NGHIÊN CỨU KHẢ NĂNG BẢO MẬT THÔNG TIN Ở LỚP VẬT LÝ TRONG THÔNG TIN VÔ TUYẾN

PHYSICAL LAYER SECURITY FOR WIRELESS COMMUNICATION

TS. Hà Đắc Bình, KS. Vũ Trọng Tân, KS. Trần Đức Dũng
Trung tâm nghiên cứu và phát triển, Trường Đại Học Duy Tân

Tóm tắt: *Trong những năm gần đây, cùng với sự phát triển bùng nổ của thông tin vô tuyến là sự quan tâm ngày càng sâu sắc đến vấn đề bảo mật thông tin trong mạng này. Khác với cách bảo mật truyền thống thực hiện ở lớp ứng dụng, 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 cố gắng giới thiệu một cách tổng quan các hướng nghiên cứu về bảo mật ở lớp vật lý và các kết quả mới nhất trên thế giới. Tiếp theo, chúng tôi phân tích một số vấn đề bảo mật ở lớp vật lý cần được tiếp tục nghiên cứu trong tương lai.*

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

Abstract: *In recent years, the explosive growth of wireless communications is bringing the deepening concern to the security of information networks. Unlike a traditional security implemented at the application layer, physical layer security is considered to be a new approach emerged as attractive themes attracted many researchers today. In this paper, we try to introduce an overview of the research directions in physical layer security and the latest results in the world. Next, we analyze some security issues at the physical layer that need to be further studied in the future.*

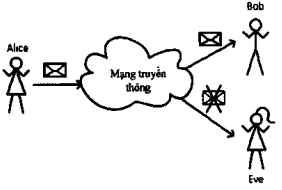
Keywords: *physical layer security, security capacity, security key, wireless communication.*

1. Giới thiệu

Trong những năm gần đây, sự phát triển nhanh chóng của truyền thông không dây 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 không dây 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 tính chất truyền quảng bá của kênh không dây nên nó cung cấp cơ hội nghe trộm và khả năng can thiệp tự nhiên cho những kẻ xấu. Bất cứ ai có một máy thu được điều chỉnh trong phạm vi mà cho phép tỉ lệ tín hiệu trên can nhiễu và nhiễu (SINR) đủ lớn đều có thể nghe trộm, như hình 1. Alice là máy phát, Bob là máy thu hợp pháp và Eve là thiết bị nghe trộm. Việc tìm ra các phương pháp bảo mật hiệu quả để đảm bảo tính bảo mật, tính toàn vẹn và tính xác thực cho tất cả các kết nối không dây là rất cần thiết đối với việc truyền thông tin.

Trong các mạng không dây hiện nay, hầu hết các hệ thống bảo mật đều sử dụng cơ chế bảo mật dựa trên sự tính toán phức tạp, mà người ta cho rằng chưa có cách giải hiệu quả ngoài cách vét cạn, ví dụ như đặt các số nguyên tố lớn hoặc tính toán logarit rời rạc trong nhóm nào đó [1]. Đây là loại bảo mật thường được gọi là "bảo mật dựa trên độ phức tạp tính toán", vì nó được dựa trên giả định rằng kẻ xấu có khả năng tính toán hạn chế và thiếu những thuật toán hiệu quả. Tuy nhiên, giả định này là thiếu sức thuyết phục do sự phát triển không ngừng và nhanh chóng của khả năng tính toán trong máy tính hiện đại (ví dụ như máy tính lượng tử) cũng như các thuật toán hiệu suất cao. Hơn nữa, cách bảo mật truyền thống được thực hiện ở lớp cao hơn (thường là lớp ứng dụng) với giả định rằng các lớp vậy lý (PHY) đã được thiết lập và kết nối không bị lỗi [2]. Tuy nhiên, với sự xuất hiện của mạng ad hoc và mạng phân cấp [3], các kỹ thuật của lớp cao hơn, chẳng hạn như mã hóa, là quá phức tạp và khó thực hiện. Ví dụ, các phương pháp dùng khóa công khai yêu cầu một khối lượng xử lý không lồ, trong khi cơ chế mã hóa khóa đối xứng là rất khó để chia sẻ và quản lý an toàn các khóa bảo mật cho một số lượng lớn người sử dụng. 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 [4]. Kết

quả là, các kỹ thuật bảo mật dựa trên độ tính toán phức tạp không phù hợp với mạng không dây động và ngẫu nhiên quy mô lớn hoặc không phù hợp với các mạng phân cấp hoặc những mạng này có yêu cầu nghiêm ngặt về bảo mật và thời gian. Vì vậy, gần đây đã có nhiều nghiên cứu về khả năng cơ bản của lớp PHY để tạo ra sự thông tin liên lạc an toàn hơn cho mạng không dây [5]. Cách tiếp cận này dựa trên thuyết thông tin đầu tiên được giới thiệu bởi Shannon [6]. Nguyên tắc cơ bản của phương pháp này là bảo mật vô điều kiện, có nghĩa là kẻ nghe trộm có thời gian và tài nguyên tính toán vô tận, có các kiến thức về thuật toán mã hóa, nhưng nó không có được bất kỳ thông tin có ích nào về các bản tin bảo mật do sự ngăn chặn hiệu quả các thông tin ẩn đã được 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 trên thuyết thông tin đã thu hút được sự quan tâm nghiên cứu của các học giả trên khắp thế giới.



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

Trong bài báo này, chúng tôi cố gắng giới thiệu một cách tổng quan các hướng nghiên cứu về bảo mật ở lớp vật lý và các kết quả mới nhất trên thế giới. Tiếp theo, chúng tôi phân tích một số vấn đề bảo mật ở lớp vật lý cần được tiếp tục nghiên cứu trong tương lai. Đặc biệt, chúng tôi phân tích khả năng khai thác những tiến bộ gần đây trong lý thuyết truyền thông không dây đối với mạng chuyển tiếp, mạng vô tuyến nhận thức và kỹ thuật MIMO để nâng cao tính riêng tư truyền thông chống lại các thiết bị nghe trộm hoặc các thiết bị làm nhiễu hoạt động.

Phần còn lại của bài báo được được sắp xếp như sau: Phần 2 giới thiệu các hướng nghiên cứu. Phần 3 đưa các vấn đề cần được tiếp tục nghiên cứu. Cuối cùng, phần 4 là phần kết luận.

2. Các hướng nghiên cứu

Các nhà nghiên cứu trên thế giới gần đây tập trung nghiên cứu vấn đề đảm bảo an toàn thông tin ở lớp vật lý theo ba hướng chính: Một là nghiên cứu bảo mật thông tin dựa trên khóa bảo mật (key-based secrecy) ở lớp vật lý; Hai là nghiên cứu bảo mật thông tin không cần khóa bảo mật (keyless security) thông qua lớp vật lý; Ba là nghiên cứu các phương pháp đánh giá khả năng đảm bảo an toàn thông tin ở lớp vật lý.

2.1. Bảo mật thông tin dựa trên khóa bảo mật

Hướng này chủ yếu tập trung vào việc tìm ra khóa bảo mật dựa trên các đặc tính của môi trường truyền. Hướng này hoàn toàn khả thi vì sự phức tạp của môi trường truyền quảng bá không dây. Ví dụ, những người sử dụng khác nhau sẽ có những phiên bản nhiễu khác nhau của tín hiệu truyền, chính sự khác nhau này cho phép có được khóa bảo mật để mã hóa thông tin, đảm bảo sự an toàn giữa những người sử dụng hợp pháp.

Một khía cạnh quan trọng của bảo mật PHY là việc tạo ra khóa bảo mật hiệu quả. Gần đây có những tiến bộ đáng kể trong việc tìm ra các khóa bảo mật. U. Maurer [7] và R. Ahlswede [8] đầu tiên nghiên cứu tạo các khóa bảo mật với các mô hình loại nguồn, có nghĩa là, hai thiết bị đầu cuối hợp pháp cùng quan sát một nguồn chung ngẫu nhiên mà thiết bị nghe trộm không thể quan sát được. Dựa vào kết quả quan sát này, hai bên thông qua kênh truyền không lỗi công khai để tiến hành thương thảo và tạo ra một khóa bảo mật thống nhất. Thông tin thương thảo thường độc lập với thông tin tạo khóa bảo mật, cho nên nếu bên nghe trộm có được thông tin thương thảo thì cũng không thể có được thông tin liên quan đến việc tạo khóa bảo mật. Trong bài báo [9], các tác giả dùng thông tin pha là nguồn ngẫu nhiên chung, đầu

tiên tiến hành trích pha của hai tín hiệu sóng mang, sau đó lấy độ sai khác của hai pha này đi lượng tử hóa, cuối cùng qua phân nhóm tuyến tính có được khóa bảo mật. Bài báo [10] trích khóa bảo mật từ các tham số ngẫu nhiên Gaussian kết hợp, qua lượng tử hóa, thỏa thuận mã Low-Density Parity-Check (LDPC) và khuếch đại HASH để có được khóa bảo mật thống nhất. Phương pháp này có tỉ lệ thống nhất của khóa bảo mật thấp hơn 10^{-4}, độ dài mã hóa LDPC là 4800bit nên trong quá trình thương thảo chiếm dụng tài nguyên tương đối lớn.

Tuy nhiên, có một số hạn chế trong các phương pháp này. Thứ nhất, thông tin trạng thái kênh (CSI) hoàn hảo được giả định trong nhiều công trình, trong khi trên thực tế tác động của nhiễu, can nhiễu và lỗi kênh là không thể bỏ qua. Thứ hai, hầu hết các phương pháp tiếp cận hiện nay đều phụ thuộc chặt chẽ vào môi trường động và ngẫu nhiên. Sự thay đổi nhanh chóng của các kênh fading trong môi trường động tạo ra thách thức lớn trong việc dự toán chính xác CSI. Ngoài ra, tỉ lệ không khớp của các cặp khóa bảo mật giữa các đối thụ phát hợp pháp trong một số cách tiếp cận hiện tại hầu hết là bội số của 10^{-2} - 10^{-3}, điều này là không thể chấp nhận được.

2.2. Bảo mật thông tin không dựa trên khóa bảo mật

Bên cạnh bảo mật thông tin bằng khóa bảo mật, các nhà nghiên cứu còn chứng minh được rằng mạng vô tuyến có khả năng bảo mật mà không cần dùng đến khóa bảo mật. Công trình tiên phong của Wyner [11] đã phân tích dung lượng bảo mật dương khi các kênh chính có nhiễu ít hơn các kênh nghe trộm. Wyner đã xây dựng một cơ chế mã hóa ngẫu nhiên, trong đó tìm cách ẩn các dòng thông tin trong nhiễu cộng để làm suy yếu thiết bị nghe trộm bằng cách ánh xạ mỗi bản tin cho nhiều từ mã (codeword) theo một phân bố xác suất thích hợp. Bằng cách này, gây ra một sự mơ hồ tối đa tại thiết bị nghe trộm, điều này cho thấy rằng thông tin liên lạc an toàn là có thể không cần sử dụng khóa bảo mật.

Hai tác giả Csiszar và Korner [12] xem xét một phiên bản chung hơn của kênh nghe trộm trong mô hình Wyner, trong đó họ có được sự đặc tả một ký tự đơn bằng ba thông số: tốc độ bản tin riêng, tốc độ mơ hồ và tốc độ bản tin chung cho kênh quảng bá hai máy thu. Kết quả nghiên cứu cho thấy rằng bảo mật thông tin có thể được thực hiện ngay cả khi kênh nghe lén tốt hơn kênh truyền hợp pháp.

Ngoài ra, một số nghiên cứu cho thấy rằng các 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. Ví dụ, công trình [13] phân tích khả năng bảo mật cho kênh fading chậm, trong đó các tác giả xem xét trường hợp CSI đầy đủ và có được dung lượng bảo mật hoàn hảo theo chiến lược phân bổ công suất và tốc độ tối ưu. Công trình [14] phân tích khả năng bảo mật cho kênh fading nhanh và [15] phân tích khả năng bảo mật cho các trường hợp đa ăn-ten khác nhau.

Trong [16], các tác giả nghiên cứu về khả năng sử dụng kỹ thuật lựa chọn các nút chuyển tiếp để tăng khả năng đảm bảo an toàn thông tin ở lớp vật lý, đồng thời chỉ ra việc chọn nút chuyển tiếp dựa trên độ lợi kênh truyền bảo mật tức thời có khả năng bảo mật tốt hơn so với kỹ thuật chọn lựa nút chuyển tiếp truyền thống.

Các công trình [17] [18] nghiên cứu việc ứng dụng truyền thông hợp tác nhằm nâng cao khả năng bảo mật thông tin ở lớp vật lý cho hệ thống vô tuyến.

Các công trình [19] [20] nghiên cứu việc áp dụng kỹ thuật lựa chọn ăn-ten để tăng dung lượng bảo mật và áp dụng lý thuyết trò chơi để giải quyết các bài toán tối ưu trong lĩnh vực này.

Như vậy, bảo mật thông tin không dựa trên khóa bảo mật thường được thực hiện thông qua việc sử dụng mã hóa theo hướng cố gắng để tối đa hóa dung lượng kênh truyền giữa máy phát và máy thu hợp pháp trong hệ thống vô tuyến, trong khi giảm thiểu dung lượng kênh truyền giữa máy phát và máy nghe trộm. Phương pháp này rất hấp dẫn để bảo mật cho các ứng dụng như mạng máy tính phân tán và mạng cảm biến. Thông thường các nút mạng như vậy là tự trị và

triển khai trong môi trường khắc nghiệt, do đó nút có thể tiết lộ thông tin về khóa bảo mật được sử dụng trong cơ chế bảo mật truyền thống dễ gây nguy hiểm cho an ninh mạng.

Tuy nhiên, phương pháp này còn có nhiều nhược điểm, chẳng hạn trong các tính toán thường cần có những thông tin về kênh nghe trộm hoặc các thông tin khác như vị trí, số lượng của máy nghe trộm. Điều này trong thực tế rất khó đạt được vì máy nghe trộm gần như vô hình đối với chúng ta. Hay nói một cách khác, mặc dù các bộ mã hóa tồn tại nhưng chúng vẫn dựa trên giả định rằng thông tin về kẻ nghe trộm kênh là có sẵn. Rõ ràng, giả thiết này không thực tế.

2.3. Các phương pháp đánh giá khả năng đảm bảo an toàn thông tin

Hướng thứ 3 là tìm ra các phương pháp đánh giá một hệ thống có khả năng đảm bảo an toàn thông tin hay không. Một hệ thống có khả năng đảm bảo an toàn thông tin khi mà dung lượng kênh dữ liệu (legitimate channel capacity) phải lớn hơn hoặc bằng dung lượng của kênh nghe trộm (eavesdropper channel capacity). Người ta đưa ra khái niệm dung lượng bảo mật của hệ thống (secrecy capacity) là độ lệch giữa dung lượng kênh dữ liệu và kênh nghe trộm. Một hệ thống được xem là có khả năng đảm bảo an toàn thông tin cao nếu dung lượng bảo mật lớn và nó được xem như là một chỉ số quan trọng để đánh giá hiệu năng bảo mật của hệ thống.

Từ dung lượng bảo mật của hệ thống, người ta đưa ra thông số xác suất khác không của dung lượng bảo mật của hệ thống. Thông số này thể hiện xác suất dung lượng kênh dữ liệu lớn hơn dung lượng của kênh nghe trộm. Bên cạnh dung lượng bảo mật, xác suất dừng bảo mật, Prob($C_s < R$), cũng là một thước đo hiệu năng quan trọng mà những người thiết kế hệ thống cần phải biết.

3. Một số vấn đề còn tồn tại

Mặc dù, bảo mật thông tin lớp vật lý có ứng dụng đầy hứa hẹn trong mạng vô tuyến, nhưng có một số vấn đề còn tồn tại cần được tiếp tục nghiên cứu, đó là:

(1) Còn có cách tạo khóa bảo mật nào mà có hiệu quả bảo mật cao hơn so với các cách hiện thời?

(2) Cơ chế tạo khóa ảnh hưởng như thế nào đến hiệu năng của hệ thống?

(3) Mức độ bảo mật của hệ thống? Các phương pháp đánh giá mức độ bảo mật này?

(4) Tác động của tương quan kênh trong thời gian và không gian đối với khả năng bảo mật như thế nào?

(5) Có thể tạo được bao nhiêu entropy của khóa từ các kênh truyền thực tế?

(6) Các trường hợp thông tin trạng thái kênh từng phần vẫn còn là một vấn đề mở, đây là trọng tâm của các nghiên cứu trong lĩnh vực này.

(7) Thiết kế các giao thức đảm bảo an toàn thông tin ở lớp vật lý dựa trên các thiết kế cơ bản đã công bố. Xây dựng phương pháp tính toán phân tích hiệu năng an toàn thông tin cho hệ thống cũng như xây dựng chương trình mô phỏng.

(8) Phân tích và đánh giá hành vi của hệ thống bằng các công cụ mô phỏng và kết quả phân tích lý thuyết.

(9) Tích hợp các kỹ thuật MIMO, beamforming, truyền thông đa chặng, truyền gia tăng, jamming để tăng cường hơn nữa năng lực đảm bảo an toàn thông tin cho mạng và tối ưu hóa hệ thống.

(10) Vấn đề bảo mật thông tin cho mạng vô tuyến nhận thức được thực hiện như thế nào trong khi mạng này chưa hoàn thiện?

4. Kết luận

Trong bài báo này, chúng tôi đã cố gắng trình bày sơ lược các nghiên cứu liên quan đến vấn đề bảo mật thông tin ở lớp vật lý trong hệ thống vô tuyến theo ba hướng khác nhau: bảo mật dựa trên khoá bảo mật, bảo mật không dựa trên khoá bảo mật và phương pháp đánh giá khả năng bảo mật của các hệ thống. Đồng thời, bài viết cũng chỉ ra nhiều vấn đề cần được tiếp tục nghiên cứu trong tương lai. Rõ ràng, do sự phát triển như vũ bão của các hệ thống vô tuyến, bảo mật thông tin cho các hệ thống này ở lớp vật lý là một mảng nghiên cứu hết sức mới mẻ và thu hút nhiều sự quan tâm trong giới nghiên cứu hiện nay.

Tài liệu tham khảo:

[1]J. A. Buchmann, "Introduction to cryptography," *New York: Springer*, 2000.

[2]M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Tech.*, vol. 54, no.6, pp.2515-34, 2008.

[3] M. Debbah, "Mobile flexible networks: the challenges ahead," *Int. Proc. ATC*, 2008, pp. 3-7.

[4] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. ISIT* 2005, pp. 2152-2155.

[5] P. Tuyls, B. Skoric, and T. Kevenaar, "Security with noisy data – on private biometrics, secure key storage and anti-counterfeiting," *Springer Verlag*, 2007.

[6] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, 1949.

[7] U. Maurer, "Secret key agreement by public discussion form common information," *IEEE Trans. Info. Theory*, vol. 39, pp. 733-742, 1993.

[8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, Part I: secret sharing," *IEEE Trans. Info. Theory*, vol. 39, pp. 1121-1132, 1993.

[9] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Key distribution for mobile radio systems," in *Proc. Japan-Canada Int. Workshop on Multimedia Wireless Communicat- ions and Computing*, Victoria, BC, Canada, 1996.

[10] C. Ye, A. Reznik and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," *Proc. Int. Symp. Inf. Theory*, pp. 2593–2597, July 2006.

[11] A. Wyner. "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[12] I. Csiszar and J. Korner, "Braodcast channels with confidential messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, pp. 339-348, 1978.

[13] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687-5403, 2008.

[14] Z. Li, R. Yates and W. Trappe, "Secure communication with a fading cavesdropper channel," in *Proc. ISIT 2007*, pp. 1296-1300.

[15] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. Info. Theory*, vol. 55, no. 6, pp. 2547-2553, 2009.

[16] Ha Nguyen Vu and Vo Nguyen Quoc Bao, "Study of Relay Selection for Dual-hop Networks under Secrecy Constraints with Multiple Eavesdroppers", *The 2011 International Conference on Advanced Technologies for Communications*, pp. 89-92, Da Nang, Vietnam, 2011.

[17] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in The 46th Annual Allerton Conference on Communication, Control, and Computing, 2008, pp. 1132-1138.

[18] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," EURASIP Journal on Wireless Communications and Networking, vol. 2009, pp. 1-14, 2009.

[19] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of Transmit Antenna Selection Physical Layer Security Schemes," IEEE Signal Processing Letters, vol. 19, pp. 372-375, 2012.

[20] H. Alves, R. D. Souza, and M. Debbah, "Enhanced physical layer security through transmit antenna selection," in IEEE GLOBECOM Workshops (GC Wkshps), 2011, 2011, pp. 879-883.

Ngày nhận bài: 15/12/2013
Ngày chấp nhận đăng: 31/12/2013
Phản Biện: TS Võ Nguyên Sơn