], [17]) is ineffective for the considered SISO systems, i.e., without cancelling AN in the intended IRs, AN cannot achieve a higher secrecy rate compared to the transmission without AN. The details can be found in Appendix B.*

The weighted sum (secrecy) rate of all K_1 IRs is given by

$$R^s_{\text{sum}} = \sum_{k \in \mathcal{K}_1} w_k \sum_{n \in \mathcal{N}} x_{k,n} R^s_{k,n}, \quad (11)$$

where w_k is the positive weight of IR k and $x_{k,n}$ is the binary SC allocation variable with $x_{k,n} = 1$ representing SC n is allocated to IR k and $x_{k,n} = 0$ otherwise. Note that in the considered system, the ERs can harvest energy from all SCs while the IRs need orthogonal SC assignment for avoiding mutual interference. In addition, if the power allocated on SC n is given by p_n, then ER l can harvest $\zeta_l p_n |h_{l,n}|^2$ on SC n regardless of which receiver it is allocated to. Notice that if $p_{k,n} > 0$ and $\alpha_{k,n} = 1$ for any SC n, then this SC is used only for energy transfer, i.e., there is no information sent over the SC. As a result, we only need to focus on the cases that SCs are allocated to IRs without loss of generality.

Thus, the harvested power at each ER $l \in \mathcal{K}_2$ is given by

$$Q_l = \zeta_l \sum_{n \in \mathcal{N}} \left(\sum_{k \in \mathcal{K}_1} x_{k,n} p_{k,n}\right) |h_{l,n}|^2, \quad (12)$$

where $0 < \zeta_l < 1$ denotes the energy harvesting efficiency.

An example of the energy utilization at receivers in an OFDMA-based SWIPT system with secrecy constraints is shown in Fig. 3, with $K_1 = 2$ and $K_2 = 1$. As it is shown, the AN does not interfere with the intended receiver but all other receivers. In addition, the ER is able to harvest energy from both information signal and AN signal.
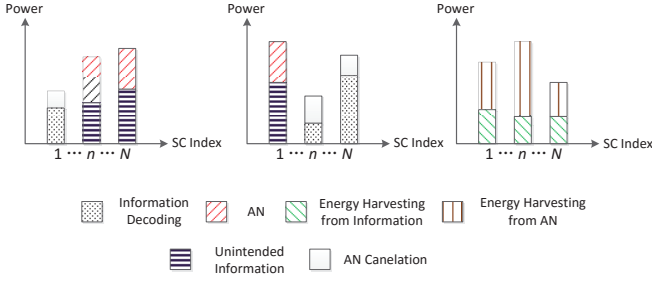
Fig. 3. An example of power utilization for an OFDMA-based SWIPT system of two IRs and one ER.

Our goal is to maximize the weighted sum rate of the IRs by optimizing transmit power and SC allocation as well as transmit power splitting ratio at each SC, subject to the harvested power constraints of all ERs. The problem can be mathematically formulated as

$$\max_{\boldsymbol{P}, \boldsymbol{X}, \boldsymbol{\alpha}} R_{\text{sum}}^s \tag{13a}$$

$$\text{s.t.} \quad Q_l \geq \bar{Q}_l, \forall l \in \mathcal{K}_2, \tag{13b}$$

$$\sum_{k \in \mathcal{K}_1} \sum_{n \in \mathcal{N}} p_{k,n} x_{k,n} \leq P_{\max} \tag{13c}$$

$$0 \leq p_{k,n} \leq P_{\text{peak}}, \forall n \in \mathcal{N}, k \in \mathcal{K}_1 \tag{13d}$$

$$0 \leq \alpha_{k,n} \leq 1, \forall n \in \mathcal{N}, k \in \mathcal{K}_1 \tag{13e}$$

$$x_{k,n} \in \{0,1\}, \forall n \in \mathcal{N}, k \in \mathcal{K}_1 \tag{13f}$$

$$\sum_{k \in \mathcal{K}_1} x_{k,n} \leq 1, \forall n \in \mathcal{N}, \tag{13g}$$

where $\boldsymbol{P} \triangleq \{p_{k,n}\}$ denotes the power allocation over SCs, $\boldsymbol{X} \triangleq \{x_{k,n}\}$ denotes the SC allocation for IRs, and $\boldsymbol{\alpha} \triangleq \{\alpha_{k,n}\}$ denotes the transmit power splitting over SCs. In (13b), $\bar{Q}_l$ denotes the harvested power constraint for ER $l \in \mathcal{K}_2$. In (13c) and (13d), $P_{\max}$ and P_{peak} represent the total power constraint over all SCs and the peak power constraint over each SC, respectively. Finally, (13f) and (13g) constrain that any SC can only be assigned to at most one IR.

III. OPTIMAL SOLUTION

Problem (13a) is a mixed integer programming and thus is NP-hard and non-convex. As shown in [26], [27], the duality gap becomes zero in OFDM-based resource allocation problems including problem (13a) as the number of SCs goes to infinity due to the so-called time-sharing condition. This implies that problem (13a) can be solved by the Lagrange duality method asymptotically optimally.

First, the Lagrangian of problem (13a) is given by

$$\mathcal{L}(\boldsymbol{P}, \boldsymbol{\alpha}, \boldsymbol{X}, \boldsymbol{\lambda}, \gamma)$$

$$= \sum_{k \in \mathcal{K}_1} w_k \sum_{n \in \mathcal{N}} x_{k,n} R_{k,n}^s - \gamma \left(\sum_{k \in \mathcal{K}_1} \sum_{n \in \mathcal{N}} x_{k,n} p_{k,n} - P_{\max} \right)$$

$$+ \sum_{l \in \mathcal{K}_2} \lambda_l (Q_l - \bar{Q}_l)$$

$$= \sum_{k \in \mathcal{K}_1} w_k \sum_{n \in \mathcal{N}} x_{k,n} R_{k,n}^s - \gamma \sum_{k \in \mathcal{K}_1} \sum_{n \in \mathcal{N}} x_{k,n} p_{k,n}$$

$$+ \sum_{n \in \mathcal{N}} \left(\sum_{k \in \mathcal{K}_1} x_{k,n} p_{k,n} \right) \sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{l,n}|^2$$

$$- \sum_{l \in \mathcal{K}_2} \lambda_l \bar{Q}_l + \gamma P_{\max}, \tag{14}$$

where $\boldsymbol{\lambda} = [\lambda_1, \lambda_2, ..., \lambda_{K_2}]$ and γ are the Lagrange multipliers (dual variables) corresponding to the minimum required harvested power constraints and the total transmit power constraint, respectively.

We then define $\mathcal{P}$ for given $\boldsymbol{X}$ as the set of all possible power allocations of $\boldsymbol{P}$ that satisfy $0 \leq p_{k,n} \leq P_{\text{peak}}$ for $x_{k,n} = 1$ and $p_{k,n} = 0$ when $x_{k,n} = 0$, $\mathcal{S}$ as the set of all possible $\boldsymbol{X}$ that satisfy constraints (13f) and (13g), and $\mathcal{A}$ as the set of all feasible $\boldsymbol{\alpha}$ that satisfy (13e). Then, we can obtain the dual function for problem (13a) as

$$g(\boldsymbol{\lambda}, \gamma) = \max_{\boldsymbol{P} \in \mathcal{P}(\boldsymbol{X}), \boldsymbol{\alpha} \in \mathcal{A}, \boldsymbol{X} \in \mathcal{S}} \mathcal{L}(\boldsymbol{P}, \boldsymbol{\alpha}, \boldsymbol{X}, \boldsymbol{\lambda}, \gamma). \tag{15}$$

The dual problem is then given by

$$\min_{\boldsymbol{\lambda} \succeq 0, \gamma \geq 0} g(\boldsymbol{\lambda}, \gamma). \tag{16}$$

From (14), we can observe that the maximization in (16) can be decomposed into N independent subproblems. Accordingly, we can rewrite the Lagrangian as

$$\mathcal{L}(\boldsymbol{P}, \boldsymbol{\alpha}, \boldsymbol{X}, \boldsymbol{\lambda}, \gamma) = \sum_{n \in \mathcal{N}} \mathcal{L}_n (\boldsymbol{P}_n, \boldsymbol{\alpha}_n, \boldsymbol{X}_n)$$

$$- \sum_{l \in \mathcal{K}_2} \lambda_l \bar{Q}_l + \gamma P_{\max}, \tag{17}$$

where

$$\mathcal{L}_n (\boldsymbol{P}_n, \boldsymbol{\alpha}_n, \boldsymbol{X}_n)$$

$$\triangleq \sum_{k \in \mathcal{K}_1} x_{k,n} \left\{ w_k R_{k,n}^s - \gamma p_{k,n} + p_{k,n} \left(\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{l,n}|^2 \right) \right\}. \tag{18}$$

Since $x_{k,n} \in \{0,1\}$ and $\sum_{k \in \mathcal{K}_1} x_{k,n} = 1$, there exists a $k^* \in \mathcal{K}_1$ such that

$$x_{k,n}^* = \begin{cases} 1, & \text{if } k = k^*, \\ 0, & \text{otherwise} \end{cases}, \forall n \in \mathcal{N}, \tag{19}$$

is the optimal solution to maximize $\mathcal{L}$.

Hence, with given $\boldsymbol{\lambda}$ and γ, the maximization of $\mathcal{L}$ can be attained by selecting

$$k^* = \arg \max_{k \in \mathcal{K}_1} \left\{ w_k R_{k,n}^s + p_{k,n} \left(\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{l,n}|^2 - \gamma \right) \right\} \tag{20}$$

for each SC n, and the optimal $(p_{k,n}^*, \alpha_{k,n}^*)$ can be solved by assuming $k = k^*$ and then solving the following subproblem for each SC n,

$$\max_{\boldsymbol{P}_n \in \mathcal{P}(\boldsymbol{X}), \boldsymbol{\alpha}_n \in \mathcal{A}} \mathcal{L}'_n(\boldsymbol{P}_n, \boldsymbol{\alpha}_n)$$
$$\triangleq w_k R_{k,n}^s + p_{k,n} \left(\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{l,n}|^2 - \gamma \right). \tag{21}$$

A. Joint Optimization of Power Allocation and Transmit Power Splitting Ratio

We cannot directly express the partial derivative of $R_{k,n}^s$ in (8) with respect to $p_{k,n}$ or $\alpha_{k,n}$. However, as we have discussed in Lemma 1, $R_{k,n}^s = 0$ when $0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$ and $R_{k,n}^s > 0$ when $p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$. In each region, $R_{k,n}^s$ is differentiable with respect to $p_{k,n}$ or $\alpha_{k,n}$. Hence, we first find the set of all feasible candidates for $(p_{k,n}^*, \alpha_{k,n}^*)$ in all regions. Then, we select $(p_{k,n}^*, \alpha_{k,n}^*)$ as the one achieving the largest value of $\mathcal{L}'_n$ in (21).

1) Region I ($p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$):

Lemma 2. *The optimal $\alpha_{k,n}$ with given $p_{k,n}$ for problem (21) is given by*

$$\alpha_{k,n}^*(p_{k,n}) = \left[\frac{1}{2} + \frac{\sigma^2}{2p_{k,n}} \left(\frac{1}{|h_{k,n}|^2} - \frac{1}{|\beta_{k,n}|^2} \right) \right]^+ < 1, \tag{22}$$

for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}$.

Proof: Please refer to Appendix C. ∎

On the other hand, by deriving the partial derivative of $\mathcal{L}'_n$ with respect to $p_{k,n}$ and equating it to zero, we have

$$a_1 p_{k,n}^3 + b_1 p_{k,n}^2 + c_1 p_{k,n} + d_1 = 0, \tag{23}$$

where

$$a_1 = \ln 2 |h_{k,n}|^2 (\alpha_{k,n}^2 - \alpha_{k,n}) |\beta_{k,n}|^4 \Omega_n, \tag{24}$$
$$b_1 = (\alpha_{k,n}^2 - \alpha_{k,n}) |\beta_{k,n}|^4 |h_{k,n}|^2 w_k$$
$$+ \ln 2 |\beta_{k,n}|^2 \sigma^2 \left[(\alpha_{k,n}^2 - 1) |h_{k,n}|^2 - |\beta_{k,n}|^2 \alpha_{k,n} \right] \Omega_n, \tag{25}$$
$$c_1 = \ln 2 (\alpha_{k,n} - 1) (|h_{k,n}|^2 - |\beta_{k,n}|^2) \sigma^4 \Omega_n$$
$$+ 2(\alpha_{k,n}^2 - \alpha_{k,n}) |\beta_{k,n}|^2 |h_{k,n}|^2 w_k \sigma^2, \tag{26}$$
$$d_1 = (\alpha_{k,n} - 1)(|h_{k,n}|^2 - |\beta_{k,n}|^2) w_k \sigma^4 - \ln 2 \sigma^6 \Omega_n, \tag{27}$$
$$\Omega_n = -\gamma + \sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{k,n}|^2. \tag{28}$$

We first define $\Phi_1(\alpha_{k,n})$ as the set of all non-negative real roots to (23) that satisfy $[\mathcal{X}_{k,n}(\alpha_{k,n})]^+ < p_{k,n} \leq P_{\text{peak}}$ with given $\alpha_{k,n}$. Then, we define another set $\Psi_1(\alpha_{k,n})$ as follows:

$$\Psi_1(\alpha_{k,n}) \triangleq \{(p_{k,n}, \alpha_{k,n}) | p_{k,n} \in \Phi_1(\alpha_{k,n})\}. \tag{29}$$

To find feasible candidates for $(p_{k,n}^*, \alpha_{k,n}^*)$, we consider the following two subregions.

- For *subregion i*, we remove the $[\cdot]^+$ operator of $\alpha_{k,n}^*(p_{k,n})$ in (22) and assume that

$p_{k,n} \geq \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right) \sigma^2$. Substituting it into (23) to eliminate $\alpha_{k,n}$, we have

$$a_2 p_{k,n}^2 + b_2 p_{k,n} + c_2 = 0, \tag{30}$$

where

$$a_2 = \ln 2 |\beta_{k,n}|^4 |h_{k,n}|^2 \Omega_n, \tag{31}$$
$$b_2 = w_k |\beta_{k,n}|^4 |h_{k,n}|^2 + \ln 2 \Omega_n |\beta_{k,n}|^2 \sigma^2, \tag{32}$$
$$c_2 = \sigma^2 \left\{ |\beta_{k,n}|^2 |h_{k,n}|^2 w_k (1 - |\beta_{k,n}|^2) \right.$$
$$\left. + \ln 2 \Omega_n^2 (|\beta_{k,n}|^2 + |h_{k,n}|^2) \right\}. \tag{33}$$

Similarly, we define Φ_2 as the set of all non-negative real roots to (30) that satisfy $[\mathcal{X}_{k,n}(\alpha_{k,n})]^+ < p_{k,n} \leq P_{\text{peak}}$. We further define Ψ_2 as the set of all feasible candidates for $(p_{k,n}^*, \alpha_{k,n}^*)$ in *subregion i* as follows:

$$\Psi_2 \triangleq \{(p_{k,n}, \alpha_{k,n}) | p_{k,n} \in \Phi_2, \alpha_{k,n} = \alpha_{k,n}^*(p_{k,n})\}$$
$$\cup (P_{\text{peak}}, \alpha_{k,n}^*(P_{\text{peak}})), \tag{34}$$

where $\alpha_{k,n}^*(p_{k,n})$ is obtained in (22).
- For *subregion ii*, $\alpha_{k,n}^*(p_{k,n}) = 0$ and $p_{k,n} < \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right) \sigma^2$ (which can be true only when $|h_{k,n}|^2 > |\beta_{k,n}|^2$). The set of all feasible candidates for $(p_{k,n}^*, \alpha_{k,n}^*)$ in this case is given by $\Psi_1(\alpha_{k,n} = 0)$ obtained via (23).

2) Region II ($0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$): As we have discussed, $R_{k,n}^s = 0$ in this case, which can be true only when $|h_{k,n}|^2 < |\beta_{k,n}|^2$. The Lagrangian can thus be rewritten as

$$\mathcal{L}'_n(\boldsymbol{P}_n, \boldsymbol{\alpha}_n) = p_{k,n} \left(\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{l,n}|^2 - \gamma \right), \tag{35}$$

which is a linear function of $p_{k,n}$ and is regardless of $\alpha_{k,n}$. Here, we set $\alpha_{k,n}^* = 0$ for convenience. The feasible candidate $(\hat{p}_{k,n}, \hat{\alpha}_{k,n})$ in this region can thus be obtained as[3]

$$(\hat{p}_{k,n}, \hat{\alpha}_{k,n}) = \left(\min\{[\mathcal{X}_{k,n}(\alpha_{k,n} = 0)]^+, P_{\text{peak}}\}, 0 \right)$$
$$= (P_{\text{peak}}, 0). \tag{36}$$

It is observed that the feasibility of the above two regions is determined by the channel conditions and the peak power constraint. Five scenarios are illustrated in Fig. 4 and explained as follows:

1) In *scenario (a)*, $|h_{k,n}|^2 < |\beta_{k,n}|^2$ and $P_{\text{peak}} > \mathcal{X}_{k,n}(\alpha_{k,n} = 1)$. Both *Region II* and *subregion i* in *Region I* are feasible. Note that curve $\alpha_{k,n}^*(p_{k,n})$ and curve $p_{k,n} = \mathcal{X}_{k,n}(\alpha_{k,n})$ intersect at $(\mathcal{X}_{k,n}(\alpha_{k,n} = 1), 1)$.
2) In *scenario (b)*, $|h_{k,n}|^2 < |\beta_{k,n}|^2$ and $P_{\text{peak}} \leq \mathcal{X}_{k,n}(\alpha_{k,n} = 1)$. Only *Region II* is feasible.
3) In *scenario (c)*, $|h_{k,n}|^2 = |\beta_{k,n}|^2$. $\alpha_{k,n}^* = \frac{1}{2}$ in this scenario so only *subregion i* in *Region I* is feasible.

---

[3]Note that here we assume $\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{k,n}|^2 > \gamma$. This is because according to the SC allocation policy as we will discuss in later, SC n will be allocated to IR k only if $\mathcal{L}_n$ is positive. If $\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{k,n}|^2 \leq \gamma$, $\mathcal{L}_n$ cannot be positive regardless of $p_{k,n}$. As a result, we ignore the case of $\sum_{l \in \mathcal{K}_2} \lambda_l \zeta_l |h_{k,n}|^2 \leq \gamma$ without loss of generality.
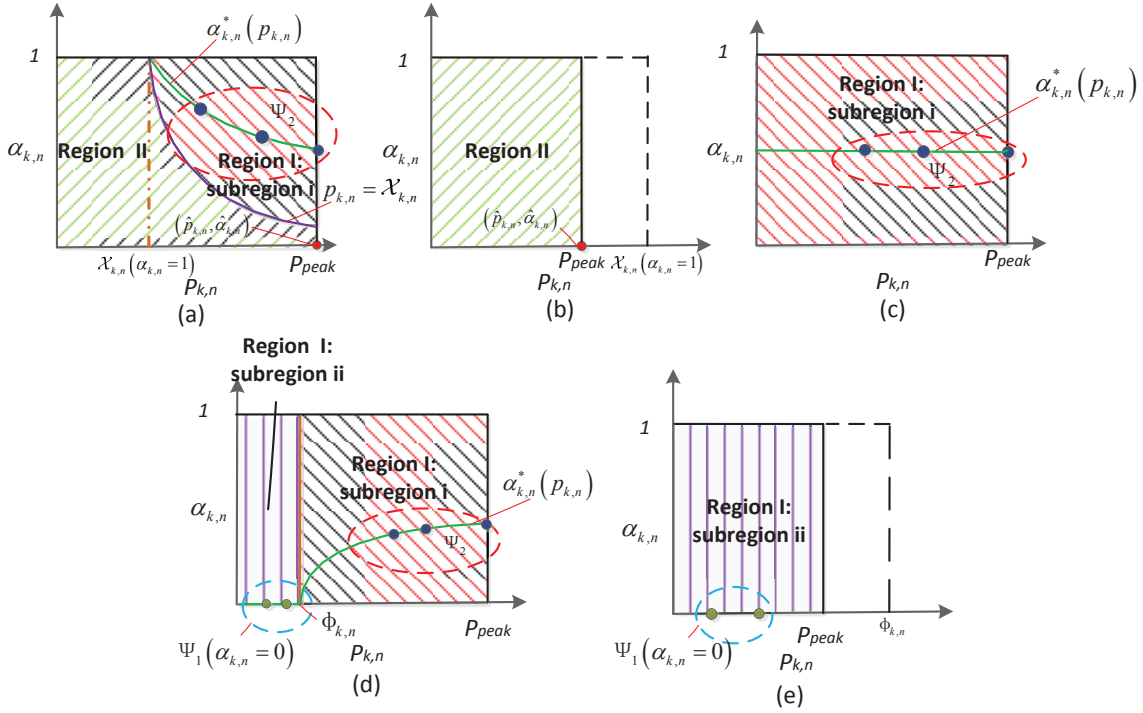
Fig. 4. Five scenarios of feasible regions, where $\phi_{k,n} = \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right)$.

4) In *scenario (d)*, $|h_{k,n}|^2 > |\beta_{k,n}|^2$ and $P_{\text{peak}} > \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right)$. Two subregions in *Region I* are feasible.

5) In *scenario (e)*, $|h_{k,n}|^2 > |\beta_{k,n}|^2$ and $P_{\text{peak}} \leq \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right)$. Only *subregion i* in *Region I* is feasible.

Next, we denote $\mathcal{F}$ as the feasible set by combining the above discussions as follows:

$$
\mathcal{F} = \begin{cases}
\Psi_2 \cup \{(P_{\text{peak}}, 0)\}, & \text{if } P_{\text{peak}} > \mathcal{X}_{k,n}(\alpha_{k,n} = 1) \\
& \text{and } |h_{k,n}|^2 < |\beta_{k,n}|^2, \\
\{(P_{\text{peak}}, 0)\}, & \text{if } P_{\text{peak}} \leq \mathcal{X}_{k,n}(\alpha_{k,n} = 1) \\
& \text{and } |h_{k,n}|^2 < |\beta_{k,n}|^2, \\
\Psi_2, & \text{if } |h_{k,n}|^2 = |\beta_{k,n}|^2, \\
\Psi_2 \cup \Psi_1(\alpha_{k,n} = 0), & \text{if } P_{\text{peak}} > \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right) \\
& \text{and } |h_{k,n}|^2 > |\beta_{k,n}|^2, \\
\Psi_1(\alpha_{k,n} = 0), & \text{if } P_{\text{peak}} \leq \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right) \\
& \text{and } |h_{k,n}|^2 > |\beta_{k,n}|^2.
\end{cases}
$$

Given SC n being allocated to IR k, the jointly optimized $(p_{k,n}^*, \alpha_{k,n}^*)$ is obtained as

$$
(p_{k,n}^*, \alpha_{k,n}^*) = \arg \max_{(p_{k,n}, \alpha_{k,n}) \in \mathcal{F}} \mathcal{L}_n(p_{k,n}, \alpha_{k,n}). \tag{37}
$$

The above algorithm is summarized as Algorithm 1.

Algorithm 1 Joint optimization of $p_{k,n}^*$ and $\alpha_{k,n}^*$

1: **if** $|h_{k,n}|^2 > |\beta_{k,n}|^2$ **then**
2:     **if** $P_{\text{peak}} > \left(\frac{1}{|\beta_{k,n}|^2} - \frac{1}{|h_{k,n}|^2} \right)$ **then**
3:         Compute $\mathcal{F} = \Psi_1(\alpha_{k,n} = 0) \cup \Psi_2$ via (23) and (30).
4:     **else**
5:         Compute $\mathcal{F} = \Psi_1(\alpha_{k,n} = 0)$ via (23).
6:     **end if**
7: **else if** $|h_{k,n}|^2 = |\beta_{k,n}|^2$ **then**
8:     Compute $\mathcal{F} = \Psi_2$ via (30).
9: **else if** $P_{\text{peak}} > \mathcal{X}_{k,n}(\alpha_{k,n} = 1)$ **then**
10:     Compute $\mathcal{F} = \Psi_2 \cup \{(P_{\text{peak}}, 0)\}$ via (30).
11: **else**
12:     Set $\mathcal{F} = \{(P_{\text{peak}}, 0)\}$.
13: **end if**
14: Compute $(p_{k,n}^*, \alpha_{k,n}^*)$ according to (37).

B. Subcarrier Allocation

Substituting the optimal $p_{k,n}^*$ and $\alpha_{k,n}^*$ into $\mathcal{L}'_n$, the optimal SC assignment policy is given by

$$
x_{k,n}^* = \begin{cases}
1, & \text{if } k = k^* = \arg \max_{k \in \mathcal{K}_1} \mathcal{L}'_n(p_{k,n}^*, \alpha_{k,n}^*) \\
& \text{and } \max_{k \in \mathcal{K}_1} \mathcal{L}'_n(p_{k,n}^*, \alpha_{k,n}^*) > 0, \\
0, & \text{otherwise}
\end{cases} \tag{38}
$$

C. Dual Update

According to [28], the dual problem is always convex; hence, the subgradient method can be used to update the dual

Algorithm 2 Optimal Algorithm for Problem (13a)

1: **repeat**
2:     Jointly optimize $p_{k,n}^*$ and $\alpha_{k,n}^*$ for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}$ according to Algorithm 1.
3:     Solve SC allocation $x_{k,n}^*$ for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}$ according to (38).
4:     Update $\boldsymbol{\lambda}$ and γ according to (39) and (40), respectively.
5: **until** $\boldsymbol{\lambda}$ and γ converges.

variables to the optimal ones by an iterative procedure:

$$\lambda_l^{t+1} = \left[\lambda_l^t - \xi_l \left(Q_l - \bar{Q}_l \right) \right]^+, \forall l \in \mathcal{K}_2, \tag{39}$$

$$\gamma^{t+1} = \left[\gamma^t - \nu \left(P_{\max} - \sum_{n \in \mathcal{N}} \sum_{k \in \mathcal{K}_1} x_{k,n} p_{k,n} \right) \right]^+, \tag{40}$$

where $t \geq 0$ is the iteration index, $[\xi_1, ..., \xi_{K_2}]$ and ν are properly designed positive step-sizes.

Note that the subgradient method is an iterative method for solving convex optimization problems in general, and the proposed algorithm is a direct application of the subgradient method to our problem. Thus the convergence and optimality of the proposed algorithm can be guaranteed.

D. Complexity

The complexity of this iterative algorithm is analyzed as follows. For each SC, $\mathcal{O}(K_2)$ computations are needed for solving Ω_n in (28) and $\mathcal{O}(K_1)$ computations are needed for searching the best IR. Since the optimization is independent at each SC, the complexity is $\mathcal{O}(KN)$ for each iteration. Last, the complexity of subgradient based updates is polynomial in the number of dual variables $K_2 + 1$ [28]. As a result, the overall complexity of the proposed algorithm for solving problem (13a) is $\mathcal{O}((K_2 + 1)^q KN)$, where q is a positive constant. Note that the complexity is polynomial.

Finally, we summarize the overall algorithm for solving problem (13a) in Algorithm 2.

IV. SUBOPTIMAL SOLUTION

The complexity of the optimal algorithm becomes high as K_1, K_2 and/or N increases, mainly due to the updating of the Lagrange multipliers $\boldsymbol{\lambda}$ and γ. By eliminating the dual updates, in this section, we present an efficient suboptimal algorithm which significantly reduces the complexity.

We design a two-stage algorithm by assuming equal power allocation, i.e., $p_{k,n} = \min\{P_{\text{peak}}, P_{\max}/N\}, \forall k \in \mathcal{K}_1, n \in \mathcal{N}$. Here we drop index k and n of $p_{k,n}$ for brevity. In the first stage, for each unsatisfied ER k, we select the SC at which ER k has the largest channel gain among all unsatisfied ERs and then assign this SC to the IR k that has the largest channel gain among all IRs. The above process is repeated until the minimum harvested power of all the ERs are satisfied. We denote N_1 as the number of SCs assigned in this stage given in the set $\mathcal{N}_1$, and N_2 as the number of unassigned SCs in the set $\mathcal{N}_2$.

Algorithm 3 Suboptimal Algorithm for Problem (13a)

1: Set $\mathcal{N}_1 = \emptyset$, and $p = \min\{P_{\text{peak}}, P_{\max}/N\}$.
2: **for** Each ER l **do**
3:     Compute $Q_l = \zeta_l p \sum_{n \in \mathcal{N}_1} |h_{l,n}|^2$.
4:     **repeat**
5:         Find unassigned SC n that has the largest channel gain for ER l.
6:         Set $\mathcal{N}_1 \leftarrow \mathcal{N}_1 \cup n$ and assign SC n to IR k having the largest channel gain.
7:         Determine the optimal transmit power splitting ratio $\alpha_{k,n}^*$ by using (22).
8:         Compute $Q_l \leftarrow Q_l + \zeta_l p |h_{l,n}|^2$.
9:     **until** $Q_l \geq \bar{Q}_l$
10: **end for**
11: **for** The rest N_2 of unassigned SCs **do**
12:     Determine the optimal transmit power splitting ratios $\alpha_{k,n}^*$ via (22), for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}_2$.
13:     Solve SC allocation variable $x_{k,n}^*$ for all $k \in \mathcal{K}_1$ and $n \in \mathcal{N}_2$ by using greedy method.
14: **end for**

In the second stage, we consider the following problem that is simplified from problem (13a).

$$\max_{\boldsymbol{X}, \boldsymbol{\alpha}} R_{\text{sum}}^s \tag{41}$$

$$\text{s.t.} \quad (13e) - (13g).$$

Note that all ERs' constraints on required harvested power are removed as they are already achieved after the first stage. The simplified problem (41) for power allocation, SC assignment and determining transmit power splitting ratios can be regarded as a special case of problem (13a). Accordingly, we can obtain the optimal transmit power splitting ratios by (22). After that, the problem is reduced to a SC assignment problem for weighted sum secrecy rate maximization, which can be optimally solved by a greedy algorithm, i.e., each SC is assigned to the IR having the largest weighted secrecy rate. Note that the ERs can harvest additional energy from the SCs assigned to the IRs in the second stage.

The above suboptimal algorithm is summarized in Algorithm 3. The complexity order of the first stage is $\mathcal{O}(K_2 N_1)$ and the complexity order of the second stage is $\mathcal{O}(K_1 N_2)$. Thus the total complexity is thus given as $\mathcal{O}(K_2 N_1 + K_1 N_2)$ which is upper-bounded by $\mathcal{O}(KN)$ and is much lower than that of Algorithm 2.

V. NUMERICAL RESULTS

In this section, we evaluate the performance of the proposed algorithms through extensive simulations. In the simulation setup, a single cell with radius of 200 meters (m) is considered. The BS is located at the centre of the cell. The carrier frequency is 900 MHz and the bandwidth is 1 MHz. We assume the noise power $\sigma^2 = -83$ dBm, and antenna gains to be 0 dB. The peak transmit power constraint is set to be $P_{\text{peak}} = \infty$. We consider $K_1 = 4$ IRs that are randomly located in the cell with distance to the BS uniformly distributed. For each IR, we set $w_k = 1, \forall k \in \mathcal{K}_1$, i.e., we consider the sum
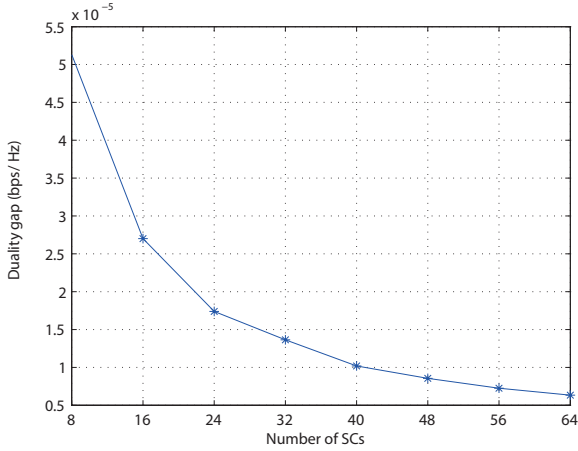
Fig. 5. Duality gap versus number of SCs.

Fig. 6. Transmit power and power split for information source on each SC.

Fig. 7. Achievable secrecy rate R_{sum}^s versus required harvested power $\bar{Q}$.

secrecy rate of all IRs. We also consider $K_2 = 4$ ERs that are uniformly distributed within the circle of radius of 2 m around the BS.[4] For each ER, we set $\zeta_l = 60\%, \forall l \in \mathcal{K}_2$. The channel coefficients consist of both large-scale fading and small-scale fading. The path loss exponent is set to be 3. The small-scale fading is modeled as Rayleigh fading and each channel realization is composed of 8 i.i.d. Rayleigh fading paths. We also assume that all ERs have the same harvested power requirement, i.e., $\bar{Q}_l = \bar{Q}, \forall l \in \mathcal{K}_2$.

For performance comparison, we also consider the following benchmarking schemes. First, the fixed transmit power splitting ratio with $\alpha_{k,n} = 0.5, \forall k \in \mathcal{K}_1, n \in \mathcal{N}$ is considered for complexity reduction, while the power and SC allocation is still optimized as in Algorithm 2. In this case we drop the index k and n of $\alpha_{k,n}$ for brevity. Second, the SC assignment is fixed (FSA) while the power allocation and transmit power splitting are jointly optimized as in Algorithm 2. Last, we also consider the scheme without using AN (NoAN). It is worth noting that NoAN performs the same as the traditional AN scheme (AN scheme without cancelling) as we have discussed in Remark 1.

First, the duality gaps with different number of SCs N are shown in Fig. 5. It is observed that duality gap is very small and becomes smaller as N increases. For the case of $N = 64$, the gap becomes smaller than 1×10^{-5} bps/Hz, thus is considered to be negligible.

We also show the allocated transmit power and power split for information source over SCs in Fig. 6, with $\bar{Q} = 100$ μW. First, we observe that for the case where $P_{\mathrm{max}} = 37$dBm, the allocated power on each SC is almost uniform, which shows that the suboptimal algorithm that allocates power uniformly over SCs may perform closer to the optimal algorithm as P_{max} increases. In addition, we observe that the power used for information source is approximately one half of the power allocated on each corresponding SC, i.e., the optimal $\alpha_{k,n} \approx 0.5$. This is because, according to (22), we have the optimal

$\alpha_{k,n}^* \approx \frac{1}{2}$ in the high SNR region. In our simulation setup, the noise power is relatively small and results in high $\frac{p_{k,n}}{\sigma^2}$ and thus the optimal solution $\alpha_{k,n}^* \approx \frac{1}{2}$.

In Fig. 7, the sum secrecy rate R_{sum}^s versus the harvested power requirement $\bar{Q}$ is shown with $P_{\mathrm{max}} = 37$ dBm and $N = 64$. First, for all schemes (except NoAN), the sum secrecy rate is observed to decrease with increasing $\bar{Q}$. It is also observed that the suboptimal algorithm and the optimal algorithm outperform FSA and NoAN and the suboptimal algorithm incurs at most 30% loss in secrecy rate compared to the optimal algorithm. An interesting observation is that the scheme with $\alpha = 0.5$ performs closely to the proposed optimal algorithm, which is in accordance to our previous discussion that $\alpha_{k,n}^* \approx \frac{1}{2}$ in the high SNR region. The poor performance of FSA compared to the proposed algorithms indicates that dynamic SC allocation provides significant gain in terms of sum secrecy rate. Moreover, all considered schemes with AN achieve significant rate-energy gains compared to NoAN, which has almost zero sum secrecy rate even if there

---

[4]We consider ERs in general closer to the BS than IRs to receive larger power (versus that of IRs used for decoding information against background noise only). However, under this circumstance, ERs in general have better channel conditions than IRs, and as a result they are more capable of eavesdropping the information sent by the BS [18].
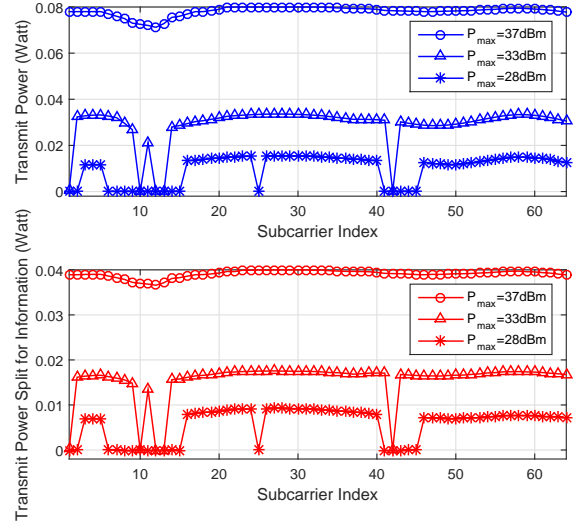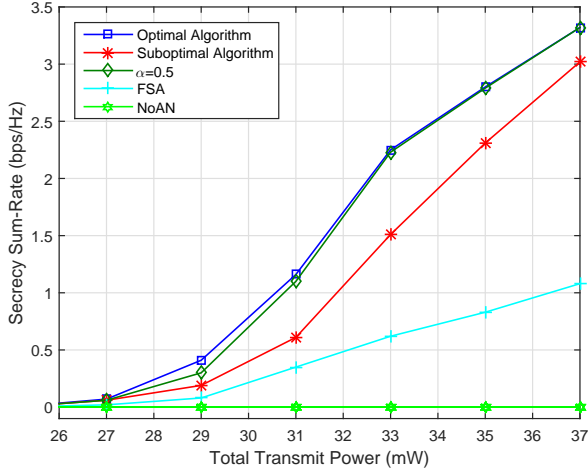
Fig. 8. Achievable secrecy rate R^s_{sum} versus total transmit power constraint $P_{\max}$.

Fig. 9. Achievable secrecy rate R^s_{sum} versus the number of ERs.

is no harvested power requirement. This is because without the effective aid of the AN, the secrecy rate on each SC is positive only when it is assigned to the receiver of largest channel gain [11]. However, in our simulation setup, the ERs possess much better channel gains compared to the IRs, due to shorter distances to the BS. As a result, $|h_{k,n}|^2 < |\beta_{k,n}|^2$ is almost true for all $n \in \mathcal{N}, k \in \mathcal{K}_1$, and hence no secrecy information can be transmitted at all. This demonstrates the effectiveness of the proposed frequency-domain AN aided approach.

Fig. 8 demonstrates the sum secrecy rate R^s_{sum} versus the total transmit power $P_{\max}$, with the harvested power constraint set as $\bar{Q} = 100 \ \mu$W and $N = 64$. Compared with FSA and NoAN, both proposed optimal and suboptimal algorithms perform better. In addition, it can be observed that suboptimal algorithm performs more closely to the optimal algorithm as the total transmit power increases, which collapses to the observation from Fig. 7 that the allocated power on SCs is more uniformly distributed as transmit power increases. Moreover, the scheme with $\alpha = 0.5$ is also observed to perform very closely to the optimal algorithm.

Fig. 9 illustrates the sum secrecy rate versus the number of ERs, with the harvested power requirement set as $\bar{Q} = 100 \ \mu$W, $P_{\max} = 37$ dBm and $N = 64$. First, we observe that with the increasing number of ERs, the sum secrecy rate of IRs for all schemes decreases. This is because when a new ER is added in the system, $|\beta_{k,n}|^2$ may increase for all IRs at any SC n. As a result, secrecy information is more easily eavesdropped. In addition, with more ERs, more power will be allocated to the SCs for satisfying the requirements of the ERs but not necessarily achieving the maximum sum secrecy rate for IRs. It is also observed that FSA becomes infeasible when the number of ERs is larger than 55, while the proposed algorithms perform with noticeably higher sum secrecy rate.

VI. CONCLUSION

This paper studies the optimal resource allocation for OFDMA-based SWIPT with secrecy constraints. With a proposed frequency-domain AN generation and removal method,
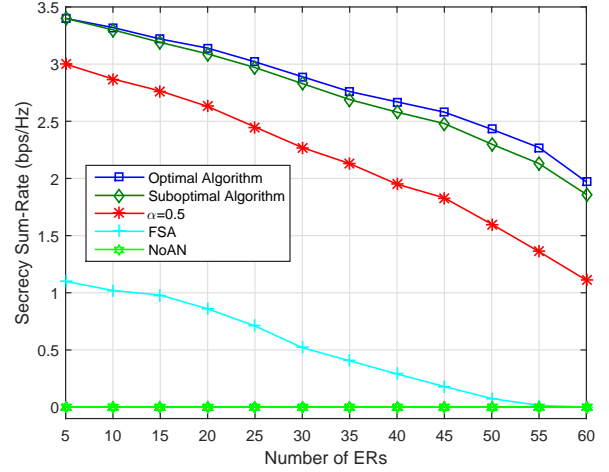
we maximize the weighted sum secrecy rate for IRs subject to individual harvested power constraints of ERs by jointly optimizing transmit power and SC allocation as well as transmit power splitting ratios over SCs for AN signals. We proposed an algorithm based on the Lagrange duality to solve the formulated problem with polynomial time complexity. We also proposed a suboptimal algorithm with lower complexity. Through extensive simulations, we showed that the proposed algorithms outperform other heuristically designed schemes with or without using the AN.

APPENDIX A
PROOF OF LEMMA 1

We consider the following two cases:

1) $\alpha_{k,n} \neq 0$: Equating $r_{k,n} - r^e_{k,n}$ to zero, we obtain

$$\frac{|h_{k,n}|^2 p_{k,n}}{\sigma^2} = \frac{|\beta_{k,n}|^2 p_{k,n}}{\alpha_{k,n}|\beta_{k,n}|^2 p_{k,n} + \sigma^2}. \tag{42}$$

We thus have $p_{k,n} = 0$ or $p_{k,n} = \mathcal{X}_{k,n}(\alpha_{k,n})$. However, $p_{k,n}$ is always non-negative, so $p_{k,n} = \mathcal{X}_{k,n}(\alpha_{k,n}) > 0$ can be true only when $|h_{k,n}|^2 < |\beta_{k,n}|^2$. Thus, it is shown that $r_{k,n} - r^e_{k,n} = 0$ has one root at $p_{k,n} = 0$, when $|h_{k,n}|^2 \geq |\beta_{k,n}|^2$, and two roots at $p_{k,n} = 0$ and $p_{k,n} = \mathcal{X}_{k,n}(\alpha_{k,n})$, when $|h_{k,n}|^2 < |\beta_{k,n}|^2$.

For brevity, we define $x \triangleq \alpha_{k,n}$, $y \triangleq p_{k,n}$, $h \triangleq |h_{k,n}|^2/\sigma^2$ and $g \triangleq |\beta_{k,n}|^2/\sigma^2$. When $|h_{k,n}|^2 < |\beta_{k,n}|^2 \Leftrightarrow h < g$, it follows that

$$\frac{\partial(r_{k,n} - r^e_{k,n})}{\partial p_{k,n}}\bigg|_{p_{k,n}=\mathcal{X}_{k,n}(\alpha_{k,n})} \triangleq \frac{\partial f}{\partial y}\bigg|_{y=\mathcal{X}_{k,n}(x)}$$

$$= \frac{g}{\ln 2[(1-g/h)/x - 1]} - \frac{gx}{\ln 2[(1-g/h) - 1]}$$

$$+ \frac{h(1-x)}{\ln 2((h/g-1)(x-1)/x + 1)}$$

$$= \frac{hx(g-h)(1-x)}{\ln 2(g-h+hx)}$$

$$\geq 0. \tag{43}$$

Hence, $r_{k,n} - r_{k,n}^e \leq 0$ when $0 \leq p_{k,n} \leq \mathcal{X}_{k,n}(\alpha_{k,n})$ and $|h_{k,n}|^2 < |\beta_{k,n}|^2$, which is equivalent to $0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$. On the other hand, $r_{k,n} - r_{k,n}^e > 0$ when i) $p_{k,n} > \mathcal{X}_{k,n}(\alpha_{k,n})$ and $|h_{k,n}|^2 < |\beta_{k,n}|^2$ or ii) $p_{k,n} > 0$ and $|h_{k,n}|^2 \geq |\beta_{k,n}|^2$, which is equivalent to $p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$.

2) $\alpha_{k,n} = 0$: In this case, we have

$$R_{k,n}^s = \begin{cases} 0, & \text{if } |\beta_{k,n}|^2 \geq |h_{k,n}|^2 \\ r_{k,n} - r_{k,n}^e > 0, & \text{if } |\beta_{k,n}|^2 < |h_{k,n}|^2 \end{cases}. \quad (44)$$

Forcing $[\mathcal{X}_{k,n}]^+ \to +\infty$ when $|\beta_{k,n}|^2 \geq |h_{k,n}|^2$ and $[\mathcal{X}_{k,n}]^+ = 0$ when $|\beta_{k,n}|^2 < |h_{k,n}|^2$, (44) is equivalently written as

$$R_{k,n}^s = \begin{cases} 0, & \text{if } 0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}]^+ \\ r_{k,n} - r_{k,n}^e > 0, & \text{if } p_{k,n} > [\mathcal{X}_{k,n}]^+ \end{cases}. \quad (45)$$

Combining the above two cases, we can finally conclude that $R_{k,n}^s = 0$ when $0 \leq p_{k,n} \leq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$, while $R_{k,n}^s = r_{k,n} - r_{k,n}^e > 0$ when $p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$.

The proof is thus completed.

APPENDIX B
OPTIMAL TRANSMIT POWER SPLITTING RATIO FOR TRADITIONAL AN SCHEME

When the AN cannot be cancelled at the intended IR, the secrecy rate in (8) should be rewritten as

$$\begin{aligned} R_{k,n}^{s,NC} &= [r_{k,n} - r_{k,n}^e]^+ \\ &= \left[\log_2\left(1 + \frac{(1-\alpha_{k,n})|h_{k,n}|^2 p_{k,n}}{\alpha_{k,n}|h_{k,n}|^2 p_{k,n} + \sigma^2}\right) \right. \\ &\quad \left. - \log_2\left(1 + \frac{(1-\alpha_{k,n})|\beta_{k,n}|^2 p_{k,n}}{\alpha_{k,n}|\beta_{k,n}|^2 p_{k,n} + \sigma^2}\right)\right]^+. \quad (46) \end{aligned}$$

We first consider the problem $\max_{\alpha_{k,n}} R_{k,n}^{s,NC}$ by focusing on the following two cases:

1) For the case that $|h_{k,n}|^2 > |\beta_{k,n}|^2$, we have $R_{k,n}^{s,NC} > 0$ and

$$\begin{aligned} &\frac{\partial R_{k,n}^{s,NC}}{\partial \alpha_{k,n}} \\ &= -\frac{1}{\ln 2}\frac{(|h_{k,n}|^2 - |\beta_{k,n}|^2)\sigma^2 p_{k,n}}{(\alpha_{k,n}|h_{k,n}|^2 p_{k,n} + \sigma^2)(\alpha_{k,n}|\beta_{k,n}|^2 p_{k,n} + \sigma^2)} \\ &\leq 0. \quad (47) \end{aligned}$$

Thus, we have that $R_{k,n}^{s,NC}$ is monotonically non-increasing with respect to $\alpha_{k,n}$ and the optimal solution is given by $\alpha_{k,n}^* = 0, \forall k, n$.

2) For the case that $|h_{k,n}|^2 \leq |\beta_{k,n}|^2$, we have $R_{k,n}^{s,NC} = 0$ regardless of $\alpha_{k,n}$.

Combining the above two cases, we conclude that $\alpha_{k,n}^* = 0, \forall k, n$, is always optimal to maximize the secrecy rate using traditional AN scheme without cancelation at the receiver, i.e., the traditional AN scheme performs no better than the transmission without AN.

In addition, to show $\alpha_{k,n}^* = 0, \forall k, n$ is also the optimal solution to the sum secrecy rate maximization problem under energy harvesting constraints similar to problem (13a), we consider the following problem

$$\max_{\boldsymbol{\alpha}} \sum_{k \in \mathcal{K}_1} \sum_{n \in \mathcal{N}} R_{k,n}^{s,NC} \quad (48)$$

$$\text{s.t.} \quad (13b) - (13g).$$

We can show the decomposed Lagrangian on each SC $\mathcal{L}_n$ of problem (48) is obtained in (18) by replacing $R_{k,n}^s$ with $R_{k,n}^{s,NC}$ and

$$\frac{\partial \mathcal{L}_n}{\partial \alpha_{k,n}} = w_k \frac{\partial R_{k,n}^{s,NC}}{\partial \alpha_{k,n}} \leq 0. \quad (49)$$

Thus, the solution $\alpha_{k,n}^* = 0, \forall k, n$ also holds optimality for problem (48).

APPENDIX C
PROOF OF LEMMA 2

By applying the KKT (Karush-Kuhn-Tucker) conditions [28], we obtain

$$\alpha_{k,n}^*(p_{k,n}) = \left[\frac{1}{2} + \frac{\sigma^2}{2p_{k,n}}\left(\frac{1}{|h_{k,n}|^2} - \frac{1}{|\beta_{k,n}|^2}\right)\right]_0^1, \quad (50)$$

for all $k \in \mathcal{K}_1, n \in \mathcal{N}$, where $[\cdot]_a^b \triangleq \min\{\max\{\cdot, a\}, b\}$.

When $|h_{k,n}|^2 < |\beta_{k,n}|^2$, $p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+ = \mathcal{X}_{k,n}(\alpha_{k,n})$, we thus have

$$\begin{aligned} \alpha_{k,n}^* &= \left[\frac{1}{2} + \frac{(|\beta_{k,n}|^2 - |h_{k,n}|^2)\sigma^2}{2|\beta_{k,n}|^2|h_{k,n}|^2 p_{k,n}}\right]_0^1 \\ &< \frac{1}{2} + \frac{(|\beta_{k,n}|^2 - |h_{k,n}|^2)\sigma^2}{2|\beta_{k,n}|^2|h_{k,n}|^2 \mathcal{X}_{k,n}(\alpha_{k,n})} \\ &= \frac{1}{2} + \frac{\alpha_{k,n}^*}{2} \\ &< 1. \quad (51) \end{aligned}$$

When $|h_{k,n}|^2 \geq |\beta_{k,n}|^2$, $p_{k,n} > [\mathcal{X}_{k,n}(\alpha_{k,n})]^+ = 0$, we thus have

$$\alpha_{k,n}^* = \left[\frac{1}{2} + \frac{\sigma^2}{2p_{k,n}}\left(\frac{1}{|h_{k,n}|^2} - \frac{1}{|\beta_{k,n}|^2}\right)\right]_0^1 < \frac{1}{2}. \quad (52)$$

To conclude the above two cases, we have $\alpha_{k,n}^* < 1$ is always true for $p_{k,n} \geq [\mathcal{X}_{k,n}(\alpha_{k,n})]^+$. Thus the optimal $\alpha_{k,n}^*$ with given $p_{k,n}$ is rewritten as

$$\alpha_{k,n}^*(p_{k,n}) = \left[\frac{1}{2} + \frac{\sigma^2}{2p_{k,n}}\left(\frac{1}{|h_{k,n}|^2} - \frac{1}{|\beta_{k,n}|^2}\right)\right]^+, \quad (53)$$

for all $k \in \mathcal{K}_1, n \in \mathcal{N}$.

The proof is thus completed.

REFERENCES

[1] M. Zhang, Y. Liu, and R. Zhang, "Secrecy information and power transfer in OFDMA systems," in *Proc. IEEE Global Commun.Conf. (Globecom)*, 2015.

[2] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[3] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: architecture design and rate-energy tradeoff," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4757–4767, November 2013.

[4] L. Liu, R. Zhang, and K. Chua, "Wireless information transfer with opportunistic energy harvesting," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 288–300, January 2013.

[5] L. Liu, R. Zhang, and K. C. Chua, "Wireless information and power transfer: a dynamic power splitting approach," *IEEE Trans. Commun.*, vol. 61, no. 9, pp. 3990–4001, September 2013.

[6] D. W. K. Ng and R. Schober, "Spectral efficient optimization in OFDM systems with wireless information and power transfer," in *Proc. European Signal Processing Conference (EUSIPCO)*, September 2013, pp. 1–5.

[7] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer in multiuser OFDM systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 4, pp. 2282–2294, April 2014.

[8] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation in multiuser OFDM systems with wireless information and power transfer," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, 2013.

[9] J. Xu, L. Liu, and R. Zhang, "Multiuser MISO beamforming for simultaneous wireless information and power transfer," *IEEE Trans. Signal Process.*, vol. 62, no. 18, pp. 4798–4810, Sept 2014.

[10] S. K. L. Y. Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, July 1978.

[11] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, September 2011.

[12] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multicarrier broadcast channel," in *Proc. Int. Conf. Telecommun. (ICT)*, January 2008, pp. 1–6.

[13] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmission over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 1354–1367, August 2012.

[14] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, January 2008.

[15] H. Qin, Y. Sun, T. Chang, X. Chen, C. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Commun.*, vol. 12, pp. 2717–2729, June 2012.

[16] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 3831–3842, October 2010.

[17] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, April 2012.

[18] L. Liu, R. Zhang, and K. C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Proc.*, vol. 62, no. 7, pp. 1850–1863, April 2014.

[19] D. W. K. Ng and R. Schober, "Resource allocation for secure communication in systems with wireless information and power transfer," in *Proc. IEEE Global Commun.Conf. (Globecom)*, 2013.

[20] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," 2015, to appear in *IEEE Trans. Veh. Technol.*. [Online]. Available: http://arxiv.org/abs/1408.1987

[21] M. Zhang and Y. Liu, "Energy harvesting for physical-layer security in OFDMA networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 154 – 162, January 2016.

[22] W. Harrison, J. Almeida, S. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 575–584, September 2011.

[23] W. Harrison and S. McLaughlin, "Tandem coding and cryptography on wiretap channels: EXIT chart analysis," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, June 2009, pp. 1939–1943.

[24] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, pp. 52–55, February 2000.

[25] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 2009.

[26] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, pp. 1310–1322, July 2006.

[27] K. Seong, M. Mohseni, and J. M. Cioffi, "Optimal resource allocation for OFDMA downlink systems," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, July 2006.

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