OFDMA-based DF Secure Cooperative Communication with Untrusted Users

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

***Abstract*—In this letter we consider resource allocation for OFDMA-based secure cooperative communication by employing a trusted Decode and Forward (DF) relay among the untrusted users. We formulate two optimization problems, namely, (i) sum rate maximization subject to individual power constraints on source and relay, and (ii) sum power minimization subject to a fairness constraint in terms of per-user minimum support secure rate requirement. The optimization problems are solved utilizing the optimality of KKT conditions for pseudolinear functions.**

***Index Terms*—DF cooperative communication, pseudolinear optimization, secure OFDMA, resource allocation**

I. Introduction

Relaying along with OFDMA is being considered as a promising technology for providing high data rate connectivity anywhere, anytime [1]. Physical layer security aspects in relay-assisted communication has recently gathered considerable attention in the research community [2]. Based on the relaying strategy, e.g., amplify-and-forward (AF) or decode-and-forward (DF), resource allocation problems are formulated differently and are thus investigated separately. Broadly, there exist two kinds of wire tapping scenarios: single eavesdropper with trusted users [3]–[5] and untrusted users [6]. The study in [3] considered subcarrier and power allocation problems in an AF relay-assisted OFDM system with single eavesdropper. Assuming availability of direct path, [4] considered sum rate maximization problem under total system power constraint in DF relay-assisted secure cooperative communication (DFSCC) for a single source-destination pair with a single eavesdropper. Multiuser resource allocation problem in OFDMA-based DFSCC with single eavesdropper was solved in [5]. Recently, resource allocation problems for improving secure capacity and system fairness in OFDMA system with untrusted users and single friendly jammer have been considered in [6]. *To the best of our knowledge, OFDMA-based DFSCC with multiple untrusted users has not yet been considered in the literature.*

We consider two resource allocation problems. First, sum secure rate maximization is studied subject to individual power constraints on source and relay, due to their geographically apart locations. Second, sum power minimization is solved subject to the fairness constraint in terms of per-user minimum support secure rate. The key contributions are as follows: (i) We derive secure rate positivity constraints for each subcarrier, which includes the optimal subcarrier allocation policy. (ii) We prove that the two problems described above belong to the class of generalized convex problems which can be solved optimally. (iii) We show that the optimal secure rate for a user is achieved when rates of source-relay and relay-user links over a subcarrier are equal. (iv) We also present analytical and graphical interpretation of the derived optimal solutions.

Manuscript received December 12, 2015; revised January 19, 2016; accepted January 21, 2016. This work has been supported by the Department of Science and Technology (DST) under Grant SB/S3/EECE/0248/2014. The associate editor coordinating the review of this paper and approving it for publication was K. Tourki.

R. Saini, D. Mishra, and S. De are with the Department of Electrical Engineering and Bharti School of Telecom, Indian Institute of Technology Delhi, New Delhi, India (e-mail: ravikant.saini@dbst.iitd.ac.in; deepak.mishra@ee.iitd.ac.in; swadesd@ee.iitd.ac.in).

Digital Object Identifier xxxxxxxxxxxxxxxx

II. System Model

We consider the downlink of an OFDMA-based cooperative communication system with a trusted DF relay controlled by a base station (hereafter referred as source $\mathcal{S}$). The users have mutual untrust and request secure communication from $\mathcal{S}$. The subcarriers on $\mathcal{S}$-to-$\mathcal{R}$ and $\mathcal{R}$-to-mth user ($\mathcal{U}_m$) links are assumed to follow quasi-static Rayleigh fading. Availability of perfect CSI for each link is assumed. All nodes are equipped with single antenna, and $\mathcal{R}$ operates in half-duplex mode [3], [4]. There is no direct connectivity between $\mathcal{S}$ and $\mathcal{U}_m$ [5].

DFSCC with trusted $\mathcal{R}$ and M untrusted users is a multiple eavesdropper scenario, where for each user there exist $M-1$ eavesdroppers, and the strongest of them is considered as the equivalent eavesdropper. Over a subcarrier n, the secure rate $R_{s_n}^m$ of $\mathcal{U}_m$ is defined as the non-negative difference of the rate R_n^m of $\mathcal{U}_m$ and the rate R_n^e of the equivalent eavesdropper $\mathcal{U}_e$ [6]. Mathematically, the secure rate is expressed as:

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

where $x^+ = \max\{0, x\}$. In half-duplex DF cooperative communication, $R_n^m = \frac{1}{2}\min\{R_n^{sr}, R_n^{rm}\}$, where R_n^{sr} and R_n^{rm} respectively denote the rates of $\mathcal{S}$-to-$\mathcal{R}$ and $\mathcal{R}$-to-$\mathcal{U}_m$ links over subcarrier n. Using this, (1) can be simplified as [4]:

$$R_{s_n}^m = (1/2)\left\{\min\left(R_n^{sr}, R_n^{rm}\right) - R_n^{re}\right\}^+ . \quad (2)$$

Next, we discuss the sum secure rate maximization problem.

III. Sum Secure Rate Maximization in DFSCC

Denoting P_n^s and P_n^r respectively as powers of $\mathcal{S}$ and $\mathcal{R}$ over subcarrier n, the optimization problem can be stated as:

$$\mathcal{P}0: \quad \underset{\pi_n^m, P_n^s, P_n^r}{\text{maximize}} \left[R_s\left(\pi_n^m, P_n^s, P_n^r\right) = \sum_{m=1}^{M}\sum_{n=1}^{N} \pi_n^m R_{s_n}^m \right]$$

$$\text{s.t.} \quad C1: \sum_{m=1}^{M} \pi_n^m \le 1 \; \forall n, \quad C2: \pi_n^m \in \{0,1\} \; \forall m, n,$$

$$C3: \sum_{n=1}^{N} P_n^s \leq P_S, \qquad C4: \sum_{n=1}^{N} P_n^r \leq P_R,$$
$$C5: P_n^s \geq 0, P_n^r \geq 0 \ \forall n \tag{3}$$

where π_n^m is a subcarrier allocation variable, indicating whether subcarrier n is allocated to $\mathcal{U}_m$ or not. Constraints $C1$ and $C2$ ensure that a subcarrier is allocated to only one user. Power budgets P_S and P_R at $\mathcal{S}$ and $\mathcal{R}$ are respectively incorporated in $C3$ and $C4$. $C5$ includes positivity constraints. For each subcarrier, there are two real variables P_n^s, P_n^r, and one binary variable π_n^m. Because of $\log$ and $\max$ functions in objective, $\mathcal{P}0$ is a mixed integer non-linear programming problem, which is NP hard. To solve $\mathcal{P}0$, first we determine subcarrier allocation and then we complete power allocation.

A. Subcarrier Allocation

The feasibility of achieving positive secure rate by $\mathcal{U}_m$ over a subcarrier n is described by the following proposition.

Proposition 1. *In DFSCC with untrusted users, positive secure rate over a subcarrier n can be obtained if and only if (i) the subcarrier is allocated to the best gain user, and (ii) $\mathcal{R}$-to-$\mathcal{U}_e$ link of the eavesdropper $\mathcal{U}_e$ is the bottleneck link compared to the $\mathcal{S}$-to-$\mathcal{R}$ link over that subcarrier.*

Proof: $R_{s_n}^m$ in (2) can be restated as:

$$R_{s_n}^m = \frac{1}{2} \begin{cases} R_n^{sr} - R_n^{re} & \text{if } R_n^{re} < R_n^{sr} < R_n^{rm} \\ R_n^{rm} - R_n^{re} & \text{if } R_n^{re} < R_n^{rm} < R_n^{sr} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

From (4) we note that, conditions for positive secure rate are: (a) $R_n^{re} < R_n^{rm}$ and (b) $R_n^{re} < R_n^{sr}$. Let γ_n^{sr}, γ_n^{rm}, and γ_n^{re} respectively denote the channel gains of $\mathcal{S}$-to-$\mathcal{R}$, $\mathcal{R}$-to-$\mathcal{U}_m$, and $\mathcal{R}$-to-$\mathcal{U}_e$ links over subcarrier n. The rates R_n^{sr}, R_n^{rm}, and R_n^{re} are given by $\log_2\left(1 + P_n^s\gamma_n^{sr}/\sigma^2\right)$, $\log_2\left(1 + P_n^r\gamma_n^{rm}/\sigma^2\right)$, and $\log_2\left(1 + P_n^r\gamma_n^{re}/\sigma^2\right)$, respectively. Here σ^2 is the additive white Gaussian noise (AWGN) variance. Condition (a) $R_n^{re} < R_n^{rm}$, simplified as $\gamma_n^{re} < \gamma_n^{rm}$, indicates the optimal subcarrier allocation policy which can be stated as:

$$\pi_n^m = \begin{cases} 1 & \text{if } \gamma_n^{rm} > \gamma_n^{re} \triangleq \max\limits_{o \in \{1,2,\cdots M\} \setminus m} \gamma_n^{ro} \\ 0 & \text{otherwise.} \end{cases} \tag{5}$$

Condition (b) $R_n^{re} < R_n^{sr}$, simplified as $P_n^r\gamma_n^{re} < P_n^s\gamma_n^{sr}$, should be incorporated as a power optimization constraint. □

Following the observations $R_n^{re} < R_n^{rm}$ and $R_n^{re} < R_n^{sr}$ in Proposition 1, $R_{s_n}^m$ can be rewritten without $\max$ operator as:

$$R_{s_n}^m = \frac{1}{2}\left[\log_2\left(\frac{1 + \min\left(\frac{P_n^s\gamma_n^{sr}}{\sigma^2}, \frac{P_n^r\gamma_n^{rm}}{\sigma^2}\right)}{1 + \frac{P_n^r\gamma_n^{re}}{\sigma^2}}\right)\right]. \tag{6}$$

B. Power Allocation

Ensuring $R_n^{re} < R_n^{rm}$ through optimal subcarrier allocation (5) and enforcing $R_n^{re} < R_n^{sr}$ as a constraint, equivalent power allocation problem for $\mathcal{P}0$ using (6) can be formulated as:

$$\mathcal{P}1: \underset{P_n^s, P_n^r, t_n}{\text{maximize}} \left[\widehat{R_s}(t_n, P_n^r) \triangleq \sum_{n=1}^{N} \frac{1}{2}\left\{\log_2\left(\frac{1 + t_n}{1 + \frac{P_n^r\gamma_n^{re}}{\sigma^2}}\right)\right\}\right]$$
$$\text{s.t.} \quad C1: t_n \leq \frac{P_n^s\gamma_n^{sr}}{\sigma^2} \ \forall n, \quad C2: t_n \leq \frac{P_n^r\gamma_n^{rm}}{\sigma^2} \ \forall n,$$
$$C3, C4, C5, \text{as in (3)}, \quad C6: P_n^r\gamma_n^{re} \leq P_n^s\gamma_n^{sr} \ \forall n. \tag{7}$$

Constraints $C1 - C2$ come from the definition of $\min\{\cdot\}$, $C6$ comes from secure rate positivity requirements given by Proposition 1. Due to non-concave objective function $\widehat{R_s}$, $\mathcal{P}1$ is non-convex. However, via the following lemma, we show that $\mathcal{P}1$ belongs to the class of generalized convex problems.

Lemma 1. *The objective function of $\mathcal{P}1$ is pseudolinear on the feasible region defined by the constraints, and the solution obtained from the KKT conditions is the global optimal.*

Proof: The objective function $\widehat{R_s}(t_n, P_n^r)$ of $\mathcal{P}1$ is a pseudolinear function [7] of t_n and P_n^r, with $\frac{\partial \widehat{R_s}}{\partial t_n} = \frac{1}{2(1+t_n)} \triangleq a_n$ and $\frac{\partial \widehat{R_s}}{\partial P_n^r} = \frac{-\gamma_n^{re}}{2(\sigma^2 + P_n^r\gamma_n^{re})} \triangleq b_n$, because $\frac{\partial \widehat{R_s}}{\partial t_n}, \frac{\partial \widehat{R_s}}{\partial P_n^r} \neq 0$ in the entire feasible region defined by the linear constraints $C1 - C6$. Moreover, the bordered Hessian is given as: $B_H = \begin{bmatrix} 0 & \frac{\partial \widehat{R_s}}{\partial t_n} & \frac{\partial \widehat{R_s}}{\partial P_n^r} \\ \frac{\partial \widehat{R_s}}{\partial t_n} & \frac{\partial^2 \widehat{R_s}}{\partial t_n^2} & \frac{\partial^2 \widehat{R_s}}{\partial t_n \partial P_n^r} \\ \frac{\partial \widehat{R_s}}{\partial P_n^r} & \frac{\partial^2 \widehat{R_s}}{\partial P_n^r \partial t_n} & \frac{\partial^2 \widehat{R_s}}{\partial P_n^{r2}} \end{bmatrix} = \begin{bmatrix} 0 & a_n & b_n \\ a_n & -a_n^2 & 0 \\ b_n & 0 & b_n^2 \end{bmatrix} = 0.$ Following this and [8, Theorem 4.3.8], along with the knowledge that constraints are linear and differentiable, it can be inferred that the KKT point is the global optimal solution. □

The optimal power allocation (P_n^s, P_n^r) obtained after solving KKT conditions is characterized by following Theorem.

Theorem 1. *In DFSCC, maximum secure rate over a subcarrier is achieved when the following relationship holds*

$$P_n^s\gamma_n^{sr} = P_n^r\gamma_n^{rm}. \tag{8}$$

Proof: Lagrangian $\mathcal{L}_1$ of the problem $\mathcal{P}1$ can be stated as:

$$\mathcal{L}_1 = \sum_{n=1}^{N} \frac{1}{2}\left\{\log_2\left(\frac{1 + t_n}{1 + \frac{P_n^r\gamma_n^{re}}{\sigma^2}}\right)\right\} - \sum_{n=1}^{N} x_n\left(t_n - \frac{P_n^s\gamma_n^{sr}}{\sigma^2}\right)$$
$$- \sum_{n=1}^{N} y_n\left(t_n - \frac{P_n^r\gamma_n^{rm}}{\sigma^2}\right) - \sum_{n=1}^{N} z_n\left(\frac{P_n^r\gamma_n^{re}}{\sigma^2} - \frac{P_n^s\gamma_n^{sr}}{\sigma^2}\right)$$
$$- \lambda\left(\sum_{n=1}^{N} P_n^s - P_S\right) - \mu\left(\sum_{n=1}^{N} P_n^r - P_R\right). \tag{9}$$

Here, x_n, y_n, z_n, λ, and μ are Lagrange multipliers. Using (7) and (9), the KKT conditions for $\mathcal{P}1$ are given by

$$\frac{\partial \mathcal{L}_1}{\partial P_n^s} = x_n\frac{\gamma_n^{sr}}{\sigma^2} + z_n\frac{\gamma_n^{sr}}{\sigma^2} - \lambda = 0 \tag{10a}$$

$$\frac{\partial \mathcal{L}_1}{\partial P_n^r} = \frac{-\gamma_n^{re}}{2\left(\sigma^2 + P_n^r\gamma_n^{re}\right)} + y_n\frac{\gamma_n^{rm}}{\sigma^2} - z_n\frac{\gamma_n^{re}}{\sigma^2} - \mu = 0 \tag{10b}$$

$$\frac{\partial \mathcal{L}_1}{\partial t_n} = \frac{1}{2\left(1 + t_n\right)} - x_n - y_n = 0 \tag{10c}$$

$$x_n\left(t_n - \frac{P_n^s\gamma_n^{sr}}{\sigma^2}\right) = 0; \quad y_n\left(t_n - \frac{P_n^r\gamma_n^{rm}}{\sigma^2}\right) = 0 \tag{10d}$$

$$z_n\left(P_n^r\gamma_n^{re} - P_n^s\gamma_n^{sr}\right) = 0 \tag{10e}$$

$$\lambda\left(\sum_{n=1}^{N} P_n^s - P_S\right) = 0; \quad \mu\left(\sum_{n=1}^{N} P_n^r - P_R\right) = 0. \tag{10f}$$

Next we consider the following three cases.

$$t_n = \begin{cases} P_n^s \gamma_n^{sr}/\sigma^2 & \text{if } P_n^s\gamma_n^{sr} < P_n^r \gamma_n^{rm} \\ P_n^r \gamma_n^{rm}/\sigma^2 & \text{if } P_n^s\gamma_n^{sr} > P_n^r \gamma_n^{rm} \\ P_n^s \gamma_n^{sr}/\sigma^2 = P_n^r \gamma_n^{rm}/\sigma^2 & \text{otherwise.} \end{cases} \quad (11)$$

Case 1: $t_n = P_n^s \gamma_n^{sr}/\sigma^2$; $x_n > 0$ and $y_n = 0$. From (10b) we get $\frac{\gamma_n^{re}}{2(\sigma^2 + P_n^r \gamma_n^{re})} + \mu + z_n \frac{\gamma_n^{re}}{\sigma^2} = 0$, which cannot be satisfied for any positive finite P_n^r and σ^2. Thus, this case is infeasible.

Case 2: $t_n = P_n^r \gamma_n^{rm}/\sigma^2$; $x_n = 0$ and $y_n > 0$, it gives $\lambda = z_n \gamma_n^{sr}/\sigma^2$ and $y_n = 1/\{2(1+t_n)\}$. Substituting in (10b),

$$\mu + \lambda \frac{\gamma_n^{re}}{\gamma_n^{sr}} + \frac{\gamma_n^{re}}{2(\sigma^2 + P_n^r \gamma_n^{re})} - \frac{\gamma_n^{rm}}{2(\sigma^2 + P_n^r \gamma_n^{rm})} = 0. \quad (12)$$

Since $P_n^r \gamma_n^{rm}/\sigma^2 < P_n^s \gamma_n^{sr}/\sigma^2$, and we know that $\gamma_n^{rm} > \gamma_n^{re}$. Thus, $P_n^r \gamma_n^{re}/\sigma^2 < P_n^r \gamma_n^{rm}/\sigma^2 < P_n^s \gamma_n^{sr}/\sigma^2$ which indicates that $z_n = 0$ (c.f. (10e)). Since $z_n = 0$, so $\lambda = 0$. Thus, (12) results in a quadratic equation in P_n^r, having following form

$$(P_n^r)^2 \gamma_n^{rm} \gamma_n^{re} + P_n^r (\gamma_n^{rm} + \gamma_n^{re}) \sigma^2 + \sigma^4 - \Delta_n = 0 \quad (13)$$

where $\Delta_n = \frac{\sigma^2}{2\mu}(\gamma_n^{rm} - \gamma_n^{re})$. For a fixed μ, the optimal P_n^r, obtained as the only positive real root of (13) is given by

$$P_n^r = \frac{-\sigma^2(\gamma_n^{rm} + \gamma_n^{re}) + \sqrt{\sigma^4 (\gamma_n^{rm} - \gamma_n^{re})^2 + 4\gamma_n^{rm}\gamma_n^{re}\Delta_n}}{2\gamma_n^{rm}\gamma_n^{re}}. \quad (14)$$

For a known P_n^r, we set $P_n^s = P_n^r \frac{\gamma_n^{rm}}{\gamma_n^{sr}} + \delta$, where δ is a very small positive number, because allocating more P_n^s does not provide a higher secure rate. The optimum μ can be found using subgradient method [9], such that $\sum_{n=1}^{N} P_n^r = P_R$.

Case 3: $t_n = P_n^r \gamma_n^{rm}/\sigma^2 = P_n^s \gamma_n^{sr}/\sigma^2$; $x_n > 0$ and $y_n > 0$. Replacing $x_n = \lambda \frac{\sigma^2}{\gamma_n^{sr}} - z_n$ (from (10a)), in (10c) we get $y_n = \frac{1}{2(1+t_n)} - \lambda \frac{\sigma^2}{\gamma_n^{sr}} + z_n$. On substituting t_n and y_n in (10b),

$$\frac{\gamma_n^{re}}{2(\sigma^2 + P_n^r \gamma_n^{re})} - \frac{\gamma_n^{rm}}{2(\sigma^2 + P_n^r \gamma_n^{rm})} + \mu + \lambda \left(\frac{\gamma_n^{rm}}{\gamma_n^{sr}}\right) = z_n (\gamma_n^{rm} - \gamma_n^{re}). \quad (15)$$

The complimentary slackness condition (10e) can be simplified as $z_n \left(P_n^r \gamma_n^{re}/\sigma^2 - P_n^r \gamma_n^{rm}/\sigma^2\right) = 0$, which indicates $z_n = 0$ because $\gamma_n^{rm} > \gamma_n^{re}$. After simplifications, (15) results in a quadratic equation in P_n^r similar to (13) with $\Delta_n = \frac{\sigma^2 \gamma_n^{sr}(\gamma_n^{rm} - \gamma_n^{re})}{2(\mu \gamma_n^{sr} + \lambda \gamma_n^{rm})}$. For fixed λ and μ, the optimal P_n^r is given by (14). The optimal λ and μ are obtained using subgradient method [9] such that $\sum_{n=1}^{N} P_n^r = P_R$ and $\sum_{n=1}^{N} P_n^s = P_S$. Since with $\delta \to 0$ case 2 is inherently contained in case 3, (8) provides an energy-efficient global optimal solution. □

C. Analytical and Graphical Interpretations

Writing (15) with $z_n = 0$ in a compact form we get

$$\frac{\frac{\gamma_n^{rm} - \gamma_n^{re}}{\sigma^2}}{2\left(1 + \frac{P_n^r \gamma_n^{rm}}{\sigma^2}\right)\left(1 + \frac{P_n^r \gamma_n^{re}}{\sigma^2}\right)} = \mu + \lambda \left(\frac{\gamma_n^{rm}}{\gamma_n^{sr}}\right) \; \forall n. \quad (16)$$

From (6) and (8), it appears intuitive that P_n^r should be allocated according to the relative gain $(\gamma_n^{rm} - \gamma_n^{re})$. However on closely observing (16), we note that P_n^r depends not only on relative gain, but also on absolute gains γ_n^{sr}, γ_n^{rm}, and γ_n^{re}.

Utilizing the secure rate definition (4), the result (8) obtained from Theorem 1 can be explained graphically using Fig. 1. When $\mathcal{S}$-to-$\mathcal{R}$ link is the bottleneck as compared to $\mathcal{R}$-to-$\mathcal{U}_m$ link i.e., $P_n^s \gamma_n^{sr} < P_n^r \gamma_n^{rm}$ (case 1 in (11), and case (a) in Fig. 1), the secure rate is given as $R_{s_n}^m = \log_2\left(\frac{\sigma^2 + P_n^s \gamma_n^{sr}}{\sigma^2 + P_n^r \gamma_n^{re}}\right)$. This case is infeasible because $R_{s_n}^m$ can be improved by either increasing P_n^s or reducing P_n^r. If there is enough P_S budget, then P_n^s could be increased till (8) gets satisfied, beyond which $\mathcal{R}$-to-$\mathcal{U}_m$ link becomes the bottleneck (considered separately as case (b) in Fig. 1). However, if P_S is limited, then P_n^r should be reduced till (8) gets satisfied. With further lowered P_n^r, $\mathcal{R}$-to-$\mathcal{U}_m$ link becomes the bottleneck. Thus, at KKT point $P_n^s \gamma_n^{sr}$ cannot be less than $P_n^r \gamma_n^{rm}$, and hence case 1 is infeasible.

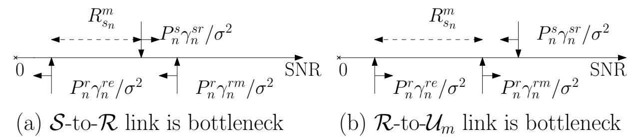

Fig. 1. Graphical interpretation of Theorem 1.

When $\mathcal{R}$-to-$\mathcal{U}_m$ link is bottleneck compared to $\mathcal{S}$-to-$\mathcal{R}$ link i.e., $P_n^r \gamma_n^{rm} < P_n^s \gamma_n^{sr}$ (case 2 in (11), and case (b) in Fig. 1), $R_{s_n}^m = \log_2\left(\frac{\sigma^2 + P_n^r \gamma_n^{rm}}{\sigma^2 + P_n^r \gamma_n^{re}}\right)$, which is an increasing function of P_n^r. In order to improve $R_{s_n}^m$, P_n^r can be increased till (8) gets satisfied, beyond which the $\mathcal{S}$-to-$\mathcal{R}$ link becomes bottleneck. If P_R is limited then just enough P_n^s should be utilized so as to satisfy (8). Higher P_n^s, though feasible, does not improve secure rate, as $R_{s_n}^m$ is independent of P_n^s. Thus, case 2 can have multiple solutions but with the same optimal value.

Remark 1. *Using (8) in (6), at KKT point $R_{s_n}^m$ is concave increasing in P_n^r, and is bounded by* $(1/2)\log_2(\gamma_n^{rm}/\gamma_n^{re})$.

IV. Sum Power Minimization in DFSCC

For the sum power minimization problem, considering sum secure rate constraint over OFDMA system is not significant from fairness point of view. Actually it would utilize power resources over those subcarriers where higher secure rate can be achieved, which may lead to scarcity of power resources and eventually very small secure rate for some users. For handling this issue, we consider a minimum support secure rate requirement R_{ssr} for each user. This results in a more complicated problem with M rate constraints, instead of one.

Following Proposition 1, first, subcarrier allocation is done based on (5). Since the maximum secure rate achievable over a subcarrier is bounded (cf. Remark 1), before optimal power allocation, it is checked whether R_{ssr} for each user can be achieved. If it can be achieved, that user is selected for power allocation, otherwise not. Considering U^a as the set of selected users for resource allocation and N_m as the set of subcarriers of $\mathcal{U}_m$, the sum power minimization problem is given by:

$$\mathcal{Q}0: \underset{P_k^s, P_k^r}{\text{minimize}} \sum_{\mathcal{U}_m \in U^a} \sum_{k \in N_m} (P_k^s + P_k^r)$$

$$\text{s.t. } C1\!: \sum_{k \in N_m} R_{s_k}^m \geq R_{ssr} \; \forall \mathcal{U}_m \in U^a, \; C2\!: P_k^s, P_k^r \geq 0. \quad (17)$$

Since all subcarriers are independent, per-user rate constraints can be handled in parallel. Thus, the optimization problem can be decomposed at user level and solved in parallel. The individual user level problem for each $\mathcal{U}_m \in U^a$ is stated as:

$$\mathcal{Q}1: \quad \underset{P_k^r, P_k^s}{\text{minimize}} \sum_{k \in N_m} \left(P_k^s + P_k^r\right)$$
$$\text{s.t. } C1: \sum_{k \in N_m} \frac{1}{2} \log_2 \left(\frac{1 + t_k}{1 + \frac{P_k^r \gamma_k^{re}}{\sigma^2}} \right) \geq R_{ssr},$$
$$C2: t_k \leq \frac{P_k^s \gamma_k^{sr}}{\sigma^2} \ \forall k, \quad C3: t_k \leq \frac{P_k^r \gamma_k^{rm}}{\sigma^2} \ \forall k,$$
$$C4: P_k^r \gamma_k^{re} \leq P_k^s \gamma_k^{sr} \ \forall k, C5: P_k^s \geq 0, P_k^r \geq 0 \ \forall k. \quad (18)$$

The objective function of $\mathcal{Q}1$ is linear, $C1$ is pseudolinear (Lemma 1), and $C2 - C5$ are linear. So, the KKT point gives the optimal solution [8]. The Lagrangian $\mathcal{L}_2$ of $\mathcal{Q}1$ with x_k, y_k, z_k, and λ as the Lagrange multipliers is given by:

$$\mathcal{L}_2 = \sum_{k \in N_m} \left(P_k^s + P_k^r\right) + \sum_{k \in N_m} x_k \left(t_k - \frac{P_k^s \gamma_k^{sr}}{\sigma^2} \right)$$
$$+ \sum_{k \in N_m} y_k \left(t_k - \frac{P_k^r \gamma_k^{rm}}{\sigma^2} \right) + \sum_{k \in N_m} z_k \left(\frac{P_k^r \gamma_k^{re}}{\sigma^2} - \frac{P_k^s \gamma_k^{sr}}{\sigma^2} \right)$$
$$- \lambda \left[\sum_{k \in N_m} \frac{1}{2} \left\{ \log_2 \left(\frac{1 + t_k}{1 + \frac{P_k^r \gamma_k^{re}}{\sigma^2}} \right) \right\} - R_{ssr} \right]. \quad (19)$$

The stationarity KKT conditions for $\mathcal{Q}1$ are given by:

$$\frac{\partial \mathcal{L}_2}{\partial P_k^s} = 1 - x_k \frac{\gamma_k^{sr}}{\sigma^2} - z_k \frac{\gamma_k^{sr}}{\sigma^2} = 0 \quad (20a)$$
$$\frac{\partial \mathcal{L}_2}{\partial P_k^r} = 1 + \frac{\lambda \gamma_k^{re}}{2\left(\sigma^2 + P_k^r \gamma_k^{re}\right)} - y_k \frac{\gamma_k^{rm}}{\sigma^2} + z_k \frac{\gamma_k^{re}}{\sigma^2} = 0 \quad (20b)$$
$$\frac{\partial \mathcal{L}_2}{\partial t_k} = x_k + y_k - \frac{\lambda}{2\left(1 + t_k\right)} = 0. \quad (20c)$$

Additionally, there are four complimentary slackness conditions, three are similar to (10d)-(10e), and fourth is given as:

$$\lambda \left[\sum_{k \in N_m} \frac{1}{2} \left\{ \log_2 \left(\frac{1 + t_k}{1 + \frac{P_k^r \gamma_k^{re}}{\sigma^2}} \right) \right\} - R_{ssr} \right] = 0. \quad (21)$$

Here also there exist three cases similar to (11). Considering the cases one by one, in case 1, $x_k > 0$ but $y_k = 0$. This case is infeasible because, if $y_k = 0$, then (20b) cannot be satisfied. Considering case 2, $x_k = 0$, $y_k > 0$, and $z_k = 0$ (by the same argument as explained in the proof of Theorem 1); thus (20a) cannot be satisfied, and hence this case is also infeasible. The only feasible case is case 3, in which, using $z_k = 0$ and on simplifying (20a)-(20c), we obtain a quadratic equation in P_k^r similar to (13) where Δ_n is replaced with $\Delta_k = \frac{\lambda \sigma^2 \gamma_k^{sr} (\gamma_k^{rm} - \gamma_k^{re})}{2\left(\gamma_k^{sr} + \gamma_k^{rm}\right)}$. The optimal P_k^r is given by (14) for a fixed value of λ, and the optimal λ is found using subgradient method [9] such that $C1$ in $\mathcal{Q}1$ is satisfied with equality.

V. Numerical Results

Here we present numerical results of OFDMA-based DFSCC with $M = 8$ users and $N = 64$ subcarriers. $\mathcal{S}$ and $\mathcal{R}$ are assumed to be respectively located at $(0, 0)$ and $(1, 0)$. The users are uniformly distributed inside a unit square, centered at $(2, 0)$. With $\sigma^2 = 1$, we consider quasi-static Rayleigh fading. Large scale fading is modeled using path loss exponent $= 3$.

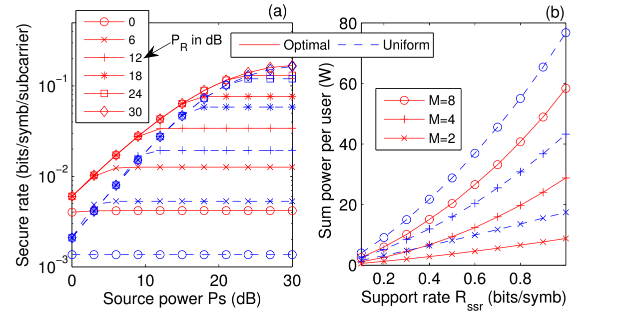

Fig. 2.(a) Secure rate versus source power; (b) Sum power versus support rate.

Fig. 2(a) presents the variation of optimal sum secure rate R_s^* (or $\widehat{R_s^*}$) with source power budget P_S, for different relay power budgets P_R. At low P_R, R_s^* is limited by P_R itself and increasing P_S does not improve R_s^* significantly. Interestingly, at high enough P_R, R_s^* increases with diminishing returns before saturating at high P_S. This indicates the existence of an upper bound on R_s^*. *The monotonicity of R_s^* corroborates pseudolinearity with respect to P_n^s and P_n^r.* Fig. 2(b) shows that sum power required per-user increases exponentially with R_{ssr}. Sum power required for a fixed R_{ssr} increases with number of users, due to effectively lesser number of subcarriers per-user. The performance improvement achieved by the proposed solutions over a benchmark scheme, namely, uniform power allocation, is also demonstrated in Figs. 2(a) and 2(b).

VI. Concluding Remarks

To summarize, we have investigated resource allocation in OFDMA-based DFSCC with multiple untrusted users. Global optimal solutions for secure rate maximization and sum power minimization problems have been obtained by exploiting the concepts of generalized convexity and pseudolinearity. Numerical results have offered insight into the optimal power required for realizing an energy-efficient DFSCC system.

References

[1] M. Salem, A. Adinoyi, M. Rahman, H. Yanikomeroglu, D. Falconer, Y.-D. Kim, E. Kim, and Y.-C. Cheong, "An overview of radio resource management in relay-enhanced OFDMA-based networks," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 3, pp. 422–438, Aug. 2010.

[2] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "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] A. Jindal and R. Bose, "Resource allocation for secure multicarrier AF relay system under total power constraint," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 231–234, Feb. 2015.

[4] 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.

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

[6] R. Saini, A. Jindal, and S. De, "Jammer-assisted resource allocation in secure OFDMA with untrusted users," *IEEE Trans. Inf. Forensics Security,* vol. PP, no. 99, pp. 1–1, 2016.

[7] S. Komlosi, "First and second order characterizations of pseudolinear functions," *Europ. J. Operational Res.*, vol. 67, no. 2, pp. 278–286, 1993.

[8] M. S. Bazaraa, H. D. Sherali, and C. M. Shetty, *Nonlinear Programming: Theory and Applications*. New York: John Wiley and Sons, 2006.

[9] S. Boyd, L. Xiao, and A. Mutapcic, *Subgradient methods*, ser. Lecture Notes. Stanford Univ., Apr. 2003.