PHÂN TÍCH VÀ ĐÁNH GIÁ KHẢ NĂNG BẢO MẬT THÔNG TIN Ở LỚP VẬT LÝ TRONG HỆ THỐNG UWB ỨNG DỤNG KỸ THUẬT TIME-REVERSAL

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

***Tóm tắt**: Bảo mật thông tin vô tuyến ở lớp vật lý đang là một cách tiếp cận mới và nổi lên thành một đề tài hấp dẫn, thu hút được nhiều nghiên cứu. Để thực hiện việc bảo mật lớp vật lý trong hệ thống vô tuyến, chúng tôi chon hệ thống siêu băng rộng UWB. Công nghệ UWB kết hợp với kỹ thuật TR (Time-Reversal) dùng để cải thiện tốc độ truyền dẫn đồng thời giảm chi phí và độ phức tạp của bộ nhận tín hiệu. Bài báo sẽ đi phân tích và đánh giá về khả năng bảo mật thông tin ở lớp vật lý trong hệ thống UWB TR dựa trên thông số kỹ thuật dung lượng bảo mật (Security Capacity), so sánh với hệ thống không áp dụng kỹ thuật TR để làm sáng tỏ ưu điểm của kỹ thuật này. Thông qua các kết quả mô phỏng sử dụng Matlab, bài báo cũng chỉ ra rằng dung lượng bảo mật của hệ thống UWB được cải thiện đáng kể khi áp dụng kỹ thuật TR.*

***Từ khóa**: bảo mật lớp vật lý, siêu băng rộng, đảo ngược thời gian, dung lượng bảo mật.*

***Abstract**: Securing radio communications at the physical layer is a new approach and emerged into a fascinating topic attracted a lot of researchers. To implement the physical layer security in wireless systems, we choose ultra-wideband UWB system. UWB technology in conjunction with TR (Time-Reversal) is used to improve the speed of transmission and reduces the cost and complexity of receiver. This article analyzes and evaluatesthe possibility of information security at the physical layer in UWB TR system based onsecurity capacity, compared to the system without using TR technique to clarify the advantages of this technique. Simulation results show that the security capacity of UWB system is significantly improved when applying TR technique.*

***Keywords**:physical layer security, UWB, time reversal, security capacity.*

1. Giới thiệu

Trong các mạng không dây hiện nay, hầu hết các hệ thống bảo mật đều sử dụng cơ chế bảo mật dựa trên sự phức tạp tính toán với 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 máy tính hiện đại (máy tính lượng tử) cũng như các thuật toán có hiệu suất cao. Hơn nữa, cách bảo mật truyền thống được thực hiện ở lớp cao hơn, thường là lớp ứng dụng (APP) với giả định rằng lớp vật lý (PHY) đã được thiết lập và không bị lỗi [1]. Với sự xuất hiện của mạng ad hoc và mạng phân cấp [3], các kỹ thuật của lớp APP, chẳng hạn như mã hóa, là quá phức tạp và khó thực hiện. Ngoài ra, việc xác thực và mã hóa trong cơ chế bảo mật ở lớp APP tạo ra độ trễ 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 hay các mạng 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 nhằm nâng cao tính bảo mật trong mạng không dây [5].Để triển khai hướng nghiên cứu về bảo mật lớp vật lý trong hệ thống vô tuyến, chúng tôi chọn hệ thống siêu băng rộng UWB.

Công nghệ UWB với khả năng truyền thông tốc độ cao trong khoảng cách ngắn của nó [6], [7]đã giải quyết hiệu quả các vấn đề hạn chế băng thông trong môi trường không dây [8]. Tuy nhiên, các kênh truyền vô tuyến trong thực tế đều là các kênh fading, vì thế các vấn đề gây ảnh hưởng đến chất lượng truyền dẫn trong hệ thống UWB phục vụ đa người dùng thực sự phức tạp.

Một giải pháp có thể khắc phục vấn đề này là sự kết hợp giữa hệ thống UWB và kỹ

thuật đảo ngược thời gian (Time-Reveral TR) để cải thiện tốc độ truyền dẫn và giảm thiểu các ảnh hưởng dẫn đến giảm chất lượng của hệ thống UWB [7]-[9] của kênh truyền.

Ở [7], các tác giả đã đưa ra các kết quả liên quan đến dung lượng kênh truyền của hệ thống MU MIMO UWB TR xét trong điều kiện môi trường có sự tương quan giữa các ăn-ten.

Ngoài ra, trong bài báo [10], các tác giả đã chỉ ra rằng, dung lượng kênh truyền của các hệ thống UWB thu được trong trường hợp có áp dụng kỹ thuật TR đã tăng đáng kể so với không áp dụng, đồng thời, kỹ thuật TR cho thấy hiệu quả tốt khi hoạt động trong môi trường nhiễu cao.

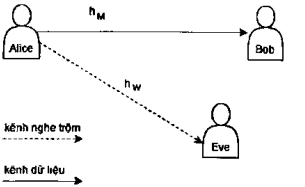
Hiện nay, vấn đề bảo mật trong hệ thống UWB đang tiếp cận ở mức chia sẻ khóa bảo mật giữa trạm phát và thu để từ đó thiết lập kênh truyền an toàn [11]. Do đó, trong bài báo này chúng tôi cố gắng phân tích và đánh giá về khả năng bảo mật thông tin ở lớp vật lý trong hệ thống UWB áp dụng kỹ thuật TR dựa trên thông số kỹ thuật dung lượng bảo mật (Security Capacity), so sánh với hệ thống không áp dụng kỹ thuật TR để làm sáng tỏ ưu điểm của kỹ thuật này.

Các phần còn lại trong bài báo này bao gồm: phần II giới thiệu về mô hình hệ thống được khảo sát, phần III trình bày về dung lượng bảo mật của hệ thống UWB-TR trong 3 trường hợp khác nhau của hệ thống, phần IV đưa ra các kết quả mô phỏng về dung lượng bảo mật của các hệ thống đã trình bày và phần V kết luận.

2. Mô hình hệ thống

Xem xét mô hình hệ thống vô tuyến ở hình 1, bao gồm một máy phát Alice và một máy thu Bob, đồng thời có sự hiện diện của máy nghe trộm Eve trong môi trường fading Rayleigh. Eve là máy nghe trộm thụ động tìm cách trích thông tin từ Alice đến Bob mà không chủ động tấn công.

Hệ thống được khảo sát là hệ thống SISO UWB, tức là bên phát và bên thu (Bob, Eve) đều sử dụng 1 ăn-ten.



Hình 1. *Mô hình hệ thống vô tuyến với một máy nghe trộm*

Dữ liệu truyền từ Alice đến Bob qua kênh truyền dữ liệu (ký hiệu là M); tuy nhiên do tính chất truyền quảng bá của kênh vô tuyến, thông tin này cũng nhận được bởi người nghe trộm Eve qua kênh nghe trộm (ký hiệu là W).

Tín hiệu thu tại kênh truyền hợp pháp Bob tại thời điểm t có dạng:

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

Trong đó: $y_M(t)$là tín hiệu nhận tại người dùng; $x(t)$ là tín hiệu phát;$n_M(t)$ là nhiễu trắng Gausian tại người dùng; $h_M(t)$ là hệ số CIR của môi trường truyền thông giữa Alice và Bob,nó được biểu diễn bằng công thức:

$$h_M\ i = \sum_{l=0}^{L-1} \alpha_l^M \delta\ i-\tau_l^M \quad (2)$$

Với α_l^M và τ_l^M lần lượt là biên độ và trễ của tap l-th [2]. Dạng rời rạc trong miền thời gian của $h_M\ i$ được biểu diễn như sau [3]:

$$h_M(t) = \left[h_M\ 0, h_M\ 1, \ldots, h_M\ L_M\text{-}1\right] \quad (3)$$

Với $h_M\ k$, k = 0,…,L_M-1 là tap k-th của CIR có chiều dài L_M, δ là hàm xung Dirac. Đối với mỗi tuyến xuống, chúng tôi giả sử rằng $h_M(i)$ và $h_W(i)$ là các biến phức Gaussian đối xứng độc lập lẫn nhau với phương sai và trung bình triệt tiêu:

$$E\left[|h_w[k]|^2\right] = e^{\frac{kT_s}{\sigma_{rms}}},$$
$$0 \le k \le L_M - 1 \quad (4)$$

T_S là thời gian lấy mẫu của hệ thống; σ_τ là trải trễ của kênh truyền [2].Tương tự, ta cũng có tín hiệu thu tại kênh nghe trộm tại thời điểm i có dạng:

$$y_W(i) = h_W(i)x + n_W(i), \quad (5)$$

Gọi C_M,C_W là dung lượng của kênh truyền dữ liệu và kênh nghe trộm, theo [12], ta có:

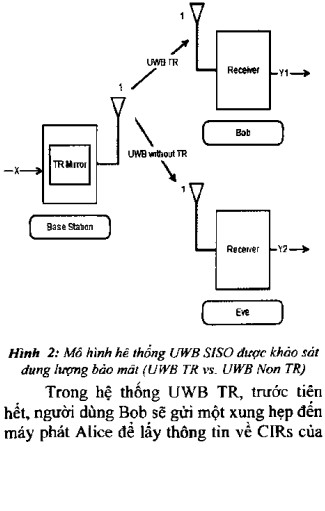
$$C_M = \log(1 + |h_M|^2 SNR_M) \quad (6)$$

$$C_W = \log(1 - |h_W|^2 SNR_W) \quad (7)$$

Với $SNR_M = \frac{P}{N_M}$, $SNR_W = \frac{P}{N_W}$ Trong đó P là công suất phát trung bình của máy phát, h_M và h_W là hệ số CIR tương ứng của kênh dữ liệu và kênh nghe trộm. N_M, N_W là công suất nhiễu tại kênh truyền hợp pháp và kênh nghe trộm.

3. Dung lượng bảo mật của hệ thống SISO UWB-TR

Từ hình 2 ta nhận thấy hệ thống truyền thông của máy phát và người nghe trộm là hệ thống SISO UWB. Dung lượng của kênh truyền bất hợp pháp này ta sử dụng công thức (7). Kênh truyền giữa người dùng và máy phát là hệ thống SISO UWB TR.



Hình 2: Mô hình hệ thống UWB SISO được khảo sát dung lượng bảo mật (UWB TR vs. UWB Non TR)

Trong hệ thống UWB TR, trước tiên hết, người dùng Bob sẽ gửi một xung hẹp đến máy phát Alice để lấy thông tin về CIRs của môi trường truyền thông. Các khối TR Mirrors của máy phát sẽ ghi và lưu trữ các thông tin nhận được và chúng sẽ được sử dụng cho quá trình xử lý tín hiệu phát đi. Do đó, kênh nghe trộm trong trường hợp này không thể sử dụng kỹ thuật TR để tránh trường bị phát hiện. Ngoài ra, trong bài báo này, chúng tôi chỉ xem xét trường hợp máy nghe trộm thụ động chỉ nghe trộm mà không chủ động tấn công hoặc gây nhiễu.

Đặt $g_M(i)$ là hệ số của TR Mirror, được biểu diễn như sau:

$$g_M(i) = \left[h_M^*[L_M - 1], h_M^*[L_M - 2], \ldots, h_M^*[0] \right] \quad (8)$$

Trong đó, $h_M^*[k]$ là liên hợp phức của $h_M[k]$, $0 \le k \le L-1$.Gọi $\hat{h}_M(i)$ là hệ số CIRs tương đương, $\hat{h}_M(i)$ được biểu diễn như sau:

$$\hat{h}_M(i) = h_M(i) * g_M(i) \quad (9)$$

Lúc này, tín hiệu thu tại Bob ở (1) được viết lại như sau:

$$y_M(i) = \hat{h}_M(i)x + n_M(i), \quad (10)$$

Do đó dung lượng kênh truyền của hệ thống SISO UWB TR được tính bằng công thức sau:

$$C_M^{TR} = \log_2\left(1 + \left|\hat{h}_M\right|^2 SNR_M\right) \quad (11)$$

Đặt $\gamma_M = \left|\hat{h}_M\right|^2 SNR_M$ và

$$\gamma_W = |h_W|^2 SNR_W$$

Lúc đó dung lượng bảo mật thông tin được định nghĩa như sau:

$$C_S = \max\left(0, C_M^{TR} - C_W\right) \quad (12)$$

$$C_S = \begin{cases} \log_2(1+\gamma_M) - \log_2(1+\gamma_W) & \text{khi } \gamma_M > \gamma_W \\ 0 \text{ khi } \gamma_M \le \gamma_W \end{cases} \quad (13)$$

Dễ dàng nhận thấy rằng, dung lượng an toàn thông tin của hệ thống là một đại lượng không âm. Dung lượng bảo mật của hệ thống thông tin sẽ bằng 0 khi mà kênh nghe trộm có dung lượng Shannon lớn hơn kênh truyền tải dữ liệu.

4. So sánh dung lượng bảo mật của các hệ thống được khảo sát

Chúng tôi sẽ lần lượt khảo sát hệ thống SISO UWB như trong hình 2 qua các trường

hợp: thay đổi số tap thu đối với kênh truyền hợp pháp và sự ảnh hưởng của SNR đối với dung lượng bảo mật.

4.1. Thay đổi số tap thu trong kênh truyền hợp pháp

Sơ đồ khối của hệ thống khảo sát được mô tả ở hình 2. Từ hình 2 ta thấy rằng, kết nối giữa máy phát và người dùng hợp pháp là hệ thống SISO UWB TR, chỉ sử dụng 1 ăn-ten cho quá trình truyền thông ở cả phía phát và phía thu ($M_T = 1$, $M_R = 1$).

4.2. Khảo sát sự ảnh hưởng của SNR đối với dung lượng bảo mật.

Sơ đồ mô hình khảo sát như trong hình 2, nhưng trong trường hợp này, chúng tôi chỉ xét đến sự ảnh hưởng của tín hiệu trên nhiễu SNR đối với dung lượng bảo mật. Chúng tôi chia thành 2 trường hợp nhỏ:

Cố định SNR của kênh truyền hợp pháp, và

Cố định SNR của kênh truyền bất hợp pháp.

Để thực hiện việc so sánh này, chúng tôi đã mô phỏng dung lượng kênh truyền của kênh truyền hợp pháp trong các hệ thống SISO UWB trong 2 trường hợp có áp dụng và không có áp dụng kỹ thuật Time Reversal; kênh truyền bất hợp pháp trong các hệ thống SISO UWB không sử dụng kỹ thuật TR bằng Matlab với các thông số mô phỏng được cho ở bảng 1.

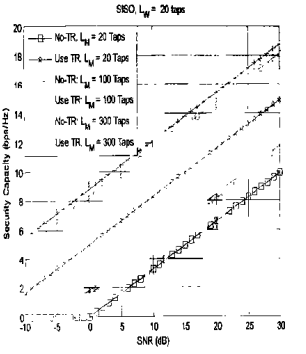
***Bảng 1.** Thông số chung mô phỏng hệ thống SISO*

Thông số	Giá trị
Môi trường	Rayleigh
Thời gian lấy mẫu (T_S)	$\frac{1}{6}10^{-9}$
Trải trễ của kênh truyền (σ_τ)	$125T_S$

Dưới đây là kết quả mô phỏng về dung lượng kênh truyền của các hệ thống UWB TR đã được trình bày trên hình 3:

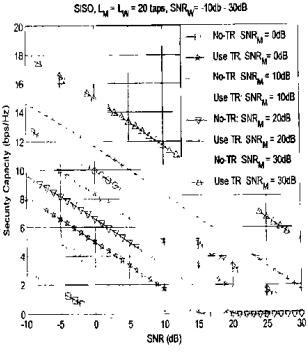
Từ hình kết quả ở hình 3 ta nhận thấy rằng, với cùng số tap thu thì hệ thống UWB sử dụng kỹ thuật TR có dung lượng bảo mật cao hơn so với hệ thống không sử dụng kỹ thuật này.

Khi tăng số lượng tap thu thì dung lượng bảo mật cũng được tăng lên đáng kể.

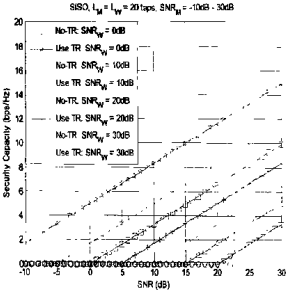


***Hình 3:** Kết quả mô phỏng thay đổi số tap thu của kênh truyền hợp pháp*

Với kết quả trong hình 4 và hình 5, chúng ta nhận thấy rằng, với hệ thống UWB, dung lượng bảo mật của hệ thống sẽ bằng 0 khi SNR của kênh bất hợp pháp cao hơn ngưỡng SNR cố định của kênh hợp pháp. Tuy nhiên, với cùng một ngưỡng SNR cố định cho trước, nếu sử dụng kỹ thuật TR thì dung lượng bảo mật lớn hơn 0 ngay cả khi $SNR_W > SNR_M$



***Hình 4.** Kết quả mô phỏng ảnh hưởng của SNR đối với dung lượng bảo mật khi cố định SNR_M*



***Hình 5.** Kết quả mô phỏng ảnh hưởng của SNR đối với dung lượng bảo mật khi cố định SNR_W*

5.Kết luận

Trong bài báo này, chúng tôi đã tập trung nghiên cứu và thực hiện mô phỏng dung lượng bảo mật kênh truyền của hệ thống SISO UWB trong các trường hợp có áp dụng và không có áp dụng kỹ thuật Time Reversal (TR) để từ đó thấy rõ được ưu điểm và hiệu quả của sự kết hợp giữa hệ thống UWB và kỹ thuật TR.

Các kết quả mô phỏng cho thấy, dung lượng bảo mật tỷ lệ thuận với số lượng tap thu của kênh hợp pháp. Ngoài ra, khi áp dụng kỹ thuật TR, dung lượng bảo mật của hệ thống lớn hơn 0 ngay cả khi SNR của kênh hợp pháp thấp hơn SNR của kênh bất hợp pháp.

Tài liệu tham khảo:

[1] 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.

[2] Andrea Goldsmith, 2005. Wireless Communications. Cambridge University, UK.

[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] R. Liu and W. Trappe, "Securing wireless communications at the physical layer," Springer, 2010.

[6] F. Han, Y.-H. Yang, B. Wang, Y. Wu, and L. K.J.R., "Timereversal division multiple access in multi-path channels," Global Telecommunications Conference 2011, pp. 1–5, 2011.

[7] T. H. Vu, N. T. Hieu, H. D. T. Linh, N. T. Dung, and L. V. Tuan, "Channel capacity of multi user TR-MIMOUWB communications system," in International Conference on Computing, Management and Telecommunications (ComManTel), 2013, pp. 22–26.

[8] D. P. A. M. M. Di Benedetto, T. Kaiser and I. Opperman, UWB Communication Systems A Comprehensive Overview. Hindawi Publising, May, 2006.

[9] R. C. Qiu, C. Zhou, N. Guo, and J. Q. Zhang, "Time reversal with miso for ultrawideband communications: Experimental results," IEEE Antennas Wireless Propag. Lett., vol. 5, no. 1, pp. 269–273, 2006.

[10] T.D.Dung, T.H.Vu, H.D.Binh," Applying Time-Reversal Technique for MU MIMO UWB Communication Systems", The World Congress on Engineering and Computer Science 2013, San Francisco, USA, 23-25 October, 2013.

[11] Wilson. R, Tse.D, Scholtz, R.A, "Channel Identification: Secret Sharing using Reciprocity in Ultrawideband Channels", IEEE International Conference , pp. 270 – 275, 2007.

[12] J. Barros, M. R. Rodrigues, "Secrecy Capacity of Wireless Channels", IEEE International Symposium on, pp. 356 360, 2006

Ngày nhận bài: 28/12/2013
Ngày chấp nhận đăng: 05/01/2014
Phản Biện: TS. Đặng Xuân Kiên