Energy-Efficient Resource Allocation for Secure OFDMA Systems

Derrick Wing Kwan Ng, *Student Member, IEEE*, Ernest S. Lo, *Member, IEEE*, and Robert Schober, *Fellow, IEEE*

***Abstract*—In this paper, resource allocation for energy-efficient secure communication in an orthogonal frequency-division multiple-access (OFDMA) downlink network is studied. The considered problem is modeled as a nonconvex optimization problem that takes into account the sum-rate-dependent circuit power consumption, multiple-antenna eavesdropper, artificial noise generation, and different quality-of-service (QoS) requirements, including a minimum required secrecy sum rate and a maximum tolerable secrecy outage probability. The power, secrecy data rate, and subcarrier allocation policies are optimized for maximization of the energy efficiency of secure data transmission (bit/joule securely delivered to the users). The considered nonconvex optimization problem is transformed into a convex optimization problem by exploiting the properties of fractional programming, which results in an efficient iterative resource allocation algorithm. In each iteration, the transformed problem is solved by using dual decomposition. Simulation results illustrate that the proposed iterative resource allocation algorithm not only converges in a small number of iterations but maximizes the system energy efficiency and guarantees a nonzero secrecy data rate for the desired users as well. In addition, the obtained results unveil a tradeoff between energy efficiency and secure communication.**

***Index Terms*—Artificial noise generation, energy efficiency, green communications, multiple-input–multiple-output (MIMO) beamforming, passive eavesdropper, physical (PHY) layer security.**

I. Introduction

ORTHOGONAL frequency-division multiple access (OFDMA) is a promising candidate for high-speed wireless multiuser communication networks, such as the Third-Generation Partnership Project (3GPP) Long-Term Evolution Advanced, IEEE 802.16 worldwide interoperability for microwave access, and IEEE 802.22 wireless regional area networks, not only because of its robustness against multipath fading, but because of its flexibility in resource allocation as well. In an OFDMA system, the fading coefficients of different subcarriers are likely to be statistically independent for different users. With channel state information at the transmitter (CSIT), the maximum system throughput (bits per second) can be achieved by selecting the best user for each subcarrier and adapting the corresponding transmit power, which yields a multiuser diversity (MUD) gain [1], [2]. On the other hand, the increasing interest in multimedia services has led to a tremendous demand for high-data-rate communications with certain guaranteed quality-of-service (QoS) properties. This demand has significant financial implications for service providers because of the rapidly increasing energy consumption. As a result, energy-efficient system designs, which adopt energy efficiency (bits per joule) as the performance metric, have recently received much attention in both industry and academia [3]–[7]. In [3] and [4], power allocation algorithms for energy-efficient multicarrier systems were studied assuming a static circuit power consumption. In [5] and [6], energy-efficient link adaptation for a sum rate-dependent dynamic circuit power consumption was considered. However, if user selection and link adaptation are jointly optimized, the algorithms proposed in [3]–[6] may no longer be applicable. In [7], a risk-return model was proposed for energy-efficient power allocation in multicarrier systems. Yet, the proposed algorithm is suboptimal and does not achieve the maximum energy efficiency.

On the other hand, a large amount of work has recently been devoted to information-theoretic physical (PHY) layer security [8]–[18] as a complement to traditional cryptographic encryption adopted in the application layer. The pioneering work on PHY layer security by Wyner [8] showed that in a wiretap channel, a source and a destination can exchange perfectly secure messages with a nonzero rate if the desired receiver enjoys better channel conditions than the passive eavesdropper(s). In [9]–[11] and [12] and [13], resource allocation with PHY layer security considerations was studied for multicarrier and multiple input multiple output (MIMO) systems, respectively. In these works, the channel state information (CSI) of the eavesdroppers is assumed to be known at the base station (BS). In other words, a secure communication with nonzero data rate can always be guaranteed by carefully adapting the transmit power. Yet, eavesdroppers are usually passive and silent to hide their existence. Thus, the CSI of the eavesdroppers cannot be obtained via feedback from the eavesdroppers or be measured at the BS based on handshaking signals. To overcome this problem, multiple antennas and artificial noise generation have been proposed for security provision. In particular, by exploiting the extra degrees of freedom in a multiple-antenna system, artificial noise or interference is generated and injected into the null space of the desired users to degrade the channels of the eavesdroppers. In [14] and [15], the power allocation problem

Manuscript received January 17, 2012; revised April 14, 2012; accepted May 4, 2012. Date of publication May 14, 2012; date of current version July 10, 2012. This paper was presented in part at the 2011 Australia Communications Theory Workshop, Melbourne, Vic., Australia. The review of this paper was coordinated by Prof. N. Kato.

D. W. K. Ng and R. Schober are with the Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: wingn@ece.ubc.ca; rschober@ece.ubc.ca).

E. S. Lo is with the Centre Tecnològic de Telecomunicacions de Catalunya–Hong Kong, Kowloon, Hong Kong (e-mail: ernest.lo@ieee.org).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2012.2199145

for maximizing the ergodic secrecy capacity in single-user single-carrier systems with artificial noise generation, assuming the CSI of the eavesdropper is perfectly known at the BS is studied. However, the assumption of ergodic channels cannot be justified for delay-sensitive applications in practice since the transmitted packets of these applications experience slow fading. Hence, a secrecy outage [16, Ch. 5] occurs whenever the scheduled secrecy data rate exceeds the secrecy capacity between the BS and the desired users in the presence of eavesdropper(s), which introduces a QoS concern for secrecy. In [17] and [18], resource allocation algorithms with consideration of a probabilistic secrecy QoS metric and artificial noise injection for combating an eavesdropper in two-hop multicarrier systems is proposed. Nevertheless, the energy efficiency of the systems in [17] and [18] is unclear, and the optimization of the amount of power devoted to artificial noise generation for maximization of the energy efficiency remains an unsolved problem. Moreover, it is still unknown if there exists a tradeoff between energy efficiency and secrecy as far as resource allocation is concerned.

Motivated by the aforementioned observations, we formulate the resource allocation problem for energy-efficient secure communication in OFDMA systems with artificial noise generation as an optimization problem. By exploiting the properties of fractional programming, the considered nonconvex optimization problem is transformed to an equivalent convex optimization problem with a tractable solution, which can be obtained with an iterative algorithm. In each iteration, the transformed problem is solved by using dual decomposition, and closed-form power, secrecy data rate, and subcarrier allocation policies maximizing the energy efficiency are obtained. The proposed algorithm not only converges fast to the optimal solution but fulfills the secrecy outage tolerance requirements of the users as well.

The remainder of this paper is organized as follows. In Section II, we outline the model for secure OFDMA systems. In Section III, we define the performance metric and formulate the resource allocation with artificial noise generation as an optimization problem. In Section IV, the nonconvex optimization problem is solved via an iterative algorithm. Section V presents numerical performance results, and in Section VI, we conclude with a brief summary of our results.

II. Orthogonal Frequency-Division Multiple Access Downlink Network Model

In this section, after introducing the notation used in this paper, we present the adopted channel and signal models.

A. Notation

A complex Gaussian random variable with mean μ and variance σ^2 is denoted by $\mathcal{CN}(\mu, \sigma^2)$, and $\sim$ means "distributed as." $[x]^+ = \max\{0, x\}$. $E_X\{\cdot\}$ denotes statistical expectation with respect to (w.r.t.) random variable X. $\mathbb{C}^{N\times M}$ is the space of all $N \times M$ matrices with complex entries. $\|\cdot\|$ denotes the Euclidean norm of a matrix/vector. $[\cdot]^\dagger$ represents the conjugate transpose operation. $\mathbf{1}(\cdot)$ denotes an indicator function that is 1 when the event is true and 0 otherwise.

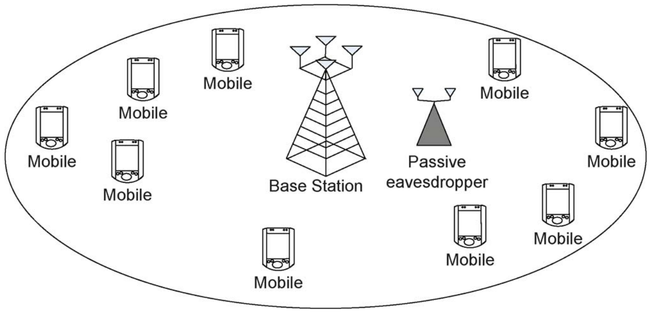

Fig. 1. OFDMA downlink network. There are one BS with $N_T = 4$ antennas, $K = 9$ desired users equipped with a single antenna, and one eavesdropper with $N_E = 2$ antennas. For an effective eavesdropping, the eavesdropper chooses a location closer to the BS compared with the locations of all the desired users.

B. Channel Model

We consider an OFDMA downlink network that consists of a BS with N_T antennas, an eavesdropper[1] with N_E antennas, and K mobile users equipped with a single antenna (cf. Fig. 1). We assume that $N_T > N_E$ to enable secure communication. The eavesdropper is passive, and its goal is to decode the information transmitted by the BS without causing interference to the communication channels. The impulse responses of all channels are assumed to be time invariant (slow fading). We consider an OFDMA system with n_F subcarriers. The received symbols at user k and the eavesdropper on subcarrier $i \in \{1, \ldots, n_F\}$ are, respectively, given by

$$\begin{aligned} y_k[i] &= \mathbf{h}_k[i]\mathbf{x}_k[i] + n[i] \\ \mathbf{y}_E[i] &= \mathbf{G}[i]\mathbf{x}_k[i] + \mathbf{e}[i] \end{aligned} \tag{1}$$

where $\mathbf{x}_k[i] \in \mathbb{C}^{N_T\times 1}$ denotes the transmitted symbol vector. $\mathbf{h}_k[i] \in \mathbb{C}^{1\times N_T}$ is the channel vector between the BS and user k on subcarrier i, and $\mathbf{G}[i] \in \mathbb{C}^{N_E\times N_T}$ is the channel matrix between the BS and the eavesdropper on subcarrier i. Both variables $\mathbf{h}_k[i]$ and $\mathbf{G}[i]$ include the effects of path loss and multipath fading. $n[i]$ is the additive white Gaussian noise (AWGN) in subcarrier i at user k with distribution $\mathcal{CN}(0, N_0)$, where N_0 is the noise power spectral density. $\mathbf{e}[i] \in \mathbb{C}^{N_E\times 1}$ is the AWGN vector in subcarrier i at the eavesdropper, and each entry of $\mathbf{e}[i]$ has distribution $\mathcal{CN}(0, N_0)$. We assume that the CSI (path loss information and multipath fading) of the desired users is perfectly known at the BS due the accurate channel measurements. On the other hand, we assume that the BS knows only the number of antennas N_E employed by the eavesdropper[2] and the associated channel distribution with an unknown variance. Since the CSI of the eavesdropper is unavailable at the BS, to secure the desired wireless communication links, an artificial noise signal is generated at the BS to degrade the channels between the BS and the eavesdropper.

[1] An eavesdropper with N_E antennas is equivalent to multiple eavesdroppers with a total of N_E antennas which are connected to a joint processing unit.

[2] Note that the eavesdropping capability increases with the number of antennas employed by the eavesdropper. In practice, the BS may not know the number of eavesdropper antennas. Hence, the BS may assume N_E as $N_E = N_T - 1$ to ensure security by considering the worst-case scenario.

Artificial Noise Generation: The BS chooses $\mathbf{x}_k[i]$ as a linear combination of the information bearing signal $u_k[i]$ and the artificial noise signal $\mathbf{v}_k[i]$, i.e.,

$$\mathbf{x}_k[i] = \underbrace{\mathbf{b}_k[i]u_k[i]}_{\text{Desired Signal}} + \underbrace{\mathbf{V}_k[i]\mathbf{v}_k[i]}_{\text{Artificial Noise}} \tag{2}$$

where $\mathbf{v}_k[i] \in \mathbb{C}^{N_T-1\times 1}$ is a vector of independent identically distributed (i.i.d.) complex Gaussian random variables with variance $\sigma_v^2[i]$, and $\mathbf{b}_k[i] \in \mathbb{C}^{N_T\times 1}$ is a beamforming vector. Since $\mathbf{h}_k[i]$ is known at the BS, without loss of generality, we define an orthogonal basis $\mathbf{V}_k[i] \in \mathbb{C}^{N_T\times N_T-1}$ for the null space of $\mathbf{h}_k[i]$ such that $\mathbf{h}_k[i]\mathbf{V}_k[i]\mathbf{v}_k[i] = 0$ and $\mathbf{V}_k^\dagger[i]\mathbf{V}_k[i] = \mathbf{I}$, where $\mathbf{I}$ is a $(N_T-1)\times(N_T-1)$ identity matrix. In other words, the artificial noise signal does not interfere with the desired users. Without loss of generality, we define the transmit power devoted to the information bearing signal for user k in subcarrier i as $p_k[i]$. Then, the signal-to-noise ratio (SNR) at user k is maximized by choosing $\mathbf{b}_k[i] = p_k[i]\mathbf{h}_k^\dagger[i]/\|\mathbf{h}_k[i]\|$ such that the information bearing signal lies in the range space of $\mathbf{h}_k[i]$. Hence, the received signals in (1) can, respectively, be rewritten as

$$\begin{aligned} y_k[i] &= \mathbf{h}_k[i]\mathbf{b}_k[i]u_k[i] + n[i] \\ &= p_k[i]\lambda_{\max_k}[i]u_k[i] + n[i] \qquad (3) \\ \mathbf{y}_E[i] &= \mathbf{G}[i]\mathbf{b}_k[i]u_k[i] + \mathbf{G}[i]\mathbf{V}_k[i]\mathbf{v}_k[i] + \mathbf{e}[i] \qquad (4) \end{aligned}$$

where $\lambda_{\max_k}[i]$ is the maximum eigenvalue of $\mathbf{h}_k^\dagger[i]\mathbf{h}_k[i]$. Suppose the total transmit power on subcarrier i for user k is $P_k[i]$. We establish the following relationships [15]:

$$\begin{aligned} P_k[i] &= p_k[i] + (N_T-1)\sigma_v^2[i] \\ p_k[i] &= \alpha_k[i]P_k[i] \\ \sigma_v^2[i] &= \frac{(1-\alpha_k[i])\,P_k[i]}{N_T-1} \end{aligned} \tag{5}$$

where $0 < \alpha_k[i] \le 1$ represents the fraction of power devoted to the information bearing signal on subcarrier i for user k.

III. Resource Allocation and Scheduling

In this section, we introduce the adopted system performance metric and formulate the corresponding resource allocation problem. Since the adopted approach is based on information theory, the buffers at the BS are assumed to be always full, and there are no empty scheduling slots due to an insufficient number of source packets at the buffers.

A. Instantaneous Channel Capacity, Secrecy Outage, and Energy Efficiency

In this section, we define the adopted system performance measure. Given perfect CSI at the receiver, the maximum channel capacity between the BS and user k on subcarrier i with subcarrier bandwidth W is given by

$$C_k[i] = W\log_2\left(1 + \frac{p_k[i]\lambda_{\max_k}[i]}{N_0W}\right). \tag{6}$$

Without loss of generality, we normalize the received symbols at the eavesdropper by a factor $\|\mathbf{G}[i]\|$. Hence, the received symbols at the eavesdropper can be expressed as

$$\tilde{\mathbf{y}}_E[i] = \frac{\mathbf{y}_E[i]}{\|\mathbf{G}[i]\|} = \tilde{\mathbf{G}}[i]\mathbf{x}_k[i] + \tilde{\mathbf{G}}[i]\mathbf{V}_k[i]\mathbf{v}_k[i] + \tilde{\mathbf{e}}[i] \tag{7}$$

where $\tilde{\mathbf{G}}[i] = \mathbf{G}[i]/\|\mathbf{G}[i]\|$, and $\tilde{\mathbf{e}}[i] = \mathbf{e}[i]/\|\mathbf{G}[i]\|$. Note that the effect of the path loss between the BS and the eavesdropper is now modeled as a position-dependent noise vector $\tilde{\mathbf{e}}[i]$ with variance $(N_0W/\|\mathbf{G}[i]\|^2)$ in each entry instead of position-dependent channel gains [14], [15]. The BS does not know the location of the eavesdropper. As a result, we design the resource allocation algorithm for the worst-case scenario. In particular, we assume that the eavesdropper is much closer to the BS than the desired users such that the eavesdropper noise is negligible, i.e., $(N_0W/\|\mathbf{G}[i]\|^2) \to 0$. The capacity between the BS and the eavesdropper on subcarrier i under this noiseless worst-case scenario is given by

$$\begin{aligned} C_E[i] &= W\log_2\left|\mathbf{I} + p_k[i]\mathbf{g}_1\mathbf{g}_1^\dagger[i]\left(\sigma_v^2[i]\mathbf{G}_2[i]\mathbf{G}_2^\dagger[i]\right)^{-1}\right| \\ &= W\log_2 \\ &\quad\times\left(1 + \frac{\alpha_k[i](N_T-1)}{1-\alpha_k[i]}\mathbf{g}_1^\dagger[i]\left(\mathbf{G}_2[i]\mathbf{G}_2^\dagger[i]\right)^{-1}\mathbf{g}_1[i]\right) \end{aligned} \tag{8}$$

where $|\cdot|$ denotes the determinant of a matrix, $\mathbf{g}_1[i] = \tilde{\mathbf{G}}[i]\mathbf{b}_k[i]$, and $\mathbf{G}_2[i] = \tilde{\mathbf{G}}[i]\mathbf{V}_k[i]$.

Therefore, the maximum achievable secrecy capacity on subcarrier i is given by the difference of the BS-to-user k channel capacity and the BS-to-eavesdropper channel capacity [14], which can be expressed as

$$C_{sec,k}[i] = (C_k[i] - C_E[i])\,\mathbf{1}\,(C_k[i] > C_E[i])\,. \tag{9}$$

If the CSI of the BS-to-eavesdropper link is available at the BS, the resource allocator can set the target secrecy data rate $R_k[i]$ and control the channel capacity $C_k[i]$ to match the channel conditions via power adaptation, i.e., $R_k[i] = C_k[i] - C_E[i]$ and $C_k[i] > C_E[i]$, such that secure communication is guaranteed for secrecy data rate $R_k[i]$. However, here, the eavesdropper is assumed to be passive, and its CSI is not available at the BS, i.e., $C_E[i]$ is a random variable for the BS. Furthermore, we assume that the channel fading between the BS and the eavesdropper is Rayleigh distributed [14], [15]. In other words, the elements in matrix $\tilde{\mathbf{G}}[i]$ in (7) are zero mean and unit variance complex Gaussian random variables. A secrecy outage [16, Ch. 5] occurs whenever the target secrecy data rate $R_k[i]$ exceeds the secrecy capacity, despite the fact that we have considered the worst case scenario in (8). To model the effect of secrecy outage, we consider the performance in terms of the secrecy outage capacity rather than the ergodic capacity [19]. The average secrecy outage capacity is defined as the total average number of bits/s securely delivered to the K

mobile users (averaged over multiple scheduling slots) and is given by

$$\begin{aligned} U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) &= \sum_{k=1}^{K} w_k \sum_{i=1}^{n_F} s_k[i] R_k[i] E_{\tilde{\mathbf{G}}[i]} \\ &\quad \times \left\{ \mathbf{1}\left(C_k[i] - C_E[i] > R_k[i] \right) \right\} \\ &= \sum_{k=1}^{K} w_k \sum_{i=1}^{n_F} s_k[i] R_k[i] \\ &\quad \times \Pr\left[R_k[i] < C_k[i] - C_E[i] \middle| \, \mathbf{h}_k[i] \right] \quad (10) \end{aligned}$$

where vector $\mathbf{h}_k[i]$ represents the CSI between the BS and user k on subcarrier i. $\mathcal{P}$, $\mathcal{R}$, and $\mathcal{S}$ are the power, secrecy data rate, and subcarrier allocation policies, respectively. $s_k[i] \in \{0,1\}$ is the subcarrier allocation indicator. w_k is a positive constant provided by the upper layers. Indeed, by varying the value of w_k, the scheduler is able to give different priorities to different users and to enforce certain notions of fairness such as proportional fairness and max–min fairness [20], [21]. On the other hand, for designing a resource allocation algorithm for energy-efficient communication, it is important to include the total power consumption in the optimization objective function. Thus, we model the power dissipation in the system as the sum of one static term and two dynamic terms that can be expressed as [5], [6]

$$\begin{aligned} U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S}) = P_C &+ \underbrace{\sum_{k=1}^{K}\sum_{i=1}^{n_F} P_k[i] s_k[i]}_{\text{Power amplifier}} \\ &+ \underbrace{\delta \sum_{k=1}^{K}\sum_{i=1}^{n_F} s_k[i] R_k[i]}_{\text{Linear sum rate dependent power}} \quad (11) \end{aligned}$$

where P_C is a static circuit power consumption of device electronics such as mixers, filters, and digital-to-analog converters. The middle term in (11) denotes the power consumption in the power amplifier. The last term[3] in (11) represents a linear sum rate dependent power dissipation, where the value of $\delta \geq 0$ reflects the relative importance of this term. Note that the linear relationship between the data rate and the signal processing power adopted in (11) is just an illustrative example. In fact, as long as the signal processing power is a convex increasing function of the data rate, the proposed algorithm is still applicable with small modifications.

The energy efficiency of the considered secure system is defined as the total average number of securely delivered bits/joule (averaged over multiple scheduling slots)

$$U_{\text{eff}}(\mathcal{P},\mathcal{R},\mathcal{S}) = \frac{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S})}{U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})}. \quad (12)$$

B. Optimization Problem Formulation

The optimal power allocation policy $\mathcal{P}^*$, secrecy data rate allocation policy $\mathcal{R}^*$, and subcarrier allocation policy $\mathcal{S}^*$ can be obtained by solving

$$\begin{aligned} &\max_{\mathcal{P},\mathcal{R},\mathcal{S}\alpha_k[i]} \; U_{\text{eff}}(\mathcal{P},\mathcal{R},\mathcal{S}) \\ \text{s.t.} \quad &\text{C1}: \Pr\left[R_k[i] \geq C_k[i] - C_E[i] \middle| \mathbf{h}_k[i] \right] \leq \varepsilon \qquad \forall k, i \\ &\text{C2}: \sum_{k=1}^{K}\sum_{i=1}^{n_F} P_k[i] s_k[i] \leq P_t \\ &\text{C3}: \sum_{k=1}^{K}\sum_{i=1}^{n_F} s_k[i] R_k[i] \geq r \\ &\text{C4}: \sum_{k=1}^{K} s_k[i] \leq 1 \qquad \forall i \\ &\text{C5}: P_k[i] \geq 0 \qquad \forall i, k \\ &\text{C6}: \; s_k[i] = \{0, 1\} \qquad \forall i, k \\ &\text{C7}: \; 0 < \alpha_k[i] \leq 1 \qquad \forall i, k. \qquad (13) \end{aligned}$$

In C1, ε denotes the maximum tolerable secrecy outage probability, i.e., C1 is a QoS metric for communication security. C2 is a transmit power constraint for the BS. The value of P_t puts a limit on the power consumption of the power amplifier to limit the amount of out-of-cell interference. C3 specifies the minimum system secrecy outage capacity requirement r. Note that although variable r in C3 is not an optimization variable in this paper, a balance between energy efficiency and aggregate system secrecy outage capacity can be struck by varying r. Without constraint C3, it is possible that the algorithm achieves a high energy efficiency but with a low secrecy data rate for satisfying C1. In contrast, imposing C3 can guarantee that the secrecy data rate of the system cannot drop below the specified r. C4 and C6 are imposed to guarantee that each subcarrier is used by one user only. C5 and C7 are the boundary constraints for the power allocation variables.

IV. Solution of the Optimization Problem

The objective function in (13) is a ratio of two functions that is generally a nonconvex function. As a result, a brute force approach may be required for obtaining a global optimal solution. However, such a method has exponential complexity w.r.t. the numbers of subcarriers that are computationally infeasible even for small size systems. To derive an efficient resource allocation algorithm, we introduce the following transformation.

A. Transformation of the Objective Function

The fractional objective function in (12) can be classified as a nonlinear fractional program [22]. For the sake of notational simplicity, we define $\mathcal{F}$ as the set of feasible points of the optimization problem in (13). Without loss of generality, we

[3] Depending on the definition of energy efficiency, the last term in (11) represents the baseband back-end processing power of the transmitter only, the receivers only, or both the transmitter and receivers.

TABLE I
ITERATIVE RESOURCE ALLOCATION ALGORITHM

Algorithm 1 Iterative Resource Allocation Algorithm

```
Initialize the maximum number of iterations $L_{max}$ and the maximum tolerance $\epsilon$
Set maximum energy efficiency $q = 0$ and iteration index $n = 0$
repeat {Main Loop}
    Solve the inner loop problem in (16) for a given $q$ and obtain resource allocation policies $\{\mathcal{P}', \mathcal{R}', \mathcal{S}'\}$
    if $U_{sec}(\mathcal{P}', \mathcal{R}', \mathcal{S}') - qU_{TP}(\mathcal{P}', \mathcal{R}', \mathcal{S}') < \epsilon$ then
        Convergence = true
        return $\{\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*\} = \{\mathcal{P}', \mathcal{R}', \mathcal{S}'\}$ and $q^* = \frac{U_{sec}(\mathcal{P}', \mathcal{R}', \mathcal{S}')}{U_{TP}(\mathcal{P}', \mathcal{R}', \mathcal{S}')}$
    else
        Set $q = \frac{U_{sec}(\mathcal{P}', \mathcal{R}', \mathcal{S}')}{U_{TP}(\mathcal{P}', \mathcal{R}', \mathcal{S}')}$ and $n = n + 1$
        Convergence = false
    end if
until Convergence = true or $n = L_{max}$
```

define the maximum energy efficiency q^* of the considered system as

$$q^* = \frac{U_{\rm sec}(\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*)}{U_{TP}(\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*)} = \max_{\mathcal{P}, \mathcal{R}, \mathcal{S}, \alpha_k[i]} \frac{U_{\rm sec}(\mathcal{P}, \mathcal{R}, \mathcal{S})}{U_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S})}. \tag{14}$$

We are now ready to introduce the following theorem.

Theorem 1: The optimal resource allocation policies $\{\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*\} \in \mathcal{F}$ achieve the maximum energy efficiency q^* if and only if

$$\begin{aligned} \max_{\mathcal{P}, \mathcal{R}, \mathcal{S}, \alpha_k[i]} \; & U_{\rm sec}(\mathcal{P}, \mathcal{R}, \mathcal{S}) - q^* U_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S}) \\ & = U_{\rm sec}(\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*) - q^* U_{TP}(\mathcal{P}^*, \mathcal{R}^*, \mathcal{S}^*) = 0 \end{aligned} \tag{15}$$

for $U_{\rm sec}(\mathcal{P}, \mathcal{R}, \mathcal{S}) \geq 0$ and $U_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S}) > 0$.

Proof: See Appendix A. ■

Theorem 1 reveals that for an optimization problem with an objective function in fractional form, there exists an equivalent[4] objective function in subtractive form, e.g., $U_{\rm sec}(\mathcal{P}, \mathcal{R}, \mathcal{S}) - q^* U_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S})$ in the considered case. As a result, we can focus on the equivalent objective function in the rest of this paper.

B. Iterative Algorithm for Energy Efficiency Maximization

In the next section, we propose an iterative algorithm (known as the Dinkelbach method [22]) for solving (13) with an equivalent objective function. The proposed algorithm is summarized in Table I, and the convergence to optimal energy efficiency is guaranteed.

Proof: See Appendix B for the proof of convergence. ■

Note that the algorithm converges to the optimal solution with a superlinear convergence rate (see [23] for a detailed proof). As shown in Table I, in each iteration in the main loop, we solve the following optimization problem for a given parameter q:

$$\begin{aligned} \max_{\mathcal{P}, \mathcal{R}, \mathcal{S}} \quad & U_{\rm sec}(\mathcal{P}, \mathcal{R}, \mathcal{S}) - qU_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S}) \\ & \text{s.t. C1, C2, C3, C4, C5, C6, C7.} \end{aligned} \tag{16}$$

In the following, we derive the solution to the main loop problem (16) by dual decomposition.

1) Solution of the Main Loop Problem: The main loop optimization problem in (16) is a mixed combinatorial and nonconvex problem. The combinatorial nature comes from the Boolean subcarrier assignment constraint C6, while the nonconvexity comes from the secrecy outage constraint C1, which is neither convex nor concave w.r.t. the optimization variables. It is convenient to incorporate the outage requirement constraint C1 in (13) into the objective function. This is possible if the constraint in C1 is fulfilled with equality for the optimal solution. Thus, in the following, we replace the "$\leq$" sign in C1 by a "$=$" sign, and the resulting optimization problem may be viewed as a restricted version of the original problem (13) since it has a smaller feasible set.[5] We are now ready to introduce the following proposition.

Proposition 1 (Equivalent Secrecy Data Rate): Assuming the channel between BS and eavesdropper is Rayleigh fading, for a given outage probability ε in C1, the equivalent secrecy data rate that incorporates the secrecy outage probability on subcarrier i for user k with optimal $\alpha_k^*[i]$ is given by

$$R_k[i] = W \left[\log_2 \left(1 + P_k[i] \Upsilon_k[i]\right) - \log_2 \left(1 + \frac{\alpha_k^*[i] \Lambda_E[i]}{1 - \alpha_k^*[i]}\right)\right]^+ \tag{17}$$

for

$$\begin{aligned} \Upsilon_k[i] &= \frac{\alpha_k^*[i] \lambda_{\max_k}[i]}{N_0 W} \\ \Lambda_E[i] &= (N_T - 1) F_{z_c}^{-1}(\varepsilon) \\ \alpha_k^*[i] &= \frac{1}{\sqrt{\Lambda_E[i]}} \end{aligned} \tag{18}$$

where $F_{z_c}^{-1}(\varepsilon)$ denotes the inverse function of $F_{z_c}(z) = \sum_{n=0}^{N_E - 1} \binom{N_T - 1}{n} z^n / (1 + z)^{N_T - 1} = \varepsilon$.

Proof: See Appendix C. ■

From the foregoing proposition, it can be observed that the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper $\Phi_E[i] = \alpha_k^*[i] \Lambda_E[i] / 1 - \alpha_k^*[i]$ approaches a constant value at high SNR. More importantly, the SINR of the eavesdropper on each subcarrier is independent of the optimization variables, which simplifies the derivation of the optimal resource allocation algorithm.

[4] Here, "equivalent" means both problem formulations will lead to the same optimal resource allocation policies.

[5] We can also adopt the chance constrained programming transformation in [24]. However, this method is only applicable to convex optimization problems with an outage probability constraint. Besides, chance programming introduces an additional search algorithm which may result in an unacceptably high complexity for the problem at hand. Although the equality constraint for the outage probability may cause some performance degradation, it has been widely adopted in the literature for deriving tractable resource allocation algorithms [25], [26].

By substituting (17) into (16), a modified objective function, which incorporates the secrecy outage requirement, can be obtained for the main loop problem in (16). To handle the combinatorial constraint C6 [cf. (13)], we follow the approach in [27] and relax constraint C6. In particular, we allow $s_k[i]$ to be a real value between 0 and 1 instead of a Boolean. Then, $s_k[i]$ can be interpreted as a time sharing factor for the K users for utilizing subcarrier i. Although the relaxation of the subcarrier allocation constraint is generally suboptimal, the authors in [28] analytically show that the duality gap due to the relaxation becomes zero when the number of subcarriers goes to infinity. Therefore, using the equivalent secrecy data rate in Proposition 1, the auxiliary powers $\tilde{P}_k[i] = P_k[i]s_k[i]$, and the continuous relaxation of C6, we can rewrite the problem in (16) for a given parameter q as

$$\begin{aligned}
&\max_{\mathcal{P},\mathcal{R},\mathcal{S}} \quad \tilde{U}_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q\tilde{U}_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})\\
&\text{s.t.} \qquad\qquad \text{C4}, \quad \text{C5}\\
&\qquad\qquad\quad \text{C2}: \sum_{k=1}^{K}\sum_{i=1}^{n_F}\tilde{P}_k[i] \le P_t\\
&\qquad\qquad\quad \text{C3}: \sum_{k=1}^{K}\sum_{i=1}^{n_F} s_k[i]\tilde{R}_k[i] \ge r\\
&\qquad\qquad\quad \text{C6}: \ 0 \le s_k[i] \le 1 \qquad \forall i,k
\end{aligned} \tag{19}$$

where $\tilde{U}_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) = U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S})|_{P_k[i]=\tilde{P}_k[i]/s_k[i]}$, $\tilde{U}_{TP}(\mathcal{P},\mathcal{R},\mathcal{S}) = U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})|_{(\tilde{P}_k[i]/s_k[i])}$, and $\tilde{R}_k[i] = R_k[i]|_{(\tilde{P}_k[i]/s_k[i])}$. Now, $\tilde{P}_k[i]$, $s_k[i]$, and $\tilde{R}_k[i]$ are the new optimization variables. Mathematically, the $[\cdot]^+$ operator in (17) destroys the concavity of the objective function. Nevertheless, as will be seen in the Karush–Kuhn–Tucker (KKT) conditions in (24), users with negative secrecy data rate will not be considered in the subcarrier selection process. Therefore, we can safely remove the $[\cdot]^+$ operator from variable $\tilde{R}_k[i]$ and preserve the concavity of the transformed problem. In addition, C7 is removed from the optimization problem as the asymptotically optimal $\alpha_k^*[i]$ in (18) always satisfies C7 for $\Lambda_E[i] \gg 1$ [cf. (41) in Appendix C]. The transformed problem (19) is jointly concave w.r.t. all optimization variables (cf. Appendix D). As a result, under some mild conditions [29], a strong duality holds, and the duality gap is equal to zero. In other words, solving the dual problem is equivalent to solving the primal problem. Therefore, numerical methods such as the interior point method and the ellipsoid method can be used to solve the transformed main loop problem in (19), and convergence to the optimal solution in polynomial time is guaranteed. However, these numerical methods do not provide any useful system design insight such as the role of energy efficiency q in the resource allocation process. Hence, in the following sections, an iterative algorithm for the transformed main loop problem in (19) will be derived based on dual decomposition.

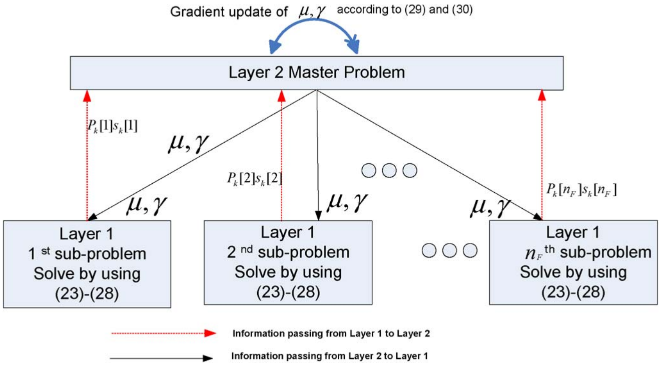

Fig. 2. Dual decomposition of a large-scale problem into a two-layer problem in each main loop iteration.

2) Dual Problem: In this section, we solve the main loop problem in (19) by solving its dual. For this purpose, we first need the Lagrangian function of the primal problem. Upon rearranging terms, the Lagrangian can be written as

$$\begin{aligned}
&\mathcal{L}(\mu,\gamma,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S})\\
&\quad= \sum_{k=1}^{K}(w_k+\gamma)\sum_{i=1}^{n_F}s_k[i]\tilde{R}_k[i] - \mu\sum_{k=1}^{K}\sum_{i=1}^{n_F}\tilde{P}_k[i]\\
&\qquad+\mu P_t + \sum_{i=1}^{n_F}\beta[i] - \gamma r - \sum_{k=1}^{K}\sum_{i=1}^{n_F}\beta[i]s_k[i]\\
&\qquad- q\left(P_C + \sum_{k=1}^{K}\sum_{i=1}^{n_F}s_k[i]\delta\tilde{R}_k[i] + \sum_{k=1}^{K}\sum_{i=1}^{n_F}\tilde{P}_k[i]\right)
\end{aligned} \tag{20}$$

where $\mu \ge 0$ and $\gamma \ge 0$ are the Lagrange multipliers corresponding to the power constraint and the minimum required secrecy outage capacity constraint, respectively. $\boldsymbol{\beta}$ is the Lagrange multiplier vector associated with the subcarrier usage constraints with elements $\beta[i] \ge 0$, $i \in \{1,\ldots,n_F\}$. The boundary constraints C5 and C6 will be absorbed into the KKT conditions when deriving the optimal solution in the following.

Thus, the dual problem of (19) is given by

$$\min_{\mu,\gamma,\boldsymbol{\beta}\ge 0}\ \max_{\mathcal{P},\mathcal{R},\mathcal{S}} \quad \mathcal{L}(\mu,\gamma,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}). \tag{21}$$

In the following, we iteratively solve the foregoing dual problem by decomposing it into two layers: 1) Layer 1 consists of n_F subproblems with identical structure, and 2) layer 2 is the master dual problem to be solved with the gradient method (cf. Fig. 2).

Dual Decomposition and Layer 1 Solution: By dual decomposition, the BS first solves the following layer 1 subproblem:

$$\max_{\mathcal{P},\mathcal{S}} \quad \mathcal{L}(\mu,\gamma,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}) \tag{22}$$

for a fixed set of Lagrange multipliers and parameter q. Let $\tilde{P}_k^*[i]$ and $s_k^*[i]$ denote the optimal solutions of the subproblem. Then, the KKT conditions reveal that

$$\begin{aligned}
\frac{\partial\mathcal{L}(\mu,\gamma,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S})}{\partial\tilde{P}_k^*[i]} &= \frac{\Upsilon_k[i](w_k+\gamma-\delta q)}{\ln(2)\left(1+\frac{\tilde{P}_k^*[i]\Upsilon_k[i]}{s_k^*[i]}\right)} - (\mu+q)\\
&\qquad\times\begin{cases} = 0, & \tilde{P}_k^*[i] > 0\\ < 0, & \text{otherwise}\end{cases}
\end{aligned} \tag{23}$$

$$\frac{\partial \mathcal{L}(\mu,\gamma,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S})}{\partial s_k^*[i]} = A_k[i]-\beta[i] \times \begin{cases} \geq 0, & 0 < s_k^*[i] \leq 1 \\ < 0, & s_k^*[i]=0 \end{cases} \tag{24}$$

$$\beta[i]\left(\sum_{k=1}^{K} s_k^*[i]-1\right)=0 \tag{25}$$

where

$$A_k[i] = W(w_k+\gamma-\delta q) \times \left(\log_2\left(1+P_k^*[i]\Upsilon_k[i]\right)-\log_2\left(1+\frac{\alpha_k^*[i]\Lambda_E[i]}{1-\alpha_k^*[i]}\right) - \frac{P_k^*[i]\Upsilon_k[i]}{(\ln(2))\left(1+P_k^*[i]\Upsilon_k[i]\right)}\right). \tag{26}$$

From (23), the optimal power allocation for user k on subcarrier i is obtained as

$$\tilde{P}_k^*[i] = s_k[i]P_k^*[i] = s_k[i]\left[\frac{W(w_k+\gamma-\delta q)}{(\ln(2))(\mu+q)} - \frac{N_0 W}{\lambda_{\max_k}[i]\alpha_k^*[i]}\right]^+. \tag{27}$$

The optimal power allocation has the form of multilevel water filling. It can be observed that the energy efficiency variable $q \geq 0$ prevents energy inefficient transmission by truncating the water levels. There is also another interesting observation from (27). Let us focus on the case of equal priority users without secrecy data rate constraint, i.e., $w_k = 1$ and $\gamma = 0$. If we require a certain energy efficiency $q = q_{\text{req}}$, then (27) reveals a simple necessary condition[6] for a nonzero feasible solution: $\delta q_{\text{req}} < 1$.

On the other hand, the optimal allocation of subcarrier i at the BS to user k is given by

$$s_k^*[i] = \begin{cases} 1, & \text{if } A_k[i] = \max\limits_j \quad A_j[i] \text{ and } A_j[i] \geq 0 \\ 0, & \text{otherwise} \end{cases} \tag{28}$$

where $A_k[i]$ is defined in (26). $A_k[i] \geq 0$ has the physical meaning that users with negative data rate on subcarrier i are not selected as they can only provide a negative marginal benefit to the system. On the contrary, if a user has a larger weighting w_k and enjoys good channel conditions with positive data rate on subcarrier i, he/she can provide a higher marginal benefit to the system. In other words, the resource allocator will only assign subcarrier i to user k if he/she is able to provide the maximum marginal benefit to the system. The derived subcarrier allocation solution (28) shows that although time sharing is assumed for solving the optimization problem, the optimal solution indicates that the maximum system performance is achieved when there is no time sharing on any subcarrier. In other words, each subcarrier is only assigned to one user, and intracell interference is completely avoided. Finally, the optimal secrecy data rate $R_k^*[i]$ is obtained by substituting (27) into the equivalent secrecy data rate in (17) for the subcarrier with $s_k^*[i] = 1$.

Solution of Layer 2 Master Problem: The dual function is differentiable, and hence, the gradient method can be used to solve the layer 2 master problem in (21), which leads to

$$\mu(t+1) = \left[\mu(t) - \xi_1(t) \times \left(P_t - \sum_{k=1}^{K}\sum_{i=1}^{n_F}\tilde{P}_k[i]\right)\right]^+ \tag{29}$$

$$\gamma(t+1) = \left[\gamma(t) - \xi_2(t) \times \left(\sum_{k=1}^{K}\sum_{i=1}^{n_F} s_k[i]\tilde{R}_k[i] - r\right)\right]^+ \tag{30}$$

where index $t \geq 0$ is the iteration index, and $\xi_u(t)$, $u \in \{1,2\}$ are positive step sizes. Updating $\beta[i]$ is not necessary as it has the same value for all users and does not affect the subcarrier allocation in (28). Therefore, we can simply set $\beta[i] = 0$ in each iteration. Indeed, in each iteration for solving the main loop problem, the layer 2 master problem adjusts the Lagrange multipliers through the gradient update equations (29) and (30). On the other hand, each subproblem in layer 1 adjusts the water level of (27) and the selection metric (28) by using the updated Lagrange multipliers. Then, the layer 1 subproblems will pass the intermediate resource allocation policies to layer 2 for updating the Lagrange multipliers. The procedure repeated until convergence is achieved or the number of iterations reaches a predefined maximum number of iterations for the main loop problem (cf. Fig. 2). Since the transformed problem for a given parameter q is convex in nature, it is guaranteed that the iteration between layers 1 and 2 converges to the optimal solution of (19) in the main loop if the chosen step sizes satisfy the infinite travel condition [29], [30].

A summary of the overall algorithm is given in Table I. In each iteration of the main loop, we solve (16) in line 4 of Algorithm 1 for a given parameter q via dual decomposition [cf. (17)–(30)]. Then, we update parameter q and use it for solving the main loop problem in the next iteration. This procedure is repeated until the proposed algorithm converges.

Remark 1: The proposed iterative algorithm consists of two nested loops. The outer loop can be proved to have a linear time complexity. On the other hand, the inner loop optimization problem is proved to be jointly concave w.r.t. the optimization variables in Appendix D. In other words, solving the inner loop optimization problem requires only a polynomial time complexity, i.e., the complexity is $O(n_F \times K)$. As a result, the proposed algorithm has a polynomial time complexity, i.e., $O(constant \times n_F \times K)$, which is desirable for real-time implementation [31, Ch. 34].

V. Results

In this section, we evaluate the system performance through simulations. A single cell with a radius of 1 km is considered (cf. Fig. 1). The number of subcarriers is $n_F = 128$ with

[6] Note that the KKT conditions provide both the necessary and sufficient conditions for the "optimality" of a solution of the considered optimization problem. In contrast, $\delta q_{\text{req}} < 1$ provides a necessary condition for the existence of a non-zero transmit power solution.

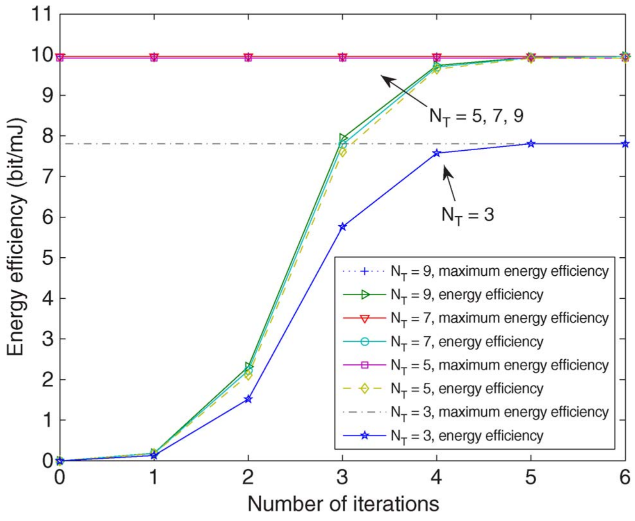

Fig. 3. Energy efficiency (bits per joule) versus the number of iterations with $K = 15$ users for different numbers of transmit antennas at the BS. The maximum transmit power at the BS is $P_t = 43$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

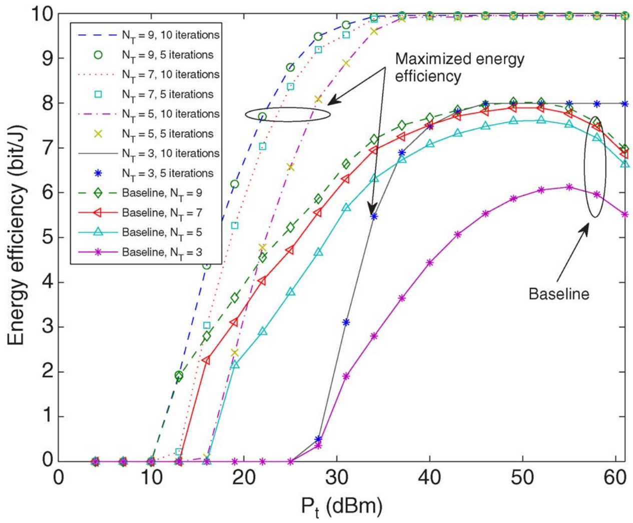

Fig. 4. Energy efficiency (bits per joule) versus maximum transmit power P_t for different numbers of transmit antennas N_T. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

carrier center frequency 2.5 GHz, bandwidth $\mathcal{B} = 3$ MHz, and $w_k = 1\ \forall k$. Each subcarrier has a bandwidth of 23.4 kHz and a noise variance of $N_0 = -130$ dBm. The 3GPP path loss model is used [32] with a reference distance of $d_0 =$ 35 m. The K desired users are uniformly distributed between the reference distance and the cell boundary at 1 km. We assume that the eavesdropper is located 35 m away from the BS, which represents an unfavorable scenario, since all the desired users are farther away from the BS than the eavesdropper. The small scale fading coefficients of the BS-to-user and BS-to-eavesdropper links are modeled as i.i.d. Rayleigh random variables. The target secrecy outage probability is set to $\varepsilon = 0.01$. The average secrecy outage capacity is obtained by counting the number of packets securely delivered to and decoded by the users averaged over both the macroscopic and microscopic fading. Unless specified otherwise, we assume a static circuit power consumption of $P_C = 40$ dBm [33], a sum-rate-dependent power consumption parameter $\delta = 0.1$, and a secrecy data rate requirement of $r = 2$ bits/s/Hz. Note that if the resource allocator is unable to guarantee the required secrecy data rate in a time slot, we set the energy efficiency in that particular time slot to 0 to account for the corresponding failure. In the following results, the "number of iterations" refers to the number of main loop iterations of Algorithm 1 in Table I. For solving a dual problem in each main loop iteration, we set the maximum number of iterations for dual decomposition to 5.

A. Convergence of Iterative Algorithm

Fig. 3 illustrates the evolution of the proposed iterative algorithm for different numbers of transmit antennas N_T and a maximum transmit power of $P_t = 43$ dBm at the BS. The eavesdropper is equipped with $N_E = 2$ receive antennas, and the result in Fig. 3 was averaged over 10 000 independent adaptation processes, where each adaptation process involves different realizations for the path loss and the multipath fading. It can be observed that the iterative algorithm converges to the optimal value within five iterations for all considered numbers of transmit antennas. In other words, the maximum system energy efficiency can be achieved within a few iterations on average with a superlinear convergence rate [23].

B. Energy Efficiency and Average Secrecy Outage Capacity Versus Transmit Power

Fig. 4 illustrates the energy efficiency versus the total transmit power for $K = 15$ users for different numbers of transmit antennas N_T at the BS. The eavesdropper is equipped with $N_E = 2$ antennas. The numbers of iterations for the proposed iterative resource allocation algorithm are 5 and 10. It can be seen that the performance difference between 5 and 10 iterations is negligible, which confirms the practicality of our proposed iterative resource allocation algorithm. On the other hand, it can be observed that an increasing number of transmit antennas N_T benefits the system in terms of energy efficiency. This is because less power is required for maintaining a high receive SNR at the desired users, which results in energy savings. In addition, when both the number of transmit antennas and the maximum transmit power at the power amplifier are large enough, e.g., $N_T = 7$ and $P_t = 43$ dBm, the energy efficiency approaches a constant value $1/\delta$ for $\delta > 0$, since the dynamic power consumption dominates the denominator in the energy efficiency equation in (12). Fig. 4 also contains the energy efficiency of a baseline resource allocation scheme. For the baseline scheme, we maximize the secrecy outage capacity (in bits per second per Hertz) with constraints C1–C7 in (13) instead of the energy efficiency. The optimal resource allocation policies for the baseline scheme can be obtained by using a similar approach as in [17]. It can be observed that the proposed algorithm provides a significant performance gain in terms of energy efficiency over the baseline scheme. This is because the latter scheme uses excess power to increase the secrecy outage capacity by sacrificing energy efficiency, particularly in the high transmit power regime.

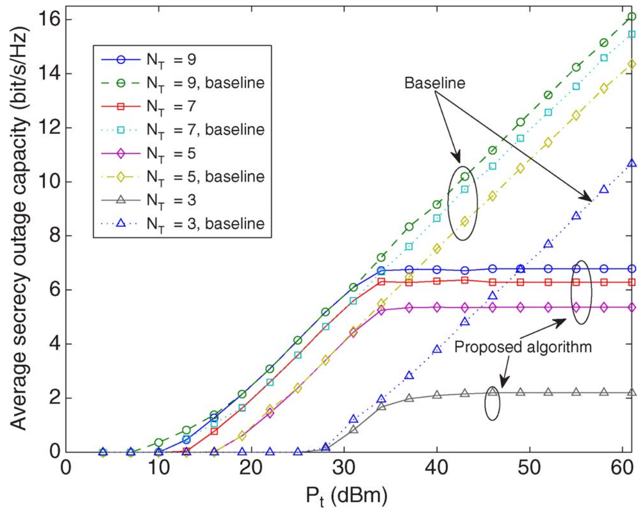

Fig. 5. Average secrecy outage capacity versus maximum transmit power P_t for different numbers of transmit antennas N_T. The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m from the BS.

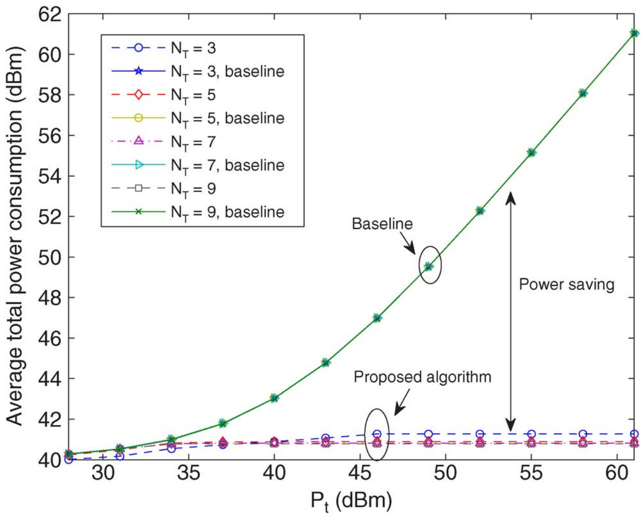

Fig. 6. Average total power consumption versus maximum transmit power P_t for different numbers of transmit antennas N_T. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

Fig. 5 shows the average secrecy outage capacity versus maximum transmit power P_t for $K = 15$ users and different numbers of transmit antennas at the BS. We compare the system performance of the proposed algorithm again with the baseline scheme. The number of iterations in the proposed algorithm is set to 5. It can be observed that the average secrecy outage capacity of the proposed algorithm approaches a constant in the high transmit power regime, the value of which depends on the number of transmit antennas. This is because the proposed algorithm clips the transmit power at the BS to maximize the system energy efficiency. As will be shown in Fig. 6, the average transmit power of the proposed algorithm remains static in the high transmit power regime. We note that, as expected, the baseline scheme achieves a higher average secrecy outage capacity than the proposed algorithm since the former scheme consumes all the available transmit power in all scenarios. However, the superior secrecy outage capacity of the baseline scheme comes at the expense of low energy efficiency.

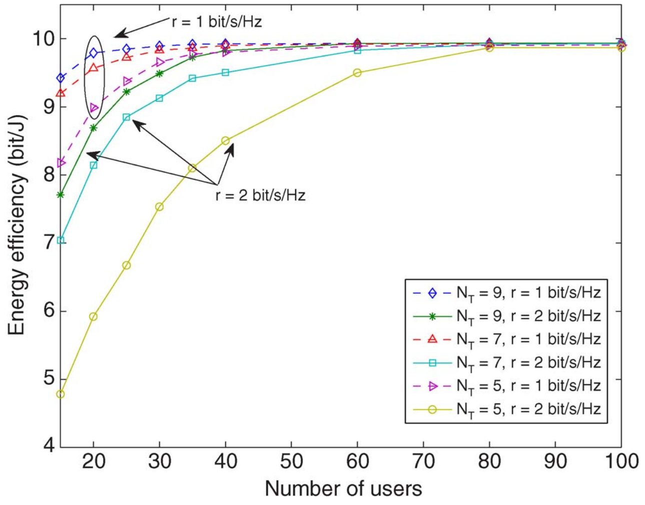

Fig. 7. Energy efficiency (bits per joule) versus the number of users K for different numbers of transmit antennas N_T and a maximum transmit power of $P_t = 22$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

On the other hand, an increasing number of antennas benefit the secrecy outage capacity because of an improved beamforming gain. Yet, there is a diminishing return when N_T is large due to the channel hardening effect [19] in the desired channels.

Fig. 6 depicts the average total power consumption, i.e., $\mathcal{E}\{U_{TP}(\mathcal{P}, \mathcal{R}, \mathcal{S})\}$, versus the maximum transmit power P_t for the proposed algorithm and the baseline scheme. As can be observed, the proposed algorithm consumes much less power than the baseline scheme, particularly in the high transmit power regime. In addition, an increasing number of transmit antennas results in less power consumption due to a larger beamforming gain. Note that for $P_t < 37$ dBm, the proposed algorithm with $N_T = 3$ consumes the smallest power among all the considered cases. This is because with fewer antennas the probability that the secrecy data rate requirement is met is lower. Therefore, an extra energy saving is achieved when the transmitter is shut down. However, this leads to both low energy efficiency and low secrecy data rate.

C. Energy Efficiency and Secrecy Outage Capacity Versus Number of Users

Figs. 7 and 8 depict the energy efficiency and the average secrecy outage capacity versus the number of users, respectively. Different numbers of transmit antennas, different secrecy data rate requirements r, $P_T = 22$ dBm, and five iterations are considered. It can be observed that both the energy efficiency and the average secrecy outage capacity grow with the number of users since the proposed resource allocation and scheduling algorithm are able to exploit MUD, despite the existence of the eavesdropper. Moreover, when the number of users is large, the energy efficiency eventually approaches a constant that is similar to the case of high transmit power. Indeed, the MUD introduces an extra power gain [19, Ch. 6.6] to the system that provides further energy savings. On the contrary, the average secrecy outage capacity scales with the number of users without an upper limit. However, for large N_T, both the average secrecy

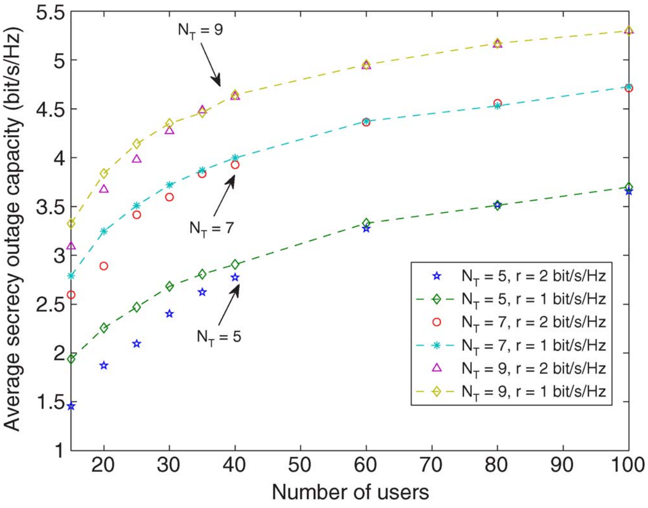

Fig. 8. Average secrecy outage capacity versus the number of users K for different numbers of transmit antennas N_T and a maximum transmit power of $P_t = 22$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

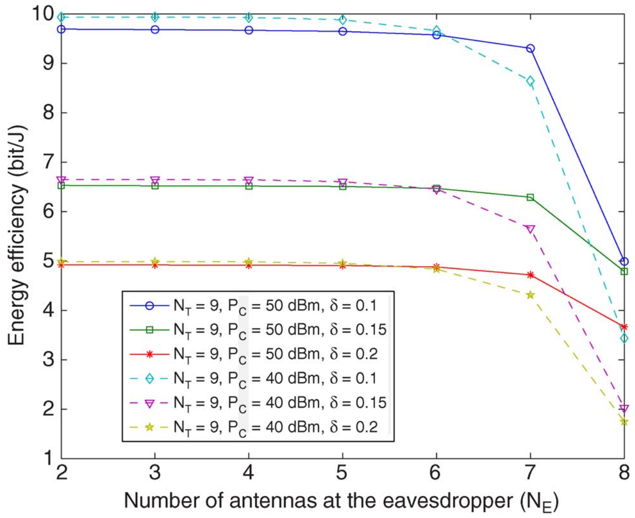

Fig. 9. Energy efficiency (bits per joule) versus the number of antennas at the eavesdropper for different static circuit powers P_C and different values of δ for a maximum transmit power of $P_t = 43$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

outage capacity and the energy efficiency scale with the number of users slowly. Indeed, since a large number of transmit antennas reduce channel fluctuations in the desired user channel and cause channel hardening, the potentially achievable MUD gain in the subcarrier allocation process is decreased.

D. Energy Efficiency and Average Secrecy Outage Capacity Versus N_E

Figs. 9 and 10 illustrate, respectively, the energy efficiency and the average secrecy outage capacity versus the number of receive antennas N_E employed at the eavesdropper for different dynamic circuit power constants δ and different static circuit powers P_C. There are $K = 15$ users and $N_T = 9$ transmit antennas at the BS. The number of iterations for the iterative algorithm is 5. It can be observed that both the energy efficiency and the secrecy outage capacity decrease as N_E increases, since more of the transmitted power has to be devoted to artificial noise generation for degrading the channels of the eavesdropper, which leaves less power for information transmission. In other words, the energy efficiency of the system decreases as the PHY layer security requirements become more challenging (i.e., as the number of eavesdropper antennas increases). In addition, the average secrecy outage capacity is insensitive to the value of δ, which suggests a constant secrecy data transmission rate when dynamic power consumption is taken into consideration. On the other hand, we observe that larger values of δ and P_C lead to a lower energy efficiency since more energy is consumed in the circuit. However, a nonzero energy efficiency and an average secrecy outage capacity can still be achieved as long as $N_T > N_E$, despite the fact that the eavesdropper is closer to the BS than the desired users. Interestingly, although a higher value of P_C results in a low energy efficiency, it increases the average secrecy outage capacity by allowing a higher transmit power.

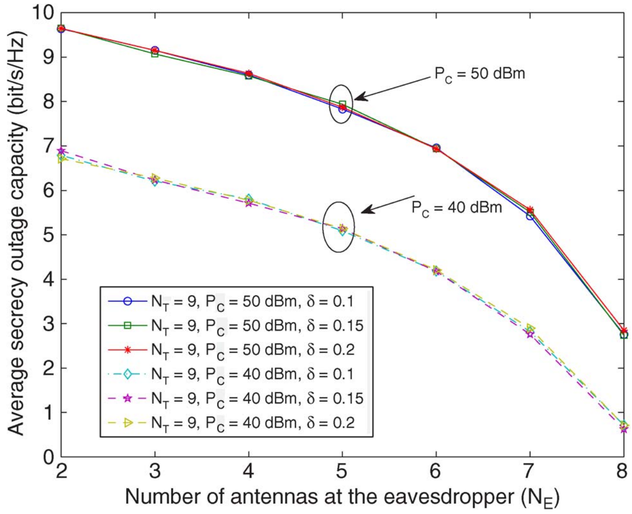

Fig. 10. Average secrecy outage capacity versus the number of antennas at the eavesdropper for different static circuit powers P_C and different values of δ for a maximum transmit power of $P_t = 43$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and located 35 m from the BS.

Remark 2: Note that in Fig. 9, the energy efficiencies for the case of $P_C = 50$ dBm and $P_C = 40$ dBm cross at $N_E = 6$. This is because we shut down the transmitter when the system cannot fulfill the secrecy data rate requirement, which impacts the energy efficiency curves.

VI. Conclusion

In this paper, we have formulated the resource allocation for energy-efficient OFDMA systems as a mixed nonconvex and combinatorial optimization problem, in which a multiple-antenna eavesdropper, dynamic circuit power consumption, artificial noise injection for secure communication, and secrecy data rate requirements were taken into consideration. By exploiting the properties of fractional programming, the considered problem was transformed into an equivalent problem with a tractable solution. An efficient iterative resource allocation algorithm with closed-form power, secrecy data rate, and subcarrier allocation was derived by dual decomposition for maximization of the number of securely delivered bits per joule. Simulation results showed that the proposed algorithm converges to the optimal solution within a small number of iterations, which demonstrated the achievable maximum energy efficiency in the presence of a multiple-antenna eavesdropper. Moreover, a tradeoff between energy efficiency and secrecy was observed that revealed that the system energy efficiency decreases as the eavesdropping capability of the eavesdropper increases.

Interesting topics for future work include studying the impact of network coding [34] and imperfect CSIT on the design of secure communication systems.

Appendix A
Proof of Theorem 1

First, we prove the forward implication of Theorem 1 by following a similar approach as in [22]. Without loss of generality, we define q^* and $\{\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*\}\in\mathcal{F}$ as the optimal energy efficiency and the optimal resource allocation policies of the original objective function in (13), respectively. Then, the optimal energy efficiency can be expressed as

$$\begin{aligned} q^* = &\frac{U_{\text{sec}}(\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*)}{U_{TP}(\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*)} \geq \frac{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S})}{U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})} \qquad \forall\{\mathcal{P},\mathcal{R},\mathcal{S}\}\in\mathcal{F} \\ \Longrightarrow &\, U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q^* U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S}) \leq 0 \text{ and} \\ & U_{\text{sec}}(\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*) - q^* U_{TP}(\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*) = 0. \end{aligned} \tag{31}$$

Therefore, we conclude that $\max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_k[i]} U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q^* U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S}) = 0$, and it is achievable by resource allocation policies $\{\mathcal{P}^*,\mathcal{R}^*,\mathcal{S}^*\}$. This completes the forward implication.

Next, we prove the converse implication of Theorem 1. Suppose $\{\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\}$ is the optimal resource allocation policy of the equivalent objective function such that $U_{\text{sec}}(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*) - q^* U_{TP}(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*) = 0$. Then, for any feasible resource allocation policies $\{\mathcal{P},\mathcal{R},\mathcal{S}\}\in\mathcal{F}$, we can obtain the following inequality:

$$\begin{aligned} & U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q^* U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S}) \\ & \qquad \leq U_{\text{sec}}\left(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\right) - q^* U_{TP}\left(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\right) = 0. \end{aligned} \tag{32}$$

The preceding inequality implies

$$\begin{aligned} \frac{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S})}{U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})} &\leq q^* \qquad \forall\{\mathcal{P},\mathcal{R},\mathcal{S}\}\in\mathcal{F} \\ \frac{U_{\text{sec}}\left(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\right)}{U_{TP}\left(\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\right)} &= q^*. \end{aligned} \tag{33}$$

In other words, the optimal resource allocation policies $\{\mathcal{P}_e^*,\mathcal{R}_e^*,\mathcal{S}_e^*\}$ for the equivalent objective function are also the optimal resource allocation policies for the original objective function.

This completes the proof of the converse implication of Theorem 1. In summary, the optimization of the original objective function and the optimization of the equivalent objective function result in the same resource allocation policies.

Appendix B
Proof of Algorithm Convergence

We follow a similar approach as in [22] to prove the convergence of Algorithm I. We first introduce the following two propositions. For the sake of notational simplicity, we define the equivalent objective function in (16) as $F(q') = \max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_k[i]}\{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q' U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})\}$.

Proposition 2: $F(q')$ is a strictly monotonic decreasing function in q', i.e., $F(q'') > F(q')$ if $q' > q''$.

Proof: Let $\{\mathcal{P}',\mathcal{R}',\mathcal{S}'\}\in\mathcal{F}$ and $\{\mathcal{P}'',\mathcal{R}'',\mathcal{S}''\}\in\mathcal{F}$ be two distinct optimal resource allocation policies for $F(q')$ and $F(q'')$, respectively, i.e.,

$$\begin{aligned} F(q'') &= \max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_k[i]} \{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q'' U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})\} \\ &= U_{\text{sec}}(\mathcal{P}'',\mathcal{R}'',\mathcal{S}'') - q'' U_{TP}(\mathcal{P}'',\mathcal{R}'',\mathcal{S}'') \\ &> U_{\text{sec}}(\mathcal{P}',\mathcal{R}',\mathcal{S}') - q'' U_{TP}(\mathcal{P}',\mathcal{R}',\mathcal{S}') \\ &\geq U_{\text{sec}}(\mathcal{P}',\mathcal{R}',\mathcal{S}') - q' U_{TP}(\mathcal{P}',\mathcal{R}',\mathcal{S}') \\ &= F(q'). \end{aligned} \tag{34}$$

■

Proposition 3: Letting $\{\mathcal{P}',\mathcal{R}',\mathcal{S}'\}\in\mathcal{F}$ be an arbitrary feasible solution and $q' = U_{\text{sec}}(\mathcal{P}',\mathcal{R}',\mathcal{S}')/U_{TP}(\mathcal{P}',\mathcal{R}',\mathcal{S}')$, then $F(q') \geq 0$.

Proof:

$$\begin{aligned} F(q') &= \max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_k[i]} \{U_{\text{sec}}(\mathcal{P},\mathcal{R},\mathcal{S}) - q' U_{TP}(\mathcal{P},\mathcal{R},\mathcal{S})\} \\ &\geq U_{\text{sec}}(\mathcal{P}',\mathcal{R}',\mathcal{S}') - q' U_{TP}(\mathcal{P}',\mathcal{R}',\mathcal{S}') = 0. \end{aligned} \tag{35}$$

We are now ready to prove the convergence of Algorithm I. ■

Proof of Convergence: We first prove that the energy efficiency q increases in each iteration. Then, we prove that if the number of iterations is large enough, then the energy efficiency q converges to the optimal q^* such that it satisfies the optimality condition in Theorem 1, i.e., $F(q^*) = 0$.

Let $\{\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n\}$ be the optimal resource allocation policies in the nth iteration. Suppose $q_n \neq q^*$ and $q_{n+1} \neq q^*$ represent the energy efficiency of the considered system in iterations n and $n+1$, respectively. By Theorem 1 and Proposition 3, $F(q_n) > 0$ and $F(q_{n+1}) > 0$ must be true. On the other hand, in the proposed algorithm, we calculate q_{n+1} as $q_{n+1} = U_{\text{sec}}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n)/U_{TP}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n)$. Thus, we can express $F(q_n)$ as

$$\begin{aligned} F(q_n) &= U_{\text{sec}}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n) - q_n U_{TP}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n) \\ &= U_{TP}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n)(q_{n+1} - q_n) > 0 \\ \Longrightarrow q_{n+1} &> q_n, \quad \because U_{TP}(\mathcal{P}_n,\mathcal{R}_n,\mathcal{S}_n) > 0. \end{aligned} \tag{36}$$

By combining $q_{n+1} > q_n$ and Propositions 2 and 1, we can show that as long as the number of iterations is large enough, $F(q_n)$ will eventually approach zero and satisfy the optimality condition as stated in Theorem 1. ■

APPENDIX C
PROOF OF PROPOSITION 1

Without loss of generality, we define the secrecy data rate as $R_k[i] = W\log_2(r_k[i])$. Now, the secrecy outage probability can be expressed as

$$\Pr\left[C_k[i] - C_E[i] \le R_k[i] \middle| \mathbf{h}_k[i]\right] = \varepsilon \tag{37}$$

$$\Longrightarrow \Pr\left[\underbrace{\left(\frac{1}{r_k[i]}\left(1+\Gamma_k[i]\right)-1\right)\frac{1-\alpha_k[i]}{(N_T-1)\alpha_k[i]}}_{\Theta_k[i]} \right.$$
$$\left. \le \underbrace{\mathbf{g}_1^\dagger[i]\left(\mathbf{G}_2[i]\mathbf{G}_2^\dagger[i]\right)^{-1}\mathbf{g}_1[i]}_{Z_k[i]} \middle| \mathbf{h}_k[i]\right] = \varepsilon \tag{38}$$

where $\Gamma_k[i] = \alpha_k[i]P_k[i]\lambda_{\max_k}[i]/N_0W$, and $Z_k[i]$ is an unknown random variable for the BS. Since the supermatrix $\mathbf{B}_k[i] = [\mathbf{b}_k[i]\ \mathbf{V}_k[i]]$ is an unitary matrix, $\mathbf{B}_k[i]\tilde{\mathbf{G}}[i]$ has i.i.d. complex Gaussian entries. As a result, $Z_k[i]$ is equivalent to the signal-to-interference ratio of an N_E-branch minimum mean square error diversity combiner for $N_T - 1$ interferers. Hence, the corresponding complementary cumulative distribution function (ccdf) is given by [15], [35]

$$F_{z_c}(z) = \frac{\sum_{n=0}^{N_E-1}\binom{N_T-1}{n}z^n}{(1+z)^{N_T-1}} \qquad \forall z \ge 0. \tag{39}$$

Therefore, for a target secrecy outage probability of ε, $\Theta_k[i]$ can be expressed as

$$\begin{aligned}\Theta_k[i] &= F_{z_c}^{-1}(\varepsilon) \Longrightarrow \\ R_k[i] &= W\left[\log_2\left(1+\frac{\alpha_k[i]P_k[i]\lambda_{\max_k}[i]}{N_0W}\right)\right. \\ &\qquad \left. - \log_2\left(1+\frac{\alpha_k[i]}{1-\alpha_k[i]}(N_T-1)F_{z_c}^{-1}(\varepsilon)\right)\right]^+\end{aligned} \tag{40}$$

where $F_{z_c}^{-1}(\varepsilon)$ is the inverse ccdf of the random variable $Z_k[i]$, which can be computed efficiently by numerical solvers or implemented as a lookup table for practical implementation. The second step in solving the optimization problem in (13) is to calculate the fraction of power allocated to each subcarrier for generating artificial noise. By standard optimization techniques, the asymptotically optimal $\alpha_k^*[i]$ maximizing the secrecy outage capacity on subcarrier i for a fixed $P_k[i]$ in high SNR is obtained as

$$\begin{aligned}\alpha_k^*[i] &= \frac{\Gamma_k[i] - \sqrt{(\Gamma_k[i])^2\Lambda_E[i] - \Gamma_k[i]\ (\Lambda_E[i])^2 + \Gamma_k[i]\ \Lambda_E[i]}}{\Gamma_k[i] - \Gamma_k[i]\ \Lambda_E[i]} \\ &\overset{(a)}{\approx} \frac{\sqrt{\Lambda_E[i]}-1}{\Lambda_E[i]-1} \approx \frac{1}{\sqrt{\Lambda_E[i]}}\end{aligned} \tag{41}$$

where (a) is due to the high SNR[7] assumption, i.e., $\Gamma_k[i] \gg \Lambda_E[i] \gg 1$. Note that $\Gamma_k[i] \gg \Lambda_E[i]$ is always valid in the high transmit power regime as $\Gamma_k[i]$ increases with the total transmit power while $\Lambda_E[i]$ remains constant. On the other hand, $\Lambda_E[i] \gg 1$ holds for a reasonably small secrecy outage requirement required in practical applications, i.e., $\varepsilon \ll 1$. ■

APPENDIX D
PROOF OF THE CONCAVITY OF THE TRANSFORMED PROBLEM IN (19)

We first consider the concavity of the objective function on a per subcarrier basis w.r.t. variables $\tilde{P}_k[i]$ and $s_k[i]$. Let the objective function in (19) on subcarrier i for user k be $f_k[i] = s_k[i](w_k\tilde{R}_k[i]) - q(\tilde{P}_k[i] + P_C + \delta s_k[i]\tilde{R}_k[i])$. As will be seen in the KKT conditions[8] in (24) and (28), $f_k[i] < 0$ will not be considered in the subcarrier selection process. Therefore, we can assume $f_k[i] \ge 0$ for proving the concavity. Let $\mathbf{H}(f_k[i])$, ρ_1, and ρ_2 be the Hessian matrix of function $f_k[i]$ and the eigenvalues of $\mathbf{H}(f_k[i])$, respectively. The Hessian matrix of function $f_k[i]$, the trace of the Hessian matrix, and ρ_1 are, respectively, given by

$$\mathbf{H}(f_k[i]) = \begin{bmatrix} \frac{-W\Upsilon_k^2[i]s_k[i](w_k-\delta q)}{\left(s_k+\Upsilon_k[i]\tilde{P}_k[i]\right)^2\ln(2)} & \frac{W\Upsilon_k^2[i]\tilde{P}_k[i](w_k-\delta q)}{\left(s_k+\Upsilon_k[i]\tilde{P}_k[i]\right)^2\ln(2)} \\ \frac{W\Upsilon_k^2[i]\tilde{P}_k[i](w_k-\delta q)}{\left(s_k+\Upsilon_k[i]\tilde{P}_k[i]\right)^2\ln(2)} & \frac{-W\Upsilon_k^2[i]\tilde{P}_k^2[i](w_k-\delta q)}{\left(s_k+\Upsilon_k[i]\tilde{P}_k[i]\right)^2 s_k[i]\ln(2)} \end{bmatrix} \tag{42}$$

$$\begin{aligned}\operatorname{tr}\left(\mathbf{H}\left(f_k[i]\right)\right) &= \sum_{t=1}^{2}\rho_t = \frac{-W\Upsilon_k^2[i]\left(\tilde{P}_k^2[i]+s_k^2[i]\right)(w_k-\delta q)}{s_k[i]\ln(2)\left(s_k[i]+\Upsilon_k[i]\tilde{P}_k[i]\right)^2} \\ \rho_1 &= 0.\end{aligned} \tag{43}$$

Note that $\operatorname{tr}(\mathbf{H}(f_k[i])) = \sum_{t=1}^{2}\rho_t \le 0$ since $f_k[i] \ge 0 \rightarrow w_k \ge q\delta$. As a result, $\rho_2 \le 0$, and $\mathbf{H}(f_k[i])$ is a negative semidefinite matrix. Therefore, $f_k[i]$ is jointly concave w.r.t. optimization variables $\tilde{P}_k[i]$ and $s_k[i]$. In addition, $f_k[i]$ is a linear nondecreasing function of $\tilde{R}_k[i]$ for $w_k \ge q\delta$, and $\tilde{R}_k[i]$ is a concave function of $P_k[i]$. Hence, $f_k[i]$ is jointly concave w.r.t. $\tilde{P}_k[i]$, $s_k[i]$, and $\tilde{R}_k[i]$ [29]. Then, the sum of $f_k[i]$ over indices k and i preserves the concavity of the objective function in (19). On the other hand, the constraints C2–C6 in (19) are convex, and thus, the transformed problem is a concave optimization problem. ■

REFERENCES

[1] J. Zeng and H. Minn, "A novel OFDMA ranging method exploiting multiuser diversity," *IEEE Trans. Commun.*, vol. 58, no. 3, pp. 945–955, Mar. 2010.

[2] P. W. C. Chan and R. S. Cheng, "Capacity maximization for zero-forcing MIMO-OFDMA downlink systems with multiuser diversity," *IEEE Trans. Wireless Commun.*, vol. 6, no. 5, pp. 1880–1889, May 2007.

[3] A. Akbari, R. Hoshyar, and R. Tafazolli, "Energy-efficient resource allocation in wireless OFDMA systems," in *Proc. IEEE Pers. Indoor Mobile Radio Commun. Symp.*, Sep. 2010, pp. 1731–1735.

[4] G. Miao, N. Himayat, and G. Li, "Energy-efficient link adaptation in frequency-selective channels," *IEEE Trans. Commun.*, vol. 58, no. 2, pp. 545–554, Feb. 2010.

[5] C. Isheden and G. P. Fettweis, "Energy-efficient multi-carrier link adaptation with sum rate-dependent circuit power," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2010, pp. 1–6.

[7] The assumption of high SNR is necessary to arrive at an efficient resource allocation algorithm. Note that the high SNR assumption does not necessarily require a high transmit power. High SNR can be achieved by exploiting multiuser diversity or using MIMO-beamforming for moderate or small transmit powers.

[8] Note that both the global optimal and the local optimal solutions have to satisfy the KKT conditions, despite the non-convexity of the optimization problem.

[6] C. Isheden and G. P. Fettweis, "Energy-efficient link adaptation with transmitter CSI," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2011, pp. 1381–1386.

[7] Z. Hasan, G. Bansal, E. Hossain, and V. Bhargava, "Energy-efficient power allocation in OFDM-based cognitive radio systems: A risk-return model," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 6078–6088, Dec. 2009.

[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. Int. Conf. Telecommun.*, Jun. 2008, pp. 1–6.

[10] Z. Li, R. Yates, and W. Trappe, "secrecy capacity of independent parallel channels," in *Proc. 44th Annu. Allerton Conf. Commun., Control Comput.*, Sep. 2006, pp. 841–848.

[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, Sep. 2011.

[12] Q. Li and W.-K. Ma, "Secrecy rate maximization of a MISO channel with multiple multi-antenna eavesdroppers via semidefinite programming," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Mar. 2010, pp. 3042–3045.

[13] J. Li and A. Petropulu, "Optimal input covariance for achieving secrecy capacity in Gaussian MIMO wiretap channels," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Mar. 2010, pp. 3362–3365.

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

[15] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Jul. 2010.

[16] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st ed. New York: Springer-Verlag, 2009.

[17] D. W. K. Ng, E. S. Lo, and R. Schober, "Resource allocation for secure OFDMA networks with imperfect CSIT," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2011, pp. 1–6.

[18] D. W. K. Ng, E. S. Lo, and R. Schober, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[19] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication,* 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[20] G. Song and Y. Li, "Cross-layer optimization for OFDM wireless networks-Part II: Algorithm development," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 625–634, Mar. 2005.

[21] I. C. Wong and B. L. Evans, "Optimal OFDMA resource allocation with linear complexity to maximize ergodic weighted sum capacity," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Apr. 2007, pp. 601–604.

[22] W. Dinkelbach, "On nonlinear fractional programming," *Manage. Sci.*, vol. 13, no. 7, pp. 492–498, Mar. 1967. [Online]. Available: http://www.jstor.org/stable/2627691

[23] S. Schaible, "Fractional programming. II, On Dinkelbach's algorithm," *Manage. Sci.*, vol. 22, no. 8, pp. 868–873, Apr. 1976. [Online]. Available: http://www.jstor.org/stable/2630018.

[24] W.-L. Li, Y. J. Zhang, A.-C. So, and M. Win, "Slow adaptive OFDMA systems through chance constrained programming," *IEEE Trans. Signal Process.*, vol. 58, no. 7, pp. 3858–3869, Jul. 2010.

[25] N. Mokari, M. Javan, and K. Navaie, "Cross-layer resource allocation in OFDMA systems for heterogeneous traffic with imperfect CSI," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 1011–1017, Feb. 2010.

[26] Y. Cui, V. K. N. Lau, and R. Wang, "Distributive subband allocation, power and rate control for relay-assisted OFDMA cellular system with imperfect system state knowledge," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5096–5102, Oct. 2009.

[27] C. Y. Wong, R. S. Cheng, K. B. Lataief, and R. D. Murch, "Multiuser OFDM with adaptive subcarrier, bit, and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 10, pp. 1747–1758, Oct. 1999.

[28] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. Commun.*, vol. 54, no. 7, pp. 1310–1321, Jul. 2006.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[30] S. Boyd, L. Xiao, and A. Mutapcic, "Notes for EE392o Stanford University Autumn," Subgradient Methods, 2003/2004.

[31] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd ed. Cambridge, MA: MIT Press, 2009.

[32] *Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations*, 3GPP TR 25.996, 7.0.0, Jun. 2007.

[33] O. Arnold, F. Richter, G. Fettweis, and O. Blume, "Power consumption modeling of different base station types in heterogeneous cellular networks," in *Proc. Future Netw. Mobile Summit*, Jun. 2010, pp. 1–8.

[34] N. Cai and R. W. Yeung, "Secure network coding on a wiretap network," *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, Jan. 2011.

[35] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

Derrick Wing Kwan Ng (S'06) received the Bachelor degree (with first-class honors) and the Masters of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST), Kowloon, Hong Kong, in 2006 and 2008, respectively. He is currently working toward the Ph.D. degree with the University of British Columbia (UBC), Vancouver, BC, Canada.

In the Summer of 2011 and Spring of 2012, he was a Visiting Scholar with the Centre Tecnològic de Telecomunicacions de Catalunya–Hong Kong, Kowloon. His research interests include cross-layer optimization for wireless communication systems, resource allocation in orthogonal frequency-division multiple access wireless systems, and communication theory.

Mr. Ng received the Best Paper Awards at the IEEE Wireless Communications and Networking Conference (WCNC) 2012, the IEEE Global Telecommunication Conference (Globecom) 2011, and the IEEE Third International Conference on Communications and Networking in China 2008. He received the IEEE Student Travel Grants for attending the IEEE WCNC 2010, the IEEE International Conference on Communications (ICC) 2011, and the IEEE Globecom 2011. He also received the R&D Excellence Scholarship from the Center for Wireless Information Technology with HKUST in 2006, the Sumida and Ichiro Yawata Foundation Scholarship in 2008, and the 2009 Four Year Doctoral Fellowship from the UBC. He has served as an Editorial Assistant to the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS since January 2012. He has been a Technical Program Committee member of various conferences, including the ICC 2012 Workshop on Green Communications and Networking, the IEEE Globecom'12 Workshop on Heterogeneous, Multihop, Wireless and Mobile Networks, the IEEE Symposium on Industrial Electronics and Applications 2012, the International Workshop on the Performance Enhancements in MIMO-OFDM Systems 2012, etc.

Ernest S. Lo (S'02–M'08) received the B.Eng. (1st Hons.), M.Phil., and Ph.D. degrees from the Hong Kong University of Science and Technology, Kowloon, Hong Kong.

He is the Founding Director and Chief Representative of the Centre Tecnològic de Tecnològic de Catalunya–Hong Kong, Kowloon. He was a Croucher Postdoc Fellow with Stanford University, Stanford, CA. He has a broad spectrum of research interests, including channel coding, resource allocation, and wireless system and architectural design, all with a goal of finding new resources and inventing new technologies for realizing a flexible, spectrally efficient, and energy-efficient wireless multiuser network. He contributed to the standardization of the IEEE 802.22 cognitive radio wireless regional area network system and holds a few pending and granted U.S. and China patents. Some of them were transferred to other companies.

Dr. Lo has received three Best Paper Awards: one at the IEEE International Conference on Communications (ICC) 2007, Glasgow, U.K.; and another two at the IEEE Global Communications Conference (GLOBECOM), 2011, Houston, TX, and the IEEE Wireless Communications and Networking Conference 2012, Paris, France, respectively. He served as an Editorial Assistant for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS when it was founded and has been a Technical Program Committee member of various conferences, including the IEEE ICC'10, 11, and 12; IEEE GLOBECOM'10, 11, and 12; IEEE International Conference on Communications in China 2012; etc. He was honored as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS.

Robert Schober (M'01–SM'08–F'10) was born in Neuendettelsau, Germany, in 1971. He received the Diplom (Univ.) and Ph.D. degrees in electrical engineering from the University of Erlangen-Nuermberg, Erlangen, Germany, in 1997 and 2000, respectively.

From May 2001 to April 2002, he was a Postdoctoral Fellow with the University of Toronto, Toronto, ON, Canada, sponsored by the German Academic Exchange Service. Since May 2002, he has been with the University of British Columbia (UBC), Vancouver, BC, Canada, where he is currently a Full Professor and a Canada Research Chair (Tier II) in Wireless Communications. Since January 2012, he has also been an Alexander von Humboldt Professor and the Chair for Digital Communication, Friedrich Alexander University, Erlangen. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing.

Dr. Schober is a Fellow of the Canadian Academy of Engineering and a Fellow of the Engineering Institute of Canada. He received the 2002 Heinz Maier–Leibnitz Award from the German Science Foundation, the 2004 Innovations Award of the Vodafone Foundation for Research in Mobile Communications, the 2006 UBC Killam Research Prize, the 2007 Wilhelm Friedrich Bessel Research Award of the Alexander von Humboldt Foundation, the 2008 Charles McDowell Award for Excellence in Research from UBC, a 2011 Alexander von Humboldt Professorship, and a 2012 Natural Sciences and Engineering Research Council of Canada E. W. R. Steacie Fellowship. In addition, he received Best Paper Awards from the German Information Technology Society, the European Association for Signal, Speech and Image Processing, the IEEE Wireless Commnications and Networking Conference 2012, the IEEE Global Communications Conference 2011, the IEEE International Conference on Ultra Wideband 2006, the International Zurich Seminar on Broadband Communications, and European Wireless 2000. He is currently the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS.