PHÂN TÍCH HIỆU NĂNG BẢO MẬT THÔNG TIN Ở LỚP VẬT LÝ VỚI CÁC KÊNH TRUYỀN FADING HỖN HỢP RAYLEIGH/HOYT

PHYSICAL LAYER SECURITY PERFORMANCE OVER MIXED RAYLEIGH AND HOYT FADING CHANNELS

Hà Đắc Bình, Văn Phú Tuấn

Khoa điện tử-viễn thông, Trường Đại Học Duy Tân

Tóm tắt: *Trong những năm gần đây, bảo mật ở lớp vật lý được coi là một cách tiếp cận mới và nổi lên thành đề tài hấp dẫn thu hút nhiều nhà nghiên cứu hiện nay. Trong bài báo này, chúng tôi khảo sát hiệu năng bảo mật ở lớp vật lý của hệ thống của các thiết bị đầu cuối đơn ăn-ten, có sự hiện diện của thiết bị nghe lén đơn ăn-ten thụ động qua các kênh truyền có fading khác nhau Rayleigh/Hoyt. Đặc biệt, chúng tôi đã tìm ra công thức tính xác suất khác không của dung lượng bảo mật và xác suất dừng bảo mật của hệ thống bằng cách sử dụng đặc tính thống kê của tỉ lệ tín hiệu trên nhiễu. Kết quả mô phỏng Monte-Carlo đã cùng cố tính đúng đắn của kết quả phân tích.*

Từ khoá: *bảo mật lớp vật lý, dung lượng bảo mật, Rayleigh fading, Hoyt fading, thông tin vô tuyến.*

Abstract: *In recent years, physical layer security is considered to be a new approach emerged as attractive themes attracted many researchers today. In this paper, we investigate the physical layer secrecy performance of a single-input single-output system consisting of single antenna devices, in the presence of a single antenna passive eavesdropper over dissimilar fading channels: The legal/illegal channels are subject to Rayleigh/Hoyt fading, respectively. Specifically, expressions for the existence probability of secrecy capacity and the secrecy outage probability are derived by using statistical characteristics of the signal-to-noise ratio. The analytical results are verified by Monte-Carlo simulations.*

Keywords: *physical layer security, security capacity, Rayleigh fading, Hoyt fading, wireless communication.*

1. Giới thiệu

Trong những năm gần đây, sự phát triển nhanh chóng của truyền thông vô tuyến đã ảnh hưởng ngày càng to lớn đến các lĩnh vực kinh tế xã hội. Điều này dẫn đến vấn đề bảo mật thông tin trong mạng vô tuyến cũng ngày càng được quan tâm và nổi lên thành một vấn đề nóng, đặc biệt trong các lĩnh vực tài chính, ngân hàng, an ninh, quân sự.

Do độ phức tạp và độ trễ thấp, cũng như tính khả thi ở lớp vật lý (PHY) và khả năng cùng tồn tại với các cơ chế bảo mật mã hóa hiện có mà nó có thể nâng cao mức độ tổng thể về an toàn thông tin. Vì vậy, bảo mật ở lớp PHY dựa trên thuyết thông tin đã thu hút được sự quan tâm nghiên cứu của các học giả trên khắp thế giới.

Các nhà nghiên cứu đã tập trung gần đây về các vấn đề an ninh thông tin ở PHY trong hai cách tiếp cận chính: bảo mật dựa trên khóa và bảo mật không dựa trên khóa [1]

Phương pháp tiếp cận đầu tiên là tìm khóa bảo mật dựa trên các đặc tính của môi trường truyền dẫn Ví dụ, người sử dụng khác nhau sẽ có một phiên bản nhiễu khác nhau của tín hiệu truyền, cho phép tạo khóa bảo mật và khóa này được sử dụng để đảm bảo an toàn thông tin giữa người sử dụng hợp pháp. Cách tiếp cận thứ hai tập trung vào việc xây dựng một cơ chế mã hóa ngẫu nhiên, nhằm mục đích che giấu dòng thông tin trong cộng đồng để làm suy yếu các thiết bị nghe trộm bằng cách ánh xạ mỗi bản tin cho nhiều từ mã theo một phân bố xác suất thích hợp. Bằng cách này, sự mơ hồ tối đa được gây ra tại thiết bị nghe trộm.

Các phương pháp đánh giá liệu hệ thống có khả năng bảo đảm an ninh tại PHY cũng đang thu hút hơn các nhà nghiên cứu trong lĩnh vực này [2-4]. Trong [2], dựa trên lý thuyết thông tin trong đó hai đối tác hợp pháp giao tiếp với kênh có cùng fading

nhưng độc lập với kênh máy nghe trộm, các tác giả đã xác định dung lượng bảo mật ứng với một xác suất dừng bảo mật và cung cấp một đặc tính hoàn chỉnh của tốc độ truyền tối đa mà các kẻ nghe trộm không thể giải mã bất kỳ thông tin. Trong [3], các tác giả khảo sát dung lượng bảo mật PHY của một hệ thống truyền thông bao gồm một máy phát đa ăn-ten sử dụng cơ chế lựa chọn ăn-ten và một máy thu đơn ăn-ten, trong sự hiện diện của một máy nghe trộm đa ăn-ten. Các tác giả của [4] đã phân tích tác động của mối tương quan giữa các ăn-ten đến hiệu năng bảo mật trong hệ thống đa ăn-ten MIMO, trong đó máy phát sử dụng cơ chế lựa chọn ăn-ten trong khi người nhận và máy nghe trộm thực hiện kết hợp tỷ lệ tối đa với tương quan tùy ý.

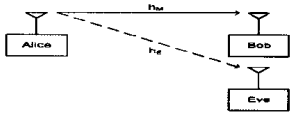
Cho đến nay, hầu hết các công trình trước đây về bảo mật PHY đều cho rằng các kênh hợp pháp tương tự như các kênh bất hợp pháp. Tuy nhiên, trong nhiều tình huống thực tế, giả định này không còn đúng do sự di chuyển của thiết bị di động tạo ra các kênh truyền có fading khác nhau. Li và các cộng sự [5] khảo sát tốc độ bảo mật thực hiện được cho kênh AWGN, trong khi kênh của kẻ nghe trộm là fading Rayleigh.

Theo sự hiểu biết của chúng tôi, chưa công trình nào đề cập việc đánh giá năng lực bảo mật của hệ thống bao gồm các thiết bị đơn ăn-ten, trong sự hiện diện của một thiết bị nghe lén thụ động đơn ăn-ten trên các kênh fading khác nhau Rayleigh/Hoyt. Mô hình kênh fading Hoyt cung cấp một phép đo kênh thử nghiệm rất chính xác với các ứng dụng truyền thông khác nhau, như thông tin di động vệ tinh [6]. Trong bài báo này, chúng tôi tính được biểu thức cho xác suất tồn tại của dung lượng bảo mật và xác suất dừng bảo mật của hệ thống sử dụng đặc tính thống kê của tín hiệu trên nhiễu (SNR) của các kênh fading khác nhau Rayleigh/Hoyt. Các biểu thức này cho phép chúng ta đánh giá khả năng bảo mật của hệ thống đơn đầu vào đầu ra (SISO).

Phần còn lại của bài báo được được sắp xếp như sau. Phần 2 giới thiệu mô hình hệ thống và kênh truyền. Phần 3 phân tích và tính toán tính xác suất khác không của dung lượng bảo mật và xác suất dừng bảo mật của hệ thống. Phần 4 là kết quả mô phỏng, phân tích và thảo luận. Cuối cùng, phần 5 là phần kết luận.

2. Mô hình hệ thống và kênh truyền

Chúng ta xem xét mô hình hệ thống như hình 1. Alice và Bob là người sử dụng hợp pháp của hệ thống SISO. Trong khi Eve là kẻ nghe trộm thụ động tìm cách trích thông tin từ Alice mà không chủ động tấn công. Alice, Bob và Eve là những thiết bị đơn ăn-ten. Kênh truyền hợp pháp có fading là Rayleigh, kênh truyền bất hợp pháp có fading là Hoyt.



Hình 1. Mạng truyền thông với máy phát (Alice), máy thu (Bob) và thiết bị nghe trộm (Eve)

Alice gửi tín hiệu x(t) cho Bob. Bob thu được tín hiệu y(t) như sau.

$$y(t) = h_M x(t) + n_M, \quad (1)$$

trong đó, h_M là hệ số fading của kênh truyền giữa Alice và Bob. n_M là nhiễu Gaussian phức có trung bình bằng 0 và công suất là N_M.

Eve nghe trộm tín hiệu gửi từ Alice. Tín hiệu Eve thu được như sau:

$$z(t) = h_W x(t) + n_W, \quad (2)$$

Trong đó, h_W là hệ số fading của kênh truyền giữa Alice và Eve. n_W là nhiễu Gaussian phức có trung bình bằng 0 và công suất là N_W.

Gọi $\gamma_M, \gamma_M, \gamma_W, \gamma_W$ lần lượt là SNR tức thời và trung bình tại Bob và Eve. Ta có:

$$\gamma_M = \frac{P_M |h_M|^2}{N_M}, \quad \bar{\gamma}_M = \frac{P_M \mathbf{E}[|h_M|^2]}{N_M},$$

$$\gamma_W = \frac{P_W |h_W|^2}{N_W}, \quad \bar{\gamma}_W = \frac{P_W \mathbf{E}[|h_W|^2]}{N_W},$$

trong đó, P_M, P_W lần lượt là công suất thu trung bình tại Bob và Eve, $\mathbf{E}[.]$ là phép tính kỳ vọng của biến ngẫu nhiên.

Gọi $f_{\gamma_M}(\gamma_M)$ và $f_{\gamma_W}(\gamma_W)$ lần lượt là hàm phân bố xác suất (PDF) của γ_M

(Rayleigh fading) và γ_W (Hoyt fading). Chúng được cho bởi [5][6]:

$$f_{\gamma_M}(\gamma_M) = \frac{1}{\overline{\gamma}_M} e^{-\frac{\gamma_M}{\overline{\gamma}_M}} \quad (3)$$

$$f_{\gamma_W}(\gamma_W) = \frac{1+q^2}{2q\overline{\gamma}_W} e^{-\frac{(1-q^4)\gamma_W}{4q^2\overline{\gamma}_W}} I_0\left(\frac{(1-q^4)}{4q^2\overline{\gamma}_W}\gamma_W\right) \quad (4)$$

$$= \frac{a}{\overline{\gamma}_W} e^{-\frac{a^2}{\overline{\gamma}_W}\gamma_W} I_0\left(\frac{b}{\overline{\gamma}_W}\gamma_W\right)$$

trong đó, q là tham số fading Hoyt ($0 \le q \le 1$), $a = \frac{1+q^2}{2q}$, $b = \frac{1-q^4}{4q^2}$ và $I_0(.)$ là hàm Bessel hiệu chỉnh bậc 0.

3. Phân tích dung lượng bảo mật

Dung lượng của kênh truyền hợp pháp $C_M = \log_2(1+\gamma_M)$. (5)

Dung lượng của kênh truyền bất hợp pháp $C_W = \log_2(1+\gamma_W)$. (6)

Dung lượng bảo mật tức thời được tính bởi:

$$C_S = \max\{0, (C_M - C_W)\}$$

$$= \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_W), & \gamma_M > \gamma_W \\ 0, & \gamma_M \le \gamma_W \end{cases} \quad (7)$$

Giả sử kênh truyền hợp pháp độc lập với kênh truyền bất hợp pháp. Xác suất khác không của dung lượng bảo mật được tính như sau.

$$P(C_S > 0) = Pcs = P(\gamma_M > \gamma_W)$$

$$= \int_0^{\infty}\int_0^{\gamma_M} f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W) d\gamma_W d\gamma_M \quad (8)$$

Thay (3) và (4) vào (8), đồng thời sử dụng chuỗi vô hạn trong [7] thay cho $I_0(.)$:

$$I_0(x) = \sum_{l=0}^{\infty} \frac{x^{2l}}{2^{2l}(l!)^2} \quad (9)$$

và sử dụng các tích phân 6.451, 8.350 và 8.352 [8] để tính biểu thức (8), ta được kết quả như sau:

$$Pcs = \sum_{l=0}^{\infty} \frac{b^{2l}(2l)!}{2^{2l}(l!)^2 a^{4l+1}} \sum_{i=0}^{2l} \frac{a^{2(2l-i)}}{(a^2\overline{\gamma}_M + \overline{\gamma}_W)^{i+1}} \quad (10)$$

Bên cạnh dung lượng bảo mật, xác suất dừng bảo mật, $P(C_S < R_S)$, cũng là một thước đo hiệu năng quan trọng mà những người thiết kế hệ thống cần phải biết.

Với các đại lượng và điều kiện như đã đề cập ở trên, xác suất dừng bảo mật được tính như sau:

$$P(C_S < R_S) = Pout$$

$$= P(C_S < R_S \mid \gamma_M > \gamma_W) P(\gamma_M > \gamma_W) \quad (11)$$

$$+ P(C_S < R_S \mid \gamma_M \le \gamma_W) P(\gamma_M \le \gamma_W)$$

$$= \Phi_1 + \Phi_2$$

Trong đó,

$$\Phi_1 = \int_0^{\infty}\int_{\gamma_W}^{2^{R_S}(1+\gamma_W)-1} f_{\gamma_M}(\gamma_M) f_{\gamma_W}(\gamma_W) d\gamma_W d\gamma_M \quad (12)$$

$$\Phi_2 = P(\gamma_M \le \gamma_W) = 1 - P(\gamma_M > \gamma_W)$$

$$= 1 - \sum_{l=0}^{\infty} \frac{b^{2l}(2l)!}{2^{2l}(l!)^2 a^{4l+1}} \sum_{i=0}^{2l} \frac{a^{2(2l-i)}\overline{\gamma}_M^{\,i}}{(a^2\overline{\gamma}_M + \overline{\gamma}_W)^{i+1}} \quad (13)$$

(Chú ý: $P(C_S < R_S \mid \gamma_M \le \gamma_W) = 1$).

Tương tự như phần tính Pcs, ta tính được kết quả Φ_1 như sau:

$$\Phi_1 = a \sum_{l=0}^{\infty} \frac{b^{2l}\overline{\gamma}_M^{2l+1}}{2^{2l}(l!)^2} (2l)! \cdot \frac{1}{(a^2\overline{\gamma}_M + \overline{\gamma}_W)^{2l+1}} \cdot \frac{e^{-\frac{2^{R_S}-1}{\overline{\gamma}_M}}}{(a^2\overline{\gamma}_M + 2^{R_S}\overline{\gamma}_W)^{2l+1}} \quad (14)$$

Thay (13) và (14) vào (11) ta được biểu thức tính Pout

4. Kết quả mô phỏng và thảo luận

Chúng tôi dùng mô phỏng Monte Carlo và tính toán phân tích (với $q = 0,5$) để mô tả hiệu năng bảo mật lớp vật lý của hệ thống mà chúng tôi đang xem xét. Số vòng lặp của mô phỏng là 10^6 và sử dụng 20 số hạng đầu tiên của chuỗi vô hạn (l=20) (tham khảo [7]) Kết quả số xác suất tồn tại của dung lượng bảo mật và xác suất dừng bảo mật của hệ thống mà chúng tôi có được như hình 2, 3, 4, 5.

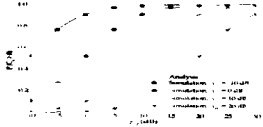
Hình 2 là kết quả mô phỏng cho xác suất khác không của dung lượng bảo mật. Từ hình này, ta có nhận xét rằng, với γ_W cố định, khi γ_M tăng thì *Pcs* tăng, hay nói cách khác, dung lượng của kênh hợp pháp càng lớn hơn dung lượng của kênh nghe trộm. Trái lại, với γ_M cố định, khi γ_W tăng thì *Pcs* giảm hay dung lượng của kênh hợp pháp càng nhỏ hơn dung lượng của kênh nghe trộm Rõ ràng là kênh truyền vô tuyến có dung lượng bảo mật là dương ngay cả khi các kênh nghe trộm có thể

tốt hơn so với kênh của người sử dụng hợp pháp. Nếu $\gamma_M >> \gamma_W$ thì $Pcs \rightarrow 1$, nếu $\gamma_M << \gamma_W$ thì $Pcs \rightarrow 0$.

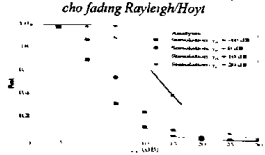
Trái với xác suất khác không của dung lượng bảo mật, xác suất dừng bảo mật *Pout* sẽ tăng khi γ_W tăng (với γ_M cố định) và giảm khi γ_M tăng (với γ_W cố định). Kết quả này được chỉ ra trong hình 3. Nếu $\gamma_M >> \gamma_W$ thì $Pout \rightarrow 0$, nếu $\gamma_M << \gamma_W$ thì $Pout \rightarrow 1$

Để khẳng định thêm tính đúng đắn của phần phân tích, chúng tôi cũng thực hiện mô phỏng và phân tích cho 2 kênh truyền fading giống nhau Rayleigh/Rayleigh. Do phần mềm Mathematica không thể tính kết quả phân tích cho trường hợp fading Rayleigh (q = 1) (trong phép tính có dạng 0^0) nên chúng tôi dùng q = 1,0001 thay thế cho q = 1, kết quả như hình 4 và hình 5 Các kết quả này khớp với các kết quả đã công bố trước đó cho 2 kênh truyền có fading giống nhau Rayleigh/Rayleigh.

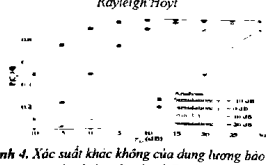
Từ 4 kết quả trên, chúng tôi nhận thấy kết quả phân tích khớp với kết quả mô phỏng.



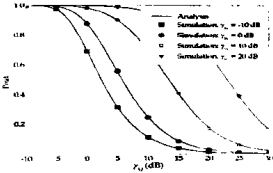
Hình 2. Xác suất khác không của dung lượng bảo mật cho fading Rayleigh/Hoyt



Hình 3. Xác suất dừng bảo mật cho fading Rayleigh/Hoyt



Hình 4. Xác suất khác không của dung lượng bảo mật cho fading Rayleigh/Rayleigh



Hình 5. Xác suất dừng bảo mật cho fading Rayleigh/Rayleigh

5. Kết luận

Trong bài báo này, chúng tôi đưa ra biểu thức xác suất tồn tại của dung lượng bảo mật và xác suất dừng bảo mật của hệ thống đơn ăn-ten, trong đó có sự hiện diện của thiết bị nghe trộm thụ động đơn ăn-ten sử dụng đặc tính thống kê của tín hiệu trên nhiễu (SNR) của các kênh fading khác nhau Rayleigh/Hoyt. Kết quả mô phỏng đã khẳng định tính đúng đắn của kết quả phân tích. Các biểu thức này cho phép chúng ta đánh giá khả năng bảo mật của hệ thống đơn đầu vào đầu ra (SISO)❑

Tài liệu tham khảo:

[1] Hà Đắc Bình, Vũ Trọng Tân, Trần Đức Dũng, "*Nghiên cứu khả năng bảo mật thông tin ở lớp vật lý trong thông tin vô tuyến*". Tạp chí khoa học giao thông vận tải số 10, 2/2014, Tr. 20-24.

[2] J. Barros and M. Rodrigues, "*Secrecy capacity of wireless channels,*" in Proc. IEEE Int Symp. Information Theory (ISIT), Seattle, USA, July 2006, pp. 356–360.

[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] 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.

(xem tiếp trang 55)