Bảo mật dữ liệu tầng vật lý trong mạng truyền tin không dây sử dụng relay theo giao thức Decode-and-Forward và Amplify-and-Forward

Nguyễn Như Tuấn, Đặng Vũ Sơn, Nguyễn Ngọc Cương

***Tóm tắt*— Trong mô hình truyền tin phân tầng, để bảo mật dữ liệu, bên cạnh việc áp dụng các kỹ thuật mã hóa truyền thống tại các tầng phía trên, ý tưởng về bảo mật tại tầng vật lý (Physical Layer Security-PLS) cho mạng truyền tin không dây đã được đề cập từ những năm 1970. Đến nay, đặc biệt là trong một thập kỷ gần đây thì ý tưởng này đang được cộng đồng các nhà nghiên cứu khoa học trên toàn thế giới quan tâm. Nếu như ban đầu kỹ thuật này đòi hỏi kênh truyền của người nghe lén có độ suy hao lớn hơn kênh truyền của người thu hợp pháp, thì trong thời gian gần đây, với sự hỗ trợ của các relay, thì không bắt buộc phải có giả thiết trên. Với sự hỗ trợ của các relay sử dụng kỹ thuật truyền tin beamforming, có hai lược đồ truyền tin bảo mật tầng vật lý cho mạng không dây được quan tâm chủ yếu hiện nay là: Decode-and-Forward (DF) và Amplify-and-Forwar (AF). Bài báo này trình bày kết quả nghiên cứu tổng quan về các kỹ thuật này và phân tích các kết quả, hướng nghiên cứu này trong thời gian gần đây.**

***Abstract*— Beside cryptography algorithms which are based on the upper layers of protocol stack to ensure confidentiality in communication systems, the idea of physical layer security (PLS) in wireless network systems dates back to (in) 1970s. In the past decade, this idea has been studied by many researchers from all around the world. Initially, this method required that the source-destination channel is better than source-eavesdropper channel. However, current advances in technology, especially with the help of relay and beamforming technique the PLS problem is now possible even though the above channel condition is not met. For wireless relay networks, there are two main relaying schemes often employed for physical layer security Decode-and-Forward (DF) and Amplify-and-Forward (AF). In this paper, we present the state-of-the-art of both these techniques in physical layer security and some future research directions related to them.**

***Từ khóa*— An toàn toàn tầng vật lý; Decodeand-Forward; Amplify-and-Forward.**

***Keywords*— Physical layer security; Decode-and-Forward; Amplify-and-Forward.**

I. GIỚI THIỆU

Hiện nay, hầu hết các phương pháp đảm bảo tính bí mật trong hệ thống truyền tin đều dựa vào kỹ thuật mật mã để mã hóa nội dung thông tin từ nơi gửi đến nơi nhận [11]. Chúng ta cùng xem xét một mô hình truyền tin cơ bản như Hình 1.

Hình 1. Mô hình truyền tin có trạm thu lén tổng quát

Người gửi, được gọi là Alice, mong muốn gửi một thông báo trọn vẹn cho người nhận, gọi là Bob. Còn Eve, người nghe lén, chưa thể biết được nội dung thông báo. Để đảm bảo yêu cầu trên, Alice sử dụng một hoặc nhiều thuật toán mã hóa kết hợp với khóa mã để mã hóa bản thông báo. Bob biết về thuật toán mã hóa được sử dụng, nên sử dụng khóa hợp lệ do anh ta có để giải mã bản thông báo. Còn Eve, có thể biết về thuật toán mã hóa được sử dụng, nhưng không biết về khóa mã được sử dụng nên rất khó có thể giải mã được thông báo do Alice gửi cho Bob.

Một xu hướng khác trong bảo mật mạng không dây được nghiên cứu nhiều trong thời gian gần đây là bảo mật dữ liệu truyền tin tầng vật lý. Hướng nghiên cứu này được khởi xướng từ năm 1975 bởi Tiến sỹ Aaron D. Wyner [35]. Trong công trình này, Wyner đã chứng minh rằng có thể truyền tin bảo mật với tốc độ C_s ($C_s > 0$) trên kênh truyền có sự xuất hiện của người nghe lén. Một giả thiết quan trọng trong các nghiên cứu của Wyner là kênh truyền giữa Alice đến Eve (sau đây gọi tắt là kênh

Bài báo được nhận ngày 20/7/2017. Bài báo được gửi cho phản biện thứ nhất vào ngày 28/7/2017 và nhận được ý kiến đồng ý đăng của phản biện thứ nhất đăng vào ngày 5/8/2017. Bài báo được gửi cho phản biện thứ hai vào ngày 28/7/2017 và nhận được ý kiến đồng ý đăng của phản biện thứ hai vào ngày 15/8/2017.

nghe lén - wire-tap channel), có độ suy hao lớn hơn kênh truyền từ Alice đến Bob, (sau đây gọi là kênh chính - main channel). Theo đó, khái niệm *secrecy rate* được chỉ ra là tốc độ mà thông tin có thể truyền một cách an toàn từ người gửi đến người nhận hợp pháp và giá trị *secrecy rate* lớn nhất có thể đạt được, được gọi là *secrecy capacity*.

Một nghiên cứu mở rộng hơn cho các kết quả của Aaron D. Wyner được công bố bởi Imre Csiszár và János Korner vào năm 1978 [4] là có thể truyền đồng thời hai loại thông báo trong cùng hệ thống. Đó là: truyền thông báo bí mật (confidential message) tại tốc độ C_s ($C_s > 0$) với độ bảo mật là tuyệt đối (perfect secrecy) và truyền quảng bá một thông báo chung (common message) cho mọi người trong hệ thống mà không cần giữ bí mật. Giá trị C_s được chỉ ra là $C_s = \max\,[I(X;Y) - I(X;Z)]$, với X là nguồn đầu vào kênh chính được phát bởi Alice, Y là đầu ra của kênh chính được thu bởi Bob và Z là đầu ra của kênh nghe lén được thu bởi Eve; $I(X;Y)$ và $I(X;Z)$ lần lượt là thông tin chung (mutual information) giữa X với Y và giữa X với Z.

Cũng trong năm 1978, kết quả của Wyner đã được phát biểu chi tiết hơn với kênh truyền Gaussian (Gaussian channel) trong [16]. Theo đó, tốc độ truyền tin an toàn có thể C_s đã được xác định là $C_s = C_M - C_{MW}$, trong đó, C_M (capacity channel) là dung lượng của kênh truyền chính và C_{MW} là dung lượng của kênh nghe lén.

Khi kỹ thuật truyền tin phát triển, thì hướng nghiên cứu này đã thực sự được quan tâm nghiên cứu rộng rãi và có tính ứng dụng cao do đã khắc phục được hạn chế về đòi hỏi kênh truyền chính có độ suy hao ít hơn kênh nghe lén. Điển hình cho các nghiên cứu gần đây như đối với kênh truyền fading trong [23] và [36], các hệ thống truyền thông có nhiều antenna trong [12], [13], [18], [22] và [26]. Đối với hệ thống có nhiều người dùng (multi-user), R.Liu và cộng sự [25] đã đề cập đến giá trị biên trong (inner bound) và biên ngoài (outer bound) của vùng an toàn (secrecy capacity regions) cho kênh quảng bá và tương tác (broadcast and interference channels). Khả năng an toàn với kênh quảng bá có nhiều antenna đã được R. Liu và cộng sự trình bày trong [19].

Cùng với sự phát triển của kỹ thuật truyền tin, một mô hình truyền tin được quan tâm nghiên cứu gần đây là người phát dùng một antenna nhưng sử dụng nhiều relay (trạm trung chuyển) hỗ trợ để tạo ra sự tương tác đa antenna. Đặc biệt, kỹ thuật truyền tin beamforming đã thu hút sự chú ý của nhiều nhà khoa học nghiên cứu và các kết quả đã được công bố trong rất nhiều công trình [7], [8], [10], [33]. Trong các hệ thống truyền tin sử dụng kỹ thuật beamforming có sự hỗ trợ của các relay được chia thành hai mô hình cơ bản với hai dạng bài toán chính là tối đa hoá khả năng truyền tin bảo mật (secrecy capacity maximization) và tối thiểu hoá năng lượng (công suất) truyền tin (transmit power minimization). Mô hình DF được L. Dong và cộng sự trình bày trong [20] từ năm 2008. Một năm sau, các nhà nghiên cứu này đã công bố các kết quả nghiên cứu của họ với mô hình AF trong [6], và năm 2010, nhóm nghiên cứu này công bố kết quả đầy đủ hơn đối với cả hai mô hình DF và AF trong [5].

Mô hình hệ thống truyền tin theo kỹ thuật beamforming có tương tác theo phương thức truyền tin DF được rất nhiều nhà nghiên cứu quan tâm. Các công trình nghiên cứu trong thời gian gần đây đề cập đến nhiều mô hình truyền tin khác nhau, trường hợp hệ thống truyền tin một chiều (one-direction) trong [5], [31], [34] hoặc truyền tin hai chiều (two-direction) trong [30], trường hợp trạm nguồn chỉ có thể truyền đến relay sau đó relay sẽ truyền đến trạm đích và trạm nghe lén, hoặc trạm đích có thể truyền đồng thời đến cả relay và trạm nhận hợp pháp cũng như trạm nghe lén trong [5]. Trong nội dung này, bài báo chỉ tập trung vào hệ thống truyền tin một chiều, từ S đến D và không có chiều ngược lại, và trường hợp trạm nguồn S chỉ truyền đến các relay, không có đường truyền trực tiếp từ trạm nguồn đến trạm thu và trạm nghe lén.

Phần còn lại của bài báo sẽ tập trung phân tích các kết quả trên các mô hình tương tác và các hướng nghiên cứu gần đây trong lĩnh vực này. Tất cả các kết quả trên thường dẫn đến các bài toán tối ưu trong lý thuyết thông tin. Tuỳ theo mô hình và độ phức tạp của bài toán mà các nhà nghiên cứu đề xuất các phương pháp giải khác nhau, trong đó một số tài liệu và công cụ được sử dụng phổ biến như công cụ giải bài toán tối ưu lồi CVX [2], các kỹ thuật tính toán trên ma trận [9], phương pháp giải bài toán tối ưu không lồi "DC Programming and DCA" [14], [24] và công cụ lập trình MATLAB [29].

Bài báo được bố cục như sau: Sau Mục I giới thiệu tổng quan về mô hình bảo mật, tiếp theo Mục II trình bày các bài toán và các kết quả về vấn đề an toàn trong mô hình truyền tin DF, Mục III trình bày các bài toán và các kết quả trong mô hình AF, và cuối cùng là Mục kết luận và hướng nghiên cứu tiếp theo của nhóm tác giả.

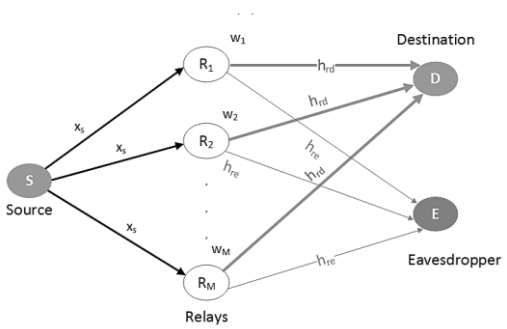
Ký hiệu: Trong phần này chúng tôi sử dụng các ký hiệu như sau: Các chữ cái hoa đậm được ký hiệu cho các ma trận (Matrix); Các chữ cái thường đậm ký hiệu cho các vector cột; Các ký hiệu $(.)^*, (.)^T, (.)^\dagger$ được dùng cho liên hợp (Conjugate), chuyển vị (Transpose) và chuyển vị liên hợp (Conjugate transpose); $\mathbf{I}_M$ là ma trận đơn vị (Identity/unit matrix) cấp $M \times M$; $diag\{\mathbf{a}\}$ hoặc $\mathbf{D}(\mathbf{a})$ ký hiệu cho ma trận đường chéo (Diagonal matrix) với các phần tử nằm trên đường chéo chính là giá trị của vector $\mathbf{a}$; $\|\mathbf{a}\|$ ký hiệu cho 2-norm (chuẩn 2) của vector $\mathbf{a}$; $E\{.\}$ ký hiệu cho kỳ vọng (Expectation); $\mathbf{A} \succcurlyeq 0$ ký hiệu cho ma trận $\mathbf{A}$ là ma trận nửa xác định dương (semidefinite positive matrix); $\mathbb{C}$ ký hiệu cho tập các giá trị phức (complex form); s.t. ký hiệu cho các ràng buộc của bài toán tối ưu (such that).

II. MÔ HÌNH DF

Tuỳ theo mô hình truyền tin có một trạm nghe lén, hay nhiều trạm nghe lén sẽ dẫn bài toán đến các dạng khác nhau. Với mô hình có nhiều trạ nghe lén, thường dẫn đến những bài toán có ràn buộc phức tạp, nên bài toán sẽ khó giải hơn so với bài toán của mô hình có một trạm nghe lén.

A. Hệ thống có một trạm nghe lén

1. Mô hình hệ thống: Mô hình truyền tin có một trạm nghe lén được xem xét như Hình 2. Hệ thống bao gồm: một trạm phát ký hiệu là *S* (Source), một trạm nhận tin hợp pháp *D* (Destination), *M* trạm relay ký hiệu là $R_1, R_2, \dots, R_M$ và một trạm nghe lén E (Eavesdropper). Chúng ta ký hiệu cho hệ số fading của kênh truyền giữa *S* và các relay là $\mathbf{h}_{sr} = [h_{s1}, \dots, h_{sM}]^T \in \mathbb{C}$, và hệ số fading của kênh truyền từ relay đến *D* là $\mathbf{h}_{rd} = [h_{1d}, \dots, h_{Md}]^T \in \mathbb{C}$, và hệ số fading của kênh truyền từ các relay đến *E* là $\mathbf{h}_{re} = [h_{1e}, \dots, h_{Me}]^T \in \mathbb{C}$.



Hình 2. Mô hình truyền tin có xuất hiện một trạm nghe lén

Trong mô hình này, với sự hỗ trợ của các relay, trạm nguồn *S* cố gắng truyền các thông báo bí mật đến trạm thu *D* với yêu cầu đảm bảo trạm thu lén *E* không thể biết được nội dung của các thông báo bí mật. Hệ thống hoạt động theo lược đồ DF sẽ hoạt động theo hai pha tương ứng với 2 khe thời gian truyền tin (time slot transmission) như sau [1], [40]:

- Pha 1: Trạm nguồn S truyền tín hiệu x_s tới các relay với công suất $E[|x_s|^2] = P_s$. Tín hiệu thu được tại relay thứ *m* là:

$$y_{rm} = h_{sr,m}x_s + n_{rm}$$

trong đó n_{rm} là nhiễu cơ sở tại relay thứ *m* có phân bố Gaussian với mức ý nghĩa không và phương sai σ_r^2. Biểu diễn các tín hiệu nhận được tại các relay dưới dạng vector như sau:

$$\mathbf{y}_r = \mathbf{h}_{sr}x_s + \mathbf{n}_r$$

- Pha 2: Tại pha 2, trước tiên, các relay tiến hành giải mã thông báo x_s và chuẩn hóa thành $x'_s = x_s/\sqrt{P_s}$. Sau đó, tín hiệu đã được chuẩn hóa được nhân với trọng số của relay $\mathbf{w} = [w_1, \dots, w_M]^T$ để tạo ra tín hiệu truyền từ relay là $x_r = x'_s w_m$. Công suất truyền tại mỗi relay R_m sẽ là:

$$E|x_r|^2 = E|x'_s w_m|^2 = |w_m|^2. \quad (1)$$

Có hai loại ràng buộc đối với công suất truyền tại các relay. Ràng buộc thứ nhất là về tổng công suất truyền tại các relay, có dạng $\|w\|^2 = w^\dagger w \leq P_R$, trong đó P_R là tổng công suất truyền cực đại của tất cả các relay. Ràng buộc thứ hai cũng thường được quan tâm đó là về giới hạn công suất truyền tại mỗi relay, có dạng $|w_m|^2 \leq p_m \, \forall m = 1, \dots, M$ trong đó p_m là công suất truyền tối đa của relay thứ *m*.

Các tín hiệu thu được tại trạm thu *D* và trạm nghe lén *E* sẽ là sự chồng lấn (superposition) của các tín hiệu thu được từ các relay, cụ thể sẽ có dạng tương ứng là:

$$y_d = \sum_{m=1}^{M} h_{rd,m}w_m x'_s + n_d = \mathbf{h}_{rd}^\dagger \mathbf{w} x'_s + n_d \quad (2)$$

$$y_e = \sum_{m=1}^{M} h_{re,m}w_m x'_s + n_e = \mathbf{h}_{re}^\dagger \mathbf{w} x'_s + n_e \quad (3)$$

trong đó $\mathbf{h}_{rd} = [h^*_{rd,1} \dots h^*_{rd,M}]^T$, $\mathbf{h}_{re} = [h^*_{re,1} \dots h^*_{re,M}]^T$, n_d và n_e là nhiễu cơ sở tại *S* và *E* theo phân bố Gaussian với mức ý nghĩa không và phương sai σ^2.

2. Phát biểu bài toán: Với hoạt động của hệ thống theo giao thức DF gồm 2 pha như ở trên, chúng ta có tỷ lệ tín hiệu trên tạp âm SNR (Signal Noise Ratior) tại *D* và *E* như sau:

$$\Gamma_d = \frac{\left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2}$$

$$\Gamma_e = \frac{\left|\sum_{m=1}^{M} h_{re,m} w_m\right|^2}{\sigma^2}$$

Lúc này giá trị *secrecy rate* (tốc độ truyền tin an toàn, có đơn vị là số bit/đơn vị truyền tin (symbol)) Rs trên kênh truyền giữa relay và trạm thu *D* sẽ là:

$$R_s = I(x_s; y_d) - I(x_s; y_e)$$
$$= \log\,(1 + \Gamma_d) - \log\,(1 + \Gamma_e)$$
$$= \log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{re,m} w_m\right|^2}\right) \quad (4)$$

Bài toán tối đa hóa giá trị *secrecy rate* R_s với ràng buộc về tổng công suất truyền và/hoặc ràng buộc về công suất truyền riêng rẽ của các relay sẽ được phát biểu như sau:

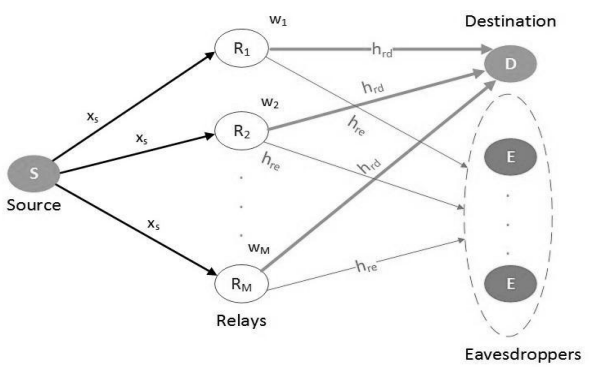
$$\max_{w} \log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{re,m} w_m\right|^2}\right) \quad (5)$$

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

(và/hoặc $|w_m|^2 \le p_m, \forall m = 1, \dots, M$).

B. Hệ thống có nhiều trạm nghe lén

1. Mô hình hệ thống: Mô mình hệ thống hoạt động theo giao thức DF có nhiều trạm nghe lén như Hình 3. Mô hình này có các thành phần và ký hiệu tương tự như mô hình DF có một trạm nghe lén, nhưng có sự suất hiện của *K* trạm nghe lén được ký hiệu là $E_1, \dots, E_K$. Hệ số fading của kênh truyền giữa các relay và các trạm nghe lén được ký hiệu là $\mathbf{h}_{re} = [h_{re,1}, \dots, h_{re,K}]^T$.



Hình 3. Hệ thống có sự xuất hiện của nhiều trạm nghe lén

Hoạt động của hệ thống theo giao thức DF có nhiều trạm nghe lén cũng gồm 2 pha tương tự như với một trạm nghe lén và lúc này tín hiệu nhận được tại trạm nghe lén thứ *j* sẽ là:

$$y_{ej} = \sum_{m=1}^{M} h_{re_j,m} w_m x'_s + n_e$$
$$= \mathbf{h}_{re}^{\dagger}\mathbf{w}x'_s + n_e \;\forall j = 1, \dots, K. \quad (6)$$

2. Phát biểu bài toán: Giá trị SNR tại trạm nghe lén thứ *j* trong mô hình *K* trạm nghe lén sẽ là:

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

Giá trị *secrecy rate* R_s khi này sẽ là:

$$R_s = \min_{j=1,\dots,K}\left(I(x_s;\, y_d) - I\left(x_s;\, y_{e_j}\right)\right)$$
$$= \min_{j=1,\dots,K}\left(\log\,(1 + \Gamma_d) - \log\left(1 + \Gamma_{e_j}\right)\right)$$
$$= \min_{j=1,\dots,K} \log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{re_j,m} w_m\right|^2}\right) \quad (7)$$

Bài toán tối đa hóa giá trị *secrecy rate* R_s với ràng buộc về tổng công suất truyền và/hoặc ràng buộc về công suất truyền riêng rẽ của các relay được phát biểu như sau:

$$\max_{w} \min_{j=1,\dots,K}\left(\log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m} w_m\right|^2}{\sigma^2 + \left|\sum_{m=1}^{M} h_{re_j,m} w_m\right|^2}\right)\right) \quad (8)$$

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

(và/hoặc $|w_m|^2 \le p_m, \forall m = 1, \dots, M$).

C. Một số kết quả

Năm 2010, Lun Dong và cộng sự [5] đã công bố một số cách giải các bài toán PLS một cách trực tiếp, để đưa ra các nghiệm suboptimal cho cả bài toán DF có một trạm nghe lén và nhiều trạm nghe lén như sau:

1. Hệ thống có một trạm nghe lén như bài toán (5): Do hàm log có tính đơn điệu tăng nên bài toán (5) có thể viết tương đương thành:

$$\max_{w} \frac{\sigma^2 + \mathbf{w}'\mathbf{H}_{rd}\mathbf{w}}{\sigma^2 + \mathbf{w}'\mathbf{H}_{re}\mathbf{w}} \quad (9)$$

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

(và/hoặc $|w_m|^2 \le p_m, \forall m = 1, \dots, M$).

trong đó, $\mathbf{H}_{rd} = \mathbf{h'}_{rd}\mathbf{h}_{rd}$ với $\mathbf{h}_{rd} = [h_{rd_1}, \dots, h_{rd_M}]^T$ và $\mathbf{H}_{re} = \mathbf{h'}_{re}\mathbf{h}_{re}$ với $\mathbf{h}_{re} = [h_{re_1}, \dots, h_{re_M}]^T$.

Trong trường hợp hệ thống truyền tin chỉ quan tâm đến ràng buộc về giới hạn tổng công suất của các relay (total relay power constraint) [5], [39], lúc này ràng buộc $\mathbf{w}^\dagger\mathbf{w} \le P_R$ sẽ tương đương với ràng buộc $\mathbf{w}^\dagger\mathbf{w} = P_R$ (do R_s là một hàm đơn điệu tăng theo giá trị của P_R. Do đó bài toán (9) được giải trực tiếp bằng phương pháp giá trị riêng tổng quát (generalized eigenvalue), cụ thể, trong trường hợp này, bài toán (9) sẽ được viết như sau:

$$\max_{|w|^2=P_R} \frac{\sigma^2 + \mathbf{w'}\mathbf{H}_{rd}\mathbf{w}}{\sigma^2 + \mathbf{w'}\mathbf{H}_{re}\mathbf{w}}$$

$$= \max_{|w|^2=P_R} \frac{\sigma^2\left(\frac{\mathbf{w'}\mathbf{I}_M\mathbf{w}}{P_r}\right) + \mathbf{w'}\mathbf{H}_{rd}\mathbf{w}}{\sigma^2\left(\frac{\mathbf{w'}\mathbf{I}_M\mathbf{w}}{P_r}\right) + \mathbf{w'}\mathbf{H}_{re}\mathbf{w}}$$

$$= \max_{|w|^2=P_R} \frac{\mathbf{w'}\left(\sigma^2\left(\frac{\mathbf{I}_M}{P_r}\right) + \mathbf{H}_{rd}\right)\mathbf{w}}{\mathbf{w'}\left(\sigma^2\left(\frac{\mathbf{I}_M}{P_r}\right) + \mathbf{H}_{re}\right)\mathbf{w}}$$

$$= \succ_{max}\left(\sigma^2\frac{\mathbf{I}_M}{P_r} + \mathbf{H}_{rd}, \sigma^2\frac{\mathbf{I}_M}{P_r} + \mathbf{H}_{re}\right) \quad (10)$$

trong đó $\succ_{max}$ $(\mathbf{A}, \mathbf{B})$ là giá trị riêng mở rộng lớn nhất (the largest generalized eigenvalue) của cặp ma trận $(\mathbf{A}, \mathbf{B})$.

Như vậy, bài toán (5) với ràng buộc về tổng công suất truyền của các relay được đưa về bài toán (10) và đưa ra nghiệm tối ưu một cách trực tiếp.

Trong trường hợp ràng buộc về giới hạn công suất truyền tại mỗi relay (individual relay power constraint) được quan tâm ($|w_m|^2 \le p_m$) thì bài toán (9) trở nên khó giải hơn. Một phương pháp được sử dụng nhiều cho trường hợp này là phương pháp SDR (SemiDefinite Relaxation) để xấp xỉ bài toán (9) thành một bài toán SemiDefinite Programming (SDP) lồi ([39]) có dạng như sau:

$$\max_{\mathbf{W},t} t \quad (11)$$

$$\text{s.t. } diag\,(\mathbf{W}) \le p_m$$

$$\mathbf{W} \succcurlyeq 0$$

$$tr\big(\mathbf{W}(\mathbf{H}_{rd} - t\mathbf{H}_{re})\big) \ge \sigma^2(t-1),$$

trong đó, $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$, $tr(.)$ là ký hiệu cho vết của ma trận (trace of a matrix).

Do bài toán (11) đã bỏ đi một ràng buộc là Rank ($\mathbf{W}$) = 1 nên nghiệm của bài toán (11) chỉ là một nghiệm xấp xỉ của bài toán (9) với ràng buộc về giới hạn công suất truyền tại mỗi relay. Bài toán (11) có thể được giải một cách hiệu quả bằng phương pháp điểm trong (interior point) với thuật toán bisection [39]. Trong quá trình thực hành, để đảm bảo nghiệm của bài toán relaxed (11) nằm trong miền ràng buộc của bài toán gốc, chúng ta có thể áp dụng kỹ thuật xấp xỉ (scalling) rank-one, khi đó giá trị mục tiêu của bài toán SDP sẽ giảm đi một lượng nhỏ. Trong [39] cũng giới thiệu hai cách tiếp cận khác để giải bài toán (9) là Simplified Suboptimal Design và Second-order Cone Program (SOCP) Approach.

2. Hệ thống có nhiều trạm nghe lén như bài toán (5): Bài toán (8) là bài toán không lồi và thường khó giải để tìm được nghiệm tối ưu toàn cục. Trong [5], các tác giả đã đề xuất một phương pháp tìm nghiệm con cho trường hợp đặc biệt (suboptimal) bằng cách thêm điều kiện là triệt tiêu hoàn toàn tín hiệu đến các trạm nghe lén tức là khi này $\mathbf{w'}\mathbf{h}_{re_j}\mathbf{w} = 0_{K\times 1}$ và chỉ xét ràng buộc về giới hạn tổng công suất truyền tại các relay, do đó trong trường hợp này bài toán (8) sẽ được đưa về dạng sau:

$$\max_{w}\left(\log\left(\frac{\sigma^2 + \left|\sum_{m=1}^{M} h_{rd,m}w_m\right|^2}{\sigma^2}\right)\right) \quad (12)$$

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

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

Do hàm log có tính đơn điệu tăng, nên việc giải bài toán (12) sẽ tương đương với giải bài toán sau:

$$\max_{w} \quad \mathbf{w'}\mathbf{H}_{rd}\mathbf{w} \quad (13)$$

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

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

với $\mathbf{H}_{rd} = \mathbf{h'}_{rd}\mathbf{h}_{rd}$ và $\mathbf{h}_{rd} = [h_{1d}, \dots, h_{Md}]^T$.

Bằng cách thay ràng buộc $\mathbf{w}^\dagger\mathbf{w} \le P_R$ bằng một ràng buộc tương đương là $\mathbf{w}^\dagger\mathbf{w} = P_R$, bài toán (13) tương ứng với trường hợp triệt tiêu toàn bộ tin hiệu truyền từ relay đến kẻ nghe lén và nghiệm của bài toán là ([5]):

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

trong đó, $\mathbf{P}_{re} = \mathbf{H}_{re}(\mathbf{H}_{re}^\dagger\mathbf{H}_{re})^{-1}\mathbf{H}_{re}^\dagger$.

Như vậy, trong trường hợp này bài toán đã được giải một cách trực tiếp, tuy nhiên nghiệm của bài toán chỉ là nghiệm suboptimal do đã đưa thêm điều kiện là triệt tiêu hoàn toàn tín hiệu truyền đến các trạm nghe lén.

III. MÔ HÌNH AF

Mô hình truyền tin hoạt động theo lược đồ AF được nghiên cứu rộng rãi và nhiều kết quả cho thấy, lược đồ này có nhiều ưu điểm hơn so với lược đồ DF. Một số kết quả điển hình của mô hình AF được trình bày trong [6], [27], [37], [1] và [39]. Mô hình này cũng thường được nghiên cứu với hai trường hợp là hệ thống có một trạm nghe lén và hệ thống có nhiều trạm nghe lén.

A. Hệ thống có một trạm nghe lén

1. Mô hình hệ thống: Trong trường hợp hệ thống truyền tin hoạt động theo giao thức AF có sự xuất hiện của một trạm nghe lén, chúng ta xét mô hình truyền tin như Hình 2, hệ thống hoạt động theo 2 pha. Trong pha một, trạm nguồn *S* truyền thông báo cần giữ bí mật x_s tới các relay, tín hiệu nhận được tại các relay là $\mathbf{y}_r = \mathbf{h}_{sr}x_s + \mathbf{n}_r$.

Trong pha 2, các relay không thực hiện giải mã như với mô hình DF mà nhân trực tiếp tín hiệu thu được y_r với hệ số $w = [w_1, \dots, w_M]^T$, sau đó truyền đến trạm đích *D*. Tín hiệu đầu ra của relay thứ *m* được biểu diễn là:

$$x_{r.m} = w_m(h_{sr_m}x_s + n_m).$$

Dạng vector biểu diễn tín hiệu phát từ các relay là:

$$\mathbf{x}_r = \mathbf{D}(\mathbf{y}_r)\mathbf{w}.$$

Các ràng buộc về công suất truyền cho trường hợp AF cũng có hai loại là ràng buộc về tổng công suất truyền của tất cả các relay $\mathbb{E}\{\|\mathbf{D}(\mathbf{y}_r)\mathbf{w}\|_2^2\} = \mathbf{w}^\dagger\mathbf{C}\mathbf{w} \le P_R$ và ràng buộc về công suất truyền tại mỗi relay $\mathbb{E}\left\{\left|y_{r,m}w_m\right|^2\right\} = \mathbf{e}_m^\dagger\mathbf{C}\mathbf{w}\mathbf{w}^\dagger\mathbf{e}_m \le p_m$ tương tự như với trường hợp DF. Trong đó, $\mathbf{C} = P_S\mathbf{D}^\dagger(\mathbf{h}_{sr})\mathbf{D}(\mathbf{h}_{sr}) + \sigma^2\mathbf{I}_m$ và e_m là vector đơn vị (vị trí thứ *m* có giá trị 1) có độ dài *M*.

Các tín hiệu nhận được tại trạm đích *D* và trạm nghe lén *E* là kết hợp của các tín hiệu được phát từ các relay, cụ thể được biểu diễn như sau:

$$y_d = \sum_{m=1}^{M} h_{rd,m}w_m\left(h_{sr_m}x_s + n_{rm}\right) + n_d$$
$$= \sqrt{P_S}\mathbf{h}_{rd}\mathbf{D}(\mathbf{h}_{sr})\mathbf{w}x_s + \mathbf{n}_r^T\mathbf{D}^\dagger(\mathbf{h}_{rd})\mathbf{w} + n_d \quad (14)$$

$$y_e = \sum_{m=1}^{M} h_{re,m}w_m\left(h_{sr_m}x_s + n_{rm}\right) + n_e$$
$$= \sqrt{P_S}\mathbf{h}_{re}\mathbf{D}(\mathbf{h}_{sr})\mathbf{w}x_s + \mathbf{n}_r^T\mathbf{D}^\dagger(\mathbf{h}_{re})\mathbf{w} + n_e \quad (15)$$

2. Phát biểu bài toán: Giá trị SNR thu được tại trạm thu D và trạm nghe lén E được tính là:

$$\Gamma_d = \frac{\left|\sum_{m=1}^{M} h_{rd_m}h_{sr_m}w_m\right|^2 P_S}{\sum_{m=1}^{M}\left|h_{rd_m}\right|^2|w_m|^2\sigma^2 + \sigma^2}$$
$$= \frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{G}\mathbf{w}+1} \quad (16)$$

và

$$\Gamma_e = \frac{\left|\sum_{m=1}^{M} h_{re_m}h_{sr_m}w_m\right|^2 P_S}{\sum_{m=1}^{M}\left|h_{re_m}\right|^2|w_m|^2\sigma^2 + \sigma^2}$$
$$= \frac{\mathbf{w}^\dagger\mathbf{B}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{H}\mathbf{w}+1} \quad (17)$$

Trong đó, $\mathbf{A} = \left(\frac{P_S}{\sigma^2}\right)\mathbf{D}^\dagger(\mathbf{h}_{sr})\mathbf{h}_{rd}\mathbf{h}_{rd}^\dagger\,\mathbf{D}(\mathbf{h}_{sr})$, $\mathbf{G} = \mathbf{D}(\mathbf{h}_{rd})\mathbf{D}^\dagger(\mathbf{h}_{rd})$, $\mathbf{B} = \left(\frac{P_S}{\sigma^2}\right)\mathbf{D}^\dagger(\mathbf{h}_{sr})\mathbf{h}_{re}\mathbf{h}_{re}^\dagger\,\mathbf{D}(\mathbf{h}_{sr})$ và $\mathbf{H} = \mathbf{D}(\mathbf{h}_{re})\mathbf{D}^\dagger(\mathbf{h}_{re})$.

Giá trị *secrecry rate* có thể đạt được khi này sẽ là:

$$R_S = I(x_s;\, y_d) - I(x_s; y_e)$$
$$= \log(1+\Gamma_d) - \log(1+\Gamma_e). \quad (18)$$

Bài toán cực đại hóa giá trị *secrecy rate* của hệ thống với ràng buộc về tổng công suất truyền của tất cả các relay và/hoặc ràng buộc công suất truyền tối đa tại mỗi relay có dạng như sau:

$$\max_{w} \log\frac{\left(\mathbf{w}^\dagger\mathbf{A}\mathbf{w} + \mathbf{w}^\dagger\mathbf{G}\mathbf{w} + 1\right)\left(\mathbf{w}^\dagger\mathbf{H}\mathbf{w} + 1\right)}{\left(\mathbf{w}^\dagger\mathbf{G}\mathbf{w} + 1\right)\left(\mathbf{w}^\dagger\mathbf{B}\mathbf{w} + \mathbf{w}^\dagger\mathbf{H}\mathbf{w} + 1\right)} \quad (19)$$

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

(và/hoặc $\mathbf{e}_m^\dagger\mathbf{C}\mathbf{w}\mathbf{w}^\dagger\mathbf{e}_m \le p_m, \forall m = 1, \dots, M$).

B. Hệ thống có nhiều trạm nghe lén

1. Mô hình hệ thống: Mô hình AF có nhiều trạm nghe lén như Hình 3 hoạt động theo 2 pha như các mô hình AF có một trạm nghe lén. Trong pha 1, tín hiệu từ trạm nguồn S được truyền đến các relay. Tín hiệu thu được tại relay được xác định là: $\mathbf{y}_r = \mathbf{h}_{sr}x_s + \mathbf{n}_r$.

Tại pha 2, các relay sẽ khuếch đại tín hiệu thu được rồi truyền đến trạm thu *D*, đồng thời thì các trạm nghe lén $E_1, \dots, E_K$ cũng thu được tín hiệu này. Tín hiệu thu được tại trạm thu *D* và trạm

nghe lén thứ $k, \forall k = 1, \dots, K$ tương ứng sẽ có dạng:

$$y_d = \sum_{m=1}^{M} h_{rd,m} w_m \left(h_{sr_m} x_s + n_{rm}\right) + n_d$$
$$= \sqrt{P_S}\mathbf{h}_{rd}\mathbf{D}(\mathbf{h}_{sr})\mathbf{w}x_s + \mathbf{n}_r^T\mathbf{D}^\dagger(\mathbf{h}_{rd})\mathbf{w} + n_d \quad (20)$$

$$y_{e,k} = \sum_{m=1}^{M} h_{re_k,m} w_m \left(h_{sr_m} x_s + n_{rm}\right) + n_{e_k}$$
$$= \sqrt{P_S}\mathbf{h}_{re_k}\mathbf{D}(\mathbf{h}_{sr})\mathbf{w}x_s + \mathbf{n}_r^T\mathbf{D}^\dagger\left(\mathbf{h}_{re_k}\right)\mathbf{w} + n_{e_k} \quad (21)$$

2. Phát biểu bài toán: Tương tự như mô hình AF có một trạm nghe lén ở trên, giá trị SNR thu được tại trạm thu D và trạm nghe lén thứ *k* sẽ có dạng:

$$\Gamma_d = \frac{\left|\sum_{m=1}^{M} h_{rd_m} h_{sr_m} l_m w_m\right|^2 P_s}{\sum_{m=1}^{M}\left|h_{rd_m}\right|^2 l_m^2 |w_m|^2 \sigma^2 + \sigma^2}$$
$$= \frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{G}\mathbf{w}+1} \quad (22)$$

và

$$\Gamma_{e_k} = \frac{\left|\sum_{m=1}^{M} h_{re_k,m} h_{sr_m} l_m w_m\right|^2 P_s}{\sum_{m=1}^{M}\left|h_{re_k,m}\right|^2 l_m^2 |w_m|^2 \sigma^2 + \sigma^2}$$
$$= \frac{\mathbf{w}^\dagger\mathbf{B}_k\mathbf{w}}{\mathbf{w}^\dagger\mathbf{H}_k\mathbf{w}+1}\ , \quad (23)$$

trong đó, $\mathbf{B}_k = \left(\frac{P_s}{\sigma^2}\right)\mathbf{D}^\dagger(\mathbf{h}_{sr})\mathbf{h}_{re_k}\mathbf{h}_{re_k}^\dagger\,\mathbf{D}(\mathbf{h}_{sr})$ và $\mathbf{H}_k = \mathbf{D}\left(\mathbf{h}_{re_k}\right)\mathbf{D}^\dagger\left(\mathbf{h}_{re_k}\right)$.

Giá trị *secrecy rate* có thể đạt được khi này sẽ là:

$$R_S = \min_{k=1,\dots,K}\left(I(x_s;\, y_d) - I(x_s; y_{e_k})\right)$$
$$= \min_{k=1,\dots,K}\left(\log(1+\Gamma_d) - \log(1+\Gamma_{e_k})\right).$$

Bài toán cực đại hóa giá trị *secrecy rate* của hệ thống với ràng buộc về tổng công suất truyền của tất cả các relay và/hoặc ràng buộc công suất truyền tối đa tại mỗi relay có dạng như sau:

$$\max_{w}\ \min_{k=1,\dots,K}\left(\log(1+\Gamma_d) - \log(1+\Gamma_{e_k})\right) \quad (24)$$
s.t. $\mathbf{w}^\dagger\mathbf{C}\mathbf{w} \le P_R$,

(và/hoặc $\mathbf{e}_m^\dagger\mathbf{C}\mathbf{w}\mathbf{w}^\dagger\mathbf{e}_m \le p_m, \forall m = 1, \dots, M$).

C. Một số kết quả

1. Trường hợp AF có một trạm nghe lén: Bài toán (19) là một bài toán không lồi (nonconvex) và nhìn chung là khó giải trực tiếp để tìm nghiệm tối ưu toàn cục. Trong [39], các tác giả đã giới thiệu hai phương pháp giải để tìm nghiệm xấp xỉ như sau:

Từ bài toán (19) và bỏ qua hàm log ta có bài toán tương đương như sau:

$$\max_{w}\left(\frac{\mathbf{w}^\dagger\mathbf{H}\mathbf{w}+1}{\mathbf{w}^\dagger\mathbf{G}\mathbf{w}+1} \times \frac{\mathbf{w}^\dagger\mathbf{A}\mathbf{w}+\mathbf{w}^\dagger\mathbf{G}\mathbf{w}+1}{\mathbf{w}^\dagger\mathbf{B}\mathbf{w}+i+1}\right) (25)$$
s.t. $\mathbf{w}^\dagger\mathbf{C}\mathbf{w} \le P_R$,

(và/hoặc $\mathbf{e}_m^\dagger\mathbf{C}\mathbf{w}\mathbf{w}^\dagger\mathbf{e}_m \le p_m, \forall m = 1, \dots, M$).

Bằng cách đặt $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$, ta có bài toán tương đương sau:

$$\max_{w}\left(\frac{tr(\mathbf{H}\mathbf{W})+1}{tr(\mathbf{G}\mathbf{W})+1} \times \frac{tr\left((\mathbf{A}+\mathbf{G})\mathbf{W}\right)+1}{tr\left((\mathbf{B}+\mathbf{H})\mathbf{W}\right)+1}\right) \quad (26)$$
s.t. $tr(\mathbf{C}\mathbf{W}) \le P_r$,

$rank(\mathbf{W}) = 1$,

$\mathbf{W} \succcurlyeq 0$,

(và/hoặc $tr(\mathbf{e}_m\mathbf{e}_m^\dagger\mathbf{C}\mathbf{W}) \le p_m, \forall m = 1, \dots, M$).

Chú ý rằng, nếu $rank(\mathbf{W}) = 1$ và $\mathbf{W}$ là ma trận đối xứng nửa xác định dương (symmetric positive semidefinite) thì $\mathbf{w}^\dagger\mathbf{A}\mathbf{w} = tr(\mathbf{A}\mathbf{W})$ với mọi ma trận $\mathbf{A}$. Bài toán (26) vẫn là bài toán rất khó giải trực tiếp để tìm nghiệm toàn cục, đặc biệt với ràng buộc $rank(\mathbf{W}) = 1$, nên thông thường bài toán (26) được giải tìm nghiệm xấp xỉ bằng cách bỏ qua ràng buộc này. Khi bỏ qua ràng buộc $rank(\mathbf{W}) = 1$, các tác giả trong [39] đề xuất cách giải để tìm nghiệm suboptimal (achievable secrecry rate) và nghiệm xấp xỉ bằng phương pháp SDP (SemiDefinite Programming) như sau:

Bằng cách đặt $t_1 = \frac{tr\left((\mathbf{A}+\mathbf{G})\mathbf{W}\right)+1}{tr\left((\mathbf{B}+\mathbf{H})\mathbf{W}\right)+1}$ và $t_2 = \frac{tr(\mathbf{H}\mathbf{W})+1}{tr(\mathbf{G}\mathbf{W})+1}$, bài toán (26) được biểu diễn về dạng sau:

$$\max_{W,t_1,t_2}\ t_1 t_2 \quad (27)$$
s.t. $tr\left(\mathbf{W}(\mathbf{H} - t_2\mathbf{G})\right) \ge t_2 - 1$

$tr\left(\mathbf{W}\left(\mathbf{A} + \mathbf{G} - t_1(\mathbf{B}+\mathbf{H})\right)\right) \ge t_1 - 1$

$W \succcurlyeq 0$, $tr(\mathbf{C}\mathbf{W}) \le P_r$,

(và/hoặc $tr(\mathbf{e}_m\mathbf{e}_m^\dagger\mathbf{C}\mathbf{W}) \le p_m, \forall m = 1, \dots, M$).

Xét trường hợp bài toán (27) chỉ quan tâm đến ràng buộc về giới hạn tổng công suất truyền của các relay, chúng ta có thể tính trực tiếp giá trị maximum

của t_1 và t_2 một cách riêng rẽ theo bài toán Rayleigh quotient như sau:

$$t_{1,max} = \max_{\mathbf{w}\mathbf{w}^\dagger \le P_R} \frac{\mathbf{w}^\dagger \mathbf{A}\mathbf{w} + \mathbf{w}^\dagger \mathbf{G}\mathbf{w} + 1}{\mathbf{w}^\dagger \mathbf{B}\mathbf{w} + \mathbf{w}^\dagger \mathbf{H}\mathbf{w} + 1}$$

$$= \max_{\mathbf{w}\mathbf{w}^\dagger \le P_R} \frac{\mathbf{w}^\dagger (\mathbf{A} + \frac{1}{P_R} + \mathbf{G})\mathbf{w}}{\mathbf{w}^\dagger (\mathbf{B} + \frac{1}{P_R} + \mathbf{H})\mathbf{w}}$$

$$= \lambda_{max}\left(\mathbf{A} + \frac{1}{P_R} + \mathbf{G}, \mathbf{B} + \frac{1}{P_R} + \mathbf{H}\right), \quad (28)$$

trong đó, $\lambda_{max}(\mathbf{A}, \mathbf{B})$ là giá trị riêng mở rộng lớn nhất (the largest generalized eigenvalue) của cặp ma trận $(\mathbf{A}, \mathbf{B})$.

Chú ý rằng, với cặp ma trận Hermitian $\mathbf{A}, \mathbf{B} \in C^{n\times n}$ thì cặp giá trị (λ, ψ) được gọi là cặp giá trị riêng, vector riêng mở rộng nếu thỏa mãn $\mathbf{A}\psi = \lambda \mathbf{B}\psi$.

Tương tự như trên, giá trị maximum của t_2 được tính như sau:

$$t_{2,max} = \max_{\mathbf{w}\mathbf{w}^\dagger \le P_R} \frac{\mathbf{w}^\dagger \mathbf{H}\mathbf{w} + 1}{\mathbf{w}^\dagger \mathbf{G}\mathbf{w} + 1} \quad (29)$$

$$= \max_{\mathbf{w}\mathbf{w}^\dagger \le P_R} \frac{\mathbf{w}^\dagger (\frac{1}{P_R} + \mathbf{H})\mathbf{w}}{\mathbf{w}^\dagger (\frac{1}{P_R} + \mathbf{G})\mathbf{w}}$$

$$= \lambda_{max}\left(\frac{1}{P_R} + \mathbf{H}, \frac{1}{P_R} + \mathbf{G}\right). \quad (30)$$

Với $t_{1,max}$ và $t_{2,max}$ được tính độc lập như ở trên thì thông thường các giá trị này sẽ đạt được tại các nghiệm $\mathbf{W} = \mathbf{w}\mathbf{w}^\dagger$ khác nhau. Để tìm giá trị *secrecy rate* có thể đạt được, các tác giả trong [39] đã đưa ra một phương pháp giải như sau: Với giá trị $\mathbf{W}$ ở trên tương ứng với giá trị $t_{1,max}$ chúng ta có thể tính ra giá trị t_2 tương ứng $t_{2,max} = \frac{tr(\mathbf{HW})+1}{tr(\mathbf{GW})+1}$. ($t_{2,max}$ được tính bằng cách thay giá trị $\mathbf{W}$ đạt được từ $t_{1,max}$). Khi này giá trị *secrecy rate* có thể đạt được của mô hình AF có một trạm nghe lén với ràng buộc về tổng công suất truyền tại các relay sẽ là $\log(t_{1,max}t_{2,max})$.

Từ giá trị *achievable secrecry rate* ở trên, trong [39] tiếp tục đề xuất thuật toán tìm kiếm quay vòng (iteratively search) trên t_1 và t_2 để tìm ra giá trị tối ưu $t_{1,opt}$ và $t_{2,opt}$ sao cho tích của t_1t_2 có giá trị lớn nhất bằng bài toán kiểm tra tính khả thi (feasibility problem) sau đây:

Tìm $\mathbf{W}$ (31)

s.t. $tr\big(\mathbf{W}(\mathbf{H} - t_2\mathbf{G})\big) \ge t_2 - 1$

$tr\left(\mathbf{W}\big(\mathbf{A} + \mathbf{G} - t_1(\mathbf{B} + \mathbf{H})\big)\right) \ge t_1 - 1$

$\mathbf{W} \succcurlyeq 0, tr(\mathbf{CW}) \le P_r,$

(xem thuật toán chi tiết trong [39]).

Xét trường hợp bài toán (27) chỉ quan tâm đến ràng buộc về giới hạn công suất truyền riêng rẽ của các relay, tương tự như với ràng buộc về tổng công suất truyền của các relay, các giá trị $t_{1,max}$ và $t_{2,max}$ trước tiên cũng được tính độc lập, tuy nhiên không thể tính trực tiếp qua λ_{max} như ở trên. Cụ thể, $t_{1,max}$ và $t_{2,max}$ được tính như sau:

$$t_{1,max} = \max_{\mathbf{W}, t_1} \frac{tr\big((\mathbf{A} + \mathbf{G})\mathbf{W}\big) + 1}{tr\big((\mathbf{B} + \mathbf{H})\mathbf{W}\big) + 1} \quad (32)$$

s.t. $\mathbf{W} \succcurlyeq 0$,

$$tr\left(\mathbf{W}\big(\mathbf{A} + \mathbf{G} - t_1(\mathbf{B} + \mathbf{H})\big)\right) \ge t_1 - 1$$

$$tr(\mathbf{e}_m\mathbf{e}_m^\dagger \mathbf{CW}) \le p_m, \forall m = 1, \dots, M$$

và

$$t_{2,max} = \max_{\mathbf{W}, t_2} \frac{tr(\mathbf{HW}) + 1}{tr(\mathbf{GW}) + 1} \quad (33)$$

s.t $\mathbf{W} \succcurlyeq 0$,

$$tr\big(\mathbf{W}(\mathbf{H} - t_2\mathbf{G})\big) \ge t_2 - 1$$

$$tr(\mathbf{e}_m\mathbf{e}_m^\dagger \mathbf{CW}) \le p_m, \forall m = 1, \dots, M.$$

Trong thực tế, với mỗi giá trị t_1 thì miền khả thi (feasible set) trong (32) là lồi. Nếu với mỗi giá trị t_1 nhận được mà bài toán convex feasibilty sau đây:

Tìm $\mathbf{W}$ (34)

s.t. $\mathbf{W} \succcurlyeq 0$,

$$tr\left(\mathbf{W}\big(\mathbf{A} + \mathbf{G} - t_1(\mathbf{B} + \mathbf{H})\big)\right) \ge t_1 - 1$$

$$tr(\mathbf{e}_m\mathbf{e}_m^\dagger \mathbf{CW}) \le p_m, \forall m = 1, \dots, M$$

là khả thi (feasible) thì ta có $t_{1,max} \ge t_1$. Ngược lại, nếu bài toán kiểm tra tính khả thi lồi (convex feasibility) ở trên là bất khả thi (infeasible) thì ta có $t_{1,max} < t_1$. Do vậy, chúng ta có thể kiểm tra khi nào thì giá trị tối ưu $t_{1,max}$ của bài toán tối ưu bán lồi (quasiconvex optimization problem) trong (32) là lớn hơn hay nhỏ hơn giá trị đã cho t_1 bằng cách giải bài toán convex feasibility (34).

2. Trường hợp AF có nhiều trạm nghe lén: Trong trường hợp có nhiều trạm nghe lén, các tác giả trong [5] đề xuất phương pháp giải tìm nghiệm suboptimal bằng cách xét trường hợp triệt tiêu hoàn toàn tín hiệu truyền đến các trạm nghe lén trong pha thứ hai và với ràng buộc về tổng công suất truyền của tất cả các relay. Bằng cách đưa thêm giả thiết $\boldsymbol{B}^{\dagger}\boldsymbol{w} = \mathbf{0}_{K\times 1}$, cũng có nghĩa là giá trị SNR tại tất cả các trạm nghe lén đều bằng không ($\Gamma_{e_j} = 0, \forall j \in K$), khi đó bài toán (24) sẽ tương đương với bài toán sau:

$$\max_{\boldsymbol{w}} \left(1 + \frac{\mathbf{w}^{\dagger}\mathbf{A}\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{G}\mathbf{w}+1}\right) \qquad (35)$$

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

$$\mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{K\times 1}$$

và tương đương với bài toán:

$$\max_{\boldsymbol{w}} \left(\frac{\mathbf{w}^{\dagger}\mathbf{A}\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{G}\mathbf{w}+1}\right) \qquad (36)$$

$$\text{s.t. } \mathbf{w}^{\dagger}\mathbf{C}\mathbf{w} = P_R,$$

$$\mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{K\times 1}$$

Nghiệm $\boldsymbol{w}$ thỏa mãn ràng buộc $\mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{K\times 1}$ sẽ có dạng $\mathbf{w} = \mathbf{F}\mathbf{v}$, trong đó $\mathbf{F} \in \mathbb{C}^{M\times(M-K)}$ là ma trận semi-unitary gồm các vector trực gia (orthogonal vectors) từ ma trận $\mathbf{B}^{\dagger}\mathbf{w} \in \mathbb{C}^{(M-K)}$ là vector cột tuỳ ý. Do vậy, bài toán (36) sẽ tương đương với:

$$\max_{\boldsymbol{v}} \left(\frac{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{A}\mathbf{F}\mathbf{v}}{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{G}\mathbf{F}\mathbf{v}+1}\right) \qquad (37)$$

$$\text{s.t. } \mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{A}\mathbf{F}\mathbf{v} = P_R$$

Bài toán (37) cũng là bài toán generalized eigenvector, nghiệm của bài toán (37) sẽ cho giá trị $\mathbf{v} \propto \mathbf{q}$ với $\mathbf{q}$ là unit-norm eigenvector của ma trận $\mathbf{F}^{\dagger}[G + P_R^{-1}C]$ tương ứng với giá trị riêng lớn nhất của nó. Khi này, nghiệm của bài toán gốc sẽ là $\mathbf{w} = \mu\mathbf{F}\mathbf{q}^{\dagger}$ với:

$$\mu = \sqrt{\frac{P_R}{\mathbf{q}^{\dagger}\mathbf{F}^{\dagger}\mathbf{C}\mathbf{F}\mathbf{q}}} \ .$$

Như vậy, các tác giả trong [5] đã chỉ ra cách giải trực tiếp cho trường hợp tín hiệu đến các trạm nghe lén bị triệt tiêu hoàn toàn và với ràng buộc về tổng công suất truyền của các relay.

Trường hợp triệt tiêu tín hiệu đến các trạm nghe lén với ràng buộc về công suất truyền riêng tại mỗi relay được các tác giả trong [37] giới thiệu cách giải sử dụng phương pháp SDR như sau:

Bài toán (24) khi đó tương đương với bài toán

$$\max_{\boldsymbol{w}} \left(1 + \frac{\mathbf{w}^{\dagger}\mathbf{A}\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{G}\mathbf{w}+1}\right) \qquad (38)$$

$$\text{s.t. } \mathbf{B}^{\dagger}\mathbf{w} = \mathbf{0}_{K\times 1}$$

$$\mathbf{e}_m^{\dagger}\mathbf{C}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{e}_m \le p_m, \forall m = 1, \dots, M.$$

Với cách lập luận như ở trên, nghiệm w thoả mãn ràng buộc thứ nhất sẽ có dạng $\mathbf{w} = \mathbf{F}\mathbf{v}$ nên bài toán sẽ có dạng như sau:

$$\min_{\mathbf{v}} \left(\frac{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{A}\mathbf{G}\mathbf{v}+1}{\mathbf{v}^{\dagger}\mathbf{F}^{\dagger}\mathbf{A}\mathbf{F}\mathbf{v}}\right) \qquad (39)$$

$$\text{s.t. } \boldsymbol{e}_m^{\dagger}\boldsymbol{C}\boldsymbol{F}\mathbf{v}\mathbf{v}^{\dagger}\boldsymbol{F}^{\dagger}\boldsymbol{e}_m \le p_m, \forall m = 1, \dots, M.$$

Bài toán (39) có dạng không lồi, nên kỹ thuật SDR [38] và phép biến đổi Charnes-Cooper ([3]) được đề xuất ứng dụng trong trường hợp này. Cụ thể, bài toán (39) được biến đổi tương đương thành:

$$\min_{X,\eta} tr\left(\mathbf{F}^{\dagger}\mathbf{G}\mathbf{F}\mathbf{X}\right) + \eta \qquad (40)$$

$$\text{s.t. } tr\left(\mathbf{F}^{\dagger}\mathbf{A}\mathbf{F}\mathbf{X}\right) = 1$$

$$tr\left(\mathbf{F}^{\dagger}\mathbf{e}_m\ \mathbf{e}_m^{\dagger}\mathbf{C}\mathbf{F}\mathbf{X}\right) \le \eta p_m, \forall m = 1, \dots, M,$$

$$\mathbf{X} \succcurlyeq 0,$$

trong đó, $\mathbf{V} = \mathbf{v}\mathbf{v}^{\dagger}$ và $\mathbf{X} = \eta\mathbf{V}$, $\eta > 0$. Bài toán (40) là bài toán tối ưu lồi, nên có thể giải hiệu quả bằng công cụ CVX. Tuy nhiên, do bỏ đi ràng buộc $rank(\mathbf{X}) = 1$, nên nghiệm tìm được chỉ là nghiệm xấp xỉ.

Trường hợp tổng quát, không triệt tiêu hoàn toàn tín hiệu truyền đến các trạm nghe lén, bài toán sẽ trở nên khó giải hơn. Trong [37], các tác giả đã sử dụng kỹ thuật dùng biến trung gian τ để chuyển bài toán (24) thành:

$$\max_{w,\tau} \left(log\left(1 + \frac{\mathbf{w}^{\dagger}\mathbf{A}\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{G}\mathbf{w}+1}\right) - log\left(\frac{1}{\tau}\right)\right) \qquad (41)$$

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

$$log\left(1 + \frac{\mathbf{w}^{\dagger}\mathbf{B}_k\mathbf{w}}{\mathbf{w}^{\dagger}\mathbf{H}_k\mathbf{w}+1}\right) \le log\left(\frac{1}{\tau}\right), \forall = 1, \dots, K,$$

(và/hoặc $\mathbf{e}_m^{\dagger}\mathbf{C}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{e}_m \le p_m, \forall m = 1, \dots, M$).

Tương đương với bài toán:

$$\min_{w,\tau} \frac{\mathbf{w}^{\dagger}\mathbf{G}\mathbf{w}+1}{(\mathbf{w}^{\dagger}(\mathbf{A}+\mathbf{G})\mathbf{w}+1)\tau} \qquad (42)$$

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

$$\frac{\mathbf{w}^{\dagger}\mathbf{H}_k\mathbf{w}+1}{\mathbf{w}^{\dagger}(\mathbf{B}_k+\mathbf{H}_k)\mathbf{w}+1} \ge \tau, \forall k = 1, \dots, K,$$

(và/hoặc $\mathbf{e}_m^{\dagger}\mathbf{C}\mathbf{w}\mathbf{w}^{\dagger}\mathbf{e}_m \le p_m, \forall m = 1, \dots, M$).

Sử dụng kỹ thuật SDR [38], ta có bài toán tương đương sau:

$$\min_{w,\tau} \frac{tr(\mathbf{G}\mathbf{W})+1}{(tr(\mathbf{w}^{\dagger}(\mathbf{A}+\mathbf{G})\mathbf{W}+1)\tau} \qquad (43)$$

s.t. $\mathrm{tr}(\boldsymbol{C}\boldsymbol{W}) \le P_R$,

$$\frac{tr(\mathbf{H}_k\mathbf{W})+1}{tr((\mathbf{B}_k+\mathbf{H}_k)\mathbf{W})+1} \ge \tau, \forall k = 1, \dots, K,$$

(và/hoặc $tr(\mathbf{e}_m^{\dagger}\mathbf{e}_m\mathbf{C}\mathbf{W}) \le p_m, \forall m1, \dots, M$).

Trong khi bài toán (43) vẫn có dạng không lồi với biến τ, các tác giả trong [37] đã đưa bài toán (43) về dạng bài toán quasi-convex [2] để giải bài toán tối ưu hai mức (two-level optimization problem), mức trong (inner level) là bài toán quasi-convex với biến τ được gắn cố định và mức ngoài (outer level) là bài toán tối ưu đơn biến tương ứng với biến τ.

Bắt đầu từ bài toán inner-level, với biến τ được gán cố định, áp dụng cách biến đổi Charnes-Cooper [3], [17] để đưa bài toán (43) về dạng SDP như sau:

$$\min_{\mathbf{Z},\xi} tr(\mathbf{G}\mathbf{Z}) + \xi \qquad (44)$$

s.t. $tr(\mathbf{C}\mathbf{Z}) \le \xi P_R$,

$\tau(tr(\mathbf{A}+\mathbf{G})\mathbf{Z}+\xi) = 1$

$tr(\mathbf{H}_k\mathbf{W}) + \xi \ge \tau(tr((\mathbf{B}_k+\mathbf{H}_k)\mathbf{W}+\xi),$

$\forall k \in K,$

$\mathbf{Z} \succcurlyeq 0,$

(và/hoặc $tr(\mathbf{e}_m^{\dagger}\mathbf{e}_m\mathbf{C}\mathbf{W}) \le p_m, \forall m1, \dots, M$),

trong đó, $\mathbf{W} = \mathbf{Z}/\xi$, $\mathbf{Z} \succcurlyeq 0$ và $\xi > 0$. Bài toán (44) là convex nên có thể giải hiệu quả bằng các công cụ giải như CVX.

Tiếp theo, với bài toán tối ưu đơn biến τ outer-level có dạng như sau:

$$\min_{\tau} \Phi(\tau) \qquad (45)$$

$$\text{s.t. } \tau_{lb} \le \tau \le \tau_{ub}.$$

Trong đó, $\Phi(\tau)$ là giá trị tối ưu của bài toán (44), và τ_{lb}, τ_{ub} là cận dưới (lower bound) và cận trên (upper bound) của biến τ trong (43). Ta thấy, $\tau_{ub} = 1$ và τ_{lb} có thể là 0 hoặc chặt hơn là $\succ_{min}((\mathbf{A}+\mathbf{G})^{-1}\mathbf{G})$. Bài toán (45) có thể sử dụng kỹ thuật tìm nghiệm tối ưu một chiều (one-dimensional) để tìm nghiệm.

Với cặp nghiệm $(\mathbf{W}^*, \tau^*)$ tìm được theo phương pháp trên của bài toán (43), chúng ta cần lấy ra nghiệm $\mathbf{w}$ từ $\mathbf{W}^*$. Nếu $\mathbf{W}^*$ thoả mãn rank-one thì $\mathbf{w}$ có thể được tính thông qua phân tích giá trị riêng (eigenvalue decomposition). Trường hợp ngược lại, chúng ta có thể áp dụng thủ tục xấp xỉ rank-one cho $\mathbf{W}^*$, ví dụ Gaussian randomization ([38]), để tìm nghiệm $\mathbf{w}$.

IV. KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU

Để tăng hiệu suất truyền tin, cũng như tăng khả năng bảo mật thông tin, các kết quả nghiên cứu trong thời gian gần đây tập trung vào một số hướng như sau:

- Lựa chọn một số antenna tham gia truyền tin (Antenna selection): Để tăng hiệu suất truyền tin, thay vì tất cả các relay hay antenna đều tham gia truyền tin như các mô hình được đề cập ở trên, mô hình hệ thống truyền tin này chỉ sử dụng một số relay, hay một số antenna trong số các relay của hệ thống để tham gia truyền tin [21].

- Kênh đa truy cập có nghe lén (Multiple-access wire-tap channel): Bài toán PLS được nghiên cứu trên kênh đa truy cập có sự xuất hiện người nghe lén [28].

- Không biết trước hệ số kênh truyền (Imperfect channel state information): Trong thực tế, thông tin về hệ số kênh có thể không được biết, hay không được xác định trước bởi người truyền tin trong hệ thống, do đó, các nghiên cứu này mở rộng cho trường hợp kênh truyền không có thông tin trước về hệ số kênh [15].

- Tiếp cận bài toán theo giá trị tỷ số tín hiệu trên nhiễu (SNR approach): Tiếp cận bài toán PLS dựa trên giá trị ngưỡng của tỷ lệ tín hiệu trên tạp âm, theo lý thuyết thông tin, bên thu chỉ có thể giải mã và khôi phục tín hiệu của bên phát khi giá trị SNR lớn hơn một ngưỡng nào đó [27].

- Giải bài toán tối ưu bằng phương pháp giải DC programming and DCA: Thay vì sử dụng các phương pháp giải tìm nghiệm xấp xỉ như giới thiệu ở các phần trên, việc áp dụng phương pháp giải DC Programming and DCA cho các bài toán không lồi đã được nghiên

cứu ứng dụng và cho kết quả khả thi trong thời gian gần đây [31], [32].

Cùng với các giải pháp bảo mật truyền thống dựa trên các thuật toán mật mã, bảo mật tầng vật lý đang được tập trung nghiên cứu để cung cấp một hướng đi khác trong bảo mật truyền tin mạng không dây. Bài báo này đã tổng hợp tình hình phát triển và các kết quả nghiên cứu về lĩnh vực này trong dó tập trung vào hai giao thức được sử dụng phổ biến là DF và AF. Bài báo cung cấp cái nhìn tổng quan về lĩnh vực PLS, thông qua các kết quả nghiên cứu của nhiều nhóm tác giả khác nhau trong nhiều giai đoạn khác nhau. Các tác giả đã cố gắng phân chia nội dung thành các mục để trình bày được đầy đủ và logic, cung cấp tư liệu tổng quan để từ đó có hướng nghiên cứu phù hợp.

TÀI LIỆU THAM KHẢO

[1] Bloch, M., Barros, J. "Physical-layer Security: From Information Theory to security Engineering", Cambridge University Press (2011).

[2] Boyd, S., Vandenberghe, L "Convex optimization. Cambridge", U.K. Cambridge Press (2004).

[3] Charnes, A., Cooper, W.W. "Programming with linear fractional functionals". In: Naval Res. Logist. Quart, vol. 9, pp. 181–186 (Dec 1962).

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

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

[6] Dong, L., Han, Z., Petropulu, A., Poor, H. "Amplify-andforward based cooperation for secure wireless communications". In Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. pp. 2613–2616 (April 2009).

[7] G. Zheng, K. Wong, A.P., Ottersten, B. "Collaborativerelay beamforming with perfect csi Optimum and distributed implementation". IEEE Trans. Signal Process Letters 16(4) (Apr 2009).

[8] G. Zheng, K. Wong, A.P., Ottersten, B. "Robust collaborative-relay beamforming". IEEE Trans. on Signal Proc 57(8) (Aug 2009).

[9] Golub, G., Loan, C.F.V. "Matrix Computations "(3rd ed).Johns Hopkins University Press (1996).

[10] Jing, Y., Jafarkhani, H. "Network beamforming using relays with perfect channel information". Information Theory, IEEE Transactions on 55(6), 2499–2517 (June 2009).

[11] Jorswieck, E., Wolf, A., Gerbracht, S. "Secrecy on the Physical Layer in Wireless Networks", ch. 20. INTECH (2010).

[12] Khisti, A. "Algorithms and architectures for multiuser, multiterminal, and multilayer information theoretic security". Ph.D. thesis, MIT (2008).

[13] Khisti, A., Wornell, G.W. "Secure transmission with multiple antennas: The misome wiretap channel". IEEE Trans. Inf. theory (Aug 2007).

[14] Le Thi, H.A. "DC Programming and DCA". *http://www.lita.univlorraine.fr/ lethi/*

[15] Lei Wang, Yue-ming Cai, L.Z., Yang, W. "Secrecy throughput of miso single-eavesdropper ropper networks with imperfect channel state information". Electronics Letters (15), pp. 1169–1170 (June 2015).

[16] Leung-Yan-Cheong, S.K., Hellman, M.E. "The Gaussian wire-tap channel". IEEE Trans. Inform. theory. Vol. 24(4), pp. 451–456 (July 1978).

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

[18] Li, Z., Trappe, W., Yates, R. "Secrete Communication via Multi-antenna Transmission". In: 41st Annual Conference on Information Sciences and Systems (CISS). pp. 905–910 (2007).

[19] Liu, R., Poor, H.V. "Secrecy capacity region of a multiantenna Gaussian broadcast channel with confidential messages". IEEE Trans. Inform. theory. vol. 55(3), pp. 1235–1249 (Jun 2009).

[20] Lun Dong, Z.H., Petropulu, A., Poor, H.V. "Secure wireless communication via cooperation". In Proc. 46th Annual Allerton Commun., Control, and Computing, Monticello, IL (Sept 2008).

[21] Muhammad Fainan Hanif, M.J., Tran, L.N. "Antenna selection with erroneous convaiance matrices under secrecy constraint". IEEE Transactions on Vehicular Technology (2015).

[22] Oggier, F., Hassibi, B. "The secrecy capacity of the MIMO wiretap channel". IEEE Trans. Inf. theory (Oct 2007).

[23] P. K. Gopala, L.L., Gamal, H.E. "On the secrecy capacity of fading channels". IEEE Trans. Inform. Theory vol. 54(10), pp. 4687–4698 (Oct 2008).

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

[25] R. Liu, I. Maric, P.S., Yates, R.D. "Discrete memoryless interference and broadcast channels

with confidential messages: Secrecy capacity regions". IEEE Trans. Inform. theory. vol. 54(6), pp. 2493–2507 (Jun 2008).

[26] Shafiee, S., Ulukus, S. "Achievable rates in gaussian miso channels with secrecy constraints". In: Information Theory, 2007. ISIT 2007. IEEE International Symposium on. pp. 2466–2470 (June 2007).

[27] Siddhartha Sarma, S.A., Kuri, J. "Secure Communication in Amplify-and-Forward Networks with Multiple Eavesdroppers: Decoding with SNR Thresholds". In: Wireless Pers Commun, Springer New York (2015).

[28] Sonee, A., Hodtani, G.A. "On the secrecy rate region of multiple-access wiretap channel with noncausal side informatiion". IEEE Transactions on infromation forensics and security (6). 2015.

[29] Sturm, J.: Using sedumi 1.02: A matlab toolbox for optimization over symmetric cones., opt. methods and software. Special issue on Interior Point Methods 11-12, pp. 625–653 (1999).

[30] Tekin, E., Yener, A. "The general gaussian multipole access and two-way wire-tap channels: Achievable rates and cooperative jamming". Information Theory, IEEE Transactions on 54(6), 2735–2751 (Jun 2008).

[31] Tran Thi Thuy, Nguyen Nhu Tuan, L.T.H.A., Gely, A. "DC programming and DCA for enhancing physical via relay beamforming strategies". In: Lecture Note in Computer Science LNCS, Springer (March 2016).

[32] Tuan, N.N., Son, D.V.: DC programming and DCA for Enhancing Physical Layer Security in Amplify-andForward Relay Beamforming Networks Based on the SNR Approach. In: Advances in Intelligent Systems and Computing, Springer International Publishing. pp. 23-33 (June 2017).

[33] V. Nassab, S. Shahbazpanahi, A.G., Luo, Z.Q. "Distributed beamforming for relay networks based on second order statistics of the channel state information"". IEEE Trans. On Signal Proc 56(9), 4306–4316 (Sept 2008).

[34] Vishwakarma, S., Chockalingam, A. "Decode-and-forward relay beamforming for security with finite-alphabet input". IEEE Communication Letters 17(5) (May 2013).

[35] Wyner, A.D. "The wire-tap channel". Bell Sys. Tech. Journ. 54, 1355–1387 (1975).

[36] Y. Liang, H.V.P., Shamai, S. "Secure communication over fading channels". IEEE Trans. Inform. Theory 54, pp. 2470– 2492 (June 2008).

[37] Y. Yang, Q. Li, W.K.M.J.G., Ching, P. "Cooperative Secure Beamforming for AF Relay Networks With Multiple Eavesdroppers". In: IEEE Signal Processing Letters. vol. 20, pp. 35–38 (2013).

[38] Z. Q. Luo, W. K. Ma, A.M.C.S.Y.Y., Zhang, S. "Semidefinite relaxatiion of quadratic optimization problems". In: IEEE Signal Processing Mag.,. vol. 27, pp. 20–34 (May 2010).

[39] Zhang, J., Gursoy, M. "Collaborative relay beamforming for secrecy". In: Communications (ICC), 2010 IEEE International Conference on. pp. 1–5 (May 2010).

[40] Zhang, J., Gursoy, M. "Relay beamforming strategies for physical-layer security". In: Information Sciences and Systems (CISS), 2010 44th Annual Conference on. pp. 1–6 (March 2010).

SƠ LƯỢC VỀ TÁC GIẢ

ThS. Nguyễn Như Tuấn

Đơn vị công tác: Tạp chí An toàn thông tin, Ban Cơ yếu Chính phủ.

Email: nguyennhutuan@bcy.gov.vn

Quá trình đào tạo: Nhận bằng Kỹ sư và Thạc sĩ chuyên ngành Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã năm 2000 và 2007. Hiện đang làm Nghiên cứu sinh khoá I 2014 -2018 tại Học viện Kỹ thuật mật mã.

Hướng nghiên cứu hiện nay: Kỹ thuật học máy và khai phá dữ liệu ứng dụng trong an toàn thông tin; An toàn và bảo mật trong điện toán đám mây; Bảo mật dữ liệu tầng vật lý trong mạng truyền tin không dây.

TS. Đặng Vũ Sơn

Đơn vị công tác: Ban Cơ yếu Chính phủ, Hà Nội.

Email: dangvuson@yahoo.com

Nhận bằng Cử nhân Toán học tại Đại học Sư phạm I Hà Nội năm 1981. Nhận bằng Tiến sĩ Toán tại Trung tâm Khoa học và Công nghệ Quân sự năm 2003.

Hướng nghiên cứu hiện nay: Khoa học và công nghệ trong lĩnh vực mật mã; An toàn thông tin.

TS. Nguyễn Ngọc Cương

Đơn vị công tác: Nguyên cán bộ Học viện Kỹ thuật mật mã.

Email:

nguyenngoccuong189@gmail.com

Quá trình đào tạo: Nhận bằng Cử nhân Toán học tại Khoa toán Đại học tổng hợp Hà Nội năm 1972; Nhận bằng Tiến sỹ toán học tại Khoa toán Đại học tổng hợp Hà Nội vào năm 1984.

Hướng nghiên cứu hiện nay: Mật mã khối; Mật mã dòng; Kỹ thuật giấu tin sử dụng mã sửa sai.