Về vấn đề đảm bảo an toàn mạng thông tin vô tuyến theo tiếp cận xử lý tín hiệu nhiều chiều

Đặng Vũ Sơn, Nguyễn Thanh Bình, Nguyễn Hữu Trung

***Tóm tắt*— Trong bài báo này, chúng tôi giới thiệu các đặc điểm của mạng thông tin vô tuyến thế hệ mới và vấn đề bảo mật trong mạng thông tin vô tuyến. Cách xác định tiêu chí bảo mật trong mạng thông tin vô tuyến bao gồm xác suất tách thấp (low probability of detection - LPD), xác suất chặn thấp (low probability of intercept - LPI) và khả năng chống nhiễu phá được trình bày trong nội dung bài báo. Các tác giả cũng giới thiệu bài toán bảo mật theo cách tiếp cận xử lý tín hiệu nhiều chiều và đề xuất thực hiện kiến trúc bảo mật nhiều chiều định nghĩa bằng phần mềm (Multi Dimesional Software Defined Crypto-MD-SDC) độc lập mạng, đồng thời chỉ ra các hướng nghiên cứu tiếp theo trong chủ đề này.**

***Abstract*— In this paper, we will demonstrate the specification of next generation network communications and encryption in the network communication systems. Determining the aspects of encryption in the radio network systems include low probability of detection – LDP, low probability of intercept – LPI and ability interference resist in systems this paper present. The encryption methods by multi-input and multi-output are also recommended and proposed with Multi-Dimensional Software Defined Crypto (MD-SDC), and next simulations researching will be discussed in this paper.**

Từ khóa— MD; MD-SDC; LPD; LPI; MIMO; SDR chống nhiễu phá; tín hiệu nhiều chiều.

I. GIỚI THIỆU

Các vấn đề về bảo mật và an toàn thông tin trong mạng thông tin vô tuyến thế hệ mới đang ngày càng tỏ rõ tầm quan trọng, khi mạng thông tin vô tuyến đang xâm nhập sâu rộng và trở thành các công cụ đắc lực trong các lĩnh vực của đời sống kinh tế - xã hội và an ninh - quốc phòng. Trước kia, bảo mật chỉ được xem như một tính năng mã hóa dữ liệu độc lập, được thực hiện tại lớp vật lý, các giao thức mật mã và được thiết kế, thực thi với điều kiện kết nối vật lý đã được thiết lập không lỗi (error-free). Ngày nay, bài toán mật mã trở nên phức tạp và khó thực hiện khi kiến trúc mạng trở nên tùy biến, phân tán trong môi trường truyền thông hội tụ đa dịch vụ.

Trong những năm gần đây, việc nghiên cứu mạng thông tin vô tuyến tập trung vào hệ thống nhiều anten ở cả bên phát và bên thu (hệ thống nhiều đầu vào, nhiều đầu ra - MIMO) do khả năng tăng hiệu suất sử dụng phổ, khả năng truyền dữ liệu tốc độ cao trong môi trường đa đường (chẳng hạn, trong môi trường indoor) và phân tập MIMO đa anten phân bố cấu hình macro cell, hoặc femto cell (phục vụ hệ thống thông tin di động 5G - massive MIMO). Vấn đề mấu chốt của hệ thống MIMO đã nêu nằm ở quy trình tiền mã hóa tại phía phát và bộ tách khôi phục tại phía thu, với kỹ thuật thông dụng là sử dụng tuyến tính cận tối ưu để cưỡng bức về mức không (zero forcing, ZF) [1]. Đã có nhiều phương pháp tiếp cận đến vấn đề tuyến tính cận tối ưu được đề xuất, tuy nhiên từ khía cạnh lý thuyết, mỗi cách có các thuận lợi, khó khăn khác nhau; nhất là trong trường hợp môi trường truyền thông đa dịch vụ phức tạp có tính phi tuyến thuộc họ thứ 3 (nhiều hiện tượng phi tuyến xảy ra đồng thời, hoặc có những điểm kỳ dị). Điều đó thông thường đòi hỏi một quy trình tuyến tính hóa khá phức tạp, trong đó mô hình động học có cả tham số lẫn bậc biến đổi theo thời gian và đôi khi biến đổi cả cấu trúc mô hình [2], [3], [4].

Về phương thức điều chế, các hệ thống thông tin vô tuyến hiện tại và tương lai đã và đang áp dụng kỹ thuật điều chế đa sóng mang (multicarrier modulation) do khả năng đạt được hiệu quả trong việc sử dụng phổ, tốc độ truyền dẫn cao (IEEE802.11a/WiMax hoặc LTE). Hệ thống thông tin di động 4G (LTE - Advanced systems) ứng dụng kỹ thuật MIMO - OFDM hỗ trợ tốc độ dữ liệu đến 1Gb/s. So với hệ thống 4G, hệ thống 5G phải đạt dung lượng lớn hơn 1000 lần, gấp 10 lần hiệu quả phổ, hiệu quả năng lượng và tốc độ dữ liệu.

Về kiến trúc mạng, truyền thông hợp tác và truyền thông cơ hội (Cognitive Radio Networks), truyền thông đa chặng ứng dụng kỹ thuật vô tuyến định nghĩa bằng phần mềm (Software-Defined Radio – SDR) đang được nghiên cứu ứng dụng trong mạng thông tin vô tuyến thế hệ mới. Các nút mạng được hưởng lợi nhờ sự hợp tác và chuyển tiếp gói, nhưng cũng đặt ra thách thức về tính toàn vẹn của thông tin được truyền qua các nút không tin cậy [5].

Bên cạnh hệ thống thông tin di động, còn tồn tại các hệ thống truyền thông khác như: hệ thống

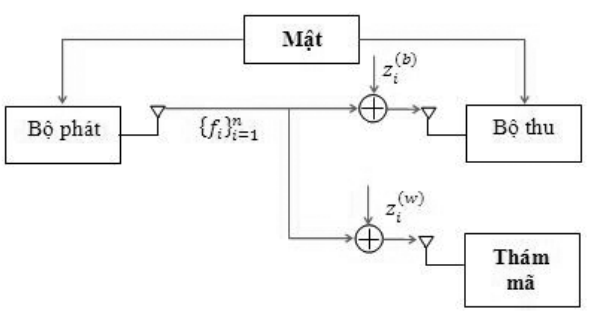
thông tin vô tuyến như WiFi, truyền thông băng thông siêu rộng (UWB) [6], truyền thông bước sóng mm (3–300 GHz), truyền thông ánh sáng nhìn thấy (visible light communications - VLC) (400-490 THz) [7].

Các thách thức truyền thông kể trên đòi hỏi phải có hướng tiếp cận lý thuyết phù hợp làm cơ sở lý luận để thiết kế các thuật toán bảo mật đảm bảo an toàn mạng thông tin vô tuyến, đảm bảo tính ổn định và toàn vẹn dữ liệu khi trao đổi trên môi trường mạng phức tạp hiện nay. Bài báo này gồm bốn mục: Sau Mục I giới thiệu, Mục II phân tích về các tiêu chí bảo mật, yêu cầu bảo mật; Mục III trình bày hướng tiếp cận xử lý tín hiệu nhiều chiều cho bảo mật và toàn vẹn dữ liệu; Mục cuối là kết luận và chỉ ra một số hướng nghiên cứu trong chủ đề này.

II. CÁC TIÊU CHÍ BẢO MẬT MẠNG THÔNG TIN VÔ TUYẾN

Nhiệm vụ quan trọng của bảo mật trong mạng thông tin vô tuyến là bảo vệ nội dung thông tin chống lại các tấn công biến đổi dữ liệu nguồn. Tương ứng với ba mục tiêu quan trọng trong mật mã bao gồm: đảm bảo *tính bảo mật* (secrecy), *tính toàn vẹn* (integrity) và *tính xác thực* (authentication), ba tính năng trong bảo mật mạng thông tin vô tuyến là: Đảm bảo *xác suất tách thấp* (low probability of detection - LPD), *xác suất chặn thấp* (low probability of intercept - LPI) và *khả năng chống nhiễu phá* (anti-jamming protection) [8].

A. Đảm bảo xác suất tách thấp (LPD)



Hình 1. Mô hình hệ thống LPD SISO

Thông thường, dữ liệu phát đi trong mạng thông tin vô tuyến được mã hóa và trao đổi khóa được thực hiện bằng một số giao thức tiêu chuẩn. Nhưng độ bảo mật của phương thức mã hóa tiêu chuẩn chưa đảm bảo, hoặc thậm chí mã mật đã được sử dụng là bền vững nhất về mặt lý thuyết song vẫn có thể bị tấn công bằng các biện pháp nghiệp vụ (tấn công kênh kề). Do vậy, đầu tiên cần phải đảm bảo truyền thông xác suất tách thấp. Tức là đảm bảo khả năng thu chặn tín hiệu của đối tượng do thám là thấp nhất.

Mô hình SISO (single input - single output) như sau: Bộ phát và bộ thu hợp pháp trao đổi khóa mã trước khi truyền dẫn. Bộ phát mã hóa thông tin thành tập các ký hiệu thực $f = \{f_i\}_{i=1}^n$ và phát trên kênh AWGN (Additive white Gaussian noise). Thám mã cố gắng phân loại vector quan sát được trên kênh $\boldsymbol{y}_w$ là vector nhiễu AWGN $\boldsymbol{z}_w = \left\{z_i^{(w)}\right\}_{i=1}^n$ hoặc vector $\left\{f_i + z_i^{(w)}\right\}_{i=1}^n$ tín hiệu phát bị nhiễu.

Khi không xác định được kênh, biện pháp tấn công do thám là đo mức năng lượng trong băng tần B trong khoảng thời gian quan sát Ts. Tín hiệu nhận được cho qua BPF (Band-pass filter), mạch bình phương và mạch tích phân. Sau đó so sánh ngưỡng để phát hiện sự tồn tại của tín hiệu. Mô hình thông dụng là mô hình nhiễu AWGN. Giả thiết không có tín hiệu hoặc có tín hiệu lần lượt là H_0 và H_1 xác định như sau:

$$f_{H_0(y)} = \frac{1}{\sqrt{2\pi}\sigma_n} e^{\left\{\frac{-(y-\mu_n)^2}{2\sigma_n^2}\right\}} \quad (1)$$

$$f_{H_1(y)} = \frac{1}{\sqrt{2\pi}\sigma_{sn}} e^{\left\{\frac{-(y-\mu_{sn})^2}{2\sigma_{sn}^2}\right\}} \quad (2)$$

Trong đó, trị trung bình và phương sai là $\mu_n = 2T_sB$, $\sigma_n^2 = 4T_s$,$\mu_{sn} = 2T_sB + 2$, $\sigma_{sn}^2 = 4T_sB + 4\gamma$ và $\gamma = E/N_0$ là tỉ số S/N.

Để xác định các giới hạn, ta cố định thời gian quan sát và giả thiết số lần quan sát N_s bằng vô cùng, hàm mũ sai lệch Chernoff được định nghĩa là tốc độ giảm hàm mũ của xác suất lỗi tách $P_{\text{det\_err}}$[9]:

$$\rho = \lim \inf_{N_s \to \infty} \frac{1}{N_s} ln P_{\text{det\_err}} \quad (3)$$

$$\rho = \inf_{\alpha \in [0,1]} \liminf_{N_s \to \infty} \frac{1}{N_s} ln \int f_{H_1}^{1-\alpha}(y_1, \dots y_{N_s}) \times f_{H_0}^{\alpha}(y_1, \dots y_{N_s}) dy_1, \dots dy_{N_s}$$

$$= \min_{\alpha \in [0,1]} \left\{(1-\alpha) ln\sigma_n + \alpha ln\sigma_{sn} - \frac{1}{2} ln[(1 - \alpha\sigma n2 + \alpha\sigma sn2 - 1 - \alpha\alpha(\mu sn - \mu n)22(1 - \alpha\sigma n2 + \alpha \sigma sn2) \quad (4)$$

Tổng quát, khó có thể biểu diễn tường minh ρ theo (4). Nhưng đối với thông tin mật mã, ta có thể giả thiết $T_sB \gg \gamma$, từ đó $\sigma_n^2 \approx \sigma_{sn}^2$ và với $\alpha = 1/2$ thì:

$$\rho \approx -\frac{\gamma^2}{4T_sB} \quad (5)$$

Trong thông tin mật mã, cần tránh khả năng tấn công chặn hoặc tách tín hiệu; có nghĩa là đảm bảo công suất phát tối thiểu; nhưng để đối phó với khả năng chống nhiễu phá thì công suất tín hiệu cần

phải lớn. Như vậy cần có sự thỏa hiệp giữa khả năng tách/chặn tín hiệu và khả năng chống nhiễu phá.

B. Đảm bảo xác suất chặn thấp (LPI)

Khả năng chặn bắt tín hiệu được xác định thông qua *dung lượng mật (secrecy capacity)*. Dung lượng mật "lý tưởng" được định nghĩa là tốc độ cực đại sao cho thông tin có thể được giải mã tin cậy tùy ý trong khi tấn công thám mã vô hiệu. Ta xét dung lượng mật (secrecy capacity) của kênh MIMO.

Xét mô hình kênh bảo mật MIMO, trong đó bộ phát sử dụng N_t anten phát, bộ thu sử dụng N_r anten thu và bộ thám mã sử dụng N_e anten. Tín hiệu thu được tại bộ thu và bộ thám mã lần lượt là:

$$\mathrm{Y}^{(i)} = \mathrm{H}^{(i)}\mathrm{X} + \mathrm{W}^{(i)} \text{ với } i = 1,\ldots, I \quad (6)$$

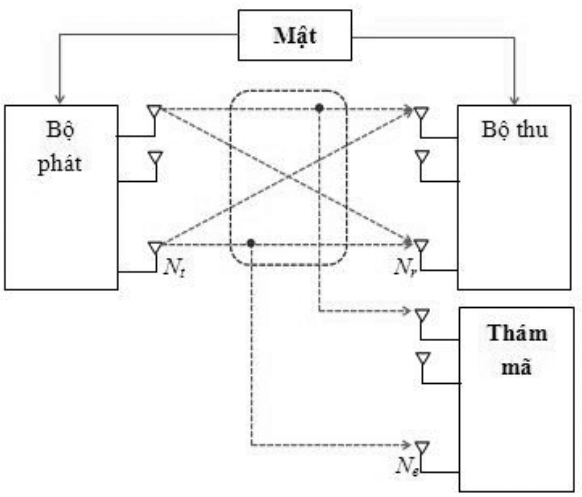
$$\mathrm{Z}^{(k)} = \mathrm{G}^{(k)}\mathrm{X} + \mathrm{E}^{(k)} \text{ với } k = 1,\ldots, K \quad (7)$$

Trong đó, H, G là các ma trận kênh MIMO, W và E là các vector ngẫu nhiên phân bố Gaussian trị trung bình không và hiệp phương sai V_r và V_e. Các ma trận hiệp phương sai V_r và V_e được giả thiết là bán xác định dương. Giả thiết đầu vào kênh thỏa mãn điều kiện cưỡng bức trung bình:

$$\frac{1}{n}\sum_{i=1}^{n} E\left\{\mathrm{X}^{(i)^T}\mathrm{X}^{(i)}\right\} \le \mathrm{P} \quad (8)$$

với j là chỉ số ký hiệu và $(.)^T$ là chuyển vị bù phức; thì dung lượng mật của kênh bảo mật MIMO được xác định bằng [9]:

$$C_S = \max_{\mathbf{Q}:\mathbf{Q}\succcurlyeq 0, Tr(\mathbf{Q})\le P} \min_{i,k} \frac{1}{2}\log \frac{\left|\mathbf{I}+\mathbf{H}^{(i)}\mathbf{Q}\mathbf{H}^{(j)^T}\right|}{\left|\mathbf{I}+\mathbf{G}^{(k)}\mathbf{Q}\mathbf{G}^{(k)^T}\right|} \quad (9)$$



Hình 2. Mô hình kênh bảo mật MIMO

Trong đó, Q là điều kiện ràng buộc của ma trận hiệp phương sai đầu vào (ký hiệu $\mathrm{Q} \succcurlyeq 0$ biểu diễn bán xác định dương) xác định bởi $\frac{1}{n}\sum_{i=1}^{n} \mathrm{C}(\mathrm{X}^{(i)}) \preccurlyeq \mathrm{Q}$ với C(.) là hiệp phương sai tại ký hiệu thứ i. Cách tính dung lượng mật theo (9) trên cơ sở dung lượng mật được xác định bằng:

$$\min_{i,k}\left\{\frac{1}{2}\log\left|\mathrm{I}+\mathrm{H}^{(i)}\mathrm{Q}\mathrm{H}^{(j)^T}\right| - \frac{1}{2}\log\left|\mathrm{I}+\mathrm{G}^{(k)}\mathrm{Q}\mathrm{G}^{(k)^T}\right|\right\} \quad (10)$$

Thực vậy, đối với kênh không nhớ, với xác suất dịch chuyển trạng thái có điều kiện $P\left(\mathrm{Y}^{(i)}, \mathrm{Z}^{(k)}\middle|\mathrm{X}\right)$, dung lượng mật được xác định bằng:

$$C_s = \max_{P(U,\mathbf{X})}\{I(U;\mathbf{Y}^{(i)}) - I(U;\mathbf{Z}^{(k)})\} \quad (11)$$

Với U là biến ngẫu nhiên tùy ý thỏa mãn quan hệ Markov $\rightarrow \mathrm{X} \rightarrow \left(\mathrm{Y}^{(i)}, \mathrm{Z}^{(k)}\right)$. Phần sai lệch có thể cực đại hóa ở biểu thức tính C_s trên được triển khai theo tính chất độc lập của tính phân đường trên đường trong bất kỳ tập kết nối mở với gradient là liên tục:

$$I\left(\mathrm{X};\mathrm{Y}^{(i)}\right) - I\left(\mathrm{X};\mathrm{Z}^{(k)}\right) = \oint_{\mathrm{V}_r}^{\mathrm{V}_e} \mathrm{V}^{-1}\mathrm{K}\mathrm{V}^{-1}\, d\mathrm{V}$$
$$= \oint_{\mathrm{V}_r}^{\mathrm{V}_e} \mathrm{V}^{-1}(\mathrm{K}_G - \mathrm{K}_0)\mathrm{V}^{-1}\, d\mathrm{V} \quad (12)$$

Trong đó, $I(.)$ là *thông tin tương hỗ* (mutual information). $I(X;Y)$ định lượng cho thông tin một biến X có thể truyền tải về biến Y:

$$I(X;Y) = H(X) - H(X|Y) = I(Y;X) \quad (13)$$

Với $H(X)$ ký hiệu *entropy* của biến X và $H(X|Y)$ là entropy có điều kiện của X với Y đã cho. Khi X là biến rời rạc, entropy được tính theo biểu thức sau:

$$H(X) = -\sum_{x\in X} p(x)log_2(p(x)) \quad (14)$$

Và entropy có điều kiện $H(X|Y)$ xác định bởi:

$$H(X|Y) = -\sum_{x\in X}\sum_{y\in Y} p(x,y)log_2\left(p(x|y)\right) \quad (15)$$

Ma trận hiệp phương sai lỗi của bộ ước lượng tối ưu bất kỳ bị giới hạn trên. Ta có K_G là hiệp phương sai lỗi của bộ ước lượng Gaussian kết hợp được xác định bởi $\mathrm{K}_G = \mathrm{V}_x - \mathrm{V}_x(\mathrm{V}_x + \mathrm{V})-1\mathrm{V}x$ với V là ma trận hiệp phương sai của nhiễu AWGN. Và K_0 tùy ý.

$$I\left(\mathrm{X};\mathrm{Y}^{(i)}\right) - I\left(\mathrm{X};\mathrm{Z}^{(k)}\right)$$
$$= \oint_{\mathrm{V}_r}^{\mathrm{V}_e} \mathrm{V}^{-1}\mathrm{K}_G\mathrm{V}^{-1}\, d\mathrm{V} - \oint_{\mathrm{V}_r}^{\mathrm{V}_e} \mathrm{V}^{-1}\mathrm{K}_0\mathrm{V}^{-1}\, d\mathrm{V}$$
$$\le \oint_{\mathrm{V}_r}^{\mathrm{V}_e} \mathrm{V}^{-1}\mathrm{K}_G\mathrm{V}^{-1}\, d\mathrm{V} \quad (16)$$

Ta được biểu thức sau:

$$C_S = \max_{\mathbf{0}\preccurlyeq\mathbf{V}_x\preccurlyeq\mathbf{Q}}\left\{\frac{1}{2}\log|\mathbf{I}+\mathbf{V}_x\mathbf{V}_r^{-1}| - \frac{1}{2}\log|\mathbf{I}+\mathbf{V}_x\mathbf{V}_e^{-1}|\right\}$$
$$= \max_{\mathbf{0}\preccurlyeq\mathbf{V}_x\preccurlyeq\mathbf{Q}}\left\{\frac{1}{2}\log|\mathbf{V}_x+\mathbf{V}_r| - \frac{1}{2}\log|\mathbf{V}_x+\mathbf{V}_e|\right\} + \frac{1}{2}\log\frac{|\mathbf{V}_e|}{|\mathbf{V}_r|}$$

$$= \max_{\mathbf{0} \preccurlyeq \mathbf{V}_x \preccurlyeq \mathbf{Q}} \left\{ -\frac{1}{2} \log \left| \mathbf{I} + (\mathbf{V}_x + \mathbf{V}_r)^{-1} (\mathbf{V}_e - \mathbf{V}_r) \right| \right\} + \frac{1}{2} \log \frac{|\mathbf{V}_e|}{|\mathbf{V}_r|}$$

$$= \frac{1}{2} \log \left| \mathbf{I} + \mathbf{Q} \mathbf{V}_r^{-1} \right| - \frac{1}{2} \log \left| \mathbf{I} + \mathbf{Q} \mathbf{V}_e^{-1} \right| \quad (17)$$

C. Khả năng chống nhiễu phá (anti-jamming protection)

Khả năng chống nhiễu phá thường được thể hiện trong các hệ thống thông tin trải phổ (DSSS) thông qua *tăng ích xử lý* (Processing Gain - PG). Vì vậy, để phân tích khái niệm tăng ích xử lý và ý nghĩa của nó đối với các hệ thống thông tin trải phổ, đầu tiên ta xét tập *D* các tín hiệu trực giao $s_i(t)$ với *i* = i, 2, ..., *D*. Trong không gian *N* chiều với *N*>>*D*, ta có thể viết:

$$s_i(t) = \sum_{j=1}^{N} a_{ij} \varphi_j(t) \quad i = 1, 2, ..., D \quad (18)$$

với:

$$a_{ij} = \int_0^T s_i(t) \varphi_j(t) dt \quad (19)$$

và:

$$\int_0^T \varphi_j(t) \varphi_k(t) dt = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases} \quad (20)$$

Tập $\{\varphi_j(t)\}$ là độc lập tuyến tính trải trong không gian *N* chiều trực giao (còn gọi là cơ sở). Với mỗi ký hiệu thông tin phát đi, một tập các hệ số $\{a_{ij}\}$ được chọn độc lập để giấu tín hiệu *D* chiều trong không gian N chiều rộng lớn.Tập các biến ngẫu nhiên $\{a_{ij}\}$ giả thiết có các giá trị ±*a* với xác suất 1/2. Tất nhiên, bộ thu có thể truy nhập đến từng hệ số được chọn để giải trải phổ.

Năng lượng trung bình cho mỗi ký hiệu:

$$E_s = \int_0^T s_i^2(t) dt = \sum_{j=1}^{N} \overline{a_{ij}^2} \qquad i = 1, 2, ..., D \quad (21)$$

Các hệ số độc lập trị trung bình không và tương quan:

$$\overline{a_{ij} a_{ik}} = \begin{cases} \frac{E_s}{N} & j = k \\ 0 & khác \end{cases} \quad (22)$$

Nhiễu phá không có thông tin gì về việc lựa chọn các hệ số $\{a_{ij}\}$. Các hệ số phân bố đơn điệu trên *N* tọa độ cơ sở. Nếu nhiễu phá chọn phân bố năng lượng đều trên toàn bộ không gian tín hiệu thì tín hiệu nhiễu phá:

$$\omega(t) = \sum_{j=1}^{N} b_j \varphi_i(t) \quad (23)$$

Năng lượng tổng:

$$E_w = \int_0^T \omega^2(t) dt = \sum_{j=1}^{N} b_j^2 \quad (24)$$

Tại bộ thu:

$$r(t) = s_i(t) + \omega(t) \quad (25)$$

được tương quan với tập các tín hiệu có thể phát đi. Đầu ra của bộ tương quan thứ *i* là:

$$z_i = \int_0^T r(t) s_i(t) dt = \sum_{j=1}^{N} a_{ij}^2 + b_j a_{ij} \quad (26)$$

trong đó, thành phần $b_j a_{ij}$ có trị trung bình không.

Giả thiết tín hiệu *m* là $s_m(t)$ được phát đi, giá trị trung bình ở đầu ra sẽ là:

$$E(z_i \mid s_m) = \sum_{j=1}^{N} \overline{a_{ij}^2} = \begin{cases} E_s & i = m \\ 0 & khác \end{cases} \quad (27)$$

Giả thiết *D* tín hiệu là giống nhau, đầu ra của bất kỳ bộ tương quan:

$$E(z_i) = \frac{E_s}{D} \quad (28)$$

Phương sai:

$$\text{var}(z_i \mid s_i) = \sum_{j,k} b_j b_k \overline{a_{ij} a_{ik}} = \sum_{j=1}^{N} b_j^2 a_{ij}^2 = \sum_{j=1}^{N} b_j^2 \frac{E_s}{N} = \frac{E_N E_s}{N} \quad (29)$$

Phương sai ở đầu ra của bộ tương quan *i* là $\text{var}(z_i|s_m)$. Tín hiệu s_m phát:

$$\text{var}(z_i \mid s_m) = \frac{E_w E_s}{N} + \frac{E_s^2}{N} \quad (30)$$

Tỷ số công suất tín hiệu cho công suất nhiễu phá:

$$SJR = \sum_{m=1}^{D} \frac{E^2(Z_i | S_m)}{\text{var}(Z_i | S_m)} = \frac{\frac{E_s^2}{D}}{\frac{E_w E_s}{N}} = \frac{E_s N}{E_w D} \quad (31)$$

Xác suất của tín hiệu *m*:

$$P(s_m) = \frac{1}{D} \quad (32)$$

Tỷ số $\frac{N}{D}$ được gọi là tăng ích xử lý, biểu diễn ưu điểm của hệ thống. Rõ ràng nếu không tiến hành trải phổ tín hiệu thì tỷ số SJR chỉ là $SJR = \frac{E_s}{E_w}$ nhưng khi tiến hành trải phổ thì tỷ số này được cải thiện thêm $\frac{N}{D}$ lần (tất nhiên trả giá là băng tần hệ thống mở rộng). Đối với tín hiệu có băng tần hữu hạn *W* và chu kỳ *T* thì số chiều của tín hiệu này là 2*WT*, do đó:

$$PG = \frac{N}{D} = \frac{2W_{ss}T}{2W_{\min}T} = \frac{W_{ss}}{R} \quad (33)$$

III. BÀI TOÁN BẢO MẬT THÔNG TIN DƯỚI GÓC ĐỘ XỬ LÝ TÍN HIỆU NHIỀU CHIỀU

A. Xử lý tín hiệu nhiều chiều

Tổng quát, tín hiệu nhiều chiều (Multidimensional - MD) là tín hiệu có miền $\mathrm{t} = (t_1, t_2, \dots t_M) \in \mathbb{R}^M$ và biểu diễn được trong miền tần số phức *s* bằng biến đổi Laplace [11]:

$$W(\mathrm{s}) = \frac{1}{(2\pi)^M} \int \omega(\mathrm{t}) e^{-\mathrm{s}^T \mathrm{t}} d\mathrm{t} \qquad (34)$$

Trong đó, ta có thể biểu diễn miền phức $\mathrm{s} = (s_1, s_2, \dots s_M) \in \mathbb{C}^M$ là ma trận cột $\mathrm{s} \triangleq [s_1 \;\; s_2 \;\; \cdots \;\; s_M]^T$. Biến đổi Fourier tương ứng của $\omega(\mathrm{t})$ là $W(j\omega)$ với $\omega \triangleq [\omega_1 \;\; \omega_2 \;\; \cdots \;\; \omega_M]^T$. Thông thường, ta xét tín hiệu 4D thời gian-không gian (*x, y, z, ct*) trong đó *t* là thời gian, $(x, y, z) \in \mathbb{R}^M$ với $M = 3$ là không gian tọa độ 3D và *c* là tốc độ ánh sáng. Quan hệ 4D giữa tín hiệu vào $w_a(\mathrm{t})$ có miền liên tục của bộ lọc tuyến tính dịch bất biến thời gian - không gian và tín hiệu ra nhân quả $y_a(\mathrm{t})$ với $\mathrm{t} \triangleq (x, y, z, ct) \in \mathbb{R}^4$ xác định bởi phương trình vi phân từng phần 4D bậc (N_x, N_y, N_z, N_{ct}) [10]:

$$\sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} p_{jklm} \frac{\partial^m}{\partial (ct)} \frac{\partial^l}{\partial z} \frac{\partial^k}{\partial y} \frac{\partial^j}{\partial x} [w_a(\mathrm{t})] \qquad (35)$$

$$= \sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} q_{jklm} \frac{\partial^m}{\partial (ct)} \frac{\partial^l}{\partial z} \frac{\partial^k}{\partial y} \frac{\partial^j}{\partial x} [y_a(\mathrm{t})] \qquad (36)$$

Trong biểu diễn này, $\frac{\partial^0 [w_a(\mathrm{t})]}{\partial t_i} = w_a(\mathrm{t})$ và $q_{0000} = 1$.Tập $\{p_{jklm}, q_{jklm}\}$ gồm $(2N_xN_yN_zN_{ct} - 1$ hệ số hằng là các thành phần trọng số được lựa chọn xấp xỉ hóa quan hệ vào - ra của hệ thống nhiều chiều này. Điều kiện biên và các trạng thái nội của bộ lọc được thiết lập sao cho hàm truyền đạt của hệ là compact support. Biến đổi Laplace:

$$\sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} p_{jklm} s_x^j s_y^k s_z^l s_{ct}^m W_a(\mathrm{s}) \qquad (37)$$

$$= \sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} q_{jklm} s_x^j s_y^k s_z^l s_{ct}^m Y_a(\mathrm{s}) \qquad (38)$$

Hàm truyền đạt 4D:

$$T(\mathrm{s}) = \frac{Y_a(\mathbf{s})}{W_a(\mathbf{s})} = \sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} \frac{p_{jklm} s_x^j s_y^k s_z^l s_{ct}^m}{q_{jklm} s_x^j s_y^k s_z^l s_{ct}^m} \qquad (39)$$

Trong đó, hàm truyền đạt của biến đổi Fourier 4D là $T(j\omega) = T(j\omega_x, j\omega_y, j\omega_z, j\omega_{ct})$, tức là phổ năng lượng liên quan đến:

$$\psi Y(\omega) = |T(j\omega)|^2 \psi w(\omega) \qquad (40)$$

Quan hệ vào, ra của bộ lọc miền rời rạc xác định bởi phương trình sai phân 4D:

$$\sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} a_{jklm} w(n_x - j, n_y - k, n_z - l, n_{ct} - m) = \sum_{m=0}^{N_{ct}} \sum_{l=0}^{N_z} \sum_{k=0}^{N_y} \sum_{j=0}^{N_x} b_{jklm} y(n_x - j, n_y - k, nz - l, nct - m \qquad (41)$$

Lưu ý:

$$w(n_x, n_y, n_z, n_{ct},) \triangleq \omega_a(n_x \Delta \mathrm{x}, n_y \Delta \mathrm{y}, n_z \Delta \mathrm{z}, n_{ct} \Delta \mathrm{T}) \qquad (42)$$

Và

$$y(n_x, n_y, n_z, n_{ct},) \triangleq Y_a(n_x \Delta \mathrm{x}, n_y \Delta \mathrm{y}, n_z \Delta \mathrm{z}, n_{ct} \Delta \mathrm{T}) \qquad (43)$$

Lấy biến đổi z ta có hàm truyền đạt miền rời rạc:

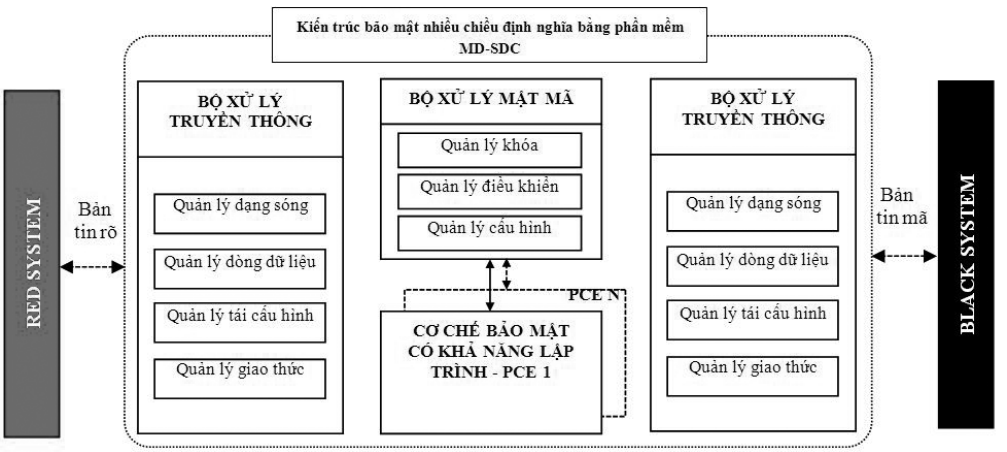
$$H(z_x, z_y, z_z, z_{ct}) \triangleq \frac{Y(z_x, z_y, z_z, z_{ct})}{W(z_x, z_y, z_z, z_{ct})} = \sum_{m=0}^{N_{ct}-1} \sum_{l=0}^{N_z-1} \sum_{k=0}^{N_y-1} \sum_{j=0}^{N_x-1} \frac{a_{jklm} z_x^{-j} z_y^{-k} z_z^{-l} z_{ct}^{-m}}{b_{jklm} z_x^{-j} z_y^{-k} z_z^{-l} z_{ct}^{-m}} \qquad (44)$$

Với $b_{0000} = 1$.

B. Bài toán bảo mật thông tin dưới góc độ hệ thống

Bản chất của việc thực hiện bảo mật thông tin là trong quá trình gia công, xử lý hoặc truyền thông tin, những khóa mật mã được cài vào một cách thích hợp. Tuy những phương thức bảo mật thông tin và những khóa mật mã là ngẫu nhiên, nhưng vẫn phải thỏa mãn yêu cầu nào đó để đối tượng nhận tin hoàn toàn có thể giải mã. Vì vậy, dù bằng bất cứ phương thức nào, việc bảo mật thông tin cũng có thể xem như là nhiễu xạ có quy luật lên tín hiệu đầu vào. Điều đó đòi hỏi rằng, dù chất lượng truyền thông của mạng có bị thay đổi thì quy luật gây nhiễu xạ lên tín hiệu vẫn được bảo toàn để cho mạng quản lý và đối tượng sử dụng có thể giải mật [11].

Thực chất của bài toán bảo mật thông tin là tìm cách thức mô tả toán học cho cơ chế động học truyền thông có tín hiệu bảo mật của hệ các phần tử trong mạng. Nghiệm của bài toán là các tham



Hình 3. Kiến trúc bảo mật thông tin nhiều chiều cho mạng thông tin vô tuyến thế hệ mới

số của mô hình toán học mô tả quá trình bảo đảm mật mã để quy trình bảo mật thông tin có tính ổn định, có thể đồng thời điều khiển và quan sát.

C. Đề xuất kiến trúc bảo mật thông tin nhiều chiều cho mạng thông tin vô tuyến thế hệ mới

Các thách thức mà hệ thống bảo mật phải đương đầu nêu ở trên có thể tóm tắt như sau:

- Kiến trúc đa giao thức (Multi-Protocol): Hệ thống thông tin phục vụ nhiều giao thức truyền thông khác nhau theo các ngữ cảnh phục vụ khác nhau.
- Kiến trúc đa kênh (Multi-Channel): Dữ liệu được phát trên nhiều sóng mang khác nhau nhằm tối ưu hóa hiệu quả phổ.
- Vô tuyến điều khiển bằng phần mềm SDR.
- Vô tuyến hợp tác và truyền thông cơ hội (Cognitive Radio).

Từ đó, chúng tôi đề xuất kiến trúc bảo mật định nghĩa bằng phần mềm (MD-SDC) độc lập mạng (Network-Independent) như biểu diễn trên Hình 3. Bộ xử lý truyền thông hỗ trợ các chức năng quản lý dạng sóng điều chế, quản lý dòng dữ liệu, quản lý tái cấu hình và quản lý giao thức sao cho có thể thích nghi được với các giao thức truyền thông khác nhau, tức là đáp ứng tiêu chí độc lập mạng.

Nhân của kiến trúc là các cơ chế bảo mật có khả năng lập trình (Programmable Crypto Engine - PCE). Có N lõi tương ứng với N chiều dữ liệu có thể xử lý. Mỗi lõi có thể mã hóa theo một thuật toán bảo mật và bộ thông số của nó được thay đổi thông qua bộ xử lý mật mã.

IV. KẾT LUẬN

Trong các giải pháp bảo mật, bảo mật thông tin lớp vật lý (physical layer security) là hết sức quan trọng, vì phương pháp này có thể ngăn chặn được tấn công trực tiếp (loại phổ biến nhất), hạn chế truy nhập và như vậy sẽ góp phần nâng cao độ bảo mật của mạng thông tin vô tuyến thế hệ mới.

Trong bài báo này, chúng tôi đã trình bày các tiêu chí bảo mật mạng thông tin vô tuyến bao gồm xác suất tách thấp LPD, xác suất chặn thấp LPI, khả năng chống nhiễu phá, cũng như đề xuất mô hình thực hiện kiến trúc bảo mật nhiều chiều định nghĩa bằng phần mềm (MD-SDC) độc lập mạng, cho phép thích nghi được với các loại hình mạng cũng như tối ưu năng lực bảo mật của hệ thống.

Trên cơ sở kết quả đã phân tích, cần tiếp tục tiến hành nghiên cứu các vấn đề liên quan đến giải pháp mã hoá nhiều chiều - đa lõi, nhằm mục tiêu đảm bảo an toàn thông tin và tính khả dụng hợp lý đối với các cấp độ bảo mật bao gồm: Mức thấp; Mức trung bình; Mức cao. Bài toán mật mã nhiều chiều trong mạng thông tin vô tuyến cần phát triển mô hình dưới góc độ động học hệ thống (tức là theo quan điểm mô hình hệ thống xét trạng thái động học dưới tác động của các tấn công tổng lực mạng). Phát triển thực nghiệm hệ thống, nhiều lõi (multi-core) trên cơ sở các công nghệ chip hoặc FPGA/DSP. Trong đó, trường hợp nghiên cứu khả thi có thể là dựa trên AES Multi-core. Hướng tiếp cận này hứa hẹn nhiều kết quả khả quan trong lĩnh vực bảo mật thông tin vô tuyến.

TÀI LIỆU THAM KHẢO

[1]. F. Khalid and J. Speidel, “Advances in MIMO techniques for mobile communications- Asurvey”, Int'l J. of Communications, Network and System Sciences, vol. 3, pp. 213-252, March 2010.

[2]. P. S. Udupa and J. S. Lehnert, “Optimizing zero-forcing precoders for MIMO broadcast systems”, IEEE Trans. Commun., vol. 55, no. 8, pp. 1516-1524, Aug. 2007.

[3]. K.-H. Park, Y.-C. Ko, M.-S. Alouini, and J. Kim, “Low complexity coordinated beamforming in 2-user

MIMO systems", inProc. Commu-nications, IEEE International Conference on, Dresden, Germany, Jun. 2009.
[4]. M. Joham, W. Utschick, and J. A. Nossek, "Linear transmit processing in MIMO communications systems", IEEE Trans. Signal Process., vol. 53, no. 8, pp. 2700-2712, Aug. 2005.
[5]. Xiang He, Aylin Yener, "Two-hop communication using an untrusted relay", EURASIP Journal on Wireless Communications and Networking, pp. 13, vol. 2009.
[6]. Yanbing Zhang, Huaiyu Dai, "A Real Or thogonal Space-Time Coded UWB Scheme for Wireless Secure Communications", EURASIP Journal on Wireless Communications and Networking, vol. 2009.
[7]. S. Rajagopal, R.D. Roberts, Sang-Kyu Lim, "IEEE 802.15.7 visible light communication: modulation schemes and dimming support", IEEE Communications Magazine, vol. 50, Issue 3, pp. 72 - 82, 2012.
[8]. Vandendorpe L., "Multitone spread spectrum multiple access communications system in a multipath Rician fading channel", IEEE Transactions on Vehicular Technology, vol. 44, pp. 327 - 337, May 1995. Man Young Rhee (2003), Internet Security, Cryptographic Principles, Algorithms and Protocols, Willey.
[9]. Ruoheng Liu, H. Vincent Poor, and Shlomo Shamai (Shitz), "An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel", EURASIP Journal on Wireless Communications and Networking, vol. 2009.
[10]. Leonard T. Bruton, and Stefan B. Williams, "Multidimensional (MD) Circuits and Systems for Emerging Applications Including Cognitive Radio, Radio Astronomy, Robot Vision and Imaging", IEEE Circuit and Systems Magazine, First quarter 2013.
[11]. Yingbin Liang, Gerhard Kramer, H. Vincent Poor, Shlomo Shamai (Shitz), "Compound Wiretap Channels", EURASIP Journal on Wireless Communications and Networking, vol. 2009.

SƠ LƯỢC VỀ TÁC GIẢ

TS. Đặng Vũ Sơn

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

E-mail: dangvuson@yahoo.com

Tốt nghiệp chuyên ngành Toán học, 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

PGS. TS. Nguyễn Hữu Trung

Đơn vị công tác: Viện Điện tử - Viễn Thông, Đại học Bách khoa Hà Nội, Hà Nội.

E-mail: Trung.nguyenhuu@hust.edu.vn

Tốt nghiệp chuyên ngành Điện tử - viễn thông, Đại học Bách khoa Hà Nội năm 1996. Tốt nghiệp Thạc sĩ và Tiến sĩ Điện tử - Viễn thông tại Đại học Bách khoa Hà Nội năm 1998 và 2004. Được phong hàm Phó Giáo Sư chuyên ngành Điện tử Viễn thông, ngành Điện - Điện tử - Tự động hóa năm 2010.

Hướng nghiên cứu hiện nay: Xử lý tín hiệu, Công nghệ nhúng, Công nghệ FPGS, Công nghệ DSP.

ThS. Nguyễn Thanh Bình

Đơn vị công tác: Vụ Khoa học - Công nghệ, Ban Cơ yếu Chính phủ, Hà Nội.

Email: binhbcy@gmail.com

Tốt nghiệp Học viện Kỹ thuật Mật mã năm 1996. Nhận bằng Thạc sĩ tại Học viện Kỹ thuật Quân sự năm 2003. Đang là nghiên cứu sinh của Học viện Công nghệ Bưu chính Viễn thông.

Hướng nghiên cứu hiện nay: Thông tin vô tuyến, Mạng di động GSM, Mạng vô tuyến Wireless, công nghệ mật mã.