PHÂN TÍCH VÀ ĐÁNH GIÁ KHÓA DỊCH HỖN LOẠN CSK SỬ DỤNG HÀM LOGISTIC MAP 1

Nguyễn Văn Thọ

Khoa Điện- Điện tử, ĐH Duy Tân

Email: vanthodn@gmail.com

Ngô Lê Minh Tâm

Khoa Điện- Điện tử, ĐH Duy Tân

Email: ngotam2611@gmail.com

Tóm tắt: **Trong lĩnh vực thông tin, kỹ thuật hỗn loạn đã được ứng dụng để xây dựng các hệ thống truyền thông an toàn. Trong các hệ thống này, thông tin được bảo mật nhờ vào các đặc điểm vận động hỗn loạn không có chu kỳ và sự phụ thuộc nhạy cảm vào điều kiện khởi động của các hệ hỗn loạn. Trong bài báo này, chúng tôi giới thiệu một phương pháp truyền thông an toàn sử dụng khóa dịch hỗn loạn. Chúng tôi cũng đã phân tích và xây dựng công thức đánh giá hiệu suất của phương pháp này trong trường hợp sử dụng chuỗi hỗn loạn logistic map 1. Các kết quả mô phỏng chứng tỏ tính đúng đắn của phép phân tích.**

Từ khóa : kỹ thuật hỗn loạn; khóa dịch hỗn loạn; chuỗi hỗn loạn logistic map1

I. GIỚI THIỆU

Lý thuyết hỗn loạn, một nhánh của lý thuyết về các hệ phi tuyến thú vị đã được nghiên cứu sâu trong nhiều thập kỷ qua. Trong [1], Poincare đã quan sát và đưa ra những công bố quan trọng đầu tiên về trạng thái hỗn loạn trong hệ thống động phi tuyến (Nonlinear dynamical system).

Năm 1963 Lorenz đã phân tích đối lưu của tầng khí quyển sử dụng mô hình phi tuyến bậc 3[2]. Nghiên cứu của Lorenz đã chỉ ra những đặc điểm quan trọng của hệ thống hỗn loạn. Thứ nhất là tính chất vận động không có chu kỳ: đường di chuyển của hệ thống trong mặt phẳng pha không đi vào bất kỳ điểm cố định hay quỹ đạo có chu kỳ nào khi thời gian vận động tiến tới vô cùng. Thứ hai, hệ hỗn loạn là một hệ xác định, nghĩa là nó không có các thông số thống kê xác suất. Đây là điểm khác nhau quan trọng giữa hệ thống hỗn loạn và hệ thống nhiễu với quá trình ngẫu nhiên. Vận động bất thường trong hệ thống hỗn loạn được tạo ra do tính phi tuyến bên trong nó chứ không phải do nhiễu. Thứ ba là sự phụ thuộc nhạy cảm với các điều kiện khởi động: đường di chuyển xuất phát từ các điều kiện khởi động có sai khác nhau rất nhỏ (gần như là như nhau) sẽ phân tách rất nhanh theo luật số mũ tạo ra các quỹ đạo di chuyển hoàn toàn khác nhau. Nghiên cứu này thúc đẩy các nghiên cứu ứng dụng hỗn loạn trong các chuyên ngành kỹ thuật khác nhau.

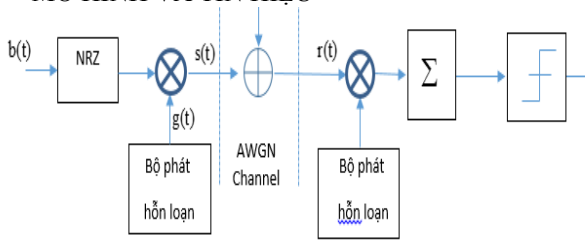
Trong lĩnh vực thông tin, các nghiên cứu ứng dụng kỹ thuật hỗn loạn được phát triển khá nhanh. Nghiên cứu ứng dụng hỗn loạn trong nén tín hiệu đã được đề xuất trong [3], ứng dụng hỗn loạn nhằm giảm nhiễu có cùng giải tần [4][5], đặc biệt đã có rất nhiều nghiên cứu ứng dụng trong lĩnh vực truyền thông an toàn. Trong điều chế tương tự, kỹ thuật mặt nạ hỗn loạn đã được đề xuất [6][7][8][9]. Trong phương pháp này, thông tin được nhúng vào trong tín hiệu hỗn loạn và truyền đi; phía phát tái tạo lại thông tin nhờ việc tạo hệ thống hỗn loạn đồng bộ với phía thu. Tuy nhiên phương pháp này gặp nhiều khó khăn bởi việc đồng bộ hệ thống hỗn loạn là vấn đề khó khăn.

Các phương pháp điều chế số hỗn loạn cũng đã được đề xuất, trong điều chế biến đổi khóa hỗn hợp nhị phân, tín hiệu hỗn loạn mang năng lượng bit khác nhau được sử dụng để truyền thông tin nhị phân [10, 11, 12, 13, 14, 15].Giải điều chế có thể tương quan hoặc không tương quan. Trong giải điều chế tương quan phía thu chứa bản sao của thông tin hệ thống máy phát hỗn loạn. Tùy thuộc vào tín hiệu được truyền đi, một trong các bản sao này sẽ đồng bộ với tín hiệu nhận được và tín hiệu còn lại sẽ không được đồng bộ hóa ở đầu thu. Do đó bộ thu sẽ biết thông tin bit truyền đi.Đối với các máy thu không tương quan, yêu cầu các tín hiệu hỗn loạn được truyền phải có các năng lượng bit khác nhau (tức là các mức thông tin khác nhau cho các bit thông tin "1" và "0"). Do đó, bằng cách so sánh năng lượng bit với ngưỡng quyết định (hoạt động giống như một bộ lọc phù hợp), chúng ta có thể dễ dàng khôi phục các bit thông tin ban đầu được truyền đi.

Trong bài báo này chúng tôi giới thiệu hệ thống truyền thông an toàn sử dụng khóa dịch hỗn loạn. Chúng tôi cũng phân tích và đánh giá hiệu năng của hệ thống truyền thông này trong trường hợp sử dụng chuỗi hỗn loạn rời rạc Logictic map 1.

Phần tiếp theo của bài báo được tổ chức như sau : Phần 2 theo giới thiệu mô hình truyền thông khóa dịch hỗn loạn và phân tích các đặc tính của hàm hỗn loạn rời rạc logictic map 1. Phần 3 phân tích và đánh giá hiệu năng BER của hệ thống. Phần 4 trình bày những kết quả mô phỏng và thảo luận. Cuối cùng là phần kết luận.

II. MÔ HÌNH VÀ TÍN HIỆU



Hình 1: Mô hình truyền thông khóa dịch hỗn loạn

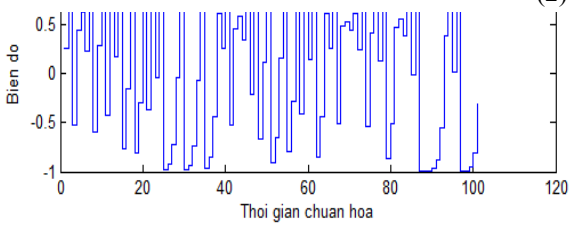
Điều chế khóa dịch hỗn loạn sử dụng chuỗi tín hiệu hỗn loạn với các năng lượng bit khác nhau để truyền thông tin nhị phân. Nếu bit dữ liệu thứ i là α_i =+1, thì chuỗi hỗn loạn g1 được phát đi, nếu bit dữ liệu thứ i α_i = -1 thì chuỗi hỗn loạn g2 được truyền đi. Trình tự hỗn loạn cho CSK g1 và g2 có thể được tạo theo ba cách khác nhau. Phương pháp đầu tiên: sử dụng hai máy phát hỗn loạn khác nhau. Phương pháp thứ hai: tạo ra hai trình tự sử dụng các điều kiện ban đầu khác nhau của cùng một bộ tạo hỗn loạn. Và phương pháp cuối cùng: hai chuỗi được tạo ra bởi cùng một bộ tạo hỗn loạn với cùng điều kiện ban đầu nhưng được nhân với hai hằng số khác nhau. Trong bài báo này, chúng tôi đã sử dụng phương pháp cuối cùng để tạo ra hai chuỗi hỗn loạn. Mô hình truyền thông khóa dịch hỗn loạn được thể hiện ở hình 1.

Trong mô hình này, hai chuỗi hỗn loạn có liên quan g2 = −g1. Giả sử chúng ta chỉ xử lý hệ nhị phân, trong đó dấu hiệu của tín hiệu nhị phân được sử dụng để xác định chuỗi hỗn loạn, do đó đầu ra của bộ phát có thể được viết dưới dạng

$$s_k = \alpha_i g_k \tag{1}$$

Trong phạm vi bài báo này chúng tôi sử dụng hàm logictic map 1 cho chuỗi hỗn loạn g(t). Hàm logictic map 1 biểu diễu bởi công thức sau

$$g_{k+1} = 1 - 2g_k^2; g_0 = (-1,1) \tag{2}$$



Hình 2. Dạng sóng biểu diễn của logictic map 1

Hàm mật độ xác suất PDF của g(t) được xác định như sau [11]

$$\rho = \begin{cases} \dfrac{1}{\pi\sqrt{1-g^2}}, & \text{if } |g| < 1 \\ 0, & \text{if other} \end{cases} \tag{3}$$

Công suất trung bình và phương sai của g.

$$P_s = E(g^2) = \int_{-\infty}^{\infty} g^2 \rho(g)dg = \int_{-1}^{1} g^2 \frac{1}{\pi\sqrt{1-g^2}} dg = \frac{1}{2} \tag{4}$$

$$\Delta = \text{var}(g^2) = E(g^4) - E^2(g^2) = \int_{-1}^{1} g^4 \rho(g)dg = \frac{1}{8} \tag{5}$$

Tại phía thu, các tham số của hệ thống hỗn loạn và điều kiện ban đầu được sử dụng để tạo tín hiệu sóng mang ở máy phát phải có sẵn tại máy thu để tạo ra tín hiệu tham khảo giống hệt ở máy phát và máy thu giải điều chế thông qua sự tương quan liên kết.(coherent correlation).

Tính an toàn của hệ thống thông tin này nhờ vào đặc tính không thể dự đoán và nhạy cảm với điều kiện đầu của hàm hỗn loạn g(t). Nếu bên thu không có các tham số của hàm hỗn loạn nó không thể tạo ra tín hiệu tham khảo tương quan để giải điều chế.

III. PHÂN TÍCH VÀ ĐÁNH GIÁ

Đối với loại bộ thu tương quan, đầu ra bộ tương quan zi của bit thứ i được cho bởi

$$z_i = \sum_{k=2\beta(1-i)+1}^{2\beta i} r_k g_k \tag{6}$$

trong đó $r_k = s_k + n_k$ là tín hiệu nhận được trong môi trường AWGN trong

2β là số mẫu hỗn loạn sử dụng để truyền 1 ký hiệu nhị phân.

Bây giờ chúng ta có:

$$z_i = \alpha_i \sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2 + \sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \tag{7}$$

BER của hệ thống có thể được xây dựng như sau:

$$BER = P(\alpha_i = 1).P(z_i < 0 | \alpha_i = 1) + P(\alpha_i = -1).P(z_i < 0 | \alpha_i = -1)$$

$$= \frac{1}{4} Q\left(\frac{E(z_i|\alpha_i=1)}{\sqrt{2\,\text{var}(z_i|\alpha_i=1)}}\right) Q\left(\frac{E(z_i|\alpha_i=-1)}{\sqrt{2\,\text{var}(z_i|\alpha_i=-1)}}\right) \tag{8}$$

Do phương sai của $z_i \big| (\alpha_i = +1)$ bằng với phương sai của $z_i \big| (\alpha_i = -1)$

và chúng ta có $E\{z_i | \alpha_i = +1\} = -E\{z_i | \alpha_i = -1\}$, trong đó E là kỳ vọng. Do đó ta có

$$BER = \frac{1}{2} Q\left(\frac{E\{z_i | \alpha_i = 1\}}{\sqrt{2 \operatorname{var}(z_i | \alpha_i = 1)}} \right) \tag{9}$$

Với $$Q(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-\lambda^2} d\lambda \tag{10}$$

$$E\{z_i | \alpha_1 = 1\} = \sum_{k=2\beta(1-i)+1}^{2\beta i} E\{g_k^2\} + \sum_{k=2\beta(1-i)+1}^{2\beta i} E[g_k] E[n_k] = 2\beta E\{g_k^2\} \tag{11}$$

Ta lần lượt tính các thành phần trong biểu thức

$$\operatorname{var}\{z_i | \alpha_1 = 1\} = 2 \operatorname{cov}\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2, \sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \right) + \operatorname{var}\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \right) + \operatorname{var}\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2 \right)$$

$$\operatorname{cov}\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2, \sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \right) \tag{12}$$

$$= E\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2 \sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \right) - E\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^2 \right) E\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k n_k \right)$$

$$= E\left(\sum_{k=2\beta(1-i)+1}^{2\beta i} g_k^3 n_k + \sum_{k=2\beta(1-i)+1}^{2\beta i} \sum_{j=2\beta(1-i)+1}^{2\beta i} n_k g_k g_j^2 \right) - \sum_{k=2\beta(1-i)+1}^{2\beta i} E\{g_k^2\} \sum_{k=2\beta(1-i)+1}^{2\beta i} E[g_k n_k]$$

$$= \sum_{k=2\beta(1-i)+1}^{2\beta i} E\{g_k^3\} E[n_k] + \sum_{k=2\beta(1-i)+1}^{2\beta i} \sum_{j=2\beta(1-i)+1}^{2\beta i} E[n_k] E\{g_k g_j^2\} = 0$$

(13)

$$= \sum_{k=2\beta(1-i)+1}^{2\beta i} \left(E\{g_k^2 n_k^2\} - E^2[g_k n_k] \right) + \sum_{j=2\beta(1-i)+1}^{2\beta i} \sum_{k=2\beta(1-i)+1}^{2\beta i} \left(E\{g_j n_j g_k n_k\} - E\{g_j n_j\} E\{g_k n_k\} \right)$$

$$= \sum_{k=2\beta(1-i)+1}^{2\beta i} \left(E\{g_k^2\} E\{n_k^2\} - E^2[g_k] E^2[n_k] \right)$$

$$+ \sum_{j=2\beta(1-i)+1}^{2\beta i} \sum_{k=2\beta(1-i)+1}^{2\beta i} \left(E\{g_j g_k\} E\{n_j n_k\} - E\{g_j\} E\{g_j\} E[g_k] E[n_k] \right)$$

$$= 2\beta \frac{N_0}{2} E\{g_k^2\} = \beta N_0 E\{g_k^2\}$$

(14)

$$= \sum_{k=2\beta(1-i)+1}^{2\beta i} \operatorname{var}\{g_k^2\} + \sum_{k=2\beta(1-i)+1}^{2\beta i} \sum_{j=2\beta(1-i)+1}^{2\beta i} \left(E\{g_j^2 g_k^2\} - E\{g_j^2\} E\{g_k^2\} \right)$$

$$= 2\beta \operatorname{var}\{g_k^2\}$$

(15)

Thay (13) (14) (15) vào biểu thức (12) ta có

$$\operatorname{var}\{z_i | \alpha_1 = 1\} = 0 + \beta N_0 E\{g_k^2\} + 2\beta \operatorname{var}\{g_k^2\} \tag{16}$$

Từ (9) (11) (16) ta có :

$$BER = \frac{1}{2} Q\left(\frac{E\{z_i | \alpha_i = 1\}}{\sqrt{2 \operatorname{var}(z_i | \alpha_i = 1)}} \right) = \frac{1}{2} Q\left(\frac{2\beta E\{g_k^2\}}{\sqrt{2\beta N_0 E\{g_k^2\} + 2\beta \operatorname{var}\{g_k^2\}}} \right) = \frac{1}{2} Q\left(\frac{1}{\sqrt{\frac{\operatorname{var}\{z_i\}}{\beta E^2\{g_k^2\}} + \frac{N_0}{E\{g_k^2\}}}} \right)$$

$$= \frac{1}{2} Q\left(\frac{1}{\sqrt{\frac{E_b^2}{\beta \operatorname{var}\{g_k^2\}} + \frac{E_b}{N_0}}} \right) \tag{17}$$

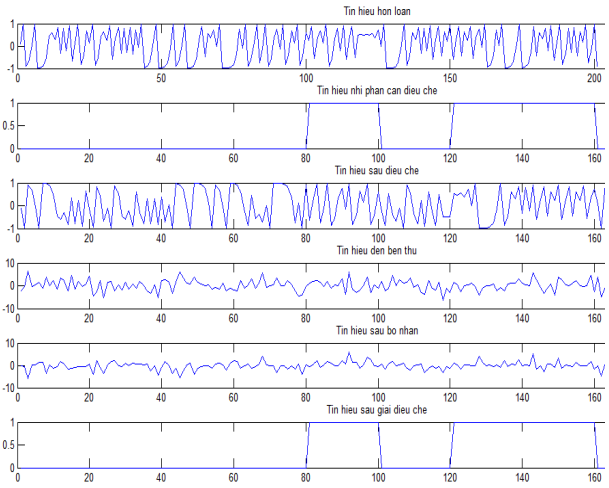
Với $E_b = 2\beta E\{g_k^2\}$

Trong trường hợp sử dụng hàm logictic map 1 cho chuỗi hỗn loạn. Thay (4) (5) vào biểu thức (17) ta có

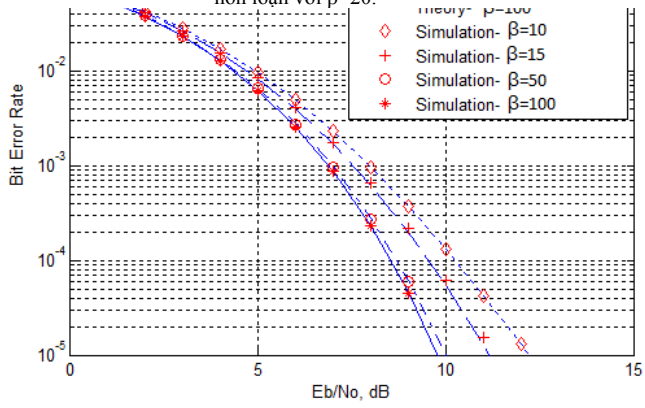
$$BER = \frac{1}{2} Q\left(\frac{1}{\sqrt{(2\beta)^{-1} + \left(\frac{E_b}{N_0} \right)^{-1}}} \right) \tag{18}$$

IV. KẾT QUẢ MÔ PHỎNG VÀ THẢO LUẬN

Chúng tôi đã tiến hành mô phỏng khóa dịch hỗn loạn. Hình 3 thể hiện kết quả mô phỏng tín hiệu điều chế và giải điều chế khóa dịch hỗn loạn đối xứng với chuỗi hỗn loạn logictic map 1, số mẫu hỗn loạn cho 1 bit β=20.



Hình 3. Kết quả mô phỏng điều chế/giải điều chế sử dụng khóa dịch hỗn loạn với β=20.



Hình 4. Kết quả mô phỏng hiệu suất BER với các trường hợp β khác nhau.

Ta có thể nhận thấy β càng lớn hiệu suất của CSK càng tốt. Mặt khác, khi giá trị β nhỏ, một sự tăng nhẹ β cũng làm tăng đáng kể hiệu suất. Tuy nhiên trong trường hợp β lớn (50-100), sự tăng giảm β không ảnh hưởng nhiều đến hiệu suất.

V. KẾT LUẬN

Trong bài báo này chúng tôi đã giới thiệu mô hình truyền thông sử dụng khóa dịch hỗn loạn. Chúng tôi cũng đã phân tích và đưa ra biểu thức đánh giá hiệu suất của phương pháp này trong trường hợp chuỗi hỗn loạn được sử dụng là hàm logictic map 1. Kết quả mô phỏng đã khẳng định tính đúng đắn của kết quả phân tích. Các kết quả này cho thấy việc tăng cường bảo mật lớp vật lý của hệ thống truyền thông sử dụng khóa dịch hỗn loạn là một phương pháp có tính khả thi cao.

TÀI LIỆU THAM KHẢO

[1] S. H. Strogatz, Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry, And Engineering.: Westview Press, 2001

[2] E. N. Lorenz, "Deterministic nonperiodic flow," Journal of the Atmospheric Sciences, vol. 20, pp. 131-140, 1963

[3] H. Dedieu and M. J. Ogorzalek, "Nonlinear approach to signal coding and compression," in European Conference on Circuit Theory and Design (ECCTD'99), Stresa-Italy, 1999, pp. 58-61

[4] Z. Jákó and G. Kolumbán, "Carrier generation for chaotic communication by fourth-order analog phase-lock loop," in International Symposium on Nonlinear Theory and its Applications (NOLTA'98), Crans-Montana, Switzerland, 1998, pp. 827-830

[5] E. J. Kostelich and T. Schreiber, "Noise reduction in chaotic time series data: A survey of common methods," Physical Review E, vol. 48, pp. 1752-1763, 1993

[6] L. Kocarev, K. Halle, K. Eckert, and L. O. Chua, "Experimental demonstration of secure communication via chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, no. 3, pp. 709-713, 1992

[7] E. J. Kostelich and T. Schreiber, "Noise reduction in chaotic time series data: A survey of common methods," Physical Review E, vol. 48, pp. 1752-1763, 1993

[8] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Digi-tal communication using chaotic-pulse-position modulation," IEEE Transactions on Circuits and Systems, vol. 48, no. 12, pp. 1436–1444, 2001.

[9]M. M. Sushchik and et al., "Chaotic pulse position modu-lation: a robust method of communicating with chaos," IEEE Communication Letters, vol. 4, no. 4, pp. 128–130, 2000.

[10]Y.-S. Lau and Z. M. Hussain, "A new approach in chaos shift keyingfor secure communication," in Proc IEEE International Conference onInformation Technology and Applications 2005, Sydney, Australia, July2005.

[11]F. C. M. Lau, C. K. Tse, M. Ye, and S. F. Hau, "Coexistence of chaos-based and conventional digitalcommunication systems of equal bit rate,"IEEE Trans. Circuits and Systems, vol. 51, pp. 391-408, Feb. 2004.

[12]F. C. M. Lau and C. K. Tse, “Coexistence of chaos-based and conventionaldigital communication system,” in Proc IEEE ISCAS, vol. 3, pp. III-204- III-207, may. 2003

[13]G. Kolumban, “Theoretical Noise Performance of Correlator-BasedChaotic Communications Schemes,” IEEE Trans. Circuits and SystemsI: Fundamental Theory and Applications,, Vol. 47, No. 12, 2000.

[14]G. Kolumban, M. P. Kennedy, Z. Jako, and G. Kis, “Chaotic communications with correlator receivers: theory and performance limits,” in Procof the IEEE, vol. 90, pp. 711-732, 2002.

[15]A. Abel and W. Schwarz, “Chaos CommunicationsŮPrinciples, Schemes,and System Analysis,” Invited paper in IEEE Proc, Vol. 90, No. 5, May2002.