Utility Regions for DF Relay in OFDMA-Based Secure Communication with Untrusted Users

Ravikant Saini, Deepak Mishra and Swades De

Utility Regions for DF Relay in OFDMA-based Secure Communication with Untrusted Users

Ravikant Saini, *Member, IEEE*, Deepak Mishra, *Student Member, IEEE*, and Swades De, *Senior Member, IEEE*

***Abstract*—This paper investigates the utility of a trusted decode-and-forward relay in OFDMA-based secure communication system with untrusted users. For deciding whether to use the relay or not, we first present optimal subcarrier allocation policies for direct communication (DC) and relayed communication (RC). Next we identify exclusive RC mode, exclusive DC mode, and mixed (RDC) mode subcarriers which can support both the modes. For RDC mode we present optimal mode selection policy and a suboptimal strategy independent of power allocation which is asymptotically optimal at both low and high SNRs. Finally, via numerical results we present insights on relay utility regions.**

***Index Terms*—Physical layer security, DF relay, maximum ratio combining, secure OFDMA, subcarrier allocation, mode selection**

I. Introduction

With growing number of users, utilization of friendly relays for providing secure communication to cell-edge users is becoming very popular [1]. Also due to its relative difficulty as compared to source based broadcast, because of the possibility of information interception in both the hops, significant research attention is being paid in this regard recently [2].

The authors in [3] proposed several cooperation strategies for secrecy enhancement in single carrier communication systems. While considering four single antenna half duplex nodes, [4] investigated the role to be played by the relay to maximize ergodic secrecy rate. For a similar setting, [5] considered the outage constrained secrecy throughput maximization problem.

In an amplify and forward (AF) relay assisted system without availability of direct source-destination link, a time division based protocol was proposed in [6] using one of the users as the helper node for secure communication to untrusted users. In another related work [7], time division based relay and user selection scheme was studied to improve secrecy of a cooperative AF relay network, assuming availability of direct link. With multi-antenna nodes, [8] investigated multiuser resource allocation for decode and forward (DF) relay assisted system without direct link, in the presence of single eavesdropper. The authors in [9] considered resource allocation problem for a DF relay assisted orthogonal frequency division multiple access (OFDMA) system with multiple untrusted users.

Assuming the availability of direct link, the optimal power allocation and transmission mode selection for DF relay-assisted secure communication was considered in [10]. Observing that *strategies for a single source-destination pair with joint transmit power budget for source and relay cannot be extended for an untrusted users' model with individual power budgets*, we intend to investigate whether utilizing a relay is always useful in multiuser secure OFDMA system.

The key contributions of this letter are four fold. *Firstly*, we present a generalized secure rate definition for DF relay assisted secure OFDMA system with the availability of direct link, while considering the possibility of tapping in both the hops. *Secondly*, observing that each subcarrier can be utilized in direct communication (DC) mode, we identify the conditions for using a subcarrier in relayed communication (RC) mode, and obtain optimal subcarrier allocation policies for both modes. *Thirdly*, noting that a set of subcarriers can be used in both the modes, we find optimal mode selection strategy resulting in higher secure rate over such subcarriers. *Finally*, asymptotically optimal and suboptimal mode selection schemes, that are independent of power allocation, are derived. *To the best of our knowledge, it is the first work studying utility of a DF relay in secure OFDMA system with untrusted users.*

II. System model

Downlink of a trusted DF relay $\mathcal{R}$ assisted secure OFDMA system, with source $\mathcal{S}$, and M untrusted users is considered. Untrusted users is a hostile scenario, where each user behaves as a potential eavesdropper for others. For each $\mathcal{U}_m$ there are effectively $M-1$ eavesdroppers, and the one having maximum signal-to-noise ratio (SNR) is called *equivalent eavesdropper*. Apart from the direct $(\mathcal{S}-\mathcal{U}_m)$ link, there exists a two hop $(\mathcal{S}-\mathcal{R})$ and $(\mathcal{R}-\mathcal{U}_m)$ link for information transfer to $\mathcal{U}_m$.

Assumptions: All nodes are equipped with single antenna, and $\mathcal{R}$ operates in two hop half duplex DF mode [8], [10]. All subcarriers on $\mathcal{S}-\mathcal{R}$, $\mathcal{S}-\mathcal{U}_m$, $\mathcal{R}-\mathcal{U}_m$ links are assumed to follow quasi-static Rayleigh fading. Perfect channel state information over all links is available at $\mathcal{S}$ [8], [10], [11]. Users are capable of utilizing maximum ratio combining (MRC)[10].

III. Proposed Secure Rate Definition

Before introducing secure rate definition in an untrusted user scenario with two tapping, we first discuss rate definitions in classical co-operative communication. Let us denote the rate achieved by user $\mathcal{U}_m$ over subcarrier n in DC and RC mode as $R_n^m|_{DC}$ and $R_n^m|_{RC}$, respectively. With $\mathcal{S}$ utilizing optimum transmission mode for achieving maximum secure rate, the effective rate R_n^m is given by $R_n^m = \max\{R_n^m|_{DC}, R_n^m|_{RC}\}$.

Manuscript received June 24, 2017; accepted July 16, 2017. This work has been supported by the Department of Science and Technology under Grant no. SB/S3/EECE/0248/2014. The associate editor coordinating the review of this paper and approving it for publication was K. Tourki.

R. Saini is with the Department of Electrical Engineering, Shiv Nadar University, Uttar Pradesh 201314, India (email: ravikant.saini@snu.edu.in).

D. Mishra and S. De are with the Department of Electrical Engineering and Bharti School of Telecommunication, Indian Institute of Technology Delhi, New Delhi 110016, India (e-mail: {deepak.mishra, swadesd}@ee.iitd.ac.in).

Digital Object Identifier xxxxxxxxxxxxxxxxx

A. Rate Definitions in Classical Co-operative Communication

Let R_n^{sm}, R_n^{sr}, and R_n^{srm}, respectively, denote the rates of $\mathcal{U}_m$ for $\mathcal{S}-\mathcal{U}_m$, $\mathcal{S}-\mathcal{R}$, and $\mathcal{S}-\mathcal{R}-\mathcal{U}_m$ links over subcarrier n. Here R_n^{srm} denotes the rate of $\mathcal{U}_m$ due to MRC of signals from $\mathcal{S}$ and $\mathcal{R}$. The rates of $\mathcal{U}_m$ in DC and RC modes are:

$$R_n^m|_{DC} = R_n^{sm}; \quad R_n^m|_{RC} = (1/2)\min\{R_n^{sr}, R_n^{srm}\}. \quad (1)$$

The factor $\frac{1}{2}$ in $R_n^m|_{RC}$ arises due to the half duplex protocol. Thus, $R_n^m = \frac{1}{2}\max\{2R_n^{sm}, \min\{R_n^{sr}, R_n^{srm}\}\}$.

Let P_n^s and P_n^r, respectively, denote source and relay power over subcarrier n. The channel gain of i–j link over subcarrier n is denoted by γ_n^{ij} where $i \in \{s, r\}$ and $j \in \{r, 1, 2, \cdots M\}$. The rates of $\mathcal{S}-\mathcal{U}_m$, $\mathcal{S}-\mathcal{R}$, and $\mathcal{S}-\mathcal{R}-\mathcal{U}_m$ links are respectively given by $R_n^{sm} = \log_2\left(1 + P_n^s\gamma_n^{sm}/\sigma^2\right)$, $R_n^{sr} = \log_2\left(1+\frac{P_n^s\gamma_n^{sr}}{\sigma^2}\right)$, and $R_n^{srm} = \log_2\left(1 + \frac{P_n^s\gamma_n^{sm}+P_n^r\gamma_n^{rm}}{\sigma^2}\right)$. After some simplifications the rate R_n^m can be restated as

$$R_n^m = \frac{1}{2}\begin{cases} R_n^{sr} & \text{if } 2R_n^{sm} \le R_n^{sr} < R_n^{srm} \\ R_n^{srm} & \text{if } 2R_n^{sm} \le R_n^{srm} \le R_n^{sr} \\ 2R_n^{sm} & \text{otherwise.} \end{cases} \quad (2)$$

$2R_n^{sm} \le R_n^{sr}$ can be simplified as $\gamma_n^{sr} \ge \gamma_n^{sm}a_n^m$ where $a_n^m = \left(2 + \frac{P_n^s\gamma_n^{sm}}{\sigma^2}\right)$, which upper bounds P_n^s as $P_n^s \le P_{n_u}^{sm} \triangleq \frac{(\gamma_n^{sr}-2\gamma_n^{sm})\sigma^2}{(\gamma_n^{sm})^2}$. $2R_n^{sm} \le R_n^{srm}$ leads to $P_n^r \ge P_{n_l}^{rm} \triangleq P_n^s\frac{\gamma_n^{sm}}{\gamma_n^{rm}}\left(1 + \frac{P_n^s\gamma_n^{sm}}{\sigma^2}\right)$. Thus, if P_n^s is below a certain threshold, and P_n^r is above a certain threshold, RC mode can be used, otherwise DC mode is a better option. $R_n^{sr} < R_n^{srm}$ leads to $\frac{P_n^r}{P_n^s} > \frac{\gamma_n^{sr}-\gamma_n^{sm}}{\gamma_n^{rm}} \triangleq \Delta_n^m$, where Δ_n^m is referred as relay versus source power (RSP) ratio. Thus, R_n^m (2) can be simplified as

$$R_n^m = \begin{cases} \frac{1}{2}R_n^{sr} & \text{if} \gamma_n^{sr} \ge \gamma_n^{sm}a_n^m, P_n^r \ge \max\{P_{n_l}^{rm}, P_n^s\Delta_n^m\} \\ \frac{1}{2}R_n^{srm} & \text{if } \gamma_n^{sr} \ge \gamma_n^{sm}a_n^m, P_n^s\Delta_n^m \ge P_n^r \ge P_{n_l}^{rm} \\ R_n^{sm} & \text{otherwise.} \end{cases} \quad (3)$$

Remark 1: From (3)*, we note that, if $P_n^r \le P_n^s\Delta_n^m$, MRC link $\mathcal{S}-\mathcal{R}-\mathcal{U}_m$ is the bottleneck compared to $\mathcal{S}-\mathcal{R}$ link, and the rate is R_n^{srm}. As $\gamma_n^{sr} \ge \gamma_n^{sm}$, MRC link remains as the bottleneck even for increased P_n^s. This rate in RC mode can be improved by increasing P_n^r till $R_n^{sr} = R_n^{srm}$, after which $\mathcal{S}-\mathcal{R}$ link becomes the bottleneck. Thus, maximum rate in RC mode is achieved when $R_n^{sr} = R_n^{srm}$, i.e., $P_n^r = P_n^s\Delta_n^m$.*

B. Incompleteness of Classical Rate Definition

The rate definition of $R_n^m|_{RC}$ in RC mode is based on an implicit assumption that $P_n^r > 0$. When $P_n^r = 0$, $R_n^{srm} = R_n^{sm}$, and $R_n^m|_{RC} = \frac{1}{2}\min\{R_n^{sr}, R_n^{sm}\}$ which is positive for $P_n^s > 0$. But this has no physical significance as the decoded information at $\mathcal{R}$ is not forwarded to $\mathcal{U}_m$. Ideally, $P_n^r = 0$ should indicate that $R_n^m|_{RC} = 0$, such that $R_n^m = R_n^m|_{DC}$.

The proposed rate definition is complete as it takes care of this gap. With $P_n^r = 0$ and $R_n^{srm} = R_n^{sm}$, the definition gets simplified to $R_n^m = \frac{1}{2}\max\{2R_n^{sm}, \min\{R_n^{sr}, R_n^{sm}\}\}$. Thus, with $P_n^r = 0$, when either $R_n^{sr} < R_n^{sm}$ or $R_n^{sr} \ge R_n^{sm}$, rate $R_n^m = 2R_n^{sm} = R_n^m|_{DC}$, i.e., subcarrier is used in DC mode.

C. Secure Rate Definition

The secure rate $R_{s_n}^m$ of $\mathcal{U}_m$ over a subcarrier n is the difference of rate R_n^m of $\mathcal{U}_m$ and rate R_n^e of the equivalent eavesdropper $\mathcal{U}_e$ [11]. Mathematically, $R_{s_n}^m$ is given by

$$R_{s_n}^m = [R_n^m - R_n^e]^+ = \left[R_n^m - \max_{o\in\{1,2,\cdots M\}\backslash m} R_n^o\right]^+ \quad (4)$$

where $x^+ = \max\{0, x\}$. The definition in (4) considers tapping in both slots. *Further, in contrast to the secure rate definition used in [5] and [8], which did not consider direct link availability, the proposed definition is a generalized one.*

IV. Subcarrier Allocation Policy

Now, we discuss the conditions for achieving positive secure rate by $\mathcal{U}_m$ over a subcarrier n. From (3), a subcarrier can be utilized in either DC or RC mode. In DC mode, the required condition is $R_n^{sm} > R_n^{se}$ which can be simplified as $\gamma_n^{sm} > \gamma_n^{se}$. With $\pi_{n_{DC}}^m$ denoting the subcarrier allocation variable in DC mode, the subcarrier allocation policy can be stated as

$$\pi_{n_{DC}}^m = \begin{cases} 1 & \text{if } m = \arg\max_{o\in\{1,2,\cdots M\}} \gamma_n^{so} \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

Positive secure rate conditions for RC mode are given below.

Proposition 1: $\mathcal{U}_m$ can use a subcarrier n in RC mode if: (i) $\gamma_n^{sr} > \max\{\gamma_n^{so}a_n^o\}$, (ii) $P_n^r > \max\{P_{n_l}^{ro}\}$ (iii) $P_n^r \le P_n^s\Delta_n^m$, and (iv) $\Delta_n^m = \min\{\Delta_n^o\}\ \forall o \in \{1, 2, \cdots M\}$.

Proof: The conditions for activating RC mode over subcarrier n are $\gamma_n^{sr} \ge \gamma_n^{sm}a_n^m$ and $P_n^r \ge P_{n_l}^{rm}$ (cf. (3)). Its generalization for M users leads to the first and the second conditions: $\gamma_n^{sr} \ge \max_{o\in\{1,2,\cdots M\}} \gamma_n^{so}a_n^o$ and $P_n^r \ge \max_{o\in\{1,2,\cdots M\}} P_{n_l}^{ro}$.

Let Δ_n^e denote RSP ratio (cf. (3)) for $\mathcal{U}_e$ over subcarrier n. If $P_n^r > P_n^s\Delta_n^m$, rate of $\mathcal{U}_m$ is R_n^{sr}. The rate of $\mathcal{U}_e$ is either R_n^{sr} when $P_n^r > P_n^s\Delta_n^e$, or R_n^{sre} otherwise. In the first case the secure rate is zero, while in the second case $R_{s_n}^m = R_n^{sr} - R_n^{sre} = \frac{1}{2}\left\{\log_2\left(\frac{\sigma^2+P_n^s\gamma_n^{sr}}{\sigma^2+P_n^s\gamma_n^{se}+P_n^r\gamma_n^{re}}\right)\right\}$, which is a decreasing function of P_n^r, enforcing $P_n^r = 0$, i.e., DC mode (cf. Section III-B). Thus, for RC mode $P_n^r \le P_n^s\Delta_n^m$ which is second condition. Lastly, we prove the third condition $\Delta_n^e > \Delta_n^m$ by contradiction that if $\Delta_n^e \le \Delta_n^m$ then positive secure rate cannot be achieved. The condition $\Delta_n^e \le \Delta_n^m$ can be restated as

$$\frac{\gamma_n^{sr}-\gamma_n^{se}}{\gamma_n^{re}} \le \frac{\gamma_n^{sr}-\gamma_n^{sm}}{\gamma_n^{rm}}. \quad (6)$$

Simplifying γ_n^{sr} from the definition of Δ_n^e, we get $\gamma_n^{sr} = \gamma_n^{se} + \Delta_n^e\gamma_n^{re}$. Substituting Δ_n^e in (6), we obtain $\gamma_n^{sr} \ge \gamma_n^{sm} + \Delta_n^e\gamma_n^{rm}$. Substituting γ_n^{sr} results in $\gamma_n^{se} + \Delta_n^e\gamma_n^{re} \ge \gamma_n^{sm} + \Delta_n^e\gamma_n^{rm}$. Multiplying both the sides with P_n^s, and substituting $P_n^s\Delta_n^e$ as P_n^r, we get $P_n^s\gamma_n^{se} + P_n^r\gamma_n^{re} \ge P_n^s\gamma_n^{sm} + P_n^r\gamma_n^{rm}$, which will lead to zero secure rate as $R_n^e \ge R_n^m$. Thus, to achieve positive secure rate $\Delta_n^e > \Delta_n^m$. Under this condition, the rates of $\mathcal{U}_m$ and $\mathcal{U}_e$ are given as R_n^{srm} and R_n^{sre}, respectively, and the secure rate definition in (4) gets simplified to

$$R_{s_n}^m = \frac{1}{2}\log_2\left(\frac{\sigma^2+P_n^s\gamma_n^{sm}+P_n^r\gamma_n^{rm}}{\sigma^2+P_n^s\gamma_n^{se}+P_n^r\gamma_n^{re}}\right). \quad (7)$$

The condition $\Delta_n^e > \Delta_n^m$ must be satisfied for all possible $\mathcal{U}_e$. Thus $\mathcal{U}_m$ has to be chosen for having minimum ratio

$\Delta_n^o \forall o \in \{1, 2, \cdots M\}$. With $\pi_{n_{RC}}^m$ as subcarrier allocation variable in RC mode, optimal subcarrier allocation policy is

$$\pi_{n_{RC}}^m = \begin{cases} 1 & \text{if } m = \arg \min\limits_{o \in \{1,2,.M\}} \left(\Delta_n^o \triangleq \frac{\gamma_n^{sr} - \gamma_n^{so}}{\gamma_n^{ro}} \right) \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

After sorting RSP ratios (Δ_n^o) over a subcarrier in ascending order, the user having the minimum value is $\mathcal{U}_m$, and the one having just next better value is the corresponding $\mathcal{U}_e$. ■

Physical Interpretation of (8)*: From* (3)*, RSP ratio $\Delta_n^o = \frac{\gamma_n^{sr} - \gamma_n^{so}}{\gamma_n^{ro}}$ is the factor by which P_n^r should be provided for a fixed P_n^s to achieve the same SNR over $\mathcal{S} - \mathcal{R}$ and $\mathcal{S} - \mathcal{R} - \mathcal{U}_m$ links. So a user having a lower ratio will require lower P_n^r to achieve maximum secure rate. Thus, once a user is chosen with minimum value of the ratio as the main user $\mathcal{U}_m$, then for any other user $\mathcal{U}_e$ having higher value of RSP ratio, its $\mathcal{R} - \mathcal{U}_e$ link becomes the bottleneck link (as it requires higher P_n^r to become equal to the $\mathcal{S} - \mathcal{R}$ link) and its rate will be lower than that of the main user. Thus, allocation in* (8) *always leads to positive secure rate over a subcarrier in RC mode.*

Remark 2: Due to the possibility of tapping in the first slot, the condition $\gamma_n^{sm} > \gamma_n^{se}$ (cf. (5)*) must be satisfied in RC mode as well. So, the main user in RC mode (cf.* (8)*) also satisfies positive secure rate requirement for DC mode (cf.* (5)*) .*

Remark 3: In case the same user is selected as main user through the policies (5) *and* (8)*, that subcarrier satisfies positive secure rate requirement for both DC and RC modes. However, corresponding eavesdroppers in the two modes can be different. With $\mathcal{U}_e$ and $\mathcal{U}_{e'}$ respectively denoting eavesdroppers in RC and DC modes over n, from* (5)*: $\gamma_n^{se'} \geq \gamma_n^{se}$.*

V. Utility of Relay: RC versus DC Mode Selection

To highlight the utility of relay, here we present the conditions for enhanced performance of RC mode over DC mode. Thus, we intend to derive conditions for $R_{s_n}^m|_{RC} > R_{s_n}^m|_{DC}$. Consider the general case where the eavesdroppers of user $\mathcal{U}_m$ are different in RC mode ($\mathcal{U}_e$) and DC mode ($\mathcal{U}_{e'}$). The condition can be simply stated as $(R_n^m - R_n^e)|_{RC} > (R_n^m - R_n^{e'})|_{DC}$.

$$\frac{1}{2} \log_2 \left(\frac{\sigma^2 + P_n^s \gamma_n^{sm} + P_n^r \gamma_n^{rm}}{\sigma^2 + P_n^s \gamma_n^{se} + P_n^r \gamma_n^{re}} \right) > \log_2 \left(\frac{\sigma^2 + P_n^s \gamma_n^{sm}}{\sigma^2 + P_n^s \gamma_n^{se'}} \right). \tag{9}$$

Using energy efficient solution $P_n^r = P_n^s \Delta_n^m$ [9], the resulting condition gets simplified as:

$$\frac{\gamma_n^{rm}}{\gamma_n^{re}} > \rho \triangleq \frac{(\gamma_n^{sr} - \gamma_n^{sm})(\sigma^2 + P_n^s \gamma_n^{sm})^2}{\rho_{den}}. \tag{10}$$

where $\rho_{den} = \gamma_n^{sr}(\sigma^2 + P_n^s \gamma_n^{se'})^2 - \gamma_n^{se}(\sigma^2 + P_n^s \gamma_n^{sm})^2 - \sigma^2\{(\sigma^2 + P_n^s \gamma_n^{se'}) + (\sigma^2 + P_n^s \gamma_n^{sm})\}(\gamma_n^{sm} - \gamma_n^{se'})$. $\rho < 0$ indicates exclusive DC mode. Next, we discuss mode selection under asymptotic conditions, and with and without known P_n^s.

A. Asymptotically Optimal Mode Selection Policy

At low SNR regime, (9) can be simplified using approximation $\log(1 + x) \approx x, \forall x \ll 1$, and $P_n^r = P_n^s \Delta_n^m$, as:

$$\frac{\gamma_n^{rm}}{\gamma_n^{re}} > \rho_l \triangleq \frac{\gamma_n^{sr} - \gamma_n^{sm}}{\gamma_n^{sr} - 2(\gamma_n^{sm} - \gamma_n^{se'}) - \gamma_n^{se}}. \tag{11}$$

Under high SNR scenario, using the approximation $\log(1 + x) \approx \log(x), \forall x \gg 1$, the condition in (9) gets simplified to:

$$\frac{\gamma_n^{rm}}{\gamma_n^{re}} > \rho_h \triangleq \frac{(\gamma_n^{sr} - \gamma_n^{sm})(\gamma_n^{sm})^2}{\gamma_n^{sr}(\gamma_n^{se'})^2 - \gamma_n^{se}(\gamma_n^{sm})^2} \tag{12}$$

B. Optimal Mode Selection for given Power Allocation

First, we show that $\rho_l < \rho$. Thus, if $\frac{\gamma_n^{rm}}{\gamma_n^{re}} < \rho_l$, the subcarrier has to be used exclusively in DC mode. Referring (10) and (11), condition $\rho_l < \rho$ can be stated as: $\gamma_n^{sr} - 2(\gamma_n^{sm} - \gamma_n^{se'}) - \gamma_n^{se} > \frac{\rho_{den}}{(\sigma^2 + P_n^s \gamma_n^{sm})^2}$. Substituting ρ_{den}, this gets simplified as:

$$\gamma_n^{sr} - 2(\gamma_n^{sm} - \gamma_n^{se'}) - \gamma_n^{se} > \gamma_n^{sr} \left(\frac{\sigma^2 + P_n^s \gamma_n^{se'}}{\sigma^2 + P_n^s \gamma_n^{sm}} \right)^2 - \sigma^2 \left(\frac{(\sigma^2 + P_n^s \gamma_n^{sm}) + (\sigma^2 + P_n^s \gamma_n^{se'})}{(\sigma^2 + P_n^s \gamma_n^{sm})^2} \right) - \gamma_n^{se}. \tag{13}$$

After arranging terms and some simplification steps, we obtain $(\gamma_n^{sm} - \gamma_n^{se'}) \left[\frac{(2\sigma^2 + P_n^s(\gamma_n^{sm} + \gamma_n^{se'}))(\sigma^2 + P_n^s \gamma_n^{sr})}{(\sigma^2 + P_n^s \gamma_n^{sm})^2} - 2 \right] > 0$. With $P_n^s > 0$ and $(\gamma_n^{sm} - \gamma_n^{se'}) > 0$, it gets reduced to $(\gamma_n^{sr} - 2\gamma_n^{sm})(2\sigma^2 + P_n^s \gamma_n^{sm}) + \sigma^2(\gamma_n^{sm} + \gamma_n^{se'}) + P_n^s \gamma_n^{sr} \gamma_n^{se'} > 0$. Observing that $\gamma_n^{sr} > 2\gamma_n^{sm}$, the above condition always holds.

Similarly, we prove that $\rho_h > \rho$, such that if $\frac{\gamma_n^{rm}}{\gamma_n^{re}} > \rho_h$, the subcarrier should be in RC mode exclusively. The equivalent condition for $\rho_h > \rho$ can be stated as (cf. (10) and (12)):

$$\left(\frac{\gamma_n^{se'}}{\gamma_n^{sm}} \right)^2 < \left(\frac{\sigma^2 + P_n^s \gamma_n^{se'}}{\sigma^2 + P_n^s \gamma_n^{sm}} \right)^2 - \frac{\sigma^2}{\gamma_n^{sr}} \left(\frac{(\sigma^2 + P_n^s \gamma_n^{sm}) + (\sigma^2 + P_n^s \gamma_n^{se'})}{(\sigma^2 + P_n^s \gamma_n^{sm})^2} \right) \tag{14}$$

After arranging the terms, this condition gets simplified as $\sigma^2(\gamma_n^{sm} - \gamma_n^{se'})\gamma_n^{sr} \left[\sigma^2(\gamma_n^{sm} + \gamma_n^{se'}) + 2P_n^s \gamma_n^{sm} \gamma_n^{se'} \right] > \sigma^2(\gamma_n^{sm} - \gamma_n^{se'})(\gamma_n^{sm})^2 \left[2\sigma^2 + P_n^s(\gamma_n^{sm} + \gamma_n^{se'}) \right]$. With $\gamma_n^{sm} > \gamma_n^{se'}$, and rearranging the terms, the condition gets reduced to $\sigma^2 \gamma_n^{sm} \left(\gamma_n^{sr} - 2\gamma_n^{sm} - \frac{P_n^s (\gamma_n^{sm})^2}{\sigma^2} \right) + \sigma^2 \gamma_n^{sr} \gamma_n^{se'} + P_n^s \gamma_n^{sm} \gamma_n^{se'} (2\gamma_n^{sr} - \gamma_n^{sm}) > 0$, which is always true as $P_n^s < P_{n_u}^{sm}$ and $\gamma_n^{sr} > \gamma_n^{sm}$. The complete mode selection policy with known power allocation can be summarized as:

$$\frac{\gamma_n^{rm}}{\gamma_n^{re}} \begin{cases} > \rho_h & R_{s_n}^m|_{RC} > R_{s_n}^m|_{DC} \ \textbf{Exclusive RC} \\ \in [\rho_l, \rho_h] & \textbf{RDC} \begin{cases} P_n^s < P_{n_{th}}^s & \textbf{RC} \\ P_n^s \geq P_{n_{th}}^s & \textbf{DC} \end{cases} \\ < \rho_l & R_{s_n}^m|_{RC} < R_{s_n}^m|_{DC} \ \textbf{Exclusive DC} \end{cases} \tag{15}$$

where $P_{n_{th}}^s$ is positive root of quadratic obtained from (10).

Physical Interpretation of (15)*: Secure rate improvement with P_n^r depends on relative gain $\frac{\gamma_n^{rm}}{\gamma_n^{re}}$. In low SNR case, all RDC mode subcarriers are in RC mode as $P_n^s < P_{n_{th}}^s$. Thus, if $\frac{\gamma_n^{rm}}{\gamma_n^{re}} < \rho_l$, the subcarrier is in DC mode, otherwise it can be in RC mode. In high SNR case, with $P_n^s > P_{n_{th}}^s$, all RDC mode subcarriers switch to DC mode. Only those subcarriers which have $\frac{\gamma_n^{rm}}{\gamma_n^{re}} > \rho_h$ are in RC mode, rest are in DC mode.*

C. Sub-optimal Mode Selection Policy

We now propose a suboptimal mode selection strategy that does not require explicit knowledge of P_n^s. Let us introduce a term 'satisfaction level' α which is considered as the minimum acceptable SNR level over a subcarrier, i.e., $\frac{P_n^s \gamma_n^{sm}}{\sigma^2} > \alpha \forall n$. As higher value of α requires higher source power on each subcarrier, it can be considered as an abstraction parameter mapping minimum supported SNR to source power budget.

Remark 4: As $\gamma_n^{sr} > \gamma_n^{sm}$ and $P_n^s \gamma_n^{sm} + P_n^r \gamma_n^{rm} > P_n^s \gamma_n^{sm}$, $\frac{P_n^s \gamma_n^{sm}}{\sigma^2} > \alpha$ is enough to ensure successful communication.

To have a higher secure rate in RC mode than in DC mode $P^s_{n_{th}} > P^s_n > \frac{\sigma^2 \alpha}{\gamma^{sm}_n}$. Substituting P^s_n, we have: $\frac{\gamma^{rm}_n}{\gamma^{re}_n} > \rho_\alpha \triangleq \frac{\alpha_{num}}{\alpha_{den}}$, where $\alpha_{num} = (\gamma^{sr}_n - \gamma^{sm}_n)(1+\alpha)^2$, and $\alpha_{den} = \gamma^{sr}_n(1 + \alpha\frac{\gamma^{se'}_n}{\gamma^{sm}_n})^2 - \gamma^{se}_n(1+\alpha)^2 - (\gamma^{sm}_n - \gamma^{se'}_n)\{(1+\alpha) + (1+\alpha\frac{\gamma^{se'}_n}{\gamma^{sm}_n})\}$. For the limiting cases $\alpha \to 0$ and $\alpha \to \infty$, ρ_α respectively tends to the low and high SNR bounds ρ_l and ρ_u on $\frac{\gamma^{rm}_n}{\gamma^{re}_n}$ discussed in Section V-A. This corroborates our reasoning behind α being a measure of source power budget.

VI. Numerical Results

The downlink of an OFDMA system is considered with $N = 64$ subcarriers which are assumed to experience quasi-static Rayleigh fading with path loss exponent $= 3$. We study performance variation with relay position, secure rate improvement due to optimal mode selection and utility regions.

Fig. 1(a) presents the effect of relay placement on its utility in improving the secure rate. Considering DC mode as a benchmark, improvement in system performance is presented by plotting the percentage of subcarriers that have higher rate in RC mode. Assuming $\mathcal{S}$ to be located at $(0, 0)$ and $M = 8$ users randomly distributed inside a unit square centered at $(2, 0)$, position of $\mathcal{R}$ is varied along a horizontal line $(x_r, 0)$ with $0.1 \leq x_r \leq 1.5$. Note that, $\mathcal{R}$ should placed closer to $\mathcal{S}$, to have $\gamma^{sr}_n \geq \gamma^{sm}_n a^m_n$ and stand against DC mode. Source power budget variation is captured by varying α. Even though optimal relay location x^*_r increases with α, it is still in the left half, i.e., $x^*_r < 0.5$, for the considered system. Note that with increased α percentage of RC mode subcarriers reduces as more and more RDC mode subcarrier switches to DC mode.

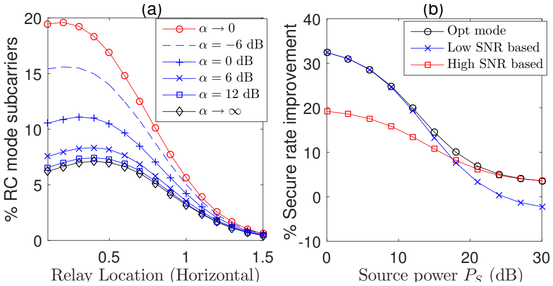

Fig. 1: (a) Performance with horizontal variation in relay position, (b) Secure rate improvement through mode selection.

Considering equal power allocation, rate improvement achieved by optimal mode selection compared to static DC mode is plotted in Fig 1(b). Following the observation from Fig 1(a), relay is placed at $(0.5, 0)$. Performance of low and high SNR based policies have been plotted to highlight efficacy of optimal policy. Rate improvement reduces with increasing P_S as all RDC subcarriers move to DC mode. At higher P_S, negative improvement is observed in low SNR based policy because RDC subcarriers which could have achieved higher rate in DC mode are pushed to RC mode.

Fig 2 presents spatial utility of relay where users' locations on a 2-D Euclidean plane are plotted after categorizing them according to the percentage of RC mode subcarriers. Assuming users to be located randomly in a 4×4 square centered around $(0, 0)$, $\mathcal{S}$ and $\mathcal{R}$ are considered to be located at $(0, 0.5)$ and $(0, -0.5)$, respectively. *Note that the best utility is around relay where more than* 14% *subcarriers are benefited by RC mode.* Due to direct link availability, decreasing trend of percentage RC mode subcarriers with distance is not symmetric.

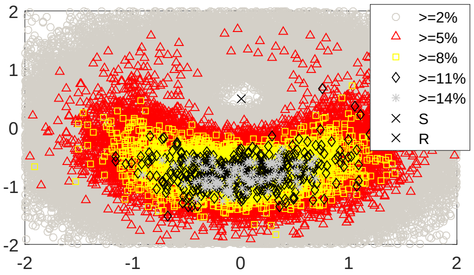

Fig. 2: Relay utility regions.

VII. Conclusion

Considering two slot tapping, this paper presents a generalized secure rate definition. After identifying conditions for RC mode, optimal subcarrier allocation policies for both RC and DC modes are obtained. A subcarrier can be used either in exclusive DC mode, in exclusive RC mode, or in RDC mode. Identifying that optimal mode selection policy for RDC mode subcarriers is integrated with power allocation, an α based suboptimal policy is discussed, which asymptotically matches with the optimal policy respectively at low and high SNR regimes. As direct link is available, results indicate that $\mathcal{R}$ should be placed closer to $\mathcal{S}$. Though the user locations around $\mathcal{R}$ are more benefited, relay utility regions are not circular.

References

[1] R. Bassily *et al.*, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Magazine*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

[2] A. Mukherjee *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[3] L. Lai and H. Gamal, "The relay eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[4] H. Deng *et al.*, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[5] T. X. Zheng *et al.*, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.

[6] H. Xu *et al.*, "Cooperative privacy preserving scheme for downlink transmission in multiuser relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 825–839, Apr. 2017.

[7] A. Mabrouk *et al.*, "Transmission mode selection scheme for physical layer security in multi-user multi-relay systems," in *Proc. IEEE PIMRC*, Sep. 2016, pp. 1–6.

[8] D. Ng *et al.*, "Secure resource allocation and scheduling for OFDMA decode-and-forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3528–3540, Oct. 2011.

[9] R. Saini *et al.*, "OFDMA-based DF secure cooperative communication with untrusted users," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 716–719, Apr. 2016.

[10] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[11] X. Wang *et al.*, "Power and subcarrier allocation for physical-layer security in OFDMA-based broadband wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 693–702, Sep. 2011.