Resource Allocation for Secure OFDMA Decode-and-Forward Relay Networks

Derrick Wing Kwan Ng and Robert Schober
Department of Electrical and Computer Engineering, University of British Columbia, Canada
Email: wingn@ece.ubc.ca, rschober@ece.ubc.ca

***Abstract*— In this paper, we formulate an optimization problem for resource allocation and scheduling in orthogonal frequency division multiple access (OFDMA) half-duplex decode-and-forward (DF) relay assisted networks. Our problem formulation takes into account artificial noise generation to combat a multiple antenna eavesdropper. The secrecy data rate, power, and subcarrier allocation policies are optimized to maximize the average secrecy outage capacity (bit/s/Hz securely delivered to the users via relays). The optimization problem is solved by dual decomposition which results in an efficient iterative algorithm. Simulation results illustrate that the proposed iterative algorithm converges in a small number of iterations and guarantees a non-zero secrecy date rate for a given target secrecy outage probability.**

I. Introduction

In recent years, there has been a growing interest in information-theoretic physical layer (PHY) security [1]-[7], as a complement to traditional cryptographic encryption adopted in the application/networks layer. The concept of creating a perfectly secure communication link was first established by Wyner [1]. Wyner demonstrated that a source and a destination can exchange perfectly secure messages, if the eavesdropper's channel is a degraded version of the main channel. As a result, secure communication via different forms of artificial noise generation has been proposed in the literature. In [2] and [3], power allocation problems for ergodic secrecy capacity maximization are studied for different system configurations. However, the assumption of ergodic channels in [2], [3] cannot be justified for delay constrained applications in practice, since the transmitted packets of these applications only experience slow fading. In [4] and [5], the resource allocation in OFDMA systems with PHY security considerations was studied. On the other hand, power allocation for systems employing cooperative jamming enabled by amplify-and-forward and decode-and-forward (DF) relays was investigated in [6] and [7], respectively. In these works, the global channel state information (CSI) of the eavesdroppers is assumed to be known at a centralized unit such that security can always be guaranteed. However, eavesdroppers are usually silent to hide their existence. Thus, the CSI of the eavesdroppers may not be available for the resource allocation in practice. As a result, a secrecy outage occurs whenever the scheduled data rate exceeds the secrecy capacity, which introduces a new quality of service (QoS) concern for secrecy.

Motivated by the aforementioned prior works, in this paper, we derive an iterative resource allocation algorithm for OFDMA DF relaying systems, which ensures secure communication in slow fading by introducing artificial noise and converges fast to the optimal solution.

II. OFDMA Relay Network model

We consider an OFDMA DF downlink system which consists of a base station (BS) with N_T antennas, M relays with N_T antennas each, an eavesdropper with N_E antennas, and K mobile users equipped with a single antenna. We assume that $N_T > N_E$ to ensure secure communication. Both the BS and the relays adopt multiple-input multiple-out beamforming (MIMO-BF) to enhance the system performance. The downlink transmission from the BSs to the users via the relays is accomplished in two time slots. In the first time slot, the BS transmits its signals to the relays. Then, in the second time slot, the relays decode the previously received signals and forward them to the corresponding users. Meanwhile, the eavesdropper attempts to eavesdrop the transmitted messages by receiving the signals in both time slots.

A. Channel Model

The impulse responses of all channels are assumed to be time-invariant (slow fading). We consider an OFDMA DF relay assisted system with n_F subcarriers. The received symbols in the first time slot at relay m for user k and the eavesdropper on subcarrier $i \in \{1, \ldots, n_F\}$ are given by, respectively,

$$\mathbf{y}_{BR_m}[i] = \mathbf{H}_{BR_m}[i]\mathbf{x}_k[i] + \mathbf{n}_m[i] \quad \text{and} \tag{1}$$

$$\mathbf{y}_{B,E}[i] = \mathbf{G}_{B,E}[i]\mathbf{x}_k[i] + \mathbf{e}_1[i], \tag{2}$$

where $\mathbf{x}_k[i] \in \mathbb{C}^{N_T \times 1}$ denotes the transmitted symbol vector and $\mathbb{C}^{N \times M}$ is the space of all $N \times M$ matrices with complex entries. $\mathbf{H}_{BR_m}[i] \in \mathbb{C}^{N_T \times N_T}$ denotes the channel matrix between the BS and relay m on subcarrier i and $\mathbf{G}_{B,E}[i] \in \mathbb{C}^{N_E \times N_T}$ is the channel matrix between the BS and the eavesdropper on subcarrier i. Both variables, $\mathbf{H}_{BR_m}[i]$ and $\mathbf{G}_{B,E}[i]$, include the effects of path loss and multipath fading of the associated channels. $\mathbf{n}_m[i] \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{e}_1[i] \in \mathbb{C}^{N_E \times 1}$ are the additive white Gaussian noise (AWGN) in subcarrier i at relay m and the eavesdropper in the first time slot, respectively. Each entry in both vectors has distribution $\mathcal{CN}(0, N_0)$, where N_0 is the noise power spectral density. Here, $\mathcal{CN}(\nu, \sigma^2)$ denotes a complex Gaussian random variable with mean ν and variance σ^2. In the second time slot, relay m decodes the message $\mathbf{x}_k[i]$ and re-encodes the message as $\mathbf{q}_{m,k}[i] \in \mathbb{C}^{N_T \times 1}$. Then, relay m forwards the re-encoded message $\mathbf{q}_{m,k}[i]$ to user k. Therefore, the signals received at user k and the eavesdropper on subcarrier i from relay m are given by, respectively,

$$y_{R_m,k}[i] = \mathbf{h}_{R_m,k}[i]\mathbf{q}_{m,k}[i] + n_k[i] \quad \text{and} \tag{3}$$

$$\mathbf{y}_{R_m,E}[i] = \mathbf{G}_{R_m,E}[i]\mathbf{q}_{m,k}[i] + \mathbf{e}_2[i]. \tag{4}$$

$\mathbf{h}_{R_m,k}[i] \in \mathbb{C}^{1 \times N_T}$ and $\mathbf{G}_{R_m,E}[i] \in \mathbb{C}^{N_E \times N_T}$ denote the channel matrices from relay m to users k and from relay m to the eavesdropper on subcarrier i, respectively. $n_k[i] \in \mathbb{C}^{1 \times 1}$ and $\mathbf{e}_2[i] \in \mathbb{C}^{N_E \times 1}$ are the AWGN in subcarrier i at user k and the eavesdropper in the second time slot, respectively. For the sake of notational simplicity and without loss of generality, a normalized noise variance of $N_0 = 1$ is assumed for all receivers in the following. We also assume that the CSI (path loss information and multipath fading) of the desired relays and users are perfectly known at the BS. On the other hand, since the CSI of the eavesdropper is unavailable at the BS and relays, in order to secure the desired wireless communication links, *artificial noise* signals are generated at both the BS and relays to degrade the channels between the BS/relays and the eavesdropper.

Artificial Noise Generation: The BS and relay m choose $\mathbf{x}_k[i]$ and $\mathbf{q}_{m,k}[i]$ as the linear combination of the information bearing signal and an artificial noise signal, i.e.,

$$\mathbf{x}_k[i] = \mathbf{b}_{m,k}[i]u_k[i] + \mathbf{V}_{B,R_m}[i]\mathbf{v}[i], \tag{5}$$

$$\mathbf{q}_{m,k}[i] = \mathbf{r}_{m,k}[i]u_k[i] + \mathbf{W}_{R_m,k}[i]\mathbf{w}[i], \tag{6}$$

978-1-4577-0742-1/11/$26.00 ©2011 IEEE

where $u_k[i] \in \mathbb{C}^{1\times 1}$ is the information bearing signal, $\mathbf{v}[i] \in \mathbb{C}^{N_T-1\times 1}$ and $\mathbf{w}[i] \in \mathbb{C}^{N_T-1\times 1}$ are artificial noise vectors whose elements are independent and identically distributed (i.i.d.) complex Gaussian random variables with variance $\sigma_v^2[i]$ and $\sigma_w^2[i]$, respectively. Since $\mathbf{H}_{BR_m}[i]$ and $\mathbf{h}_{R_m,k}[i]$ are known at the BS and relay m, respectively, MIMO-BF can be used to maximize the received signal-to-noise (SNR) ratio at the desired receivers. The beamforming vectors adopted at the BS and relay m, i.e, $\mathbf{b}_{m,k}[i] \in \mathbb{C}^{N_T\times 1}$ and $\mathbf{r}_{m,k}[i] \in \mathbb{C}^{N_T\times 1}$, are chosen to be the power amplified eigenvectors corresponding to the maximum eigenvalue of $\mathbf{H}_{BR_m}^{\dagger}[i]\mathbf{H}_{BR_m}[i]$ and $\mathbf{h}_{R_m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}[i]$, respectively. Here, $[\cdot]^{\dagger}$ represents the conjugate transpose operation. Furthermore, we define two orthogonal bases, $\mathbf{V}_{B,R_m}[i] \in \mathbb{C}^{N_T\times N_T-1}$ and $\mathbf{W}_{R_m,k}[i] \in \mathbb{C}^{N_T\times N_T-1}$, by using the remaining eigenvectors of $\mathbf{H}_{BR_m}^{\dagger}[i]\mathbf{H}_{BR_m}[i]$ and $\mathbf{h}_{R_m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}[i]$, respectively. Hence, the received signals in (1) and (2) can be rewritten as

$$\mathbf{y}_{BR_m}[i] = \mathbf{H}_{BR_m,k}[i]\big(\mathbf{b}_{m,k}[i]u_k[i] + \mathbf{V}_{B,R_m}[i]\mathbf{v}[i]\big) + \mathbf{n}_m[i], \quad (7)$$

$$\mathbf{y}_{B,E}[i] = \mathbf{G}_{B,E}[i]\big(\mathbf{b}_{m,k}[i]u_k[i] + \mathbf{W}_{R_m,k}[i]\mathbf{w}[i]\big) + \mathbf{e}[i], \quad (8)$$

respectively. On the other hand, relay m eliminates the artificial noise by pre-processing the received signal, which yields

$$\begin{aligned}\tilde{\mathbf{y}}_{BR_m}[i] &= (\mathbf{H}_{BR_m}[i]\mathbf{b}_{m,k}[i])^{\dagger}\mathbf{y}_{BR_m}[i] \\ &= \alpha_{m,k}[i]P_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i]s_k[i] + \tilde{\mathbf{n}}_m[i], \quad (9)\end{aligned}$$

where $\lambda_{\max_{BR_m}}[i]$ is the maximum eigenvalue of $\mathbf{H}_{BR_m}^{\dagger}[i]\mathbf{H}_{BR_m}[i]$, $P_{BR_m,k}[i]$ represents the transmit power at the BS on subcarrier i to relay m for serving user k, $0 < \alpha_{m,k}[i] \leq 1$ represents the fraction of power devoted to the information bearing signal on subcarrier i for user k via relay m, and $\tilde{\mathbf{n}}_m[i] = \mathbf{b}_{m,k}^{\dagger}[i]\mathbf{H}_{BR_m,k}^{\dagger}[i]\mathbf{n}_m[i]$ is AWGN which has the same distribution as $\mathbf{n}_m[i]$. In other words, the artificial noise signal generated at the BS does not interfere with the desired relay. Similar signal processing techniques are also adopted for the relay-to-user links. Hence, the equivalent received signal at user k from relay m on subcarrier i is given by

$$\begin{aligned}\tilde{y}_{R_m,k}[i] &= (\mathbf{h}_{R_m,k}[i]\mathbf{r}_{m,k}[i])^{\dagger}y_{m,k}[i] \\ &= \alpha_{m,k}[i]P_{R_m,k}[i]\lambda_{\max_{R_m,k}}[i]s_k[i] + \tilde{n}_k[i], \quad (10)\end{aligned}$$

where $\lambda_{\max_{R_m,k}}[i]$ is the maximum eigenvalue of $\mathbf{h}_{R_m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}[i]$, $P_{R_m,k}[i]$ represents the transmit power at relay m on subcarrier i to user k, and $\tilde{n}_k[i] = \mathbf{r}_{m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}^{\dagger}[i]n_k[i]$ is the AWGN which has the same distribution as $n_k[i]$.

Suppose the total transmit power on subcarrier i in the two time slots for user k via relay m is $P_{m,k}[i]$. We define the following variables [3]:

$$P_{BR_m,k}[i] + P_{R_m,k}[i] = P_{m,k}[i], \quad (11)$$

$$\gamma_{m,k}[i] + (N_T-1)(\sigma_v^2[i] + \sigma_w^2[i]) = P_{m,k}[i], \quad (12)$$

$$\gamma_{m,k}[i] = \alpha_{m,k}[i]P_{m,k}[i], \quad (13)$$

$$\frac{(1-\alpha_{m,k}[i])P_{m,k}[i]}{2(N_T-1)} = \sigma_v^2[i] = \sigma_w^2[i], \quad (14)$$

where $\gamma_{m,k}[i]$ denotes the power allocated to the desired signal on subcarrier i for user k via relay m.

III. Resource Allocation and Scheduling

A. Instantaneous Channel Capacity and Secrecy Outage

Given perfect CSI at the receiver, the capacity between the BS and user k on subcarrier i via relay m is given by [8]

$$C_{m,k}[i] = \frac{1}{2}\log_2\Big(1 + \gamma_{m,k}[i]\Upsilon_{m,k}[i]\Big), \quad (15)$$

$$\Upsilon_{m,k}[i] = \frac{\lambda_{\max_{BR_m}}[i]\lambda_{\max_{R_m,k}}[i]}{\lambda_{\max_{BR_m}}[i] + \lambda_{\max_{R_m,k}}[i]}. \quad (16)$$

On the other hand, the eavesdropper has to be close to either the BS or the relays for effective eavesdropping. Thus, one of the signals received in the two time slots will be much stronger than the other end, selection combining is performed at the eavesdropper for combining the two signals. Since the BS and the relays do not have any CSI of the eavesdropper, we follow the approach in [2], [3] and consider a capacity upper bound for the eavesdropper for resource allocation purposes assuming the absence of thermal noise at the eavesdropper receiver. The capacity of the eavesdropper is upper bounded by

$$C_{m,E}[i] = \frac{1}{2}\log_2\Big(1 + \max\{\Gamma_{B,E}[i], \Gamma_{R_m,E}[i]\}\Big), \quad (17)$$

$$\Gamma_{B,E}[i] = \frac{2\alpha_{m,k}[i](N_T-1)}{1-\alpha_{m,k}[i]}\mathbf{g}_1^{\dagger}[i](\mathbf{G}_1[i]\mathbf{G}_1^{\dagger}[i])^{-1}\mathbf{g}_1[i], \quad (18)$$

$$\Gamma_{R_m,E}[i] = \frac{2\alpha_{m,k}[i](N_T-1)}{1-\alpha_{m,k}[i]}\mathbf{g}_2^{\dagger}[i](\mathbf{G}_2[i]\mathbf{G}_2^{\dagger}[i])^{-1}\mathbf{g}_2[i], \quad (19)$$

where $\mathbf{g}_1[i] = \mathbf{G}_{B,E}[i]\mathbf{b}_{m,k}[i]$, $\mathbf{G}_1[i] = \mathbf{G}_{B,E}[i]\mathbf{V}_{B,R_m}[i]$, $\mathbf{g}_2[i] = \mathbf{G}_{R_m,E}[i]\mathbf{q}_{m,k}[i]$, and $\mathbf{G}_2[i] = \mathbf{G}_{R_m,E}[i]\mathbf{W}_{R_m,k}[i]$.

Therefore, the maximum achievable secrecy capacity between the BS and user k via relay m on subcarrier i can be expressed as [2]

$$C_{sec_{m,k}}[i] = \big(C_{m,k}[i] - C_{m,E}[i]\big)\ 1(C_{m,k}[i] > C_{m,E}[i]), \quad (20)$$

where $1(\cdot)$ denotes an indicator function which is 1 when the event is true and 0 otherwise. A *secrecy outage* occurs whenever the target secrecy data rate $R_{m,k}[i]$ exceeds the secrecy capacity. In order to model the insecurity due to *secrecy outage*, we consider the performance in terms of the secrecy outage capacity. The *average secrecy outage capacity* is defined as the total average bits/s/Hz securely delivered to the K mobile users via M relays (averaged over multiple scheduling slots) and is given by $U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S}) =$

$$\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\frac{w_k s_{m,k}[i]}{n_F}R_{m,k}[i] \times \Pr\Big[C_{m,k}[i] - C_{m,E}[i] > R_{m,k}[i]\Big|\mathbf{\Delta}_{m,k}[i]\Big], \quad (21)$$

where $\mathcal{P},\mathcal{R}$, and $\mathcal{S}$ are the power, secrecy data rate, and subcarrier allocation policies, respectively. $\mathcal{U}_m$ is the set of users associated with relay m. $s_{m,k}[i] \in \{0,1\}$ is the subcarrier allocation indicator. w_k is a positive constant which allows the resource allocator to give different priorities to different users. Matrix $\mathbf{\Delta}_{m,k}[i]$ represents the channel CSI between the BS-to-relay m and relay m-to-user k channels on subcarrier i.

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 from

$$\begin{aligned}
&\arg \max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_{m,k}[i]} U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S})\\
&\text{s.t. C1: } \Pr\Big[R_{m,k}[i] \geq C_{m,k}[i] - C_{m,E}[i]\Big|\boldsymbol{\Delta}_{m,k}[i]\Big] = \varepsilon, \forall k, i,\\
&\quad \text{C2: } \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\Big(P_{BR_m,k}[i] + P_{R_m,k}[i]\Big)s_{m,k}[i] \leq P_T,\\
&\quad \text{C3: } \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}^{K} s_{m,k}[i] = 1, \forall i\\
&\quad \text{C4: } s_{m,k}[i] = \{0,1\}, \forall i,k,m\\
&\quad \text{C5: } P_{BR_m,k}[i], P_{R_m,k}[i] \geq 0,\ \forall i,k,m\\
&\quad \text{C6: } 0 < \alpha_{m,k}[i] \leq 1,\ \forall i,k
\end{aligned} \tag{22}$$

In C1, ε denotes the required secrecy outage probability in the system, i.e., C1 represents a quality-of-service (QoS) metric for communication security. C2 is the joint power constraint for the BS and the relays with total maximum power P_T. Constraints C3 and C4 are imposed to guarantee that each subcarrier will be used by one user only.

IV. Solution of the Optimization Problem

A. Transformation of the Optimization Problem

For derivation of an efficient resource allocation algorithm, it is convenient to incorporate the secrecy outage probability constraint C1 in (22) into the objective function.

Lemma 1 (Equivalent Secrecy Rate): For a given outage probability ε in C1, the equivalent secrecy data rate in subcarrier i for user k is given by $R_{m,k}[i] =$

$$\frac{1}{2}\Big[\log_2\Big(1+\alpha_{m,k}[i]\Gamma_{m,k}[i]\Big) - \log_2\Big(1+\frac{2\alpha_{m,k}[i]\Lambda_E[i]}{1-\alpha_{m,k}[i]}\Big)\Big]^+,$$

$$\Gamma_{m,k}[i] = P_{m,k}[i]\Upsilon_{m,k}[i], \quad \Lambda_E[i] = (N_T-1)F_{z_c}^{-1}(\varepsilon), \tag{23}$$

where $[x]^+ = \max\{0,x\}$ and $F_{z_c}^{-1}(\varepsilon)$ denotes the inverse function of $F_{z_c}(z) = \varepsilon$. Here, $F_{z_c}(z)$ is given by

$$\begin{aligned}
F_{z_c}(z) &= \frac{\sum_{n=0}^{N_E-1}\binom{N_T-1}{n}2z^n}{(1+z)^{N_T-1}}\\
&- \frac{\sum_{n=0}^{N_E-1}\sum_{m=0}^{N_E-1}\binom{N_T-1}{n}\binom{N_T-1}{m}z^{m+n}}{(1+z)^{2N_T-2}}.
\end{aligned} \tag{24}$$

Please refer to the related technical report [9] for a proof of (23).

The second step in solving the optimization problem in (22) is to calculate the fraction of power allocated to each subcarrier for generating the artificial noise. By standard optimization techniques, the asymptotic optimal $\alpha_{m,k}^*[i]$ that maximizes the secrecy outage capacity on subcarrier i for a fixed $P_{m,k}[i]$ in high SNR can be obtained as

$$\alpha_{m,k}^*[i] \approx \frac{-\Gamma_{m,k}[i] + \sqrt{2\Gamma_{m,k}^2[i]\Lambda_E[i]}}{\Gamma_{m,k}[i](2\Lambda_E[i]-1)} \approx \frac{1}{\sqrt{2\Lambda_E[i]}} \tag{25}$$

By putting (25) into (23) for high SNR, the secrecy data rate in subcarrier i for user k with asymptotically optimal $\alpha_{m,k}^*[i]$ and target secrecy outage probability requirement ε at high SNR is given by $R_{m,k}[i]$

$$= \frac{1}{2}\Big[\log_2\Big(1+\frac{P_{m,k}[i]\Upsilon_{m,k}[i]}{\sqrt{(N_T-1)F_{z_c}^{-1}(\varepsilon)}}\Big) - \log_2\Big(1+\Phi_E[i]\Big)\Big]^+, \tag{26}$$

where $\Phi_E[i] = \frac{2\Lambda_E[i]}{\sqrt{2\Lambda_E[i]}-1}$. It can be observed that the SNR of the eavesdropper in each subcarrier approaches a constant in the high transmit power regime. By substituting (26) into (21), a modified objective function is obtained. Then, we follow the approach in [10] and relax constraint C4 in (22) to handle the combinatorial subcarrier assignment. In particular, we allow $s_{m,k}[i]$ to be any real value between zero and one. Therefore, using the equivalent secrecy data rate in Lemma 1, the auxiliary powers $\tilde{P}_{m,k}[i] = P_{m,k}[i]s_{m,k}[i]$, and the continuous relaxation of C4, we can rewrite problem (22) as

$$\begin{aligned}
&\arg\max_{\mathcal{P},\mathcal{R},\mathcal{S}} \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F} w_k s_{m,k}[i]\tilde{R}_{m,k}[i]\\
&\text{s.t. C2: } \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{m,k}[i] \leq P_T\\
&\quad \text{C3,}\quad \text{C5,}\quad \text{C4: } 0 \leq s_{m,k}[i] \leq 1, \qquad \forall i,k,m
\end{aligned} \tag{27}$$

where $\tilde{R}_{m,k}[i] = R_{m,k}[i]\Big|_{P_{m,k}[i]=\tilde{P}_{m,k}[i]/s_{m,k}[i]}$. Note that in general, the operator $[\cdot]^+$ in (26) destroys the concavity of the objective function. Yet, as will be seen in the Karush-Kuhn-Tucker (KKT) conditions in (32), those users with negative data rate will not be considered in the subcarrier selection process. Therefore, we can remove the $[\cdot]^+$ operator from variable $R_{m,k}[i]$ in (26) and preserve the concavity of the transformed problem. Besides, C6 is removed from the optimization problem as the asymptotically optimal $\alpha_{m,k}^*[i]$ in (25) always satisfies the constraint since we assume $\Lambda_E[i] \gg 1/2$. Now, the transformed problem is jointly concave with respect to all optimization variables and it can be shown that under some mild conditions solving the dual problem is equivalent to solving the primal problem [11].

B. Dual Problem Formulation

In this subsection, we solve the optimization problem by solving its dual. The Lagrangian is given by

$$\begin{aligned}
\mathcal{L}(\mu,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}) &= \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m} w_k\sum_{i=1}^{n_F} s_{m,k}[i]\tilde{R}_{m,k}[i] + \sum_{i=1}^{n_F}\beta[i]\\
&-\mu(\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{m,k}[i] - P_T) - \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\beta[i]s_{m,k}[i],
\end{aligned} \tag{28}$$

where $\mu \geq 0$ is the Lagrange multiplier corresponding to the power constraint and $\boldsymbol{\beta}$ is the Lagrange multiplier vector associated with the subcarrier usage constraints with elements $\beta[i] \geq 0$, $i \in \{1,\ldots,n_F\}$. The boundary constraints C4 and C5 will be absorbed into the KKT conditions when deriving the optimal solution in Section IV-C. Thus, the dual problem is

$$\min_{\mu,\boldsymbol{\beta}\geq 0}\ \max_{\mathcal{P},\mathcal{R},\mathcal{S}}\quad \mathcal{L}(\mu,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}). \tag{29}$$

In the following section, we solve the above dual problem iteratively by decomposing it into n_F subproblems with identical structure and a master dual problem.

C. Dual Decomposition and Solution

By dual decomposition, the BS solves the subproblem

$$\max_{\mathcal{P},\mathcal{R},\mathcal{S}}\quad \mathcal{L}(\mu,\boldsymbol{\beta},\mathcal{P},\mathcal{R},\mathcal{S}) \tag{30}$$

for a fixed set of Lagrange multipliers. Using standard optimization techniques, the optimal power allocation for user k on subcarrier i in using relay m is given by Using standard optimization techniques and the KKT conditions, the optimal power allocation for user k on subcarrier i is obtained as

$$\begin{aligned}
\tilde{P}_k^*[i] &= s_k[i]P_k^*[i]\\
&= s_k[i]\Big[\frac{w_k(1-\varepsilon_k)}{(\ln(2))\lambda} - \frac{\sqrt{(N_T-1)F_{z_c}^{-1}(\varepsilon_k)}}{\|\mathbf{h}_{s,k}[i]\|^2}\Big]^+.
\end{aligned} \tag{31}$$

The optimal power allocation on each subcarrier has the form of *multi-level* water-filling. In order to obtain the optimal subcarrier allocation, we take the derivative of the subproblem with respect to $s_{m,k}[i]$ and set it to zero, which yields $\frac{\partial \mathcal{L}}{\partial s_{m,k}[i]}\Big|_{P_{m,k}[i]=P^*_{m,k}[i]} = A_{m,k}[i] - \beta[i] = 0$, where $A_{m,k}[i] \geq 0$ is the marginal benefit in assigning subcarrier i to user k via relay m and can be expressed as

$$A_{m,k}[i] = \frac{w_k}{2}\Big(\log_2 \Big(1 + \frac{P^*_{m,k}[i]\Upsilon_{m,k}[i]}{\sqrt{(N_T-1)F^{-1}_{z_c}(\varepsilon)}}\Big) - \log_2\Big(1+\Phi_E[i]\Big) - \frac{P^*_{m,k}[i]\Theta_{m,k}[i]}{(\ln(2))(1+P^*_{m,k}[i]\Theta_{m,k}[i])}\Big), \quad (32)$$

where $\Theta_{m,k}[i] = \Upsilon_{m,k}[i]/\sqrt{(N_T-1)F^{-1}_{z_c}(\varepsilon)}$. Thus, the optimal allocation of subcarrier i is given by

$$s^*_{m,k}[i] = \begin{cases} 1 & \text{if } A_{m,k}[i] = \max\limits_{a,b} \quad A_{a,b}[i] \geq 0 \\ 0 & \text{otherwise} \end{cases}. \quad (33)$$

Note that each subcarrier will be used for serving only one user eventually. Finally, the optimal secrecy data rate $R^*_{m,k}[i]$ is obtained by substituting (31) into the equivalent secrecy data rate in (26) for the subcarrier with $s^*_{m,k}[i] = 1$.

On the other hand, since the dual function is differentiable, the gradient method can be used to solve the master problem (outer loop) in (29) which leads to

$$\mu(t+1) = \Big[\mu(t) - \xi(t) \times (P_T - \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{m,k}[i])\Big]^+, \quad (34)$$

where t and $\xi(t)$ are the iteration index and the step size, respectively. Then, the updated Lagrange multiplier in (34) is used for solving the subproblems in (30) and updating the power and subcarrier allocation. This procedure is repeated iteratively until convergence is achieved. Convergence to the optimal solution is guaranteed [11]. On the other hand, updating $\beta[i]$ is not necessary as it has the same value for all users.

V. Simulation Results

A single cell with a radius of 1 km is considered. There are $M = 3$ relays equally distributed on the boundary of a circle with a radius of 500 m and the BS as the center. The K active users are uniformly distributed and have a distance between 500 m and 1 km from the BS. The number of subcarriers is $n_F = 64$ and $w_k = 1, \forall k$, for illustration. The 3GPP path loss model is used. We assume that the eavesdropper is located 35 m away from the BS which represents an unfavorable scenario to the desired users, since the users are farther away from the BS than the eavesdropper. The small scale fading coefficients of the BS-to-relay links are assumed to be i.i.d. Rician random variables with a Rician factor of 6 dB, while the small scale fading coefficients of all other links are i.i.d. Rayleigh random variables. The target secrecy outage probability is set to $\varepsilon = 5\%$. The average secrecy outage capacity is obtained by counting the number of packets securely decoded by the users averaged over both the macroscopic and microscopic fading.

Figure 1 illustrates the average secrecy outage capacity versus the total transmit power for $K = 45$ users for different numbers of transmit antennas employed at the BS and the relays. The eavesdropper is equipped with $N_E = 2$ antennas. The performance of the proposed iterative resource allocation algorithm is shown for 5 and 10 iterations. It can be observed that the achievable average secrecy outage capacities for 5 and 10 iterations are virtually the same. In other words, the proposed iterative resource allocation algorithm is able to converge to the optimal solution in a few iterations. On the other hand, Figure 1 also depicts the average throughput achieved by the eavesdropper. As suggested by (26), the average throughput achieved at the eavesdropper does not increase with the total transmit power due to the artificial noise generation at both the BS and the relays, despite the fact that the eavesdropper performs selection combining to increase his/her eavesdropping capability. Besides, it can be observed that an increasing number of transmit antennas does not enhance the performance of the eavesdropper, but it improves the secrecy outage capacity of the desired users.

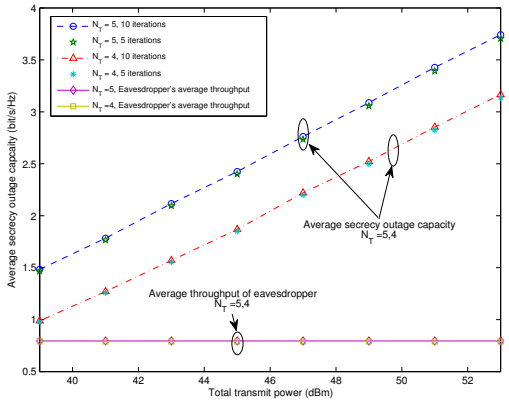

Fig. 1. Average secrecy outage capacity versus transmit power for different numbers of transmit antennas N_T. The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m from the BS.

VI. Conclusion

In this paper, we formulated the resource allocation and scheduling design for OFDMA DF relaying systems as a non-convex and combinatorial optimization problem. An efficient iterative resource allocation algorithm with closed-form power, secrecy data rate, and subcarrier allocation was derived by dual decomposition. Simulation results not only demonstrate that the performance of the proposed algorithm converges to the optimal performance within a small number of iterations, but also reveal the effectiveness of artificial noise generation in combatting the eavesdropper.

References

[1] A. D. Wyner, "The Wire-Tap Channel," Tech. Rep., Oct 1975.

[2] S. Goel and R. Negi, "Guaranteeing Secrecy using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180 – 2189, June 2008.

[3] X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Veh. Technol.*, pp. 3831 – 3842, July 2010.

[4] E. A. Jorswieck and A. Wolf, "Resource Allocation for the Wire-Tap Multi-Carrier Broadcast Channel," in *Proc. International Conf. on Telecommun.*, June 2008, pp. 1 – 6.

[5] Z. Li, R. Yates, and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," in *Proc. 44th Annu. Allerton Conf. Commun., Control and Computing*, Sep 2006, pp. 841–848.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-Forward Based Cooperation for Secure Wireless Communications," in *Proc. IEEE Inter. Conference on Acoustics, Speech and Signal Process.*, Apr 2009, pp. 2613 – 2616.

[7] L. Jiangyuan, A. P. Petropulu, and S. Weber, "Secrecy Rate Optimization under Cooperation with Perfect Channel State Information," in *Proc. the Forty-Third Asilomar Conf. on Signals, Systems and Computers*, Nov 2009, pp. 824 – 828.

[8] C. N. Hsu, H. J. Su, and P. H. Lin, "Joint Subcarrier Pairing and Power Allocation for OFDM Transmission with Decode-and-Forward Relaying," *IEEE Trans. Signal Process.*, pp. 1–1, Sept. 2010.

[9] D. W. K. Ng and R. Schober, "Resource Allocation for Secure OFDMA Decode-and-Forward Relaying Networks," http://www.ece.ubc.ca/~wingn/CWIT2011_full.pdf, Tech. Rep.

[10] C. Y. Wong, R. S. Cheng, K. B. Lataief, and R. D. Murch, "Multiuser OFDM with Adaptive Subcarrier, Bit, and Power Allocation," *IEEE J. Select. Areas Commun.*, vol. 17, pp. 1747–1758, Oct 1999.

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