BẢO MẬT LỚP VẬT LÝ TRONG MẠNG KHÔNG DÂY

Trương Tiến Vũ[a*], Trần Đức Dũng[a], Hà Đắc Bình[a], Võ Nhân Văn[a]

[a]Khoa Công nghệ Thông tin,Trường Đại học Duy Tân, Đà Nẵng, Việt Nam

Nhận ngày 04 tháng 01 năm 2016
Chỉnh sửa lần 01 ngày 17 tháng 03 năm 2016 | Chỉnh sửa lần 02 ngày 19 tháng 03 năm 2016
Chấp nhận đăng ngày 31 tháng 03 năm 2016

Tóm tắt

Trong bài báo này, chúng tôi trình bày cách tiếp cận để giải quyết vấn đề bảo mật trong mạng không dây ở lớp vật lý. Để áp dụng các cách tiếp cận này, chúng tôi xét mô hình mạng truyền thông không dây MISO (Multi Input-Single Output) có nhiễu giả và sử dụng kênh truyền không đồng nhất Rayleigh/Rician. Để đánh giá hiệu năng bảo mật của mô hình, chúng tôi phân tích, đánh giá các yếu tố: dung lượng bảo mật, xác suất bảo mật, xác suất dừng bảo mật của hệ thống và kiểm chứng kết quả tính toán với kết quả mô phỏng theo phương pháp Monte-Carlo. Kết quả nghiên cứu này cho thấy tính khả thi của việc triển khai bảo mật ở lớp vật lý trong mạng không dây và đánh giá được hiệu năng bảo mật của mô hình đề xuất.

Từ khóa: Bảo mật lớp vật lý; Dung lượng bảo mật; Xác suất bảo mật; Xác suất dừng bảo mật.

1. GIỚI THIỆU

Trong môi trường mạng không dây, do tính chất truyền quảng bá làm cho mạng dễ bị tấn công, nghe lén thông qua giao tiếp không dây. Các phương pháp bảo mật hiện tại là áp dụng các kỹ thuật mã hóa, xác thực phức tạp (như WEP, WPA…) và thường được triển khai ở lớp ứng dụng. Nhưng các giải pháp bảo mật trên ngày càng khó triển khai, kém hiệu quả do các yêu cầu tích hợp, kỹ thuật tính toán và phương thức tấn công mạng không dây thay đổi không ngừng.

Để giải quyết vấn đề trên, một hướng nghiên cứu mới đang được quan tâm nhằm tìm ra các giải pháp tăng cường khả năng bảo mật cho mạng không dây ở lớp vật lý (PHY Secrecy). Hướng tiếp cận bảo mật lớp vật lý xây dựng dựa trên lý thuyết bảo mật thông tin, với nguyên lý cơ bản: một hệ thống truyền thông không dây có khả năng bảo

* Tác giả liên hệ: Email: truongtienvu@dtu.edu.vn

mật nếu dung lượng kênh truyền hợp pháp lớn hơn dung lượng kênh truyền bất hợp pháp [1-2].

Cách tiếp cận này tuy đơn giản nhưng hiệu quả do tập trung giải quyết vấn đề bảo mật ngay ở mức thông tin nhằm hạn chế khả năng thu nhận thông tin bất hợp pháp.

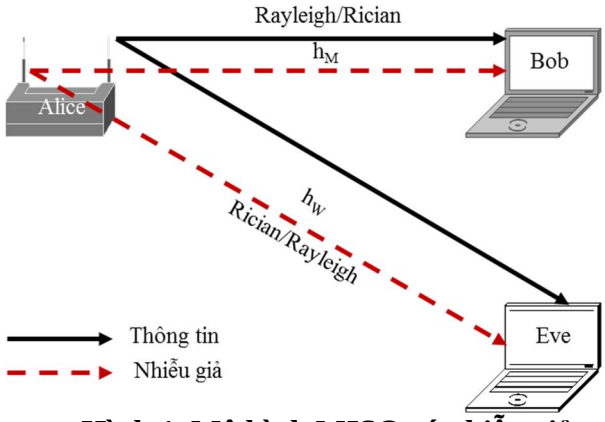
Có 3 hướng nghiên cứu chính trong bảo mật thông tin lớp vật lý bao gồm: bảo mật thông tin lớp vật lý dựa trên khóa bảo mật (Key-Based Secrecy) [3-5], bảo mật thông tin lớp vật lý không sử dụng khóa bảo mật (Keyless Secrecy) [6-8] và nghiên cứu các phương pháp đánh giá khả năng đảm bảo an toàn thông tin ở lớp vật lý [9-10].

Trong phần nghiên cứu liên quan, chúng tôi xét mô hình mạng truyền thông không dây MISO có sử dụng nhiễu giả, kênh truyền pha-đinh không đồng nhất Rayleigh/Rician. Để đánh giá hiệu năng bảo mật của mô hình chúng tôi phân tích, đánh giá các yếu tố: dung lượng bảo mật, xác suất bảo mật, xác suất dừng bảo mật của hệ thống và kiểm chứng kết quả tính toán với kết quả mô phỏng theo phương pháp Monte-Carlo.

Phần còn lại của bài báo được trình bày như sau: phần 2 trình bày mô hình hệ thống và kênh truyền, phần 3 phân tích hiệu năng bảo mật của hệ thống, phần 4 trình bày kết quả mô phỏng, phần 5 trình bày kết luận và định hướng phát triển của nghiên cứu này.

2. MÔ HÌNH HỆ THỐNG VÀ KÊNH TRUYỀN

Xét mô hình hệ thống như Hình 1, Alice là thiết bị phát thông tin sử dụng 2 ăng-ten, một ăng-ten để phát thông tin và một ăng-ten để phát nhiễu giả với công suất bằng nhau bằng và bằng P/2. Bob là thiết bị thu hợp pháp sử dụng kênh truyền pha-đinh Rayleigh/Rician, giả sử Bob có khả năng loại bỏ nhiễu giả. Trong khi đó, Eve là thiết bị thu bất hợp pháp sử dụng kênh truyền pha-đinh Rician/Rayleigh và do là thiết bị bất hợp pháp nên Eve không có khả năng nhận biết và khử nhiễu giả.



Hình 1. Mô hình MISO có nhiễu giả

Khi Alice phát thông tin $x_0(t)$ và nhiễu giả $x_1(t)$ thì tín hiệu thu nhận được tại Bob *y(t)* và tín hiệu nhận được tại Eve *z(t)* được tính như sau:

$$y(t) = h_M x_0(t) + h_M x_1(t) + 2n_M \quad (1)$$

$$z(t) = h_W x_0(t) + h_W x_1(t) + 2n_W \quad (2)$$

Trong đó: h_M và h_W là hệ số kênh truyền, n_M và n_W là nhiễu phức Gaussian.

Gọi γ_M, $\overline{\gamma}_M$, $\overline{\gamma_W}, \gamma_W$ lần lượt là tỷ số tín hiệu trên nhiễu (SNR) tức thời và trung bình tại Bob và Eve:

$$\gamma_M = \frac{P_M |h_M|^2}{2N_M}, \ \overline{\gamma}_M = \frac{P_M E\left[|h_M|^2\right]}{2N_M} \quad (3)$$

$$\gamma_W = \frac{P_W |h_W|^2}{P_W |h_W|^2 + 2N_M}, \ \overline{\gamma}_M = \frac{P_W E\left[|h_W|^2\right]}{P_W |h_W|^2 + 2N_W} \quad (4)$$

Trong đó*:* P_M *và* P_w là công suất phát trung bình đến Bob và Eve, *E[.]* là phép tính kỳ vọng của biến ngẫu nhiên.

2.1. Xét mô hình kênh truyền pha-đinh không đồng nhất Rayleigh/Rician

Hàm mật độ xác suất (PDF) của γ_M có dạng như sau:

$$f_{\gamma_M}^{(1)}(\gamma_M) = \frac{1}{\bar{\gamma}_M} e^{-\frac{\gamma_M}{\bar{\gamma}_M}} \tag{5}$$

Hàm phân bố xác suất (CDF) của γ_M được tính bởi:

$$F_{\gamma_M}^{(1)}(\gamma_M) = 1 - e^{-\frac{\gamma_M}{\bar{\gamma}_M}} \tag{6}$$

Hàm mật độ xác suất của γ_{W} là:

$$f_u(u) = \frac{(K+1)e^{-K}}{E[u]} e^{-\frac{(K+1)}{E[u]}u} I_0\left(2\sqrt{\frac{K(K+1)}{E[u]}u}\right) \tag{7}$$

Trong đó, $u = |h_{\mathrm{W}}|^2$, K là tham số pha-đinh Rician và là tỷ số công suất giữa đường trực tiếp và các đường còn lại. $I_o(.)$ là hàm Bessel hiệu chỉnh bậc 0 được biểu diễn trong [11].

$$I_0(x) = \sum_{l=0}^{\infty} \frac{x^{2l}}{2^{2l}(l!)^2} \tag{8}$$

Chúng ta có thể viết lại (7) như sau:

$$f_{\mathrm{u}}(u) = a_1 e^{-bu} I_0\left(2\sqrt{b_1 K u}\right) \tag{9}$$

Trong đó $a_1 = \frac{(K+1)e^{-K}}{E[u]}, b_1 = \frac{K+1}{E[u]}$

CDF của biến ngẫu nhiên (RV) *u* được tính như sau:

$$F_u(u) = 1 - \sum_{l=0}^{\infty}\sum_{q=0}^{l} \frac{a_1 K^l b_1^q}{l! b_1 q!} e^{-b_1 u} u^q \tag{10}$$

Để tính toán các thông số hiệu năng bảo mật của hệ thống như xác suất tồn tại dung lượng bảo mật và xác suất dừng bảo mật, chúng tôi đề xuất các định lý sau:

Định lý 1. *Trong kênh truyền pha-đinh Rician, CDF và PDF của* γ_{W} *được tính như sau:*

$$F_{\gamma_{\mathrm{W}}}^{(1)}(\gamma)=\begin{cases}\Phi_1(\gamma), & y<1\\ 1, & y>1\end{cases} \tag{11}$$

$$f_{\gamma_{\mathrm{W}}}^{(1)}(\gamma)=\begin{cases}\Phi_2(\gamma), & \gamma<1\\ 0, & \gamma>1\end{cases} \tag{12}$$

trong đó:

$$\Phi_1(\gamma)=1-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_1K^l b_1^q}{l!b_1q!}e^{-\frac{2N_w b_1\gamma}{P(1-\gamma)}}\left(\frac{2N_w\gamma}{P(1-\gamma)}\right)^q$$

$$\Phi_2(\gamma)=-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_1K^l b_1^q\left(2N_w\right)^q}{l!b_1q!P^q}e^{-\frac{2N_w b_1\gamma}{P(1-\gamma)}}\times\left[\frac{\gamma^{q-1}}{(1-\gamma)^{q+1}}\left(-\frac{2N_w b_1\gamma}{P(1-\gamma)}+q\right)\right].$$

Chứng minh : trình bày ở (23) và (24)

2.2. Xét mô hình kênh truyền pha-đinh không đồng nhất Rician/ Rayleigh

Ngược lại với trường hợp trên, trong trường hợp này, kênh hợp pháp là kênh Rician, trong khi kênh bất hợp pháp là kênh Rayleigh.

Định lý 2. *Trong kênh truyền pha-đinh Rician, PDF và CDF của* γ_M *là:*

$$\begin{aligned}f_{\gamma_M}^{(2)}(\gamma)&=\frac{(K+1)e^{-K}}{\bar{\gamma}}e^{-\frac{(K+1)\gamma}{\bar{\gamma}}}I_0\left(2\sqrt{\frac{K(K+1)\gamma}{\bar{\gamma}}}\right)\\&=a_2e^{-d\gamma}\sum_{l=0}^{\infty}\frac{\left(b_2K\right)^l\gamma^l}{(l!)^2}\end{aligned} \tag{13}$$

$$F_{\gamma_M}^{(2)}(\gamma)=\sum_{l=0}^{\infty}\frac{a_2\left(b_2K\right)^l}{l!b_2^{l+1}}-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_2K^l b_2^{q-1}\gamma^q}{q!l!}e^{-b_2\gamma} \tag{14}$$

trong đó, $a_2 = \dfrac{(K+1)e^{-K}}{\overline{\gamma}}$ và $b_2 = \dfrac{K+1}{\overline{\gamma}}$.

Chứng minh: trình bày ở (25)

Định lý 3. *Trong kênh truyền pha-đinh Rayleigh, CDF và PDF của* γ_{W} *là:*

$$F_{\gamma_{\mathrm{W}}}^{(2)}(\gamma) = \begin{cases} 1 - \mathrm{e}^{-\frac{2N_{\mathrm{W}}\gamma}{\mathrm{E}[u]P_{\mathrm{W}}(1-\gamma)}}, & \gamma < 1 \\ 1, & \gamma > 1 \end{cases} \tag{15}$$

$$f_{\gamma_{\mathrm{W}}}^{(2)}(\gamma) = \begin{cases} \dfrac{2N_{\mathrm{W}}\mathrm{e}^{-\frac{2N_w\gamma}{\mathrm{E}[u]P_w(1-\gamma)}}}{\mathrm{E}[u]P_{\mathrm{W}}(1-\gamma)^2}, & \gamma < 1 \\ 0, & \gamma > 1 \end{cases} \tag{16}$$

Chứng minh: trình bày ở (26) và (27)

3. PHÂN TÍCH HIỆU NĂNG BẢO MẬT

Dung lượng bảo mật của hệ thống C_S được định nghĩa là độ lệch giữa dung lượng của kênh truyền hợp pháp và dung lượng kênh truyền bất hợp pháp. Do đó:

$$\begin{aligned} C_S &= \left[C_M - C_{\mathrm{W}}\right]^+ \\ &= \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_{\mathrm{W}}), & \gamma_M > \gamma_{\mathrm{W}} \\ 0, & \gamma_M \le \gamma_{\mathrm{W}} \end{cases} \end{aligned} \tag{17}$$

3.1. Xác suất tồn tại dung lượng bảo mật

3.1.1. Trường hợp kênh truyền pha-đinh không đồng nhất Rayleigh/Rician.

$$\begin{aligned} P_{CS1} = {} & e^{-\frac{1}{\overline{\gamma}_M}} + \sum_{l=0}^{\infty} \frac{a_1 K^l}{l! b_1} \left(1 - e^{-\frac{1}{\overline{\gamma}_M}}\right) \\ & - \sum_{l=0}^{\infty} \sum_{q=0}^{l} \sum_{k=0}^{q} \binom{q}{k} (-1)^{q-k} \frac{a_1 K^l b_1^q (2N_{\mathrm{W}})^q}{l! q! b_1 P^q \overline{\gamma}_M} \\ & \times e^{\frac{2b_1 N_{\mathrm{W}}}{P} - \frac{1}{\overline{\gamma}_M}} \int_1^{\infty} e^{-\frac{2b_1 N_{\mathrm{W}}}{P} t + \frac{1}{\overline{\gamma}_M}} t^{k-2} dt. \end{aligned} \tag{18}$$

Chứng minh: trình bày ở (28)

3.1.2. Trường hợp kênh truyền pha-đinh không đồng nhất Rician/Rayleigh.

$$P_{CS2} = \sum_{l=0}^{\infty} \frac{a_2 K^l}{l! b_2} - \int_0^1 a_2 e^{-b_2 \gamma_M} \sum_{l=0}^{\infty} \frac{(b_2 K)^l \gamma_M{}^l}{(l!)^2} e^{-\frac{2N_w \gamma_M}{E[u] P_w (1-\gamma_M)}} d\gamma_M \quad (19)$$

Chứng minh: trình bày ở (29)

3.2. Xác suất dừng bảo mật

Xác suất dừng bảo mật (P_{out}) là xác suất dung lượng bảo mật C_S nhỏ hơn một ngưỡng xác định cho trước. Khi đó :

$$P_{out} = P(C_S < R_S) = \int_0^{\infty} f_{\gamma_W}(\gamma_W) F_{\gamma_M}(2^{R_S}(1+\gamma_W)-1) d\gamma_W . \quad (20)$$

3.2.1. Trường hợp kênh truyền pha-đinh không đồng nhất Rayleigh/Rician.

$$P_{out1} = -v \sum_{k=0}^{q} \sum_{m=0}^{k} \binom{q}{k} (-1)^{q-k} \left(\frac{P}{2N_W b_1} \right)^{k-m} \frac{k!}{m!} + qv \sum_{k=0}^{q-1} \sum_{m=0}^{k} \binom{q-1}{k} (-1)^{q-1-k} \left(\frac{P}{2N_W b_1} \right)^{k+1-m} \frac{k!}{m!}$$

$$+v \left[\frac{2N_W}{P} \sum_{k=0}^{q} \binom{q}{k} (-1)^{q-k} - q \sum_{k=0}^{q-1} \binom{q-1}{k} (-1)^{q-1-k} \right] \times exp\left(\frac{1}{\bar{y}_M} - \frac{2^{R_s+1}}{\bar{y}_M} + \frac{2N_W b_1}{P} \right) \int_1^{\infty} e^{-\frac{2b_1 N_W}{P} t + \frac{2}{\bar{y}_M t}} t^k dt \quad (21)$$

trong đó, $v = -\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_1 K^l b_1^q \left(2N_w\right)^q}{l! b_1 q! P^q}$

Chứng minh: trình bày ở (30)

3.2.2. Trường hợp kênh truyền pha-đinh không đồng nhất Rician/Rayleigh.

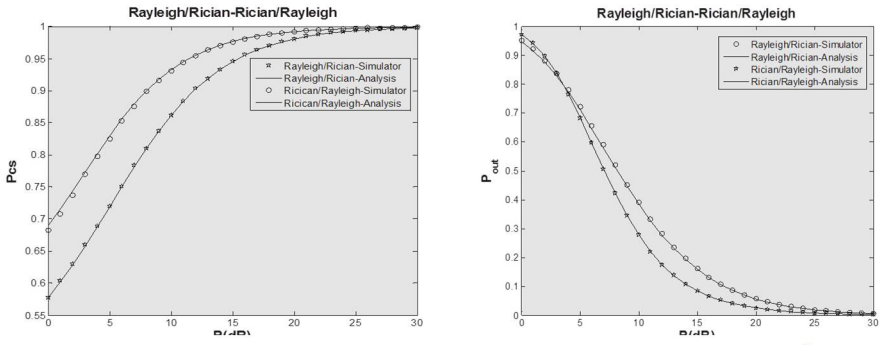
$$P_{out2} = \sum_{l=0}^{\infty}\frac{a_2 K^l}{l! b_2} - \sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_2 K^l b_2^{q-1} 2N_{\mathrm{W}}}{l! q! E[u] P_{\mathrm{W}}} \times\left(\sum_{h=0}^{q}\binom{q}{h}(-2)^h (2.2^{R_S}-1)^{q-h}\right) \times e^{\frac{2N_{\mathrm{W}}}{E[u]P_{\mathrm{W}}}} e^{-2b_2 2^{R_S}+d}\int_1^{\infty} e^{-\frac{2N_{\mathrm{W}}t}{E[u]P_{\mathrm{W}}}} e^{\frac{b_2 2^{R_S}}{t}} t^{-h} dt \quad (22)$$

Chứng minh: trình bày ở (31)

3.3. Kết quả mô phỏng

Sử dụng phương pháp mô phỏng Monte-carlo để phân tích, đánh giá hiệu năng bảo mật của hệ thống. Một số kết quả mô phỏng xác suất bảo mật, xác suất dừng bảo mật của hệ thống với ngưỡng R_S = 1bit/s/Hz như sau.

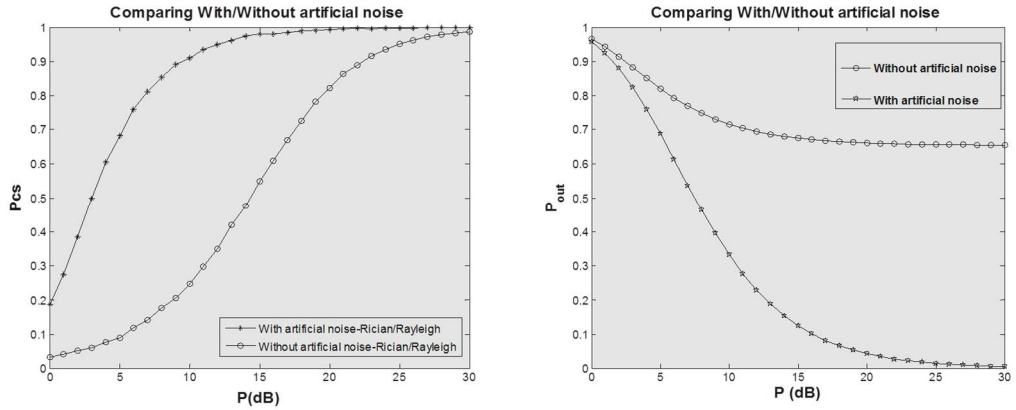
Hình 2 lần lượt thể hiện xác suất bảo mật (P_{cs}) và xác suất dừng bảo mật (P_{out}) với hai mô hình kênh truyền pha-đinh không đồng nhất Rayleigh/Rician và Rician/Rayleigh.



Hình 2. So sánh P_{CS} và P_{out} của hai mô hình kênh truyền

Kết quả cho thấy: P_{cs} tăng và P_{out} giảm khi công suất P tăng. Đồng thời, khi công suất tăng: P_{cs} trong trường hợp kênh truyền Rician/Rayleigh tăng nhanh hơn so với mô hình kênh truyền Rayleigh/Rician và ngược lại P_{out} giảm nhanh hơn. Đặc biệt, kết quả mô phỏng hoàn toàn trùng khớp với kết quả tính toán ở các thông số liên quan cho thấy cách tiếp cận, mô hình tính toán là chính xác.

Để làm rõ thêm tính chất quan trọng của việc sử dụng nhiễu giả nhằm cải thiện hiệu năng bảo mật của hệ thống, chúng tôi tiến hành mô phỏng thêm trường hợp hệ thống có sử dụng nhiễu giả và hệ thống không sử dụng nhiễu giả. Kết quả ở Hình 3 cho thấy hệ thống có sử dụng nhiễu giả có hiệu năng bảo mật tốt hơn thể hiện ở cả hai thông số được tiến hành mô phỏng so sánh là xác suất bảo mật và xác suất dừng bảo mật.



Hình 3. So sánh P_{CS} và P_{out} của hệ thống có nhiễu giả với hệ thống không có nhiễu giả với kênh truyền Rician/ Rayleigh.

4. KẾT LUẬN

Qua việc nghiên cứu, chọn lựa cách tiếp cận giải quyết vấn đề bảo mật trong mạng không dây ở lớp vật lý, tập trung vào hướng nghiên cứu không sử dụng khóa bảo mật, nhóm tác giả đề xuất mô hình mạng không dây MISO có sử dụng nhiễu giả, có kênh truyền pha-đinh không đồng nhất Rayleigh/Rician. Dựa trên phương pháp đánh giá hiệu năng bảo mật lớp vật lý đã được đề xuất, tác giả tiến hành phân tích, tính toán dung lượng bảo mật, xác suất tồn tại bảo mật và xác suất dừng bảo mật của hệ thống. Từ kết quả tính toán, mô phỏng cho thấy hệ thống có sử dụng nhiễu giả có hiệu năng bảo mật tốt hơn hệ thống không sử dụng nhiễu giả. Đây là kết quả quan trọng để xem xét và áp dụng mô hình này trong thực tế. Bên cạnh đó, bài báo cũng đóng góp những

kết quả tính toán quan trọng để đánh giá hiệu năng bảo mật của mạng không dây có sử dụng nhiễu giả trong trường hợp kênh truyền không đồng nhất Rayleigh/Rician.

Tuy nhiên, nghiên cứu này chưa đánh giá mức độ tiêu hao năng lượng, sự ảnh hưởng đến hiệu năng hệ thống khi đưa nhiễu giả vào hay xem xét các trường hợp kênh truyền sử dụng các pha-đinh khác và đó cũng chính là hướng phát triển tiếp theo của nghiên cứu này.

TÀI LIỆU THAM KHẢO

[1] C. E. Shannon, *"Communication theory of secrecy systems"*, Bell system technical journal, vol. 28, pp. 656-715, (1949).

[2] A. Wyner, *"The wire-tap channel"*, Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, (1975).

[3] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, *"Performance of transmit antenna selection physical layer security schemes"*, IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, (2012).

[4] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, *"Joint relay and jammer selection for secure two-way relay networks,"* IEEE Trans. Inf. Forensics Security, vol. 7(1), pp. 310–320, (2012).

[5] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, *"Physical layer security of TAS/MRC with antenna correlation"*, IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 254 – 259, (2013).

[6] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and K. Karagiannidis, *"Secure multiuser multiple amplify-and-forward relay networks in presence of multiple eavesdroppers"*, in IEEE GLOBECOM, Austin, USA, 8-12 December, (2014).

[7] A. P. Shrestha and K. S. Kwak, *"Performance of opportunistic scheduling for physical layer security with transmit antenna selection"* EURASIP Journal on Wireless Communications and Networking, vol. 2014:33, pp. 1–9, (2014).

[8] S. Liu, Y. Hong, and E. Viterbo, *"Practical secrecy using artificial noise"*, IEEE Communications Letter, vol. 17, no. 7, pp. 1483–1486, (2013).

[9] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, *"Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels"*, IEEE Transactions on Information Forensics and Security, vol. 9(2), pp. 247–258, (2014).

[10] D.-B. Ha, T. Q. Duong, D.-D. Tran, H.-J. Zepernick, and T. T. Vu, *"Physical layer secrecy performance over Rayleigh/Rician fading channels"*, in The 2014 International Conference on Advanced Technologies for Communications (ATC'14), Hanoi, Vietnam, Oct. 15- 17, pp. 113–118, (2014)

[11] I. Gradshteyn and I. Ryzhik, Table of Integrals, Series, and Products, D. Zwillinger, Ed. Elsevier Academic Press, (2007).

PHỤ LỤC

Trình bày một số kết quả tính toán, chứng minh liên quan:

$$F_{\gamma_{\mathrm{W}}}^{(1)}(\gamma)=\Pr(\gamma_{\mathrm{W}}<\gamma)=\Pr(\frac{Pu}{Pu+2N_{\mathrm{W}}}<\gamma)=\begin{cases}Fu(\frac{2N_{\mathrm{W}}\gamma}{P(1-\gamma)}), & \gamma<1\\ 1 & \gamma\geq 1\end{cases}$$
$$=\begin{cases}1-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{aK^{l}b^{q}}{l!bq!}e^{-\frac{2N_{\mathrm{W}}b\gamma}{P(1-\gamma)}}\left(\frac{2N_{\mathrm{W}}\gamma}{P(1-\gamma)}\right)^{q}, & \gamma<1\\ 1 & \gamma\geq 1\end{cases} \quad (23)$$

$$f_{\gamma_{\mathrm{W}}}^{(1)}(\gamma)=\frac{\partial F\gamma_{\mathrm{W}}(\gamma)}{\partial\gamma}=\begin{cases}-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{aK^{l}b^{q}(2N_{\mathrm{W}})^{q}}{l!bq!P^{q}}e^{-\frac{2N_{\mathrm{W}}b\gamma}{P(1-\gamma)}}\frac{\gamma^{q-1}}{(1-\gamma)^{q+1}}\left[-\frac{2bN_{\mathrm{W}}\gamma}{P(1-\gamma)}+q\right], & \gamma<1\\ 0 & \gamma\geq 1\end{cases} \quad (24)$$

$$F_{\gamma_{M}}^{(2)}(\gamma)=a_{2}e^{-b_{2}x}\sum_{i=0}^{\infty}\frac{(b_{2}K)^{l}x^{l}}{(l!)^{2}}dx=\sum_{i=0}^{\infty}\frac{a_{2}(b_{2}K)^{l}}{(l!)^{2}}\int_{0}^{\gamma}e^{-b_{2}x}x^{l}dx$$
$$=\sum_{i=0}^{\infty}\frac{a_{2}(b_{2}K)^{l}}{(l!)^{2}b_{2}^{\,l+1}}l!\left(1-e^{-b_{2}\gamma}\sum_{q=0}^{l}\frac{(b_{2}\gamma)^{q}}{q!}\right) \quad (25)$$
$$=\sum_{i=0}^{\infty}\frac{a_{2}(b_{2}K)^{l}}{l!b_{2}^{\,l+1}}-\sum_{i=0}^{\infty}\sum_{q=0}^{l}\frac{a_{2}b_{2}^{\,q-1}K^{l}\gamma^{q}}{l!q!}e^{-b_{2}\gamma}$$

$$F_{\gamma_{\mathrm{W}}}^{(2)}(\gamma)=\Pr(\gamma_{\mathrm{W}}<\gamma)=\Pr(\frac{2Pu}{Pu+2N_{\mathrm{W}}}<\gamma)$$
$$=\begin{cases}F_{u}\left[\frac{2N_{\mathrm{W}}\gamma}{P(1-\gamma)}\right], & \gamma<1\\ 1, & \gamma\geq 1\end{cases} \quad (26)$$
$$=\begin{cases}1-e^{-\frac{2N_{\mathrm{W}}\gamma}{E[u]P(1-\gamma)}}, & \gamma<1\\ 1, & \gamma\geq 1\end{cases}$$

$$f_{\gamma_{\mathrm{W}}}^{(2)}(\gamma)=\frac{\partial F_{2\gamma_{\mathrm{W}}}(\gamma)}{\partial\gamma}=\begin{cases}\frac{2N_{\mathrm{W}}}{E[u]P(1-\gamma)^{2}}e^{-\frac{2N_{\mathrm{W}}\gamma}{E[u]P(1-\gamma)}}, & \gamma<1\\ 0, & \gamma\geq 1\end{cases} \quad (27)$$

$$P_{CS1}=\int_0^1 f_{\gamma_M}^{(1)}(\gamma_M)F_{\gamma_W}^{(1)}(\gamma_M)d\gamma_M+\int_1^\infty f_{\gamma_M}^{(1)}(\gamma_M)F_{\gamma_W}^{(1)}(\gamma_M)d\gamma_M$$
$$=e^{-\frac{1}{\bar{\gamma}_M}}+\sum_{l=0}^{\infty}\frac{a_1K^l(1-e^{-\frac{1}{\bar{\gamma}_M}})}{l!b_1}\left(-\sum_{i=0}^{\infty}\sum_{q=0}^{l}\sum_{k=0}^{q}\binom{q}{k}(-1)^{q-k}\frac{a_1K^lb_1^q(2N_W)^q}{l!b_1q!\bar{\gamma}_MP^q}e^{-\frac{2b_1N_W}{P}-\frac{1}{\bar{\gamma}_M}}\int_1^\infty e^{\frac{1}{\bar{\gamma}_Mt}-\frac{2b_1N_Wt}{P}}t^{k-2}dt\right) \quad (28)$$

$$P_{CS2}=\int_0^1 f_{\gamma_M}^{(2)}(\gamma_M)F_{\gamma_W}^{(2)}(\gamma_M)d\gamma_M+\int_1^\infty f_{\gamma_M}^{(2)}(\gamma_M)F_{\gamma_W}^{(2)}(\gamma_M)d\gamma_M$$
$$=\int_0^1 a_2e^{-b_2\gamma_M}\sum_{l=0}^{\infty}\frac{(b_2K)^l\gamma_M^l}{(l!)^2}\left(1-e^{-\frac{2N_W\gamma_M}{E[u]P_W(1-\gamma_M)}}\right)d\gamma_M+\int_1^\infty a_2e^{-b_2\gamma_M}\sum_{l=0}^{\infty}\frac{(b_2K)^l\gamma_M^l}{(l!)^2}d\gamma_M \quad (29)$$
$$=\sum_{l=0}^{\infty}\frac{a_2K^l}{l!b_2}-\int_0^1 a_2e^{-b_2\gamma_M}\sum_{l=0}^{\infty}\frac{(b_2K)^l\gamma_M^l}{(l!)^2}e^{-\frac{2N_w\gamma_M}{E[u]P_w(1-\gamma_M)}}d\gamma_M$$

$$P_{out1}=\int_0^1 f_{\gamma_W}^{(1)}(\gamma_W)F_{\gamma_M}^{(1)}(2^{R_s}(1+\gamma_W)-1)d\gamma_W+\int_1^\infty f_{\gamma_W}^{(1)}(\gamma_W)F_{\gamma_M}^{(1)}\left(2^{R_s}(1+\gamma_W)-1\right)d\gamma_W$$
$$=-v\sum_{k=0}^{q}\sum_{m=0}^{k}\binom{q}{k}(-1)^{q-k}\left(\frac{P}{2N_Wb}\right)^{k-m}\frac{k!}{m!}+qv\sum_{k=0}^{q-1}\sum_{m=0}^{k}\binom{q-1}{k}(-1)^{q-1-k}\left(\frac{P}{2b_1N_W}\right)^{k+1-m}\frac{k!}{m!}$$
$$+v\left[\frac{2b_1N_W}{P}\sum_{k=0}^{q}\binom{q}{k}(-1)^{q-k}-q\sum_{k=0}^{q-1}\binom{q-1}{k}(-1)^{q-1-k}\right]e^{\frac{1}{\bar{\gamma}_M}-\frac{2^{R_s}+1}{\bar{\gamma}_M}+\frac{2b_1N_w}{P}}\int_1^\infty\left(e^{-\frac{2b_1N_Wt}{P}+\frac{2}{\bar{\gamma}_Mt}}t^k\right)dt \quad (30)$$

$$P_{out2}=\int_0^\infty f_{\gamma_W}^{(2)}(\gamma_W)F_{\gamma_M}^{(2)}(2^{R_s}(1+\gamma_W)-1)d\gamma_W=\int_0^1 f_{\gamma_W}^{(2)}(\gamma_W)F_{\gamma_M}^{(2)}(2^{R_s}(1+\gamma_W)-1)d\gamma_W$$
$$=\int_0^1\frac{2N_W}{E[u]P_W(1-\gamma_W)^2}e^{-\frac{2N_W}{E[u]P_W(1-\gamma_W)}}\left(\sum_{l=0}^{\infty}\frac{a_2K^l}{l!b_2}-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_2K^lb_2^{q-1}(2^{R_s}(1+\gamma_W)-1)^q}{l!q!}e^{-b_2(2^{R_s}(1+\gamma_W)-1)}\right)$$
$$=\sum_{l=0}^{\infty}\frac{a_2K^l}{l!b_2}-\sum_{l=0}^{\infty}\sum_{q=0}^{l}\frac{a_2K^lb_2^{q-1}2N_W}{l!q!E[u]P_W}\times\left(\sum_{h=0}^{q}\binom{q}{h}(-2)^h(2.2^{R_s}-1)^{q-h}\right)e^{\frac{2N_W}{E[u]P_W}}e^{-2b_2^{2^{R_s}}+b_2}\int_1^\infty e^{-\frac{2N_Wt}{E[u]P_W}}e^{\frac{b_2^{2^{R_s}}}{t}}t^{-h}dt \quad (31)$$

PHYSICAL LAYER SECRECY ON WIRELESS NETWORK

Truong Tien Vu[a*], Tran Duc Dung[a], Ha Dac Binh[a], Vo Nhan Van[a]

[a]The Faculty of Information Technology, Duytan University, Danang, Vietnam
[*]Corresponding author: truongtienvu@dtu.edu.vn

Article history
Received: January 04th, 2016
Received in revised form (1st) March 17th, 2016 | Received in revised form (2nd): March 19th, 2016
Accepted: March 31st, 2016

Abstract

In this paper, we present an approach for wireless security based on physical layer. The basic principle of physical layer secrecy (PHY Secrecy) is ensuring secure information transmission in the the system that consists of illegal receiver without using any coding solution on application layer. Applying this approach, we evaluate the physical layer secrecy performance of MISO (Multi Input-Single Output) system that consists of double antennas transmitter and single antenna receiver in the presence of a single antenna passive eavesdropper's over heterogeneous fading channels Rayleigh/Rician. We evaluate, analyse secrecy capacity, existence probability of secrecy capacity and secrecy outage probability and verify the numerical results with Monte-Carlo simulation results. Our results have presented the utility of using physical layer secrecy to enhance the secrecy performance of wireless networks.

Keywords: Existence probability of secrecy capacity; Physical layer secrecy; Secrecy capacity; Secrecy outage probability.