Optimal Power Allocation for Achieving Perfect Secrecy Capacity in MIMO Wire-Tap Channels

Jia Liu*, Y. Thomas Hou†, and Hanif D. Sherali‡

* Bradley Department of Electrical and Computer Engineering
† Grado Department of Industrial and Systems Engineering
Virginia Polytechnic Institute and State University, Blacksburg, VA 24061

Abstract—In this paper, we investigate optimal power allocation to achieve perfect secrecy capacity in Gaussian MIMO wire-tap channels. The number of antennas in the MIMO wire-tap channel is arbitrary at the transmitter, the intended receiver, and the eavesdropper. For this challenging non-convex optimization problem, we design a novel global optimization algorithm called branch-and-bound with reformulation and linearization technique (BB/RLT). As opposed to convex programming methods that only yield local optimal solutions, our proposed BB/RLT method guarantees finding a global optimal solution. The main contribution in this paper is that our proposed BB/RLT algorithm is the first method that solves the optimal power allocation problem for achieving perfect secrecy capacity problem in MIMO wire-tap channels. Numerical examples are also given to demonstrate the efficacy of the proposed algorithm.

I. INTRODUCTION

Security and privacy protection is one of the most important issues in wireless communications due to the broadcast nature of wireless channels—anyone within communication range can listen to the transmission in the air and could possibly extract the information. Aside from traditional cryptographic security mechanisms, information-theoretic-based security techniques have gained increasing attention in recent years.

The present information-theoretic security framework was established by Wyner [1], who developed the concept of “wire-tap channel.” Wyner showed that, if a wire-tap channel satisfies certain degradedness conditions, perfectly secure communication with non-zero rate between the transmitter and the intended receiver is achievable. Meanwhile, the eavesdropper learns nothing about the secret messages from its observations. The maximum rate of secrecy information from the transmitter to the intended receiver is called secrecy capacity. A follow-up work by Leung-Yan-Cheong and Hellman further determined the secrecy capacity of scalar Gaussian wire-tap channel [2]. Wyner’s work was later extended by Csiszár and Kőner to the case of secret communication over general broadcast channels [3] and scalar Gaussian multiple access channels [4]–[6].

Recently, researchers began to consider exploiting the physical layer characteristics of multiple-input multiple-output (MIMO) channels to further increase the capacity of secrecy communications. The secrecy communication problem for MIMO systems was first studied in [7], where Hero showed that under the restricted case where the eavesdropper is uninformed about its channel, the transmitter can enforce a zero information rate to the eavesdropper while delivering a positive information rate to the intended receiver. In [8], Negi et al. proposed a scheme to transmit artificial noise in the intended receiver’s null space so that the eavesdropper’s channel is degraded. The optimal power allocation strategy for Gaussian multiple-input single-output (MISO) wire-tap channels is studied in [9] and [10]. By somewhat different approaches, both [9] and [10] showed the same result that, under the relatively simpler MISO setting, the optimization problem can be transformed into the well-known Rayleigh quotient problem and thus can be solved analytically.

In a very recent paper, Oggier et al. [11] showed that the perfect secrecy capacity of general MIMO wire-tap channels is achieved by Gaussian signalling, thus showing the secrecy capacity inner bound in [9] is tight. However, finding the optimal power allocation under Gaussian signalling for MIMO wire-tap channels is very challenging and remains an open problem. This is because the power allocation problem for MIMO wire-tap channels is non-convex and, unlike simple MISO cases [9], [10], there does not exist a simple way to get around the complex problem structure. In this paper, our major goal is to fill this void and design an algorithm that guarantees finding an optimal solution for such a non-convex optimization problem.

The main contribution of this paper is that we provide an effective solution method to solve the optimal power allocation problem for achieving perfect secrecy capacity in MIMO wire-tap channels. To solve the power allocation problem, we propose a global optimization technique called branch-and-bound with reformulation linearization technique (BB/RLT). The basic idea of BB/RLT is that we first use RLT to obtain a linear relaxation for the original problem. By solving the linear relaxation, a global upper bound for the original problem is achieved. We then use this relaxation solution as a starting point to search for a solution that is feasible to the original problem. This feasible solution serves as a global lower bound and an incumbent optimal solution. The branch-and-bound process will then tighten the global upper bound and global lower bound during each iteration, and stop when the gap between global upper and lower bounds is sufficiently small. In this paper, we develop the key problem-specific components in BB/RLT to solve the problem and the related convergence speedup techniques. Specifically, we develop a linearization scheme to generate a higher dimensional upper-bounding problem. We also utilize a polyhedral outer approximation method.
to accurately approximate the logarithmic function. To speed up the branch-and-bound convergence process, we propose a variable selection policy based not only on the relaxation error, but also on the relative significance of the variables in our problem. To the best of our knowledge, our proposed method is the first one that guarantees finding a global optimal solution for the optimal power allocation problem in MIMO wire-tap channels.

The remainder of this paper is organized as follows. In Section II, we introduce the system model and problem formulation. Section III introduces our proposed BB/RLT solution procedure. A convergence speedup technique for the proposed BB/RLT algorithm is presented in Section IV and a numerical example is given in Section V. Section VI concludes this paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, in a Gaussian MIMO wire-tap channel, a transmitter equipped with \( n_t \) antennas wishes to reliably communicate a secret message to an intended receiver in the presence of an eavesdropper. The intended receiver has \( n_r \) antennas and the eavesdropper has \( n_e \) antennas.

A secret message \( S \) of rate \( R \) is a random integer from the set \( \{1, 2, \ldots, 2^{nR}\} \), which is transmitted in \( n \) channel uses. The transmitter transmits the coded signal \( x \in \mathbb{C}^{n_t} \) to the receiver, who decodes \( S \) based on the output \( y \in \mathbb{C}^{n_r} \). The eavesdropper overhears the output \( z \in \mathbb{C}^{n_e} \). Define the equivocation rate \( \Delta \) as \( \Delta = H(S|z)/H(S) \), i.e., the ratio between the conditional entropy conditioned on the overheard signal and the unconditional entropy. The equivocation rate is a measure of the amount of information the eavesdropper can learn about the message and quantifies the secrecy level [3]. In this paper, we focus on the case \( \Delta = 1 \), i.e., the eavesdropper learns arbitrary little information regarding message \( S \).

The received signals at the receiver and the eavesdropper can be respectively written as

\[
y = \sqrt{\rho_H} H x + n_1, \quad z = \sqrt{\rho_G} G x + n_2, \tag{1}
\]

where \( H \in \mathbb{C}^{n_r \times n_t} \) and \( G \in \mathbb{C}^{n_e \times n_t} \) are the channel gain matrices from the transmitter to the intended receiver and to the eavesdropper, respectively, \( \rho_H \) and \( \rho_G \) are the corresponding signal-to-noise ratios (SNR), respectively, and \( n_1 \in \mathbb{C}^{n_r} \), \( n_2 \in \mathbb{C}^{n_e} \) are the corresponding normalized complex circularly symmetric Gaussian random noise terms with identity covariance matrix. In this paper, it is assumed that the transmitter has full knowledge of both channels.

Denote \( Q \) the covariance matrix of the input signal, i.e., \( Q = E[xx^\top] \). Then, the power constraint on \( Q \) is \( Q \preceq I \) and \( \text{Tr}(Q) \leq 1 \). In a very recent paper [11], Oggier et al. showed that the perfect secrecy capacity of general MIMO wire-tap channels is achieved by Gaussian signaling. As a result, the perfect secrecy capacity problem of MIMO wire-tap channels can be written as follows:

\[
\begin{align*}
\text{Maximize} & \quad \log |I + \rho_H H Q H^\top| - \log |I + \rho_G G Q G^\top| \\
\text{subject to} & \quad \text{Tr}(Q) \leq 1, \quad Q \succeq 0, \quad Q = Q^\top. 
\end{align*} \tag{2}
\]

Clearly, problem (2) is a challenging non-convex optimization problem and many local maxima may exist. This can be seen by noticing that the objective function is a difference of two concave functions (in the the form of \( \log |\cdot| \)). As a result, the convexity is not definite. For such a non-convex optimization problem, conventional convex optimization methods do not work well since they yield local optimal solutions at best. In the next section, we will develop an algorithm based on global optimization approach.

III. A GLOBAL OPTIMIZATION APPROACH

We develop our algorithm by using a state-of-the-art global optimization technique called branch and bound with reformulation-linearization technique (BB/RLT) [12]. The basic idea of BB/RLT is rather simple: First, by using RLT, we obtain a linear relaxation for the original problem. By solving the linear relaxation, we have a relaxation solution that can use it as a starting point to do a local search to determine a feasible solution. Then, this feasible solution will serve as a global lower bound \( LB \) and an incumbent optimal solution to the original problem. The branch-and-bound process will then tighten \( UB \) and \( LB \) during each iteration, and stop when \( LB \geq (1-\epsilon)UB \) is satisfied.

The motivation of using BB/RLT is that BB/RLT guarantees the convergence to a global optimal solution for any non-convex optimization problem as long as the feasible region of the problem is compact (see [12] for further details). This condition is clearly satisfied for problem (2). We summarize the general framework of BB/RLT in Algorithm 1.

We note that the BB/RLT method in Algorithm 1 is a general framework. In order to use Algorithm 1 to solve problem (2), several key problem-specific components remain to be developed and the design is far from trivial. First and foremost, how to construct an RLT linear relaxation for problem (2) is critical to the success of using BB/RLT. Also, the branch-and-bound strategy and the according convergence speed up technique is also very important. In what follows, we will describe in detail how to develop these problem-specific components.

A. Objective Function Linearization

In problem (2), the objective function is nonlinear. To linearize it, we introduce two new variables \( A = \ln |I + \rho_H H Q H^\top| \)}
\[ \sum_{i=1}^{n} \rho_i D_{i}^{H}Q_{i}^{H} \] and \( B = \ln |I + \rho_{G} D_{i}Q_{i}^{H}|. \) The objective function can then be linearized to
\[
\text{Maximize } \frac{1}{2} \ln (A - B).
\]
For convenience, we let \( D = I + \rho_{H} D_{i}Q_{i}^{H} \) and \( R = I + \rho_{G} D_{i}Q_{i}^{H}. \) It is clear that, to evaluate \( A \) and \( B, \) we need to compute \( \ln |D| \) and \( \ln |R|. \)

Generally, determinant computation is cumbersome because a matrix’s determinant is in essence a high-order polynomial of all matrix entries. Fortunately, in problem (2), there exist special structures in \( D \) and \( R \) to make determinant computation easier. Noting that \( D \) and \( R \) are positive definite Hermitian matrices, Cholesky decompositions of \( D \) and \( R \) exist. Take \( D \) for example, we have
\[
A = \ln |D| = \ln \left| D^{(L)} \cdot (D^{(L)})^{H} \right| = \ln (\prod_{i=1}^{n} \| d_{i,i}^{(L)} \|^2) = \sum_{i=1}^{n} \ln \| d_{i,i}^{(L)} \|^2 = \sum_{i=1}^{n} \left( \ln \Re^2(d_{i,i}^{(L)}) + \Im^2(d_{i,i}^{(L)}) \right),
\]
where \( D^{(L)} \) is a lower triangular matrix and \( d_{i,i}^{(L)} \) denotes the \( i \)-th diagonal entry of \( D^{(L)}. \) Noting that \( A \) is a summation of the log values of the square of \( d_{i,i}^{(L)} \)'s norm, we can introduce two new groups of variables \( Y_i \) and \( X_i \) to perform reformulation as follows:
\[
A = \sum_{i=1}^{n} Y_i, \quad Y_i = \ln X_i, \quad X_i = \Re^2(d_{i,i}^{(L)}) + \Im^2(d_{i,i}^{(L)}).
\]

Likewise, after introducing two more groups of variables \( V_i \) and \( W_i, \) \( B \) can be computed using the same method.

Another difficulty in linearizing the objective function lies in handling \( \ln \{ \}. \) Our basic idea to linearize the curve of the log function is to construct a polyhedral outer approximation. As shown in Fig. 2, the curve \( y = \ln x \) over an interval can be relaxed to a polyhedron formed by three tangential segments I, II, and III, which are constructed at \((x_L, \ln x_L), (x_B, \ln x_B), \) and \((u_X, \ln u_X), \) where \( x_B \) is computed as follows:
\[
x_B = \frac{x_L x_U (\ln x_U - \ln x_L)}{x_U - x_L}.
\]

Here, \( x_B \) is the \( x \)-value for the point at the intersection of the extended tangent segments I and III. Segment IV is the chord that joins \((x_L, \ln x_L)\) and \((u_X, \ln u_X).\) The polyhedron defined by the four line segments can be described by the following four linear constraints:
\[
x_L \cdot y - x \leq x_L (\ln x_L - 1), \quad x_B \cdot y - x \leq x_B (\ln x_B - 1), \quad x_U \cdot y - x \leq x_U (\ln x_U - 1), \quad (x_U - x_L) y + (\ln x_L - \ln x_U) x \geq x_U \cdot \ln x_L - x_L \cdot \ln x_U.
\]

We remark that this polyhedral approximation is a very accurate approximation of the log function. For illustrative purpose, the \( x_L \)-value in Fig. 2 is deliberately chosen to be close to zero to generate a significant curvature. Otherwise, segments I, II, III, and IV almost superimpose one another, making the figure hard to discern.

### B. Linear Relaxation of Cholesky Decomposition

As indicated earlier, \( D \) and \( R \) can be decomposed into a product form by Cholesky decomposition. Now, it remains to linearize the product terms in the Cholesky decompositions. Take \( D \) for example, we have the following relationship between the entries of \( D \) and the entries of \( D^{(L)}: \)
\[
d_{(i,j)} = \sum_{k=1}^{j} d_{(i,k)}^{(L)}\tilde{d}_{(j,k)}^{(L)}
\]
for $1 \leq i \leq n_t$, $1 \leq j \leq i$, and $1 \leq k \leq j$. Expanding the RHS of (4), we have

$$\Re(d_{i,j}) = \sum_{k=1}^{j} \left[ \Re(d_{i,k}^{(L)}) \Re(d_{j,k}^{(L)}) + \Im(d_{i,k}^{(L)}) \Im(d_{j,k}^{(L)}) \right],$$

$$\Im(d_{i,j}) = \sum_{k=1}^{j} \left[ \Im(d_{i,k}^{(L)}) \Re(d_{j,k}^{(L)}) - \Re(d_{i,k}^{(L)}) \Im(d_{j,k}^{(L)}) \right].$$

For the diagonal entries of $D$, we can further simplify the expansions to

$$\Re(d_{i,i}) = \sum_{k=1}^{i} \left[ \Re^2(d_{i,k}^{(L)}) + \Im^2(d_{i,k}^{(L)}) \right], \quad \Im(d_{i,i}) = 0.$$

Now, we introduce the so-called RLT variables to linearize these expansion expressions. For convenience, we use a generic term $(xy)$ to represent the terms $\Re(d_{i,k}^{(L)} \Re(d_{j,k}^{(L)})), \Im(d_{i,k}^{(L)}) \Im(d_{j,k}^{(L)}), \Re(d_{i,k}^{(L)}) \Im(d_{j,k}^{(L)})$, and $\Re(d_{i,k}^{(L)}) \Im(d_{j,k}^{(L)})$. Also, we use a generic term $x^2$ to represent the terms $\Re^2(d_{i,k}^{(L)})$ and $\Im^2(d_{i,k}^{(L)})$.

For a product term $xy$, we have

$$x - x_L \geq 0, \quad x - y \geq 0, \quad y - y_L \geq 0, \quad y_U - y \geq 0,$$

where $x_L$ and $y_L$ denote the lower bounds on $x$ and $y$, respectively, and $x_U$ and $y_U$ denote the upper bounds on $x$ and $y$, respectively. From (5), we can derive the following four bounding factor constraints:

$$(x - x_L) \times (y - y_L) \geq 0, \quad (x - x_U) \times (y_U - y) \geq 0,$$

$$(x_U - x) \times (y - y_L) \geq 0, \quad (x_U - x) \times (y_U - y) \geq 0,$$

which can be further expanded to the following four constraints:

$$xy - yLx - x_Ly \geq -x_LyL, \quad -xy + y_Ux + x_Ly \geq x_Ly_U,$$

$$-xy + y_Lx + x_Uy \geq y_Ux_L, \quad xy - y_Ux - x_Uy \geq -x_Uy_U.$$

Similarly, for a general square term $x^2$, we have

$$x - x_L \geq 0, \quad x_U - x \geq 0$$

From (7), we can derive the following three bounding constraints:

$$(x - x_L)^2 \geq 0, \quad (x_U - x)^2 \geq 0, \quad (x - x_L) \times (x_U - x) \geq 0$$

which can be expanded to the following three constraints:

$$x^2 - 2x_Lx \geq -x_L^2, \quad x^2 - 2x_Ux \geq -x_U^2,$$

$$x^2 - (x_L + x_U)x \leq x_Uy_U.$$

Now, by treating $xy$ and $x^2$ as independent variables rather than the products of two terms, all constraints in (6) and (8) become linear constraints.

C. Entrywise Expansions of $D$ and $R$ with Respect to $Q$

So far, $D$ and $R$ are expressed using matrix products of $Q$, $H$, and $G$. However, such matrix product expressions are not convenient to use under BB/RLT framework. Thus, it is necessary to expand these matrices products entry-wise for algorithm design. For example, by expanding $D = I + \rho H HQH^T$, the real and imaginary parts of $d_{i,j}$, $i \neq j$, can be written as the following linear equalities with respect to $\Re(q_{(x,y)})$ and $\Im(q_{(x,y)})$:

$$0 = \Re(d_{i,j}) - \rho_H \sum_{x=1}^{n_t} \Re(q_{(x,x)}) \Re(h_{(i,x)} \overline{h}_{(j,x)})$$

$$-\rho_H \sum_{x=1}^{n_t} \sum_{y=1}^{n_t} \Re(q_{(x,y)}) \left[ \Re(h_{(i,x)} \overline{h}_{(j,y)}) + \Re(h_{(i,y)} \overline{h}_{(j,x)}) \right]$$

$$-\rho_H \sum_{x=1}^{n_t} \sum_{y=1}^{n_t} \Im(q_{(x,y)}) \left[ \Im(h_{(i,x)} \overline{h}_{(j,x)}) - \Im(h_{(i,x)} \overline{h}_{(j,y)}) \right]$$

$$0 = \Im(d_{i,j}) - \rho_H \sum_{x=1}^{n_t} \Re(q_{(x,x)}) \Im(h_{(i,x)} \overline{h}_{(j,x)})$$

$$-\rho_H \sum_{x=1}^{n_t} \sum_{y=1}^{n_t} \Re(q_{(x,y)}) \left[ \Im(h_{(i,y)} \overline{h}_{(j,x)}) + \Im(h_{(i,x)} \overline{h}_{(j,x)}) \right]$$

$$-\rho_H \sum_{x=1}^{n_t} \sum_{y=1}^{n_t} \Im(q_{(x,y)}) \left[ \Re(h_{(i,x)} \overline{h}_{(j,y)}) - \Re(h_{(i,y)} \overline{h}_{(j,y)}) \right]$$

For the diagonal elements $d_{i,i}$, the expansion can be simplified to

$$\Re(d_{i,i}) = \rho_H \sum_{x=1}^{n_t} \Re(q_{(x,x)}) \|h_{(i,x)}\|^2$$

$$+\rho_H \sum_{x=2}^{n_t} \sum_{y=1}^{n_t} \Re(q_{(x,y)}) \cdot 2\Re(h_{(i,x)} \overline{h}_{(i,y)})$$

$$+\rho_H \sum_{x=2}^{n_t} \sum_{y=1}^{n_t} \Im(q_{(x,y)}) \cdot 2\Im(h_{(i,x)} \overline{h}_{(i,y)}) + 1$$

and $\Im(d_{i,i}) = 0$. Since $\Im(d_{i,i}) = 0$, $\forall i$, we can remove these variables from our RLT-based relaxation to reduce the number of variables and constraints without changing the problem. Following the same line, we can derive the expansion of $R = I + \rho G GQG^T$ and the expressions are omitted here for brevity.

D. Linear Relaxation for Power Covariance Matrix $Q$

In problem (2), the input covariance matrix $Q$ is subject to $Q \succeq 0$ and $\text{Tr}(Q) \leq 1$. The trace constraint on $Q$ is simply the following linear constraint:

$$\sum_{i=1}^{n_t} \Re(q_{(i,i)}) \leq 1.$$  

However, it is more involved to express the PSD constraint of $Q$ in a linear form. In what follows, we will uncover the hidden
entrywise relationship implied by $Q \succeq 0$. We first introduce the following result, for which the proof can be found in [13].

**Theorem 1.** For any Hermitian PSD matrix $Q \in \mathbb{C}^{n \times n}$, the entry having the largest modulus must appear on the main diagonal of $Q$. Further, the entries in $Q$ satisfy the following inequality:

$$\|q_{i,j}\| \leq \frac{q_{i,i} + q_{j,j}}{2}, \quad 1 \leq i, j \leq n.$$  

(11)

Since $|\text{Re}(q_{i,j})| \leq \|q_{i,j}\|$ and $|\text{Im}(q_{i,j})| \leq \|q_{i,j}\|$, by Theorem 1, we have the following relaxation constraints on the entries of $Q$:

$$\text{Re}(q_{i,j}) \leq \frac{1}{2}(\text{Re}(q_{i,i}) + \text{Re}(q_{j,j})), \quad \forall i,$$  

(12)

$$\text{Im}(q_{i,j}) \leq \frac{1}{2}(\text{Re}(q_{i,i}) - \text{Re}(q_{j,j})), \quad \forall i.$$  

(13)

**E. RLT-Based Linear Relaxation**

By putting together all new variables and constraints, we have the final RLT linear relaxation of problem (2) as follows:

Max $\frac{1}{2n^2}(A - B)$

s.t. $A - \sum_{i=1}^{n} Y_i = 0$

$B - \sum_{i=1}^{n} W_i = 0$

Polyhedral approximation for $(Y_i, X_i)$

Polyhedral approximation for $(W_i, V_i)$

$X_i - \text{Re}(d(i,i)_L) - \text{Im}(d(i,i)_L) = 0, \forall i$

$V_i - \text{Re}(r(i,i)_L) - \text{Im}(r(i,i)_L) = 0, \forall i$

Bounding factor constraints for terms in the forms of $\text{Re}(\cdot)\text{Re}(\cdot)$, $\text{Im}(\cdot)\text{Im}(\cdot)$, and $\text{Re}(\cdot)\text{Im}(\cdot)$.

**F. Partitioning Variables and Their Bounds**

In BB/RLT, partitioning variables are those that are involved in nonlinear terms, for which we have therefore defined new variables, and whose bounding intervals will need to be partitioned during the BB process [12]. In RLT relaxation (14), these BB variables include $X_i$, $V_i$, $\text{Re}(d(i,i)_L)$, $\text{Im}(d(i,i)_L)$, $\text{Re}(r(i,i)_L)$, and $\text{Im}(r(i,i)_L)$. For these variables, we need to derive tight upper and lower bounds, which are crucial to the convergence speed of BB/RLT.

1) $\text{Re}(d(i,i)_L)$, and $\text{Im}(d(i,i)_L)$: To derive upper and lower bounds for $\text{Re}(d(i,i)_L)$, and $\text{Im}(d(i,i)_L)$, we need the following result.

**Lemma 1.** For any PSD Hermitian matrix $M \in \mathbb{C}^{n \times n}$, the summation of the modulus of all off-diagonal elements satisfy the following inequality:

$$\sum_{i=2}^{n} \sum_{j=1}^{i-1} \|m_{i,j}\| \leq \frac{n-1}{2} \text{Tr}\{M\}.$$  

Lemma 1 follows directly from Theorem 1. Due to space limitation, we refer readers to [13] for more details. From Lemma 1, we have the following theorem and the proof is also relegated to [13] due to space limitation.

**Theorem 2.** The $m$th diagonal entry of $D$ can be upper bounded by

$$(d(i,i)) = \left[ \rho_H \left( D(i,i)^1 + D(i,i)^2 \right) \right] + 1,$$  

(15)

where $D(i,i)^1 = \max \|h(i,x)\|^2$, for $1 \leq i \leq n$, $1 \leq x \leq n$, and $D(i,i)^2$ is the optimal objective value of the following linear programming problem:

$$\max \sum_{x=1}^{n} \sum_{y=1}^{n} \left[ \text{Re}(q(x,y)) \cdot 2\text{Im}(h(i,y)) \cdot \text{Im}(q(x,y)) \right]$$

s.t. $-\frac{n-1}{2} \leq \sum_{x=1}^{n} \sum_{y=1}^{n} \text{Re}(q(x,y)) \leq \frac{n-1}{2}$

$-\frac{n-1}{2} \leq \sum_{x=1}^{n} \sum_{y=1}^{n} \text{Im}(q(x,y)) \leq \frac{n-1}{2}$

$-\text{Re}(q(x,y)) \cdot \text{Im}(q(x,y)) \leq 1, \forall x, y.$

With Theorem 2, we are ready to bound $\text{Re}(d(i,i)_L)$ and $\text{Im}(d(i,i)_L)$. Since $d(i,i) = \sum_{k=1}^{n} \text{Re}^2(d(i,k)_L) + \text{Im}^2(d(i,k)_L)$, we can bound all $\text{Re}(d(i,k)_L)$ and $\text{Im}(d(i,k)_L), 1 \leq k \leq i, 1 \leq i \leq n_t$, in the following intervals

$$\left[ -\sqrt{\rho_H(D(i,i)^1 + D(i,i)^2)} , \sqrt{\rho_H(D(i,i)^1 + D(i,i)^2)} + 1 \right].$$

Since $D$ and $R$ are of the identical form, the upper and lower bounds of $\text{Re}(d(i,k)_L)$ and $\text{Im}(r(i,k)_L), 1 \leq k \leq i, 1 \leq i \leq n_t$ can be derived in exactly the same way and are omitted in here for brevity.

2) $X_i$, and $V_i$: Since $X_i$ and $V_i$ are of identical form, we only show how to derive upper and lower bounds for $X_i$ and omit the derivations of $V_i$ for brevity. Recall that $X_i = \text{Re}^2(d(i,i)_L) + \text{Im}^2(d(i,i)_L)$, we can upper bound $X_i$ as follows:

$$X_i = \|d(i,i)_L\|^2 \leq d(i,i) \leq \left( d(i,i) \right)_U.$$

Since $\text{det}(I + A) \geq 1 + \text{det} A$ for any $A \geq 0$ (Minkowski inequality [14]), we have $|D| = |I + \rho_H Q | = \prod_{i=1}^{n} \|d(i,i)_L\|^2 \geq 1$. Hence, $X_i$ can be lower bounded by

$$X_i = \|d(i,i)_L\|^2 \geq \frac{1}{\prod_{i=1}^{n} \|d(i,i)_L\|^2} = \frac{1}{\prod_{j=1}^{n} (d(j,j))_U}.$$

**G. Local Search Algorithm**

As indicated earlier, the solution to the linear relaxation (14), denoted by $Q$, may not be feasible to the original problem (2). Therefore, during each iteration, we need to obtain a feasible solution based on $Q$ via a local search algorithm if $Q$ is infeasible. The basic idea of our local search is to project $Q$ onto the positive semidefinite cone.

This projection task can be formulated as the following minimization problem: given a Hermitian matrix $Q$, we wish to find a matrix $\bar{Q}$ satisfying $Q \succeq 0$ and $\text{Tr}\{Q\} \leq 1$ such that $Q$ minimizes $\|Q - \bar{Q}\|_F$, where $\| \cdot \|_F$ represent the Frobenius norm. Mathematically, this can be written as

Minimize $\frac{1}{2} \|Q - \bar{Q}\|_F$

subject to $\text{Tr}(Q) \leq 1$, $Q \succeq 0.$
Due to space limitation, we refer reader to [13] for more details about how to solve problem (16).

IV. CONVERGENCE SPEEDUP TECHNIQUE

BB/RLT has exponential complexity due to the NP-hardness of problem (2). However, it is possible to exploit the special structure of problem (2) to significantly speedup its convergence. From our computational experience, we note that the decrease of the global upper bound plays the most important role in the convergence process. Thus, \( X_i \) and \( V_i \), should be partitioned with higher priority since they directly impact the global upperbound. We summarize our convergence speedup technique in Algorithm 2.

**Algorithm 2 BB Variable Selection Strategy**

1. Among all \( X_i \) and \( V_i \), choose the one having the largest relaxation error and denoted it as \( Z_1^* \).
2. If \((ln(Z_1^*)_L - ln(Z_1^*)_L) \leq \epsilon_1\) then
   a) Among all \( \Re(Z_1^*_{i,k}) \)’s, \( 3\Re(Z_1^*_{i,k}) \)’s, \( \Re(Z_1^*_{i,k}) \)’s, and \( 3\Re(Z_1^*_{i,k}) \)’s, choose one with the largest relaxation error. Denote this relaxation error as \( E_p \).
   b) If \( E_p \leq \epsilon_2 \), then remove this subproblem; else return the selected variable; else return \( Z_1^* \).

V. NUMERICAL EXAMPLE

In this section, we use a numerical example to demonstrate the computational experience of BB/RLT. The simulation setting is as follows: \( n_t = n_r = n_c = 4 \), \( \rho \) = 10dB, and \( \rho_G = 5\)dB. We plot the convergence process of BB/RLT in Fig. 3, where the global UB and LB for the secrecy capacity (in b/s/Hz) are illustrated in each iteration. The desired error bound is chosen to be \( \epsilon = 0.01 \). In this example, after approximately 30000 iterations, the UB and LB values are both driven to 5.45 b/s/Hz, meaning that the secrecy capacity is 5.45 b/s/Hz. Although the number of iterations is seemingly large, the running time of BB/RLT is quite short thanks to the efficiency and robustness of modern day linear programming solvers.

However, we remark that the convergence speedup technique discussed in Section IV is crucial for the success of BB/RLT. For this example, without using the speedup technique, the BB process would easily stall, although it should converge theoretically. This is because without careful consideration in selecting partitioning variables, the algorithm may waste most of its time in partitioning those variables who have very minor effect on closing the gap between global upper and lower bounds. Also, the size of the subproblem list in BB/RLT may become large quickly.

VI. CONCLUSION

In this paper, we investigated the optimal power allocation problem of Gaussian MIMO wire-tap channels. For this challenging non-convex optimization problem, we designed a global optimization algorithm called branch-and-bound with reformulation and linearization technique (BB/RLT). We developed key problem-specific components for BB/RLT and the related convergence speedup technique for solving the optimal power allocation problem. To the best of knowledge, our proposed BB/RLT algorithm is the first method that guarantees finding the global optimal power allocation to achieve perfect secrecy capacity for Gaussian MIMO wire-tap channels.

**REFERENCES**