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

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

***Abstract*—In this paper, we formulate an optimization problem for secure 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 passive multiple antenna eavesdropper and the effects of imperfect channel state information at the transmitter (CSIT) in slow fading. The optimization problem is solved by dual decomposition which results in a highly scalable distributed iterative resource allocation algorithm. The packet data rate, secrecy data rate, power, and subcarrier allocation policies are optimized to maximize the average secrecy outage capacity (bit/s/Hz securely and successfully delivered to the users via relays). Simulation results illustrate that our proposed distributed iterative algorithm converges to the optimal solution in a small number of iterations and guarantees a non-zero secrecy data rate for given target secrecy outage and channel outage probability requirements.**

***Index Terms*—Physical (PHY) layer security, imperfect CSI, passive eavesdropper, decode-and-forward relay, artificial noise generation, MIMO beamforming.**

I. Introduction

ORTHOGONAL frequency division multiple access (OFDMA) is a promising candidate for high speed wireless multiuser communication networks, such as 3GPP Long Term Evolution (LTE), IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX), and IEEE 802.22 Wireless Regional Area Networks (WRAN), not only because of its robustness against multipath fading, but also its flexibility in resource allocation. In an OFDMA system, the fading coefficients of different subcarriers are likely independent for different users and the maximum system throughput can be achieved by selecting the best user for each subcarrier and adapting the corresponding transmit power, which is known as *multiuser diversity* [1], [2]. On the other hand, cooperative relaying is an attractive technique to increase the range of communication systems and to enhance the link reliability without incurring the high cost of additional base station (BS) deployment. Different relaying strategies such as amplify-and-forward (AF), compress-and-forward, and decode-and-forward (DF) have been proposed in the literature [3]-[5]. There is no uniformly optimal relaying protocol and each protocol can outperform the others, depending on the system configuration. However, DF relaying has the advantage that conventional transmitter and receiver structures can be employed.

Recently, a large amount of work has been devoted to information-theoretic physical (PHY) layer security [6]-[16], as a complement to the traditional cryptographic encryption adopted in the application layer. The pioneering work on PHY layer security by Wyner [6] showed that a source and a destination can exchange perfectly secure messages with a non-zero rate if the desired receiver enjoys better channel conditions than the passive eavesdropper(s). In [7], [8], and [9], resource allocation in multi-carrier systems with PHY layer security considerations was studied for the case of a single-user system, a two-user system, and a multi-user system, respectively. On the other hand, power allocation for systems employing cooperative jamming enabled by AF and DF relays was investigated in [10] and [11], respectively. In these works, the channel state information (CSI) of the eavesdroppers is assumed to be known at the BS such that secure communication can be guaranteed. Yet, eavesdroppers are usually passive and silent in order to hide their existence. Thus, the CSI of the eavesdroppers cannot be measured at the BS by estimating handshaking signals or be obtained via feedback from the eavesdroppers. On the other hand, secure communication systems employing multiple antennas have been proposed for the case where the eavesdropper's CSI is not available. By exploiting the extra degrees of freedom in a multiple antennas system, artificial noise or interference is injected into the null space of the desired users to degrade the channels of the eavesdroppers. In [12] and [13], the authors studied the power allocation problem 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. However, the assumption of ergodic channels cannot be justified for delay sensitive applications in practice since the transmitted packets of these applications experience quasi-static fading. Hence, a secrecy outage [14, Chapter 5] occurs whenever the scheduled secrecy data rate exceeds the secrecy capacity between the BS and the eavesdroppers, which introduces a quality of service (QoS) concern for secrecy. In [15] and [16], under the assumption of perfect CSI of the desired users, the authors proposed resource allocation algorithms with secrecy

Manuscript received March 25, 2011; revised July 13, 2011; accepted July 28, 2011. The associate editor coordinating the review of this paper and approving it for publication was R. Nabar.

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

E. S. Lo is with Centre Tecnològic de Telecomunicacions de Catalunya - Hong Kong Branch (CTTC-HK) (e-mail: ernest.lo@ieee.org).

This paper will be presented in part at the IEEE Global Communications Conference (Globecom 2011).

Digital Object Identifier 10.1109/TWC.2011.082011.110538

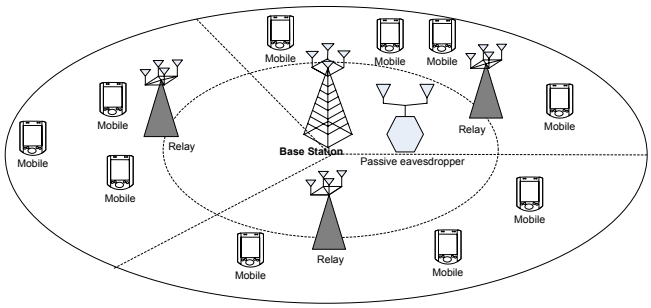

Fig. 1. An illustration of a downlink OFDMA DF relay network. There are one BS and $M = 3$ DF relays with $N_T = 4$ antennas, $K = 10$ desired users equipped with a single antenna, and one eavesdropper with $N_E = 2$ antennas. For an effective eavesdropping, the eavesdropper chooses a location closer to either the BS or a relay than all the desired users.

QoS consideration in multi-carrier single-hop and two-hop systems, respectively. Yet, the CSI of the desired users may be outdated at the transmitter even if the users are moving with pedestrian speeds. The imperfect channel state information at transmitter (CSIT) introduces two kinds of performance degradation which have not been taken into account in [7]-[16]. First, in quasi-static fading without perfect CSIT, the transmitted packet is corrupted whenever the transmit data rate exceeds the channel capacity between the active legitimate transceivers even if channel capacity achieving codes are used for error protection. i.e., a channel outage occurs [17, Chapter 5.4]. Second, with imperfect user CSIT, the artificial noise not only interferes with the eavesdropper, but also interferes with the desired users since their null space information is inaccurate. Therefore, in this paper, a distributed resource allocation algorithm which takes into account secrecy outage, channel outage, and the potentially negative effects of artificial noise generation is proposed.

II. OFDMA Downlink Network Model

A. Channel Model

We consider a downlink OFDMA network which consists of a BS with N_T antennas, M DF relays with N_T antennas each, an eavesdropper[1] with N_E antennas, and K mobile users equipped with a single antenna, cf. Figure 1. A single cell with two ring-shaped boundary regions is studied. The region between the inner boundary and the outer boundary is divided into M sectors of equal size as shown in Figure 1 and each user is assigned to only one relay according to some predefined criteria such as average signal-to-noise ratio (SNR). Users in all sectors are competing for resources with each other. We assume that there is no direct transmission between the BS and the mobile users due to heavy blockage and long distance transmission. We also assume that the resource allocation for relay assisted users (located between the inner and the outer boundaries) and non-relay assisted users (located inside the inner boundary) is done separately. Both the BS and the relays adopt multiple-input multiple-output beamforming (MIMO-BF) to enhance the system performance. 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.

[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.

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 $m \in \{1, \ldots, M\}$ for user $k \in \{1, \ldots, K\}$ and the eavesdropper on subcarrier $i \in \{1, \ldots, n_F\}$ are given by, respectively,

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

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

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 $\mathbf{G}_{BE}[i] \in \mathbb{C}^{N_E \times N_T}$ is the channel matrix between the BS and the eavesdropper on subcarrier i. Both variables, $\mathbf{H}_{BR_m}[i]$ and $\mathbf{G}_{BE}[i]$, include the effects of path loss and multipath fading. $\mathbf{n}_{R_m}[i] \in \mathbb{C}^{N_T \times 1}$ 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 variance. 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 message $\mathbf{x}_k[i]$ and re-encodes the message as $\mathbf{q}_{R_m,k}[i] \in \mathbb{C}^{N_T \times 1}$. Then, relay m forwards the re-encoded message $\mathbf{q}_{R_m,k}[i]$ to user k. Therefore, the signals received at user k and the eavesdropper on subcarrier i from relay m are given by, respectively,

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

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

$\mathbf{h}_{R_m,k}[i] \in \mathbb{C}^{1 \times N_T}$ 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.

B. Channel State Information

The resource allocation and scheduling problem presented in the next section can be solved either centrally at the BS or in a distributed fashion. For the centralized solution, the BS requires the CSI of all BS-to-relay and relay-to-user links at the beginning of each scheduling slot. In contrast, for the distributed solution the relays only require the CSI of their own BS-to-relay and relay-to-user links, whereas the BS does not need any CSI. We assume a Frequency Division Duplex (FDD) system where the CSI of the relay-to-user links is obtained through feedback from the users to the relays at the beginning of each scheduling slot, while the CSI of the BS-to-relay links can be obtained at the relays either in the handshaking phase or from a previous transmission. In the following, since path loss is a slowly varying random

process which changes on the order of seconds, we assume that the path loss can be estimated perfectly. For the multipath fading, we take into account the different natures of the BS-to-relay and the relay-to-user links. In particular, since both the BS and the relays are static, the BS-to-relay links are assumed to be time-invariant. Thus, the BS-to-relay fading gains $\mathbf{H}_{BR_m}[i]$, $m \in \{1,\ldots,M\}$, $i \in \{1,\ldots,n_F\}$, can be reliably estimated at the relays with negligible estimation error. Therefore, we can assume perfect CSIT for the BS-to-relay links. On the other hand, although we also assume that the users can obtain perfect estimates of the relay-to-user fading gains $\mathbf{h}_{R_m,k}[i]$, $m \in \{1,\ldots,M\}$, $k \in \{1,\ldots,K\}$ for signal detection purpose, the corresponding CSI may be outdated at the relays (for the distributed solution) and at the BS (for the centralized solution) because of the mobility of the users and the feedback delay. To capture this effect, we model the multipath fading CSIT of the link between user k and relay m on subcarrier i as

$$\mathbf{h}_{R_m,k}[i] = \hat{\mathbf{h}}_{R_m,k}[i] + \Delta\mathbf{h}_{R_m,k}[i], \tag{5}$$

where $\hat{\mathbf{h}}_{R_m,k}[i]$ and $\Delta\mathbf{h}_{R_m,k}[i]$ denote, respectively, the estimated CSI vector and the CSIT error vector. $\hat{\mathbf{h}}_{R_m,k}[i]$ and $\Delta\mathbf{h}_{R_m,k}[i]$ are Gaussian random vectors and each vector has independent and identically distributed (i.i.d.) elements. Besides, the elements of vectors $\mathbf{h}_{R_m,k}[i]$, $\hat{\mathbf{h}}_{R_m,k}[i]$, and $\Delta\mathbf{h}_{R_m,k}[i]$ have zero means and variance $\sigma^2_{h_{R_m,k}}$, $\sigma^2_{\hat{h}_{R_m,k}} - \sigma^2_e$, and σ^2_e, respectively. Assuming a minimum mean square error (MMSE) estimator, the CSI error vector and the actual CSI vector are mutually uncorrelated [18, p.177].

On the other hand, the CSI of the eavesdropper is unavailable at both the BS and the relays. Thus, in order to secure the desired wireless communication links, *artificial noise* signals are generated at both the BS and the relays to degrade the channels between the BS/relays and the eavesdropper.

C. Artificial Noise Generation

The BS and relay m choose $\mathbf{x}_k[i]$ and $\mathbf{q}_{R_m,k}[i]$ as the linear combination of the information bearing signal and an artificial noise signal which can be presented as

$$\mathbf{x}_k[i] = \underbrace{\mathbf{b}_{BR_m,k}[i]u_k[i]\sqrt{\alpha_{BR_m,k}[i]P_{BR_m,k}[i]}}_{\text{Desired Signal}} + \underbrace{\mathbf{V}_{BR_m}[i]\mathbf{v}[i]}_{\text{Artificial Noise}} \quad \text{and} \tag{6}$$

$$\mathbf{q}_{R_m,k}[i] = \underbrace{\hat{\mathbf{r}}_{R_m,k}[i]u_k[i]\sqrt{\alpha_{R_m,k}[i]P_{R_m,k}[i]}}_{\text{Desired Signal}} + \underbrace{\mathbf{W}_{R_m,k}[i]\mathbf{w}[i]}_{\text{Artificial Noise}}, \tag{7}$$

respectively. $u_k[i] \in \mathbb{C}^{1\times 1}$ 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 i.i.d. complex Gaussian random variables with variance $\sigma^2_v[i]$ and $\sigma^2_w[i]$, respectively. Since $\mathbf{H}_{BR_m}[i]$ and $\hat{\mathbf{h}}_{R_m,k}[i]$ are known at the BS and relay m, respectively, MIMO-BF can be used to maximize the received SNR ratio at the desired receivers. The beamforming vectors adopted at the BS and relay m, i.e, $\mathbf{b}_{BR_m,k}[i] \in \mathbb{C}^{N_T\times 1}$ and $\hat{\mathbf{r}}_{R_m,k}[i] \in \mathbb{C}^{N_T\times 1}$, are chosen to be the eigenvectors corresponding to the maximum eigenvalue of $\mathbf{H}^{\dagger}_{BR_m}[i]\mathbf{H}_{BR_m}[i]$ and $\hat{\mathbf{h}}^{\dagger}_{R_m,k}[i]\hat{\mathbf{h}}_{R_m,k}[i]$, respectively. Here, $[\cdot]^{\dagger}$ denotes the conjugate transpose operation. Furthermore, we define two orthogonal bases, $\mathbf{V}_{BR_m}[i] \in \mathbb{C}^{N_T\times N_T-1}$ and $\mathbf{W}_{R_m,k}[i] \in \mathbb{C}^{N_T\times N_T-1}$, by using the remaining eigenvectors of $\mathbf{H}^{\dagger}_{BR_m}[i]\mathbf{H}_{BR_m}[i]$ and $\hat{\mathbf{h}}^{\dagger}_{R_m,k}[i]\hat{\mathbf{h}}_{R_m,k}[i]$, respectively. $P_{BR_m,k}[i]$ represents the transmit power at the BS on subcarrier i to relay m for serving user k. $P_{R_m,k}[i]$ denotes the transmit power at relay m on subcarrier i to user k. Variables $0 < \alpha_{BR_m,k}[i] \leq 1$ and $0 < \alpha_{R_m,k}[i] \leq 1$ are the fractions of power devoted to the information bearing signal at the BS and relay m on subcarrier i for user k, respectively. Since the CSI of the eavesdropper is unavailable at both the BS and the relays, the remaining powers at the BS and relay m on subcarrier i are equally distributed across $N_T - 1$ dimensions for generating the artificial noises with variances $\sigma^2_v[i] = \frac{(1-\alpha_{BR_m,k}[i])P_{BR_m,k}[i]}{N_T-1}$ and $\sigma^2_w[i] = \frac{(1-\alpha_{R_m,k}[i])P_{R_m,k}[i]}{N_T-1}$, respectively. Hence, the received signals in (1) can be rewritten as

$$\begin{aligned}\mathbf{y}_{BR_m}[i] &= \mathbf{H}_{BR_m}[i]\big(\mathbf{b}_{BR_m,k}[i]u_k[i]\sqrt{\alpha_{BR_m,k}[i]P_{BR_m,k}[i]} \\ &\quad + \mathbf{V}_{BR_m}[i]\mathbf{v}[i]\big) + \mathbf{n}_{R_m}[i], \end{aligned}\tag{8}$$

$$\begin{aligned}\mathbf{y}_{BE}[i] &= \mathbf{G}_{BE}[i]\big(\mathbf{b}_{BR_m,k}[i]u_k[i]\sqrt{\alpha_{BR_m,k}[i]P_{BR_m,k}[i]} \\ &\quad + \mathbf{V}_{BR_m}[i]\mathbf{v}[i]\big) + \mathbf{e}_1[i]. \end{aligned}\tag{9}$$

In the second time slot, relay m eliminates the artificial noise by pre-processing the received signal as

$$\begin{aligned}\tilde{\mathbf{y}}_{BR_m}[i] &= (\mathbf{H}_{BR_m}[i]\mathbf{b}_{BR_m,k}[i])^{\dagger}\mathbf{y}_{BR_m}[i] \\ &= \sqrt{\alpha_{BR_m,k}[i]P_{BR_m,k}[i]}\lambda_{\max_{BR_m}}[i]u_k[i] + \tilde{\mathbf{n}}_{R_m}[i], \end{aligned}\tag{10}$$

where $\tilde{\mathbf{n}}_{R_m}[i] = \mathbf{b}^{\dagger}_{BR_m,k}[i]\mathbf{H}^{\dagger}_{BR_m}[i]\mathbf{n}_{R_m}[i]$ is AWGN which has the same distribution as $\mathbf{n}_{R_m}[i]$ and $\lambda_{\max_{BR_m}}[i]$ is the maximum eigenvalue of $\mathbf{H}^{\dagger}_{BR_m}[i]\mathbf{H}_{BR_m}[i]$. It can be observed that the artificial noise signal generated at the BS does not interfere with the desired signal at relay m due to the adopted pre-processing. On the other hand, the signal received at user k and the eavesdropper on subcarrier i from relay m in (3) and can be rewritten as

$$\begin{aligned}y_{R_m,k}[i] &= \mathbf{h}_{R_m,k}[i]\Big(\hat{\mathbf{r}}_{R_m,k}[i]u_k[i]\sqrt{\alpha_{R_m,k}[i]P_{R_m,k}[i]} \\ &\quad + \mathbf{W}_{R_m,k}[i]\mathbf{w}[i]\Big) + n_k[i] \text{ and} \end{aligned}\tag{11}$$

$$\begin{aligned}\mathbf{y}_{R_m,E}[i] &= \mathbf{G}_{R_m,E}[i]\Big(\hat{\mathbf{r}}_{R_m,k}[i]u_k[i]\sqrt{\alpha_{R_m,k}[i]P_{R_m,k}[i]} \\ &\quad + \mathbf{W}_{R_m,k}[i]\mathbf{w}[i]\Big) + \mathbf{e}_2[i], \end{aligned}\tag{12}$$

respectively. Note that due to the imperfect CSIT at relay m, there is an artificial noise leakage from the null space to the range space of user k on subcarrier i. The negative effects of artificial noise generation with imperfect CSIT are demonstrated in the next section via channel capacity equations and the concept of outages.

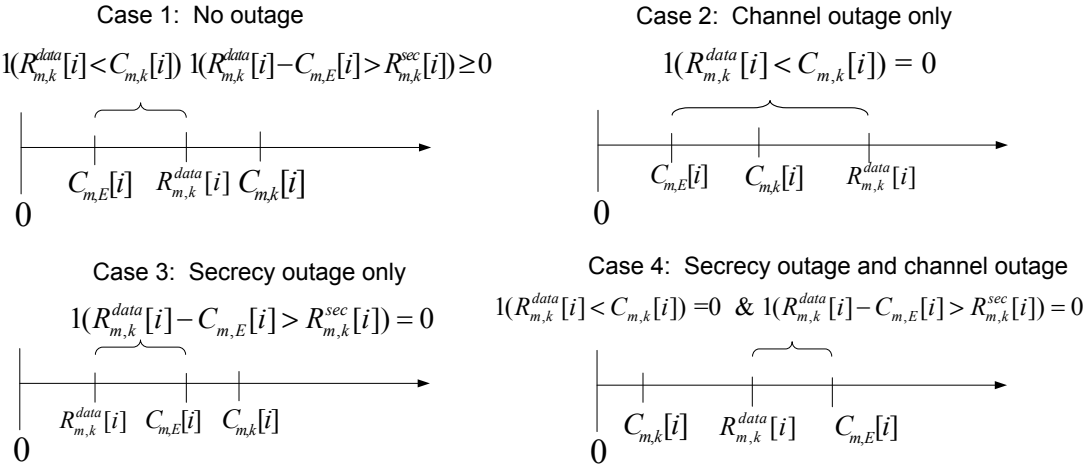

Fig. 2. An illustration of the relationship between packet data rate $R^{data}_{m,k}[i]$, secrecy data rate $R^{sec}_{m,k}[i]$, the capacity of the user channel, $C_{m,k}[i]$, and the capacity of the eavesdropper channel, $C_{m,E}[i]$, for four possible cases.

III. Resource Allocation and Scheduling

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

Since we assume perfect CSI at the receiver (CSIR), the instantaneous channel capacity between the BS and relay m on subcarrier i is given by

$$C_{BR_m,k}[i]=\log_2\Big(1+\alpha_{BR_m,k}[i]P_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i]\Big). \tag{13}$$

On the other hand, user k first estimates the effective channel $\mathbf{h}_{R_m,k}[i]\hat{\mathbf{r}}_{R_m,k}[i]$ for coherent detection. Hence, the instantaneous channel capacity between relay m and users k on subcarrier i is obtained as

$$C_{R_m,k}[i] = \log_2\Big(1+\frac{\alpha_{R_m,k}[i]P_{R_m,k}[i]\|\mathbf{h}_{R_m,k}[i]\hat{\mathbf{r}}_{R_m,k}[i]\|^2}{1+(1-\alpha_{R_m,k})P_{R_m,k}[i]\sigma_e^2}\Big), \tag{14}$$

where $\|\cdot\|$ denotes the Euclidean norm of a vector. Thus, the channel capacity between the BS and user k via relay m on subcarrier i is given by

$$C_{m,k}[i]=\frac{1}{2}\min\Big\{C_{BR_m,k}[i],C_{R_m,k}[i]\Big\}, \tag{15}$$

where the pre-log factor $\frac{1}{2}$ is due to the two channel uses required for transmitting one message.

In practice, the eavesdropper has to be close to either the BS or one of the relays for effective eavesdropping. Thus, one of the signals received in the two time slots will be much stronger than the other one making selection combining of the two received signals at the eavesdropper near optimal. Besides, since we assume the BS and the relays do not have any CSI of the eavesdropper, we follow the approach in [12], [13] and consider a capacity upper bound for the eavesdropper for resource allocation purposes assuming the absence of thermal noise at the eavesdropper receiver. Therefore, the capacity of the eavesdropper is upper bounded[2] by

$$C_{m,E}[i]= \frac{1}{2}\log_2\Big(1+\max\{\Gamma_{B,E}[i],\Gamma_{R_m,E}[i]\}\Big), \tag{16}$$

$$\Gamma_{B,E}[i]= \frac{\alpha_{BR_m,k}[i](N_T-1)}{1-\alpha_{BR_m,k}[i]}\mathbf{g}_1^\dagger[i](\mathbf{G}_1[i]\mathbf{G}_1^\dagger[i])^{-1}\mathbf{g}_1[i], \tag{17}$$

$$\Gamma_{R_m,E}[i]= \frac{\alpha_{R_m,k}[i](N_T-1)}{1-\alpha_{R_m,k}[i]}\mathbf{g}_2^\dagger[i](\mathbf{G}_2[i]\mathbf{G}_2^\dagger[i])^{-1}\mathbf{g}_2[i], \tag{18}$$

where $\mathbf{g}_1[i]=\mathbf{G}_{BE}[i]\mathbf{b}_{BR_m,k}[i]$, $\mathbf{G}_1[i]=\mathbf{G}_{BE}[i]\mathbf{V}_{BR_m}[i]$, $\mathbf{g}_2[i]=\mathbf{G}_{R_m,E}[i]\mathbf{q}_{R_m,k}[i]$, and $\mathbf{G}_2[i]=\mathbf{G}_{R_m,E}[i]\mathbf{W}_{R_m,k}[i]$. We note that the proposed resource allocation algorithm (see next section) can also be applied if other combining schemes such as optimal maximum ratio combining (MRC) are used. (We substitute $F_{z_c}^{-1}(\cdot,i)$ in (22) by the inverse cumulative distribution function (cdf) of the resultant MRC SIR.)

The maximum achievable secrecy data rate $R^{sec}_{m,k}[i]$ of a perfectly secure communication between the BS and user k on subcarrier i via relay m with outage consideration can be expressed as

$$\begin{aligned} R^{sec}_{m,k}[i] \quad &\times \quad 1(R^{data}_{m,k}[i]<C_{m,k}[i]) \\ &\times \quad 1(R^{data}_{m,k}[i]-C_{m,E}[i]>R^{sec}_{m,k}[i]), \end{aligned} \tag{19}$$

where $1(\cdot)$ denotes an indicator function which is 1 when the event is true and 0 otherwise and $R^{data}_{m,k}[i]$ denotes the actual packet data rate transmitted from the BS to user k via relay m. The relationships between the variables in (19) are illustrated in Figure 2. In the considered system, there are two types of outage measures. The first one is known as channel outage [17, Chapter 5.4] which corresponds to the first indictor function in (19). It occurs whenever the transmit data rate exceeds the instantaneous channel capacity between two desired transceivers, i.e., $R^{data}_{m,k}[i]>C_{m,k}[i]$. If $R^{data}_{m,k}[i]>C_{m,k}[i]$, any transmitted packet is corrupted even if a channel capacity achieving code is applied for error protection. Indeed, channel

[2]The upper bound is referring to the individual signal-to-interference ratio (SIR) equations in (17) and (18) for which the absence of thermal noise at the eavesdropper is assumed.

outage can be avoided by data rate adaptation when the CSIT of the desired user channel can be perfectly obtained. Yet, highly accurate CSIT is difficult to obtain if the users are not static. The second type of outage is secrecy outage [14, Chapter 5] which corresponds to the second indicator function in (19). If the CSI of all links (including the links of the eavesdropper) are available at the BS, the resource allocator can set the target secrecy data rate $R_{m,k}^{sec}[i]$ to match the channel conditions [12], i.e., $R_{m,k}^{sec}[i] < R_{m,k}^{data}[i] - C_{m,E}[i]$ and $R_{m,k}^{data}[i] > C_{m,E}[i]$, such that a packet with secrecy data rate $R_{m,k}^{sec}[i]$ and data rate $R_{m,k}^{data}[i]$ can be securely delivered and successfully decoded by the desired user. However, here the eavesdropper is assumed to be passive and its CSI is not available at the BS, i.e., $C_{m,E}[i]$ is a random variable for the BS. Hence, a *secrecy outage* occurs whenever the target secrecy data rate $R_{m,k}^{sec}[i]$ exceeds the secrecy capacity, i.e., $R_{m,k}^{data}[i] - C_{m,E}[i]$.

In order to model the unreliability and the insecurity due to both *channel outage* and *secrecy outage*, respectively, we consider the performance in terms of the *average secrecy outage capacity*, which is defined as the total average bit/s/Hz securely and successfully delivered to the K mobile users (averaged over multiple scheduling slots) and is given by

$$\begin{aligned}
&U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S})\\
&=\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m} w_k \sum_{i=1}^{n_F}\frac{s_{m,k}[i]}{n_F}\mathcal{E}\Big\{R_{m,k}^{sec}[i]\\
&\times 1\Big(R_{m,k}^{data}[i]-C_{m,E}[i]>R_{m,k}^{sec}[i]\Big)\ 1\Big(R_{m,k}^{data}[i]<C_{m,k}[i]\Big)\Big\}\\
&=\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m} w_k \sum_{i=1}^{n_F}\frac{s_{m,k}[i]}{n_F}\Bigg\{R_{m,k}^{sec}[i]\\
&\times \Pr\left[R_{m,k}^{data}[i]-C_{m,E}[i]>R_{m,k}^{sec}[i]\Big|\boldsymbol{\Delta}_{m,k}[i]\right]\\
&\times \Pr\left[R_{m,k}^{data}[i]<C_{m,k}[i]\Big|\boldsymbol{\Delta}_{m,k}[i]\right]\Bigg\},
\end{aligned}\tag{20}$$

where $\mathcal{E}\{\cdot\}$ denotes statistical expectation. Here, $\mathcal{P},\mathcal{R}$, and $\mathcal{S}$ are the power, data rate (secrecy data rate and packet data rate), and subcarrier allocation policies, respectively. $\mathcal{U}_m$ denotes 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 provided by the upper layers, which allows the resource allocator to give different priorities to different users and to enforce certain notions of fairness. $\boldsymbol{\Delta}_{m,k}[i]$ represents a pair of CSI vectors, namely the perfect CSI vector of the BS-to-relay m link and the imperfect CSI vector of the relay m-to-user k channel on subcarrier i.

B. Optimization Problem Formulation

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

Problem 1 (Optimization Problem Formulation):

$$\begin{aligned}
&\arg\max_{\mathcal{P},\mathcal{R},\mathcal{S},\alpha_{BR_m,k}[i],\alpha_{R_m,k}[i]} U_{sec}(\mathcal{P},\mathcal{R},\mathcal{S})\\
\text{s.t. C1:}\ &\Pr\left[R_{m,k}^{data}[i]\ge C_{m,k}[i]\Big|\boldsymbol{\Delta}_{m,k}[i]\right]\le\varepsilon,\quad\forall k,i,\\
\text{C2:}\ &\Pr\left[R_{m,k}^{sec}[i]\ge R_{m,k}^{data}[i]-C_{m,E}[i]\Big|\boldsymbol{\Delta}_{m,k}[i]\right]\le\delta,\forall k,i,\\
\text{C3:}\ &\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}P_{BR_m,k}[i]s_{m,k}[i]\le P_{B_T},\\
\text{C4:}\ &\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}P_{R_m,k}[i]s_{m,k}[i]\le P_{R_T},\quad\forall m,\\
\text{C5:}\ &\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}s_{m,k}[i]\le 1,\quad\forall i,\\
\text{C6:}\ &s_{m,k}[i]=\{0,1\},\ \forall i,k,m,\\
\text{C7:}\ &P_{BR_m,k}[i],P_{R_m,k}[i]\ge 0,\quad\forall i,k,m,\\
\text{C8:}\ &0<\alpha_{BR_m,k}[i],\alpha_{R_m,k}[i]\le 1,\ \forall i,k,m.
\end{aligned}\tag{21}$$

Here, C1 represents the required data rate outage probability due to the imperfect CSI of the relay-to-user channels. In C2, δ denotes the required secrecy outage probability in the system. Note that C1 and C2 represent two QoS metrics for communication reliability and communication security, respectively. C3 (C4) represents the individual power constraint for the BS (relays) with maximum transmit power P_{B_T} (P_{R_T}). Constraints C5 and C6 are imposed to guarantee that each subcarrier will be used by one user only. C7 and C8 are the boundary constraints of the power allocation variables.

Remark 1: The optimal amount of artificial noise strikes a balance between the channel capacity and the secrecy capacity. When there is no power allocated to the artificial noise generation, the channel capacity will be maximized since all the power is allocated to the information bearing signal. However, a certain secrecy outage probability cannot be guaranteed and the secrecy capacity decreases dramatically to zero for most channel conditions. On the contrary, when nearly all the power is allocated to the artificial noise generation, although the capacity of the eavesdropper channel approaches zero, because of the imperfect CSIT, the excessive artificial noise will also interfere with the desired user signal which decreases both the channel capacity and the secrecy capacity. Besides, even with perfect CSIT, the channel capacity decreases if we allocate more power to the artificial noise.

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 channel outage constraint C1 and the secrecy outage probability constraint C2 in (21) into the objective function. This is possible if the constraints in C1 and C2 are fulfilled with equality for the optimal solution. Thus, in the following we replace the "$\le$"-signs in C1 and C2 by "$=$"-signs and the resulting optimization problem may be viewed as a restricted version of the original problem (21) since the latter has a smaller feasible set. We are now ready to introduce the following Lemma.

Lemma 1 (Equivalent Objective Function): For a given channel outage probability ε and a given secrecy outage probability δ in C1 and C2, respectively, the equivalent secrecy data rate in high SNR on subcarrier i for user k via relay m is lower bounded by

$$R_{m,k}^{sec}[i] > \left[R_{m,k}^{data}[i] - \frac{1}{2}\log_2\left(1+\frac{\alpha_{BR_m,k}^*[i]\Lambda_E[i]}{1-\alpha_{BR_m,k}^*[i]}\right)\right]^+, \text{where}$$

$$R_{m,k}^{data}[i] = \frac{\min\left\{\log_2\left(1+\Gamma_{BR_m,k}[i]\right), \log_2\left(1+\Gamma_{R_m,k}[i]\right)\right\}}{2},$$

$$\Gamma_{BR_m,k}[i] = \alpha_{BR_m,k}^*[i]P_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i],$$

$$\Gamma_{R_m,k}[i] = \frac{\alpha_{BR_m,k}^*[i]P_{R_m,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)}{1+(1-\alpha_{BR_m,k}^*)P_{R_m,k}[i]\sigma_e^2},$$

$$\Lambda_E[i] = (N_T-1)F_{z_c}^{-1}(\delta,i),$$

$$\alpha_{BR_m,k}^*[i] = \alpha_{R_m,k}^*[i] = \frac{1}{\sqrt{\Lambda_E[i]}}. \quad (22)$$

where $[x]^+ = \max\{0,x\}$, $F_{z_c}^{-1}(\cdot,i)$ denotes the inverse function of $F_{z_c}(z,i)$ which is defined in the Appendix in (46), and $F_{\chi_2}^{-1}(\cdot,i)$ denotes the inverse cumulative distribution function (cdf) of a non-central chi-square random variable with two degrees of freedom and non-centrality parameter $\hat{\mathbf{h}}_{R_m,k}[i]\hat{\mathbf{h}}_{R_m,k}^\dagger[i]$.

Proof: Please refer to the Appendix.

There are two important observations from the above lemma. First, the asymptotically optimal $\alpha_{BR_m,k}^*[i]$ and $\alpha_{R_m,k}^*[i]$ in (22) suggests that in high SNR, the optimal fraction of power devoted to the artificial noise only depends on the channel statistic of the eavesdropper channel and the secrecy outage probability requirement. Second, the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper, $\frac{\alpha_{R_m,k}^*[i]}{1-\alpha_{R_m,k}^*[i]}\Lambda_E[i]$, approaches a constant value at high SNR. More importantly, the SINR of the eavesdropper on each subcarrier is independent of the transmit power variables in both hops, which simplifies the derivation of the optimal resource allocation algorithm. This important observation will be verified in Section V via simulation.

By substituting (22) into (20), a modified objective function is obtained and the considered problem becomes an NP-hard mixed combinatorial and convex optimization problem, where the combinatorial nature comes from the binary constraints in the subcarrier assignment. Therefore, we follow the approach in [19] and relax constraint C6 in (21). In particular, we allow $s_{m,k}[i]$ to assume any real value between zero and one. Then, $s_{m,k}[i]$ can be interpreted as a time sharing factor for the K users for utilizing subcarrier i. For facilitating the time sharing on each subcarrier, we introduce two new variables and define them as $\tilde{P}_{BR_m,k}[i] = P_{BR_m,k}[i]s_{m,k}[i]$ and $\tilde{P}_{R_m,k}[i] = P_{R_m,k}[i]s_{m,k}[i]$. These two variables are the actual transmit power of the BS and relay m on subcarrier i for user k under the time-sharing assumption. Then, we can transform Problem 1 in (21) into its epigraph form [20]:

Problem 2 (Transformed Optimization Problem):

$$\max_{\mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i]} \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F} w_k z_{m,k}[i]$$

$$\text{s.t.} \quad \text{C5, C7,}$$

$$\text{C3:} \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{BR_m,k}[i] \le P_{B_T},$$

$$\text{C4:} \sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{R_m,k}[i] \le P_{R_T}, \quad \forall m,$$

$$\text{C6: } 0 \le s_{m,k}[i] \le 1, \quad \forall m,k,i,$$

$$\text{C9:} s_{m,k}[i]\widetilde{R}_{m,k}^{1st}[i] \ge z_{m,k}[i], \forall m,k,i,$$

$$\text{C10:} s_{m,k}[i]\widetilde{R}_{m,k}^{2nd}[i] \ge z_{m,k}[i], \forall m,k,i, \quad (23)$$

where

$$\widetilde{R}_{m,k}^{1st}[i] = \frac{1}{2}\Big[\log_2\left(1+\alpha_{BR_m,k}^*[i]\tilde{P}_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i]\right) - \log_2\left(1+\frac{\alpha_{BR_m,k}^*[i]\Lambda_E[i]}{1-\alpha_{BR_m,k}^*[i]}\right)\Big]^+ \text{and}$$

$$\widetilde{R}_{m,k}^{2nd}[i] = \frac{1}{2}\Big[\log_2\left(1+\frac{\alpha_{R_m,k}^*[i]\tilde{P}_{R_m,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)}{1+(1-\alpha_{R_m,k}^*)\tilde{P}_{R_m,k}[i]\sigma_e^2}\right) - \log_2\left(1+\frac{\alpha_{R_m,k}^*[i]\Lambda_E[i]}{1-\alpha_{R_m,k}^*[i]}\right)\Big]^+ \quad (24)$$

are the achievable secrecy data rate in the first and second hop, respectively. The extra constraints C9 and C10 represent the hypograph [20] of the original optimization problem in (21). Mathematically, the operators $[\cdot]^+$ in C9 and C10 in (23) destroy the concavity of the problem. Nevertheless, as will be seen in the Karush-Kuhn-Tucker (KKT) conditions in (34), those users with negative secrecy data rate will not be considered in the subcarrier selection process, since, secure communication cannot be guaranteed for those users. Therefore, we can remove the operators $[\cdot]^+$ from $\widetilde{R}_{m,k}^{1st}[i]$ and $\widetilde{R}_{m,k}^{2nd}[i]$ in (24), while preserving the concavity of the transformed problem. On the other hand, the constant term $\frac{1}{n_F}$ was removed from the transformed objective function for simplicity as it does not affect the values of the arguments which maximize the objective function. Besides, C8 was also removed from the optimization problem as the asymptotically optimal $\alpha_{R_m,k}^*[i]$ and $\alpha_{BR_m,k}^*[i]$ in (22) always satisfy the constraint. The extra constraints C9 and C10 represent the hypograph [20] of the original optimization problem in (21). Now, the transformed problem is jointly concave with respect to all optimization variables, and under some mild conditions [20], solving the dual problem is equivalent to solving the primal problem.

B. Dual Problem Formulation

In this subsection, we solve the resource allocation and scheduling optimization problem 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

$$\begin{aligned}
&\mathcal{L}(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\boldsymbol{\nu},\mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i])\\
&=\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}(w_k-(\mu_{m,k}[i]+\nu_{m,k}[i]))z_{m,k}[i]\\
&-\lambda\Big(\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{BR_m,k}[i]-P_{B_T}\Big)\\
&-\sum_{m=1}^{M}\gamma_m\Big(\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{R_m,k}[i]-P_{R_T}\Big)\\
&+\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}s_{m,k}[i]\Big(\mu_{m,k}[i]\widetilde{R}^{1st}_{m,k}[i]+\nu_{m,k}[i]\widetilde{R}^{2nd}_{m,k}[i]\Big)\\
&-\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\beta[i](s_{m,k}[i]-1),
\end{aligned}\tag{25}$$

where $\lambda\geq 0$ is the Lagrange multiplier corresponding to the power constraint at the BS. $\boldsymbol{\gamma}$ is the Lagrange multiplier vector corresponding to the individual relay power constraints with elements $\gamma_m\geq 0$, $m\in\{1,\ldots,M\}$. $\boldsymbol{\beta}$ is the Lagrange multiplier vector associated with the subcarrier usage constraints with elements $\beta[i]\geq 0$, $i\in\{1,\ldots,n_F\}$. $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ are the Lagrange multiplier vectors for constraints C9 and C10 in (23) with elements $\mu_{m,k}[i]$ and $\nu_{m,k}[i]$. The boundary constraints C6 and C7 will be absorbed into the KKT conditions when deriving the optimal solution in Section IV-C.

Thus, the dual problem is given by

$$\min_{\lambda,\ \boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\boldsymbol{\nu},\geq 0}\ \max_{\mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i]}\mathcal{L}(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\boldsymbol{\nu},\mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i]).\tag{26}$$

In general, the above dual problem can be unbounded if $z_{m,k}[i]\to\infty$. Consider the parts of the dual function in the inner maximization which are related to $z_{m,k}[i]$:

$$\begin{aligned}
&\max_{z_{m,k}[i]}\sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}(w_k-(\mu_{m,k}[i]+\nu_{m,k}[i]))z_{m,k}[i]\\
&=\begin{cases}0 & \text{if } \mu_{m,k}[i]+\nu_{m,k}[i]=w_k\\ \infty & \text{otherwise}\end{cases}.
\end{aligned}\tag{27}$$

In order to have a bounded dual function, the Lagrange multipliers $\mu_{m,k}[i]$ and $\nu_{m,k}[i]$ must satisfy $\mu_{m,k}[i]+\nu_{m,k}[i]=w_k$. Thus, the dual problem is simplified to

$$\min_{\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\geq 0}\ \max_{\mathcal{P},\mathcal{R},\mathcal{S}}\ \widetilde{\mathcal{L}}(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i]),\tag{28}$$

where $\widetilde{\mathcal{L}}(\lambda,\ \boldsymbol{\beta},\ \boldsymbol{\gamma},\ \boldsymbol{\mu},\ \mathcal{P},\mathcal{R},\mathcal{S})=\mathcal{L}(\lambda,\boldsymbol{\beta},\ \boldsymbol{\gamma},\ \boldsymbol{\mu},\ \boldsymbol{\nu},\ \mathcal{P},\mathcal{R},\mathcal{S},z_{m,k}[i])|_{\nu_{m,k}[i]=w_k-\mu_{m,k}[i]}$.
Note that the auxiliary variables $z_{m,k}[i]$ vanish when we set $\nu_{m,k}[i]=w_k-\mu_{m,k}[i]$.

C. Dual Decomposition and Sub-Problem Solution

By dual decomposition, the dual problem is decomposed into two parts (nested loops): the first part (inner loop) consists of $M\times n_F$ sub-problems with identical structure; the second part (outer loop) is the master dual problem. The dual problem can be solved iteratively where in each iteration each relay solves n_F local sub-problems (inner loop) by utilizing the local CSI and exchanges some information with the BS which solves the master problem (outer loop) with the gradient method.

The sub-problem to be solved by relay m is given by

$$\max_{\mathcal{P},\mathcal{R},\mathcal{S}}\quad\widetilde{\mathcal{L}}_m(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\mathcal{P},\mathcal{R},\mathcal{S})\tag{29}$$

for a fixed set of Lagrange multipliers where $\widetilde{\mathcal{L}}_m(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\mathcal{P},\mathcal{R},\mathcal{S})=$

$$\begin{aligned}
&\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}s_{m,k}[i]\Big(\mu_{m,k}[i]\widetilde{R}^{1st}_{m,k}[i]+\nu_{m,k}[i]\widetilde{R}^{2nd}_{m,k}[i]\Big)\\
&+\lambda P_{B_T}+\gamma_{m,k}[i]P_{R_T}-\gamma_m\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{R_m,k}[i]\\
&-\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\beta[i]\Big(s_{m,k}[i]-1\Big)-\lambda\Big(\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F}\tilde{P}_{BR_m,k}[i]\Big).
\end{aligned}\tag{30}$$

Note that the above sub-problem is the inner loop optimization in (28).

Using standard optimization techniques and the KKT conditions, the optimal power allocation for both hops for user k via relay m on subcarrier i are obtained as

$$P^*_{BR_m,k}[i]=\left[\frac{\mu_{m,k}[i]}{(2\ln(2))\lambda}-\frac{1}{\alpha^*_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i]}\right]^+,\tag{31}$$

$$\begin{aligned}
P^*_{R_m,k}[i]=\Bigg[&\frac{\sqrt{\Omega_{m,k}[i](\Omega_{m,k}[i]\gamma_m\ln(2)+2\Xi_{m,k}[i]\nu_{m,k}[i])}}{2\Xi_{m,k}[i]\sqrt{\gamma_m}\sqrt{\ln(2)}}\\
&-\frac{2(1-\alpha^*_{R_m,k}[i])\sigma_e^2+\Omega_{m,k}[i]}{2\Xi_{m,k}[i]}\Bigg]^+,
\end{aligned}\tag{32}$$

where $\Xi_{m,k}[i]=(1-\alpha^*_{R_m,k}[i])\sigma_e^2(\Omega_{m,k}[i]+\sigma_e^2(1-\alpha^*_{R_m,k}[i]))$ and $\Omega_{m,k}[i]=F^{-1}_{\chi^2}(\varepsilon,i)\alpha^*_{R_m,k}[i]$. The optimal power allocations in (31) and (32) have the form of *multi-level* water-filling. It can be observed that the dual variable $\mu_{m,k}[i]$ affects the power allocation by changing the water-level, $\frac{\mu_{m,k}[i]}{(2\ln(2))\lambda}$, of user k for satisfying constraint C9 in (23). On the other hand, the water level of each user in (32) depends not only on his/her priority via $\nu_{m,k}[i]$, but also on the CSIT error statistic of the desired channel and the required channel outage probability, i.e., $F^{-1}_{\chi^2}(\varepsilon,i)\alpha^*_{R_m,k}[i]$.

In order to obtain the optimal subcarrier allocation, we take the derivative of the sub-problem with respect to $s_{m,k}[i]$, which yields $\frac{\partial\widetilde{\mathcal{L}}_m(\lambda,\boldsymbol{\beta},\boldsymbol{\gamma},\boldsymbol{\mu},\mathcal{P},\mathcal{R},\mathcal{S})}{\partial s_{m,k}[i]}=A_{m,k}[i]-\beta[i]$, where $A_{m,k}[i]\geq 0$ is the marginal benefit [21] for allocating subcarrier i to user k via relay m and is given by $A_{m,k}[i]=$

$$\begin{aligned}
&\frac{\nu_{m,k}[i]}{2}\Bigg(\log_2\big(1+\Gamma^*_{R_m,k}[i]\big)-\frac{\Gamma^*_{R_m,k}[i]/\Big(\ln(2)(1+\Gamma^*_{R_m,k}[i])\Big)}{1+\sigma_e^2P^*_{R_m,k}[i](1-\alpha^*_{R_m,k}[i])}\\
&-\log_2\Big(1+\frac{\alpha^*_{R_m,k}[i]\Lambda_E[i]}{1-\alpha^*_{R_m,k}[i]}\Big)\Bigg)\\
&+\frac{\mu_{m,k}[i]}{2}\Bigg(\log_2\big(1+\Gamma^*_{BR_m,k}[i]\big)-\frac{\Gamma^*_{BR_m,k}[i]}{\ln(2)(1+\Gamma^*_{BR_m,k}[i])}\\
&-\log_2\Big(1+\frac{\alpha^*_{BR_m,k}[i]\Lambda_E[i]}{1-\alpha^*_{BR_m,k}[i]}\Big)\Bigg)
\end{aligned}\tag{33}$$

for $\alpha^*_{BR_m,k}[i] = \alpha^*_{R_m,k}[i]$, where $\Gamma^*_{BR_m,k}[i] = \Gamma_{BR_m,k}[i]\Big|_{P_{BR_m,k}[i]=P^*_{BR_m,k}[i]}$ and $\Gamma^*_{R_m,k}[i] = \Gamma_{R_m,k}[i]\Big|_{P_{R_m,k}[i]=P^*_{R_m,k}[i]}$. On the contrary, if a user has good channel conditions with positive secrecy data rate on subcarrier i, he/she can provide a higher marginal benefit to the system. Thus, the optimal subcarrier selection determined by relay m on subcarrier i is given by

$$s^*_{m,k}[i] = \begin{cases} 1 & \text{if } A_{m,k}[i] = \max\limits_{a,b} \quad A_{a,b}[i] \geq \beta[i] \geq 0 \\ 0 & \text{otherwise} \end{cases}. \quad (34)$$

The dual variable $\beta[i] \geq 0$ acts as the global price in using subcarrier i in the system. Only users who can provide large marginal benefits to the system are considered for selection by the resource allocator. $A_{m,k}[i] \geq 0$ has the physical meaning that users with negative secrecy data rate on subcarrier i are not selected as they can only provide a negative marginal benefit to the system. Note that each subcarrier will be used for serving only one user eventually. Finally, the optimal transmitted packet data rate $R^{*data}_{m,k}[i]$ and secrecy data rate $R^{*sec}_{m,k}[i]$ are obtained by substituting (31), (32) into the equivalent packet data rate and secrecy data rate in Lemma 1 for the subcarrier with $s^*_{m,k}[i] = 1$.

D. Solution of the Master Problem

For solving the master problem at the BS, each relay forwards the local resource allocation policies (i.e., $\mathcal{P}, \mathcal{R}$, and $\mathcal{S}$) to the BS. Since the dual function is differentiable, the gradient method can be used to solve the minimization of the master problem in (26). The solution is given by

$$\lambda(t+1) = \Big[\lambda(t) - \xi_1(t) \times (P_{B_T} - \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F} P_{BR_m,k}[i]s_{m,k}[i])\Big]^+, \quad (35)$$

$$\gamma_m(t+1) = \Big[\gamma_m(t) - \xi_2(t) \times (P_{R_T} - \sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F} P_{R_m,k}[i]s_{m,k}[i])\Big]^+, \forall m, \quad (36)$$

$$\mu_{m,k}[i](t+1) = \Big[\mu_{m,k}[i](t) - \xi_3(t) \times s_{m,k}[i](\widetilde{R}^{1st}_{m,k}[i] - \widetilde{R}^{2nd}_{m,k}[i])\Big]^+_{\mathbb{U}_{m,k}[i]}, \forall m,k,i, \quad (37)$$

$$\beta[i](t+1) = \Big[\beta[i](t) - \xi_4(t) \times (1 - \sum_{m=1}^{M}\sum_{k\in\mathcal{U}_m}\sum_{i=1}^{n_F} s_{m,k}[i])\Big]^+, \forall i, \quad (38)$$

where $t \geq 0$ is the iteration index and $\xi_a(t)$, $a \in \{1,2,3,4\}$, are positive step sizes. $\nu_{m,k}[i]$ can be obtained from $\nu_{m,k}[i] = [w_k - \mu_{m,k}[i]]^+$. $\mathbb{U}_{m,k}[i]$ in (37) denotes the projection operator on the feasible set $\mathbb{U}_{m,k}[i] = \{\mu_{m,k}[i] \Big| 0 \leq \mu_{m,k}[i] \leq w_k\}$. Since the transformed problem is convex in nature, it is guaranteed that the algorithm converges to the optimal solution if the chosen step sizes satisfy the general conditions stated in [22, Chapter 1.2]. In summary, the master problem adjusts the water-levels of (31) and (32) through the gradient update equations (35) and (36) until the individual power constraints of the BS and the relays are satisfied, respectively. Finally, (37) reduces the difference between the capacity of user k in the first and second hops, which corresponds to the selection of the minimum capacity in (15). We note that there is no intra-cell/inter-sector interference in the considered system since the resource allocation algorithm is applied to the entire cell and all users in all sectors are competing for resources. By combining (34) and (38), it can be shown that, for the optimal solution, there is no time-sharing between the assigned subcarriers. The overall distributed algorithm is illustrated in Figure 3.

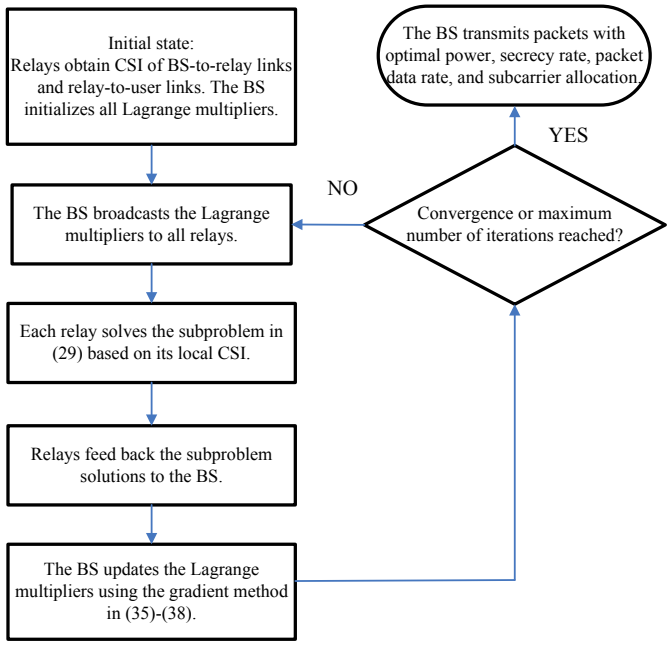

Fig. 3. A flow chart of the proposed iterative distributed resource allocation and scheduling algorithm.

V. Results

In this section, we evaluate the system performance using simulations. A cell is modeled as two concentric ring-shaped discs where the outer boundary has a radius of 1 km and the inner boundary a radius of 0.5 km, cf. Figure 1. The number of subcarriers is $n_F = 128$ with carrier center frequency 2.5 GHz, bandwidth $\mathcal{B} = 5$ MHz, and $w_k = 1, \forall k$. Each subcarrier has a bandwidth of 39 kHz and a noise variance of $N_0 = -128$ dBm. The 3GPP path loss model is used [23] with a reference distance of $d_0 = 35$ m. There are $M = 3$ relay stations in the cell which are equally distributed at the inner cell boundary for assisting the transmission. The K desired users are uniformly distributed between 0.5 km 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. On the other hand, a strong line of sight communication channel

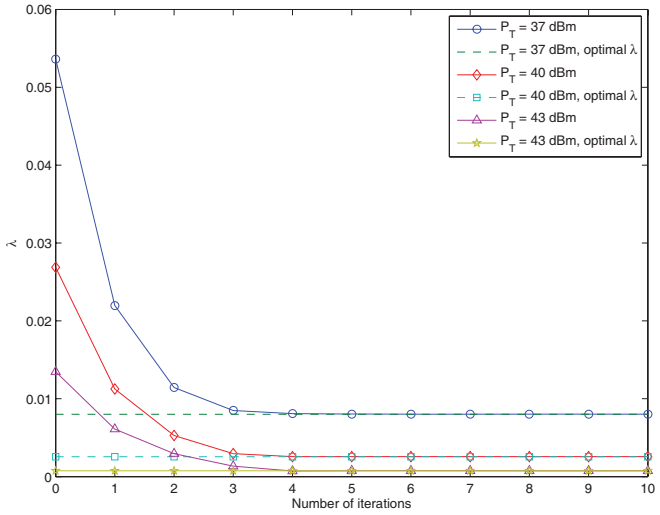

Fig. 4. Lagrange multiplier λ versus number of iterations with $K = 15$ users and $M = 3$ relays for different transmit power levels. The BS and each relay are equipped with $N_T = 9$ antennas. There are $N_E = 2$ receive antennas at the eavesdropper.

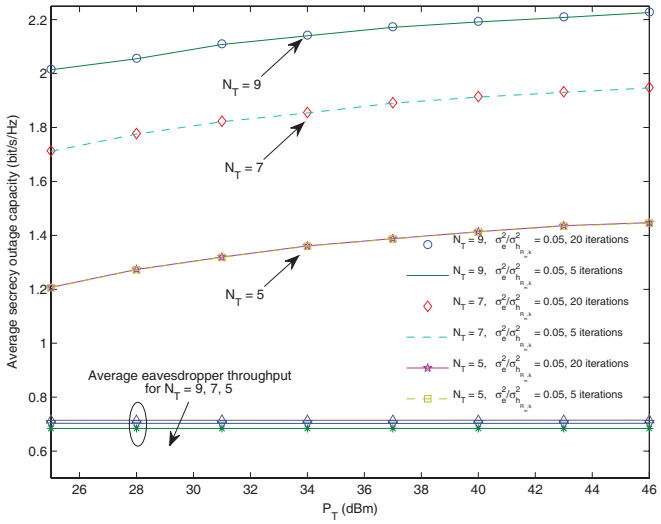

Fig. 5. Average secrecy outage capacity versus transmit power for different numbers of transmit antennas N_T. The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m from the BS.

between the BS and the relays is expected since they are placed in relatively high positions in practice and the number of blockages between them is limited. Hence, the small scale fading coefficients of the BS-to-relay links are modelled as i.i.d. Rician random variables with Rician factor $\kappa = 6$ dB. The channel estimation error-to-signal ratio (ESR) is set to $\frac{\sigma_e^2}{\sigma_{h_{R_m,k}}^2} = 0.05$, unless further specified. The target secrecy outage probability and channel outage probability are set to $\delta = 0.05$ and $\varepsilon = 0.05$, respectively, unless further specified. We assume that the maximum transmit power at each transmission device is P_T, i.e., the BS and the relay have a maximum transmit power of $P_{R_T} = P_{B_T} = P_T$. 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.

A. Convergence of Distributed Iterative Algorithm

Figure 4 illustrates the evolution of the Lagrange multiplier λ of the distributed iterative algorithm over time for different maximum transmit powers P_T with $K = 15$ users and $M = 3$ relays. Both the BS and each relay have $N_T = 9$ transmit antennas, while the eavesdropper has $N_E = 2$ receive antennas. Positive constant step sizes $\xi_1(t), \xi_2(t), \xi_3(t)$, and $\xi_4(t)$, which were optimized for fast convergence, were adopted in (35)-(38). The result in Figure 4 was averaged over 10000 independent adaptation processes. For the considered transmit power values, it can be observed that the distributed iterative algorithm converges fast and typically achieves at least 95% of the optimal value within 5 iterations.

B. Average Secrecy Outage Capacity versus Transmit Power and ESR

Figure 5 illustrates the average secrecy outage capacity and the throughput of the eavesdropper versus the total transmit power for $K = 15$ users for different numbers of transmit antennas N_T at both the BS and the relays. The eavesdropper is equipped with $N_E = 2$ antennas. The number of iterations for the proposed iterative resource allocation algorithm is 5 and 20. It can be seen that the performance difference between 5 iterations and 20 iterations is negligible which confirms the practicality of our proposed iterative resource allocation algorithm. On the other hand, for a better illustration of the effectiveness of the artificial noise generation, Figure 5 also includes the performance of the eavesdropper in terms of average throughput. As observed in Lemma 1, the average throughput between the BS and the eavesdropper does not scale with the transmit power in the high transmit power regime due to the artificial noise introduced by the BS, despite the fact that the eavesdropper is located closer to the BS than all the desired users. On the other hand, it can be observed that although the imperfect CSI has a negative impact on the average secrecy outage capacity due to the artificial noise leakage, the system performance scales with the transmit power thanks to the proposed optimization technique. Besides, it can be observed that an increasing number of transmit antennas N_T benefits the desired users in terms of average secrecy outage capacity. Yet, there is a diminishing return when N_T is large due to the *channel hardening* effect [17] in the desired channels. On the contrary, the throughput of the eavesdropper is limited by artificial noise and the performance gain achieved at the eavesdropper due to increasing N_T is marginal.

Figure 6 illustrates the average secrecy outage capacity versus ESR $\frac{\sigma_e^2}{\sigma_{h_{R_m,k}}^2}$ for $K = 15$ users with different numbers of receive antennas at the eavesdropper and different numbers of transmit antennas at the BS and relays. The number of iterations is set to 5. It can be observed that as the estimation error increases, the system performance decreases since the CSI available for resource allocation becomes less accurate, and the resource allocation has to be more conservative in order to satisfy the outage requirements of the selected users. Besides, when N_T is not significantly larger than N_E, the average

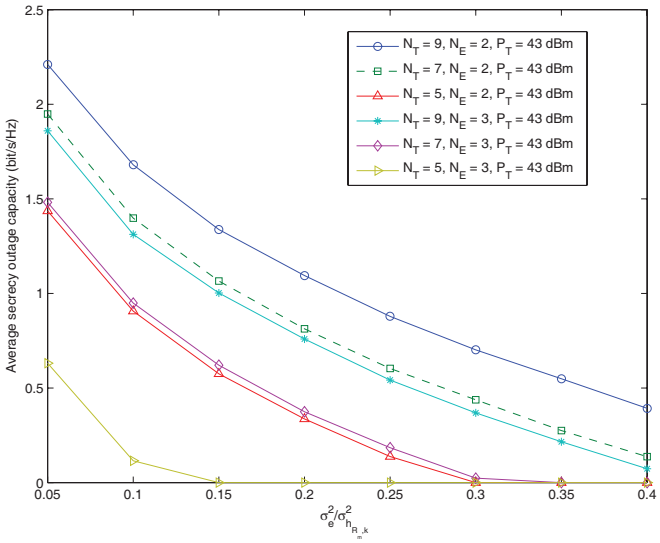

Fig. 6. Average secrecy outage capacity versus ESR $\frac{\sigma_e^2}{\sigma^2_{h_{R_m,k}}}$ for different numbers of transmit antennas N_T and eavesdropper antennas N_E.

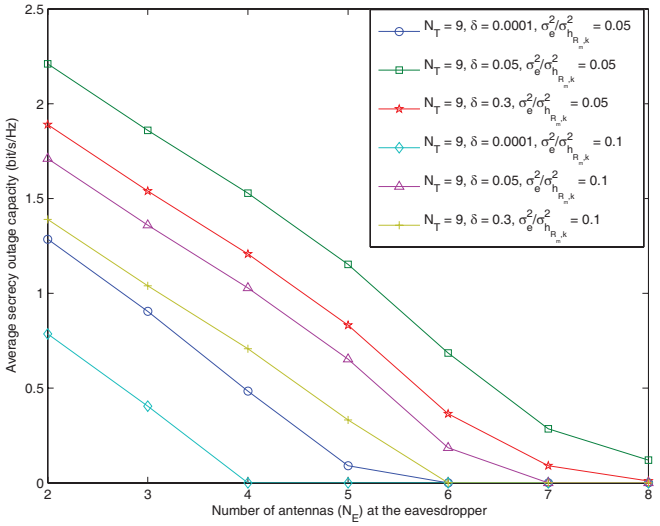

Fig. 7. Average secrecy outage capacity versus the number of antennas N_E employed at the eavesdropper for different ESR $\frac{\sigma_e^2}{\sigma^2_{h_{R_m,k}}}$ and different secrecy outage requirements δ. $N_T = 9$ antennas at the BS and relays.

secrecy outage capacity is comparatively small for moderate ESRs values. This is because the resource allocator shuts down some subcarriers if the channel conditions of all the users are not good enough to guarantee secure communication, which results in a low average system performance. On the other hand, Figure 6 suggests that if the number of transmit antennas N_T is large enough compared to the number of eavesdropper receive antennas N_E, e.g, $N_T = 9$ and $N_E = 2$, the proposed resource allocation scheme is able to guarantee an average secrecy outage capacity of 0.5 bit/s/Hz (corresponding to 2.5 Mbps for a 5 MHz bandwidth) even in high ESR (e.g. $\frac{\sigma_e^2}{\sigma^2_{h_{R_m,k}}} = 0.35$, estimation error of 35%), while satisfying both the channel outage and secrecy outage requirements.

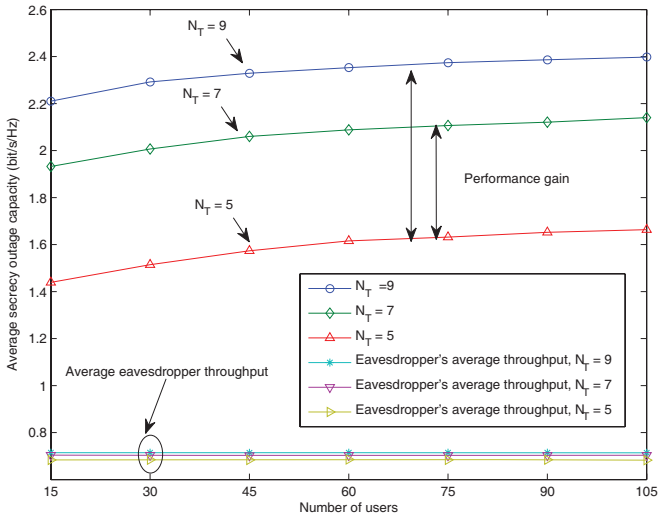

Fig. 8. Average secrecy outage capacity versus the number of desired users for different numbers of transmit antennas N_T at the BS with a total transmit power $P_T = 43$ dBm. The eavesdropper is equipped with $N_E = 2$ antennas and is located 35 m away from the BS. The double arrows indicate the performance gain achieved by an increasing number of transmit antennas N_T.

C. Average Secrecy Outage Capacity versus N_E

Figure 7 depicts the average secrecy outage capacity versus the number of receive antennas N_E employed at the eavesdropper for different secrecy outage requirements and ESRs. There are $K = 15$ users and $N_T = 9$ transmit antennas at the BS and the relays. The number of iterations for the iterative algorithm is 5. It can be observed that the secrecy outage capacity decreases as N_E increases, since more of the transmitted power has to be devoted to the artificial noise generation for degrading the channels of the eavesdropper, which results in less transmit power for information transmission. On the other hand, we observe that a more stringent secrecy outage probability requirement does not necessarily lead to a higher average secrecy outage capacity. This is because a larger fraction of power has to be allocated to the artificial noise for degrading the channel of the eavesdropper and less power is available for information transmission. Yet, a less stringent secrecy outage probability requirement may also lead to an unsatisfactory system performance since the eavesdropper has a higher chance in decoding the desired information. As observed in Figure 7, there exists an optimal secrecy outage requirement δ for each ESR value, which maximizes the overall system performance. However, optimizing the value of δ in the physical layer may require further information from the application layer (e.g., tolerable information leakage of a particular data type such as video or email), which is beyond the scope of this paper.

D. Average Secrecy Outage Capacity versus Number of Users

Figure 8 depicts the average secrecy outage capacity versus the number of users for different numbers of transmit antennas for $P_T = 43$ dBm. The number of iterations is 5. It can be observed that the average secrecy outage capacity grows with the number of users since the proposed resource allocation and scheduling algorithm is able to exploit multi-user diversity

(MUD), despite the existence of the eavesdropper. However, for large N_T, the system performance scales 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*, they decrease the potentially achievable MUD gain in the subcarrier allocation process. On the other hand, the performance of the eavesdropper does not scale with the number of users since the channels between the eavesdropper and the desired users are generally uncorrelated.

Remark 2: Simulation results for when the eavesdropper is located close to a relay are not shown since the resulting system performance is close to that of the considered case where the eavesdropper is located close to the BS. This is because when the capacity upper bound of the eavesdropper in (16) is adopted for resource allocation, a large amount of artificial noise is generated to combat the eavesdropper which saturates the throughput of the eavesdropper, cf. Figure 5.

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, where a multiple antenna eavesdropper, artificial noise generation for secure communication, and the negative effect of imperfect CSIT were taken into consideration. By relaxing the combinatorial subcarrier allocation constraints, the considered problem was transformed into a convex problem. An efficient iterative and distributed resource allocation algorithm with closed-form power, secrecy data rate, packet data rate, and subcarrier allocation requiring only local CSI at each relay was derived by dual decomposition. Simulation results not only showed that the performance of the proposed algorithm converges to the optimal performance within a small number of iterations, but also demonstrated the achievable secrecy outage capacity when the eavesdropper is closer to the BS/relay than the desired users.

Interesting topics for future work include studying the impact of finite queue sizes at the relays and end-to-end flow control.

Appendix: Proof of Lemma 1

The proof of the Lemma 1 involves three steps. We first derive the channel outage data rate between the BS and user k via relay m on subcarrier i by considering the channel outage probability requirement C1 in (21), i.e.,

$$\Pr\left[R_{m,k}^{data}[i] > \frac{1}{2}\min\left\{C_{BR_m,k}[i], C_{R_m,k}[i]\right\}\middle|\boldsymbol{\Delta}_{m,k}[i]\right] = \varepsilon. \tag{39}$$

Note that $C_{R_m,k}[i]$ is the only random variable in (39) and both $R_{m,k}^{data}[i]$ and $C_{BR_m,k}[i]$ can be controlled via power and packet data rate adaptations. In other words, $R_{m,k}^{data}[i] \leq \frac{1}{2}C_{BR_m,k}[i]$ is guaranteed. Therefore, the left hand side of (39) can be written as

$$\Pr\left[R_{m,k}^{data}[i] > \frac{1}{2}C_{R_m,k}[i]\middle|\boldsymbol{\Delta}_{m,k}[i], C_{BR_m,k}[i] > C_{R_m,k}[i]\right] \times \Pr\left[C_{BR_m,k}[i] > C_{R_m,k}[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right]. \tag{40}$$

On the other hand, it can be observed that the outage capacity $R_{m,k}^{data}[i](1-\varepsilon)$ is linearly increasing with $R_{m,k}^{data}[i]$ for a fixed target outage requirement ε and is upper bounded by $\frac{1}{2}C_{BR_m,k}[i]$. Therefore, the outage capacity is maximized if we control $\frac{1}{2}C_{BR_m,k}[i]$ such that it is equal to $R_{m,k}^{data}[i]$. Therefore, (40) can be further simplified as

$$\begin{aligned}
&\Pr\left[C_{BR_m,k}[i] > C_{R_m,k}[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\
&= \Pr\left[\frac{(2^{2R_{m,k}^{data}[i]}-1)(1+(1-\alpha_{R_m,k}[i])P_{R_m,k}[i]\sigma_e^2)}{\alpha_{R_m,k}[i]P_{R_m,k}[i]}\right. \\
&\quad \left.> \hat{\mathbf{r}}_{m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}^{\dagger}[i]\mathbf{h}_{R_m,k}[i]\hat{\mathbf{r}}_{R_m,k}[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\
&= F_{\chi_2}\Big(\frac{(2^{2R_{m,k}^{data}[i]}-1)(1+(1-\alpha_{R_m,k}[i])P_{R_m,k}[i]\sigma_e^2)}{\alpha_{R_m,k}[i]P_{R_m,k}[i]}, i\Big) \\
&= \varepsilon \\
&\Rightarrow R_{m,k}^{data}[i] = \min\Big\{\frac{1}{2}\log_2\Big(1+\frac{\alpha_{R_m,k}[i]P_{R_m,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)}{1+(1-\alpha_{R_m,k})P_{R_m,k}[i]\sigma_e^2}\Big), \\
&\qquad \frac{1}{2}C_{BR_m,k}[i]\Big\},
\end{aligned} \tag{41}$$

where $F_{\chi_2}(\cdot,i)$ denotes the cdf of a non-central chi-square random variable with 2 degrees of freedom and non-centrality parameter $\hat{\mathbf{h}}_{R_m,k}[i]\hat{\mathbf{h}}_{R_m,k}^{\dagger}[i]$ [24]. Then, we can derive the outage secrecy data rate by calculating the secrecy outage probability in C2. Without loss of generality, we define the secrecy data rate and outage data rate as $R_{m,k}^{sec}[i] = \frac{1}{2}\log_2(r_{m,k}^{sec}[i])$ and $R_{m,k}^{data}[i] = \frac{1}{2}\log_2(r_{m,k}^{data}[i])$, respectively. We assume that $\alpha_{R_m,k}[i] = \max\{\alpha_{R_m,k}[i], \alpha_{BR_m,k}[i]\}$. This assumption is necessary for deriving an efficient resource allocation algorithm. It results in an upper bound on the secrecy outage capacity and a lower bound on the secrecy data rate. Then, the secrecy outage probability can be expressed as

$$\begin{aligned}
&\Pr\left[R_{m,k}^{data}[i] - C_{m,E}[i] \leq R_{m,k}^{sec}[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\
&= \Pr\left[(\frac{r_{m,k}^{data}[i]}{r_{m,k}^{sec}[i]}-1)\frac{1}{(N_T-1)}\right. \\
&\quad \left.\leq \max\Big\{\frac{\alpha_{BR_m,k}[i]}{1-\alpha_{BR_m,k}[i]}\Omega_1[i], \frac{\alpha_{R_m,k}[i]}{1-\alpha_{R_m,k}[i]}\Omega_2[i]\Big\}\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\
&\leq \Pr\left[(\frac{r_{m,k}^{data}[i]}{r_{m,k}^{sec}[i]}-1)\frac{1-\alpha_{R_m,k}[i]}{\alpha_{R_m,k}[i](N_T-1)}\right. \\
&\quad \left.\leq \max\Big\{\Omega_1[i], \Omega_2[i]\Big\}\middle|\boldsymbol{\Delta}_{m,k}[i]\right],
\end{aligned} \tag{42}$$

where $\Omega_1[i] = \mathbf{g}_1^{\dagger}[i](\mathbf{G}_1[i]\mathbf{G}_1^{\dagger}[i])^{-1}\mathbf{g}_1[i]$ and $\Omega_2[i] = \mathbf{g}_2^{\dagger}[i](\mathbf{G}_2[i]\mathbf{G}_2^{\dagger}[i])^{-1}\mathbf{g}_2[i]$. Note that the upper bound on the secrecy outage probability in (42) is due to the assumption of $\alpha_{R_m,k}[i] = \max\{\alpha_{R_m,k}[i], \alpha_{BR_m,k}[i]\}$. If $\alpha_{BR_m,k}[i] = \max\{\alpha_{R_m,k}[i], \alpha_{BR_m,k}[i]\}$, the inequality is also valid by replacing $\alpha_{R_m,k}[i]$ by $\alpha_{BR_m,k}[i]$ in (42). On the other hand, since $\Omega_1[i]$ and $\Omega_2[i]$ are i.i.d. random variables, we have the following equality

$$\Pr\left[z \leq \Omega_1[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] = \Pr\left[z \leq \Omega_2[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right], \tag{43}$$

where $z = \frac{(r_{m,k}^{data}[i]-r_{m,k}^{sec}[i])(1-\alpha_{R_m,k}[i])}{r_{m,k}^{sec}[i]\alpha_{R_m,k}[i](N_T-1)}$. Hence, the secrecy outage probability in (42) can be written as

$$\begin{aligned} F_{z_c}(z,i) &= \Pr\left[z \le \max\left\{\Omega_1[i],\Omega_2[i]\right\}\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\ &= \Pr\left[z \le \Omega_1[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] + \Pr\left[z \le \Omega_2[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \\ &\quad - \Pr\left[z \le \Omega_1[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] \times \Pr\left[z \le \Omega_2[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right]. \end{aligned} \tag{44}$$

On the other hand, it can be observed that $\Omega_1[i]$ is equivalent to the signal-to-interference ratio (SIR) of an N_E-branch MMSE diversity combiner for N_T-1 interferers. The corresponding complementary cumulative distribution function (ccdf) is given by [13], [25]

$$\Pr\left[z \le \Omega_1[i]\middle|\boldsymbol{\Delta}_{m,k}[i]\right] = F_\Omega(z) = \frac{\sum_{n=0}^{N_E-1}\binom{N_T-1}{n}z^n}{(1+z)^{N_T-1}}. \tag{45}$$

Therefore, the target secrecy outage probability $F_{z_c}(z,i)$ can be obtained by substituting (45) into (44), which yields

$$\begin{aligned} &F_{z_c}(z,i) = F_\Omega(z) + F_\Omega(z) - F_\Omega(z)\times F_\Omega(z) \\ &= \frac{\sum_{n=0}^{N_E-1}\binom{N_T-1}{n}2z^n}{(1+z)^{N_T-1}} \\ &\quad - \frac{\sum_{n=0}^{N_E-1}\sum_{m=0}^{N_E-1}\binom{N_T-1}{n}\binom{N_T-1}{m}z^{m+n}}{(1+z)^{2N_T-2}}. \end{aligned} \tag{46}$$

For a target secrecy outage probability of δ, z can be expressed as

$$\begin{aligned} &z = F_{z_c}^{-1}(\delta,i) \Longrightarrow R_{m,k}^{sec}[i] = \\ &\left[R_{m,k}^{data}[i] - \frac{1}{2}\log_2\left(1+\frac{\alpha_{R_m,k}[i](N_T-1)F_{z_c}^{-1}(\delta,i)}{1-\alpha_{R_m,k}[i]}\right)\right]^+, \end{aligned} \tag{47}$$

where $F_{z_c}^{-1}(\delta,i)$ is the inverse ccdf of random variable $\max\left\{\Omega_1[i],\Omega_2[i]\right\}$, which can be computed efficiently by numerical solvers or implemented as a look-up table in practice. The final step in deriving the lemma is to calculate the asymptotically optimal $\alpha_{R_m,k}^*[i]$ and $\alpha_{BR_m,k}^*[i]$ in high SNR. Let $\Phi_{BR_m,k}[i] = P_{BR_m,k}[i]\lambda_{\max_{BR_m}}[i]$, $\Phi_{R_m,k}[i] = F_{\chi_2}^{-1}(\varepsilon,i)/\sigma_e^2$, and $\Lambda_E[i] = (N_T-1)F_{z_c}^{-1}(\delta,i)$. The expression for the secrecy data rate of user k on subcarrier i depends on the link qualities of the BS-to-relay link and the relay-to-user link, cf. (42), (47). If the BS-to-relay link is weaker than the relay-to-user link, then the secrecy data rate can be expressed as

$$\begin{aligned} R_k^{sec}[i] &= \frac{1}{2}C_{BR_m,k}[i] \\ &- \frac{1}{2}\log_2\left(1+\frac{\alpha_{BR_m,k}[i]F_{z_c}^{-1}(\delta,i)(N_T-1)}{1-\alpha_{BR_m,k}[i]}\right). \end{aligned} \tag{48}$$

On the other hand, if the relay-to-user link is weaker than the BS-to-relay link, the secrecy data rate of user k on subcarrier i in high SNR is lower bounded by

$$\begin{aligned} R_k^{sec}[i] > \frac{1}{2}\Bigg\{ &\log_2\left(1+\frac{P_{R_m,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}^*[i]}{1+P_{R_m,k}[i]\sigma_e^2}\right) \\ - &\log_2\left(1+\frac{\alpha_{R_m,k}[i]F_{z_c}^{-1}(\delta,i)(N_T-1)}{1-\alpha_{R_m,k}[i]}\right)\Bigg\}. \end{aligned} \tag{49}$$

In fact, the term $\frac{P_{R_m,k}[i]F_{\chi_2}^{-1}(\varepsilon,i)\alpha_{B,k}^*[i]}{P_{R_m,k}[i]\sigma_e^2}$ in (49) can be interpreted as an signal-to-interference-plus-noise ratio (SINR) under a virtual interferer with interference power $P_{R_m,k}[i]\sigma_e^2$. By standard optimization techniques, it can be shown that the optimal $\alpha_{BR_m,k}^*[i]$ and $\alpha_{R_m,k}^*[i]$ maximizing (48) and (49) have the same asymptotic expression in high SNR ($P_{BR_m,k}[i], P_{R_m,k} \to \infty$):

$$\begin{aligned} &\alpha_{BR_m,k}^*[i] \\ &= \frac{-\Phi_{BR_m,k}[i] + \sqrt{\Phi_{BR_m,k}[i]\Lambda_E[i](\Phi_{BR_m,k}[i]-\Lambda_E[i]+1)}}{\Phi_{BR_m,k}[i](\Lambda_E[i]-1)} \\ &\overset{(a)}{\approx} \frac{1}{\sqrt{\Lambda_E[i]}} \quad \text{and} \\ &\alpha_{R_m,k}^*[i] \\ &= \frac{-\Phi_{R_m,k}[i] + \sqrt{\Phi_{R_m,k}[i]\Lambda_E[i](\Phi_{R_m,k}[i]-\Lambda_E[i]+1)}}{\Phi_{R_m,k}[i](\Lambda_E[i]-1)} \\ &\overset{(b)}{\approx} \frac{1}{\sqrt{\Lambda_E[i]}}, \end{aligned} \tag{50}$$

respectively. (a) is due to the high SNR assumption, i.e., $\Phi_{BR_m,k}[i] \gg \Lambda_E[i] \gg 1$. The assumption of high SNR is necessary for arriving at an efficient resource allocation algorithm. Note that $\Phi_{BR_m,k}[i] \gg \Lambda_E[i]$ is always valid in the high transmit power regime as $\Phi_{BR_m,k}[i]$ increases with the total transmit power while $\Lambda_E[i]$ remains constant. On the other hand, (b) is due to $\Phi_{R_m,k}[i] \gg \Lambda_E[i] \gg 1$, which holds for reasonably small channel estimation error variance σ_e^2 (e.g. $\sigma_e^2 \ll \sigma_{h_{R_m,k}}^2$) and secrecy outage requirement δ (e.g. $\delta \ll 1$).

REFERENCES

[1] G. Song and Y. Li, "Utility-based resource allocation and scheduling in OFDM-based wireless broadband networks," *IEEE Commun. Mag.*, vol. 43, pp. 127–134, Dec. 2005.

[2] G. Song, Y. Li, and L. J. Cimini, "Joint channel-and queue-aware scheduling for multiuser diversity in wireless OFDMA networks," *IEEE Trans. Commun.*, vol. 57, pp. 2109–2121, July 2009.

[3] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[4] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3037–3063, Apr. 2005.

[5] I. Hammerstrom and A. Wittneben, "Power allocation schemes for amplify-and-forward MIMO-OFDM relay links," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 2798–2802, Aug. 2007.

[6] A. D. Wyner, "The wire-tap channel," Tech. Rep., Oct. 1975.

[7] 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.

[8] 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.

[9] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in OFDMA networks," in *Proc. IEEE Intern. Commun. Conf.*, June 2011, pp. 1–5.

[10] 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.

[11] 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.

[12] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2180–2189, June 2008.

[13] 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, pp. 3831–3842, July 2010.

[14] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*, 1st edition. Springer, 2009.

[15] D. W. K. Ng and R. Schober, "Resource allocation for secure OFDMA communication systems," in *Proc. 2011 Australia Communications Theory Workshop*, Feb. 2011, pp. 13–18.
[16] ——, "Resource allocation for secure OFDMA decode-and-forward relaying network," in *Proc. 2011 Canadian Workshop on Information Theory*, May 2011, pp. 202–205.
[17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*, 1st edition. Cambridge University Press, 2005.
[18] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 3rd edition. McGraw-Hill, 1991.
[19] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch, "Multiuser OFDM with adaptive subcarrier, bit, and power allocation," *IEEE J. Sel. Areas Commun.*, vol. 17, pp. 1747–1758, Oct. 1999.
[20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[21] W. Yu and J. M. Cioffi, "FDMA capacity of Gaussian multiple-access channels with ISI," *IEEE Trans. Commun.*, vol. 50, pp. 102–111, Jan. 2002.
[22] D. P. Bertsekas, *Nonlinear Programming*, 2nd edition. Athena Scientific, 1999.
[23] "Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations," 3GPP TR 25.996 V7.0.0 (2007-06), Tech. Rep.
[24] V. Annapureddy, D. Marathe, T. Ramya, and S. Bhashyam, "Outage probability of multiple-input single-output (MISO) systems with delayed feedback," *IEEE Trans. Commun.*, vol. 57, pp. 319–326, Feb. 2009.
[25] 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, pp. 666–672, May 1998.

Derrick Wing Kwan Ng (S'06) received the bachelor degree with First class honors and Master of Philosophy (M.Phil.) degree in electronic engineering from the Hong Kong University of Science and Technology (HKUST) in 2006 and 2008, respectively. He is currently working toward the Ph.D. degree in the University of British Columbia (UBC). In the summer of 2011, he was a visiting scholar at the Centre Tecnològic de Telecomunicacions de Catalunya - Hong Kong Branch (CTTC-HK). His research interests include cross-layer optimization for wireless communication systems, resource allocation in OFDMA wireless system, and communication theory. He received the Best Paper Award at the IEEE Third International Conference on Communications and Networking in China 2008. He was awarded the IEEE Student Travel Grants for attending the IEEE WCNC 2010 and the IEEE ICC 2011. He was also the recipient of the 2009 Four Year Doctoral Fellowship from the UBC, Sumida & Ichiro Yawata Foundation Scholarship in 2008, and R&D Excellence scholarship from the Center for Wireless Information Technology in the HKUST in 2006.

Ernest S. Lo (S'02-M'08) is the Chief Representative of the Centre Tecnològic de Telecomunicacions de Catalunya - Hong Kong Branch (CTTC-HK). Prior to this, he was a Croucher Postdoctoral Fellow at Stanford University. He received his Ph.D., M.Phil. and B.Eng. (1st Hons.) from the Hong Kong University of Science and Technology and his previous works involved resource allocation, channel coding and wireless system-level design. His current research is focused on investigating new resources and design opportunities for wireless and wireline multiuser communications networks.

Dr. Lo was the Best Paper Award recipient at the IEEE ICC'07, Glasgow, and the award winner of the Croucher Fellowships in 2008. He contributed to the standardization of the IEEE 802.22 cognitive radio WRAN system and holds several pending and granted US and China patents with some of them successfully transferred to companies. He served as an Editorial Assistant of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS when it was founded and has been a TPC member of various conferences, including the IEEE PIMRC'09, IEEE ICC'10, IEEE GLOBECOM'10, IEEE ICC'11, IEEE GLOBECOM'11, ICNC'12 and IEEE ICC'12. He has also been honored as an Exemplary Reviewer of IEEE COMMUNICATIONS LETTERS.

Robert Schober (M'01, SM'08, F'10) was born in Neuendettelsau, Germany, in 1971. He received the Diplom (Univ.) and the Ph.D. degrees in electrical engineering from the University of Erlangen-Nuermberg in 1997 and 2000, respectively. From May 2001 to April 2002 he was a Postdoctoral Fellow at the University of Toronto, Canada, sponsored by the German Academic Exchange Service (DAAD). Since May 2002 he has been with the University of British Columbia (UBC), Vancouver, Canada, where he is now a Full Professor and Canada Research Chair (Tier II) in Wireless Communications. His research interests fall into the broad areas of Communication Theory, Wireless Communications, and Statistical Signal Processing.

Dr. Schober received the 2002 Heinz Maier-Leibnitz Award of the German Science Foundation (DFG), 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, and the 2008 Charles McDowell Award for Excellence in Research from UBC. In addition, he received best paper awards from the German Information Technology Society (ITG), the European Association for Signal, Speech and Image Processing (EURASIP), IEEE ICUWB 2006, the International Zurich Seminar on Broadband Communications, and European Wireless 2000. Dr. Schober is also the Area Editor for Modulation and Signal Design for the IEEE TRANSACTIONS ON COMMUNICATIONS.