Initial point for enhancing DC Programming and DCA in Physical Layer Security

Nguyen Nhu Tuan

***Abstract*— Physical layer security (PLS) is to enable confidential data transmission through wireless communication systems in the presence of illegitimate receivers, without basing on higher-layer encryption. The goal of PLS is to make use of the properties of the physical to enable critical aspects of secure communication. PLS's additional strength is that it is based on information-theoretic security, which assumes no limit on the opponent's computational power and is thus inherently quantum-resistant. In general, PLS problems are non-convex programming and thus hard to deal with. One approach to handling these problems is based on DC programming and DCA, in which finding a good initial point of DCA scheme is still a complicated, challenging and open problem. This paper proposal some good initial points for the PLS problem DCA-DF scheme on Decode-and-Forward relaying wireless networks.**

***Tóm tắt*—Bảo mật tầng vật lý đang được nghiên cứu ứng dụng với mục tiêu bảo mật dữ liệu trong mạng truyền tin vô tuyến có sự xuất hiện của các trạm nghe lén mà không sử dụng các thuật toán mật mã tại các tầng phía trên. Bản chất của bảo mật tầng vật lý là dựa vào các đặc trưng vật lý của tín hiệu để bảo mật truyền thông. Một trong những ưu điểm của bảo mật tầng vật lý khiến giới khoa học đang tập trung nghiên cứu đó là chúng không phụ thuộc vào bài toán khó của quá trình phân tích mã, hay nói cách khác là tính bí mật của phương pháp không bị ảnh hưởng khi máy tính lượng tử ra đời. Theo lý thuyết thông tin, thường thì các bài toán bảo mật tầng vật lý được mô hình hóa thành các bài toán quy hoạch không lồi và khó giải tìm nghiệm tối ưu. Một trong những phương pháp giải các bài toán quy hoạch không lồi này đang được nghiên cứu và công bố gần đây là ứng dụng Quy hoạch DC và giải thuật DCA. Trong đó, việc tìm được một điểm ban đầu tốt cho giải thuật DCA đang được cho là khó và được các nhà nghiên cứu quan tâm. Bài báo này đề xuất một số điểm ban đầu tốt để nâng cao hiệu quả ứng dụng Quy hoạch DC và giải thuật DCA cho bài toán bảo mật tầng vật lý đối với mạng vô tuyến chuyển tiếp hoạt động theo kỹ thuật Giải mã – Chuyển tiếp.**

Keywords—Physical layer security; DC programming and DCA; decode-and-forward.

Từ khóa— Bảo mật tầng vật lý; quy hoạch DC và thuật toán DCA; giải mã chuyển tiếp.

I. INTRODUCTION

The concept of secrecy communication was first proposed in the pioneering work from 1949 by Shannon [1], in which secrecy communication was investigated from the viewpoint of information theory. Recently, the traditional communication security methods rely on cryptographic algorithms at the upper layers of multi-layer communication models that are being studied and widely applied. In wireless networks, another trend for security communication that has been extensively researched lately is physical layer security (PLS) without using cryptographic algorithms and resistance to quantum computers. Actually, the research on physical layer security was pioneered by Dr. Aaron D. Wyner since 1975 [2]. Wyner has demonstrated that it is possible to transmit security information at C_s rate (bits/symbol) in a communication system that has the presence of an eavesdropper ($C_s \geq 0$). C_s is the secrecy capacity of a discrete memoryless channel, that was the maximum value of the difference between the mutual information of the legitimate channel and the mutual information of the wiretap channel.

Over the past two decades, with the rapid development of wireless communications technology, physical layer security methods have been studied widely [3, 4, 5, 6]. A great effort to increase the achievable secrecy rate in PLS is cooperative nodes networks with act two roles are cooperative jamming [5] and cooperative relaying [3, 7]. Therefore, the secrecy rate value is defined as follows:

This manuscript is received on December 07, 2022. It is commented on December 08, 2022 and is accepted on December 20, 2022 by the first reviewer. It is commented on December 08, 2022 and is accepted on December 21, 2022 by the second reviewer.

$$R_s = min\{log(1 + SNR_d) - log(1 + SNR_e)\}.$$

Where, SNR_d and SNR_e are the signal-to-noise ratios at the legitimate user destination and the eavesdropper, respectively.

This paper focused on the cooperative relaying network with Decode-and-Forward (DF) technique in the present of one eavesdropper. The wireless relay beamforming network problem in this paper is modeled as a nonconvex optimization problem. In which, the objective function is the value of the secrecy rate of the system R_s (bits/symbol) and the solutions of this optimization problem are the beamforming weights of the relay stations. We investigate in the case of having perfect channel state information (CSI) in both legitimate and illegitimate users. This paper presents the state-of-the-art DF cooperative relaying networks and the experiments to show in detail the effects of our proposal.

The rest of the paper is organized as follows: Section II presents the DF system model and PLS programming problem; Some approaches and proposals are introduced in Section III; Section IV is the experiments and results; and the last one is the conclusion section.

Notations: In this paper, the bold uppercase letters are denoted for the matrices; The bold lowercase letters indicate the column vector; The symbols $(.)^T$, $(.)^\dagger$ are used for transpose and conjugate transpose, respectively; $\boldsymbol{I}_M$ is identity/unit matrix with dimension M; *diag{**a**}* or ***D(a)*** is denoted for Diagonal matrix with elements on the diagonal is the value of the vector ***a***; $\|\boldsymbol{a}\|$ is denoted for 2norm of vector ***a***; $\boldsymbol{A} \succcurlyeq 0$ is denoted for matrix ***A*** working as a semidefinite positive matrix; $\mathbb{C}$ is denoted for a complex form; s.t. (subject to) is denoted for constraints of the optimal problem; *trace(**A**)* is a trace of matrix ***A***.

II. System model and problem

The system includes a source station (S), a destination station (D), M trusted relay stations and an eavesdropper station (E), as shown in Figure 1.

As all the source and the relays are located in a small trusted zone, the relays can receive the signal properly, and the power of the signal, which are broadcast from the source would be not strong enough to send directly to destination and eavesdropper stations. The channel gain from the relays to D and E denoted by the complex constraints h_{rd} and h_{re} ($h_{rd}, h_{\text{re}} \in \mathbb{C}$), respectively.

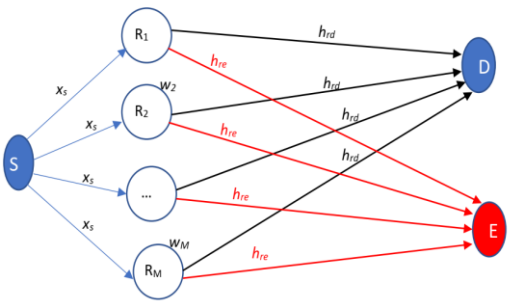

Figure 1. The system model Decode-and-Forward with one eavesdropper

The S station sends signal x_s to M relay stations, these relays decode the received signal and re-encode it, then cooperatively transmit the re-encode symbols to the destination station. At the D station and E station, the received SNR are:

$$SNR_d = \frac{\left|\sum_{m=1}^{M} h_{\text{rd,m}}\, w_m\right|^2}{\sigma^2}$$
$$SNR_e = \frac{\left|\sum_{m=1}^{M} h_{\text{re,m}}\, w_m\right|^2}{\sigma^2} \quad (1)$$

Where $w_i, i = 1 \div M$ are relaying weight; σ is variance of Gaussian distribution with zero mean of noises at D and E stations.

The secrecy rate of this system model formulated as:

$$R_S = log(1 + SNR_d) - log(1 + SNR_e)$$
$$R_S = log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{\text{rd,m}}\, w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{\text{re,m}}\, w_m\right|^2}\right) \quad (2)$$

The maximizing problem of secrecy rate with the constraints on power of each relay is:

$$\max_{w} log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{\text{rd,m}}\, w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{\text{re,m}}\, w_m\right|^2}\right) \quad (3)$$
$$s.t. |w_m|^2 \leqslant p_m, \forall m = 1 \ldots M.$$

By

- $\boldsymbol{H}_d = \boldsymbol{h}_{rd}\boldsymbol{h}_{rd}^\dagger; \boldsymbol{h}_{rd} = [h_{rd,1}, h_{rd,2}, \ldots, h_{rd,M},]^\dagger,$
- $\boldsymbol{H}_{\text{re}} = \boldsymbol{h}_{\text{re}}\boldsymbol{h}_{\text{re}}^\dagger; \boldsymbol{h}_{\text{re}} = [h_{\text{re},1}, h_{\text{re},2}, \ldots, h_{\text{re},M},]^\dagger.$

The problem (3) is equivalent to

$$\max_{w} \frac{\sigma^2 + \boldsymbol{w}^{\dagger}\boldsymbol{H}_d\boldsymbol{w}}{\sigma^2 + \boldsymbol{w}^{\dagger}\boldsymbol{H}_e\boldsymbol{w}} \quad (4)$$
$$s.t. |w_m|^2 \leqslant p_m, \forall m = 1 \dots M.$$

The secrecy rate maximization problem (4) above is a non-convex programming then it might be difficult for solving to find global solution.

III. THE RECENT APPROACHES AND A PROPOSAL

A. Semi-Definite Relaxation technique

In [7], the authors dial problem 0 by reformulated to Semi-Definite Programming (SDP) as:

$$\begin{gathered} \max_{w,t} t \\ s.t. diag(\boldsymbol{W}) \leqslant p_m \\ Rank(\boldsymbol{W}) = 1 \\ \boldsymbol{W} \succcurlyeq 0 \\ trace\big(\boldsymbol{W}(\boldsymbol{H}_{\mathrm{d}} - t\boldsymbol{H}_{\mathrm{e}})\big) \geqslant \sigma^2(t-1). \end{gathered} \quad (5)$$

Where:

- $\boldsymbol{W} = \boldsymbol{w}\boldsymbol{w}^{\dagger}$,

- $trace(\boldsymbol{A})$ is trace of matrix $\boldsymbol{A}$,

- $diag(\boldsymbol{W})$ is the diagonal vector of matrix $\boldsymbol{W}$,

- $\boldsymbol{W} \succcurlyeq 0$ means $\boldsymbol{W}$ is symmetric positive semi-definite matrix.

Then apply Semi-Definite Relaxation (SDR) method by considering relaxation on rank one symmetric positive semi-definite constraint. The optimization program above (5) has all objective function and constraints that are convex so it can be solve as a convex optimization problem.

B. DCA method to solve the problem

In [8], we proposed DC (Difference of Convex functions) programming and DCA (DC Algorithm) method to address the problem above by reformulated problem (4) to:

$$\begin{gathered} \min_{x,t} 0 - \frac{\sigma^2 + \boldsymbol{x}^T\boldsymbol{H}\boldsymbol{x}}{t} \\ s.t. |x_m|^2 \leqslant p_m \\ \boldsymbol{x}_m = [x_m, x_{M+m}]^T, \forall m = 1 \dots M \\ \sigma^2 + \boldsymbol{x}^T\boldsymbol{Z}\boldsymbol{x} \leqslant t \end{gathered} \quad (6)$$

Where:

- $\boldsymbol{H} = \begin{bmatrix} \mathrm{Re}(\boldsymbol{H}_d) & -\mathrm{Im}(\boldsymbol{H}_d) \\ \mathrm{Im}(\boldsymbol{H}_d) & \mathrm{Re}(\boldsymbol{H}_d) \end{bmatrix}$,

- $\boldsymbol{Z} = \begin{bmatrix} \mathrm{Re}(\boldsymbol{H}_e) & -\mathrm{Im}(\boldsymbol{H}_e) \\ \mathrm{Im}(\boldsymbol{H}_e) & \mathrm{Re}(\boldsymbol{H}_e) \end{bmatrix}$,

- $\boldsymbol{x} = [\mathrm{Re}(\boldsymbol{w}^T)\mathrm{Im}(\boldsymbol{w}^T)]$.

In problem (6), the objective function has form of DC as $f(\boldsymbol{x}, t) = g(\boldsymbol{x}, t) - h(\boldsymbol{x}, t)$, with $g(\boldsymbol{x}, t) = 0$ and $h(\boldsymbol{x}, t) = \frac{\sigma^2 + \boldsymbol{x}^T\boldsymbol{H}\boldsymbol{x}}{t}$.

Following the DC programming and DCA method applied to problem (6) has DCA-DF scheme as below,

INPUT: $\boldsymbol{H}, \boldsymbol{Z}, \sigma$

INITIALIZE: SET $\boldsymbol{u}^0 = (\boldsymbol{x}^0, t^0), t_{count} \leftarrow 0, \varepsilon = 10^{-5}, l \leftarrow 0$

REPEAT:

CALCULATE: $\boldsymbol{u}^{l+1} = (\boldsymbol{x}^{l+1}, t^{l+1})$ by solving

$$\min_{x,t} \frac{\sigma^2 + (\boldsymbol{x}^l)^T\boldsymbol{H}(\boldsymbol{x}^l)}{(t^l)^2}(t - t^l) - \frac{2\boldsymbol{H}\boldsymbol{x}^l}{t^l}(\boldsymbol{x} - \boldsymbol{x}^l)$$
$$s.t. |x_m|^2 \leqslant p_m$$
$$\boldsymbol{x}_m = [x_m, x_{M+m}]^T, \forall m = 1 \dots M$$
$$\sigma^2 + \boldsymbol{x}^T\boldsymbol{Z}\boldsymbol{x} \leqslant t$$

INCREMENT: $l \leftarrow l + 1$

UNTIL:

$$\frac{\|\boldsymbol{u}^{l+1} - \boldsymbol{u}^l\|}{1 + \|\boldsymbol{u}^l\|} < \varepsilon \text{ or } \frac{|h(\boldsymbol{u}^{l+1}) - h(\boldsymbol{u}^l)|}{1 + |h(\boldsymbol{u}^l)|} < \varepsilon;\ \boldsymbol{u}^l = (\boldsymbol{x}^l, t^l)$$

OUTPUT: $R_s = log_2 h(\boldsymbol{u});\ t_{count}$.

C. Propose initial points.

The PLS problems in wireless networks focus on both the secrecy rate value and the timing cost of problems. The timing cost for solving PLS problems plays an important role to apply it in real application.

As with DC programming and DCA method [9], finding a good initial point for each problem is an open challenge, it relates to the convergence and running time of DCA algorithm. In [8], we studied problem DCA-DF with random initial point ($\boldsymbol{x}^0 = rand(2 * M, 1)$).

In this paper, we propose three initial points for the DCA-DF problem above. Two of them come from the idea that the solution of PLS problems is strongly related to the channel gains of legitimate users and eavesdroppers, so we propose two initial points: the eigen values of $\boldsymbol{H}$ and $\boldsymbol{Z}$, which are:

- IniP_1: The eigenvalues of channel gains matrix $\boldsymbol{H}$ from relays to D ($\boldsymbol{x}^0 = eig(\boldsymbol{H})$);

- IniP_2: The eigenvalues of channel gains matrix $\boldsymbol{Z}$ from relays to E ($\boldsymbol{x}^0 = eig(\boldsymbol{Z})$);

- IniP_3: The solution to problem (4) in the case of total relays power (P_T) constraint is considered. In this case, the problem (4) and becomes to:

$$\max_{w} \frac{\sigma^2 + \boldsymbol{w}^\dagger \boldsymbol{H}_d \boldsymbol{w}}{\sigma^2 + \boldsymbol{w}^\dagger \boldsymbol{H}_e \boldsymbol{w}} \quad s.t. \boldsymbol{w}^\dagger \boldsymbol{w} \leqslant P_T. \tag{7}$$

The problem (7) can reformulated as:

$$\begin{aligned} &\max_{w^\dagger w = P_T} \frac{\sigma^2 + \boldsymbol{w}^\dagger \boldsymbol{H}_d \boldsymbol{w}}{\sigma^2 + \boldsymbol{w}^\dagger \boldsymbol{H}_e \boldsymbol{w}} \\ &= \max_{w^\dagger w = P_T} \frac{\boldsymbol{w}^\dagger \left(\sigma^2 \left(\frac{\boldsymbol{I}}{P_T}\right) + \boldsymbol{H}_d\right) \boldsymbol{w}}{\boldsymbol{w}^\dagger \left(\sigma^2 \left(\frac{\boldsymbol{I}}{P_T}\right) + \boldsymbol{H}_e\right) \boldsymbol{w}} \\ &= \lambda_{max}\left(\sigma^2 \left(\frac{\boldsymbol{I}}{P_T}\right) + \boldsymbol{H}_d, \sigma^2 \left(\frac{\boldsymbol{I}}{P_T}\right) + \boldsymbol{H}_e\right) \end{aligned} \tag{8}$$

In which: $\lambda_{max}(\boldsymbol{A}, \boldsymbol{B})$ is the largest generalized eigenvalue of the pair of matrix $\boldsymbol{A}$ and $\boldsymbol{B}$. And $\boldsymbol{I}$ is an identity/unit matrix with dimension 2*M. The problem (8) is completely solved [7] so we propose to use this solution as the initial point of DCA-DF problem.

The experiments and results will show that the DCA-DF scheme has different number of iterations and different running time in each iteration due to these initial points.

IV. Experiments and results

A. Experimental setups

We implemented experimental in a PC Intel ® core i3-6100 CPU @ 3.7Ghz 3.7 Ghz, 4.0 GB RAM with Matlab R2017 and CVX tools.

The channel coefficients gain $\boldsymbol{h}_{rd}$ and $\boldsymbol{h}_{\mathrm{re}}$ are assumed to be complex, circularly symmetric Gaussian random variables with zero mean and variances ${\sigma_d}^2$ and ${\sigma_e}^2$, respectively.

$\boldsymbol{h}_{\mathrm{rd}} = \sigma_d/\sqrt{(2)} + \left(\mathrm{rand}(M,1) + 1i * \mathrm{rand}(M,1)\right)$,

$\boldsymbol{h}_{\mathrm{re}} = \sigma_e/\sqrt{(2)} + \left(\mathrm{rand}(M,1) + 1i * \mathrm{rand}(M,1)\right)$.

In these tests, we assume that the channel gain of both legitimate users and eavesdroppers has the same quality (${\sigma_d}^2 = {\sigma_e}^2 = 2$). We perform on two cases of numbers of relays in model system, those are $M = 5$ and $M = 10$. It is also assumed that the relays have equal power budget ($p_m = \frac{P_T}{M} \forall m$).

B. Numerical results

We test DCA-DF algorithm with four cases of initial points, these are the random and proposed initial points. All experiments are done with 100 independent Rayleigh fading channel realizations. The average secrecy rates and runtimes of both algorithms obtained are recorded.

TABLE I. R_s VS $M = 5$

P_T (mW)	R_s (bits/symbol)				
	DCA-DF				SDR-DF
	Rand	IniP_1	IniP_2	IniP_3	
20	7.732	7.732	7.731	7.729	6.595
40	8.727	7.727	8.719	8.723	7.569
60	9.310	9.310	9.299	9.299	8.146
80	9.724	9.724	9.719	9.721	8.556
100	10.045	10.046	10.039	10.043	8.875

TABLE II. R_S VS $M = 10$

P_T (mW)	R_s (bits/symbol)				
	DCA-DF				SDR-DF
	Rand	IniP_1	IniP_2	IniP_3	
20	8.948	8.948	8.948	8.990	7.998
40	9.946	9.946	9.946	9.988	8.994
60	10.530	10.530	10.530	10.572	9.578
80	10.945	10.945	10.945	10.987	9.992
100	11.267	11.267	11.267	11.309	10.314

In term of the secrecy rate, it can be seen from TABLE I. and Table II that between four cases of initial points for DCA-DF scheme have no change about secrecy rate values. It also means that the initial points have no effect on the value of the objective function of DCA problems. Compared to SDR method, the secrecy rate values from DCA-DF are clearly higher than SDR-DF secrecy values.

The optimal values of secrecy rate obtained by both algorithms in all cases show an increasing trend as the ratio of total power constraint (P_T).

TABLE III. THE RUNNING TIME VS $M = 5$

P_T (mW)	*The running time (seconds)*				
	DCA-DF				***SDR-DF***
	Rand	*IniP_1*	*IniP_2*	*IniP_3*	
20	2.273	**1.863**	**1.768**	2.559	9.358
40	2.276	**1.575**	**1.594**	2.266	9.117
60	2.270	**1.578**	**1.592**	2.195	9.175
80	2.141	**1.609**	**1.544**	2.840	9.267
100	2.221	**1.652**	**1.537**	2.959	9.481

TABLE IV. THE RUNNING TIME VS $M = 10$

P_T (mW)	*The running time (seconds)*				
	DCA-DF				***SDR-DF***
	Rand	*IniP_1*	*IniP_2*	*IniP_3*	
20	3.217	**2.178**	**2.179**	3.051	10.424
40	3.016	**2.176**	**2.006**	3.036	9.598
60	2.981	**2.112**	**2.002**	3.049	9.469
80	2.951	**2.196**	**2.015**	3.071	9.511
100	2.922	**2.144**	**2.014**	3.009	9.626

Concerning the running time, the Table III and Table IV show that DCA-DF algorithm with proposal initial points IniP_1 and IniP_2 is the best in all cases. The proposal initial point IniP_3 and the random initial point have a similar value. More specifically, the gaps between the running times obtained by DCA-DF and SDR-DF algorithms are significant.

TABLE V. THE NUMBER OF ITERATION VS $M = 5$

P_T (mW)	*The number of iterations*			
	DCA-DF			
	Rand	*IniP_1*	*IniP_2*	*IniP_3*
20	3.230	**2.343**	**2.485**	3.471
40	3.11	**2.285**	**2.371**	3.243
60	3.080	**2.257**	**2.328**	3.143
80	3.020	**2.243**	**2.300**	3.043
100	3.020	**2.228**	**2.287**	3

TABLE VI. THE NUMBER OF ITERATION VS $M = 10$

P_T (mW)	*The number of iterations*			
	DCA-DF			
	Rand	*IniP_1*	*IniP_2*	*IniP_3*
20	2.91	**2.05**	**2.01**	3.01
40	2.85	**2.01**	**1.99**	2.99
60	2.79	**1.99**	**1.99**	2.97
80	2.77	**1.99**	**1.98**	2.97
100	2.72	**1.99**	**1.98**	2.91

More specifically, in terms of the number of iterations for DCA-DF scheme in each initial point, the TABLE V. and Table IV show that two proposal initial points IniP_1 and IniP_2 make DCA-DF scheme have less number iterations in average than two others in both cases of number of relays. The IniP_3, solution of DCA-DF problem in total power relays is considered with the hope that it will near the solution of DCA-DF but have nearly the same iterations and runtimes with the random initial point case.

All things considered, it seems reasonable to say that the proposed IniP_1 and IniP_2 are two good initial points of DCA-DF scheme in terms of running time.

IV. CONCLUSION

PLS has been considered an alternative approach to securing future wireless communication systems. In which, Decode-and-Forward and Amplify-and-Forward relaying technique and those problems are openning researched. Some of previous research has shown that PLS problems can be solved efficiently by DC programming and DCA method.

In this paper, we have reviewed Decode-and-Forward relaying wireless networks and those problems in PLS. To deal with one of major problems to apply PLS in real applications, which is the timing cost of solving PLS problems, we proposed two specific initial points for DCA-DF algorithms, which are IniP_1 and IniP_2.

The experimental performances reveal the efficiency of the proposed initial points for DCA-DF scheme in terms of running time.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The Wire-Tap Channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x

[3] Tuan, N.N., Son, D.V.: DC programming and DCA for Enhancing physical layer security in amplify-and-forward relay beamforming networks based on the SNR approach. In: Le, N.-T., Van Do, T., Nguyen, N.T., Thi, H.A.L. (eds.) *ICCSAMA 2017. AISC (Advances in Intelligent Systems and Computing)*, vol. 629, pp. 23–33. Springer, Cham. 2018.

[4] Nhu Tuan Nguyen, Decode-and-Forward vs. Amplify-and-Forward Scheme in Physical Layer Security for Wireless Relay Beamforming Networks. *Journal of Science and Technology on Information Security*. ISSN 2615-9570, Vol. 10, No. 2, pp. 9-17, 2019.

[5] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2734–2771, 2019, doi: 10.1109/COMST.2018.2865607.

[6] D. Wang, B. Bai, W. Zhao, and Z. Han, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *ArXiv190107955 Cs Math*, Jan. 2019.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010, doi: 10.1109/TSP.2009.2038412.

[8] Thuy, T.T., Tuan, N.N., An, L.T.H., Gély, A.: DC programming and DCA for enhancing physical layer security via relay beamforming strategies. In: Nguyen, N.T., Trawiński, B., Fujita, H., Hong, T.-P. (eds.) *ACIIDS 2016. LNCS (LNAI)*, vol. 9622, pp. 640–650. *Springer, Heidelberg* (2016).

[9] Le Thi, H.A., Pham, D.T.: The DC (Difference of convex functions) programming and DCA revisited with DC models of real world nonconvex optimization problems. Ann. Oper. Res. 133, 23–46 (2005).

ABOUT THE AUTHOR

Name: Nguyen Nhu Tuan

Workplace: Vietnam Information Security Journal

Email: nhuwtuaans@gmail.com

website: antoanthongtin.vn; isj.vn.

Education: He received Bachelor degree of Engineering in Academy of Cryptography Techniques in 2000, Master degree in 2007 and PhD degree in 2022.

Recent research direction: Machine learning and data mining in cyber security; Cloud computing security; Physical layer security.