# Fast Power Allocation for Secure Communication With Full-Duplex Radio

Lei Chen, *Student Member, IEEE*, Qiping Zhu, *Student Member, IEEE*, Weixiao Meng, *Senior Member, IEEE*, and Yingbo Hua, *Fellow, IEEE*

***Abstract*—This paper considers a method for improving physical layer security of wireless networks with full-duplex radio. In particular, fast algorithms are developed to compute power allocations in subcarriers, subject to power and rate constraints, to maximize the secrecy capacity of a three-node network consisting of a source, a full-duplex destination, and an eavesdropper. A residual level of radio self-interference channel is considered. The optimal power allocation at the destination is found to be significant especially when its power budget is high. Also studied in this paper are a network with multiple full-duplex destinations and another network with multiple sources. Using the algorithms developed in this paper, we are able to show that a multiuser strategy that optimizes the power distributions among the users (in terms of either the sources or the destinations) can yield a substantial gain of secrecy capacity over a single-user strategy.**

***Index Terms*—Full-duplex, multicarrier, OFDM, power allocation, secure communication, physical layer security.**

## I. Introduction

With ubiquitous mobile communication devices and increasing flexibility of wireless networking for wide range of activities (including banking), the security of wireless communication has become more important than ever. Some level of security against conventional eavesdroppers, to and from which the channel state information is typically unknown, can be provided by cryptography [2]. But for eavesdroppers hidden in our own devices (such as Malware), channel state information to and from these devices can be estimated and utilized to provide an additional layer of security known as physical layer security.

Manuscript received January 19, 2017; accepted April 22, 2017. Date of publication April 12, 2017; date of current version May 22, 2017. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Chandra R. Murthy. This work was supported in part by the National Natural Science Foundation of China under Grant 61471143 and in part by the Science and Technology Plan Projects of the Ministry of Public Security under Grant 2015GABJC37. This paper was presented in part at the 2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications [1]. *(Corresponding author: Yingbo Hua.)*

L. Chen was with the Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA. He is now with the Communications Research Center, Harbin Institute of Technology, Harbin 150001, China (e-mail: leichen@hit.edu.cn).

Q. Zhu and Y. Hua are with the Department of Electrical and Computer Engineering, University of California, Riverside, CA 92521 USA (e-mail: qzhu005@ucr.edu; yhua@ece.ucr.edu).

W. Meng is with the Communications Research Center, Harbin Institute of Technology, Harbin 150001, China (e-mail: wxmeng@hit.edu.cn).

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

Digital Object Identifier 10.1109/TSP.2017.2701318

A basic goal of physical layer security is to ensure a sufficient level of secrecy capacity against eavesdroppers while maintaining a desired level of reception quality for desired receivers. The research in this area includes both information theoretical study [3]–[8] and signal processing study [9]–[26]. The former mostly focuses on bounds and asymptotical limits while the latter tends to be innovative in the design of architectures and algorithms. This paper is about the latter. However, the exact classification of a work on physical layer security into one of these two categories is not always suitable.

The signal processing study of physical layer security includes those on transmit antenna beamforming which steers transmitted signal towards desired receivers and away from eavesdroppers [9], [10], artificial noise injection which deteriorates the signal-to-interference-plus-noise ratio (SINR) at eavesdroppers [11]–[13], and cooperative relays which perform beamforming, jamming or both [14]–[16]. More recently, there have been research activities to utilize full-duplex radio for enhanced physical layer security [19]–[25]. A latest implementation of full duplex radio for short range communications is reported in [27]. Such a radio that can transmit and receive at the same time and same frequency can be used not only for increased spectral efficiency but also for increased security, the latter of which is the focus of this paper.

We will first consider a three-node multi-subcarrier network consisting of a source (*Alice*), a full-duplex destination (*Bob*) and an eavesdropper (*Eve*). *Bob* is able to receive the signal from *Alice* and at the same time to transmit a jamming noise against *Eve*. We will study how to allocate transmission power in the subcarriers for both *Alice* and *Bob* to maximize the secrecy capacity against *Eve*. We will also consider extensions to multiple full-duplex destinations and multiple sources.

In practice, the three-node network considered here may correspond to a special operation where for example a key is distributed from *Alice* to *Bob*, and *Eve* is considered illegitimate to receive the key. But under normal circumstances where for example some public information is shared, all nodes can communicate friendly with each other and their channel state information be made available to all. For this reason, we will assume in this paper that *Alice* and *Bob* know their channel amplitudes with respect to *Eve* during such a special operation. We will utilize the knowledge of channel amplitudes in computing power allocations for maximum secrecy capacity. We will focus on developing fast algorithms for this purpose. Such a fast algorithm can be used for real-time applications in mobile scenario.

Unlike [19], [21], [23], we take into account the residual self-interference at *Bob*. It is known that even with the state of the art radio self-interference cancellation methods, there is always certain amount of residual self-interference [28]–[32].

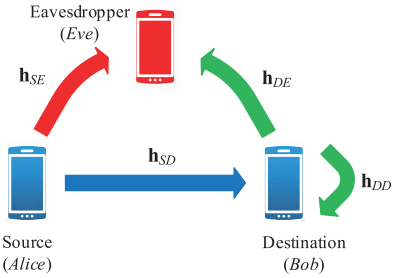



Fig. 1. A three-node wireless network with a full-duplex destination.

Another unique feature of this work is that we consider both power and rate constraints in maximizing the secrecy capacity while most of the prior works on physical layer security such as [8]–[11], [13], [16]–[18], [20], [21], [23] only considered power constraints. Obviously, in order to transmit a packet from *Alice* to *Bob*, a preselected data rate for the packet should be guaranteed.

Much of this paper is a development of fast algorithms to solve non-convex optimization problems. These problems cannot be solved directly by such optimization software as CVX. We exploit in great depth the problem structures via the Karush-Kuhn-Tucker (KKT) conditions. For several non-convex subproblems, we are able to find their optimal solutions by solving the KKT conditions.

The rest of this paper is organized as follows. In Section II, we show in detail the problem description of the three-node network under consideration and some propositions useful to simplify the problem. In Section III, we formulate and solve the problem of power allocation to maximize the secrecy capacity of the network subject to power-only constraints, which provides important preparation for the rest of this paper. An asymptotic limit of the secrecy capacity subject to high power is also given in Section III. In Section IV, we consider the above mentioned problem but subject to both power and rate constraints. We consider the extension to multiple destinations in Section V, and the extension to multiple sources in Section VI. The simulation results are presented in Section VII. Several proofs are detailed in appendices.

## II. A Three-Node Network

A three-node wireless network is shown as Fig. 1. This is an ad hoc network where every node uses the same frequency band to communicate with other nodes. In this network (or a snapshot of this network), the source (*Alice*) plans to transmit some sensitive information to its legitimate destination (*Bob*) while a potential eavesdropper (*Eve*) is to be prevented from "wiretapping" the transmission. We assume that the channel on each link consists of $N$ orthogonal subcarriers and the fading on each subcarrier is flat. To actively deteriorate the SINR at *Eve*, *Bob* will use its full-duplex capacity to transmit interference noise in the same channel where at the same time it receives the signal from *Alice*. Potentially, all nodes could work in full duplex. But this would make the network much more complicated. If all nodes only work in half duplex, then this is a conventional network for which the conventional methods can be applied. The setting of our problems is somewhere in between the two extremes.

Let $\mathbf{x}_S(t) \in \mathbb{C}^{N\times 1}$ be the signal vector (of i.i.d. symbols of zero mean and unit variance) to be transmitted by *Alice* and $\mathbf{x}_D(t) \in \mathbb{C}^{N\times 1}$ be the jamming noise vector (of i.i.d. symbols of zero mean and unit variance) to be transmitted by *Bob*. Then the signal vectors to be received by *Bob* and *Eve* can be respectively expressed as:

$$\mathbf{y}_D(t) = \mathbf{h}_{SD} \circ \sqrt{\mathbf{p}_S} \circ \mathbf{x}_S(t) + \sqrt{\rho}\mathbf{h}_{DD} \circ \sqrt{\mathbf{p}_D} \circ \mathbf{x}_D(t) + \mathbf{n}_D(t),$$

$$\mathbf{y}_E(t) = \mathbf{h}_{SE} \circ \sqrt{\mathbf{p}_S} \circ \mathbf{x}_S(t) + \mathbf{h}_{DE} \circ \sqrt{\mathbf{p}_D} \circ \mathbf{x}_D(t) + \mathbf{n}_E(t),$$

where $\mathbf{h}_{SD} \in \mathbb{C}^{N\times 1}$ is the channel response vector from *Alice* to *Bob*, $\mathbf{h}_{SE} \in \mathbb{C}^{N\times 1}$ is that from *Alice* to *Eve*, $\mathbf{h}_{DE} \in \mathbb{C}^{N\times 1}$ is that from *Bob* to *Eve*, and $\mathbf{h}_{DD} \in \mathbb{C}^{N\times 1}$ is the self-interference channel response vector of *Bob*. $\mathbf{p}_S \in \mathbb{R}_{\geq 0}^{N\times 1}$ and $\mathbf{p}_D \in \mathbb{R}_{\geq 0}^{N\times 1}$ are the transmitting power vectors of *Alice* and *Bob* respectively; $\sqrt{\mathbf{p}_S}$ and $\sqrt{\mathbf{p}_D}$ denote the element-wise square roots of $\mathbf{p}_S$ and $\mathbf{p}_D$, respectively. Both $\mathbf{n}_D(t) \in \mathbb{C}^{N\times 1}$ and $\mathbf{n}_E(t) \in \mathbb{C}^{N\times 1}$ are independent white Gaussian noise of zero mean and unit variance. The symbol '$\circ$' denotes the *Hadamard product* (i.e., element-wise product). And $\rho$ is the self-interference attenuation factor.

Let $p_S^{(n)}$ denote the $n$th element of $\mathbf{p}_S$, and other similar notations are defined accordingly. The SINRs of the $n$th subcarrier at *Bob* and *Eve* are respectively:

$$\gamma_D^{(n)} = \frac{A_n x_n}{1 + B_n y_n} \quad \text{and} \quad \gamma_E^{(n)} = \frac{C_n x_n}{1 + D_n y_n}, \tag{1}$$

where $A_n = |h_{SD}^{(n)}|^2$, $B_n = \rho|h_{DD}^{(n)}|^2$, $C_n = |h_{SE}^{(n)}|^2$, $D_n = |h_{DE}^{(n)}|^2$, $x_n = p_S^{(n)}$ and $y_n = p_D^{(n)}$.

Note that we will assume that the channel amplitudes $A_n$, $B_n$, $C_n$ and $D_n$, $\forall n$ are available for computing power allocations. None of the channel phases is required. In practice, the amplitudes are much slower in changing and much easier to estimate than the phases are. Since the channel amplitudes have a large coherence time, any data transmission from *Eve* to *Alice* and *Bob* could allow *Alice* and *Bob* to know the required channel amplitude responses from *Alice* and *Bob* to *Eve* via the reciprocal property. We also assume that *Alice* and *Bob* are fully cooperative.

The secrecy capacity of the system in bits per channel use is known as [33]:

$$\mathcal{R}_s(\mathbf{x}, \mathbf{y}) = \frac{1}{N}\sum_{n=1}^{N} \max\{0, \Delta\mathcal{R}_n(x_n, y_n)\}, \tag{2}$$

where $\Delta\mathcal{R}_n(x_n, y_n) = \log(1 + \gamma_D^{(n)}) - \log(1 + \gamma_E^{(n)})$. The pre-multiplier $1/N$ in (2) should be removed if the $N$ subcarriers are spatial subcarriers (due to use of multiple antennas) instead of temporal subcarriers (due to time and/or frequency divisions). This paper is concerned about maximizing the secrecy capacity $\mathcal{R}_s(\mathbf{x}, \mathbf{y})$ through power allocations at both *Alice* and *Bob*. And most of the technical details are aimed to reduce the computational complexity.

In relation to $\mathcal{R}_s(\mathbf{x}, \mathbf{y})$, we define $\tilde{\mathcal{R}}_s(\mathbf{x}, \mathbf{y})$ as:

$$\tilde{\mathcal{R}}_s(\mathbf{x}, \mathbf{y}) = \max\{0, \Delta\mathcal{R}(\mathbf{x}, \mathbf{y})\}, \tag{3}$$

where $\Delta\mathcal{R}(\mathbf{x}, \mathbf{y}) = \frac{1}{N}\sum_{n=1}^{N} \Delta\mathcal{R}_n(x_n, y_n)$.

Shown below are three important propositions. *Proposition 1* will be used to simplify the secrecy capacity as an objective function from a form of "summation of maximums" to a form of "maximum of sums". *Proposition 2* is a precursor of *Proposition 3*, the latter of which provides a necessary condition to determine whether a subcarrier at *Bob* needs to be allocated with nonzero power.

*Proposition 1:* $\mathcal{R}_s(\mathbf{x},\mathbf{y})$ is no less than $\tilde{\mathcal{R}}_s(\mathbf{x},\mathbf{y})$, and $\max(\mathcal{R}_s(\mathbf{x},\mathbf{y})) = \max(\tilde{\mathcal{R}}_s(\mathbf{x},\mathbf{y}))$ subject to $\sum_{n=1}^{N} x_n \le P_S$ and $\sum_{n=1}^{N} y_n \le P_D$.

*Proof:* See Appendix A. ■

*Proposition 2:* For any given $x_n \in (0,+\infty)$, there is at most one stationary point for $\Delta\mathcal{R}_n(x_n,y_n)$ with regard to $y_n \in (0,+\infty)$.

*Proof:* See Appendix B. ■

*Proposition 3:* For any given $x_n, \forall n$, a necessary condition that the optimal value of $y_n$ is nonzero is that $\frac{B_n}{D_n} < 1$ and $\frac{A_n}{C_n} > \frac{B_n}{D_n}$.

*Proof:* See Appendix C. ■

## III. Power Allocation Under Power Constraints

In this section, we consider the problem of power allocation for maximization of secrecy capacity subject to power-only constraints. Specifically, we consider the following problem:

$$\max_{\mathbf{x},\mathbf{y}} \quad \mathcal{R}_s(\mathbf{x},\mathbf{y}) \tag{4a}$$

$$s.t. \quad \sum_{n=1}^{N} x_n \le P_S, \sum_{n=1}^{N} y_n \le P_D,$$
$$x_n \ge 0, y_n \ge 0, \forall n \in \mathsf{N}. \tag{4b}$$

where we assume the power budget $P_S$ at source and the power budget $P_D$ at destination. Note that $\mathsf{N} \doteq \{1,\ldots,N\}$.

With *Proposition 1*, the power allocation problem (4a) can be transformed equivalently to:

$$\max_{\mathbf{x},\mathbf{y}} \quad \Delta\mathcal{R}(\mathbf{x},\mathbf{y})$$
$$s.t. \quad Power\ constraint\ (4b). \tag{5}$$

Solving this non-convex optimization problem (5) directly is still difficult. We will treat this problem in two phases: in phase one, we optimally allocate the source power for a given destination power vector; and in phase two, we optimally allocate the destination power for a given source power vector. The two phases will be iterated until convergence. Note that since the two-phase iteration algorithm increases the same (upper bounded) objective function at each iteration and each phase, this algorithm is guaranteed to be locally convergent. Such a property is a special case of one that is discussed in [34].

In the following two sections, the two phases of the two-phase algorithm are discussed separately in detail.

### A. Source Power Allocation

With a fixed destination power allocation, the source power allocation problem from (5) is:

$$\max_{\mathbf{x}} \quad \frac{1}{N}\sum_{n=1}^{N}\log(1+\alpha_n x_n) - \frac{1}{N}\sum_{n=1}^{N}\log(1+\beta_n x_n)$$
$$s.t. \quad \sum_{n=1}^{N} x_n \le P_S, x_n \ge 0, \forall n \in \mathsf{N}. \tag{6}$$

where

$$\alpha_n = \frac{A_n}{1+B_n y_n} \quad \text{and} \quad \beta_n = \frac{C_n}{1+D_n y_n}. \tag{7}$$

The above problem is still non-convex due to the non-convex cost function. But we will be able to find the solution to this problem by finding the solution to its KKT conditions as follows.[1] The Lagrangian function of the problem can be written as:

$$\mathcal{L}(\mathbf{x},\boldsymbol{\lambda},\upsilon) = -\frac{1}{N}\sum_{n=1}^{N}\log\left(\frac{1+\alpha_n x_n}{1+\beta_n x_n}\right) - \boldsymbol{\lambda}^T\mathbf{x} + \upsilon\left(\sum_{n=1}^{N} x_n - P_S\right). \tag{8}$$

The solution to the problem (6) must satisfy the following KKT conditions [35]:

$$\begin{cases} \frac{\partial\mathcal{L}}{\partial x_n} = -\varphi_n(x_n) - \lambda_n + \upsilon = 0, \\ \sum_{n=1}^{N} x_n \le P_S, \upsilon \ge 0, \upsilon(\sum_{n=1}^{N} x_n - P_S) = 0, \\ x_n \ge 0, \lambda_n \ge 0, \lambda_n x_n = 0, \forall n \in \mathsf{N}, \end{cases} \tag{9}$$

where

$$\varphi_n(x_n) = \frac{1}{N}\frac{\alpha_n}{1+\alpha_n x_n} - \frac{1}{N}\frac{\beta_n}{1+\beta_n x_n}. \tag{10}$$

Before solving these KKT conditions, we introduce the following proposition:

*Proposition 4:* Let $\mathbf{x}^\dagger$ be the solution of the source power allocation phase. Then, for any $n$, if $\alpha_n \le \beta_n$, then $x_n^\dagger = 0$. Furthermore, we have either $\sum_{n=1}^{N} x_n^\dagger = 0$ or $\sum_{n=1}^{N} x_n^\dagger = P_S$.

*Proof:* See Appendix D. ■

So, we have $x_n^\dagger = 0$ for $n \in \{n|\alpha_n \le \beta_n, n \in \mathsf{N}\}$, and for the remaining subcarriers, the power allocation results can be obtained by solving the following simplified KKT conditions:

$$\begin{cases} \frac{\partial\mathcal{L}}{\partial x_n} = -\varphi_n(x_n) - \lambda_n + \upsilon = 0, \\ x_n \ge 0, \lambda_n \ge 0, \lambda_n x_n = 0, \forall n \in \Theta_y, \\ \sum_{n\in\Theta_y} x_n = P_S, \Theta_y \doteq \{n|\alpha_n > \beta_n, n \in \mathsf{N}\}. \end{cases} \tag{11}$$

It can be verified that $\frac{\partial\varphi_n(x_n)}{\partial x_n} < 0, \forall n \in \Theta_y$. From the first equation in (11), we know that $\upsilon$ is a decreasing function of $x_n, \forall n \in \Theta_y$. Thus, these simplified KKT conditions can be solved by a bisection search algorithm as shown in the table of Algorithm 1[2]. This algorithm is similar to a solution in [33].

[1] In general, the KKT conditions are necessary conditions for the optimal solution. But for all convex problems and some non-convex problems, the KKT conditions are both necessary and sufficient conditions for the optimal solution. When the solution to the KKT conditions is unique, it must be the optimal solution to the original problem. When KKT conditions (of a non-convex problem) have more than one solutions, one has to be innovative to exploit other properties associated with the optimal solution to rule out the non-optimal solutions if possible.

[2] For KKT conditions, all the Lagrange multipliers (such as $\upsilon$ and $\lambda_n$) associated with the inequalities must be non-negative. For a given $\upsilon$ and $\lambda_n = 0$, the solution to $\varphi_n(x_n^\dagger) = \upsilon$ may or may not be positive. If there is a positive solution of $x_n$, the corresponding $\lambda_n$ is zero as assumed in the first place. If there is no positive solution of $x_n$, the corresponding optimal solution of $x_n$ is zero and the corresponding $\lambda_n$ should be positive (although its actual value is now useless).Also, $\varphi_n(x_n^\dagger) = \upsilon$ is equivalent to an quadratic equation which has two roots, only one of the two roots can be greater than or equal to 0, which is the valid solution.

**Algorithm 1:** Source power allocation algorithm—Solution to (11).

**Input:**
$A_n, B_n, C_n, D_n, y_n, \forall n \in \mathsf{N}$; Source power constraint $P_S$; Accuracy threshold $\varepsilon$.
**Output:**
$\upsilon^+ = \max_{n\in\Theta_y}\{\varphi_n(0)\}$; $\upsilon^- = \max_{n\in\Theta_y}\{\varphi_n(P_S)\}$;

```
Temporary variable μ = 0; x_1^† = x_2^† =, ..., = x_N^† = 0.
while (|P_S − μ| > ε) do
    υ = (υ^− + υ^+)/2;
    for n ∈ Θ_y do
        if υ ≥ φ_n(0) then
            x_n^† = 0;
        else
            Solve φ_n(x_n^†) = υ (By solving an equivalent quadratic equation. There is only one positive solution to this equation due to the nature of the function φ_n(x_n).) and set x_n^† = x_n;
        end if
    end for
    μ = Σ_{n∈Θ_y} x_n^†;
    if μ > P_S then
        υ^− = υ;
    else
        υ^+ = υ;
    end if
end while
return x_1^†, x_2^†, ..., x_N^†.
```

### B. Destination Power Allocation

With a given source power allocation, the destination power allocation problem from (5) is as follows:

$$\max_{\mathbf{y}} \quad \frac{1}{N}\sum_{n=1}^{N}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right)-\log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right)$$
$$s.t. \quad \sum_{n=1}^{N} y_n \le P_D, y_n \ge 0, \forall n \in \mathsf{N}. \tag{12}$$

By *Proposition 3*, the above problem is equivalent to:

$$\max_{\mathbf{y}} \quad \frac{1}{N}\sum_{n\in\Phi}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right)-\log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right)$$
$$s.t. \quad \sum_{n\in\Phi} y_n \le P_D, y_n \ge 0, \forall n \in \Phi, \tag{13}$$

where

$$\Phi \doteq \left\{ n | n \in \mathsf{N}, \frac{B_n}{D_n} < 1, \frac{A_n}{C_n} > \frac{B_n}{D_n} \right\}, \tag{14}$$

and $y_n = 0, \forall n \notin \Phi$.

The above problem is once again non-convex. To find its solution, we will consider its KKT conditions. The Lagrangian function of this problem is:

$$\mathcal{L}(\mathbf{y}, \boldsymbol{\lambda}, \upsilon) = -\frac{1}{N}\sum_{n\in\Phi}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right)-\log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right) - \boldsymbol{\lambda}^T\mathbf{y} + \upsilon\left(\sum_{n\in\Phi} y_n - P_D\right). \tag{15}$$

The KKT conditions of (13) are:

$$\begin{cases} \frac{\partial\mathcal{L}}{\partial y_n} = -\psi_n(y_n) - \lambda_n + \upsilon = 0, \\ \sum_{n\in\Phi} y_n \le P_D, \upsilon \ge 0, \upsilon(\sum_{n\in\Phi} y_n - P_D) = 0, \\ y_n \ge 0, \lambda_n \ge 0, \lambda_n y_n = 0, \quad \forall n \in \Phi, \end{cases} \tag{16}$$

where

$$\psi_n(y_n) = \frac{1}{N}\frac{\partial\Delta\mathcal{R}_n}{\partial y_n} = \frac{1}{N}\left(\frac{B_n}{1+B_n y_n + A_n x_n} - \frac{B_n}{1+B_n y_n} - \frac{D_n}{1+D_n y_n + C_n x_n} + \frac{D_n}{1+D_n y_n}\right). \tag{17}$$

Appendix C shows that for any $n \in \Phi$, $\Delta\mathcal{R}_n$ has four unique cases/patterns as shown in Fig. 12(b) (i.e., case I, case II, case III and case IV). Since $\psi_n(y_n) = \frac{1}{N}\frac{\partial\Delta\mathcal{R}_n}{\partial y_n}$, then $\psi_n(y_n)$ has two kinds of patterns as shown in Fig. 2. The first kind corresponds to the cases II, III and IV in Fig. 12(b), for which there must be nonzero power allocation. From (17), we know that the region of interest for $y_n$ is where $\psi_n(y_n) > 0$. In this region, $\psi_n(y_n)$ is decreasing with increasing $y_n$:

*Proposition 5:* $\psi_n(y_n)$ is decreasing with increasing $y_n$ as long as $\psi_n(y_n) > 0$ if $\frac{A_n}{B_n} > \frac{B_n}{D_n}$ and $\frac{B_n}{D_n} < 1$.

*Proof:* See Appendix E. ■

Whereas, the second kind corresponds to the case I in Fig. 12(b), for which the optimal $y_n$ should obviously be set to zero. So the KKT conditions in (16) can be solved with a bisection search of $\upsilon$ as shown in Algorithm 2.

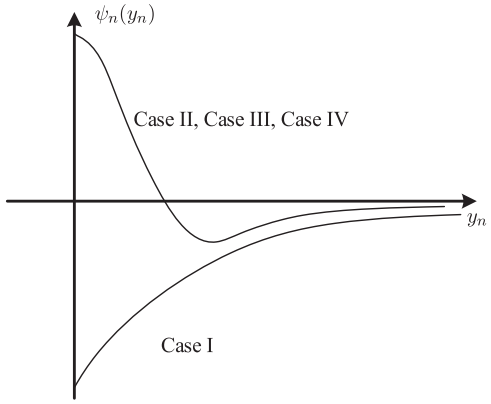



Fig. 2. Property of $\psi_n(y_n)$ derived from the cases I-IV in Fig. 12(b).

### C. Asymptotic Performance Analysis

In this section, we present the achievable upper bound on the secrecy capacity of the three-node network when the power budget is large. For the subcarrier $n \in \Phi$ and a given source power $x_n$, the optimal destination power $y_n^*$ is given by (based

**Algorithm 2:** Destination allocation algorithm—Solution to (16).

**Input:**
$A_n, B_n, C_n, D_n, x_n, \forall n \in \Phi$; Destination power constraint $P_D$; Accuracy threshold $\varepsilon$.
**Output:**
$\upsilon^+ = \max_{n\in\Phi}\{\psi_n(0)\}$; $\upsilon^- = \max\{0, \max_{n\in\Phi}\{\psi_n(P_D)\}\}$;

**for** $n \in \Phi$ **do**
  **if** $\psi_n(0) \le 0$ **then**
    $y_n^\dagger = 0$;
  **else**
    Solve $\psi_n(y_n^\dagger) = 0$ by solving an equivalent 2nd-order polynomial which has only one positive root;
  **end if**
**end for**
**if** ($\sum y_n^\dagger > P_D$ or $\upsilon^- > 0$) **then**
  Temporary variable $\mu = 0$; $y_n^\dagger = 0, \forall n \in \Phi$.
  **while** ($|P_D - \mu| > \varepsilon$) **do**
    $\upsilon = \frac{\upsilon^- + \upsilon^+}{2}$;
    **for** $n \in \Phi$ **do**
      **if** $\upsilon \ge \psi_n(0)$ **then**
        $y_n^\dagger = 0$;
      **else**
        Solve $\psi_n(y_n^\dagger) = \upsilon$ by solving an equivalent 4th-order polynomial which has only one positive root. The roots of general polynomials of up to the 4th-order have closed-form expressions;
      **end if**
    **end for**
    $\mu = \sum_{n\in\Phi} y_n^\dagger$;
    **if** $\mu > P_D$ **then**
      $\upsilon^- = \upsilon$;
    **else**
      $\upsilon^+ = \upsilon$;
    **end if**
  **end while**
**end if**
**return** $y_n^\dagger, \forall n \in \Phi$.

on the solution of (B.2)):

$$y_n^* = \frac{-(A_n - C_n) + \sqrt{(A_n - C_n)^2 - \frac{A_n D_n - B_n C_n}{B_n D_n} T_n(x_n)}}{A_n D_n - B_n C_n}, \tag{18}$$

where $T_n(x) = A_n B_n - C_n D_n + (B_n - D_n) A_n C_n x$. Then, for large $x_n$, we have that $y_n^* = \omega_n x_n^{\frac{1}{2}}$, where $\omega_n = \sqrt{\frac{(D_n - B_n) A_n C_n}{(A_n D_n - B_n C_n) B_n D_n}}$.

So for this subcarrier, the achievable upper bound of the secrecy capacity is:

$$\begin{aligned}\mathcal{R}_n^\dagger &= \lim_{x_n \to +\infty} \left( \log\left(1 + \frac{A_n x_n}{1 + B_n y_n^*}\right) - \log\left(1 + \frac{C_n x_n}{1 + D_n y_n^*}\right)\right) \\ &= \lim_{x_n \to +\infty} \left( \log\left(\frac{1 + B_n \omega_n x_n^{\frac{1}{2}} + A_n x_n}{1 + D_n \omega_n x_n^{\frac{1}{2}} + C_n x_n}\right) + \log\left(\frac{1 + D_n \omega_n x_n^{\frac{1}{2}}}{1 + B_n \omega_n x_n^{\frac{1}{2}}}\right)\right) \\ &= \log\left(\frac{A_n}{C_n}\right) + \log\left(\frac{D_n}{B_n}\right). \end{aligned} \tag{19}$$

For $n \notin \Phi$, we have $y_n = 0$ and hence:

$$\mathcal{R}_n^\dagger = \max\left\{0, \log\left(\frac{A_n}{C_n}\right)\right\}. \tag{20}$$

Therefore, the achievable upper bound of the secrecy capacity for the entire system is:

$$\begin{aligned}\mathcal{R}^\dagger &= \sum_{n\in\Phi} \left( \log\left(\frac{A_n}{C_n}\right) + \log\left(\frac{D_n}{B_n}\right)\right) + \sum_{n\notin\Phi} \max\left\{0, \log\left(\frac{A_n}{C_n}\right)\right\} \\ &= \sum_{n=1}^{N} \max\left\{0, \log\left(\frac{A_n}{C_n}\right) + \max\left\{0, \log\left(\frac{D_n}{B_n}\right)\right\}\right\}. \end{aligned} \tag{21}$$

In this upper bound, the term $\max\{0, \log(\frac{D_n}{B_n})\}$ is the contribution from the full-duplex transmission in the destination. The necessary and sufficient condition for the full-duplex transmission to improve the secrecy capacity in the $n$th subcarrier (where both $x_n$ and $y_n$ are large) is $D_n > B_n$. We also see that the less is the self-interference, the more is the secrecy capacity generated.

### D. Computational Complexity

Let $\varepsilon$ denote the required accuracy for the multiplier $\upsilon$ for both phases. Assuming that $N_{two-phase}$ iterations are required before the two-phase iteration algorithm converges. Then, the order of the complexity of the (bisection-based) two-phase algorithm in terms of $\varepsilon$ and $N_{two-phase}$ is $\mathcal{O}(2N_{two-phase} \log_2(\frac{1}{\varepsilon}))$. A brute-force search of the multiplier $\upsilon$ would have $\mathcal{O}(2N_{two-phase}\frac{1}{\varepsilon})$ as the complexity order. Note that, the simulation results[3] show that the typical value of $N_{two-phase}$ is around 5.

## IV. Power Allocation under Power and Rate Constraints

In this section, we consider power allocation for maximizing the secrecy capacity of the three-node network subject to power constraints as well as a source-to-destination data rate constraint. Namely, we consider the following non-convex problem:

$$\begin{aligned} \max_{\mathbf{x},\mathbf{y}} \quad & \frac{1}{N} \sum_{n\in\Theta_y} \Delta\mathcal{R}_n(x_n, y_n) \\ s.t. \quad & \frac{1}{N} \sum_{n=1}^{N} \log\left(1 + \frac{A_n x_n}{1 + y_n B_n}\right) \ge \mathcal{C}_{SD}, \\ & Power\ constraint\ (4b). \end{aligned} \tag{22}$$

where $\mathcal{C}_{SD}$ is the required source-to-destination rate. (In the scenario of the key transmission, this rate should be the rate of the data packet containing the key.) The set $\Theta_y$ is the same set defined in (11), and $\Delta\mathcal{R}_n(x_n, y_n) < 0, \forall n \notin \Theta_y$ (which contribute zero to the secrecy capacity). This is why the sum in the objective function is over $n \in \Theta_y$. However, due to the rate constraint, the optimal $x_n$ may be positive for some $n \notin \Theta_y$. So, the sum in the rate constraint must still be done over all $n \in \mathsf{N}$. The larger is the secrecy capacity (the first line in

[3]The iteration stops when the normalized difference between the current result and the previous result is less than $10^{-2}$.

(22)), the more secure is a packet with that data rate from the source to the destination (the second line in (22)). Depending on the channel conditions, it is possible that some subcarriers are not secure (i.e., $\Delta\mathcal{R}_n(x_n, y_n) \leq 0$ for some $n$). But as long as $\mathcal{C}_S \doteq \frac{1}{N}\sum_{n\in\mathsf{N}} \max(\Delta\mathcal{R}_n(x_n, y_n), 0) > 0$, there are always some secure subcarriers, and a packet encoded across all the subcarriers to meet the secrecy capacity $\mathcal{C}_S$ (and the rate constraint $\mathcal{C}_{SD}$) is said to be secure with the secrecy capacity $\mathcal{C}_S$.

Although the rate constraint introduces a complex situation where $x_n, \forall n$ and $y_n, \forall n$ now have a shared constraint, the two-phase iteration method is still applicable. Each of the two phases is discussed next.

### A. Source Power Allocation

In this phase, $\mathbf{y}$ is fixed and the optimization problem (22) reduces to the following *convex* problem:

$$\begin{aligned} \max_{\mathbf{x}} \quad & \frac{1}{N}\sum_{n\in\Theta_y} [\log(1+\alpha_n x_n) - \log(1+\beta_n x_n)] \\ s.t. \quad & \frac{1}{N}\sum_{n=1}^{N} \log(1+\alpha_n x_n) \geq \mathcal{C}_{SD}, \\ & \sum_{n=1}^{N} x_n \leq P_S, x_n \geq 0, \forall n \in \mathsf{N}. \end{aligned} \tag{23}$$

where $\alpha_n$ and $\beta_n$ are defined in (7). The Lagrangian function of this problem is:

$$\begin{aligned} \mathcal{L}(\mathbf{x}, \lambda, \boldsymbol{\mu}, \upsilon) = & -\frac{1}{N}\sum_{n\in\Theta_y} (\log(1+\alpha_n x_n) - \log(1+\beta_n x_n)) \\ & + \lambda\left(\mathcal{C}_{SD} - \frac{1}{N}\sum_{n=1}^{N}\log(1+\alpha_n x_n)\right) - \boldsymbol{\mu}^T\mathbf{x} + \upsilon\left(\sum_{n=1}^{N} x_n - P_S\right). \end{aligned} \tag{24}$$

The KKT conditions of (23) are

$$\begin{cases} \frac{\partial\mathcal{L}}{\partial x_n} = -\bar{\varphi}_n(x_n) - \frac{\lambda}{N}\frac{\alpha_n}{1+\alpha_n x_n} - \mu_n + \upsilon = 0, \\ \lambda \geq 0, \frac{1}{N}\sum_{n=1}^{N}\log(1+\alpha_n x_n) \geq \mathcal{C}_{SD}, \\ \lambda(\frac{1}{N}\sum_{n=1}^{N}\log(1+\alpha_n x_n) - \mathcal{C}_{SD}) = 0, \\ x_n \geq 0, \mu_n \geq 0, \mu_n x_n = 0, \forall n \in \mathsf{N}, \\ \upsilon \geq 0, \sum_{n=1}^{N} x_n \leq P_S, \upsilon(\sum_{n=1}^{N} x_n - P_S) = 0, \end{cases} \tag{25}$$

where $\bar{\varphi}_n(x_n) = \varphi_n(x_n)$ as defined by (10) for $n \in \Theta_y$, and $\bar{\varphi}_n(x_n) = 0$ for $n \notin \Theta_y$. From the first equation in (25), we see that if $\lambda$ is fixed, $\upsilon$ is a decreasing function of $x_n$, and if $\upsilon$ is fixed, $\lambda$ is an increasing function of $x_n$. Hence, the conditions of (25) can be solved by a two-dimensional bisection search as summarized in the table of Algorithm 3. The bisection search of $\upsilon$ is to meet the power constraint, and the bisection search of $\lambda$ is to meet the rate constraint. For each given pair of $\upsilon$ and $\lambda$, the first equation in (25) is equivalent to a quadratic equation of $x_n$ and hence has a closed-form solution for $x_n$.

**Algorithm 3:** Algorithm to solve the problem (23) by solving the KKT conditions (25), which uses 2-D bisection search for $\upsilon$ and $\lambda$.

**Input:**
$A_n, B_n, C_n, D_n, y_n, \forall n \in \mathsf{N}$; Source power constraint $P_S$; SD capacity constraint $\mathcal{C}_{SD}$; Accuracy threshold $\varepsilon, \zeta$.

**Output:**

1: Set $\lambda = 0$ (i.e., removing the rate constraint), do the search for $\upsilon$ and $\mathbf{x}$ (similar to Algorithm 1);
2: Calculate SD capacity $C(\mathbf{x})$;
3: **if** $C(\mathbf{x}) > \mathcal{C}_{SD}$ **then**
4: **return** $\mathbf{x}$ (This means that the rate constraint is satisfied by the solution without the rate constraint even imposed.);
5: **else**
6: **Two-Dimensional bisection search**: Do bisection search for $\upsilon > 0$ to meet the power constraint up to the precision $\varepsilon$. For each given $\upsilon$, do bisection search for $\lambda > 0$ to meet the rate constraint up to the precision $\zeta$. For each given pair of $\upsilon$ and $\lambda$, find $x_n \geq 0$ as the solution to the first equation in (25) for each $n \in \mathsf{N}$.
7: **return** $\mathbf{x}$.
8: **end if**

### B. Destination Power Allocation

In this phase, $\mathbf{x}$ is fixed and the problem (22) reduces to the following (still non-convex) problem:

$$\begin{aligned} \max_{\mathbf{y}} \quad & \frac{1}{N}\sum_{n\in\Theta_y}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right) - \log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right) \\ s.t. \quad & \frac{1}{N}\sum_{n=1}^{N}\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right) \geq \mathcal{C}_{SD}, \\ & \sum_{n=1}^{N} y_n \leq P_D, y_n \geq 0, \forall n \in \mathsf{N}. \end{aligned} \tag{26}$$

By *Proposition 3*, the problem (26) can be rewritten as

$$\begin{aligned} \max_{\mathbf{y}} \quad & \frac{1}{N}\sum_{n\in\Psi_y}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right) - \log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right) \\ s.t. \quad & \frac{1}{N}\sum_{n\in\Psi_y}\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right) \geq \tilde{\mathcal{C}}_{SD}, \\ & \sum_{n\in\Psi_y} y_n \leq P_D, y_n \geq 0, \forall n \in \Psi_y, \end{aligned} \tag{27}$$

where

$$\Psi_y = \Theta_y \cap \Phi, \tag{28}$$

$$\tilde{\mathcal{C}}_{SD} = \mathcal{C}_{SD} - \frac{1}{N}\sum_{n\in\Psi_y^{\perp}}\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right),$$

$$\Psi_y^{\perp} = \{n | n \in \mathsf{N}, n \notin \Psi_y\}, \tag{29}$$

and $y_n = 0, \forall n \in \Psi_y^{\perp}$.

Because the set $\Psi_y$ is a function of $y_n, \forall n$, we will use the following approach to determine $\Psi_y$:

We start with the largest possible set of $\Psi_y$ which is $\Psi_y^{(0)} = \Phi$. Then, for any given $\Psi_y = \Psi_y^{(k)}$, solve the problem (27), substitute the solution $\mathbf{y}^{(k)}$ into the equation (28) to obtain a new $\Psi_y^{(k+1)}$. If $\Psi_y^{(k)} = \Psi_y^{(k+1)}$, stop, and $\mathbf{y}^{(k)}$ is the solution; otherwise, let $\Psi_y = \Psi_y^{(k+1)}$, and continue the iteration.

Now the main challenge is how to solve the problem (27) with a given $\Psi_y$. Since solving the exact KKT conditions of (27) is very tedious even if feasible, we will now use a sequential convex programming (SCP) method [36] to relax the nonconvex rate constraint into a convex one by sequential linearization.

Let

$$F(\mathbf{y}) = \frac{1}{N}\sum_{n\in\Psi_y} \log\left(1+\frac{A_n x_n}{1+B_n y_n}\right). \tag{30}$$

By the first order Taylor's series expansion around $\mathbf{y} = \mathbf{y}^{(k)}$, $F(\mathbf{y})$ can be approximated as:

$$\begin{aligned} F_T(\mathbf{y},\mathbf{y}^{(k)}) &= F(\mathbf{y}^{(k)}) + (\nabla F(\mathbf{y}^{(k)}))^T(\mathbf{y}-\mathbf{y}^{(k)}) \\ &= F(\mathbf{y}^{(k)}) + \frac{1}{N}\sum_{n\in\Psi_y}\phi_n\cdot(y_n - y_n^{(k)}), \end{aligned} \tag{31}$$

where $\phi_n = -\frac{B_n}{1+B_n y_n^{(k)}} + \frac{B_n}{1+B_n y_n^{(k)}+A_n x_n}$.

We compute the updated estimate $\mathbf{y}^{(k+1)}$ by the following:

$$\begin{aligned} \mathbf{y}^{(k+1)} = \arg\max_{\mathbf{y}} \Bigg\{ &\frac{1}{N}\sum_{n\in\Psi_y}\Bigg(\log(1+\frac{A_n x_n}{1+B_n y_n}) \\ &- \log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\Bigg)\Bigg\} \end{aligned} \tag{32}$$

$$\begin{aligned} s.t. \quad & F_T(\mathbf{y},\mathbf{y}^{(k)}) \geq \tilde{\mathcal{C}}_{SD}, \\ & \sum_{n\in\Psi_y} y_n \leq P_D, y_n \geq 0, \forall n \in \Psi_y. \end{aligned}$$

The Lagrangian function of this problem is:

$$\begin{aligned} &\mathcal{L}(\mathbf{y},\lambda,\boldsymbol{\mu},\upsilon) = \\ &-\frac{1}{N}\sum_{n\in\Psi_y}\left(\log\left(1+\frac{A_n x_n}{1+B_n y_n}\right) - \log\left(1+\frac{C_n x_n}{1+D_n y_n}\right)\right) \\ &-\boldsymbol{\mu}^T\mathbf{y} + \upsilon\left(\sum_{n\in\Psi_y} y_n - P_D\right) + \lambda\left(\tilde{\mathcal{C}}_{SD} - F_T(\mathbf{y},\mathbf{y}^{(k)})\right). \end{aligned} \tag{33}$$

The KKT conditions of (32) are:

$$\begin{cases} \frac{\partial\mathcal{L}}{\partial y_n} = -\psi_n(y_n) - \frac{\lambda}{N}\phi_n - \mu_n + \upsilon = 0, \\ y_n \geq 0, \mu_n \geq 0, \mu_n y_n = 0, \quad \forall n \in \Psi_y, \\ \upsilon \geq 0, \sum_{n\in\Psi_y} y_n \leq P_D, \upsilon(\sum_{n\in\Psi_y} y_n - P_D) = 0, \\ \lambda \geq 0, F_T(\mathbf{y},\mathbf{y}^{(k)}) - \tilde{\mathcal{C}}_{SD} \geq 0, \lambda\left(\tilde{\mathcal{C}}_{SD} - F_T(\mathbf{y},\mathbf{y}^{(k)})\right) = 0, \end{cases} \tag{34}$$

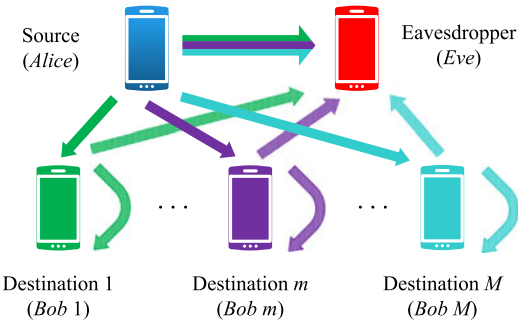



Fig. 3. A network with multiple full-duplex destinations - also referred to as "broadcast (BC)".

where $\psi_n(y_n)$ is defined in Eq. (17). From the first condition of (34), one can verify by using Proposition 5 that $\lambda$ and $\upsilon$ are each monotonic functions of $y_n$ as long as $\psi_n(y_n) > 0$. So, the KKT conditions in (34) can be solved by a 2-D bisection algorithm which is similar to Algorithm 3 but omitted here. Every new solution of $y_n, \forall n$ needs to be used to update the problem (32) until convergence.

### C. Computational Complexity

Let $\varepsilon$ denote the required accuracy in the bisection search for $\upsilon$, and $\zeta$ denote that for $\lambda$.

For source power allocation, the complexity is $\mathcal{O}(N_{2D,S}(\log_2(\frac{1}{\upsilon})+\log_2(\frac{1}{\zeta})))$ where $N_{2D,S}$ is the required number of iterations in the 2-D bisection search.

For destination power allocation, the complexity is $\mathcal{O}(N_{2D,D} N_{\Psi_y} N_{SCP}(\log_2(\frac{1}{\upsilon})+\log_2(\frac{1}{\zeta})))$ where $N_{2D,D}$ is the required number of iterations in the 2-D bisection search, $N_{SCP}$ is the number of iterations required in the SCP processing, and $N_{\Psi_y}$ is the number of iterations to determine the set $\Psi_y$ with $N_{\Psi_y} \leq N$.

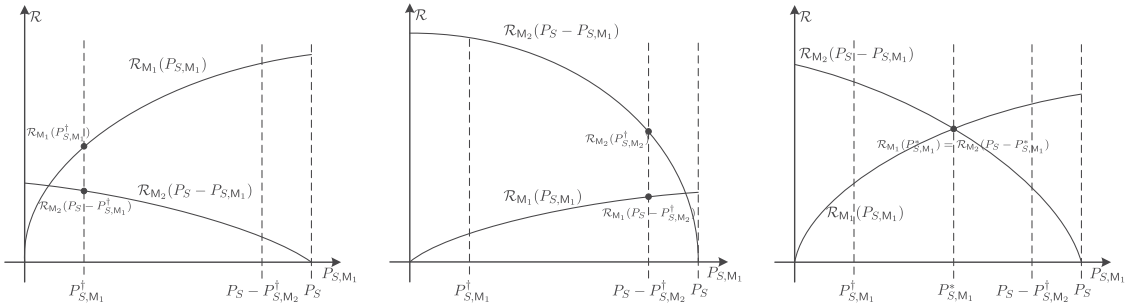
Then, the total complexity for the proposed two-phase iteration algorithm is the sum of the above two expressions scaled by $N_{two-phase}$.

We see that with both power and rate constraints, the destination power allocation typically dominates the complexity of the two-phase algorithm. The simulation results[4] show that the typical values of $N_{2D,D}$ and $N_{SCP}$ are less than 10 and that of $N_{2D,S}$ is less than 50.

## V. Extension to Multiple Destinations

In this section, we consider a network with one source, one eavesdropper and multiple full-duplex destinations as shown in Fig. 3. The source sends an independent message to each destination using an independent set of subcarriers. (This differs from a conventional definition of broadcast where all destinations use a common channel at the same time. The corresponding problem for the conventional broadcast goes beyond the scope of this paper.) Let $\mathbf{x}_S^{(m)}(t) \in \mathbb{C}^{N\times 1}$ be the message sent to the $m$th destination, and $\mathbf{y}_D^{(m)}(t) \in \mathbb{C}^{N\times 1}$ be the signal received by

[4]The iteration of SCP stops when the normalized difference between the current result and the previous result is less than the threshold $10^{-4}$. For the 2D bisection, the threshold is $10^{-3}$.




(a) Case I (line 5 to line 8) (b) Case II (line 10 to line 13) (c) Case III (line 15 to line 27)

Fig. 4. An illustration of the ideas behind Algorithm 4. In each of the subfigures, $\mathcal{R}_{\mathsf{M}_1}(P_{S,\mathsf{M}_1})$ is the rate of group $\mathsf{M}_1$ with the source power $P_{S,\mathsf{M}_1}$, and $\mathcal{R}_{\mathsf{M}_2}(P_S - P_{S,\mathsf{M}_1})$ is the rate of group $\mathsf{M}_2$ with the source power $P_S - P_{S,\mathsf{M}_1}$. $P^\dagger_{S,\mathsf{M}_1}$ is the minimum required power to meet the rate constraint for group $\mathsf{M}_1$. $P^\dagger_{S,\mathsf{M}_2}$ is that for group $\mathsf{M}_2$. The heavy dots in each of the three cases indicate the optimal solution for $P_{S,\mathsf{M}_1}$ and $P_{S,\mathsf{M}_2}$.

the $m$th destination. Then, we can write:

$$\mathbf{y}_D^{(m)}(t) = \mathbf{h}_{SD}^{(m)} \circ \sqrt{\mathbf{p}_S^{(m)}} \circ \mathbf{x}_S^{(m)}(t) + \sqrt{\rho}\mathbf{h}_{DD}^{(m)} \circ \sqrt{\mathbf{p}_D^{(m)}} \circ \mathbf{x}_D^{(m)}(t) + \mathbf{n}_D^{(m)}(t). \quad (35)$$

where $\mathbf{x}_D^{(m)}(t)$ is the interference noise sent by the $m$th full-duplex destination. The signal received by the eavesdropper is

$$\mathbf{y}_E^{(m)}(t) = \mathbf{h}_{SE}^{(m)} \circ \sqrt{\mathbf{p}_S^{(m)}} \circ \mathbf{x}_S^{(m)}(t) + \mathbf{h}_{DE}^{(m)} \circ \sqrt{\mathbf{p}_D^{(m)}} \circ \mathbf{x}_D^{(m)}(t) + \mathbf{n}_E^{(m)}(t). \quad (36)$$

So, the secrecy capacity in bits per channel use for the $m$th destination/*Bob* is:

$$\mathcal{R}_m(\mathbf{x}^{(m)}, \mathbf{y}^{(m)}) = \frac{1}{MN}\sum_{n=1}^{N} \max\{0, \Delta\mathcal{R}_{m,n}(x_{m,n}, y_{m,n})\}, \quad (37)$$

where

$$\Delta\mathcal{R}_{m,n}(x_{m,n}, y_{m,n}) = \log\left(1 + \frac{x_{m,n}A_{m,n}}{1 + y_{m,n}B_{m,n}}\right) - \log\left(1 + \frac{x_{m,n}C_{m,n}}{1 + y_{m,n}D_{m,n}}\right). \quad (38)$$

Note that $\mathbf{x}^{(m)} = \mathbf{p}_S^{(m)}, \mathbf{y}^{(m)} = \mathbf{p}_D^{(m)}, A_{m,n} = |h_{SD}^{(m,n)}|^2, B_{m,n} = |h_{DD}^{(m,n)}|^2$, $C_{m,n} = |h_{SE}^{(m,n)}|^2$, $D_{m,n} = |h_{DE}^{(m,n)}|^2$, $x_{m,n} = p_S^{(m,n)}$ and $y_{m,n} = p_D^{(m,n)}$.

For this network, we will use $\min_{m\in\mathsf{M}} \mathcal{R}_m(\mathbf{x}^{(m)}, \mathbf{y}^{(m)})$ as the objective function for power allocation where $\mathsf{M} = \{1, 2, \cdots, M\}$. Assuming that each destination has an individual power budget, a generalization of the problem from the previous section is:

$$\max_{\mathbf{x}^{(m)}, \mathbf{y}^{(m)}, \forall m\in\mathsf{M}} \quad \min_{m\in\mathsf{M}} \mathcal{R}_m(\mathbf{x}^{(m)}, \mathbf{y}^{(m)})$$
$$s.t. \quad \sum_{m=1}^{M} \mathbf{1}^T\mathbf{x}^{(m)} \le P_S, \mathbf{1}^T\mathbf{y}^{(m)} \le P_{D,m}, \mathcal{C}_{SD}^{(m)} \ge \mathcal{C}_m,$$
$$x_{m,n} \ge 0, y_{m,n} \ge 0, \forall n \in \mathsf{N}, \forall m \in \mathsf{M}, \quad (39)$$

where $\mathbf{1}$ is the vector of all ones, $P_{D,m}$ and $\mathcal{C}_m$ are the power budget and the target rate for *Bob* $m$, and

$$\mathcal{C}_{SD}^{(m)} = \frac{1}{MN}\sum_{n=1}^{N} \log\left(1 + \frac{x_{m,n}A_{m,n}}{1 + y_{m,n}B_{m,n}}\right). \quad (40)$$

To present a fast algorithm to solve the problem (39), we first denote its solution by $(\mathcal{R}_\mathsf{M}, \mathbf{x}_\mathsf{M}, \mathbf{y}_\mathsf{M})$ where $\mathcal{R}_\mathsf{M}$ is the maximum of the objective function, and $\mathbf{x}_\mathsf{M} = \{\mathbf{x}^{(m)}, \forall m \in \mathsf{M}\}$ and $\mathbf{y}_\mathsf{M} = \{\mathbf{y}^{(m)}, \forall m \in \mathsf{M}\}$ are the corresponding sets of vectors of power allocations at the source and the destinations. Furthermore, $\mathcal{R}_\mathsf{M}$ depends on $P_S$, $P_{D,m}, \forall m \in \mathsf{M}$ and $\mathcal{C}_m, \forall m \in \mathsf{M}$. We will also express this relationship by $\mathcal{R}_\mathsf{M}(P_S, P_{D,\mathsf{M}}, \mathcal{C}_\mathsf{M})$ or simply $\mathcal{R}_\mathsf{M}(P_{S,\mathsf{M}})$. Note that while $\mathcal{R}_\mathsf{M}$ and $P_{S,\mathsf{M}}$ are always scalars here, $P_{D,\mathsf{M}}$ and $\mathcal{C}_\mathsf{M}$ can be viewed as sets, i.e., $P_{D,\mathsf{M}} = \{P_{D,m}, \forall m \in \mathsf{M}\}$ and $C_\mathsf{M} = \{C_m, \forall m \in \mathsf{M}\}$.

It is obvious that if the set $\mathsf{M}$ has only one entry, then the solution to (39) can be readily obtained by the algorithms shown in the previous sections where $M = 1$.

If $M = 2$, we can decompose $\mathsf{M}$ into two subsets $\mathsf{M}_1$ and $\mathsf{M}_2$ where each subset has only one entry. Then, we can obtain $\mathcal{R}_{\mathsf{M}_1}(P_{S,\mathsf{M}_1})$ and $\mathcal{R}_{\mathsf{M}_2}(P_S - P_{S,\mathsf{M}_1})$ for any given $P_{S,\mathsf{M}_1}$ satisfying $P_S \ge P_{S,\mathsf{M}_1} \ge 0$. For $\mathsf{M}_1$, there is a minimum amount of power $P^\dagger_{S,\mathsf{M}_1}$ to meet the rate constraint, which can be obtained by the standard water-filling algorithm. Similarly, for $\mathsf{M}_2$, there is a corresponding $P^\dagger_{S,\mathsf{M}_2}$. If $\mathcal{R}_{\mathsf{M}_1}(P^\dagger_{S,\mathsf{M}_1}) \ge \mathcal{R}_{\mathsf{M}_2}(P_S - P^\dagger_{S,\mathsf{M}_1})$ which is denoted as Case I as shown in Fig. 4, then there is no way to increase the secrecy capacity for the whole set $\mathsf{M}$ from $\min(\mathcal{R}_{\mathsf{M}_1}(P^\dagger_{S,\mathsf{M}_1}), \mathcal{R}_{\mathsf{M}_2}(P_S - P^\dagger_{S,\mathsf{M}_1}))$. This is because $\mathcal{R}_{\mathsf{M}_i}(P_{S,\mathsf{M}_i})$ is strictly increasing (or possibly staying at zero initially) with increasing $P_{S,\mathsf{M}_i}$ according to *Proposition 4*. In this case, $\mathcal{R}_\mathsf{M}(P_{S,\mathsf{M}}) = \mathcal{R}_{\mathsf{M}_2}(P_S - P^\dagger_{S,\mathsf{M}_1})$. Similarly, if $\mathcal{R}_{\mathsf{M}_1}(P_S - P^\dagger_{S,\mathsf{M}_2}) \le \mathcal{R}_{\mathsf{M}_2}(P^\dagger_{S,\mathsf{M}_2})$ which is denoted as Case II as shown in Fig. 4, then $\mathcal{R}_\mathsf{M}(P_{S,\mathsf{M}}) = \mathcal{R}_{\mathsf{M}_1}(P_S - P^\dagger_{S,\mathsf{M}_2})$. If none of the above two cases is true, we have the Case III as shown in Fig. 4, for which we can apply a bisection search to find $P^*_{S,\mathsf{M}_1}$ such that $\mathcal{R}_{\mathsf{M}_1}(P^*_{S,\mathsf{M}_1}) = \mathcal{R}_{\mathsf{M}_2}(P_S - P^*_{S,\mathsf{M}_1})$ and hence $\mathcal{R}_\mathsf{M}(P_{S,\mathsf{M}}) = \mathcal{R}_{\mathsf{M}_1}(P^*_{S,\mathsf{M}_1})$.

If $M > 2$, we can start with the above decomposition from $\mathsf{M}$ to $\mathsf{M}_1$ and $\mathsf{M}_2$. Then, we can further decompose $\mathsf{M}_1$ and/or $\mathsf{M}_2$ into smaller subsets. We can repeat the above process until each

**Algorithm 4:** $(\mathcal{R}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}})$ = Recursive_Bisection_Search_BC ($\mathsf{M}$, $P_S$, $P_{D,\mathsf{M}}, \mathcal{C}_{\mathsf{M}}$) - Solution to (39),

**if** size($\mathsf{M}$) $\geq 2$ **then**
  $\mathsf{M}_1 = \lfloor \frac{\mathsf{M}}{2} \rfloor$, $\mathsf{M}_2 = \mathsf{M} \backslash \mathsf{M}_1$;
  $P^{\dagger}_{S,\mathsf{M}_1}$ = Minimum_Power_Require($\mathsf{M}_1, \mathcal{C}_{\mathsf{M}_1}$);
  $P^{\dagger}_{S,\mathsf{M}_2}$ = Minimum_Power_Require($\mathsf{M}_2, \mathcal{C}_{\mathsf{M}_2}$);
  $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_1, P^{\dagger}_{S,\mathsf{M}_1}, P_{D,\mathsf{M}_1}, \mathcal{C}_{\mathsf{M}_1}$);
  $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_2, P_S - P^{\dagger}_{S,\mathsf{M}_1}, P_{D,\mathsf{M}_2}, \mathcal{C}_{\mathsf{M}_2}$);
  **if** $\mathcal{R}_{\mathsf{M}_1} \geq \mathcal{R}_{\mathsf{M}_2}$ **then**
    **return** $\mathcal{R}_{\mathsf{M}_2}, [\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
  **else**
    $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_1, P_S - P^{\dagger}_{S,\mathsf{M}_2}, P_{D,\mathsf{M}_1}, \mathcal{C}_{\mathsf{M}_1}$);
    $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_2, P^{\dagger}_{S,\mathsf{M}_2}, P_{D,\mathsf{M}_2}, \mathcal{C}_{\mathsf{M}_2}$);
    **if** $\mathcal{R}_{\mathsf{M}_1} \leq \mathcal{R}_{\mathsf{M}_2}$ **then**
      **return** $\mathcal{R}_{\mathsf{M}_1}, [\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
    **else**
      $P^{+}_{S1} = P_S - P^{\dagger}_{S,\mathsf{M}_2}$, $P^{-}_{S1} = P^{\dagger}_{S,\mathsf{M}_1}$;
      **while** $(\mu > \epsilon)$ **do**
        $P_{S1} = \frac{P^{+}_{S1} + P^{-}_{S1}}{2}$, $P_{S2} = P_S - P_{S1}$;
        $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_1, P_{S1}, P_{D,\mathsf{M}_1}, \mathcal{C}_{\mathsf{M}_1}$);
        $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2})$ = Recursive_Bisection_Search_BC ($\mathsf{M}_2, P_{S2}, P_{D,\mathsf{M}_2}, \mathcal{C}_{\mathsf{M}_2}$);
        $\mu = |\mathcal{R}_{\mathsf{M}_1} - \mathcal{R}_{\mathsf{M}_2}|$;
        **if** $\mathcal{R}_{\mathsf{M}_1} > \mathcal{R}_{\mathsf{M}_2}$ **then**
          $P^{+}_{S1} = P_{S1}$
        **else**
          $P^{-}_{S1} = P_{S1}$
        **end if**
      **end while**
      **return** $\frac{\mathcal{R}_{\mathsf{M}_1} + \mathcal{R}_{\mathsf{M}_2}}{2}$, $[\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
    **end if**
  **end if**
**else**
  $(\mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}})$ = Two_Phases_Allocation_with_Rate ($P_{S\mathsf{M}}, P_D$);
  $\mathcal{R}_{\mathsf{M}}$ = Secrecy_Capacity ($\mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}$);
  **return** $\mathcal{R}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}$;
**end if**

subset has only one entry. At each of these decompositions, we perform the optimal partition of a given source power between two groups/subsets. Also note that this is a recursive process where an upper layer operation needs to call upon lower layer operations repeatedly until convergence. The number of these layers of recursions is (or about) $\log_2 M$.

The details of the entire algorithm are shown as Algorithm 4. In Algorithm 4, the function *Minimum_Power_Require*(.,.) is to calculate the minimum required power to achieve the target rates which can be obtained by the standard waterfilling algorithm. The function *Two_Phases_Allocation_with_Rate*(.,.) is the entire algorithm developed in section IV. The function *Secrecy_Capacity*(.) computes the corresponding secrecy capacity.

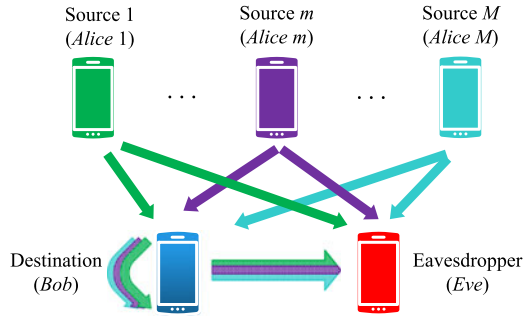



Fig. 5. A network with multiple sources - also referred to as "multiple access (MAC)".

## VI. Extension to Multiple Sources

In this section, we consider a network with multiple sources, one full-duplex destination and one eavesdropper as shown in Fig. 5. We assume that the $M$ sources use $M$ orthogonal sets of subcarriers for transmission (not via a common channel as in the conventional sense of multiple access). While the source $m$ transmits $\mathbf{x}_S^{(m)}(t) \in \mathbb{C}^{N\times 1}$, the full-duplex destination transmits the artificial noise $\mathbf{x}_D^{(m)}(t) \in \mathbb{C}^{N\times 1}$ using the same set of subcarriers. Then, the signal vector received by *Bob*, corresponding to the source $m$, is the same as (35), and the signal vector received by *Eve* is the same as (36). Furthermore, the corresponding secrecy capacity is the same as (37). As a dual form of (39), we now have the following power allocation problem:

$$\max_{\mathbf{x}^{(m)},\mathbf{y}^{(m)},\forall m\in\mathsf{M}} \quad \min_{m\in\mathsf{M}} \mathcal{R}_m(\mathbf{x}^{(m)},\mathbf{y}^{(m)})$$

$$s.t. \quad \mathbf{1}^T\mathbf{x}^{(m)} \leq P_{S,m}, \sum_{m=1}^{M} \mathbf{1}^T\mathbf{y}^{(m)} \leq P_D, \mathcal{C}_{SD}^{(m)} \geq \mathcal{C}_m,$$

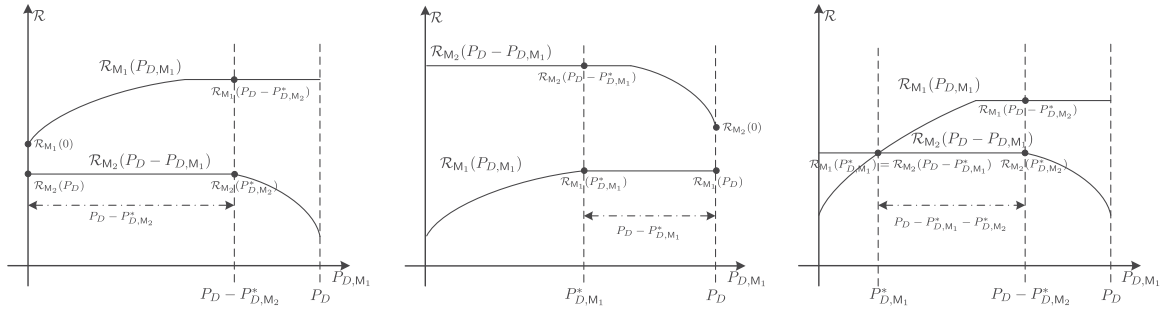
$$x_{m,n} \geq 0, y_{m,n} \geq 0, \forall n \in \mathsf{N}, \forall m \in \mathsf{M}, \tag{41}$$

where $P_{S,m}$, $\mathcal{C}_m$ and $\mathcal{C}_{SD}^{(m)}$ are similarly defined (although $m$ is now the index of the sources but not the destinations). For example, $P_{S,m}$ is now the power budget to be used by the $m$th source for transmission to the destination.

Let us denote the solution to the problem (41) by $(\mathcal{R}_{\mathsf{M}}, \mathbf{z}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}})$ where $\mathcal{R}_{\mathsf{M}}$, $\mathbf{x}_{\mathsf{M}}$ and $\mathbf{y}_{\mathsf{M}}$ are similarly defined as before. The $m$th entry of the $M \times 1$ vector $\mathbf{z}_{\mathsf{M}}$, denoted by $\mathbf{z}_{\mathsf{M}}(m)$, is either 1 or 0. If the allocated power $P_{D,m}$ is to be completely utilized by the (*full-duplex*) destination *for* receiving the signal from the source $m$, $\mathbf{z}_{\mathsf{M}}(m)$ is set to be zero. Otherwise, it is set to be one. Since $\mathcal{R}_{\mathsf{M}}$ depends on $P_{S,m}, \forall m \in \mathsf{M}$, $P_D$ and $\mathcal{C}_m, \forall m \in \mathsf{M}$, we will express such a dependency by $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}})$ where $P_{D,\mathsf{M}}$ denotes all the power *available for* (*but not necessarily to be actually used by*) the destination when receiving the signals from the sources in the set $\mathsf{M}$. Note that it is possible in some cases that to achieve the maximum secrecy capacity, the full-duplex destination should not use all its available power in transmitting the artificial noise. Also note that $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}})$ is a non-decreasing function of $P_{D,\mathsf{M}}$.

Obviously, if $M = 1$ or equivalently $\mathsf{M}$ has only one entry, the problem (41) can be solved by the algorithm developed before for the three-node network.

Now assume $M = 2$. Let $\mathsf{M}$ be partitioned into $\mathsf{M}_1$ and $\mathsf{M}_2$. In this case, each of $\mathsf{M}_1$ and $\mathsf{M}_2$ has only one entry.




(a) Case I (b) Case II (c) Case III

Fig. 6. An illustration of the ideas behind *Algorithms* 5 and 6. $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}})$ is the rate for group $\mathsf{M}$ with total destination power $P_{D,\mathsf{M}}$. $P^*_{D,\mathsf{M}}$ is such that $\mathcal{R}_{\mathsf{M}}(P_D) = \mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}})$ if and only if $P^*_{D,\mathsf{M}} \le P_{D,\mathsf{M}} \le P_D$. The right two heavy dots in case I, the left two heavy dots in Case II and the right two heavy dots in Case III indicate the optimal solutions for $P_{D,\mathsf{M}_1}$ and $P_{D,\mathsf{M}_2}$.

Then, we can obtain $\mathcal{R}_{\mathsf{M}_1}(0)$ and $\mathcal{R}_{\mathsf{M}_2}(P_D)$, where all the destination power is made available only to $\mathsf{M}_2$. If $\mathcal{R}_{\mathsf{M}_1}(0) \ge \mathcal{R}_{\mathsf{M}_2}(P_D)$, which is Case I shown in Fig. 6, then we have obtained the optimal secrecy capacity for $\mathsf{M}$: $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}}) = \min(\mathcal{R}_{\mathsf{M}_1}(0), \mathcal{R}_{\mathsf{M}_2}(P_D)) = \mathcal{R}_{\mathsf{M}_2}(P_D)$. However, it is possible that there is $P^*_{D,\mathsf{M}_2} < P_D$ such that $\mathcal{R}_{\mathsf{M}_2}(P_D) = \mathcal{R}_{\mathsf{M}_2}(P_{D,\mathsf{M}_2})$ if and only if $P^*_{D,\mathsf{M}_2} \le P_{D,\mathsf{M}_2} \le P_D$. In this case, we can utilize $P_D - P^*_{D,\mathsf{M}_2}$ for $\mathsf{M}_1$ so that the secrecy capacity for $\mathsf{M}_1$ can be increased although the optimal secrecy capacity for $\mathsf{M}$ remains the same. See Case I in Fig. 6.

If Case I does not hold, we can similarly obtain $\mathcal{R}_{\mathsf{M}_1}(P_D)$ and $\mathcal{R}_{\mathsf{M}_2}(0)$, where all the destination power is made available only to $\mathsf{M}_1$. If $\mathcal{R}_{\mathsf{M}_1}(P_D) \le \mathcal{R}_{\mathsf{M}_2}(0)$, which is Case II shown in Fig. 6, then we have obtained the optimal secrecy capacity for $\mathsf{M}$: $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}}) = \mathcal{R}_{\mathsf{M}_1}(P_D)$. It is possible here that there is $P^*_{D,\mathsf{M}_1} < P_D$ such that $\mathcal{R}_{\mathsf{M}_1}(P_D) = \mathcal{R}_{\mathsf{M}_1}(P_{D,\mathsf{M}_1})$ if and only $P^*_{D,\mathsf{M}_1} \le P_{D,\mathsf{M}_1} \le P_D$. Then, we can use $P_D - P^*_{D,\mathsf{M}_1}$ for $\mathsf{M}_2$ to increase the secrecy capacity for $\mathsf{M}_2$ although the optimal secrecy capacity for $\mathsf{M}$ stays the same. See Case II in Fig. 6.

If none of Cases I and II is true, we must have Case III as shown in Fig. 6 for which we can use a bisection search to find $P^*_{D,\mathsf{M}_1}$ such that $\mathcal{R}_{\mathsf{M}_1}(P^*_{D,\mathsf{M}_1}) = \mathcal{R}_{\mathsf{M}_2}(P_D - P^*_{D,\mathsf{M}_1})$ and hence the optimal secrecy capacity for $\mathsf{M}$ is $\mathcal{R}_{\mathsf{M}}(P_{D,\mathsf{M}}) = \mathcal{R}_{\mathsf{M}_1}(P^*_{D,\mathsf{M}_1})$.

More generally, if $M > 2$, we can first partition $\mathsf{M}$ into $\mathsf{M}_1$ and $\mathsf{M}_2$ and compute the optimal binary partition of the destination power $P_D$ into $P^*_{D,\mathsf{M}_1}$ and $P^*_{D,\mathsf{M}_2} = P_D - P^*_{D,\mathsf{M}_1}$. If $\mathsf{M}_i$ for some $i \in \{1,2\}$ has more than one entries, we then further partition $\mathsf{M}_i$ into two smaller sets $\mathsf{M}_{i,1}$ and $\mathsf{M}_{i,2}$ and compute the optimal binary partition of any given power value $P_{D,\mathsf{M}_i}$ into $P^*_{D,\mathsf{M}_{i,1}}$ and $P^*_{D,\mathsf{M}_{i,2}} = P_{D,\mathsf{M}_i} - P^*_{D,\mathsf{M}_{i,1}}$.

The above process can be repeated recursively, which leads to Algorithm 5 and Algorithm 6. Note that Algorithm 5 is part of Algorithm 6. The purpose of using Algorithm 6 instead of using just Algorithm 5 is to ensure that all available power $P_D$ is utilized to improve the secrecy capacities for all sources although Algorithm 5 alone would yield the same secrecy capacity for the entire network (in terms of "max min of") as Algorithm 6.

## VII. Simulation Results

In this section, we present the simulation results based on our proposed algorithms. In the simulation, all channel magnitudes are Rayleigh distributed with unit mean square, and the self-interference attenuation factor $\rho$ is set to be 0.5 unless stated otherwise.

### A. Three-Node Network Under Power-Only Constraints

With $N = 8$ and $P_S = P_D = P$, shown in Fig. 7(a) are four curves of averaged secrecy capacity versus the power $P$. We see that in the very low power region, "optimal source power allocation" has an advantage over "optimal destination power allocation". This is because at low power, the SINR on each subcarrier (see (1)) is dominated by the source power and the destination power has little effect.

While in the high power region, "optimal destination power allocation" is much more effective than "optimal source power allocation". This is because at higher power, the uniform source power allocation approaches its optimal allocation, and hence optimal destination power allocation subject to uniform source power allocation approaches the joint optimality at both source and destination. However, the uniform destination power allocation is generally not optimal at high power. We see indeed that the results for "optimal destination power allocation" and "joint optimal power allocation" achieve the same upper bound at high power. The effect of the optimal destination power allocation at high power is very significant.

Shown in Fig. 7(b) are results for a varying level of self-interference channel magnitude. Clearly, the less the self-interference, the higher secrecy capacity achievable.

The two-phase iterations typically take less than 5 iterations to converge. The bisection search within each of the two phases converges rapidly (logarithmic fast) as expected.

### B. Three-Node Network Under Power and Rate Constraints

Shown in Fig. 8(a) and (b) is a comparison of three different cases in terms of the secrecy capacity against *Eve* (Fig. 8(a)) and the *Alice*-to-*Bob* data rate (Fig. 8(b)) for a specific realization of all channels where $A_n < C_n, \forall n \in \mathsf{N}$ (i.e., *Eve* has a stronger channel from *Alice* than *Bob* has from *Alice* for all subcarriers).

In case I, the data rate is maximized subject to power constraints at *Alice* and *Bob* but there is no secrecy capacity constraint. The resulting data rate is denoted by $\mathcal{C}_{SD,I}$ (which is obtained by the standard waterfilling algorithm). And the resulting secrecy capacity $\mathcal{R}_{SE,I}$ is zero for this channel realization as expected.

**Algorithm 5:** $(\mathcal{R}_{\mathsf{M}}, \mathbf{z}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}})$ = Recursive_Bisection_Search_MAC($\mathsf{M}, P_{S,\mathsf{M}}, P_D, \mathcal{C}_{\mathsf{M}}$) - Solution to (41).

**if** size($\mathsf{M}$) $\geq 2$ **then**
  $\mathsf{M}_1 = \lfloor \frac{\mathsf{M}}{2} \rfloor$, $\mathsf{M}_2 = \mathsf{M} \backslash \mathsf{M}_1$
  $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1}) =$ Recursive_Bisection_Search_MAC ($\mathsf{M}_1, P_{S,\mathsf{M}_1}, 0, \mathcal{C}_{\mathsf{M}_1}$);
  $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{z}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2}) =$ Recursive_Bisection_Search_MAC ($\mathsf{M}_2, P_{S,\mathsf{M}_2}, P_D, \mathcal{C}_{\mathsf{M}_2}$);
  **if** $\mathcal{R}_{\mathsf{M}_1} \geq \mathcal{R}_{\mathsf{M}_2}$ **then**
    **return** $\mathcal{R}_{\mathsf{M}_2}, [\mathbf{z}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_2}], [\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
  **else**
    $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1}) =$ Recursive_Bisection_Search_MAC ($\mathsf{M}_1, P_{S,\mathsf{M}_1}, P_D, \mathcal{C}_{\mathsf{M}_1}$);
    $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{z}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2}) =$ Recursive_Bisection_Search_MAC ($\mathsf{M}_2, P_{S,\mathsf{M}_2}, 0, \mathcal{C}_{\mathsf{M}_2}$);
    **if** $\mathcal{R}_{\mathsf{M}_1} \leq \mathcal{R}_{\mathsf{M}_2}$ **then**
      **return** $\mathcal{R}_{\mathsf{M}_1}, [\mathbf{z}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_2}], [\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
    **else**
      $P_{D1}^{+} = P_D, P_{D1}^{-} = 0$;
      **while** $(\mu > \epsilon)$ **do**
        $P_{D1} = \frac{P_{D1}^{+} + P_{D1}^{-}}{2}, P_{D2} = P_D - P_{D1}$;
        $(\mathcal{R}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_1}) =$ Recursive_Bisection_Search_MAC($\mathsf{M}_1, P_{S,\mathsf{M}_1}, P_{D1}$);
        $(\mathcal{R}_{\mathsf{M}_2}, \mathbf{z}_{\mathsf{M}_2}, \mathbf{x}_{\mathsf{M}_2}, \mathbf{y}_{\mathsf{M}_2}) =$ Recursive_Bisection_Search_MAC($\mathsf{M}_2, P_{S,\mathsf{M}_2}, P_{D2}$);
        $\mu = |\mathcal{R}_{\mathsf{M}_1} - \mathcal{R}_{\mathsf{M}_2}|$;
        **if** $\mathcal{R}_{\mathsf{M}_1} > \mathcal{R}_{\mathsf{M}_2}$ **then**
          $P_{D1}^{+} = P_{D1}$;
        **else**
          $P_{D1}^{-} = P_{D1}$;
        **end if**
      **end while**
      **return** $\frac{\mathcal{R}_{\mathsf{M}_1} + \mathcal{R}_{\mathsf{M}_2}}{2}, [\mathbf{z}_{\mathsf{M}_1}, \mathbf{z}_{\mathsf{M}_2}], [\mathbf{x}_{\mathsf{M}_1}, \mathbf{x}_{\mathsf{M}_2}], [\mathbf{y}_{\mathsf{M}_1}, \mathbf{y}_{\mathsf{M}_2}]$;
    **end if**
  **end if**
**else**
  $(\mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}) =$ Two_Phases_Allocation_with_Rate ($P_{S,\mathsf{M}}, P_D$);
  $\mathcal{R}_{\mathsf{M}} =$ Secrecy_Capacity ($\mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}$);
  **if** sum($\mathbf{y}_{\mathsf{M}}$) == $P_D$ **then**
    $\mathbf{z}_{\mathsf{M}} = 0$;
  **else**
    $\mathbf{z}_{\mathsf{M}} = 1$;
  **end if**
  **return** $\mathcal{R}_{\mathsf{M}}, \mathbf{z}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}$;
**end if**

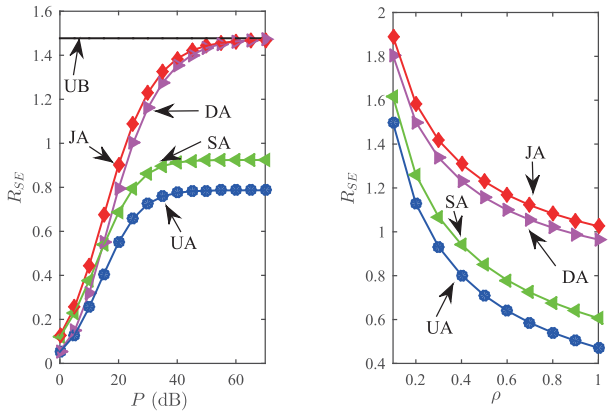
**Algorithm 6:** Refined solution to (41).

**while** $(\mathsf{M} \neq \emptyset \,\&\&\, P_D > 0 \,\&\&\, \mathbf{z}_{\mathsf{M}} \neq \mathbf{0} \,\&\&\, \mathbf{z}_{\mathsf{M}} \neq \mathbf{1})$ **do**
  $(\mathcal{R}_{\mathsf{M}}, \mathbf{z}_{\mathsf{M}}, \mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}) =$ Recursive_Bisection_Search_MAC($\mathsf{M}, P_{S,\mathsf{M}}, P_D, \mathcal{C}_{\mathsf{M}}$);
  $\mathcal{R}_{\mathsf{M}} =$ Secrecy_Capacity ($\mathbf{x}_{\mathsf{M}}, \mathbf{y}_{\mathsf{M}}$);
  $\mathsf{K} = \{m | \mathcal{R}_m = \mathcal{R}_{\mathsf{M}}, \mathbf{z}_{\mathsf{M}}(m) = 1, \forall m \in \mathsf{M}\}$, $\mathsf{M} = \mathsf{M} \backslash \mathsf{K}$;
  $P_D = P_D$ - Sum($\mathbf{y}_{\mathsf{K}}$);
**end while**

In case II, the secrecy capacity is maximized subject to power constraints at *Alice* and *Bob* and also a *Alice*-to-*Bob* rate constraint. The constrained rate (i.e., the lower bound on the rate) is set at $\mathcal{C}_{SD}^{\dagger} = 0.9\mathcal{C}_{SD,I}$. The corresponding achieved rate is denoted by $\mathcal{C}_{SD,II}$, the curve of which is, as expected, indistinguishable from that of $\mathcal{C}_{SD}^{\dagger}$. The resulting secrecy capacity is denoted by $\mathcal{R}_{SE,II}$, which is large and not far from that of case III.

In case III, the secrecy capacity is maximized with power-only constraints at *Alice* and *Bob* but no rate constraint. The resulting secrecy capacity is denoted by $\mathcal{R}_{SE,III}$ and the resulting data rate is $\mathcal{C}_{SD,III}$.

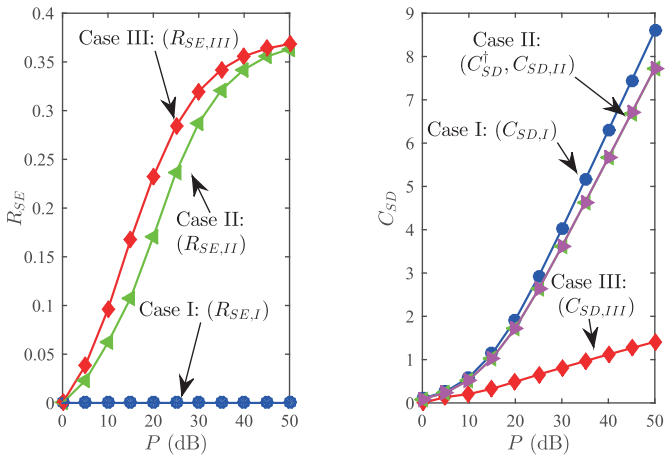
We see that because of the rate constraint, case II results in a much better tradeoff between the source-to-destination data rate and the network's secrecy capacity than the other two cases.




(a) Secrecy capacity vs. power budget $P = P_S = P_D$ ($\rho = 0.5$)

(b) The secrecy capacity vs. self-interference attenuation factor $\rho$ ($P_S = P_D = 30$dB)

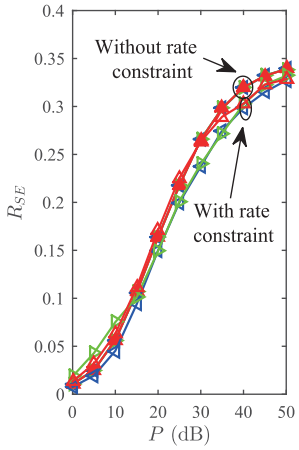
Fig. 7. The achieved secrecy of four different schemes (averaged over 100 channel realizations). Here, "UB" means "asymptotical limit at high power", "JA" means "joint optimal power allocation at both source and destination", "DA" means "optimal destination power allocation while uniform source power allocation", "SA" means "optimal source power allocation while uniform destination power allocation", and "UA" means "uniform power allocation at both source and destination".



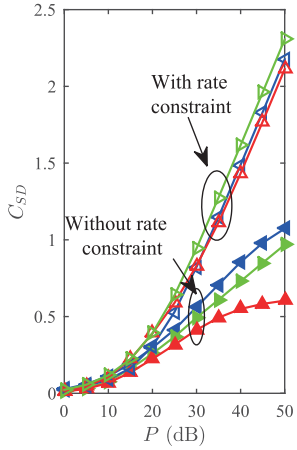

(a) Secrecy capacity

(b) *Alice*-to-*Bob* Rate.

Fig. 8. The achieved secrecy capacity under power and rate constraints ($\mathcal{C}_{SD}^{\dagger} = 0.9\mathcal{C}_{SD,I}$. With rate constraint, i.e. Case II, the constrained rates and achieved rates are indistinguishable.).

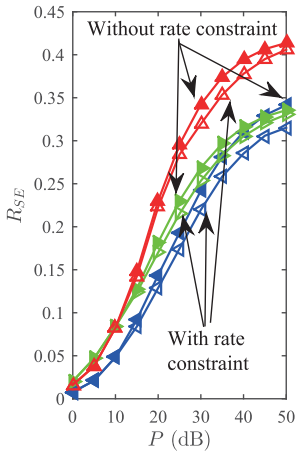



(a) Secrecy capacity.

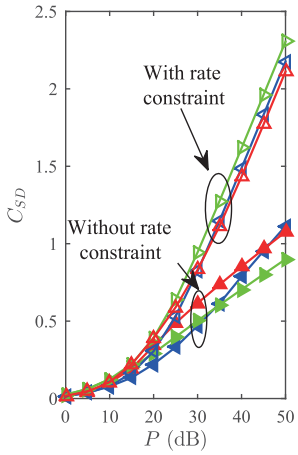



(b) *Alice*-to-*Bob* Rate.

Fig. 9. Results for three destinations where $P_S = P$, $P_{D,m} = \frac{P}{3}$ for $m = 1, 2, 3$, $N = 8$, and $\gamma = 0.9$ (In (a), the three curves with rate constraint and the other three curves without rate constraint are relatively intertwined together here. In (b), with rate constraint, the constrained rates and achieved rates are indistinguishable and hence not plotted separately.).




(a) Secrecy capacity.




(b) *Alice*-to-*Bob* Rate.

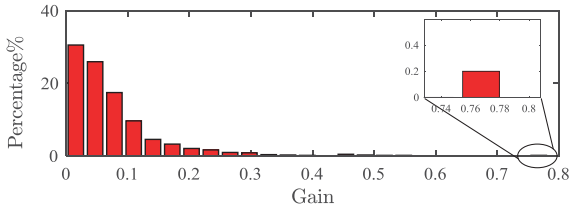
Fig. 10. Results for three sources where $P_D = P$, $P_{S,m} = \frac{P}{3}$ for $m = 1, 2, 3$, $N = 8$, and $\gamma = 0.9$ (In (a), the three curves with rate constraint and the other three curves without rate constraint are also somewhat intertwined here. In (b), with rate constraint, the constrained rates and achieved rates are indistinguishable and hence not plotted separately.).

### C. Joint Power Allocation for Multiple Destinations

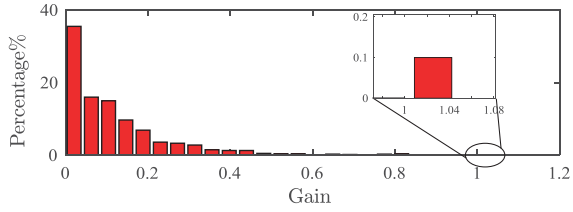
We choose $\mathcal{C}_m = \gamma \mathcal{C}_m^\dagger$, where $\mathcal{C}_m^\dagger$ is the maximum achievable data rate from *Alice* to *Bob* when $\frac{P_S}{M}$ is allocated at *Alice* for transmission to the $m$th destination. With $\gamma = 0.9$ and $M = 3$, the achieved secrecy capacities and source-to-destination data rates are shown in Fig. 9(a) and (b) respectively. Also shown in these two figures are the corresponding results without any rate constraint. We see that with rate constraints, we lose a small amount of secrecy capacities while maintaining a substantial gain of data rates.

### D. Joint Power Allocation for Multiple Sources

Here, the rate constraint for the $m$th source is set to be $\mathcal{C}_m = \gamma \mathcal{C}_m^\dagger$ where $\mathcal{C}_m^\dagger$ is the maximum achievable rate from the $m$th source to the destination with the power $P_{S,m} = \frac{P_S}{M}$ allocated to the $m$th source. The secrecy capacities and data rates for total three sources are presented in Fig. 10(a) and (b). We also see here that with rate constraint even though we lose a small amount of secrecy capacity, we obtain a substantial gain of data rate.




(a) Multi-user strategy with two destinations, $P_S = P = 30$dB and $P_{D,1} = P_{D,2} = 30$dB. For the corresponding single-user strategy, $P_{S,1} = P_{S,2} = \frac{P}{2} = 27$dB and $P_{D,1} = P_{D,2} = 30$dB.




(b) Multi-user strategy with two sources, $P_{S,1} = P_{S,2} = 30$dB and $P_D = P = 10$dB. For the corresponding single-user strategy, $P_{S,1} = P_{S,2} = 30$dB and $P_{D,1} = P_{D,2} = \frac{P}{2} = 7$dB.

Fig. 11. Distribution of the gain of the multi-user strategy where $N = 4$, $M = 2$, and $\gamma = 0.9$.

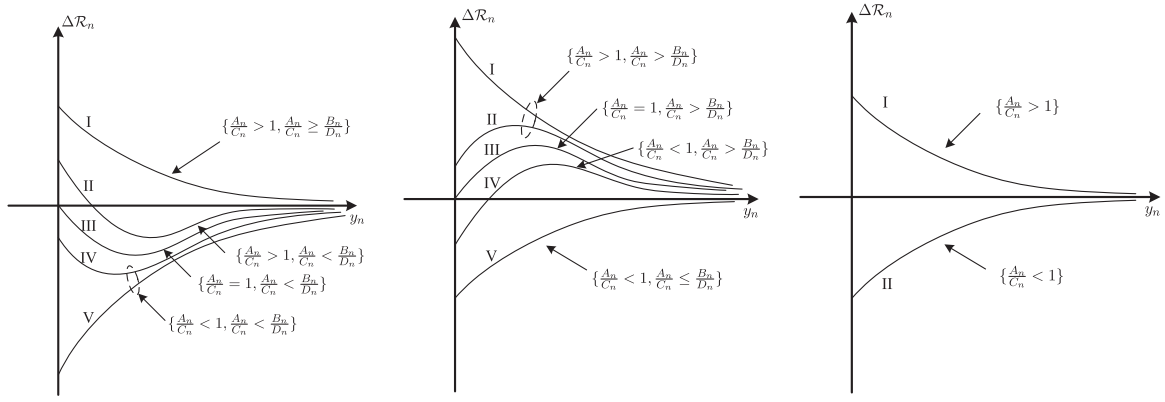
### E. Comparison Between Single-User Strategy and Multi-User Strategy

The extension from the single-user strategy (i.e., a single source and a single destination) to the multi-user strategy (i.e., a single source and multiple destinations, or multiple sources and a single destination) in the previous section was established in terms of power allocation algorithm. It is clear that the single-user strategy developed before is a special case of the multi-user strategy. There should be no doubt that the multi-user strategy should yield result no worse than the single-user strategy. However, before an optimal algorithm for the multi-user strategy was developed, there would be no way to know how much better the multi-user strategy can do than the single-user strategy. But with our algorithm developed in the previous section, we can here provide a quantitative comparison.

Assume $N = 4, M = 2$ and $\mathcal{C}_m = \gamma \mathcal{C}_m^\dagger$ with $\gamma = 0.9$. Define the gain of the multi-user strategy over the single-user strategy as

$$\text{Gain} = \frac{\mathcal{R}_{\mathsf{M}} - \min(\mathcal{R}_1, \mathcal{R}_2)}{\min(\mathcal{R}_1, \mathcal{R}_2)} \tag{42}$$

where $\mathcal{R}_{\mathsf{M}}$ is the optimal multi-user secrecy capacity achieved via joint power allocation under two users with total power $P$, and $\mathcal{R}_1$ and $\mathcal{R}_2$ are the optimal single-user secrecy capacities for user 1 and user 2 respectively each with total power $\frac{P}{2}$. Clearly, the gain is a function of the channel realization. We




(a) $\frac{B_n}{D_n} > 1$ (b) $\frac{B_n}{D_n} < 1$ (c) $\frac{B_n}{D_n} = 1$

Fig. 12. Patterns of the function $\Delta\mathcal{R}_n(x_n, y_n)$ as in (2) with respect to $y_n \in (0, +\infty)$.

will consider the distribution of the gain over 1000 independent channel realizations.

Fig. 11(a) shows a distribution of the gain with two destinations, and Fig. 11(b) shows a distribution of the gain with two sources. We see that for most of the channel realizations, the gain is not significant. But for some channel realizations, the gain can be as high as $30\%$ to $80\%$. In fact, the maximum gain can be infinity in theory. Although the probability of such a high gain under random channel realizations does not seem large, the fact that such a high gain exists signifies the importance of the fast power allocation algorithm developed for multi-users.

## VIII. Conclusion

In this paper, we have studied fast power allocation algorithms for maximizing secrecy capacity of a three-node network subject to both power and rate constraints. The rate constraint along with self-interference of the full-duplex destination makes this study unique from many previous works. We have also extended this study to a case of multiple sources and another case of multiple destinations. The algorithms developed in this paper have made it possible to show that with a small but non-negligible probability the multi-user strategy can yield a much higher secrecy capacity than the single-user strategy. Future works should consider more scenarios of networks that are of importance in practice.

## Appendix A
## Proof of Proposition 1

*Proof:* It is easy to verify the following inequality:

$$\mathcal{R}(\mathbf{x},\mathbf{y}) = \frac{1}{N}\sum_{n=1}^{N}\max\{0, \Delta\mathcal{R}_n(x_n, y_n)\}$$
$$\geq \max\left\{0, \frac{1}{N}\sum_{n=1}^{N}\Delta\mathcal{R}_n(x_n, y_n)\right\} = \tilde{\mathcal{R}}(\mathbf{x},\mathbf{y}), \qquad \text{(A.1)}$$

where the equality holds if and only if $R_n(x_n, y_n) \geq 0, \forall n$. This property also follows from the fact that $\max(0, a)$ is a convex function of $a$ and hence $\frac{1}{N}\sum_n \max(0, a_n) \geq \max(0, \frac{1}{N}\sum_n a_n)$.

Let $(\mathbf{x}^*, \mathbf{y}^*) = \arg\max(\mathcal{R}(\mathbf{x},\mathbf{y}))$ subject to $\sum_{n=1}^{N} x_n \leq P_S$ and $\sum_{n=1}^{N} y_n \leq P_D$. Obviously, if $\Delta\mathcal{R}_n(x_n^*, y_n^*) < 0$ was true, $x_n^*$ and $y_n^*$ should be reset to zero and the saved power could be used to improve positive secrecy components on other subcarriers, and hence the original $x_n^*$ and $y_n^*$ would not be optimal. Hence, it must be true that $\Delta\mathcal{R}_n(x_n^*, y_n^*) \geq 0$. Then we have

$$\max_{\substack{\sum_{n=1}^{N} x_n \leq P_S \\ \sum_{n=1}^{N} y_n \leq P_D}} (\mathcal{R}(\mathbf{x},\mathbf{y})) = \frac{1}{N}\sum_{n=1}^{N}\max\{0, \Delta\mathcal{R}_n(x_n^*, y_n^*)\}$$
$$= \frac{1}{N}\sum_{n=1}^{N}\Delta\mathcal{R}_n(x_n^*, y_n^*) = \max\left\{0, \frac{1}{N}\sum_{n=1}^{N}\Delta\mathcal{R}_n(x_n^*, y_n^*)\right\}$$
$$= \tilde{\mathcal{R}}(\mathbf{x}^*, \mathbf{y}^*) \qquad \text{(A.2)}$$

Since $\mathcal{R}(\mathbf{x},\mathbf{y}) \geq \tilde{\mathcal{R}}(\mathbf{x},\mathbf{y})$, the above implies

$$\max(\mathcal{R}(\mathbf{x},\mathbf{y})) = \max(\tilde{\mathcal{R}}(\mathbf{x},\mathbf{y})). \qquad \text{(A.3)}$$

■

## Appendix B
## Proof of Proposition 2

*Proof:* Taking the first-order partial derivative of the function $\Delta\mathcal{R}_n(x_n, y_n)$ with respect to $y_n$, we have

$$\frac{\partial\Delta\mathcal{R}_n}{\partial y_n} = \frac{B_n}{1 + B_n y_n + A_n x_n} - \frac{B_n}{1 + B_n y_n} - \frac{D_n}{1 + D_n y_n + C_n x_n} + \frac{D_n}{1 + D_n y_n}. \qquad \text{(B.1)}$$

Setting it equal to zero, we have

$$a y_n^2 + b y_n + c = 0, \qquad \text{(B.2)}$$

where

$$a = A_n D_n - B_n C_n, \quad b = 2(A_n - C_n),$$
$$c = \frac{A_n B_n - C_n D_n + (B_n - D_n) A_n C_n x_n}{B_n D_n}. \qquad \text{(B.3)}$$

Because (B.2) is quadratic and it has at most two positive roots, the function $\Delta\mathcal{R}_n(x_n, y_n)$ has at most two stationary points with

regard to $y_n \in (0, +\infty)$. However, the hypothesis that (B.2) has two positive roots is invalid, which is proved next by contradiction.

We assume that (B.2) has two positive roots $y_n^{(1)}$ and $y_n^{(2)}$, then it must be true that

$$y_n^{(1)} + y_n^{(2)} = -\frac{b}{a} = -\frac{2(A_n - C_n)}{A_n D_n - B_n C_n} > 0. \tag{B.4}$$

$$y_n^{(1)} y_n^{(2)} = \frac{c}{a} = \frac{A_n B_n - C_n D_n + (B_n - D_n) A_n C_n x_n}{B_n D_n (A_n D_n - B_n C_n)} > 0. \tag{B.5}$$

If $A_n > C_n$, then (B.4) implies $A_n D_n < B_n C_n$, and hence $1 < \frac{A_n}{C_n} < \frac{B_n}{D_n}$, and hence $A_n B_n > C_n D_n$ and $B_n > D_n$. This implies that (B.5) is invalid.

On the other hand, if $A_n < C_n$, then (B.4) implies $A_n D_n > B_n C_n$, and hence $1 > \frac{A_n}{C_n} > \frac{B_n}{D_n}$, and hence $A_n B_n < C_n D_n$ and $B_n < D_n$. This implies that (B.5) is invalid.

In conclusion, (B.4) and (B.5) can not be satisfied at the same time, and hence there is at most one stationary point for $\Delta\mathcal{R}_n(x_n, y_n)$ with regard to $y_n \in (0, +\infty)$.

## APPENDIX C
## PROOF OF PROPOSITION 3

*Proof:* With *Proposition 2*, we know that for any given $x_n \in (0, +\infty)$, there is at most one stationary point for $\Delta\mathcal{R}_n(x_n, y_n)$ with regard to $y_n \in (0, +\infty)$. One can also verify that

$$\begin{cases} \lim_{y_n \to +\infty} \Delta\mathcal{R}_n(x_n, y_n) = 0^+, \text{ when } \frac{A_n}{C_n} > \frac{B_n}{D_n}, \\ \lim_{y_n \to +\infty} \Delta\mathcal{R}_n(x_n, y_n) = 0^-, \text{ when } \frac{A_n}{C_n} < \frac{B_n}{D_n}. \end{cases} \tag{C.1}$$

When $\frac{B_n}{D_n} > 1$, the patterns of $\Delta\mathcal{R}_n(x_n, y_n)$ versus $y_n$ are illustrated in Fig. 12(a). These patterns can be inferred by examining (B.4) and (B.5). For example, for Case I in Fig. 12(a), we have

$$y_n^{(1)} + y_n^{(2)} = -\frac{b}{a} = -\frac{2(\overbrace{A_n - C_n}^{>0})}{\underbrace{A_n D_n - B_n C_n}_{>0}} < 0, \tag{C.2}$$

$$y_n^{(1)} y_n^{(2)} = \frac{c}{a} = \frac{\overbrace{A_n B_n - C_n D_n}^{>0} + \overbrace{(B_n - D_n)}^{>0} A_n C_n x_n}{B_n D_n (\underbrace{A_n D_n - B_n C_n}_{>0})} > 0. \tag{C.3}$$

which means that (B.2) has no positive root and hence there is no stationary point for $\Delta\mathcal{R}_n(x_n, y_n)$ with respect to $y_n \in (0, +\infty)$. Also, since $\Delta\mathcal{R}_n(x_n, 0) > 0$ and $\lim_{y_n \to +\infty} R_n(x_n, y_n) = 0^+$, $\Delta\mathcal{R}_n(x_n, y_n)$ is always decreasing with regard to $y_n \in (0, +\infty)$.

For the other two cases where $\frac{B_n}{D_n} < 1$ or $\frac{B_n}{D_n} = 1$, the patterns of $\Delta\mathcal{R}_n(x_n, y_n)$ versus $y_n$ are illustrated in Fig. 12(b) and (c), respectively. All these patterns can be verified using the above mentioned method.

Note that a positive $y_n$ should make a contribution to $\Delta\mathcal{R}_n(x_n, y_n)$ that is both positive and increased from $\Delta\mathcal{R}_n(x_n, 0)$. By observing all the patterns shown in Fig. 12(a)–(c), one can conclude that the necessary condition for the optimal value of $y_n$ to be nonzero is that $\frac{B_n}{D_n} < 1$ and $\frac{A_n}{C_n} > \frac{B_n}{D_n}$, which corresponds to the cases II, III and IV in Fig. 12(b).

## APPENDIX D
## PROOF OF PROPOSITION 4

*Proof:* The partial derivative of $\Delta\mathcal{R}(\mathbf{x}, \mathbf{y})$ with respect to $x_n$ is given as

$$\frac{\partial \Delta\mathcal{R}(\mathbf{x}, \mathbf{y})}{\partial x_n} = \frac{1}{N} \frac{\partial \Delta\mathcal{R}_n(x_n, y_n)}{\partial x_n} = \varphi_n(x_n). \tag{D.1}$$

where $\varphi_n(x_n)$ is defined in (10).

First, consider the case $\alpha_n \le \beta_n$. It follows that $\frac{\partial \Delta\mathcal{R}(\mathbf{x}, \mathbf{y})}{\partial x_n} \le 0$, i.e., $\Delta\mathcal{R}_n(x_n, y_n)$ is a non-increasing function with respect to $x_n$. Since $\Delta\mathcal{R}_n(0, y_n) = 0$, then $\Delta\mathcal{R}_n(x_n, y_n) \le 0$ for any $x_n > 0$. Hence, the optimal power $x_n^\dagger$ must be zero.

Next, consider the case $\alpha_n > \beta_n$. It follows that $\frac{\partial \Delta\mathcal{R}(\mathbf{x}, \mathbf{y})}{\partial x_n} > 0$, i.e., $\Delta\mathcal{R}_n(x_n, y_n)$ is a increasing function with respect to $x_n$. Hence, $\Delta\mathcal{R}_n(x_n, y_n) > 0$ for any $x_n > 0$, and hence the optimal power $x_n^\dagger$ must be positive. Furthermore, all the power $P_s$ must be utilized and shared by those subcarriers where $\alpha_n > \beta_n$.

So, if $\alpha_n \le \beta_n, \forall n \in \mathsf{N}$, no power will be allocated, and we have $\sum_{n=1}^N x_n^\dagger = 0$. Otherwise, all powers must be utilized and we have $\sum_{n=1}^N x_n^\dagger = P_S$. ■

## APPENDIX E
## PROOF OF PROPOSITION 5

*Proof:* It is equivalent to consider the cases II, III and IV shown in Fig. 12(b) where $\frac{A_n}{C_n} > \frac{B_n}{D_n}$ and $\frac{B_n}{D_n} < 1$, which was established in Appendix C. Let $y_n^\ddagger$ denote a stationary point of $\Delta\mathcal{R}_n$ for any of the three cases. So we have that

$$\psi_n(y_n) = \frac{1}{N} \frac{\partial \Delta\mathcal{R}_n}{\partial y_n} = \frac{1}{N} \left( \frac{B_n}{1 + B_n y_n + A_n x_n} - \frac{B_n}{1 + B_n y_n} - \frac{D_n}{1 + D_n y_n + C_n x_n} + \frac{D_n}{1 + D_n y_n} \right) > 0, \tag{E.1}$$

where $y_n \in (0, y_n^\ddagger)$. We can rewrite (E.1) as

$$\underbrace{\frac{D_n}{1 + D_n y_n} - \frac{D_n}{1 + D_n y_n + C_n x_n}}_{\alpha} > \underbrace{\frac{B_n}{1 + B_n y_n} - \frac{B_n}{1 + B_n y_n + A_n x_n}}_{\beta} > 0. \tag{E.2}$$

where $\alpha$ and $\beta$ are defined such that $\alpha > \beta$ for $y_n \in (0, y_n^\ddagger)$. Taking the derivative of the function $\psi_n(y_n)$ with regard to $y_n$, we have

$$\frac{\partial \psi_n(y_n)}{\partial y_n} = \frac{1}{N}(\beta\theta - \alpha\xi), \tag{E.3}$$

where

$$\theta = \frac{B_n}{1+B_n y_n} + \frac{B_n}{1+B_n y_n + A_n x_n},$$
$$\xi = \frac{D_n}{1+D_n y_n} + \frac{D_n}{1+D_n y_n + C_n x_n}. \tag{E.4}$$

Since $\frac{A_n}{C_n} > \frac{B_n}{D_n}$ and $\frac{B_n}{D_n} < 1$, it follows that

$$\frac{D_n}{1+D_n y_n} - \frac{B_n}{1+B_n y_n} > 0, \tag{E.5}$$

and

$$\frac{D_n}{1+D_n y_n + C_n x_n} - \frac{B_n}{1+B_n y_n + A_n x_n} = \frac{\overbrace{D_n - B_n}^{>0} + \overbrace{(A_n D_n - B_n C_n)}^{>0} x_n}{(1+D_n y_n + C_n x_n)(1+B_n y_n + A_n x_n)} > 0 \tag{E.6}$$

Combining (5) and (6) yields

$$\underbrace{\left(\frac{D_n}{1+D_n y_n} + \frac{D_n}{1+D_n y_n + C_n x_n}\right)}_{\xi} > \underbrace{\left(\frac{B_n}{1+B_n y_n} + \frac{B_n}{1+B_n y_n + A_n x_n}\right)}_{\theta} > 0. \tag{E.7}$$

Now with $\alpha > \beta$ for $y_n \in (0, y_n^{\ddagger})$ and $\xi > \theta$, we obtain that

$$\frac{\partial \psi_n(y_n)}{\partial y_n} = \frac{1}{N}(\beta\theta - \alpha\xi) < 0, \tag{E.8}$$

for $y_n \in (0, y_n^{\ddagger})$. ■

## ACKNOWLEDGMENT

L. Chen and Y. Hua would like to thank Dr. X. Tang of AT&T, a former member of Hua's Lab, for his valuable suggestions on an earlier draft of this paper.

## REFERENCES

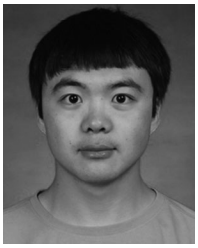
[1] L. Chen, Q. Zhu, and Y. Hua, "Fast computation for secure communication with full-duplex radio," in *Proc. IEEE 17th Int. Workshop Signal Process. Adv. in Wireless Commun.*, Jul. 2016, pp. 1–5.
[2] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering*. Hoboken, NJ, USA: Wiley, 2010.
[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[4] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[5] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[6] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4/5, pp. 355–580, Apr. 2009. [Online]. Available: http://dx.doi.org/10.1561/0100000036
[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas i: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part ii: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[12] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE 10th Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2009, pp. 344–348.
[13] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
[14] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[15] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[16] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.
[17] X. Tang, R. Liu, P. Spasojevic, and H. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.
[18] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 4, pp. 682–694, Apr. 2013.
[19] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[20] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[21] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex bob in the MIMO gaussian wiretap channel: Scheme and performance," *IEEE Signal Process. Lett.*, vol. 23, no. 1, pp. 107–111, Jan. 2016.
[22] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.
[23] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
[24] S. Parsaeefard and T. Le-Ngoc, "Improving wireless secrecy rate via full-duplex relay-assisted protocols," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 10, pp. 2095–2107, Oct. 2015.
[25] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5511–5526, Aug. 2016.
[26] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.
[27] H. Krishnaswamy and G. Zussman, "1 chip 2× the bandwidth," *IEEE Spectr.*, vol. 53, no. 7, pp. 38–54, Jul. 2016.
[28] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.
[29] Y. Hua, P. Liang, Y. Ma, A. C. Cirik, and Q. Gao, "A method for broadband full-duplex MIMO radio," *IEEE Signal Process. Lett.*, vol. 19, no. 12, pp. 793–796, Dec. 2012.
[30] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4296–4307, Dec. 2012.
[31] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5g and beyond," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 114–121, Feb. 2014.
[32] Y. Hua, Y. Ma, A. Gholian, Y. Li, A. C. Cirik, and P. Liang, "Radio self-interference cancellation by transmit beamforming, all-analog cancellation and blind digital tuning," *Signal Process.*, vol. 108, pp. 322–340, 2015.

[33] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*. Boston, MA, USA: Springer US, 2010, pp. 1–18. [Online]. Available: http://dx.doi.org/10.1007/978-1-4419-1385-2_1

[34] A. Beck and L. Tetruashvili, "On the convergence of block coordinate descent type methods," *SIAM J. Optim.*, vol. 23, no. 4, pp. 2037–2060, 2013.

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

[36] C. Fleury, "Sequential convex programming for structural optimization problems," in *Optimization of Large Structural Systems*. New York, NY, USA: Springer, 1993, pp. 531–553.



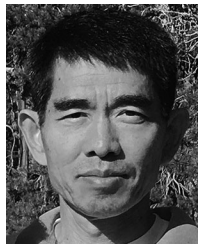
**Lei Chen** (S'13) received the B.S. and M.E. degrees in communication engineering from Harbin Institute of Technology, Harbin, China, in 2010 and 2012, respectively. He is currently working toward the Ph.D. degree in the Communications Research Center, Harbin Institute of Technology. From 2015 to 2017, he was a Visiting Student at the Laboratory of Signals, Systems and Networks, University of California, Riverside, Riverside, CA, USA.

His research interests include power allocation, transmitting beamforming, and GNSS signal processing.

**Qiping Zhu** (S'15) received the B.E. degree in electrical engineering from the Beijing Institute of Petrochemical Technology, Beijing, China, in 2013. He is currently working toward the Ph.D. degree in electrical engineering at the University of California, Riverside, Riverside, CA, USA.

His research interests include PHY layer secure communications, full-duplex radio, and MIMO channel estimation.

**Weixiao Meng** (SM'10) received the B.Eng., M. Eng., and Ph.D. degrees from Harbin Institute of Technology (HIT), Harbin, China, in 1990, 1995, and 2000, respectively. From 1998 to 1999, he worked at NTT DoCoMo on adaptive array antenna and dynamic resource allocation for beyond 3G as a Senior Visiting Researcher. He is currently a Full Professor in the School of Electronics and Information Engineering, HIT. His research interests include broadband wireless communications and networking, MIMO, GNSS receiver, and wireless localization technologies. He has published 3 books and more than 200 papers on journals and international conferences. He is the Chair of IEEE Communications Society Harbin Chapter, a senior member of the IEEE ComSoc, IET, the China Institute of Electronics, and the China Institute of Communication. He has been an editorial board member for Wileys *WCMC* Journal since 2010, an area editor for *PHYCOM* journal since 2014, and an editorial board member for IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He acted as a leading TPC Co-Chair of ChinaCom2011, leading Services and Applications track Co-Chair of IEEE WCNC2013, Awards Co-Chair of IEEE ICC2015, and Wireless Networking Symposia Co-Chair of Globecom 2015. In 2005, he was honored provincial excellent returnee and selected into New Century Excellent Talents (NCET) plan by the Ministry of Education, China, in 2008.



**Yingbo Hua** (S'86–M'88–SM'92–F'02) received the B.S. degree from Southeast University, Nanjing, China, in 1982, and the Ph.D. degree from Syracuse University, Syracuse, NY, USA, in 1988. He was on the faculty with the University of Melbourne, Melbourne, Vic, Australia, during 1990–2000, where he was promoted to the rank of Reader and Associate Professor in 1995. Following a sabbatical leave as a Visiting Professor with Hong Kong University of Science and Technology in 1999–2000, and as a Consultant with Microsoft Research, Redmond, WA, USA, in summer 2000, he joined the University of California, Riverside, Riverside, CA, USA, in 2001, where he has been a Senior Full Professor since 2009. He has published extensively in the fields of Signal Processing, Wireless Communications and Sensor Networks, including such topics as high-resolution methods, sensor array processing, blind source separation, blind system identification, reduced rank estimation, principal component analysis, subspace tracking, MIMO relay beamforming, MIMO channel estimation, multihop networks, full-duplex radio, resource allocation, and physical layer security.

He has served regularly on Editorial Boards of IEEE and EURASIP since 1994. He is currently a Senior Area Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING, a Steering Committee Member for IEEE WIRELESS COMMUNICATIONS LETTERS, and an Associate Editor for IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS. He is a Fellow of AAAS.