Decode-and-Forward vs. Amplify-and-Forward Scheme in Physical Layer Security for Wireless Relay Beamforming Networks

Nhu Tuan Nguyen

***Abstract*— To secure communication from the sender to the receiver in wireless networks, cryptographic algorithms are usually used to encrypt data at the upper layers of a multi-tiered transmission model. Another emerging trend in the security of data transmitted over wireless networks is the physical layer security based on beamforming and interference fading communication technology and not using cryptographic algorithms. This trend has attracted increasing concerns from both academia and industry. This paper addresses how physical layer security can protect secret data compare with the traditional cryptographic encryption and which is the better cooperative relaying scheme with the state of the art approached methods in wireless relaying beamforming network.**

***Tóm tắt*— Việc bảo mật truyền thông vô tuyến từ nơi gửi đến nơi nhận thường sử dụng các thuật toán mật mã để mã hoá dữ liệu tại các tầng phía trên trong mô hình phân lớp. Một xu hướng khác đang được quan tâm rộng rãi là bảo mật tầng vật lý dựa trên kỹ thuật truyền tin beamforming và kỹ thuật tương tác fading kênh chủ động. Xu hướng này hiện đang được thu hút cả trong giới công nghiệp và nghiên cứu. Đóng góp của bài báo này là làm rõ khả năng bảo mật tầng vật lý và so sách chúng với phương pháp bảo mật dùng kỹ thuật mật mã truyền thống. Bài báo cũng so sánh hai kỹ thuật chuyển tiếp được sử dụng chính trong bảo mật tầng vật lý cho mạng vô tuyến chuyển tiếp là Amplify-and-Forward và Decode-and-Forward.**

***Keywords*— Physical layer security; DC Programming and DCA; Amplify-and-Forward.**

***Từ khoá*— Bảo mật tầng vật lý; DC Programming and DCA; Amplify-and-Forward.**

This manuscript is received on July 18, 2019. It is commented on November 20, 2019 and is accepted on November 30, 2019 by the first reviewer. It is commented on December 15, 2019 and is accepted on December 25, 2019 by the second reviewer.

I. INTRODUCTION

Most of the recent methods of ensuring security in the communication system are based on cryptography techniques or algorithms to encrypt the content of the messages from the sender to the receiver. 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. It was proposed therein that the approach termed "one-time pad" could achieve the perfect secrecy. The traditional communication security methods often use cryptographic algorithms at the upper layers of multi-layer communication models being studied and widely applied. Recently, these methods have still been considered to be safe in many application models. However, the security of these cryptographic algorithms often depends on the computational complexity of decryption without private keys. Therefore, when quantum computers are actually applied, this difficulty will no longer be a challenge in crypto analysis.

Another trend for radio network security that has been extensively researched lately is physical layer security (PLS) without the use of cryptographic algorithms and resistance to quantum computers. In the recent years, PLS has been investigated both as an alternative and as a complementary approach to conventional cryptographic methods [2,3]. Actually, the research on physical layer security was pioneered by Dr. Aaron D. Wyner since 1975 [4]. Wyner has demonstrated that it is possible to transmit security information at C_s rate in a communication system that has the presence of an eavesdropper ($C_s \geq 0$). That is the secrecy capacity of a discrete memoryless channel was the maximum value of the difference between the mutual information of the legitimate channel and the mutual information of the

wiretap channel. At that time, Wyner made an important assumption in his results that the channel between Alice and Eve, called the wire-tap channel, had a greater loss than the channel from Alice to the legal recipient Bob, also known as the main channel. This assumption is not easy to guarantee because the wire-tap channel is often unchecked. Hence, the Wyner's idea was not really interested in the following years.

Over the past decade, with the development of wireless communications technology, especially multi-antenna communications and beamforming techniques, physical layer security solutions have been studied widely [5,9]. A great effort to increase the achievable secrecy rate in physical layer security is cooperative nodes networks [3, 9] with act two roles are cooperative relaying and cooperative jamming (CJ) [10, 12]. In which, the secrecy rate value is defined as

$$R_s = \min_{j=1,K}(\log(1+SNR_d) - \log(1+SNR_{ej})). \quad (1)$$

Where, SNR_d and SNR_{ej} are the signal-to-noise-ratio at the legitimate destination and the j^{th} eavesdropper, respectively; K is the number of eavesdroppers in system.

This paper focused on the cooperative relaying network with two main relaying schemes are Amplify-and-Forward (AF) and Decode-and-Forward (DF). This paper presents the state-of-the-art cooperative relaying networks and the experiments to show detail the effects of some techniques and schemes in it. These wireless relay beamforming networks are modeled as nonconvex optimization problems. In which, the solution of these optimization problem are the beamforming weights of the relay stations, the objective function is the value of the secrecy rate of the system R_s (bits/symbol).

We investigate in the case of having perfect channel state information (CSI) in both legitimate destination and eavesdropper. In fact, the eavesdroppers may exist in the system as the legitimate users are registered in the system, they may misbehave and eavesdrop the secret signal of other legitimate receivers when they are idle. Thus, idle legitimate receivers are potential eavesdroppers.

The rest of paper is organized as follows: Section II presents about the traditional cryptographic encryption and physical layer security; Section III presents the models and problems of wireless relaying network with AF and DF scheme; Section IV introduces some recent approaches with problems above; Section IV is the experimental result and The last one is the conclusion section.

Notations: Throughout this paper, the uppercase letters are denoted for the matrices; The lowercase letters indicate the column vector; The symbols $(.)^*$, $(.)^T$, $(.)^\dagger$ are used for Conjugate, Transpose and Conjugate transpose, respectively; $\boldsymbol{I}_M$ is Identity/unit matrix with dimension M; $diag\{\boldsymbol{a}\}$ or $\boldsymbol{D}(\boldsymbol{a})$ is denoted for Diagonal matrix with elements on the diagonal is the value of the vector $\boldsymbol{a}$; $\|\boldsymbol{a}\|$ is denoted for 2-norm of vector $\boldsymbol{a}$; $E\{.\}$ is denoted for Expectation; $\boldsymbol{A} \succcurlyeq 0$ is denoted for matrix $\boldsymbol{A}$ 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; $trace(\boldsymbol{A})$ is a trace of matrix $\boldsymbol{A}$.

II. CRYPTOGRAPHIC ENCRYPTION AND PHYSICAL LAYER SECURITY

Recent advances in wireless technologies, such as the long-term evolution for cellular networks and Wi-Fi systems, have caused an exponential growth in the number of connected devices [13] which in turn entails the risk of increasing security threats. Through cryptographic approaches, data security has been traditionally addressed at the higher layers of the open system's interconnected model, whereby the plain text message is encrypted by using a powerful algorithm that assumes limited computational capacity of potential eavesdroppers [14]. However, due to current enhancements in computational power of devices and optimization strategies for breaking encryption codes, there is a need for better security strategies to protect information from unauthorized devices. Another drawback of the conventional cryptographic schemes is the requirement for key management to exchange the secret key between legitimate entities. Key sharing requires a trusted entity which cannot always be ensured in distributed wireless networks.

TABLE 1: SOME QUALITY OF PHYSICAL LAYER SECURITY COMPARE TO CRYPTOGRAPHIC ENCRYPTION [3, 15]

	Cryptographic encryption	**Physical layer security**
Theoretical basis	Cryptography	Information theory
Secrecy level	Can be deciphered by brute-force computing, under the computational model, measured by whether it survives a set of attacks or not	Achieving perfect secrecy, No computation restrictions placed on eavesdropper
Computing ability requirements	Heavily relying on the computing ability	Being independent of computing ability
Key management	Heavy costs resulting from key generation, management, and distribution; No publicly-know, efficient attacks on public-key systems	With no need of any key; Quantum key distribution implemented
Evaluation criterion	Being unable to accurately assess the leakage of confidential information	Evaluating secrecy precisely by equivocation rate that may not be accurate in practice
Adaptability to channel changes	Poor channel adaptability	Adjusting transmission strategies and parameters to well adapt the channel changes
Deployed	Systems are widely deployed, technology is readily available, inexpensive	Wireless solutions appear, a few systems are deployed but the technology is not as widely available and can be expensive

On the other hand, the lower layers (physical and data link layers) are oblivious of any security consideration. Considering the recent challenges, security must be considered on the physical layer to increase the robustness. of existing schemes [3, 8, 11].

The authors in [3] and [15] have shown some differences between cryptographic encryption and physical layer security from six viewpoints as in Table 1. Although the PLS not really widely used in industry and the technology is not as widely available but this comparison made PLS would be interested in many researchers.

III. SYSTEM MODELS AND PROBLEMS

As all the source and the relays located in a trusted zone, then distance between them are quite close, the relays can receive signal properly, and the power of the signal broadcasted by the source would be small so that the faraway destination and eavesdroppers can receive none of it.

A. AF system model and problem

The system includes a source (S), a destination (D), M trusted relays stations and K eavesdroppers, as shown in Fig.1. In this system, we assume that there is no any direct transmission from the source to the destination or to the eavesdroppers.

The channel gain from the relays to D is denoted by the complex constants h_{rd}, and from the relays to eavesdroppers denoted by h_{re}.

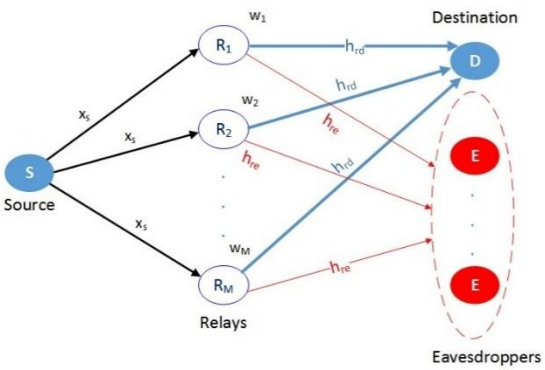

Fig.1. A wireless relay network with multiple eavesdroppers

In the AF cooperate scheme, M trusted relays forward to the destination the signal that they received from the source. The received SNR values at D and E as follow:

$$SNR_d = \frac{\left|\sum_{i=1}^{M} h_{si} w_i h_{id}\right|^2}{1+\sum_{i=1}^{M}\left|w_i h_{id}\right|^2}\frac{P_s}{\sigma^2} \quad (2)$$

$$SNR_l = \frac{\left|\sum_{i=1}^{M} h_{si} w_i h_{il}\right|^2}{1+\sum_{i=1}^{M}\left|w_i h_{il}\right|^2}\frac{P_s}{\sigma^2}, \; l = 1,2,\ldots\kappa.$$

We consider the maximizing the received SNR achievable at the destination when the received SNR at the eavesdroppers are below their respective predefined thresholds problem as [16, 17].

$$\max_{\boldsymbol{w}} \frac{\left|\sum_{i=1}^{M} h_{si} w_i h_{id}\right|^2}{1+\sum_{i=1}^{M}|w_i h_{id}|^2}\frac{P_s}{\sigma^2} \quad (3)$$

$$s.t.\frac{\left|\sum_{i=1}^{M} h_{si} w_i h_{il}\right|^2}{1+\sum_{i=1}^{M}|w_i h_{il}|^2}\frac{P_s}{\sigma^2} \le \gamma_l; l \in \kappa,$$

$$|w|^2 \le w_{max,i}^2, i \in M.$$

Where, γ_l is a real number and represent the predefined threshold for the l^{th} eavesdropper; h_{id} is the channel gain from i^{th} relay to the destination node; h_{il} is the channel gain of i^{th} relay and l^{th} eavesdropper node; $\mathbf{w} = \{w_1, w_2, ..., w_M\}^T$ are weight factors (beamforming) of relays; The background noise at the relays, destination and eavesdroppers have Gaussian distribution with zero mean and variance σ^2; P_s is transmission power of the source node.

B. DF system model and problem

The DF system model has the same structure as AF system, which includes a source (S), a destination (D), M trusted relays stations and K eavesdroppers, as in Fig. 1. In this system, we also assume that there is no any direct transmission from the source to the destination or to the eavesdroppers. The channel gain from the relays to D and eavesdroppers denoted by the complex constant h_{rd} and h_{re}, respectively.

In the DF cooperate scheme, all the trusted relays decode the message from source then re-encode the message and cooperatively transmit the re-encoded symbols to the destination. The received SNR at D and at j^{th} E are

$$SNR_d = \frac{\left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2} \quad (4)$$

$$SNR_{e_j} = \frac{\left|\sum_{m=1}^{M} h_{re_j,m} w_m\right|^2}{\sigma^2}, j = 1, \dots, K.$$

As (1) and (4), the optimization problem of DF system model formulated as following [18]

$$\max_{w} \min_{j=1,\dots,K} \log \frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{re_j,m} w_m\right|^2} \quad (5)$$

$$\text{s.t. } \mathbf{w}^{\dagger}\mathrm{w} \le P_R,$$

$$(\text{or } |w_m|^2 \le p_m, \forall m = 1, \dots, M).$$

Where $\mathbf{w} = \{w_1, w_2, ..., w_M\}^T$ are weight factors (beamforming weight) of relays; σ^2 is the variance of the Gaussian background noise at relays, destination and eavesdroppers; P_R is limit total power relays, p_m is limit power of m^{th} relay.

IV. THE RECENT APPROARCHES

A. The approaches for AF problem

1) SubOpt Solution

The authors in [17] introduce a SDR (Semi-Definite Relaxation) method following transformations as

Set variables

$$v_i = w_i h_{id} \text{ and } u_i = \frac{v_i}{\sqrt{1+\boldsymbol{v}^{\dagger}\boldsymbol{v}}}.$$

If we consider the vector variables $\boldsymbol{u} = [u_1, u_2, \dots, u_M]^T$ and $\boldsymbol{v} = [v_1, v_2, \dots, v_M]^T$, then we can write

$$\boldsymbol{u} = \frac{\boldsymbol{v}}{\sqrt{1+\boldsymbol{v}^{\dagger}\boldsymbol{v}}} \Leftrightarrow \boldsymbol{v} = \frac{\boldsymbol{u}}{\sqrt{1-\boldsymbol{u}^{\dagger}\boldsymbol{u}}}.$$

In terms of these new variables and parameters, the problem (3) can be rewritten as:

$$\begin{aligned} &\min_{\boldsymbol{u}} -\boldsymbol{u}^{\dagger}\boldsymbol{h}_s\boldsymbol{h}_s{}^{\dagger}\boldsymbol{u} \\ &st.\boldsymbol{u}^{\dagger}\boldsymbol{C}_k\boldsymbol{u} \le 1, k \in \kappa \\ &\boldsymbol{u}^{\dagger}\boldsymbol{D}_i\boldsymbol{u} \le 1,\ i \in M, \end{aligned} \quad (6)$$

where:

$$\boldsymbol{\rho}_k = \left[\rho_{1,k}, ..., \rho_{M,k}\right], \text{ and } \rho_{i,k} = \left|\frac{h_{ik}}{h_{id}}\right|$$

$$\boldsymbol{h}_s = \left[h_{s,1}, ..., h_{s,M}\right]^{\dagger}$$

$$\boldsymbol{D}_{\rho,k} = diag\left(\left|\rho_k\right|^2\right), \quad \gamma_k{}' = \gamma_k \frac{\sigma^2}{P_s}, \forall k \in \kappa;$$

$$\boldsymbol{C}_k = \frac{\boldsymbol{h}_{s\rho,k}\boldsymbol{h}_{s\rho,k}^{\dagger}}{\gamma_k{}'} + \boldsymbol{I} - \boldsymbol{D}_{\rho,k}$$

when

$$\boldsymbol{h}_{s\rho,k} = \left[h_{s,1}\rho_{1,k}, h_{s,2}\rho_{2,k}, ..., h_{s,M}\rho_{M,k}\right]^{\dagger}$$

$$(\mathbf{D}_i)_{jk} = \begin{cases} 1 + \frac{1}{|h_{i,d}|^2 \beta_{i,\max}^2}, \text{ if } \quad k = j = i \\ 1, \text{if} \qquad k = j \neq i \\ 0, \text{otherwise} \end{cases}$$

As the objective function of problem (6) is nonconvex and the constraints could be convex or not, if $\rho_{i,k} = \left|\frac{h_{ik}}{h_{id}}\right| \leq 1, \forall i,k$ then $\mathbf{I} - \mathbf{D}_{\rho,k}$ is diagonal matrix with positive entries, therefor, $\mathbf{C}_k$ is a positive definite matrix so all the constraints are convex. But, in general scenarios, $\mathbf{C}_k$ may not be positive-semidefinite the K first constraints are nonconvex. Therefore, the problem (6) is hard to get the optimal solution in general.

Recalled that the problem (6) has form of Quadratically Constrained Quadratic Program (QCQP) with nonconvex objective function and nonconvex constraints. It is difficult to find the global optimal solution of that problem by solving directly in general. The existing method proposed in [18] is to find suboptimal solution by Semi-definite Relaxation (SDR) method as following.

By defined $\mathrm{U} = \mathrm{uu}^{\dagger}$ and considering relaxation on rank one symmetric positive semi-definite (PSD) constraint (rank(U) = 1), the optimization program (6) can be written as

$$\begin{aligned} &\max_{\boldsymbol{U}} \ trace\left(\boldsymbol{h}_s \boldsymbol{h}_s^{\dagger} * \boldsymbol{U}\right) \\ &s.t. \ trace(\boldsymbol{C}_k * \boldsymbol{U}) \leq 1, k \in \kappa \\ &trace(\boldsymbol{D}_i * \boldsymbol{U}) \leq 1, i \in M \end{aligned} \tag{7}$$

As the objective function and all constraints in (7) are convex, this problem can be solved by CVX optimization tool. Once problem (7) is solved, we can find the corresponding optimal **u** and thereby **w** by applying eigenvalue decompression on matrix **U**.

2) DC programming and DCA Solution

In [16], we proposed to apply DC programming and DCA to solve the problem (6). By define

$$\rho_k^+ = \begin{cases} 1 - |\rho_{i,k}|^2, if |\rho_{i,k}| \leq 1 \\ 0, else \end{cases}$$

$$\rho_k^- = \begin{cases} |\rho_{i,k}|^2 - 1, if |\rho_{i,k}| \geq 1 \\ 0, else \end{cases}$$

The problem (6) can be rewritten as

$$\begin{aligned} &\min_{\boldsymbol{u}} \quad 0 - \boldsymbol{u}^{\dagger} \boldsymbol{H}_s \boldsymbol{u} \\ &s.t. \boldsymbol{u}^{\dagger} \boldsymbol{C}_k^{+} \boldsymbol{u} - \boldsymbol{u}^{\dagger} \boldsymbol{C}_k^{-} \boldsymbol{u} \leq 1, \forall k \in \kappa, \\ &\boldsymbol{u}^{\dagger} \boldsymbol{D}_i \boldsymbol{u} \leq 1, \forall i \in M. \end{aligned} \tag{8}$$

Where

$$\boldsymbol{H}_s = \boldsymbol{h}_s \boldsymbol{h}_s^{\dagger}; \boldsymbol{C}_k^{+} = \frac{\boldsymbol{h}_{sp,k} \boldsymbol{h}_{sp,k}^{\dagger}}{\boldsymbol{\gamma}_k'} + diag(\boldsymbol{\rho}_k^{+})$$

and $\boldsymbol{C}_k^{-} = diag(\boldsymbol{\rho}_k^{-})$.

Convert to real form, the problem (8) reformulate as following

$$\begin{aligned} &\min_{\mathbf{x},t} \quad 0 - \frac{\sigma^2 + \mathbf{x}^T \mathbf{Z} \mathbf{x}}{t} \\ &s.t. \ \mathbf{x}^T \mathbf{B}_j \mathbf{x} \leq t - \sigma^2, \forall j \in K \\ &\quad \mathbf{x}^T \mathbf{x} \leq P_R, t > 0. \end{aligned} \tag{9}$$

Where:

$$\mathbf{Z} = \begin{bmatrix} Re(\mathbf{R}_{rd}) & -Im(\mathbf{R}_{rd}) \\ Im(\mathbf{R}_{rd}) & Re(\mathbf{R}_{rd}) \end{bmatrix}, \quad x = \begin{bmatrix} Re(\mathbf{w}) \\ Im(\mathbf{w}) \end{bmatrix}$$

$$\mathbf{B}_j = \begin{bmatrix} \mathrm{Re}(\mathbf{R}_{re,j}) - \mathrm{Im}(\mathbf{R}_{re,j}) \\ \mathrm{Im}(\mathbf{R}_{re,j}) \mathrm{Re}(\mathbf{R}_{re,j}) \end{bmatrix}^T.$$

The problem (9) is actually a general DC program at the objective function and first K constrains [19], then we proposed DCA-AFME scheme by applied DCA to solve this problem as the following.

DCA-AFME SCHEME

Input: Channel coefficients from source to relays $\boldsymbol{h}_s$, from relays to destination $\boldsymbol{h}_d$ and from relays to eavesdroppers $\boldsymbol{H}_{il}$, the predefined threshold γ.

Initialization. Chose a random initial point $\mathbf{x}^0$, *l=0*

Repeat: $l = l+1$, calculate $\mathbf{x}^l$ by solve this subproblem:

$$\min_{x,t} -(\boldsymbol{H}_s\boldsymbol{x}^{t-1})^\dagger\boldsymbol{x} + \tau t$$
$$s.t.\, \boldsymbol{x}^\dagger\boldsymbol{C}_k^+\boldsymbol{x} - 2(\boldsymbol{C}_k^-\boldsymbol{x}^{l-1})^\dagger\boldsymbol{x}\langle\boldsymbol{x} - \boldsymbol{x}^{l-1}, 2(\boldsymbol{C}_k^-\boldsymbol{x}^{l-1})\rangle\boldsymbol{x} \le 1 + (\boldsymbol{x}^{l-1})^\dagger\boldsymbol{C}_k^-\boldsymbol{x}^{l-1} + 2((\boldsymbol{x}^{l-1})^\dagger\boldsymbol{C}_k^-\boldsymbol{x}^{l-1}) + t, \forall k \in \kappa,$$
$$\boldsymbol{x}^\dagger\boldsymbol{D}_i\boldsymbol{x} \le 1, \forall i \in M, t \ge 0$$

Until:

$$\frac{\|\boldsymbol{x}^l - \boldsymbol{x}^{l-1}\|}{1+\|\boldsymbol{x}^{l-1}\|} \le \varepsilon \text{ or } \frac{|f(\boldsymbol{x}^l) - f(\boldsymbol{x}^{l-1})|}{1+|f(\boldsymbol{x}^{l-1})|} \le \varepsilon$$

where $f(\boldsymbol{x}^l) = (\boldsymbol{x}^l)^\dagger\boldsymbol{H}_s\boldsymbol{x}^l$

Output: $R_s = h(t^l, x^l)$, SNR_e, SNR_e (2).

B. The approaches for DF problem

Null steering

The authors in [9] focus on the case of Null steering beamforming. In which, the signal is completely nulled out at all eavesdroppers, then the problem (5) addition constraints

$$\mathbf{w}'\mathbf{h}_{re_j}\mathbf{w} = 0_{K\times 1}$$

and rewrite as

$$\max_{\boldsymbol{w}} \left(\log\left(\frac{\sigma^2 + \left|\sum_{m=1}^M h_{rd,m}w_m\right|^2}{\sigma^2}\right)\right)$$
$$\text{s.t. } \mathbf{w}^\dagger\mathbf{w} \le P_R \quad (10)$$
$$\mathbf{w}'\mathbf{h}_{re_j}\mathbf{w} = 0_{K\times 1}.$$

Then can be rewritten as

$$\max_{\boldsymbol{w}} \ \mathbf{w}'\mathbf{H}_{rd}\mathbf{w}$$
$$\text{s.t. } \mathbf{w}^\dagger\mathbf{w} \le P_R \quad (11)$$
$$\mathbf{w}'\mathbf{h}_{re_j}\mathbf{w} = 0_{K\times 1}.$$

Where

$\mathbf{H}_{rd} = \mathbf{h}'_{rd}\mathbf{h}_{rd}$ and $\mathbf{h}_{rd} = [h_{rd,1}, \dots, h_{rd,M}]^T$

By used the equality power constrain $w^\dagger w = P_R$ instead of inequality power constrain as

$$\max_{\mathbf{w}^\dagger\mathbf{w}=P_R} \ \mathbf{w}'\mathbf{H}_{rd}\mathbf{w}$$
$$\text{s.t. } \mathbf{w}'\mathbf{h}_{re_j}\mathbf{w} = 0_{K\times 1}. \quad (12)$$

The optimization problem (12) has the optimal solution given by

$$\boldsymbol{w} = \frac{\sqrt{P_R}}{\|(\mathbf{I}_M - \mathbf{P}_{re})\mathbf{h}_{rd}\|}(\mathbf{I}_M - \mathbf{P}_{re})\mathbf{h}_{rd},$$

where $\mathbf{P}_{re} = \mathbf{H}_{re}\left(\mathbf{H}_{re}^\dagger\mathbf{H}_{re}\right)^{-1}\mathbf{H}_{re}^\dagger$ is the orthogonal projection matrix onto the subspace spanned by the columns of $\boldsymbol{H}_{re}$.

3) DC programming and DCA approach

In [18], we proposed a DC decomposition by recall problem (5) with the total power constrain as

$$\max_{\boldsymbol{w}} \frac{\sigma^2 + \boldsymbol{w}^\dagger\boldsymbol{H}_{rd}\boldsymbol{w}}{max_{j=1..K}\left(\sigma^2 + \boldsymbol{w}^\dagger\boldsymbol{H}_{re,j}\boldsymbol{w}\right)} \quad (13)$$
$$s.t\ \boldsymbol{w}^\dagger\boldsymbol{w} \le P_R$$

equivalent to

$$\min_{\boldsymbol{w},t} -\frac{\sigma^2 + \boldsymbol{w}^\dagger\boldsymbol{H}_{rd}\boldsymbol{w}}{t}$$
$$\text{s.t. } \boldsymbol{w}^\dagger\boldsymbol{w} \le P_R, t > 0, \quad (14)$$
$$\sigma^2 + \boldsymbol{w}^\dagger\boldsymbol{H}_{re,j}\boldsymbol{w} \le t, \forall j \in K.$$

Change to real variables form we have an equivalent problem as

$$\min_{x,t}\ 0 - \frac{\sigma^2 + \boldsymbol{x}^T\boldsymbol{Z}\boldsymbol{x}}{t}$$
$$s.t.\, \boldsymbol{x}^T\boldsymbol{B}_j\boldsymbol{x} \le t - \sigma^2, \forall j \in K \quad (15)$$
$$\boldsymbol{x}^T\boldsymbol{x} \le P_R, t \ge 0$$

where

$$\boldsymbol{Z} = \begin{bmatrix} Re(\boldsymbol{H}_{rd}) & -Im(\boldsymbol{H}_{rd}) \\ Im(\boldsymbol{H}_{rd}) & Re(\boldsymbol{H}_{rd}) \end{bmatrix}, x = \begin{bmatrix} Re(\boldsymbol{w}) \\ Im(\boldsymbol{w}) \end{bmatrix}$$
$$\boldsymbol{B}_j = \begin{bmatrix} Re(\boldsymbol{H}_{re,j}) & -Im(\boldsymbol{H}_{re,j}) \\ Im(\boldsymbol{H}_{re,j}) & Re(\boldsymbol{H}_{re,j}) \end{bmatrix}^T.$$

The problem (15) is restated as a standard DC program, then we can apply DCA algorithm to have DCA-DFME scheme following:

The DCA-DFME scheme [18]**:**

Input: The channel coefficient matrix $\boldsymbol{B}_j$, $\boldsymbol{Z}$

Initialization: the random initial points $\boldsymbol{x}^0$, $t^0>0$ and set $l=0$, $\boldsymbol{u}^0 = (t^0, \boldsymbol{x}^0)$

Repeat: $l=l+1$, to calculate $\boldsymbol{u}^l = (t^l, \boldsymbol{x}^l)$ by solving the following subproblem:

$$\min_{\boldsymbol{u}=(t,\boldsymbol{x})} 0 - \langle y^{l-1}, \boldsymbol{u}\rangle$$

$$s.t. \boldsymbol{x}^T \boldsymbol{B}_j \boldsymbol{x} \le t - \sigma^2, \forall j \in K$$

$$\boldsymbol{x}^T \boldsymbol{x} \le P_r, t > 0,$$

Until: $\frac{\|\boldsymbol{u}^l - \boldsymbol{u}^{l-1}\|}{1+\|\boldsymbol{u}^l\|} \le \varepsilon$ or $\frac{|f(\boldsymbol{u}^l) - f(\boldsymbol{u}^{l-1})|}{1+|f(\boldsymbol{u}^l)|} \le \varepsilon$

where $f(\boldsymbol{u}^l) = \frac{\sigma^2 + (\boldsymbol{x}^l)^T \boldsymbol{Z} \boldsymbol{x}^l}{t^l}$

Output: $R_s = h(t^l, \boldsymbol{x}^l) = f(\boldsymbol{u}^l)$, SNR_d, SNR_e.

V. EXPERIMENT AND RESULTS

This section presents the experimental results and evaluation of all four proposed methods in part IV. We compare the quality of AF scheme to DF scheme in wireless relying network from the perspectives of the values of secrecy rate. It shows that, DF scheme has better secrecy performance than AF scheme. In the rest of this section, we also describe received signal-to-noise-ratio at destination and eavesdroppers. From this viewpoint, it is clear that, the signal received at eavesdroppers is too bad then they cannot decode to get the messages which send from relays.

A. Generating experimental datasets:

We focus on the wireless communication model operating under both AF and DF schemes with the appearance of multiple eavesdropping station as Fig.1 with the two cases of number of eavesdropping stations used as K = 5 and 7 eavesdroppers; The relay nodes variable from 5 to 40 nodes; the power consumption P = 30 dBm. Assuming a one-way communication system, these channel coefficients are randomly generated according to the Gaussian distribution and are known in advance.

For each case, we generated 100 datasets of channel coefficient values from the source station to the relay station and from the relay stations to the destination one and to the eavesdroppers with the given configuration parameters as above mentioned. These datasets are shared for all four methods.

B. Experimental results

With the assumption of one-way communication system model (considering only the direction from source station S to receiver D without the opposite direction) as illustrated in Fig.2 with the given parameters. For each case, 100 independent tests were carried out and took the average result for the optimal solution value and the signal-to-noise-ratio received at legitimate destination and eavesdroppers for the comparison. The experimental results are as follows:

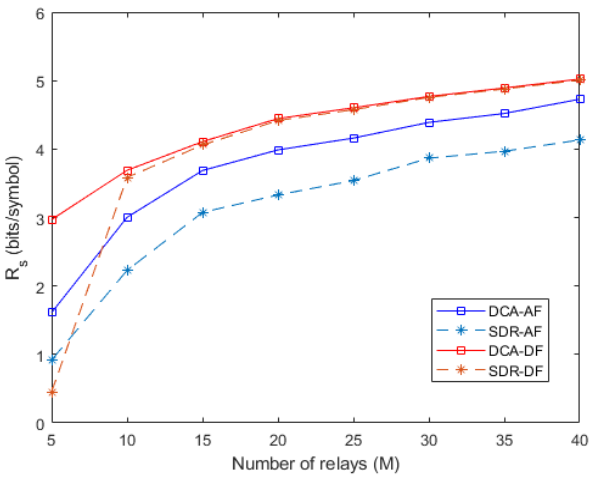

Fig.2. AF vs. DF in wireless relay beamforming network with 5 eavesdroppers

The optimal solution values: The results shown in Fig.2 and Fig.3 reflect the fact that, the value of the secrecy rate R_S always increasing with the number of relay stations. Specially, it shown an important thing that, the value R_s has strong increasing when the number of relay nodes reached around three times of the number of eavesdroppers, after that it is lightly increasing.

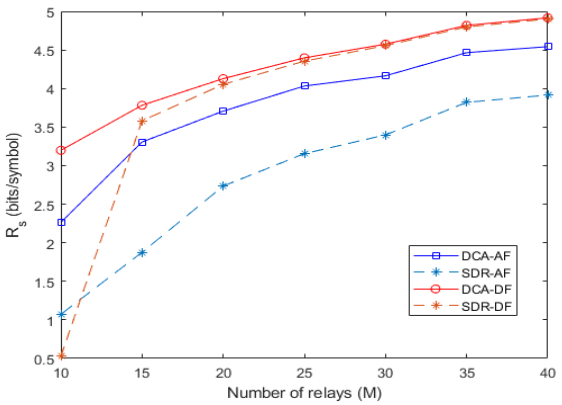

Fig.3: AF vs. DF in wireless relay beamforming network with 7 eavesdroppers

The secrecy rate efficiency of DF scheme is definitely higher than AF scheme as in figures. The gap of DC programming and DCA method with SDR method in AF network is clear. In contrast, this gap in DF network is quite small.

The maximum value $R_s = 5$ *bits/symbol* when the number of relay nodes is 40 respected to the case of DF network and 40 relays with 5 eavesdroppers (Fig.2). When the number of relays equal to the number of eavesdroppers then the R_s value down to zero for the case of Null steering method as in (12).

The SNR values: The data in Table 2 illustrates the SNR values at both destination (D) and eavesdroppers (E) as formula (2) and (4). It is clearly that, with the optimal beamforming weights at the relays, the SNRs received at eavesdropper are too small. As Wyner's condition [4] that the wire-tap channel had a greater loss than the main channel is not difficult to satisfy with the beamforming and fading techniques. The SNR values at eavesdroppers in the Null steering case as in the Tables 2 is suitable with the constrain of this system model (11). When the number of relays and eavesdroppers are equally, these SNRs become to similar then the R_s values down to zero (1) as in Fig.2 and Fig.3.

IV. CONCLUSION

With the emergence of 5G communication networks and the powerful development of IoT networks, wireless communication networks are gradually replacing fiber optic communication networks. Therefore, the study of the security method of physical layers for wireless networks is very necessary and really being widely concerned around the world.

According to the information theory, the physical layer security problem for the wireless network based on Amplify-and-Forward scheme is used as the optimal form with the goal of increasing the speed of secrecy rate (Rs) with a primary constraint on signal source power and considering the amplification factor at transition stations. This problem has a non-convex form and is difficult to solve to find a globally optimal solution. Some solutions for finding solutions to this optimization problem are the amplification values of the transition stations so that the most optimal security rate published recently is often the solution to an approximated solution. Therefore, the results suggest a new solution method based on the study of applying DC programming and DCA to solve these difficult problems to find better optimal solutions that have shown new and scientific features.

TABLE 2: THE SNR RECEIVED AT D AND E VS. NUMBER OF RELAYS WITH PS = 30 dBm, 5 EAVESDROPPERS.

Number of Relays	5		10		15		20		25		30		35	
SNR	***D***	***E***	***D***	***E***	***D***	***E***	***D***	***E***	***D***	***E***	***D***	***E***	***D***	***E***
DCA_AF	9.4	0.31	70.4	0.30	172.1	0.31	260.3	0.32	325.4	0.32	451.2	0.33	534.8	0.33
SDR_AF	3.0	0.43	25.1	0.46	77.5	0.58	105.9	0.51	140.7	0.50	220.2	0.50	252.1	0.53
DCA_DF	60.4	2.46	165.5	0.03	296.4	0.01	473.7	0.00	589.3	0.00	741.7	0.00	880.7	0.00
SDR_DF	30.3	37.5	157.9	0.00	292.2	0.00	470.5	0.00	587.0	0.00	740.0	0.00	879.3	0.00

REFERENCE

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

[2]. G. de Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks," in 2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2008, pp. 580–585, doi: 10.1109/WiMob.2008.16.

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

[4]. 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.

[5]. I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[6]. 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.

[7]. Tạp chí An toàn thông tin, "Bảo mật dữ liệu tầng vật lý trong mạng truyền tin không dây: Những ý tưởng đầu tiên và hướng nghiên cứu hiện nay", http://antoanthongtin.gov.vn/gp-atm/chi-tiet-bai-viet-cua-101779. [Accessed: 15-Feb-2020].

[8]. X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security," IEEE Commun. Surv. Tutor., vol. 19, no. 2, pp. 1027–1053, Secondquarter 2017.

[9]. 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.

[10]. Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing Physical-Layer Secrecy in Multiantenna Wireless Systems: An Overview of Signal Processing Approaches," IEEE Signal Process. Mag., vol. 30, no. 5, pp. 29–40, Sep. 2013, doi: 10.1109/MSP.2013.2256953.

[11]. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," IEEE Commun. Surv. Tutor., vol. 16, no. 3, pp. 1550–1573, 2014.

[12]. H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," IEEE Commun. Mag., vol. 53, no. 12, pp. 47–53, Dec. 2015, doi: 10.1109/MCOM.2015.7355565.

[13]. O. G. Aliu, A. Imran, M. A. Imran, and B. Evans, "A Survey of Self Organisation in Future Cellular Networks," IEEE Commun. Surv. Tutor., vol. 15, no. 1, pp. 336–361, First 2013.

[14]. F. I. Kandah, O. Nichols, and Li Yang, "Efficient key management for Big Data gathering in dynamic sensor networks," in 2017 International Conference on Computing, Networking and Communications (ICNC), 2017, pp. 667–671, doi: 10.1109/ICCNC.2017.7876209.

[15]. Physical Layer Security: Bounds, Codes and Protocols (João Barros) - Part 2 (SPCodingSchool).

[16]. N. N. Tuan and D. V. Son, "DC Programming and DCA for Enhancing Physical Layer Security in Amplify-and-Forward Relay Beamforming Networks Based on the SNR Approach," in Advanced Computational Methods for Knowledge Engineering, vol. 629, N.-T. Le, T. van Do, N. T. Nguyen, and H. A. L. Thi, Eds. Cham: Springer International Publishing, 2018, pp. 23–33.

[17]. S. Sarma, S. Agnihotri, and J. Kuri, "Secure Communication in Amplify-and-Forward Networks with Multiple Eavesdroppers: Decoding with SNR Thresholds," Wirel. Pers. Commun., vol. 85, no. 4, pp. 1945–1956, Dec. 2015.

[18]. N. N. Tuan and T. T. Thuy, "Physical Layer Security Cognitive Decode-and-Forward Relay Beamforming Network with Multiple Eavesdroppers," in Intelligent Information and Database Systems, vol. 11432, N. T. Nguyen, F. L. Gaol, T.-P. Hong, and B. Trawiński, Eds. Cham: Springer International Publishing, 2019, pp. 254–263.

[19]. H. A. Le Thi, V. N. Huynh, and T. P. Dinh, "DC Programming and DCA for General DC Programs," in Advanced Computational Methods for Knowledge Engineering, Cham, 2014, pp. 15–35, doi: 10.1007/978-3-319-06569-4_2.

ABOUT THE AUTHOR

M.Sc Nhu Tuan Nguyen

Workplace: Vietnam Information Security Journal

Email:nguyennhutuan@bcy.gov.vn

The education process: received the Master of science degree in Engineering from Academy of Cryptography Technique in 2007. He is a PhD student in Academy of Cryptography Technique.

Research today: machine learning and data mining in cyber security, cloud computing security, physical layer security.