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 multiser user 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, 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.

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 an 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].
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 $x_S(t) \in \mathbb{C}^{N \times 1}$ be the signal vector (of i.i.d. symbols of zero mean and unit variance) to be transmitted by Alice and $x_D(t) \in \mathbb{C}^{N \times 1}$ 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:

$$y_D(t) = h_{SD} \odot \sqrt{p_D} \odot x_S(t) + \sqrt{\rho_D} h_{DD} \odot \sqrt{p_D} \odot x_D(t) + n_D(t),$$

$$y_E(t) = h_{SE} \odot \sqrt{p_E} \odot x_S(t) + h_{DE} \odot \sqrt{\rho_E} \odot x_D(t) + n_E(t),$$

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

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

$$\gamma_{DN}^{(n)} = \frac{A_n x_n}{1 + B_n y_n},$$

$$\gamma_{EN}^{(n)} = \frac{C_n x_n}{1 + D_n y_n},$$

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

Note that we will assume that the channel amplitudes $A_n$, $B_n$, $C_n$, and $D_n$, $y_n$ 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]:

$$R_s(x, y) = \frac{1}{N} \sum_{n=1}^{N} \max \{0, \Delta R_n(x_n, y_n)\},$$

where $\Delta R_n(x_n, y_n) = \log(1 + \gamma_{DN}^{(n)}) - \log(1 + \gamma_{EN}^{(n)})$. 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 $R_s(x, y)$ through power allocations at both Alice and Bob. And most of the technical details are aimed to reduce the computational complexity.

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

$$\tilde{R}_s(x, y) = \max \{0, R_s(x, y)\},$$

where $\Delta R(x, y) = \frac{1}{N} \sum_{n=1}^{N} \Delta R_n(x_n, y_n)$. 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: $\mathcal{R}_s(x, y)$ is no less than $\tilde{\mathcal{R}}_s(x, y)$, and max $(\mathcal{R}_s(x, y)) = \max (\tilde{\mathcal{R}}_s(x, y))$ subject to $\sum_{n=1}^{N} x_n \leq P_S$ and $\sum_{n=1}^{N} y_n \leq P_D$.

Proof: See Appendix A.

Proposition 2: For any given $x_n \in (0, +\infty)$, there is at most one stationary point for $\Delta \mathcal{R}_s(x_n, y_n)$ 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 $\frac{A_n}{C_n} < 1$ 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:

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

s.t. $\sum_{n=1}^{N} x_n \leq P_S$, $\sum_{n=1}^{N} y_n \leq P_D$,

$$x_n \geq 0, y_n \geq 0, \forall n \in \mathbb{N}. \quad (4b)$$

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

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

$$\max_{x, y} \quad \Delta \mathcal{R}(x, y) \quad (5)$$

s.t. Power constraint (4b).

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:

$$\max_x \quad \frac{1}{N} \sum_{n=1}^{N} \log(1 + \alpha_n x_n) - \frac{1}{N} \sum_{n=1}^{N} \log(1 + \beta_n x_n) \quad (6)$$

s.t. $\sum_{n=1}^{N} x_n \leq P_S$, $x_n \geq 0, \forall n \in \mathbb{N}$.

where

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

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.\footnote{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.}

The Lagrangian function of the problem can be written as:

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

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

$$\begin{aligned}
\frac{\partial \mathcal{L}}{\partial x_n} &= -\varphi_n(x_n) - \lambda_n + v = 0, \\
\sum_{n=1}^{N} x_n &\leq P_S, \forall v \geq 0, v(\sum_{n=1}^{N} x_n - P_S) = 0, \\
x_n \geq 0, \lambda_n \geq 0, \lambda_n x_n = 0, \forall n \in \mathbb{N},
\end{aligned} \quad (9)$$

where

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

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

Proposition 4: Let $x^1$ be the solution of the source power allocation phase. Then, for any $n$, if $\alpha_n \leq \beta_n$, then $x_n = 0$.

Furthermore, we have either $\sum_{n=1}^{N} x_n = 0$ or $x_n = P_S$.

Proof: See Appendix D.

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

$$\begin{aligned}
\frac{\partial \mathcal{L}}{\partial x_n} &= -\varphi_n(x_n) - \lambda_n + v = 0, \\
x_n \geq 0, \lambda_n \geq 0, \lambda_n x_n = 0, \forall n \in \Theta_y, \\
\sum_{n \in \Theta_y} x_n &\leq P_S, \forall n \in \Theta_y \quad (11)
\end{aligned}$$

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 $v$ 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.\footnote{For KKT conditions, all the Lagrange multipliers (such as $v$ and $\lambda_n$) associated with the inequalities must be non-negative. For a given $v$ and $\lambda_n = 0$, the solution to $\varphi_n(x_n) = v$ 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, $\varphi_n(x_n) = v$ 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: 
\(A_n, B_n, C_n, D_n, y_n, \forall n \in N\); Source power constraint \(P_S\); Accuracy threshold \(\varepsilon\).

Output: 
\(v^+ = \max_{n \in \Theta_\varepsilon} \{\varphi_n(0)\}; v^- = \max_{n \in \Theta_\varepsilon} \{\varphi_n(P_S)\};\)

1: Temporary variable \(\mu = 0; x_1^\dagger = x_2^\dagger = \ldots = x_N^\dagger = 0.\)
2: while \((P_S - \mu) > \varepsilon)\) do
3: \(v = \frac{v + v^-}{2};\)
4: for \(n \in \Theta_\varepsilon\) do
5: \(\text{if } v \geq \varphi_n(0) \text{ then }
6: x_n^\dagger = 0;\)
7: \(\text{else}
8: \varphi_n(x_n^\dagger) = v \text{ (By solving an equivalent quadratic equation. There is only one positive solution to this equation due to the nature of the function } \varphi_n(x_n^\dagger) \text{ and set } x_n^\dagger = x_n;\)
9: \(\text{end if}\)
10: end for
11: \(\mu = \sum_{n \in \Theta_\varepsilon} x_n^\dagger;\)
12: if \(\mu > P_S\) then
13: \(v^- = v;\)
14: else
15: \(v^+ = v;\)
16: end if
17: end while
18: return \(x_1^\dagger, x_2^\dagger, \ldots, x_N^\dagger.\)

B. Destination Power Allocation

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

\[
\max_y \frac{1}{N} \sum_{n=1}^{N} \left( \log \left( 1 + \frac{A_n x_n}{1 + B_n y_n} \right) - \log \left( 1 + \frac{C_n x_n}{1 + D_n y_n} \right) \right)
\]

s.t. \(\sum_{n=1}^{N} y_n \leq P_D, y_n \geq 0, \forall n \in N.\) (12)

By Proposition 3, the above problem is equivalent to:

\[
\max_y \frac{1}{N} \sum_{n \in \Phi} \left( \log \left( 1 + \frac{A_n x_n}{1 + B_n y_n} \right) - \log \left( 1 + \frac{C_n x_n}{1 + D_n y_n} \right) \right)
\]

s.t. \(\sum_{n \in \Phi} y_n \leq P_D, y_n \geq 0, \forall n \in \Phi.\) (13)

where

\[
\Phi = \left\{ n | n \in N, \frac{B_n}{D_n} < 1, \frac{A_n}{C_n} > \frac{B_n}{D_n} \right\},\]

and \(y_n = 0, \forall n \not\in \Phi.\)

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:

\[
\mathcal{L}(y, \lambda, v) = -\frac{1}{N} \sum_{n \in \Phi} \left( \log \left( 1 + \frac{A_n x_n}{1 + B_n y_n} \right) - \log \left( 1 + \frac{C_n x_n}{1 + D_n y_n} \right) \right)
\]

\[\lambda^T y + v \left( \sum_{n \in \Phi} y_n - P_D \right).\] (15)

The KKT conditions of (13) are:

\[
\begin{align*}
\frac{\partial \mathcal{L}}{\partial y_n} &= -\psi_n(y_n) - \lambda_n + v = 0, \\
\sum_{n \in \Phi} y_n &\leq P_D, v \geq 0, v(\sum_{n \in \Phi} y_n - P_D) = 0, \\
y_n \geq 0, \lambda_n \geq 0, \forall n \in \Phi, \forall n \in \Phi.
\end{align*}\]

where

\[
\psi_n(y_n) = \frac{1}{N} \frac{\partial \Delta R_n}{\partial y_n} = \frac{1}{N} \left( -\frac{B_n}{1 + B_n y_n} + \frac{A_n x_n}{1 + B_n y_n} \right) - \frac{B_n}{1 + B_n y_n} + \frac{B_n}{1 + D_n y_n}.
\]

Appendix C shows that for any \(n \in \Phi, \Delta R_n\) has four unique cases/patterns as shown in Fig. 12(b) (i.e., case I, case II, case III and case IV). Since \(\psi_n(y_n) = \frac{1}{N} \frac{\partial \Delta R_n}{\partial y_n}\), 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 \(\frac{B_n}{D_n} > \frac{B_n}{D_n} \) 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 \(v\) as shown in Algorithm 2.

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 \(y_n^\ast\) 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: $v^+ = \max_{n \in \Phi} \{\psi_n(0)\}$; $v^- = \max_{n \in \Phi} \{\max_{n \in \Phi} \{\psi_n(P_D)\}\}$;
1: for $n \in \Phi$ do
2: if $\psi_n(0) \leq 0$ then
3: $y_n^1 = 0$;
4: else
5: Solve $\psi_n(y_n^1) = 0$ by solving an equivalent 2nd-order polynomial which has only one positive root;
6: end if
7: end for
8: if $(\sum y_n^1 > P_D$ or $v^- > 0)$ then
9: Temporary variable $\mu = 0$; $y_n^1 = 0, \forall n \in \Phi$.
10: while ($|P_D - \mu| > \varepsilon$) do
11: $v = v^+ + \frac{v^-}{2}$;
12: for $n \in \Phi$ do
13: if $v \geq \psi_n(0)$ then
14: $y_n^1 = 0$;
15: else
16: Solve $\psi_n(y_n^1) = v$ 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;
17: end if
18: end for
19: $\mu = \sum_{n \in \Phi} y_n^1$;
20: if $\mu > P_D$ then
21: $v^- = v$;
22: else
23: $v^+ = v$;
24: end if
25: end while
26: end if
27: return $y_n^1, \forall n \in \Phi$.

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

$$\mathcal{R}_n^1 = \max \left\{0, \log \left(\frac{A_n}{C_n}\right)\right\}. \quad (20)$$

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

$$\mathcal{R}^1 = \sum_{n \notin \Phi} \left[\log \left(\frac{A_n}{C_n}\right) + \log \left(\frac{D_n}{B_n}\right)\right] + \sum_{n \in \Phi} \max \left\{0, \log \left(\frac{A_n}{C_n}\right)\right\}$$

$$= \sum_{n=1}^{N} \max \left\{0, \log \left(\frac{A_n}{C_n}\right) + \max \left\{0, \log \left(\frac{D_n}{B_n}\right)\right\} \right\}. \quad (21)$$

In this upper bound, the term $\max \{0, \log(D_n/B_n)\}$ 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 $v$ 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 $O(2N_{two-phase} \log_{3}(\frac{1}{\varepsilon}))$. A brute-force search of the multiplier $\nu$ would have $O(2N_{two-phase} \frac{1}{\varepsilon})$ as the complexity order. Note that, the simulation results 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:

$$\max_{x,y} \quad \frac{1}{N} \sum_{n \in \Theta_y} \Delta R_n(x_n, y_n)$$

s.t. \hspace{1cm} \frac{1}{N} \sum_{n=1}^{N} \log \left(1 + \frac{A_n x_n}{1 + y_n B_n}\right) \geq C_{SD}, \quad (22)$$

Power constraint (4b).

where $C_{SD}$ 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 $\Delta R_n(x_n, y_n) < 0, \forall n \notin \Theta_y$ (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 $n \in \mathbb{N}$. The larger is the secrecy capacity (the first line in

\textsuperscript{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., \( \Delta R_n(x_n, y_n) \leq 0 \) for some \( n \)). But as long as \( C_S \geq \frac{1}{N} \sum_{n \in \Theta} \max(\Delta R_n(x_n, y_n), 0) > 0 \), there are always some secure subcarriers, and a packet encoded across all the subcarriers to meet the secrecy capacity \( C_S \) (and the rate constraint \( C_{SD} \)) is said to be secure with the secrecy capacity \( C_S \).

Although the rate constraint introduces a complex situation where \( x_n, y_n \), and \( y_n \) 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, \( y \) is fixed and the optimization problem (22) reduces to the following convex problem:

\[
\max_x \quad \frac{1}{N} \sum_{n \in \Theta} \left[ \log(1 + \alpha_n x_n) - \log(1 + \beta_n x_n) \right] \\
\text{s.t.} \quad \frac{1}{N} \sum_{n = 1}^{N} \log(1 + \alpha_n x_n) \geq C_{SD}, \\
\sum_{n = 1}^{N} x_n \leq P_S, x_n \geq 0, \forall n \in \mathbb{N}. \tag{23}
\]

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

\[
\mathcal{L}(x, \lambda, \mu, \nu) = -\frac{1}{N} \sum_{n \in \Theta} \left( \log(1 + \alpha_n x_n) - \log(1 + \beta_n x_n) \right) + \lambda \left( \sum_{n = 1}^{N} \log(1 + \alpha_n x_n) - C_{SD} \right) + \mu^T x + \nu \left( \sum_{n = 1}^{N} x_n - P_S \right). \tag{24}
\]

The KKT conditions of (23) are:

\[
\frac{\partial \mathcal{L}}{\partial x_n} = -\tilde{\varphi}_n(x_n) - \frac{\lambda}{N} \frac{x_n}{1 + \alpha_n x_n} - \mu_n + \nu = 0, \\
\lambda \geq 0, \quad \frac{1}{N} \sum_{n = 1}^{N} \log(1 + \alpha_n x_n) \geq C_{SD}, \\
\lambda \left( \sum_{n = 1}^{N} \log(1 + \alpha_n x_n) - C_{SD} \right) = 0, \\
x_n \geq 0, \mu_n \geq 0, \mu_n x_n = 0, \forall n \in \mathbb{N}, \\
\nu \geq 0, \sum_{n = 1}^{N} x_n \leq P_S, \nu \left( \sum_{n = 1}^{N} x_n - P_S \right) = 0, \tag{25}
\]

where \( \tilde{\varphi}_n(x_n) = \varphi_n(x_n) \) as defined by (10) for \( n \in \Theta_y \), and \( \varphi_n(x_n) = 0 \) for \( n \notin \Theta \). From the first equation in (25), we see that if \( \lambda \) is fixed, \( \nu \) is a decreasing function of \( x_n \), and if \( \nu \) 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 \( \nu \) is to meet the power constraint, and the bisection search of \( \lambda \) is to meet the rate constraint. For each given pair of \( \nu \) and \( \lambda \), the first equation in (25) is equivalent to a quadratic equation of \( x_n \) and hence has a closed-form solution for \( x_n \).

### B. Destination Power Allocation

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

\[
\max_y \quad \frac{1}{N} \sum_{n \in \Theta_y} \left( \log(1 + \frac{A_n x_n}{1 + B_n y_n}) - \log(1 + \frac{C_n x_n}{1 + D_n y_n}) \right) \\
\text{s.t.} \quad \frac{1}{N} \sum_{n = 1}^{N} \log(1 + \frac{A_n x_n}{1 + B_n y_n}) \geq C_{SD}, \\
\sum_{n = 1}^{N} y_n \leq P_D, y_n \geq 0, \forall n \in \mathbb{N}. \tag{26}
\]

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

\[
\max_y \quad \frac{1}{N} \sum_{n \in \Theta_y} \left( \log(1 + \frac{A_n x_n}{1 + B_n y_n}) - \log(1 + \frac{C_n x_n}{1 + D_n y_n}) \right) \\
\text{s.t.} \quad \frac{1}{N} \sum_{n = 1}^{N} \log(1 + \frac{A_n x_n}{1 + B_n y_n}) \geq \tilde{C}_{SD}, \\
\sum_{n \in \Theta_y} y_n \leq P_D, y_n \geq 0, \forall n \in \Psi_y, \tag{27}
\]

where

\[
\Psi_y = \Theta_y \cap \Phi, \\
\tilde{C}_{SD} = C_{SD} - \frac{1}{N} \sum_{n \in \Psi_y} \log \left( 1 + \frac{A_n x_n}{1 + B_n y_n} \right), \\
\Psi_y^\perp = \{ n | n \in \mathbb{N}, n \notin \Psi_y \}, \tag{28}
\]

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 $y^{(k)}$ into the equation (28) to obtain a new $\Psi_y^{(k+1)}$. If $\Psi_y^{(k)} = \Psi_y^{(k+1)}$, stop, and $y^{(k)}$ 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

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

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

$$F_T(y, y^{(k)}) = F(y^{(k)}) + (\nabla F(y^{(k)}))^T(y - y^{(k)})$$

$$= F(y^{(k)}) + \frac{1}{N} \sum_{n \in \Psi_y} \phi_n \cdot (y_n - y^{(k)}),$$

where $\phi_n = -\frac{B_n}{1 + B_n y^{(k)}_n} + \frac{1}{1 + B_n y^{(k)}_n}$.

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

$$y^{(k+1)} = \arg \max_y \left\{ \frac{1}{N} \sum_{n \in \Psi_y} \left( \log(1 + \frac{A_n x_n}{1 + B_n y_n}) - \log \left( 1 + \frac{C_n x_n}{1 + D_n y_n} \right) \right) \right\}$$

subject to $F_T(y, y^{(k)}) \geq \tilde{C}_SD$

$$\sum_{n \in \Psi_y} y_n \leq P_D, y_n \geq 0, \forall n \in \Psi_y.$$  

The Lagrangian function of this problem is:

$$\mathcal{L}(y, \lambda, \mu, \nu) =$$

$$-\frac{1}{N} \sum_{n \in \Psi_y} \left( \log(1 + \frac{A_n x_n}{1 + B_n y_n}) - \log \left( 1 + \frac{C_n x_n}{1 + D_n y_n} \right) \right)$$

$$- \mu^T y + \nu \left( \sum_{n \in \Psi_y} y_n - P_D \right) + \lambda \left( \tilde{C}_SD - F_T(y, y^{(k)}) \right).$$

The KKT conditions of (32) are:

$$\frac{\partial \mathcal{L}}{\partial y_n} = -\psi_n(y_n) - \frac{A_n x_n}{1 + B_n y_n} - \mu_n + \nu = 0,$$

$$y_n \geq 0, \mu_n \geq 0, \mu_n y_n = 0, \quad \forall n \in \Psi_y,$$

$$\nu \geq 0, \sum_{n \in \Psi_y} y_n \leq P_D, \nu \left( \sum_{n \in \Psi_y} y_n - P_D \right) = 0,$$

$$\lambda \geq 0, F_T(y, y^{(k)}) - \tilde{C}_SD \geq 0, \lambda \left( \tilde{C}_SD - F_T(y, y^{(k)}) \right) = 0,$$

(34)

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 $\nu$ 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 $\nu$, and $\zeta$ denote that for $\lambda$.

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

For destination power allocation, the complexity is $\mathcal{O}(N_{2D,D} N_{\Psi_y} N_{SCP} (\log_2(\frac{1}{\varepsilon}) + \log_2(\frac{1}{\zeta})))$ 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 $N_{\mu v = \text{phase}}$.

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 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 $x_S^{(m)}(t) \in \mathbb{C}^{N \times 1}$ be the message sent to the $m$th destination, and $y_D^{(m)}(t) \in \mathbb{C}^{N \times 1}$ 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 $10^{-4}$. For the 2D bisection, the threshold is $10^{-3}$.
the \(m\)th destination. Then, we can write:

\[
y_D^{(m)}(t) = h_S^{(m)} \circ P_S^{(m)} \circ x_S^{(m)}(t) + \sqrt{\rho}h_D^{(m)} \circ P_D^{(m)} \circ x_D^{(m)}(t) + n_D^{(m)}(t). \quad (35)
\]

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

\[
y_E^{(m)}(t) = h_S^{(m)} \circ P_S^{(m)} \circ x_S^{(m)}(t) + h_D^{(m)} \circ P_D^{(m)} \circ x_D^{(m)}(t) + n_E^{(m)}(t). \quad (36)
\]

So, the secrecy capacity in bits per channel use for the \(m\)th destination/Bob is:

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

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 \(x^{(m)} = P_S^{(m)}, y^{(m)} = P_D^{(m)}, A_{m,n} = |h_{SD}^{(m,n)}|^2, B_{m,n} = |h_{DD}^{(m,n)}|^2, C_{m,n} = |h_{SE}^{(m,n)}|^2, D_{m,n} = |h_{DE}^{(m,n)}|^2\), and \(m,n \in P_S^{(m,n)}\).

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

\[
\begin{align*}
\max & \quad \sum_{m=1}^{M} \mathcal{R}_m(x^{(m)}, y^{(m)}) \\
\text{s.t.} & \quad P_S, P_D, P_{D,m}, C_m \geq 0, m \in M, \forall n \in \mathbb{N}, \forall m \in M, \tag{39}
\end{align*}
\]

where \(1\) is the vector of all ones, \(P_{D,m}\) and \(C_m\) are the power and the target rate for Bob \(m\), and

\[
C_S^{(m)} = \frac{1}{MN} \sum_{n=1}^{N} \log\left(1 + \frac{x_{m,n}A_{m,n}}{1 + y_{m,n}B_{m,n}}\right). \quad (40)
\]

To present a fast algorithm to solve the problem (39), we first denote its solution by \((\mathcal{R}_m, x_{S,m}, y_{M})\) where \(\mathcal{R}_m\) is the maximum of the objective function, and \(x_{S,m} = \{x_{s,m}^{(m)} \mid \forall m \in M\}\) and \(y_{M} = \{y_{m}^{(m)} \mid \forall m \in M\}\) are the corresponding sets of vectors of power allocations at the source and the destinations. Furthermore, \(\mathcal{R}_m\) depends on \(P_S, P_{D,m}, \forall m \in M\) and \(C_m, \forall m \in M\). We will also express this relationship by \((\mathcal{R}_m, P_{D,m,1}, C_m)\) or simply \(\mathcal{R}_m(\mathcal{P}_{D,M,1})\). Note that while \(\mathcal{R}_m\) and \(P_{D,m,1}\) are always scalars here, \(P_D\) and \(C_m\) can be viewed as sets, i.e., \(P_D = \{P_{D,m} \mid \forall m \in M\}\) and \(C_m = \{C_m \mid \forall m \in M\}\).

It is obvious that if the set \(M\) 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 \(M\) into two subsets \(M_1\) and \(M_2\) where each subset has only one entry. Then, we can obtain \(\mathcal{R}_{M_1}(P_{S,M_1})\) and \(\mathcal{R}_{M_2}(P_{S,M_2})\) for any given \(P_{S,M_1}\) satisfying \(P_S \geq P_{S,M_1} \geq 0\). For \(M_1\), there is a minimum amount of power \(P_{S,M_1}^{1}\) to meet the rate constraint, which can be obtained by the standard water-filling algorithm. Similarly, for \(M_2\), there is a corresponding \(P_{S,M_2}^{1}\). If \(\mathcal{R}_{M_1}(P_{S,M_1}) \leq \mathcal{R}_{M_2}(P_{S,M_2})\) 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 \(M\) from \(\min(\mathcal{R}_{M}, P_{S,M_1}), \mathcal{R}_{M_2}(P_{S,M_2})\). This is because \(\mathcal{R}_{M_2}(P_{S,M_2})\) is strictly increasing (or possibly staying at zero initially) with increasing \(P_{S,M}\) according to Proposition 4. In this case, \(\mathcal{R}_{M_1}(P_{S,M}) = \mathcal{R}_{M_2}(P_{S,M})\).

Similarly, if \(\mathcal{R}_{M_1}(P_{S,M_1}) \geq \mathcal{R}_{M_2}(P_{S,M_2})\) which is denoted as Case II as shown in Fig. 4, then \(\mathcal{R}_{M_1}(P_{S,M}) = \mathcal{R}_{M_2}(P_{S,M})\). 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 \(P_{S,M_1}^{1}\), such that either \(\mathcal{R}_{M_1}(P_{S,M_1}^{1}) = \mathcal{R}_{M_2}(P_{S,M_2})\) and hence \(\mathcal{R}_{M}(P_{S,M}) = \mathcal{R}_{M_2}(P_{S,M})\).

If \(M > 2\), we can start with the above decomposition from \(M\) to \(M_1\) and \(M_2\). Then, we can further decompose \(M_1\) and/or \(M_2\) into smaller subsets. We can repeat the above process until each
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 \( \text{Minimum\_Power\_Require}(\cdot) \) is to calculate the minimum required power to achieve the target rates which can be obtained by the standard waterfilling algorithm. The function \( \text{Two\_Phases\_Allocation\_with\_Rate}(\cdot) \) is the entire algorithm developed in section IV. The function \( \text{Secrecy\_Capacity}(\cdot) \) computes the corresponding secrecy capacity.

### Algorithm 4: \((R_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_BC}(M, P_S, P_{D,M}, C_M)\) - Solution to (39),

1. if size(M) \( \geq 2 \) then
   2. \( M_1 = \{M \backslash y\} \), \( M_2 = M \backslash M_1 \);
   3. \( P_{S,M_1}^i = \text{Minimum\_Power\_Require}(M_1, C_M) \);
   4. \( P_{S,M_2}^i = \text{Minimum\_Power\_Require}(M_2, C_M) \);
   5. \((R_{M_1}, x_{M_1}, y_{M_1}) = \text{Recursive\_Bisection\_Search\_BC}(M_1, P_{S,M_1}^i, P_{D,M}, C_M) \);
   6. \((R_{M_2}, x_{M_2}, y_{M_2}) = \text{Recursive\_Bisection\_Search\_BC}(M_2, P_S - P_{S,M_1}^i, P_{D,M}, C_M) \);
   7. if \( R_{M_2} \geq R_{M_1} \) then
      8. return \( R_{M_1}, [x_{M_1}, x_{M_2}], [y_{M_1}, y_{M_2}] \);
   9. else
      10. \((R_{M_1}, x_{M_1}, y_{M_1}) = \text{Recursive\_Bisection\_Search\_BC}(M_1, P_{S,M_2}^i, P_{D,M}, C_M) \);
      11. \((R_{M_2}, x_{M_2}, y_{M_2}) = \text{Recursive\_Bisection\_Search\_BC}(M_2, P_{S,M_2}^i, P_{D,M}, C_M) \);
      12. if \( R_{M_1} \leq R_{M_2} \) then
         13. return \( R_{M_2}, [x_{M_1}, x_{M_2}], [y_{M_1}, y_{M_2}] \);
      14. else
         15. \( P_{S,M_1}^* = P_S - P_{S,M_2}^i \), \( P_{S_1}^* = P_{S,M_1}^i \);
         16. while \((\mu > \epsilon)\) do
            17. \( P_{S_1} = \frac{P_{S,M_2}^i + P_{S_1}^*}{2} \), \( P_{S_2} = P_S - P_{S_1}^* \);
            18. \((R_{M_1}, x_{M_1}, y_{M_1}) = \text{Recursive\_Bisection\_Search\_BC}(M_1, P_{S_1}, P_{D,M}, C_M) \);
            19. \((R_{M_2}, x_{M_2}, y_{M_2}) = \text{Recursive\_Bisection\_Search\_BC}(M_2, P_{S_2}, P_{D,M}, C_M) \);
            20. if \( R_{M_1} \geq R_{M_2} \) then
               21. \( P_{S_1}^* = P_{S_1}^* \);
               22. else
                  23. \( P_{S_1}^* = P_{S_1}^* \);
                  24. end if
            25. end while
            26. return \( R_M, [x_M, x_M], [y_M, y_M] \);
      27. end if
   28. end if
   29. else
      30. \((x_M, y_M) = \text{Two\_Phases\_Allocation\_with\_Rate}(P_{S,M}, P_D) \);
      31. \( R = \text{Secrecy\_Capacity}(x_M, y_M) \);
      32. return \( R, x_M, y_M \);
      33. end if

\[ \text{Fig. 5. A network with multiple sources - also referred to as “multiple access (MAC)”}. \]

### 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 \( x_M^m(m) \), \( m \in \mathbb{N} \), the full-duplex destination transmits the artificial noise \( x_D^m(m) \), \( m \in \mathbb{N} \), 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:

\[
\begin{align*}
\max_{x(m), y(m), m \in \mathbb{M}} & \quad \min_{m \in \mathbb{M}} R_M(x(m), y(m)) \\
\text{s.t.} & \quad 1^T x(m) \leq P_{S,m} \sum_{m=1}^M 1^T y(m) \leq P_D, C_{SD}^m(m) \geq C_m, \\
& \quad x_{m,n} \geq 0, y_{m,n} \geq 0, \forall n \in \mathbb{N}, \forall m \in \mathbb{M},
\end{align*}
\]

(41)

where \( P_{S,m}, C_m \) and \( C_{SD}^m(m) \) 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 \((R_M, x_M, y_M)\) where \( R_M, x_M \) and \( y_M \) are similarly defined as before. The \( m \)th entry of the \( M \times 1 \) vector \( z_M(m) \), denoted by \( z_M(m) \), 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 \( m \), \( z_M(m) \) is set to be zero. Otherwise, it is set to be one. Since \( R_M \) depends on \( P_{S,m} \), \( \forall m \in \mathbb{M}, P_D \) and \( C_m, \forall m \in \mathbb{M}, \) we will express such a dependency by \( R_M(P_{D,m}) \) where \( P_{D,m} \) 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 \( M \).

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 \( R_M(P_{D,m}) \) is a non-decreasing function of \( P_{D,m} \).

Obviously, if \( M = 1 \) or equivalently \( M \) 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 \( M \) be partitioned into \( M_1 \) and \( M_2 \). In this case, each of \( M_1 \) and \( M_2 \) has only one entry.
Then, we can obtain $R_M(0)$ and $R_M(P_D)$, where all the destination power is made available only to $M_2$. If $R_M(0) \leq R_M(P_D)$, which is Case I shown in Fig. 6, then we have obtained the optimal secrecy capacity for $M$: $R_M(P_{D,M}) = \min(R_M(0), R_M(P_D))$. However, it is possible that there is $P_{D,M_1} < P_D$ such that $R_M(P_{D,M_1}) = R_M(P_{D,M_2})$ if and only if $P_{D,M_1} \leq P_{D,M_2} \leq P_D$. In this case, we can utilize $P_D - P_{D,M_1}$ for $M_1$ so that the secrecy capacity for $M_1$ can be increased although the optimal secrecy capacity for $M$ remains the same. See Case I in Fig. 6.

If Case I does not hold, we can similarly obtain $R_M(0)$ and $R_M(P_D)$, where all the destination power is made available only to $M_1$. If $R_M(P_D) \leq R_M(0)$, which is Case II shown in Fig. 6, then we have obtained the optimal secrecy capacity for $M$: $R_M(P_{D,M}) = \min(R_M(0), R_M(P_D))$. However, it is possible that there is $P_{D,M_1} < P_D$ such that $R_M(P_{D,M_1}) = R_M(P_{D,M_2})$ if and only if $P_{D,M_1} \leq P_{D,M_2} \leq P_D$. In this case, we can utilize $P_D - P_{D,M_1}$ for $M_1$ to increase the secrecy capacity for $M_1$ although the optimal secrecy capacity for $M$ 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 $P_{D,M_1}^*$ such that $R_M(P_{D,M_1}^*) = R_M(P_{D,M_2}^*)$ and hence the optimal secrecy capacity for $M$ is $R_M(P_{D,M}) = R_M(P_{D,M_1}^*)$.

More generally, if $M > 2$, we can first partition $M$ into $M_1$ and $M_2$ and compute the optimal binary partition of the destination power $P_D$ into $P_{D,M_1}$ and $P_{D,M_2} = P_D - P_{D,M_1}$. If $M_i$ for some $i \in \{1, 2\}$ has more than one entries, we then further partition $M_i$ into two smaller sets $M_{i,1}$ and $M_{i,2}$ and compute the optimal binary partition of any given power value $P_{D,M_i}$ into $P_{D,M_{i,1}}$ and $P_{D,M_{i,2}} = P_{D,M_i} - P_{D,M_{i,1}}$.

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 $A_n < C_n, \forall n \in N$ (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 $C_{S,D,1}$ (which is obtained by the standard waterfilling algorithm). And the resulting secrecy capacity $R_{S,E,1}$ is zero for this channel realization as expected.

1: if size(M) \(\geq 2\) then
2: \(M_1 = \left\lceil \frac{M}{2} \right\rceil, M_2 = M \setminus M_1\)
3: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_1, P_{S,M}, 0, C_M);\)
4: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_2, P_{S,M}, P_D, C_M);\)
5: if \(R_M \geq R_{M_1}\) then
6: \(\text{return } R_M, [z_M, z_{M_2}], [x_M, x_{M_2}], [y_M, y_{M_2}];\)
7: else
8: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_1, P_{S,M}, P_D, C_M);\)
9: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_2, P_{S,M}, 0, C_M);\)
10: if \(R_M \leq R_{M_1}\) then
11: \(\text{return } R_M, [z_M, z_{M_2}], [x_M, x_{M_2}], [y_M, y_{M_2}];\)
12: else
13: \(P_{D_1}^+ = P_D, P_{D_1}^- = 0;\)
14: while \((\mu > 0)\) do
15: \(P_{D_1} = \frac{P_{D_1}^+ + P_{D_1}^-}{2};\)
16: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_1, P_{S,M}, P_D, C_M);\)
17: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M_2, P_{S,M}, P_D, C_M);\)
18: \(\mu = |R_M - R_{M_1}|;\)
19: if \(R_M > R_{M_1}\) then
20: \(P_{D_1}^+ = P_D;\)
21: else
22: \(P_{D_1}^- = P_D;\)
23: end if
24: end while
25: return \(R_M, [z_M, z_{M_2}], [x_M, x_{M_2}], [y_M, y_{M_2}];\)
26: end if
27: end if
28: else
29: \((x_M, y_M) = \text{Two\_Phases\_Allocation\_with\_Rate}(P_{S,M}, P_D);\)
30: \(R_M = \text{Secrecy\_Capacity}(x_M, y_M);\)
31: if sum(y_M) = \(P_D\) then
32: \(z_M = 0;\)
33: else
34: \(z_M = 1;\)
35: end if
36: return \(R_M, z_M, x_M, y_M;\)
37: end if

Algorithm 6: Refined solution to (41).

1: while \((M \neq \emptyset \& \& P_D > 0 \& \& z_M \neq 0 \& \& z_M \neq 1)\) do
2: \((R_M, z_M, x_M, y_M) = \text{Recursive\_Bisection\_Search\_MAC}(M, P_{S,M}, P_D, C_M);\)
3: \(R_M = \text{Secrecy\_Capacity}(x_M, y_M);\)
4: \(K = \{m | R_M, z_M(m) = 1, \forall m \in M\};\)
5: \(P_D = P_D - \text{Sum}(y_M);\)
6: 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 \(C_{SD,D}^0 = 0.9C_{SD,I}\). The corresponding achieved rate is denoted by \(C_{SD,II}\), the curve of which is as expected, indistinguishable from that of \(C_{SD,D}^0\). The resulting secrecy capacity is denoted by \(R_{SE,II}\), 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 \(R_{SE,III}\) and the resulting data rate is \(C_{SD,III}\).

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.
C. Joint Power Allocation for Multiple Destinations

We choose $C_m = \gamma C^\dagger_m$, where $C^\dagger_m$ is the maximum achievable data rate from Alice to Bob when $P_{S,M}$ 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 $C_m = \gamma C^\dagger_m$ where $C^\dagger_m$ is the maximum achievable rate from the $m$th source to the destination with the power $P_{S,m} = P_{S,M}$ 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.

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 $C_m = \gamma C^\dagger_m$ with $\gamma = 0.9$. Define the gain of the multi-user strategy over the single-user strategy as

$$\text{Gain} = \frac{R_M - \min(R_{1}, R_{2})}{\min(R_{1}, R_{2})}$$

(42)

where $R_M$ is the optimal multi-user secrecy capacity achieved via joint power allocation under two users with total power $P$, and $R_1$ and $R_2$ 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
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:

\[
R(x, y) = \frac{1}{N} \sum_{n=1}^{N} \max \{0, \Delta R_n(x_n, y_n)\} \\
\geq \max \left\{0, \frac{1}{N} \sum_{n=1}^{N} \Delta R_n(x_n, y_n) \right\} = \hat{R}(x, y), \tag{A.1}
\]

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 \((x^*, y^*) = \arg \max(R(x, y))\) subject to \(\sum_{n=1}^{N} x_n \leq P_S\) and \(\sum_{n=1}^{N} y_n \leq P_D\). Obviously, if \(\Delta R_n(x^*_n, y^*_n) < 0\) 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 \(\Delta R_n(x^*_n, y^*_n) \geq 0\). Then we have

\[
\max \left\{0, \Delta R_n(x^*_n, y^*_n) \right\} = \hat{R}(x^*, y^*). \tag{A.2}
\]

Since \(R(x, y) \geq \hat{R}(x, y)\), the above implies

\[
\max(R(x, y)) = \max(\hat{R}(x, y)). \tag{A.3}
\]

\[
\begin{align*}
\frac{\partial \Delta R_n}{\partial y_n} &= \frac{B_n}{1 + B_n y_n + A_n x_n} - \frac{B_n}{1 + B_n y_n} \\
&\quad - \frac{D_n}{1 + D_n y_n + C_n x_n} + \frac{D_n}{1 + D_n y_n}.
\end{align*}
\]

Setting it equal to zero, we have

\[
y_n^2 + by_n + c = 0, \tag{B.2}
\]

where

\[
a = A_n D_n - B_n C_n, \quad b = 2(A_n - C_n), \quad c = \frac{A_n B_n - C_n D_n + (B_n - D_n) A_n C_n x_n}{B_n D_n}. \tag{B.3}
\]

Because (B.2) is quadratic and it has at most two positive roots, the function \(\Delta R_n(x_n, y_n)\) 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 $\Delta R_n(x_n, y_n)$ 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 $\Delta R_n(x_n, y_n)$ with regard to $y_n \in (0, +\infty)$. One can also verify that

$$\lim_{y_n \to +\infty} \Delta R_n(x_n, y_n) = 0^+, \text{ when } \frac{A_n}{C_n} > \frac{B_n}{D_n},$$

$$\lim_{y_n \to -\infty} \Delta R_n(x_n, y_n) = 0^-, \text{ when } \frac{A_n}{C_n} < \frac{B_n}{D_n}. \tag{C.1}$$

When $\frac{B_n}{D_n} > 1$, the patterns of $\Delta R_n(x_n, y_n)$ 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

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

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

which means that (B.2) has no positive root and hence there is no stationary point for $\Delta R_n(x_n, y_n)$ with respect to $y_n \in (0, +\infty)$. Also, since $\Delta R_n(x_n, 0) > 0$ and $\lim_{y_n \to +\infty} R_n(x_n, y_n) = 0^+$, $\Delta R_n(x_n, y_n)$ 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 $\Delta R_n(x_n, y_n)$ 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 $\Delta R_n(x_n, y_n)$ that is both positive and increased from $\Delta R_n(x_n, 0)$. 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 $\Delta R(x, y)$ with respect to $x_n$ is given as

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

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

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

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

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

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 $y_n^\dagger$ denote a stationary point of $\Delta R_n$ for any of the three cases. So we have that

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

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

$$\frac{D_n}{1 + D_n y_n} > \frac{D_n}{1 + D_n y_n + C_n x_n} \Rightarrow \frac{B_n}{1 + B_n y_n} > \frac{B_n}{1 + B_n y_n + A_n x_n} \Rightarrow \frac{B_n}{1 + B_n y_n} + A_n x_n > 0, \tag{E.2}$$

where $\alpha$ and $\beta$ are defined such that $\alpha > \beta$ for $y_n \in (0, y_n^\dagger)$. 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
\[
\theta = \frac{B_n}{1 + B_n y_n + A_n x_n},
\]
\[
\xi = \frac{D_n}{1 + D_n y_n + C_n x_n}.
\]
(4.4)

Since \( \frac{n}{n} > \frac{n}{B_n} \) and \( \frac{n}{n} < 1 \), it follows that
\[
\frac{D_n}{1 + D_n y_n + C_n x_n} - \frac{B_n}{1 + B_n y_n + A_n x_n} > 0,
\]
(4.5)

and
\[
\frac{D_n}{1 + D_n y_n + C_n x_n} - \frac{B_n}{1 + B_n y_n + A_n x_n} = \frac{B_n}{1 + B_n y_n + A_n x_n} > 0.
\]
(4.6)

Combining (5) and (6) yields
\[
\left( \frac{D_n}{1 + D_n y_n + C_n x_n} \right) > \frac{B_n}{1 + B_n y_n + A_n x_n} > 0.
\]
(4.7)

Now with \( \alpha > \beta \) for \( y_n \in (0, y^*) \) and \( \xi > \theta \), we obtain that
\[
\frac{\partial \psi_n(y_n)}{\partial y_n} = \frac{1}{N} (\beta \theta - \alpha \xi) < 0,
\]
(4.8)

for \( y_n \in (0, y^*) \).

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


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.