# DC programming and DCA for enhancing Physical Layer Security via cooperative jamming

**Le Thi Hoai An, Tran Thi Thuy, Pham Dinh Tao**

***Tóm tắt*— Sự phát triển nhanh của những công cụ tính toán ngày nay đang là một mối đe dọa đối với sự an toàn của các thuật toán mã hóa vốn được xem như là các phương pháp truyền thống để đảm bảo an toàn thông tin. Phương pháp đảm bảo an toàn tại tầng vật lý được đưa ra không những để tăng cường tính bảo mật trong quá trình phân phối khóa bí mật trong mật mã mà còn làm cho việc truyền dữ liệu được bảo mật không cần dựa vào mã hóa ở các tầng cao hơn. Trong bài báo này, mô hình kết hợp nhiễu - một trong những mô hình được sử dụng trong tầng vật lý được đề cập và bài toán phân bổ công suất với mục đích cực đại hóa tổng của tốc độ truyền tin an toàn với các ràng buộc về công suất được phát biểu như một bài toán tối ưu không lồi. Hàm mục tiêu của bài toán là hiệu của hai làm lồi, được gọi là hàm DC và tập ràng buộc chứa một số ràng buộc kép. Chúng tôi đề xuất một phân tích DC mới cho hàm mục tiêu và sử dụng DCA (giải thuật DC) để giải bài toán này. Ưu điểm của phân tích DC này là nó sinh ra các bài toán con lồi mạnh bậc hai với các biến riêng rẽ trong hàm mục tiêu, do đó chúng có thể được giải dễ dàng bởi cả hai phương pháp tập trung hoặc chia rẽ biến. Các kết quả thực nghiệm đã chỉ ra tính hiệu quả của phân tích DC này so với phân tích DC được đưa ra trước đó [2].**

***Abstract*— The explosive development of computational tools these days is threatening security of cryptographic algorithms those are regarded as primary traditional methods for ensuring information security. Physical layer security approach is introduced as a method for both improving confidentiality of the secret key distribution in cryptography and enabling the data transmission without relaying on higher-layer encryption. In this paper, the cooperative jamming paradigm-one of the techniques used in the physical layer is mentioned and the resulting power allocation problem with the aim of maximizing the sum of secrecy rates subject to power constraints is formulated as a nonconvex optimization problem. The objective function is difference of two convex functions, called DC function and some constraints are coupling. We propose a novel DC decomposition for the objective function and use DCA (DC algorithms) to solve this problem. The main advantage of the proposed DC decomposition is that it leads to strongly convex quadratic sub-problems that can be easily solved by both distributed and centralized methods. The numerical results show the efficiency of this DC decomposition compared with the one proposed in [2].**

***Keywords*— *resource allocation; physical layer; DC programming; DCA.***

## I. INTRODUCTION AND RELATED WORKS

The broadcast nature of wireless channels makes it difficult to protect transmitted data from unauthorized receivers. Therefore, the issues of privacy and security have played an increasingly vital role in wireless networks, especially in military and homeland security applications. The targets of secure communications are both to enable the legitimate destination to successfully obtain source information and to restrain the eavesdroppers from interpreting this information. The security of data transmission has been traditionally assigned to cryptographic techniques at the network layer. However, in dynamic wireless networks, this raises issues such as key distribution for symmetric cryptosystems, and high computational complexity of asymmetric cryptosystems. Furthermore, all cryptographic algorithms are relied on the mathematically unproven hypothesis that it is computationally infeasible for eavesdroppers to decipher the received signals without the secret key. In fact, the rapid development of computational power nowadays makes it possible to analyze larger data and compute bigger amount of operations in a shorter time compared to those in the past, thus the vulnerability of some implemented crytographic schemes [9, 3, 22] does make sense.

These challenges motivate researchers to discover various methods for ensuring the confidentiality of data transmissions, beside of cryptography. Physical (PHY) layer security approaches based on an information-theoretic point of view have recently considerably the researchers' attention in this context. On the one hand, these methods can be combined with cryptography to improve confidentiality in exchanging messages over a wireless medium with the presence of unauthorized eavesdroppers.

On the other hand, the physical layer security has been also considered as a promising technique to ensure confidentiality of the transmitted messages without relying on higher-layer encryption, through the use of coding strategies, jamming or beamforming. More specifically, the fundamental principle behind physical layer security is to exploit the inherent randomness of noise or the friendly jammer and communication channels to restrict the amount of information that can be extracted by a fraudulent receiver. With reasonably designed coding and transmit precoding schemes in addition to the exploitation of any available channel state information, physical layer security schemes enable secret communication over a wireless medium without the assistance of an encryption key [18]. For instance, the cooperative transmission technique using friendly jammers (CJ paradigm) to make artificial noise in order to confuse the eavesdropper is mentioned in [6]. Another technique is based on cooperating with relays [5, 7, 17, 23], with the well-known decode-and-forward and amplify-and-forward schemes. This one is regarded as one of the effective methods to overcome the obstacles of wireless channel requirements in physical layer security.

Physical layer security approach was pioneered by Wyner [25] in 1975. In this work, he proved that a positive secrecy capacity can be achieved if the receiver has a better channel than the eavesdropper. The later researches have generalized this idea in various situations by taking advantage of user cooperation techniques mentioned above. The concepts appeared repeatedly in the articles linked to PHY layer security are achievable secrecy rate and secrecy capacity. An achievable secrecy rate is a rate at which information can be transmitted secretly from source to its intended destination, and secrecy capacity is defined as the maximal achievable secrecy rate. It is given by the maximum difference of mutual informations. Constructing the suitable strategies to attain secrecy capacity actually leads us to solving an optimization problem that is often nonconvex and thus hard to solve. DC programming and DCA are shown as an efficient approach to deal with such problems. It is due to the fact that almost all of the challenging nonconvex optimization problems in general and the ones related to physical layer security in partic can be reformulated as DC programs. Furthermore, many evidences have also shown that DCA outp erforms other algorithms in a lot of cases [15, 16, 12, 13]. In fact, there are more and more researchers using DC programming and DCA as an innovative approach to nonconvex programming because of its effectiveness [24, 10, 1]. Nevertheless, the results obtained from DCA heavily depend on how the problem is decomposed into a DC program. In other words, finding a suitable DC decomposition plays an essential role in achieving a good result for DC program as well as optimizing the running time of computer.

In this paper, we consider the cooperative jamming paradigm, where the friendly jammers cooperate with the users to introduce an interference disturbing the eavesdropper. The purpose of this problem is to find an effective way to allocate the power of sources from users as well as from friendly jammers so as to maximize the sum of their secrecy rates. This model is introduced and solved by three authors Alberth Alvarado, Gesualdo Scutari, and Jong-Shi Pang from the United State, using their novel decomposition technique proposed in [2]. They have formulated the system design as a game where the legitimate users are players who cooperate with the jammers to maximize their own secrecy rate. We will propose here in a new DC decomposition technique for this problem, which can result in strongly convex quadratic subproblems with separate variables. The resulting problems are easy to solve by both centralized and distributed methods.

## II. A NOVEL RESOURCE ALLOCATION PROBLEM IN THE EMERING AREA OF COOPERATIVE PHYSICAL LAYER SECURITY

We take into account a wireless communication system comprised of $Q$ transmitter and receiver pairs-the legitimate users, $J$ friendly jammers, and a single eavesdropper. OFDMA transmissions are assumed for the legitimate users over flat-fading and quasi-static (constant within the transmission) channels. Let us denote $H_{qq}^{SD}$, $H_{jq}^{JD}$, $H_{je}^{JE}$, $H_{qe}^{SE}$ respectively as the channel gain of the legitimate source-destination pair $q$, the channel gain between the transmitter of jammer $j$ and the receiver of user $q$, the channel gain between the transmitter of jammer $j$ and the receiver of the eavesdropper, the channel gain between the source of user $q$ and the eavesdropper. We also assume CSI of the eavesdropper's channels; This is a common assumption in PHY security literature; see, e.g., [8]. CSI on the eavesdropper's channel can be obtained when the eavesdropper is active in the network and its transmissions can be monitored.

We follow the cooperative jamming (CJ) paradigm, in which the friendly jammers cooperate with the users by giving a proper interference profile to mask the eavesdropper. The power allocation of source $q$ is denoted by $p$; $p_{jq}^{j}$ is the fraction of power allocated by friendly jammer $j$ over the channel used by user $q. \mathbf{p}_q^j \triangleq \left(p_{jq}^{j}\right)$ is the power profile allocated by all the jammers over the channel of user $q$. The power budget of user $q$ and jammer $j$ do not exceed $P_q$ and $P_j^J$, respectively.

From information theoretical assumption, the maximum achievable rate on link $q$ is

$$r_{qq}\left(p_q, \mathbf{p}_q^J\right) \triangleq \log\left(1 + \frac{H_{qq}^{SD} p_q}{\sigma^2 + \sum_{j=1}^{J} H_{jq}^{JD} p_{jq}^{J}}\right) \quad (1)$$

Similarly, the rate on the channel between source $q$ and the eavesdropper is

$$r_{qe}\left(p_q, \mathbf{p}_q^J\right) \triangleq \log\left(1 + \frac{H_{qe}^{SE} p_q}{\sigma^2 + \sum_{j=1}^{J} H_{je}^{JE} p_{jq}^{J}}\right) \quad (2)$$

The secrecy rate of user $q$ is then (see, e.g., [8])

$$r_q^s \triangleq \left[r_{qq}\left(p_q, \mathbf{p}_q^J\right) - r_{qe}\left(p_q, \mathbf{p}_q^J\right)\right] + \quad (3)$$

**Problem Formulation**: The system design is formulated as a game where the legitimate users are the players who cooperate with the jammers to maximize their own secrecy rate. More generally, each user $q$ seeks together with the jammers the tuple $\left(p_q, \mathbf{p}_q^j\right)$ satisfying the following optimization problem:

$$\begin{aligned} &\mathrm{Max}_{\left(p_q, \mathbf{P}_q^J\right)_q \geq 0} \; r(\mathbf{p}, \mathbf{p}^J) \triangleq \sum_{q=1}^{Q} r_q^s \\ &\mathrm{s.t} \quad p_q \leq P_q, \quad \forall q = 1, \dots, Q, \\ &\qquad \sum_{r=1}^{Q} p_{jr}^J \leq P_j^J, \; \forall j = 1, \dots, J \end{aligned} \quad (4)$$

Note that

$$r_{qq}\left(p_q, \mathbf{p}^J\right) \geq r_{qe}\left(p_q, \mathbf{p}^J\right)$$

$$\Leftrightarrow \left[\begin{array}{c} p_{q=0} \\ \dfrac{H_{qq}^{SD}}{\sigma^2 + \sum_{j=1}^{J} H_{jq}^{JD} p_{jq}^J} \geq \dfrac{H_{qe}^{SE}}{\sigma^2 + \sum_{j=1}^{J} H_{je}^{JE} p_{jq}^J} \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{c} p_q = 0 \\ \sum_{j=1}^{J}\left(H_{qq}^{SD} H_{je}^{JE} - H_{qe}^{SE} H_{jq}^{JD}\right) p_{jq}^J \\ + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0 \end{array}\right. \quad (*)$$

If (*) is violated, it means that $r_q^s = 0$, i.e., the secrecy rate of the players equal to zero, which is insignificant since players try to maximize their secrecy rate. Therefore, we can ignore the feasible players' strategy profiles not satisfying (*). It leads us to solving the following smooth problem:

$$\begin{aligned} &\mathrm{Max}_{\left(p_q, \mathbf{P}_q^J\right)_{q \geq 0}} \; r(\mathbf{p}, \mathbf{p}^J) \\ &\quad \triangleq \sum_{q=1}^{Q} \left[r_{qq}\left(p_q, \mathbf{p}_q^J\right) - r_{qe}\left(p_q, \mathbf{p}_q^J\right)\right] \\ &\mathrm{s.t.} \quad p_q \leq P_q, \quad \forall q = 1, \dots, Q, \\ &\qquad \sum_{r=1}^{Q} p_{jr}^J \leq P_j^J, \; \forall j = 1, \dots, J \\ &\qquad \sum_{j=1}^{J}\left(H_{qq}^{SD} H_{je}^{JE} - H_{qe}^{SE} H_{jq}^{JD}\right) p_{jq}^J \\ &\qquad + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0, \\ &\qquad\qquad \forall q = 1, \dots, Q \end{aligned} \quad (5)$$

Instead of solving the problem (5), we will solve the following equivalent problem.

$$\begin{aligned} &\mathrm{Min}_{\left(p_q, \mathbf{p}_q^J\right) \geq 0} \; r_1(\mathbf{p}, \mathbf{p}^J) \\ &\quad \triangleq \sum_{q=1}^{Q} \left[-r_{qq}\left(p_q, \mathbf{p}_q^J\right) + r_{qe}\left(p_q, \mathbf{p}_q^J\right)\right] \\ &\mathrm{s.t.} \quad p_q \leq P_q, \quad \forall q = 1, \dots, Q, \\ &\qquad \sum_{r=1}^{Q} p_{jr}^J \leq P_j^J, \; \forall j = 1, \dots, J \\ &\qquad \sum_{j=1}^{J}\left(H_{qq}^{SD} H_{je}^{JE} - H_{qe}^{SE} H_{jq}^{JD}\right) p_{jq}^J \\ &\qquad + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0 \\ &\qquad\qquad \forall q = 1, \dots, Q \end{aligned} \quad (6)$$

## III. DC PROGRAMMING AND DCA FOR SOLVING THE PROBLEM (6)

### *A. A brief introduction of DC programming and DCA*

DC Programming and DCA constitute the backbone of smooth/nonsmooth nonconvex programming and global optimization. They are introduced by Pham Dinh Tao in 1985 in their preliminary form and extensively developed by Le Thi Hoai An and Pham Dinh Tao since 1994 to become now classic and more and more popular. DCA is a continuous primal dual subgradient approach. It is based on local optimality and duality in DC programming in order to solve standard DC programs which are of the form

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

with $g, h \in \Gamma_0(\mathbb{R}^n)$, which is a set of lower semi-continuous proper convex functions on $\mathbb{R}^n$. Such a function $f$ is called a DC function, and $g - h$, a DC decomposition of *f*, while the convex functions $g$ and $h$ are DC components of *f*. A constrained DC program whose feasible set *C* is convex always can be transformed into an unconstrained DC program by adding the indicator function of *C* to the first DC component.

Recall that, for a convex function $\phi$, the subgradient of $\phi$ at $x_0$, denoted as $\partial\phi(x_0)$, is defined by

$$\partial\phi(x_0) := \{y \in \mathbb{R}^n : \phi(x) \geq \phi(x_0) + \langle x - x_0, y\rangle, \forall x \in \mathbb{R}^n\}$$

The main principle of DCA is quite simple, that is, at each iteration of DCA, the convex function $h$ is approximated by its affine minorant at $y^k \in \partial h(x^k)$, and it leads to solving the resulting convex program.

$$y^k \in \partial h(x^k)$$
$$x^{k+1} \in \arg\min_{x\in\mathbb{R}^n}\{g(x) - h(x^k) - \langle x - x^k, y^k\rangle\}. (P_k)$$

The computation of DCA is only dependent on DC components $g$ and $h$ but not the function $f$ itself. Actually, there exist infinitely many DC decompositions corresponding to each DC function and they generate various versions of DCA. Choosing the appropriate DC decomposition plays a key role since it influences on the properties of DCA such as convergence speed, robustness, efficiency, globality of computed solutions,... DCA is thus a philosophy rather than an algorithm. For each problem, we can design a family of DCA based algorithms. To the best of our knowledge, DCA is actually one of the rare algorithms for nonsmooth nonconvex programming which allow to solve large-scale DC programs. DCA was successfully applied for solving various nonconvex optimization problems, which quite often gave global solutions and is proved to be more robust and more efficient than related standard methods [19–21] and the list of reference in [11].

This is a DCA generic scheme:

```
• Initialization. Choose an initial point $x_0$. $0 \longleftarrow k$
• Repeat.
    Step 1. For each $k, x^k$ is known, computing $y^k \in \partial h(x^k)$.
    Step 2. Calculating $x^{k+1} \in \partial g^*(y^k)$
    where $\partial g^*(y^k) = \arg\min_{x\in\mathbb{R}^n}\{g(x) - h(x^k) - \langle x - x^k, y^k\rangle : x \in C\}$
    Step 3. $k \longleftarrow k+1$
Until stopping condition is satisfied.
```

The convergence properties of DCA and its theoretical basis is analyzed and proved completely in [19, 14, 20]). Some typical important properties of DCA are worth being recalled here.

**i)** DCA is a descent method without line search but with global convergence : the sequences $\{g(x^k) - h(x^k)\}$ and $\{h^*(y^k) - g^*(y^k)\}$ are decreasing.

**ii)** If the optimal value $\alpha$ of DC program is finite and the infinite sequences $\{x^k\}$ and $\{y^k\}$ are bounded, then every limit point $x^*(\text{resp.}\, y^*)$ of sequence $\{x^k\}$ (resp. $\{y^k\}$) is a critical point of $(g - h)(\text{resp.}\,(h^* - g^*))$, i.e. $\partial g(x^*) \cap \partial h(x^*) \neq \emptyset$ (resp. $\partial h^*(y^*) \cap \partial g^*(y^*) \neq \emptyset$ )

**iii)** DCA has a linear convergence for DC programs.

**iv)** DCA has a finite convergence for polyhedral DC programs.

*B. DC programming and DCA for the problem* (6)

The new DC decomposition for the objective function of (6)

For any value of ρ, the objective function of the problem (6) can be written in the form:

$$r_1(\mathbf{p}, \mathbf{p}^J) = G(\mathbf{p}, \mathbf{p}^J) - H(\mathbf{p}, \mathbf{p}^J),$$

where

$$G(\mathbf{p}, \mathbf{p}^J) = \rho\left(\sum_{q=1}^{Q} p_q^2 + \sum_{j=1}^{J}\sum_{q=1}^{Q} p_{jq}^{J2}\right)$$

$$H(\mathbf{p}, \mathbf{p}^J) = \left[\rho\left(\sum_{q=1}^{Q} p_q^2 + \sum_{j=1}^{J}\sum_{q=1}^{Q} p_{jq}^{J2}\right) - \sum_{q=1}^{Q}\left(-r_{qq}(p_q, \mathbf{p}_q^J) + r_{qe}(p_q, \mathbf{p}_q^J)\right)\right]$$

**Proposition 1.** *If* $\rho \geq \frac{M^2}{\sigma^4}\sqrt{1+2J+4J^2}$, *then both* $G(\mathbf{p}, \mathbf{p}^J)$ *and* $H(\mathbf{p}, \mathbf{p}^J)$ *are convex, where* $M = \max_{q=1,\dots,Q; j=1,\dots,J}\left\{H_{qe}^{SE},\ H_{qq}^{SD}, H_{jq}^{JD}, H_{je}^{JE}\right\}$.

From this proposition with $\rho \geq \frac{M^2}{\sigma^4}\sqrt{1+2J+4J^2}$, $G(\mathbf{p}, \mathbf{p}^J) - H(\mathbf{p}, \mathbf{p}^J)$ is a DC decomposition of the objective of (6), which is different from that in [2]. As a result, we obtain a new DC program as follows

$$
\begin{aligned}
\text{Min}\quad & r_1(\mathbf{p}, \mathbf{p}^J) \triangleq G(\mathbf{p}, \mathbf{p}^J) - H(\mathbf{p}, \mathbf{p}^J) \\
\text{s.t.}\quad & (p_q, \mathbf{p}_q^J)_q^Q \geq 0 \\
& p_q \leq P_q, \quad \forall q = 1,\dots,Q, \\
& \sum_{r=1}^{Q} p_{jr}^J \leq P_j^J,\ \ \forall j = 1,\dots,J \\
& \sum_{j=1}^{J}\left(H_{qq}^{SD}H_{je}^{JE} - H_{qe}^{SE}H_{jq}^{JD}\right)p_{jq}^J \\
& + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0, \\
& \qquad \forall q = 1,\dots,Q
\end{aligned}
$$

Following the generic DCA scheme described in Section III.A, DCA applied on (6) is given by the algorithm below.

**DCA scheme for DC program (6)**

- **Initialization.** Choose an initial point $x^0 = (\boldsymbol{p}^0, \boldsymbol{p}^{J,0}), 0 \leftarrow k$.
- **Repeat**.

**Step 1.** For each $k, x^k = (\mathbf{p}^k, \mathbf{p}^{J,k})$ is known, compute $y^k = \left(\bar{\mathbf{p}}^k, \bar{\mathbf{p}}^{J,k}\right) = \nabla \mathrm{H}\left(x^k\right)$ with

$$
\nabla \mathrm{H}(x) = \begin{bmatrix} \left(2\rho p_q - \dfrac{H_{qe}^{SE}}{\sigma^2 + H_{qe}^{SE}p_q + A} + \dfrac{H_{qq}^{SD}}{\sigma^2 + H_{qq}^{SD}p_q + B}\right) \\ \left(\begin{array}{c} 2\rho p_{jq}^J - \dfrac{H_{je}^{JE}}{\sigma^2 + H_{qe}^{SE}p_q + A} + \dfrac{H_{je}^{JE}}{\sigma^2 + A} + \\ \dfrac{H_{jq}^{JD}}{\sigma^2 + H_{qq}^{SD}p_q + B} - \dfrac{H_{jq}^{JD}}{\sigma^2 + B} \end{array}\right) \end{bmatrix}
$$

where $q = 1,\dots,Q;\ j = 1,\dots,J$,

$A = \sum_{k=1}^{J} H_{ke}^{JE}p_{kq}^J$, $B = \sum_{k=1}^{J} H_{kq}^{JD}p_{kq}^J$.

**Step 2.** Find $x^{k+1} = \left(\mathbf{p}^{k+1}, \mathbf{p}^{J,k+1}\right)$ by solving the following convex subproblem.

$$
\text{Min}\quad \rho\left(\textstyle\sum_{q=1}^{Q} p_q^2 + \sum_{j=1}^{J}\sum_{q=1}^{Q} p_{jq}^{J2}\right) - \langle y^k, x\rangle \quad (7)
$$

s.t.

$$
\mathrm{x} = (x_q)_{q=1}^{Q} = (p_q, \mathbf{p}_q^J)_{q=1}^{Q} \geq 0
$$

$$
p_q \leq P_q, \quad \forall q = 1,\dots,Q,
$$

$$
\sum_{r=1}^{Q} p_{jr}^J \leq P_j^J,\ \ \forall j = 1,\dots,J \qquad (8)
$$

$$
\begin{aligned}
& \sum_{j=1}^{J}\left(H_{qq}^{SD}H_{je}^{JE} - H_{qe}^{SE}H_{jq}^{JD}\right)p_{jq}^J \\
& + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0, \\
& \qquad \forall q = 1,\dots,Q \qquad (9)
\end{aligned}
$$

**Step 3.** $k \leftarrow k+1$

- **Until** the stopping condition is satisfied.

**The distributed dual-decomposition method to solve the convex subproblem (7)**

In the DCA scheme proposed above, we use the distributed dual-decomposition approach for solving the convex subproblem in (7). The distributed method is often used when one has to face the large scale optimization problem in order to divide the original problem into smaller ones. However, the barrier to applying this method to the subproblem (7) is the appearance of coupling constraints (8). Therefore, a dual approach combined with a distributed method is a perfect way to overcome this difficulty.

Firstly, we form partial Lagrangian

$$
\begin{aligned}
& L(\mathbf{p}, \mathbf{p}^J, \lambda) \\
&= \rho\left(\sum_{q=1}^{Q} p_q^2 + \sum_{j=1}^{J}\sum_{q=1}^{Q} p_{jq}^{J2}\right) - \langle y^k, x\rangle \\
&\quad + \sum_{j=1}^{J}\lambda_i\left(\sum_{r=1}^{Q} p_{jr}^J - P_j^J\right) \\
&= \sum_{\boldsymbol{q=1}}^{\boldsymbol{Q}}\left(\rho p_q^2 + \rho\sum_{j=1}^{J} p_{jq}^{J2} - \langle y_q^k, x_q\rangle + \sum_{j=1}^{J}\lambda_i p_{jq}^J\right) \\
&\quad - \sum_{j=1}^{J}\lambda_i p_j^J \\
&= \sum_{q=1}^{Q} L_q(p_q, \mathbf{P}_q^J, \lambda) - \sum_{j=1}^{J}\lambda_i p_j^J
\end{aligned}
$$

where $x_q = \left(p_q, (p_{jq}^J)_{j=1,\dots,J}\right)$,

$y_q^k = \left(\bar{p}_q^k, \bar{p}_{jq}^{J,k})_{j=1,\dots,J}\right)$.

The dual problem associated with (7) is then

$$
\text{Max}_{\lambda \geq 0}\left\{g(\lambda) = \text{Min}_{(\mathbf{p},\mathbf{p}^J)\in S} L(\mathbf{p}, \mathbf{p}^J, \lambda)\right\} \quad (10)
$$

where $S = \{x = (\mathbf{p}, \mathbf{p}^J)\}$ satisfies the following constraints

$$x = (x_q)_{q=1}^{Q} = (p_q, \mathbf{p}_q^J)_{q=1}^{Q} \geq 0$$
$$p_q \leq P_q \quad \forall q = 1, \dots, Q,$$
$$\sum_{j=1}^{J} \left(H_{qq}^{SD} H_{je}^{JE} - H_{qe}^{SE} H_{jq}^{JD}\right) p_{jq}^{J} + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \geq 0,$$
$$\forall q = 1, \dots, Q$$

The inner minimization in (10) has an unique solution $\hat{x}(\lambda) \triangleq (\hat{x}_q(\lambda))_{q=1}^{Q}$, that is

$$\hat{x}_q(\lambda) \triangleq \text{argmin}_{x_q \in S_q}\{ L_q(p_q, \mathbf{P}_q^J, \lambda)\} \quad (11)$$

With $S_q = \{x_q\text{=}(p_q, \mathbf{p}_q^J)\}$ satisfies the following constraints

$$x_q\text{=} (p_q, \mathbf{p}_q^J) \geq 0$$
$$p_q \leq P_q$$
$$\sum_{j=1}^{J} \left(H_{qq}^{SD} H_{je}^{JE} - H_{qe}^{SE} H_{jq}^{JD}\right) p_{jq}^{J} + \left(H_{qq}^{SD} - H_{qe}^{SE}\right)\sigma^2 \quad \geq 0$$

**Proposition 2.** *$g(\lambda)$ is differentiable on $\mathbb{R}_+^J$, with gradient*

$$\nabla\lambda g(\lambda) = \sum_{q=1}^{Q} \hat{\mathbf{p}}_q^J - P$$

*where $P = (P_j^J)_{j=1,\dots,J}$*

We now can solve the dual problem by using the well-known gradient algorithm ([4]) as the following scheme

**Distributed dual-decomposition based Algorithm**

- **Initialization.** Choose an initial point $\lambda^0 \geq 0$ and a sequence $\{\alpha^t\}$ such that $\{\alpha^t\}$ satisfies $\alpha^t > 0$, $\alpha^t \to 0$, $\sum_t \alpha_t = \infty$, $\sum_t {\alpha_t}^2 < \infty$, set $t = 0$.
- **Repeat.**

**Step 1.** Solve (11) for all $q = 1, \dots, Q$ to find the solutions $\left(\hat{x}_q(\lambda^t)\right)_{q=1}^{Q}$

**Step 2.** Update λ by the following formula

$$\lambda^{t+1} \triangleq \left[\lambda^t + \alpha^t \left(\sum_{q=1}^{Q} \hat{\mathbf{p}}_q^{J,t} - P\right)\right]_+$$

**Step 3.** *t ← t + 1.*

- **Until** the stopping condition is satisfied.

**Theorem 1.** *The sequence $\{\lambda^t\}$ generated by the above algorithm converges to a solution of (10) and the sequence $\{\hat{x}_q(\lambda^t)\}$ converges to the unique solution of (7).*

## IV. NUMERICAL RESULTS

### A. Datasets

The position of the users, jammers, and eavesdropper are randomly generated within a square area; the channel gain $H_{qq}^{SD}$, $H_{jq}^{JD}$, $H_{je}^{JE}$, $H_{qe}^{SE}$ are Rayleigh distributed with mean equal to one and normalized by the distance between the transmitter and the receiver. The results are collected only for the channel realizations satisfying condition (9).

TABLE 1. SYSTEM SECRECY RATE (SSR) VERSUS NUMBER *Q* OF LEGITIMATE USERS

| **Q** | **DCA** | | | **SCA** | | |
|---|---|---|---|---|---|---|
| | **SSR** | **SSR Best** | **CPU (s)** | **SSR** | **SSR Best** | **CPU (s)** |
| 10 | 5,192<br>(0,072) | **5,303** | 122,9 | 4,915<br>(0,011) | 4,923 | 194,8 |
| 20 | 13,221<br>(0,044) | **13,280** | 864,9 | 13,199<br>(0,052) | 13,205 | 677,2 |
| 30 | 15,611<br>(0,062) | 15,683 | 1748,8 | 15,901<br>(0,043) | **15,909** | 1861,1 |
| 40 | 19,268<br>(0,059) | **19,319** | 2021,1 | 18,974<br>(0,007) | 18,982 | 2615,7 |
| 50 | 28,549<br>(0,064) | **28,605** | 3809,8 | 26,719<br>(0,025) | 26,720 | 4000,3 |

TALBE 2. SYSTEM SECRECY RATE (SSR) VERSUS THE VARIOUS VALUES OF *SNR* IN THE CASE OF 20 USERS

| | snr | 10 | 20 | 30 | 40 |
|---|---|---|---|---|---|
| **DCA** | **SSR** | **10,054** | 13,208 | **14,831** | **15,822** |
| **SCA** | **SSR** | 9,842 | **13,220** | 14,676 | 15,817 |

### B. Setting parameter and stopping criteria

In this paper, we present some experiment results obtained from DCA and make a comparision with those obtained from SCA mentioned in [2]. Therefore, to ensure fair comparison, all parameters are set in the same way as in [2]. All users and jammers have the same power budget, i.e. $P_q = P_j^J = P$ and we set snr $= \frac{P}{\sigma^2} = 10dB$. The number of jammers, *J*, is set to equal $\left[\frac{Q}{2}\right]$.

The initial points are randomly generated five times and then they are shared for both DCA and SCA. In each table, the average of the gained results corresponding to each initial point is chosen as the final value of System Secrecy Rate (SSR) and the standard deviation is also accompanied (that is indicated in parenthesis). The best values of SSR are collected and reported in the SSR Best column. The distributed dual-decomposition based Algorithm is finished when the norm of the difference of $\lambda$ obtained from two successive iterations is less than $1e-2$. The DCA-based algorithms are terminated when at least one of the following criteria are satisfied:

• The absolute value of the difference of SSR in two consecutive iterations becomes smaller than $1e-5$.

• The norm of the difference of two tuples $(\mathbf{p},\mathbf{p}^J)$ obtained from two consecutive iterations becomes smaller than $1e-5$.

### *C. Numerical result and comments*

In Table 1, we compare the value of SSR versus the number Q of legitimate users obtained by DCA and SCA, respectively. This table also shows the running times of both algorithms versus the number of legitimate users. In Table 2, we show the dependence of SSR on *snr* in the case of 20 users. In general, the numerical results show that SSR achieved by both algorithms tends to increase with the number of users as well as *snr*. It can be observed from the Table 1 that the DCA yields system secrecy rates better than those of SCA in almost all cases while it is less expensive. Table 2 expresses the comparison of the gains from both algorithms corresponding to the different values of *snr* in the case of 20 users. This table shows that the increase of *snr* tends to lead to the rise of SSR. The gains of DCA is always better than those of SCA.

## V. CONCLUSIONS

In this paper, we have used one of the cooperative transmission techniques in physical layer so as to assure confidentiality of transmitted data over a wireless network, that is cooperative jamming technique. The confidentiality task indicated in this paper leads to maximizing sum of secrecy rates of all users subject to power constraints of sources and jammers. The resulting power allocation problem is solved by a new and efficient distributed DCA based algorithm. The experimental results on some datasets have shown the robustness as well as the efficiency of DCA based on this new DC decomposition in term of both the running time and the objective value. It provides more evidences to show that DC programming and DCA is an efficient and robust approach for solving the nonconvex optimization problems in the wide range of areas. In addition, the technique of decomposing DC proposed in this paper can be also applied to various optimization problems. The advantage of this DC decomposition technique is that it leads to quadratic convex subproblems with separate variables, which facilitates use of distributed method. This distributed approach is used when one have to deal with the large scale problem often arising in communication system, signal processing and networking.

## REFERENCES

[1]. Al-Shatri, A. Weber, T, “Achieving the maximum sum rate using dc programming in cellular networks”. IEEE Trans. Signal Process 60(3), pp. 1331-1341, March 2012.

[2]. Alvarado, A., Scutari, G., Pang, J.S, “A new decomposition method for multiuser dc-programming and its application”. Signal Pro cessing, IEEE Transactions on 62(11), pp. 2984-2998, 2014.

[3]. Barenghi, A., Breveglieri, L., Koren, I., Naccache, D, “Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures”. Proc. IEEE 100(11), pp. 3056-3076, November 2012.

[4]. Bertsekas, D .P., Nedic, A., Ozdaglar, E, “Convex analysis and optimization. Athena Sicientific Belmont, 2003.

[5]. Dong, L., Han, Z., Petropulu, A., Poor, H, “Improving wireless physical layer security via cooperating relays”. IEEE Trans. Signal Process 58(3), pp. 1875-1888, March 2010.

[6]. Goel, S., Negi, R, “Guaranteeing secrecy using artificial noise”. Wireless Communications, IEEE Transactions on 7(6), pp. 2180-2189, June 2008.

[7]. He, X., Yener, A, “Cooperative jamming: The tale of friendly interference for secrecy”, pp. 65-88, Spinger, 2010.

[8]. Jorswieck, E., Wolf, A., Gerbracht, S, “Secrecy on the Physical Layer in Wireless Networks”, vol. ch. 20, INTECH 2010.

[9]. Kapoor, G., Piramithu, S, “Vulnerabilities in some recently proposed rfid ownership transfer protocols”. IEEE Commun. Lett. 14(3), pp. 260-262, March 2010.

[10]. Kha, H.H., Tuan, H.D., Nguyen, H.H, “Fast global optimal power allocation in wireless network by local dc programming”. IEEE Trans. On Wireless Communications 11(2), pp. 510-512, February 2012.

[11]. Le Thi, H.A, “DC Programming and DCA”. http://www.lita.univ-lorraine.fr/~lethi/

[12]. Le Thi, H.A., Nguyen, M.C., Pham Dinh, T, “A DC Programming Approach for Finding Communities in Networks”. Neural Computation 26(12), pp. 2827-2854, September 2014.

[13]. Le Thi, H.A., Nguyen, M.C., Pham Dinh, T, “Self-Organizing Maps by Difference of Convex functions optimization”. Data Mining and Knowledge Discovery 28, pp. 1336-1365, September 2014.

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

[15]. Le Thi, H.A., Vo, X.T., Le, H.M., Pham Dinh, T, “DC approximation approaches for sparse optimization”. European Journal of Operational Research 244(1), pp. 26-46, 2015.

[16]. Le Thi, H.A., Vo, X.T., Pham Dinh, T, “Feature selection for linear SVMs under uncertain data:Robust optimization based on difference of convex functions algorithms”, Neural Networks 59, pp. 36-50, 2014.

[17]. Li, J., Petropulu, A., Web er, S, “On cooperative relaying schemes for wireless physical layer security”. IEEE Trans. Signal Pro cess 59(10), pp. 4985-4997, October 2011.

[18]. Mutherjee, A., Fako orian, S.A.A., Huang, J., Swindlehurst, A.L, “Principle of physical layer security in multiuser wireless networks: A survey. Communication Survey and Tutorials”, IEEE 16(3), pp. 1550–1573, 2014.

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

[20]. Pham Dinh, T., Le Thi, H.A, “Optimization algorithms for solving the trust region subproblem”. SIAM J. Optimization 8, pp. 476-505, 1998.

[21]. Pham Dinh, T., Le Thi, H.A, “Recent Advances in DC Programming and DCA”, vol. 8342. Springer Berlin Heidelberg, 2014.

[22]. Schneier, “Cryptographic design vulnerabilities”. IEEE Computer 31(9), pp. 26-33, 1998.

[23]. Stano jev, I., Yener, A, “Improving secrecy rate via sp ectrum leasing for friendly jamming”. IEEE Trans. Inf. Forensics Security 12(1), pp. 134-145, January 2013.

[24]. Vucic, N., Schubert, M, “Dc programming approach for resource allocation in wireless networks”. IEEE, Proceedings of the 8th International Symp osium on Mo deling and Optimization in Mobile, Ad Hoc and Wireless Networks, pp. 380-386, May 2010.

[25]. Wyner, A.D, “The wire-tap channel”. Bell Sys. Tech. Journ. 54, pp. 1355-1387, 1975.

## AUTHORS PROFILE

**Prof. PhD. Le Thi Hoai An**

Workplace: Laboratory of Theoretical & Applied Computer Science, University of Lorraine.

Email: hoai-an.le-thi@univ-lorraine.fr

The education process: earned her PhD with Highest Distinction in Optimization in 1994, and her Habilitation in 1997 both from university of Rouen, France. From 1998 to 2003 she was Associate Professor at the National Institute for Applied sciences, Rouen. Since 2003 she is Full Professor at the University of Paul Verlaine - Metz (which becomes University of Lorraine in 2012).

Research today: Machine Learning, Optimization and Operations Research and applications in Information Systems and various complex Industrial Systems.

**Prof. Dr. Pham Dinh Tao**

Workplace: National Institute for Applied Sciences, Rouen, France.

Email: taopham@insa-rouen.fr

Research today: numerical analysis, optimization and operations research and their applications in various fields of applied sciences (mechanics, image and signal processing, machine learning, bioinformatics, cryptology, finance, commun-ication/transport systems, etc.).

**Tran Thi Thuy**

Workplace: Laboratory of Theoretical & Applied Computer Science, University of Lorraine.

Email: thi-thuy.tran@univ-loraine.fr

The education process: Between 2001 and 2008, she was with the Mathematics Division at Water Resources University, has been a mathematics lecturer at FPT University since 2009. She is currently a PhD student at the Laboratory of Theoretical & Applied Computer Science, University of Lorraine.

Research today: nonconvex optimization applied on communication system.