ĐÁNH GIÁ KHẢ NĂNG BẢO MẬT LỚP VẬT LÝ CỦA HỆ THỐNG siso VỚI sự hiện diện của nhiều thiết bị nghe lén

Physical Layer Secrecy Performance Analysis WITH MANY PASSIVE EAVESDROPPERS IN SISO SYSTEM

Hoàng Quang Vũ1, , Nguyễn Văn Thọ1 , Hà Đắc Bình1

1Trường Đại học Duy Tân

**Tóm tắt -** Bảo mật lớp vật lý trong những năm gần đây đang là đề tài hấp dẫn thu hút của nhiều nhà nghiên cứu, đặc biệt là bảo mật lớp vật lý trong truyền thông không dây. Do bản chất phát sóng ra không gian tự do nên nó rất dễ bị tấn công nghe lén. Trong bài báo này chúng tôi khảo sát và đánh giá hiệu năng bảo mật lớp vật lý của hệ thống truyền thông đơn ăn-ten có sự hiện diện của nhiều thiết bị nghe lén thụ động đơn ăn-ten qua các kênh truyền có fading khác nhau Hoyt/Rayleigh. 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 khảo sát, đồng thời mô phỏng Monte-Carlo để chứng tỏ tính đúng đăn của kết quả tính toán. Các kết quả bài báo có thể ứng dụng trong thiết kế các hệ thống thực tế, lựa chọn các tham số để đảm bảo được yêu cầu bảo mật của hệ thống.

**Từ khóa -** Bảo mật lớp vật lý; dung lượng bảo mật; hệ thống SISO; Rayleight pha-đing; Hoyt pha-đing.**Abstract -** Physical layer security is a topic attracted many researchers in recent years . In this paper, we in- vestigate the physical layer secrecy performance of single-input single-output (SISO) system in the presence of many passive eavesdroppers over dissimilar fading channels. Especially, the exact close-form expressions for the probability of non-zero secrecy capacity and the secrecy outage probability using statistical characteristics of the signal-to-noise ratio of these scenarios are derived. Monte-Carlo simulation results are also contributed to confirm the correctness of the analysis results.The numerical result discussion provides practical design into the effect of various system parameters on the secrecy performance of considered system.

**Key words -** physical layer secrecy;secrecy capacity; SISO system; Rayleight fading; Hoyt fading

# Giới thiệu

Những năm gần đây, sự phát triển nhanh chóng của thông tin vô tuyến đã và đang ảnh hưởng ngày càng to lớn đến nhiều lĩnh lực khác nhau trong đời sống kinh tế xã hội. Điều này dẫn đến vấn đề bảo mật trong thông tin vô tuyến lại trở thành tâm điểm của nhiều nhà nghiên cứu trong và ngoài nước, đặc biệt là trong các lĩnh vực quan trọng đòi hỏi tính bảo mật cao như an ninh, quốc phòng, tài chính…

Bên cạnh sự tiện lợi, linh hoạt trong quá trình sử dụng thì thông tin vô tuyến cũng có những hạn chế, đặc biệt là vấn đề bảo mật, do bản chất của truyền thông vô tuyến là truyền công khai (quảng bá) bằng tín hiệu vô tuyến trong không khí cho phép truy cập đa phương tiện và thông tin không hạn chế về vị trí của người dùng. Do vậy mạng vô tuyến có nhiều nguy cơ tiềm ẩn trong an ninh vì bất kỳ ai có một máy thu nằm trong phạm vi phủ sóng của máy phát đều có thể nghe trộm. Cho nên nếu kênh truyền không được bảo mật tốt thì nhiều thông tin quan trọng sẽ bị kẻ xấu đánh cắp trong quá trình truyền thông tin từ máy phát đến máy thu. Đó là nguyên nhân làm cho bảo mật trong thông tin vô tuyến trở thành vấn đề ngày càng được quan tâm và nổi lên thành chủ đề nghiên cứu của nhiều học giả trên thế giới.

Trong mạng không dây hiện nay, hầu hết các hệ thống bảo mật đều sử dụng cơ chế bảo mật dựa trên việc tính toán phức tạp, mà người ta cho rằng chưa có cách nào hiệu quả ngoài cách vét cạn vì với giả định rằng kẻ xấu có khả năng tính toán hạn chế và không có đủ những thuật toán hiệu quả. Tuy nhiên, việc giả định này là thiếu sức thuyết phục bởi sự phát triển không ngừng của các máy tính có khối lượng tính toán khổng lồ (như máy tính lượng tử). Hơn nữa, việc xác thực và mã hóa trong cơ chế bảo mật ở lớp cao hơn tạo ra độ trễ đường truyền quá lớn, tiêu thụ điện năng cao và giảm dung lượng hệ thống do sự quá tải trong tính toán và báo hiệu [1].

Do đó, đã có một nghiên cứu đáng chú ý gần đây về các khả năng cơ bản của lớp vật lý để cung cấp thông tin liên lạc không dây an toàn. Mô hình này được gọi là bảo mật thông tin ở lớp vật lý. Bảo mật lớp vật lý là một lĩnh vực nghiên cứu mới, nghiên cứu về khả năng truyền và tải dữ liệu được bảo mật hoàn hảo giữa máy thu và máy phát.

Các nền tảng cho lý thuyết về hệ thống bảo mật đã được đặt bởi Claude Shannon[2]. Ông đã cho thấy rằng bảo mật hoàn hảo khi thông tin người nhận có thể giải mã các thông điệp mà không có lỗi, trong khi nghe trộm có thể không giải mã được các thông điệp bí mật.

Các giả định cơ bản trong phân tích này là:

+ Những kẻ nghe trộm có thể sử dụng sức mạnh tính toán vô hạn về thời gian.

+ Có cả bộ thu và nghe lén được áp dụng chính xác các tín hiệu tương tự.

+ Có cả những kiến thức về thuật toán và mã hóa.

Do tính bảo mật gần như tuyệt đối, độ phức tạp và độ trễ thấp, cũng như tính khả thi ở lớp vật lý 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 vào thuyết thông tin đã thu hút được sự quan tâm nghiên cứu của các học giả trên khắp thế giới. Đã có nhiều nghiên cứu về các phương pháp đánh giá liệu hệ thống có đảm bảo an ninh tại lớp vật lý [3, 4,5]

Trong thực tế, do sự di chuyển của các thiết bị di động nên kênh hợp pháp và kênh bất hợp pháp có thể khác nhau. Trong [6] các tác giả đã khảo sát tốc độ bảo mật thực hiện trên kênh AWGN, trong khi kênh bất hợp pháp là fading Rayleigh.

Trong bài báo này chúng tôi khảo sát và đánh giá hiệu năng bảo mật lớp vật lý của hệ thống truyền thông đơn ăn-ten (SISO) có sự hiện diện của nhiều thiết bị nghe lén thụ động đơn ăn-ten qua các kênh truyền có fading khác nhau Hoyt/Rayleigh. 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 [7]. 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 khảo sát, đồng thời mô phỏng Monte-Carlo để chứng tỏ tính đúng đăn của kết quả tính toán. Các kết quả bài báo có thể ứng dụng trong thiết kế các hệ thống thực tế, lựa chọn các tham số để đảm bảo được yêu cầu bảo mật của hệ thống.

# Mô hình hệ thống

*Hình 1. Mô hình hệ thống*

Chúng ta xem xét mô hình hệ thống như hình 1. Trong đó, máy phát A là thiết bị di động mặt đất, B là vệ tinh thu hợp pháp, với sự hiện diện của N thiết bị nghe trộm thụ động En (n={1, 2, ..., N}). Các thiết bị nghe trộm thu động En tìm cách trích thông tin hợp pháp truyền từ A đến B mà không chủ động tấn công. A, B và En là những thiết bị đơn antenna. Kênh truyền hợp pháp từ thiết bị di động A đến vệ tinh B có pha-đinh Hoyt và kênh truyền bất hợp pháp từ A đến các thiết bị nghe trộm En có pha-đinh Rayleigh hoàn toàn độc lập với nhau

Gọi là tín hiệu mà A truyền đến vệ tinh B, tín hiệu nhận tại B là:

 (1)

trong đó, là hệ số pha-đinh Hoyt của kênh truyền hơp pháp giữa A và B; là nhiễu phức Gaussian có trung bình bằng 0 và công suất là . Tỷ lệ tín hiệu trên nhiễu (SNR) tức thời tại B là , SNR trung bình là trong đó là công suất truyền trung bình, là phép tính kỳ vọng.

Hàm mật độ xác suất (PDF) của là [2]:

 (2)

trong đó, *q* là hệ số pha-đinh Hoyt và là hàm Bessael hiệu chỉnh bậc 0.

Đặt , , biểu thức (2) được viết lại như sau

 (3)

Đối với các thiết bị nghe trộm, *En*, có khả năng nghe trộm tín hiệu được gửi từ bộ truyền hợp pháp. Chúng tôi ký hiệu tín hiệu thu được tại *En* là có dạng như sau:

 (4)

trong đó, là hệ số kênh truyền pha-đinh Rayleigh giữa máy phát với *En* và là nhiễu phức Gaussian có trung bình bằng 0 và công suất . Tương tự như trên ta có, SNR tức thời tại thiết bị nghe trộm *En* là , SNR trung bình là .

Ở [8] ta biết rằng, với , hệ thống có khả năng đảm bảo bảo mật thông tin khi . Như vậy, trong trường hợp này, khả năng bảo mật thông tin của hệ thống đạt được khi và chỉ khi . Từ lý do này, chúng tôi định nghĩa đại lượng được tính bởi công thức:

, (5)

hệ thống sẽ đảm bảo tính bảo mật khi . Hàm PDF của được cho bởi [9]:

 (6)

# Phân tích mô hình bảo mật

# Trước tiên là dung lượng bảo mật CS, nó được định nghĩa là sự sai khác giữa dung lượng kênh truyền hợp pháp CM và dung lượng kênh truyền bất hợp pháp CW được tính như sau:

 (7)

 (8)

Từ đó, dung lượng bảo mật là:

 (9)

Vì và độc lập với nhau, nên từ hàm mật độ liên hợp ở trên ta có thể tính xác suất tồn tại dung lượng bảo mật như sau

 (10)

trong đó,  và  lần lượt là PDF của  và CDF của .

 được tính như sau:

 (11)

Sử dụng công thức trong [10]  và triển khai nhị thức Newton

, (10) được viết lại như sau:

(12) (15)

Ta biết rằng, khi *q = 1*, kênh truyền Hoyt sẽ trở thành kênh truyền Rayleigh. Lúc đó, *a = 1, b = 0* và (12) có dạng như sau:

 (13)

Cuối cùng, xác suất dừng bảo mật (*POut*) được định nghĩa là xác suất dung lượng bảo mật tức thời *CS* giảm xuống dưới một mức ngưỡng tốc độ bảo mật cho trước *RS* > 0. Biểu thức tính toán cho *POut* là:

 (14)

Từ (9) ta có :

 (15)

trong đó, ,.

Dựa vào [3],  được tính như sau:

 (16)

với .

Đặt , ta có:

 (17)

trong đó,  là CDF của . Sử dụng (3) và (11),  được tính như sau:

 (21)

Áp dụng 8.310, 8.339 và 8.352.7 trong [11] cho hàm Gamma ta được:

 (18)

Do đó, *I1* là:

 (19)

Thay (19) vào (16), tương tự với các tính toán ở trên, ta có kết quả của  như sau :

(20)

* **Tính **

Từ (9) ta có,  khi , do đó  và

 (21)

Vậy, xác suất dừng bảo mật của hệ thống được tính bởi công thức:

(22)

trong đó,







Tương tự như trường hợp *PCS*, với *q = 1* và *N = 1*, (13) cũng cho kết quả giống với kết quả của xác suất dừng bảo mật trong công trình [3]:

 (23)

# Kết quả mô phỏng và thảo luận

Chúng tôi dùng mô phỏng Monte Carlo với số lượng máy thu bất hợp pháp N=3 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 106 và sử dụng 20 số hạng đầu tiên của chuỗi vô hạn (*l=20*) (tham khảo [12]) Kết quả chúng tôi có được như hình 2, 3.

*Hình 2. Xác suất khác không của dung lượng bảo mật*



*Hình 3. Xác suất dừng bảo mật hệ thống*

Từ hình 2, ta có nhận xét rằng, với giá trị của  cố định, khi  tăng thì *PCS* tăng, do trong trường hợp này, dung lượng của kênh hợp pháp càng lớn hơn dung lượng của kênh nghe trộm. Trái lại, với  cố định, khi  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. Hình 2 cũng chỉ ra rằng, nếu  thì *PCS*  1, nếu  thì *PCS* 0.

Trái với xác suất khác không của dung lượng bảo mật, xác suất dừng bảo mật (*POut*) sẽ tăng khi  tăng (với  cố định) và giảm khi  tăng (với  cố định). Kết quả này được chỉ ra trong hình 3. Ngoài ra, ta thấy rằng nếu  thì *POut*  0, nếu  thì *POut*1.

Chúng tôi cũng đã mô phỏng sự thay đổi của *PCS* và *POut* theo  với các giá trị khác nhau được lựa chọn của số lượng máy thu bất hợp pháp *N* (người nghe trộm). Kết quả của *PCS* và *POut* trong trường hợp này được chỉ ra lần lượt ở các hình 4 và 5.

Từ hai hình này, ta có nhận xét rằng, khi *N* tăng thì *PCS* giảm, *Pout* tăng và ngược lại. Hay nói cách khác, dung lượng của kênh hợp pháp càng nhỏ hơn dung lượng kênh nghe trộm khi *N* tăng. Điều này đã cho thấy rằng khả năng bảo mật thông tin ở lớp vật lý của hệ thống sẽ giảm khi có nhiều người nghe lén thông tin.



*Hình 4. Ảnh hưởng của số thiết bị nghe trộm đến xác suất khác không của dung lượng bảo mật.*



*Hình 5. Ảnh hưởng của số thiết bị nghe trộm đến xác suất dừng bảo mật hệ thống*

Từ tất cả các kết quả trên ta có nhận xét rằng, hiệu năng bảo mật thông tin ở lớp vật lý của hệ thống sẽ tăng khi tỷ số tín hiệu trên nhiễu trung bình tại phía thu hợp pháp  tăng, giảm khi tỷ số tín hiệu trên nhiễu trung bình tại phía thu bất hợp pháp  và số lượng người nghe trộm *N* tăng.

# Kết luận :

Trong bài báo này chúng tôi đã tính toán để đưa ra biểu thức xác suất tồn tại dung lượng bảo mật và xác suất dừng bảo mật của hệ thống SISO với sự hiện diện của nhiều thiết bị nghe lén thụ động đơn ăn-ten sử dụng đặc tính thống kê của tín hiệu trên nhiễu của các kênh pha-đing khác nhau. Kết quả này có thể sử dụng để lựa chọn các tham số khi thiết kế các hệ thống thực tế để đảm bảo tính bảo mật của hệ thống. Sự trùng khớp giữa kết quả phân tích và mô phỏng cho thấy tính đúng đắn trong nghiên cứu của chúng tôi.

Tài liệu tham khảo

1. P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” *in Proc. ISIT*, 2005, pp. 2152-2155.
2. C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst.Technol. J., vol. 28, pp. 656–715, Oct. 1949.
3. J. Barros and M. Rodrigues, “Secrecy capacity of wireless channel,” in Proc. IEEE Int. Symp. Information Theory (ISIT), Seattle, USA, July 2006, pp. 356-360.
4. 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.
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. Z. Li, R. Yates, and W. Trappe, “Secure communication with a fading eavesdropper channel,” in Pro. IEEE Int. Symp. Information Theory (ISIT), Nice, France, June 24-26, 2007, pp. 1296-1300.
7. Juan M. Romero-Jerez, F. Javier Lapez-Martinex, “A New Framework for the Performance Analysis of Wireless Communications under Hoyt (Nakagami-q) Fading”. IEEE Transaction on Information Theory (Submitted on 3 Mar 2014)
8. J A. D. Wyner, “The wire-tap channel,” *Bell Syst. Technol. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975
9. P. Wang, G. Yu, and Z. Zhang, “On the secrecy capacity of fading wireless channel with multiple eavesdroppers,” in *IEEE International Symposium on Information Theory (ISIT), Nice, France*, June 2007, pp. 1301–1305.
10. D.-B Ha, N.-S. Vo, “Physical layer secrecy performance with transmitter antenna selection over dissimilar fading channels,” *IEEE International Conference on Computer, Communications, and Control Technology (I4CT)*, Malaysia, 2014, pp. 140 – 144.
11. I. Gradshteyn and I. Ryzhik, “Table of Integrals, Series, and Products,” D. Zwillinger, Ed. Elsevier Academic Press, 2007
12. H. A. Suraweera, G. K. Karagiannidis, and P. J. Smith, “*Performance analysis of the dual-hop asymmetric fading channel*,” IEEE Trans. On Wireless Communi., vol. 8, no. 6, pp. 2783–2788, 2009

(BBT nhận bài: …/…/2014, phản biện xong: …/…/2014))

**Thông tin về tác giả**