DC programming and DCA for secrecy rate maximization in a wireless network with multiple eavesdroppers

HOAI AN LETHI,THI THUY TRAN
University of Lorraine
Theoretical and Applied Computer Science Lab
Ile du Saulcy, 57045 Metz
FRANCE
hoai-an.le-thi@univ-lorraine.fr
thi-thuy.tran@univ-lorraine.fr

TAO PHAM DINH
INSA-Rouen, University of Normandie
Laboratory of Mathematic
76801 Saint-Etienne-du-Rouvray
FRANCE
pham@insa-rouen.fr

Abstract: In this paper, we consider a wireless network where a source tries to send messages to a destination while keeping them secret from multiple eavesdroppers. To enhance secrecy, the transmission is performed with a cooperation of friendly jammers which make artificial noise to confound eavesdroppers and beamforming technique to direct jamming signal to intended targets. The purpose is to determine beamforming coefficients in order to maximize secrecy rate under the total jammer power constraint. The existing method solved this problem in a special case in which the beamforming coefficients were designed to completely eliminate jamming signal at the destination and a heuristic approach was applied to obtain a suboptimal solution for this case. We address this problem via a new approach based on DC (Difference of Convex functions) programming and DCA (DC Algorithm). We first reformulate this problems as a general DC program, i.e. minimizing a DC function under some DC constraints, and develop a DCA based algorithm for solving it. The experimental results show that the secrecy rate obtained by the proposed algorithm is better than those achieved by the existing one.

Key–Words: Cooperative Jamming, Beamforming, Physical Layer Security, DC programming and DCA.

1 Introduction

The confidentiality and privacy of user data are always the main issues of interest in communication systems. They are traditionally relied on cryptographic algorithms. However, the explosive development of computational tools nowadays becomes a threat to the security of cryptographic algorithms. Therefore, it requires to develop new technologies in data transmission to ensure security and confidentiality for transmitted data, besides cryptography. In this context, physical layer security emerges as an effective method for both ensuring the secure transmission without using encryption and aiding secret key exchange in cryptography. It was introduced for the first time in [21] based on the information-theoretic point of view. In this seminal work, Wyner showed that for a wiretap chanel in which the channel of the eavesdropper is noisier than that of the user, it was possible to design a code such that a nonzero achievable secrecy rate can be achieved without relying on encryption. This approach has been later extended to parallel channels ([22],[23]), fading channel ([12]), multiple access channel ([17],[18]), broadcast channel with confidential messages ([2],[4]).

In parallel with designing codes for meeting a secrecy rate, various techniques of signal processing are exploited and developed in a wide range of communication systems in order to improve their secrecy. Among them, node cooperation techniques are increasingly used in many works and their efficiency in enhancing secrecy is shown. In the node cooperation techniques, one installs external nodes with the aim of increasing secrecy rate. These nodes can play a role as either relays to forward the information to destinations with two well-known relaying protocols amplify-and-forward (AF) and decode-and-forward (DF) or friendly jammers to make artificial noise in order to confound eavesdroppers. The cooperative AF/DF relaying and cooperative jamming (CJ) are to refer to such node cooperation techniques, respectively. In addition, these node cooperation techniques are often combined with the beamforming technique to direct the received information to intended targets. An arising issue is how to design appropriate beamforming coefficients so as to maximize the secrecy rate subject to some power constraints. The various relaying protocols lead to the mathematically different forms of the secrecy rate maximization (SRM) problem. Overall, the SRM problems derived in the DF case are often simpler than those in the AF and

CJ cases and the optimal/suboptimal solutions were found in several specific DF schemes ([3], [10]). For the AF and CJ scenario, rather than directly dealing with complex programs, one can choose a simpler approach using zero-forcing or null-space in which the beamforming coefficients are designed to completely eliminate signal at eavesdroppers (with respect to the AF scenario) or artificial noise at destinations (with respect to the CJ scenario) ([3],[25],[20]). Nevertheless, the solution obtained by this method is only a suboptimal. Besides, some works proposed a two-level algorithm based on semidefinite relaxation technique to directly tackle the SRM problem in the AF scenario ([24],[11]). However, the convergence of this method is not guaranteed. Recently, some works employ the sequential convex approximation method which is actually a special version of DCA to handle the models in the AF scenario ([19]).

In this paper, we consider the SRM problem in a wireless system including one source, one destination, multiple friendly jammers and multiple eavesdroppers. The joint beamforming and CJ techniques are employed to enhance secrecy. This problem were established in [3] and solved in a special case, namely a null-space cooperative beamforming scheme, where the artificial noise is assumed to be eliminated completely at the destination. It means that one constraint is added, which helps simplify the problem. Despite that, only a suboptimal solution was found for the simplified problem via a heuristic approach. Here, we want to explore more efficient methods to deal with this SRM problem. The approach based on DC programming and DCA is an appropriate choice due to the fact that it has been successfully applied to many intractable nonconvex programs in various areas including, among of others, communication systems (e.g. [1], [19], [26], [9], [16] and the references in [8], [5]). DC programming and DCA were introduced by Pham Dinh Tao in 1985 and have been extensively developed by Le Thi Hoai An and Pham Dinh Tao since 1994 to become now classic and more and more popular (see e.g. [13], [7], [6], [15], [6], [5] and references therein). A standard DC program involves minimizing a DC function over a convex set while a general DC program involves minimizing a DC function on a set defined by some convex constraints and some DC constraints. The main idea of DCA is approximating the second DC components by their linear minorant and then solving the resulting convex subproblem at each iteration.

Our contribution is to propose a new approach based on DC programming and DCA for dealing with the considered SRM problem in the null-space cooperative beamforming scheme. We first reformulate this problem as a general DC program and design a general DCA for solving it. It should be noted that in DC programming, the standard DCA (DCA for minimizing a DC function under some convex constraints) has been exploited and successfully applied for solving nonconvex optimization problems in various areas of applied science since many years. However the use of the general DCA, which is generalized from the standard DCA, for DC programs with some DC constraints are relative new in the literature (see [15], [6]). General DCAs permit to solve a wider class of nonconvex problems compared to standard DCAs, thus being a promising nonconvex optimization tool. The simulation results imply that the secrecy rate obtained by the proposed general DCA schemes are considerably better than those gained by the existing one.

The rest of this paper is organized as follows. In Section 2, we describe the considered SRM problem. The solution method is presented in Section 3. We first give a brief introduction of DC programming and DCA and then show how to apply these tools to solve the considered problem in the null-space cooperative beamforming scheme. Experimental results are reported in Section 4. Finally, Section 5 concludes the paper.

Notation: Let $()^T$, $()^\dagger$ and $(.)^*$ denote transpose, conjugate transpose and conjugate, respectively; $\mathbf{I}_m$ is the identity matrix of size $m \times m$; $\langle ., . \rangle$ denotes the inner product and $\|.\|$ denotes the Euclidean norm. Re(.) and Im(.) are the real part and the imaginary part of its argument. A circularly symmetric Gaussian complex random vector Z is denoted by $Z \sim \mathcal{CN}(0, \Gamma)$.

2 Secrecy rate maximization via cooperative jamming combined with beamforming technique

In this section, we reconsider the model proposed in [3]. The system is comprised of a source, a destination, M relays and K eavesdroppers. Each node is equipped with a single antenna. In cooperative jamming technique (CJ), the relays play a role as jammers which transmit a weighted version of a jamming signal z to the channel with the aim of confusing the eavesdroppers, whereas the source sends the signal $\sqrt{P_s}x$ to the channel. Denote $h^*_{SD} \in \mathbb{C}$ as the channel coefficient between the source and the destination, $\mathbf{h}^*_{SE} \in \mathbb{C}^K$ as the vector of channel coefficients between the source and K eavesdroppers, $\mathbf{h}^*_{RD} \in \mathbb{C}^M$ as the vector of channel coefficients between M relays and the destination, $\mathbf{H}^*_{RE}$ as the $M \times K$ matrix of channel coefficients between M relays and K eavesdroppers. Denote P_{tot} as the total transmit power budget of all relays and **w** as a vector of relay weights.

The received signal at the destination is

$$y_d = \sqrt{P_s} h_{SD}^* x + \mathbf{h}_{RD}^\dagger \mathbf{w} z + n_d$$

and the received signals at the eavesdroppers are given by

$$\mathbf{y}_e = \sqrt{P_s} \mathbf{h}_{SE}^* x + \mathbf{H}_{RE}^\dagger \mathbf{w} z + \mathbf{n}_e,$$

where n_d represents complex Gaussian noise at the destination with variance of σ^2, and $\mathbf{n}_e \sim \mathcal{CN}(0, \sigma^2 \mathbf{I}_K)$ is a noise vector at the K eavesdroppers. Therefore, the achievable rate at the destination is

$$R_d = \log_2 \left(1 + \frac{P_s |h_{SD}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w} + \sigma^2} \right)$$

and the achievable rate at the jth eavesdropper is

$$R_{e_j} = \log_2 \left(1 + \frac{P_s |\mathbf{h}_{SE}(j)|^2}{\mathbf{w}^\dagger \mathbf{R}_{RE_j} \mathbf{w} + \sigma^2} \right),$$

where $\mathbf{h}_{SE}(j)$ is the jth element of the vector $\mathbf{h}_{SE}$, $\mathbf{R}_{RD} = \mathbf{h}_{RD} \mathbf{h}_{RD}^\dagger, \mathbf{R}_{RE_j} = \mathbf{H}_{RE}(:, j) \mathbf{H}_{RE}(:, j)^\dagger$ with $\mathbf{H}_{RE}(:, j)$ is the jth column of the matrix $\mathbf{H}_{RE}$.

The problem of achievable secrecy rate maximization can be formulated as below ([3]).

$$\begin{aligned} \max_{\mathbf{w}} \min_{j=1,\dots,K} & \log_2 \left(1 + \frac{P_s |h_{SD}|^2}{\mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w} + \sigma^2} \right) \quad (1) \\ & - \log_2 \left(1 + \frac{P_s |\mathbf{h}_{SE}(j)|^2}{\mathbf{w}^\dagger \mathbf{R}_{RE_j} \mathbf{w} + \sigma^2} \right) \\ \text{s.t } & \mathbf{w}^\dagger \mathbf{w} \le P_{tot}. \end{aligned}$$

This problem is nonsmooth and nonconvex and thus it is intractable. Therefore, one tries to simplify it and then find a suboptimal solution. Because the jamming signal, which is emitted by the friendly jammers to confuse the eavesdroppers, might also affect the destination, thus in a natural way one wants to design beamforming coefficients in order to completely eliminate this noise at the destination. It means that apart from the power constraint, **w** has to satisfy an additional constraint $\mathbf{h}_{RD}^\dagger \mathbf{w} = 0$. This constraint makes the first term of the objective function in (1) become a constant, so the problem (1) is simplified to the following form.

$$\begin{aligned} \max_{\mathbf{w}} \min_{j=1,\dots,K} & - \log_2 \left(1 + \frac{P_s |\mathbf{h}_{SE}(j)|^2}{\mathbf{w}^\dagger \mathbf{R}_{RE_j} \mathbf{w} + \sigma^2} \right) (2) \\ \text{s.t } & \mathbf{w}^\dagger \mathbf{w} \le P_{tot}. \\ & \mathbf{h}_{RD}^\dagger \mathbf{w} = 0. \end{aligned}$$

Despite that, the existing method in [3] only provided a suboptimal solution to (2) via a heuristic search. In what follows, we will address the problem (2) based on a general DCA that is a new tool in DC programming.

3 Solution methods based on DC programming and DCA

First, to facilitate the reader, let us introduce shortly DC programming and DCA.

3.1 A brief introduction to DC programming and DCA

DC Programming and DCA constitute the backbone of smooth/nonsmooth nonconvex programming and global optimization ([13],[14],[7]). They address a problem of minimizing a function f which is a difference of convex functions on the whole space $\mathbb{R}^n$ or a convex set $C \subset \mathbb{R}^n$. Generally speaking, a standard DC program takes the form

$$\alpha = \inf\{f(x) := g(x) - h(x) : \ x \in \mathbb{R}^n\} \ \ (P_{dc}),$$

with $g, h \in \Gamma_0(\mathbb{R}^n)$, the convex cone of all lower semicontinuous proper (i.e., not identically equal to $+\infty$) convex functions defined on $\mathbb{R}^n$ and taking values in $\mathbb{R} \cup \{+\infty\}$. Such a function f is called a DC function, and $g - h$ is a DC decomposition of f, while the convex functions g and h are DC components of f. The vector space of DC functions, $\text{DC}(\mathbb{R}^n) = \Gamma_0(\mathbb{R}^n) - \Gamma_0(\mathbb{R}^n)$, forms a wide class encompassing all convex functions in particular and most real-life nonconvex objective functions in general. DC programming therefore constitutes an extension of convex programming and covers most nonconvex programs.

The constrained DC program whose feasible set C is convex always can be transformed into the unconstrained DC program by adding the indicator function of C, denoted by χ_C which is defined by $\chi_C(x) = 0$ if $x \in C$, and $+\infty$ otherwise to the first DC component.

Recall that, for a convex function, the subdifferential of φ at $x_0 \in \text{dom}(\varphi)$, denoted by $\partial\varphi(x_0)$, is defined by

$$\begin{aligned} \partial\varphi(x_0) := \ & \{y \in \mathbb{R}^n : \varphi(x) \ge \varphi(x_0) + \langle x - x_0, y \rangle, \\ & \forall x \in \mathbb{R}^n\}. \end{aligned}$$

The main idea of standard DCA is quite simple. Starting from an initial point x^0, the standard DCA consists in constructing two sequences $\{x^l\}$ and $\{y^l\}$ such that, for any $l = 0, 1, 2, \dots \ y^l \in \partial h(x^l)$ and $x^{l+1} \in \arg\min\{g(x) - \langle y^l, x \rangle : x \in \mathbb{R}^n\}$.

Recently, the generalization of the standard DCA was studied in [15], [6] to solve general DC programs with DC constraints as follows

$$\begin{aligned} \min_{x} \quad & f_0(x), \\ \text{s.t} \quad & f_i(x) \le 0 \; \forall i = 1, ..., m, \\ & x \in C, \end{aligned} \tag{3}$$

where $C \subseteq \mathbb{R}^n$ is a nonempty closed convex set; $f, f_i : \mathbb{R}^n \to \mathbb{R} (i = 0, 1, ..., m)$ are DC functions. It is apparent that this class of nonconvex programs is the most general in DC programming and as a consequence it is more challenging to deal with than standard DC programs. Two approaches for general DC programs were proposed in [15], [6] to overcome the difficulty caused by the nonconvexity of the constraints. Both approaches are built on the main idea of the philosophy of DC programming and DCA, that is approximating (3) by a sequence of convex programs. The former was based on penalty techniques in DC programming while the latter was relied on the convex inner approximation method. Because we use the idea of the second approach to solve the problem mentioned in this article, we presented herein its main scheme.

Since $f_i (i = 0, ..., m)$ are DC functions, they can be decomposed into the difference of two convex functions

$$f_i(x) = g_i(x) - h_i(x), \; x \in \mathbb{R}^n, i = 0, ..., m.$$

By linearizing the concave part of DC decompositions of all DC objective function and DC constraints, it results in sequential convex subproblems of the following form:

$$\begin{aligned} \min_{x} \quad & g_0(x) - \langle y_0^k, x \rangle \\ \text{s.t} \quad & g_i(x) - h_i(x^k) - \langle y_i^k, x - x^k \rangle \le 0, \\ & \forall i = 1, ..., m, \\ & x \in C, \end{aligned} \tag{4}$$

where $x^k \in \mathbb{R}^n$ is a point at the current iteration, $y_i^k \in \partial h_i(x^k) \; \forall \, i = 0, ..., m$.

This linearization introduces an inner convex approximation of the feasible set of (3) due to the fact that $h_i(x) \ge h_i(x^k) + \langle y_i^k, x - x^k \rangle$.

The general DCA scheme for the general DC program (3) is described as follows:

The general DCA scheme

- **Initialization.** Choose an initial point x^0; set $0 \longleftarrow k$.
- **Repeat.**
  Step 1. Compute $y_i^k \in \partial h_i(x^k), \;\; i = 0, .., m$,
  Step 2. Compute x^{k+1} by solving the convex subproblem (4)
  Step 3. $k \leftarrow k + 1$,
- **Until** stopping condition

3.2 DC Programming and DCA for solving (2)

The problem (2) can be equivalently rewritten as follows

$$\begin{aligned} & \min_{\mathbf{w}} \max_{j=1,\dots,K} \\ & \log_2 \left\{ \frac{\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RE_j} \mathbf{w} + P_s |\mathbf{h}_{SE}(j)|^2}{\sigma^2 + \mathbf{w}^\dagger \mathbf{R}_{RE_j} \mathbf{w}} \right\} \\ & \text{s.t } \; \mathbf{w}^\dagger \mathbf{w} \le P_{tot}, \\ & \quad \mathbf{h}_{RD}^\dagger \mathbf{w} = 0. \end{aligned} \tag{5}$$

Denote $C_j = \sigma^2 + P_s |\mathbf{h}_{SE}(j)|^2, \mathbf{T}_j = \begin{bmatrix} \mathrm{Re}(\mathbf{R}_{RE_j}) & -\mathrm{Im}(\mathbf{R}_{RE_j}) \\ \mathrm{Im}(\mathbf{R}_{RE_j}) & \mathrm{Re}(\mathbf{R}_{RE_j}) \end{bmatrix}, j = 1, \dots, K$, $\mathbf{M} = \begin{bmatrix} \mathrm{Re}(\mathbf{h}_{RD}^\dagger) & -\mathrm{Im}(\mathbf{h}_{RD}^\dagger) \\ \mathrm{Im}(\mathbf{h}_{RD}^\dagger) & \mathrm{Re}(\mathbf{h}_{RD}^\dagger) \end{bmatrix}, \mathbf{x} = \begin{bmatrix} \mathrm{Re}(\mathbf{w}^T) & \mathrm{Im}(\mathbf{w}^T) \end{bmatrix}^T$. The problem (5) is transformed into the real form below.

$$\begin{aligned} \min_{\mathbf{x},t} \quad & t \\ \text{s.t.} \quad & \mathbf{x}^T \mathbf{x} \le P_{tot}, \\ & \mathbf{M}\mathbf{x} = 0, \\ & \ln \left(\frac{C_j + \mathbf{x}^T \mathbf{T}_j \mathbf{x}}{\sigma^2 + \mathbf{x}^T \mathbf{T}_j \mathbf{x}} \right) \le t, \;\; \forall j = 1, \dots, K. \end{aligned}$$

The DC formulation of the above problem is given by

$$\begin{aligned} \min_{\mathbf{x},t} \quad & t \\ \text{s.t.} \quad & \mathbf{x}^T \mathbf{x} \le P_{tot}, \\ & \mathbf{M}\mathbf{x} = 0. \\ & G_j(\mathbf{x}) - H_j(\mathbf{x}) \le t \;\; \forall j = 1, \dots, K, \end{aligned} \tag{6}$$

where $G_j(\mathbf{x}) = \frac{\rho_j}{2} \|\mathbf{x}\|^2, H_j(\mathbf{x}) = \frac{\rho_j}{2} \|\mathbf{x}\|^2 - \ln(C_j + \mathbf{x}^T \mathbf{T}_j \mathbf{x}) + \ln(\sigma^2 + \mathbf{x}^T \mathbf{T}_j \mathbf{x})$, in which ρ_j is chosen such that both functions G_j and H_j are convex. The choice of such ρ_j can be deduced from the lemma below.

Lemma 1 *Let $\boldsymbol{B}$ be a $2M \times 2M$ symmetric and positive semidefinite matrix and N_0 be a positive number.*
(i) If ρ is greater than the maximal eigenvalue of matrix $\frac{2\boldsymbol{B}}{N_0}$ then the function $v_1(\boldsymbol{x}) = \frac{1}{2}\rho\|\boldsymbol{x}\|^2 - \ln(\boldsymbol{x}^T \boldsymbol{B} \boldsymbol{x} + N_0)$ is convex.
(ii) If ρ is greater than the maximal eigenvalue of matrix $\frac{\boldsymbol{B}}{2N_0}$ then the function $v_2(\boldsymbol{x}) = \frac{1}{2}\rho\|\boldsymbol{x}\|^2 + \ln(\boldsymbol{x}^T \boldsymbol{B} \boldsymbol{x} + N_0)$ is convex.

Proof 1 *(i) The necessary and sufficient condition for the function $v_1(\boldsymbol{x})$ to be convex is that $\bigtriangledown^2 v_1(\boldsymbol{x}) \succeq 0 \; \forall \boldsymbol{x} \in \mathbb{R}^{2M}$.*

We have $\bigtriangledown^2 v_1(\boldsymbol{x}) = \rho \boldsymbol{I} - \frac{2\boldsymbol{B}}{\boldsymbol{x}^T\boldsymbol{B}\boldsymbol{x}+N_0} + \frac{4\boldsymbol{Bx}(\boldsymbol{Bx})^T}{(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2}$. Thus

$$\begin{aligned} &\bigtriangledown^2 v_1(\boldsymbol{x}) \succeq 0 \\ \Leftrightarrow\ & \rho\|\boldsymbol{y}\|^2 - \frac{2\boldsymbol{y}^T\boldsymbol{By}}{\boldsymbol{x}^T\boldsymbol{Bx}+N_0} + \frac{4\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y}}{(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2} \geq 0 \\ & \forall \boldsymbol{y}, \boldsymbol{x} \in \mathbb{R}^{2M}. \end{aligned}$$

Since ρ is greater than the maximal eigenvalue of matrix $\frac{2\boldsymbol{B}}{N_0}$, $\rho\boldsymbol{I} \succeq \frac{2B}{N_0}$. Thus $\boldsymbol{y}^T\left(\rho\boldsymbol{I} - 2\frac{\boldsymbol{B}}{N_0}\right)\boldsymbol{y} \geq 0\ \forall \boldsymbol{y} \in \mathbb{R}^{2M}$. In addition, $\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y} = (\boldsymbol{y}^T\boldsymbol{Bx})^2 \geq 0\ \forall \boldsymbol{y},\boldsymbol{x} \in \mathbb{R}^{2M}$ and $\boldsymbol{x}^T\boldsymbol{Bx} \geq 0\ \forall \boldsymbol{x} \in \mathbb{R}^{2M}$ due to the positive semidefinite property of $\boldsymbol{B}$. Therefore

$$\begin{aligned} &\rho\|\boldsymbol{y}\|^2 - \frac{2\boldsymbol{y}^T\boldsymbol{By}}{\boldsymbol{x}^T\boldsymbol{Bx}+N_0} + \frac{4\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y}}{(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2} \\ &\quad \geq \frac{2\boldsymbol{y}^T\boldsymbol{By}}{N_0} - \frac{2\boldsymbol{y}^T\boldsymbol{By}}{\boldsymbol{x}^T\boldsymbol{Bx}+N_0} \geq 0. \end{aligned}$$

(ii) Similarly to the part (i), the function $v_2(\boldsymbol{x})$ is convex if and only if

$$\begin{aligned} &\bigtriangledown^2 v_2(\boldsymbol{x}) \succeq 0\ \ \forall \boldsymbol{x} \in \mathbb{R}^{2M} \\ \Leftrightarrow\ & \rho\|\boldsymbol{y}\|^2 + \frac{2\boldsymbol{y}^T\boldsymbol{By}}{\boldsymbol{x}^T\boldsymbol{Bx}+N_0} - \frac{4\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y}}{(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2} \geq 0 \\ & \forall \boldsymbol{y}, \boldsymbol{x} \in \mathbb{R}^{2M} \\ \Leftrightarrow\ & \rho\|\boldsymbol{y}\|^2(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2 + 2\boldsymbol{y}^T\boldsymbol{By}(\boldsymbol{x}^T\boldsymbol{Bx}+N_0) \\ & -4\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y} \geq 0\ \forall \boldsymbol{y}, \boldsymbol{x} \in \mathbb{R}^{2M}. \end{aligned}$$

The Cauchy-Schwarz inequality implies that

$$\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y} \leq (\boldsymbol{x}^T\boldsymbol{Bx})(\boldsymbol{y}^T\boldsymbol{By})\ \forall \boldsymbol{y}, \boldsymbol{x} \in \mathbb{R}^{2M}.$$

Moreover, the Cauchy inequality shows that

$$(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2 \geq 4N_0(\boldsymbol{x}^T\boldsymbol{Bx})\ \forall \boldsymbol{x} \in \mathbb{R}^{2M}.$$

Therefore

$$\begin{aligned} & \rho\|\boldsymbol{y}\|^2(\boldsymbol{x}^T\boldsymbol{Bx}+N_0)^2 + 2\boldsymbol{y}^T\boldsymbol{By}(\boldsymbol{x}^T\boldsymbol{Bx}+N_0) \\ & -4\boldsymbol{y}^T\boldsymbol{Bx}(\boldsymbol{Bx})^T\boldsymbol{y} \\ \geq\ & 4N_0(\rho\|\boldsymbol{y}\|^2)(\boldsymbol{x}^T\boldsymbol{Bx}) - 2(\boldsymbol{y}^T\boldsymbol{By})(\boldsymbol{x}^T\boldsymbol{Bx}) \\ \geq\ & 0\ \forall \boldsymbol{y}, \boldsymbol{x} \in \mathbb{R}^{2M} \end{aligned}$$

The last inequality is deduced from the fact that ρ is greater than the maximal eigenvalue of matrix $\frac{\boldsymbol{B}}{2N_0}$, hence $\rho\boldsymbol{I} \succeq \frac{B}{2N_0}$ that implies $4N_0\rho\|\boldsymbol{y}\|^2 \geq 2\boldsymbol{y}^T\boldsymbol{By}$ and $\boldsymbol{x}^T\boldsymbol{Bx} \geq 0$ since $B \succeq 0$.

From Lemma 1 we can deduce that if ρ_j is the maximal eigenvalue of the matrix $\left(\frac{2}{C_j} + \frac{1}{2\sigma^2}\right)\mathbf{T}_j$. then G_j and H_j are convex. Following the idea of DCA, at the kth iteration with the iterate $\mathbf{x}^k$, we compute $\nabla H_j(\mathbf{x}^k) = \rho_j\mathbf{x}^k - \frac{2\mathbf{T}_j\mathbf{x}^k}{C_j+\mathbf{x}^T\mathbf{T}_j\mathbf{x}} + \frac{2\mathbf{T}_j\mathbf{x}^k}{\sigma^2+\mathbf{x}^T\mathbf{T}_j\mathbf{x}}$ and then solve the derived convex subproblem below.

$$\min_{\mathbf{x},t} \quad t \tag{7}$$

$$\text{s.t} \quad \mathbf{x}^T\mathbf{x} \leq P_{tot}, \tag{8}$$

$$\mathbf{Mx} = 0, \tag{9}$$

$$G_j(\mathbf{x}) - H_j(\mathbf{x}^k) - \langle \nabla H_j(\mathbf{x}^k), \mathbf{x} - \mathbf{x}^k \rangle \leq t, \forall j = 1, \ldots, K. \tag{10}$$

The general DCA scheme applied to (6), namely DCA-NS, can be described as follows.

DCA-NS

Initialization: choose randomly $\mathbf{V}^0 = (\mathbf{x}^0, t^0) \in (\mathbb{R}^{2M}, \mathbb{R}^+)$ as an initial guess, set a tolerance ϵ for DCA-NS, $k \leftarrow 0$.

Repeat

- Calculate $\mathbf{V}^{k+1} = (\mathbf{x}^{k+1}, t^{k+1})$ by solving the subproblem (7).
- $k \leftarrow k+1$.

Until $\left(\frac{\|\mathbf{V}^k - \mathbf{V}^{k-1}\|}{1+\|\mathbf{V}^{k-1}\|} < \epsilon \text{ or } \frac{|F(\mathbf{V}^k) - F(\mathbf{V}^{k-1})|}{1+|F(\mathbf{V}^{k-1})|} < \epsilon\right)$ where $F(\mathbf{V}^k) = t^k$.

4 Numerical Results

4.1 The Comparative algorithm

The existing method, namely SubOpt-NS, given in [3] provided a suboptimal solution to the problem (2). More particularly, the problem (2) is equivalent to the problem below.

$$\begin{aligned} \max_{\mathbf{w}} \min_{j=1,\ldots,K} \quad & \frac{|\mathbf{w}^\dagger \mathbf{H}_{RE}(:,j)|^2 + \sigma^2}{|\mathbf{h}_{SE}(j)|^2} \\ \text{s.t.} \quad & \mathbf{w}^T\mathbf{w} \leq P_t, \\ & \mathbf{w}^\dagger \mathbf{h}_{RD} = 0, \end{aligned} \tag{11}$$

For each $j = 1, \ldots, K$, the problem

$$\begin{aligned} \max_{\mathbf{w}} \quad & \frac{|\mathbf{w}^\dagger \mathbf{H}_{RE}(:,j)|^2 + \sigma^2}{|\mathbf{h}_{SE}(j)|^2} \\ \text{s.t.} \quad & \mathbf{w}^T\mathbf{w} \leq P_t, \\ & \mathbf{w}^\dagger \mathbf{h}_{RD} = 0, \end{aligned} \tag{12}$$

can be explicitly solved and its closed-form solution was indicated in [3]. A suboptimal solution to (11) is the one that obtains the highest secrecy rate among K solutions attained from (12) when $j = 1, \ldots, K$.

4.2 Experimental setups

In this experiment, all the algorithms were implemented in the Matlab 2013b, and performed on a PC Intel Core i5-2500S CPU 2.70GHz of 4GB RAM. We stopped the DCA schemes with the tolerance $\epsilon = 10^{-4}$. The channel coefficients $\mathbf{h}^*_{RD}, \mathbf{h}^*_{RE}, \mathbf{H}^*_{RE}$ are drawn from a circularly-symmetric and zero mean complex normal distribution with covariance matrix $\mathbf{I}_M$, i.e. $\mathcal{CN}(0, \mathbf{I}_M)$ and h^*_{SD} is generated from the distribution $\mathcal{CN}(0, 1)$. The noise variance is set to $\sigma^2 = 1$. The number of jammers is $M = 10$. The jammers are constrained by the total power budget, which is chosen from the set $\{20, 40, 60, 80, 100\}$. The reported results were taken average over 100 independent trials.

4.3 Numerical results

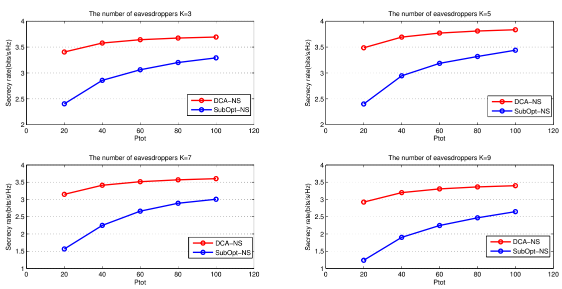

Figure 1: Secrecy rate versus total jammer power P_{tot}

The Figure 1 illustrates the secrecy rate obtained by two algorithms DCA-NS and SubOpt-NS versus the total jammer power in four cases of the number of eavesdroppers. Overall, it can be seen that the secrecy rate is increasing with increase in the total jammer power and decreasing with increase in the number of eavesdroppers. In all four cases of the number of eavesdroppers, DCA-NS furnishes the better secrecy rates than SubOpt. The gaps of secrecy rate obtained by the DCA scheme and SubOpt are significant, especially when the total jammer power is small.

5 Conclusion

We have investigated DC programming and DCA for solving the secrecy rate maximization problem in a wireless network including multiple eavesdroppers and using joint cooperative jamming and beamforming technique. The general DCA based algorithm is designed to deal with this problem in the null-space cooperative beamforming scheme. Compared to the existing method, the proposed DCA scheme achieves superior secrecy rates. The efficiency of the proposed DCA suggests that the approach based on DC programming and DCA is worth considering when coping with hard nonconvex optimization problems in physical layer security in particular as well as in communication systems in general. The general DCA adopted in this paper is a new approach in DC programming, which permits to solve a wider class of nonconvex optimization problems compared to the standard DCA, thus contributing to an expansion of applications of DC programming and DCA to more diverse fields of applied science.

References:

[1] Alberth Alvarado, Gesualdo Scutari, and Jong-Shi Pang. A new decomposition method for multiuser DC-programming and its application. *Signal Processing, IEEE Transactions on*, 62(11):2984–2998, 2014.

[2] Csiszr and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24(3):339–348, May 1978.

[3] L. Dong, Z. Han, A. Petropulu, and H. Poor. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process*, 58(3):1875–1888, March 2010.

[4] A. Khisti, A. Tchamkerten, and Gregory W. Wornell. Secure broadcasting over fading channels. *Information Theory, IEEE Transactions on*, 54(6):2453–2469, June 2008.

[5] H. A. Le Thi. DC Programming and DCA. `http://www.lita.univ-lorraine.fr/~lethi/`.

[6] H. A. Le Thi, V. N. Huynh, and T. Pham Dinh. DC Programming and DCA for General DC Programs. In Tien van Do, Hoai An Le Thi, and Ngoc Thanh Nguyen, editors, *Advanced Computational Methods for Knowledge Engineering: Proceedings of the 2nd International Conference on Computer Science, Applied Mathematics and Applications (ICCSAMA 2014)*, pages 15–35. Springer International Publishing, 2014.

[7] H. A. Le Thi and T. Pham Dinh. The DC (Difference of Convex Functions) Programming and DCA Revisited with DC Models of Real World Nonconvex Optimization Problems. *Annals of Operations Research*, 133:23–46, 2005.

[8] H. A. Le Thi and T. Pham Dinh. DC programming in Communication Systems: challenging models and methods. *Vietnam Journal of Computer Science*, 1 (1):15–28, 2013.

[9] Hoai An Le Thi and Tao Pham Dinh. Network utility maximisation: A DC programming approach for Sigmoidal utility function. In *2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, pages 50–54, 2013.

[10] J. Li, A. Petropulu, and S. Weber. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Signal Process*, 59(10):4985–4997, October 2011.

[11] L. Li, L. Li, Z. Chen, and J. Fang. Optimal transmit design at relay nodes for secure af relay networks. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–6, May 2015.

[12] Yingbin Liang, H.V. Poor, and S. Shamai. Secure communication over fading channels. *Information Theory, IEEE Transactions on*, 54(6):2470–2492, June 2008.

[13] T. Pham Dinh and H. A. Le Thi. Convex analysis approach to DC programming: Theory, algorithms and applications. *Acta Mathematica Vietnamica*, 22(1):289–357, 1997.

[14] T. Pham Dinh and H. A. Le Thi. Optimization algorithms for solving the trust region subproblem. *SIAM J. Optimization*, 8:476–505, 1998.

[15] T. Pham Dinh and H. A. Le Thi. Recent Advances in DC Programming and DCA. *Transactions on Computational Intelligence*, 13 (8342):1–37, 2014.

[16] T. T. Tran and H. A. Le Thi and T. Pham Dinh. DC programming and DCA for enhancing physical layer security via cooperative jamming. *Computers & Operations Research*, Published online december 2016.

[17] Xiaojun Tang, Ruoheng Liu, P. Spasojevic, and H.V. Poor. Multiple access channels with generalized feedback and confidential messages. In *Information Theory Workshop, 2007. ITW '07. IEEE*, pages 608–613, Sept 2007.

[18] E. Tekin and A. Yener. The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *Information Theory, IEEE Transactions on*, 54(6):2735–2751, June 2008.

[19] Chao Wang, Hui-Ming Wang, D.W.K. Ng, Xiang-Gen Xia, and Chaowen Liu. Joint beamforming and power allocation for secrecy in peer-to-peer relay networks. *Wireless Communications, IEEE Transactions on*, 14(6):3280–3293, June 2015.

[20] H. M. Wang, F. Liu, and M. Yang. Joint cooperative beamforming, jamming, and power allocation to secure af relay systems. *IEEE Transactions on Vehicular Technology*, 64(10):4893–4898, Oct 2015.

[21] A. D. Wyner. The wire-tap channel. *Bell Sys. Tech. Journ.*, 54:1355–1387, 1975.

[22] H. Yamamoto. On secret sharing communication systems with two or three channels. *Information Theory, IEEE Transactions on*, 32(3):387–393, May 1986.

[23] H. Yamamoto. A coding theorem for secret sharing communication systems with two gaussian wiretap channels. *Information Theory, IEEE Transactions on*, 37(3):634–638, May 1991.

[24] Yunchuan Yang, Cong Sun, Hui Zhao, Hang Long, and Wenbo Wang. Algorithms for secrecy guarantee with null space beamforming in two-way relay networks. *Signal Processing, IEEE Transactions on*, 62(8):2111–2126, April 2014.

[25] Gan Zheng, P. Arapoglou, and B. Ottersten. Physical layer security in multibeam satellite systems. *Wireless Communications, IEEE Transactions on*, 11(2):852–863, February 2012.

[26] Jian Zhou, Ruohan Cao, Hui Gao, Cong Zhang, and Tiejun Lv. Secure beamforming design in wiretap miso interference channels. In *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pages 1–5, May 2015.