hoặc tương tự. Kết quả này được công bố công trình số 1 của luận án.

2. Đề xuất phương pháp tạo chuỗi trải MLS sử dụng mã cyclic cục bộ trên phân hoạch vành đa thức cho phép tạo được nhiều bộ mã có độ dài từ mã khác nhau. Các bộ mã được tạo ra bằng phương pháp này có thể thay thế cho chuỗi trải MLS tạo bằng LFSR truyền thống và hoàn toàn có thể áp dụng cho các hệ thống CCSK và DSSS. Kết quả này được công bố công trình số 3 của luận án.

3. Đánh giá ảnh hưởng của hệ thống CCSK trên các kênh pha-đinh biến đổi nhanh, đề xuất phương pháp mã hóa/giải mã vi sai ở mức chip cho phép cải thiện phẩm chất BER của hệ thống CCSK. Đề xuất này đem lại khả năng ứng dụng của CCSK trong các hệ thống thực tế, nhằm hạn chế yêu cầu khó khăn về ước lượng kênh truyền biến đổi nhanh. Kết quả này được thể hiện tại công trình số 2 và 4 của luận án.

4. Đề xuất một phương pháp san bằng trên miền tần số cho hệ thống CCSK đơn sóng mang nhằm đem lại hiệu quả về phẩm chất BER trên kênh chọn lọc theo tần số. Phương pháp đề xuất sử dụng san bằng MRC hứa hẹn thích hợp cho ứng dụng vào các hệ thống thực tế nhờ tính chất đơn giản và hiệu quả lớn. Kết quả được thể hiện tại công trình số 5 của luận án.

B. Hướng phát triển của luận án

Để khắc phục hai hiệu ứng của kênh truyền là tính chất chọn lọc theo thời gian và tính chất chọn lọc theo tần số, luận án đã đề xuất hai giải pháp là sử dụng mã hóa/giải mã vi sai ở mức chip và san bằng trên miền tần số. Tuy nhiên, hai giải pháp này mới chỉ được đề xuất độc lập. Trong môi trường làm việc thực tế kênh truyền có thể chịu ảnh hưởng đồng thời của cả hai hiện tượng này. Vì vậy, việc nghiên cứu đề xuất một giải pháp kết hợp hoàn chỉnh sẽ có ý nghĩa hơn. Đây cũng chính là một hướng phát triển tiếp theo của luận án.

GIỚI THIỆU LUẬN ÁN

Tính cấp thiết của đề tài

Hiện nay các hệ thống thông tin vô tuyến điện quân sự đang được đầu tư nghiên cứu nhằm đáp ứng các yêu cầu tác chiến trong chiến tranh hiện đại. Vì vậy, đòi hỏi hệ thống phải có khả năng bảo mật, *chống lại hiện tượng chế áp điện tử và các hình thức thu chặn tin tức*. Một trong các giải pháp hiệu quả đáp ứng các yêu cầu nói trên là kỹ thuật trải phổ (SS: Spread Spectrum). Sử dụng một chuỗi trải ngẫu nhiên để trải tín hiệu phát. Chuỗi trải ngẫu nhiên tốt và sử dụng phổ biến nhất chính là chuỗi có độ dài cực đại (MLS: Maximal Length Sequence), thường được tạo ra nhờ sử dụng các thanh ghi dịch có phản hồi tuyến tính. Tuy nhiên, phương pháp này có nhược điểm là *số chuỗi tạo ra ít do giới hạn về số đa thức sinh* có được. Để khắc phục các nhược điểm trên của các hệ thống trải phổ, kỹ thuật khóa dịch mã tuần hoàn (CCSK: Cyclic Code Shift Keying) đã được giới thiệu gần đây. Nguyên lý hoạt động của kỹ thuật khóa dịch mã tuần toàn CCSK tương tự như của hệ thống DSSS, điểm khác biệt cơ bản so với DSSS là *chuỗi trải của hệ thống CCSK biến đổi theo dữ liệu đầu vào.* Mặt khác, để nâng cao tính bảo mật, chống thu chặn của CCSK, tác giả đề xuất áp dụng một phương pháp tạo chuỗi mới dựa trên mã cyclic cục bộ. Ưu điểm của mã cyclic cục bộ là có thể xây dựng được mã trên mọi vành đa thức (n bất kỳ), nên việc dò mã và thu chặn của đối phương sẽ gặp khó khăn hơn. Vì vậy, việc nghiên cứu đánh giá phẩm chất của CCSK một chủ đề nghiên cứu cần thiết, có ý nghĩa khoa học và thực tiễn nên tác giả chọn đề tài: ***" Nghiên***

cứu đánh giá phẩm chất hệ thống khóa dịch mã tuần hoàn sử dụng mã quasi cyclic”.

Mục tiêu nghiên cứu của đề tài

Nghiên cứu đánh giá chất lượng của CCSK trên các kênh truyền pha-đinh Rayleigh và Rice chịu ảnh hưởng của hiệu ứng Doppler. Nghiên cứu đề xuất phương pháp mã hóa và giải mã cho CCSK làm việc trên kênh pha-đinh biến đổi nhanh. Nghiên cứu kỹ thuật san bằng trên miền tần số cho hệ thống CCSK.

Phương pháp nghiên cứu

Phương pháp nghiên cứu sử dụng trong luận án là kết hợp giải tích với mô phỏng Monte-Carlo. Phương pháp giải tích được sử dụng để biểu diễn, xây dựng mã và thiết lập mô hình hệ thống. Mô phỏng Monte-Carlo được sử dụng để ước lượng các tham số đánh giá chất lượng hệ thống (BER).

Đối tượng nghiên cứu

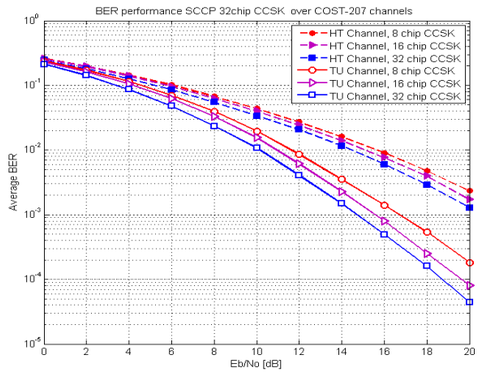
Kênh vô tuyến; mã cyclic và cyclic cục bộ; các hệ thống trải phổ; các hệ thống truyền dẫn CCSK**.**

Phạm vi nghiên cứu

Nghiên cứu các chuỗi trải CCSK tạo ra từ mã cyclic cục bộ, khảo sát, đánh giá hệ thống trên kênh pha-đinh.

Bố cục luận án

Luận án được trình bày 122 trang ngoài phần mở đầu và kết luận, luận án chia thành 4 chương. Chương 1: Tổng quan về kênh truyền vô tuyến. Chương 2: Kỹ thuật trải phổ và phương pháp tạo chuỗi trải. Chương 3: Kỹ thuật khóa dịch mã tuần hoàn sử dụng chuỗi trải từ mã



Hình 4-5 Phẩm chất BER trên các kênh HT và TU theo COST-207 $M = \{8,16,32\}$, $f_D T_c = 0.001$

4.6 Kết luận chương

Chương 4 luận án đã đề xuất phương pháp san bằng trên miền tần số cho hệ thống CCSK đơn sóng mang sử dụng tiếp đầu tuần hoàn. Phương pháp đề xuất sử dụng tính tương quan và quyết định trực tiếp trên miền tần số nên cho phép giảm thiểu độ phức tạp tính toán so với trường hợp tính tương quan trên miền thời gian. Kết quả khảo sát cho thấy bộ san bằng sử dụng MRC đạt được hiệu quả cao nhất, các bộ san bằng có thể đạt được hiệu quả san bằng tốt hơn trên kênh TU so với kênh HT do tính chất chọn lọc theo tần số thấp hơn.

KẾT LUẬN

Nội dung luận án đã thực hiện được các nhiệm vụ đề ra là tiến hành nghiên cứu về hệ thống khóa dịch mã tuần hoàn (CCSK), đánh giá khả năng ứng dụng của CCSK trong thông tin quân sự.

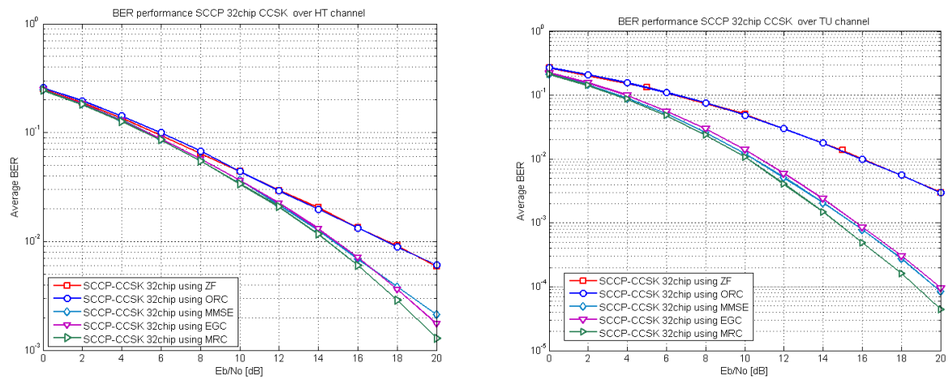
A. Các kết quả của luận án

1. Đề xuất một phương pháp biểu diễn mã cyclic cục bộ mới trên miền tần số. Phương pháp biểu diễn mới này thích hợp cho các hệ thống xử lý tín hiệu trên miền tần số như các hệ thống kết hợp trải phổ và OFDM

là kênh pha-đinh Rayleigh chọn lọc theo tần số, mô hình kênh đô thị (TU: Typical Urban) và kênh đồi núi (HT: Hilly Terrain).

4.5.2 Kết quả mô phỏng

Thứ nhất, trong số các bộ san bằng thì bộ san bằng sử dụng kết hợp tỉ lệ cực đại MRC cho phẩm chất BER tốt nhất, tiếp theo là hai bộ san bằng MMSE và EGC, và cuối cùng là hai bộ san bằng ORC và ZF.



(a) Hilly Terrain Channel (b) Typical Urban channel

Hình 4-4 Phẩm chất BER của các bộ san bằng FDE trên các kênh HT và TU theo COST-207 $M = 32$, $f_D T_c = 0.001$

Nhận xét thứ hai có thể thấy là phẩm chất bộ san bằng có thể đạt được tốt hơn trên kênh TU so với kênh HT. Có thể thấy rõ trên hình vẽ là với san bằng sử dụng kết hợp MRC tại $E_b / N_0 = 20\text{dB}$ tỉ lệ lỗi thu được là $\text{BER} = 4{,}5 \times 10^{-5}$ trên kênh TU, trong khi đó trên kênh HT chỉ là $\text{BER} = 1{,}5 \times 10^{-3}$. Hình 4-5 so sánh phẩm chất BER trong các trường hợp sử dụng chuỗi trải CCSK có độ dài khác nhau (*M* = 8, 16, 32). Có thể quan sát thấy là đối với cả hai kênh TU và HT có thể đạt được hiệu quả tốt hơn khi tăng chiều dài chuỗi trải. Hiệu quả đạt được vào khoảng 1dB trên kênh TU và khoảng 0,5dB trên kênh HT.

cyclic cục bộ. Chương 4: Kỹ thuật san bằng trên miền tần số cho hệ thống CCSK.

CHƯƠNG 1: TỔNG QUAN VỀ KÊNH TRUYỀN VÔ TUYẾN

1.1 Thông tin vô tuyến

Thông tin vô tuyến là phương thức truyền dẫn thông tin thông qua môi trường không gian tự do.

1.2 Đặc tính kênh truyền vô tuyến

1.2.1 Truyền sóng trong không gian tự do

Mô hình truyền sóng trong không gian tự do được sử dụng để ước lượng suy hao của tín hiệu thu trong môi trường truyền thẳng không có các vật che chắn.

1.2.2 Ảnh hưởng của phản xạ, tán xạ và nhiễu xạ

Phản xạ, tán xạ, nhiễu xạ là ba yếu tố gây ảnh hưởng nhiều đến quá trình truyền sóng trong các hệ thống thông tin vô tuyến.

1.2.3 Hiện tượng bóng che vô tuyến

Hiện tượng bóng che vô tuyến xảy ra khi quá trình truyền sóng gặp phải các vật che chắn lớn liên tiếp.

1.2.4 Đáp ứng xung của kênh truyền

Đáp ứng xung của kênh truyền là đặc tính băng rộng của kênh.

1.2.5 Trải trễ

Trải trễ trung bình của kênh truyền $\bar{\tau}$ là một tham số được sử dụng để đánh giá mức độ phân tán của kênh.

1.2.6 Băng thông liên kết

Băng thông liên kết B_c được định nghĩa là trải trễ hiệu dụng (*rms: root mean square delay spread*).

1.2.7 Dịch tần Doppler

Khi có sự chuyển động tương đối giữa máy thu và máy phát dẫn đến thay đổi tần số một cách ngẫu nhiên, từng sóng đa đường bị dịch tần số. Dịch tần số trong tần số thu do chuyển động tương đối này được gọi là dịch tần Doppler.

1.2.8 Thời gian liên kết

Thời gian liên kết T_{ch} được sử dụng để đặc trưng cho bản chất tán xạ theo tần số của kênh trên miền thời gian.

1.3 Hiện tượng pha-đinh đa đường

Tín hiệu phát thường đến được ăng-ten thu qua nhiều đường khác nhau do hiện tượng bị phản xạ hoặc tán xạ bởi các vật cản và che chắn. Hiện tượng truyền sóng như trên được gọi là hiện tượng truyền sóng đa đường.

1.3.1 Kênh pha đinh chọn lọc và không chọn lọc theo tần số

1.3.1.1 Pha đinh phẳng

Một tín hiệu được coi là chịu ảnh hưởng của pha-đinh phẳng nếu $B_s \ll B_c$ và $T_s \gg \sigma_\tau$, trong đó T_s là thời gian symbol, tức là $T_s = 1/B_s$.

1.3.1.2 Pha đinh chọn lọc theo tần số

Một tín hiệu chịu ảnh hưởng của pha-đinh chọn lọc theo tần số nếu $B_s > B_c$ và $T_s < \sigma_\tau$

1.3.2 Kênh biến thiên và không biến thiến theo thời gian

1.3.2.1 Kênh biến thiên theo thời gian

Kênh biến thiên theo thời gian hay còn gọi *kênh pha-đinh biến đổi nhanh* nếu thời gian liên kết T_{ch} của kênh nhỏ hơn T_s của tín hiệu phát. ($T_s > T_{ch}$ và $B_s < f_m$).

1.3.2.2 Kênh không biến thiên theo thời gian

$$W_n^{\mathrm{MMSE}} = \frac{H_n^*}{\left|H_n\right|^2 + \frac{\sigma_z^2}{\sigma_c^2}}. \tag{4.13}$$

4.3.3 Kết hợp tỉ lệ cực đại (MRC)

Phương pháp san bằng MRC được phát triển trên cơ sở phương pháp kết hợp phân tập không gian

$$W_n^{\mathrm{MRC}} = H_n^*. \tag{4.14}$$

4.3.4 Kết hợp đồng độ lợi (EGC)

Phương pháp kết hợp EGC là một trường hợp rút gọn đơn giản của phương pháp MRC

$$W_n^{\mathrm{EGC}} = \frac{H_n^*}{\left|H_n^*\right|} \tag{4.15}$$

4.3.5 Kết hợp khôi phục trực giao (ORC)

Mục đích của phương pháp ORC là nhằm khôi phục tính chất trực giao của các mã.

$$W_n^{\mathrm{ORC}} = \frac{H_n^*}{\left|H_n^*\right|^2} \tag{4.16}$$

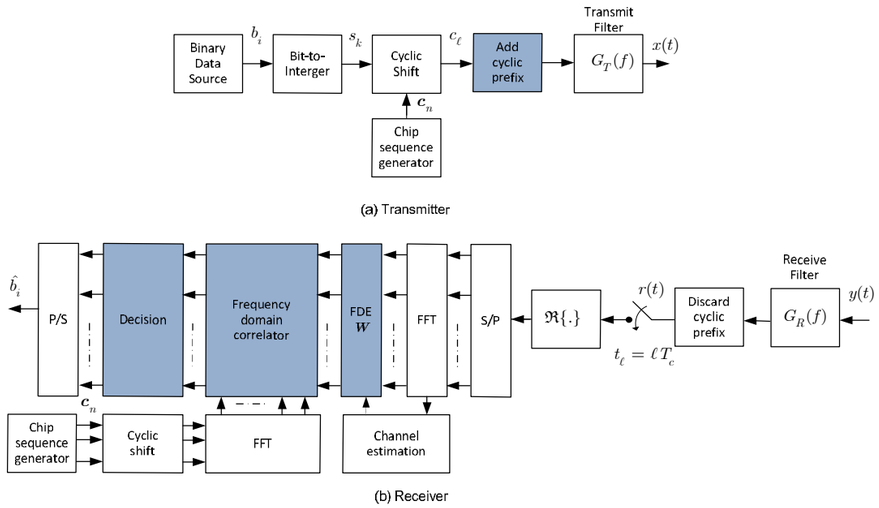
4.4 Phương pháp giảm độ phức tạp tính toán

Giải pháp luận án đề xuất cho phép giảm bớt một bộ biến đổi IFFT và một bộ biến đổi song song sang nối tiếp (P/S) sau san bằng.

4.5 Phân tích phẩm chất BER

4.5.1 Tham số mô phỏng

Để phân tích phẩm chất BER của hệ thống, sử dụng các mô phỏng Monte-Carlo, cấu hình như ở Hình 4-1. Kênh truyền sử dụng



Hình 4-1 Sơ đồ hệ thống truyền dẫn CCSK sử dụng san bằng trên miền tần số.

Giải pháp tính tương quan trong miền tần số cho CCSK thông qua phép biến đổi FFT lần lượt để thu được các chuỗi trải trong miền tần số $\hat{c}_n$. Các chuỗi trải này được tính tương quan với chuỗi chip thu được sau san bằng $\hat{y}$ và thực hiện quyết định để tìm ra chỉ số *k* tương ứng với tổ hợp bit nhị phân đã truyền $k = \arg\max_k \{\tilde{s}_k\} = \arg\max_k \left\{ \sum_{k=0}^{M-1} \hat{y}^H \hat{c}_k \right\}$. Do thao tác tính tương quan và quyết định thực hiện trực tiếp trên miền tần số nên trong sơ đồ máy thu không cần sử dụng bộ biến đổi IFFT để biến đổi các mẫu ngược lại miền thời gian. *Đây cũng là điểm mới mà luận án đề xuất.*

4.3 Nguyên lý san bằng trên miền tần số

4.3.1 San bằng cưỡng bức không (ZF)

San bằng cưỡng bức không được tính theo công thức:

$$W_n^{ZF} = \frac{1}{H_n}. \tag{4.12}$$

4.3.2 San bằng sai số bình phương trung bình nhỏ nhất (MMSE)

San bằng sai số bình phương trung bình nhỏ nhất tính bởi công thức sau

Kênh *không biến thiên theo thời gian* hay còn gọi là *pha-đinh chậm* nếu $T_s \ll T_{ch}$ và $B_s \gg f_m$.

1.4 Mô hình toán học kênh biến thiên theo thời gian

Giả thiết đường bao tín hiệu thu là

$$\tilde{y}(t) = \tilde{s}(t) \sum_{l=0}^{\mathcal{L}-1} \alpha_l e^{j2\pi f_m \cos(\phi_l)t} = g(t)\tilde{s}(t), \tag{1.25}$$

Do thành phần góc pha biến đổi theo thời gian nên hệ số phức $g(t)$ của kênh truyền cũng biến đổi theo thời gian. Dẫn đến hiện tượng tín hiệu thu bị trải trên trục tần số so với tín hiệu phát và được gọi là hiện tượng *trải Doppler*.

1.5 Kênh pha-đinh Rayleigh và Rice

1.5.1 Kênh pha-đinh Rayleigh

Một kênh pha-đinh được gọi là pha-đinh Rayleigh nếu phân bố của đường bao tín hiệu tuân theo phân bố Rayleigh.

1.5.2 Kênh pha-đinh Rice

Phân bố Rice thường được đặc trưng bởi tham số $\mathcal{K} = A^2 / (2\sigma_y^2)$. Khi $\mathcal{K} = 0$, kênh trở thành kênh pha-đinh Rayleigh và khi $\mathcal{K} = \infty$ có kênh không đổi.

1.6 Hậu quả ảnh hưởng của pha-đinh

Mặc dù thường được xem như tạp âm nhưng một trong các đặc điểm khác biệt cơ bản của pha-đinh so với tạp âm là tính chất ảnh hưởng đến tín hiệu phát đi. Trong khi ảnh hưởng của tạp âm có tính chất cộng (additive) thì pha-đinh lại có tinh chất nhân (multiplicative).

1.7 Tóm tắt chương

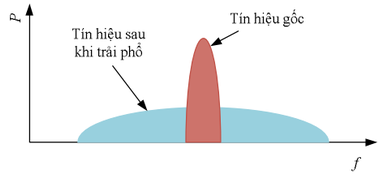
Chương 1 trình bày các vấn đề cơ bản về kênh truyền vô tuyến và có thể thấy kênh truyền vô tuyến chịu ảnh hưởng lớn của các tác động

như pha-đinh đa đường, hiệu ứng dịch tần Doppler. Nội dung chương này làm nền tảng xây dựng mô hình kênh, phục vụ cho các chương sau.

CHƯƠNG 2: KỸ THUẬT TRẢI PHỔ VÀ PHƯƠNG PHÁP TẠO CHUỖI TRẢI

2.1 Giới thiệu

Trải phổ là kỹ thuật tạo tín hiệu có băng thông lớn hơn rất nhiều so với tín hiệu cần truyền.

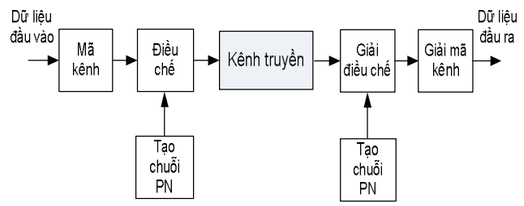


Hình 2-1 Phổ của tín hiệu trải phổ.

2.2 Trải phổ chuỗi trực tiếp

2.2.1 Nguyên lý truyền dẫn tín hiệu DSSS

Sơ đồ của một hệ thống trải phổ điển hình minh họa ở Hình 2-2



Hình 2-2 Sơ đồ hệ thống và tín hiệu trải phổ chuỗi trực tiếp.

2.2.2 Độ lợi xử lý và biên chế áp

Từ công thức $$\frac{E_b}{J_0} = \frac{P_{av}/R}{J_{av}/W} = \frac{W/R}{J_{av}/P_{av}} \quad (2.11)$$

Tỉ số J_{av}/P_{av} được gọi là *biên chế áp* của hệ thống trải phổ. Tỉ số $W/R = T_b/T_c = B_e = N_c$ là tỉ số mở rộng băng thông và còn được gọi là *độ lợi xử lý* của hệ thống DSSS.

các chuỗi trải PN được tạo từ mã cyclic cục bộ. Các mô phỏng đánh giá trên kênh pha-đinh Rayleigh và Rice cho thấy hệ thống CCSK có thể đạt được phẩm chất BER tốt trên các kênh biến đổi nhanh nhờ thu được bậc phân tập thời gian. Khi kênh biến đổi nhanh thì bài toán tách tín hiệu kết hợp trở nên khó khăn. Giải pháp mã hóa/giải mã vi sai ở mức chip do luận án đề xuất cho thấy hệ thống CCSK hoạt động tốt khi số chip dùng cho mã hóa lớn. Đối với kênh pha-đinh Rayleigh hệ thống thích hợp với kênh có tần số Doppler chuẩn hóa $f_D T_s = 0,1$ và tương đương. Với kênh Rice hệ thống có tác dụng khi máy thu có hệ số Rice nhỏ.

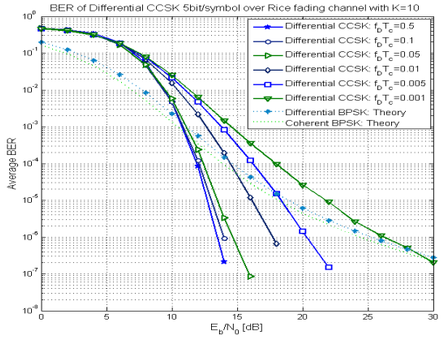
CHƯƠNG 4: KỸ THUẬT SAN BẰNG TRÊN MIỀN TẦN SỐ CHO HỆ THỐNG CCSK

4.1 Giới thiệu

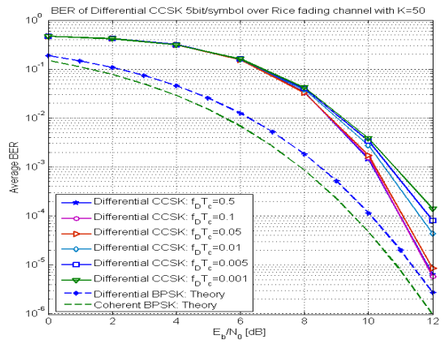
Ngoài tính chất lựa chọn theo thời gian, kênh truyền vô tuyến còn chịu ảnh hưởng của tính chất chọn lọc theo tần số do ảnh hưởng của hiện tượng trải trễ của kênh truyền khi $\sigma_\tau > T_c$. Vì vậy, san bằng kênh nhằm hạn chế ảnh hưởng của tính chất chọn lọc theo tần số của kênh là một bài toán cần thiết.

4.2 Cấu hình hệ thống đề xuất

Cấu hình đề xuất của hệ thống truyền dẫn CCSK trên Hình 4-1. Sự khác biệt của hệ thống SC-FDE với hệ thống OFDM là ở chỗ máy phát không sử dụng bộ biến đổi Fourier nhanh ngược (IFFT). *Khác với các hệ thống trước đây đã đề cập ở trên, luận án đề xuất thực hiện tính tương quan và thực hiện quyết định trên miền tần số*, cho phép giảm độ phức tạp tính toán hơn so với trên miền thời gian.

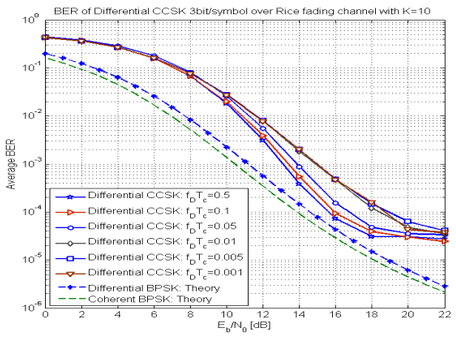


(a) Chuỗi cơ sở 32 chip - Hệ số $\mathcal{K} = 10$

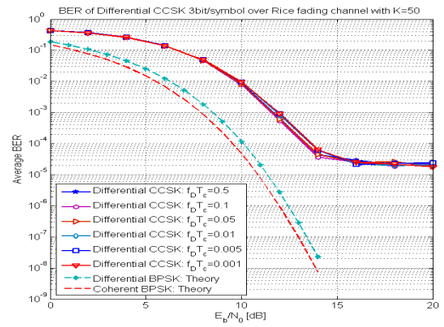


(b) Chuỗi cơ sở 32 chip - Hệ số $\mathcal{K} = 50$

Hình 3-12 Phẩm chất BER của CCSK (32 chip) vi sai trên kênh pha-đinh Rice.



(a) Chuỗi cơ sở 8 chip - Hệ số $\mathcal{K} = 10$



(b) Chuỗi cơ sở 8 chip - Hệ số $\mathcal{K} = 50$

Hình 3-13 Phẩm chất BER của CCSK (8 chip) vi sai trên kênh pha-đinh Rice.

Kết quả nghiên cứu cho thấy việc áp dụng phương pháp mã hóa và giải mã vi sai đem lại hiệu quả lớn và rất phù hợp với kênh pha-đinh biến đổi nhanh. Tác giả cũng đã chỉ ra rằng sử dụng CCSK vi sai thích hợp với kênh pha-đinh Rayleigh có $f_D T_c = 0,1$ và tương đương. Vì vậy, phương pháp CCSK vi sai đề xuất có thể áp dụng tốt cho các hệ thống thông tin vô tuyến làm việc trong môi trường pha-đinh biến đổi nhanh.

3.7 Tóm tắt chương

Chương 3 luận án đã trình bày nguyên lý hoạt động của hệ thống CCSK và tiến hành mô phỏng đánh giá phẩm chất của CCSK sử dụng

2.2.3 Ứng dụng của trải phổ DSSS

Các hệ thống trải phổ DSSS đã được ứng dụng rộng rãi trong các hệ thống điện tử và truyền thông. Tuy nhiên, trong thông tin quân sự quan tâm đến chống chế áp điện tử và truyền tín hiệu có xác suất phát hiện thấp.

2.3 Chuỗi trải PN và phương pháp tạo chuỗi trải

Các chuỗi PN nhị phân phổ biến nhất là chuỗi MLS tạo bởi các LFSR có độ dài $n = 2^m - 1$ bit. Trong các ứng dụng chống nhiễu chế áp, chu kỳ của chuỗi MLS cần chọn với giá trị m lớn để ngăn đối phương có thể dò tìm kết nối phản hồi trong mạch LFSR tạo PN. Vì vậy, luận án đề xuất một phương pháp mới tạo chuỗi trải PN từ mã cyclic cục bộ.

2.4 Tạo chuỗi trải từ mã cyclic cục bộ

2.4.1 Cơ sở của đề xuất

Do chuỗi MLS là một loại mã thuộc họ mã cyclic nên thay cho việc tạo chuỗi MLS nhờ sử dụng LFSR bằng các phương pháp đại số sử dụng vành đa thức. Việc ứng dụng LCC cho phép tạo được các chuỗi PN có phẩm chất tốt thuộc dạng bất quy tắc nhằm nâng cao xác suất thu chặn.

2.4.2 Nguyên lý tạo mã cyclic cục bộ

Mã cyclic cục bộ là một mã tuyến tính có các dấu mã là một tập con không trống tuỳ ý các lớp kề trong phân hoạch của vành đa thức theo một nhóm nhân cyclic. Ưu điểm của mã cyclic cục bộ là có thể xây dựng được mã trên mọi vành đa thức (n bất kỳ), kể cả vành chẵn.

2.4.3 Các phương pháp biểu diễn mã cyclic cục bộ

Phương pháp truyền thống là biểu diễn trên miền thời gian, có nhược điểm là cần sử dụng tích chập giữa đa thức thông tin $s(x)$ và đa

thức sinh $g(x)$ để biểu diễn mã. Để hạn chế độ phức tạp của quá trình tạo mã sử dụng tích chập trên miền thời gian, luận án đề xuất sử dụng phương pháp biểu diễn mã cyclic cục bộ mới trên miền tần số sử dụng biến đổi Fourier trên trường hữu hạn.

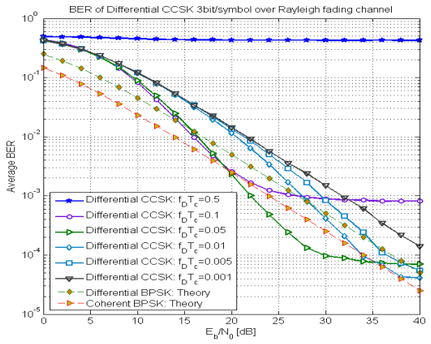
Bảng 2-2 Biểu diễn mã cyclic cục bộ (7,4) trên miền tần số.

TT	Từ mã trên miền thời gian							Từ mã trên miền tần số						
	v_6	v_5	v_4	v_3	v_2	v_1	v_0	V_6	V_5	V_4	V_3	V_2	V_1	V_0
1	0	0	0	0	0	0	0	**0**	**0**	0	**0**	0	0	**0**
2	1	1	0	1	0	0	1	α^0	α^0	0	α^0	0	0	**0**
3	0	1	1	1	0	1	0	α^2	α^4	0	α	0	0	**0**
4	1	0	0	1	1	1	0	α^4	α	0	α^2	0	0	**0**
5	1	0	1	0	0	1	1	α^6	α^5	0	α^3	0	0	**0**
6	1	1	1	0	1	0	0	α	α^2	0	α^4	0	0	**0**
7	0	0	1	1	1	0	1	α^3	α^6	0	α^5	0	0	**0**
8	0	1	0	0	1	1	1	α^5	α^3	0	α^6	0	0	**0**
9	1	1	1	1	1	1	1	**0**	**0**	0	**0**	0	0	**1**
10	0	0	1	0	1	1	0	α^0	α^0	0	α^0	0	0	**1**
11	1	0	0	0	1	0	1	α^2	α^4	0	α	0	0	**1**
12	0	1	1	0	0	0	1	α^4	α	0	α^2	0	0	**1**
13	0	1	0	1	1	0	0	α^6	α^5	0	α^3	0	0	**1**
14	0	0	0	1	0	1	1	α	α^2	0	α^4	0	0	**1**
15	1	1	0	0	0	1	0	α^3	α^6	0	α^5	0	0	**1**
16	1	0	1	1	0	0	0	α^5	α^3	0	α^6	0	0	**1**

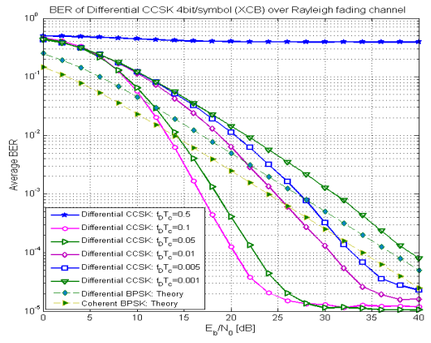
Trong miền tần số, hoạt động mã hóa có thể được viết đơn giản thành $C_f = G_f \cdot S_f$, trong đó G_f là phổ của đa thức sinh, S_f là phổ của tín hiệu, còn C_f là phổ của từ mã thu được qua phép biến đổi Fourier. Do phổ tín hiệu S_f là tùy ý, nên G_f đóng vai trò đáng kể nhất để xác định tần số nơi mà phổ từ mã C_f bằng không.

2.4.4 Xây dựng chuỗi trải từ mã cyclic cục bộ

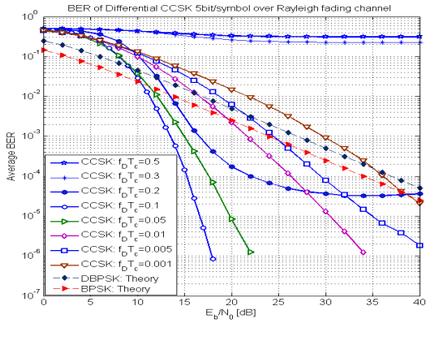
2.4.4.1 Tạo chuỗi m bằng nhóm nhân đối xứng



(a) Chuỗi cơ sở CCSK cyclic cục bộ (8 chip)

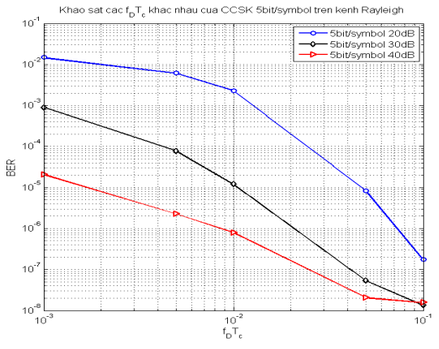


(b) Chuỗi cơ sở CCSK cyclic cục bộ (16 chip)



(c) Chuỗi cơ sở CCSK cyclic cục bộ (32 chip)

Hình 3-10 Phẩm chất BER của CCSK vi sai trên kênh pha-đinh Rayleigh.



Hình 3-11 Khảo sát các tần số chuẩn hóa Doppler $f_D T_c$ khác nhau.

Từ Hình 3-10 thấy rõ là tỉ số BER giảm nhanh khi tần số Doppler tăng dần trên kênh pha-đinh Rayleigh. Tuy nhiên, trong trường hợp kênh biến đổi nhanh quá (VD: $f_D T_c = 0.5$) làm cho quan hệ pha giữa các tín hiệu kề nhau bị thay đổi hoàn toàn và vì vậy, máy thu không thể tách lại thông tin đã mã hóa dẫn đến số BER = 0,5. Kênh pha-đinh Rayleigh gây ảnh hưởng lớn đến đặc tính BER hơn kênh Rice, kênh pha-đinh Rice khi hệ số $\mathcal{K} = 50$ tia trội đóng vai trò chính và vì vậy ảnh hưởng của Doppler là ít thể hiện ở Hình 3-12 và Hình 3-13.

Chuỗi chip đã mã hóa vi sai α_ℓ sau đó được đưa tới bộ lọc phát $G_T(f)$ để tạo tín hiệu phát $x(t)$.

Tại phía thu, tín hiệu thu được từ kênh truyền $y(t)$ được đưa qua bộ lọc thu $G_R(f)$ rồi lấy mẫu với tốc độ $R_c = 1/T_c$. Các mẫu thu rời rạc r_ℓ sau đó được giải mã vi sai sử dụng thuật toán sau

$$\hat{r}_\ell = \mathrm{Re}\{r_\ell r_{\ell-1}^*\} \tag{3.54}$$

Các mẫu chip thu ước lượng được $\hat{r}_\ell$ tiếp tục được nhóm với nhau thành các tổ hợp M chip. Các tổ hợp này sẽ được so sánh với các chuỗi dịch vòng tuần hoàn $\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{M-1}$ để tìm ra chỉ số k

$$k = \arg\max_k \{\tilde{s}_k\} = \arg\max_k \left\{ \sum_{\ell=0}^{M-1} \boldsymbol{c}_k \hat{\boldsymbol{r}} \right\} \tag{3.55}$$

sau đó sẽ được ánh xạ ngược lại thành tổ hợp k bit tương ứng tương tự trường hợp tách kết hợp.

3.6.2 Mô phỏng đánh giá phẩm chất

Để làm tham chiếu các kết quả BER cho hai trường hợp BPSK sử dụng tách tín hiệu đồng bộ và tách vi sai với kênh không biến đổi, $f_D T_c = 0$, cũng được vẽ trên cùng hình vẽ. Từ các hình vẽ này có thể rút ra các nhận xét quan trọng sau đây. Phương pháp mã hóa và giải mã vi sai cho CCSK cho phép đạt được phẩm chất BER tốt khi tăng chiều dài chuỗi cơ sở từ 8 chip lên 32 chip. Hiện tượng sàn lỗi do pha-đinh nhanh vẫn xảy ra ở vùng E_b / N_0 cao. Hình 3-11 có kết luận rằng khi giá trị $\mathrm{E_b/N_0[dB]}$ tiến đến khoảng 40 dB sẽ về vùng sàn lỗi tương ứng vùng tỉ số $\mathrm{BER} < 10^{-8}$.

2.4.4.2 Tạo chuỗi m bằng phương pháp phân hoạch theo modulo $h(x)$.

2.4.4.3 Xây dựng chuỗi m lồng ghép trên vành đa thức có hai lớp kề cyclic theo modulo $h(x)$.

2.4.5 Thuật toán tạo chuỗi trải MLS từ mã cyclic cục bộ bằng phương pháp phân hoạch vành đa thức

Bước 1: Chọn phần tử sinh xây dựng nhóm nhân cyclic.

Bước 2: Xây dựng cấp số nhân cyclic $A_{(a,q)} = \{a(x) \cdot q^i(x), i = 1,2,\ldots,m_s\}$

Bước 3: Lặp lại bước 2 cho đến khi $A_{(a,q)}$ lặp lại giá trị ban đầu.

2.5 Tóm tắt chương

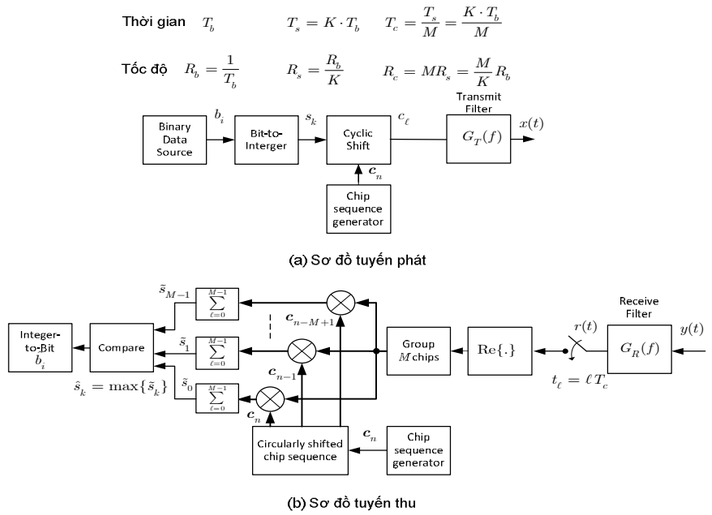
Chương 2 luận án đã trình bày tổng quan về hệ thống trải phổ chuỗi trực tiếp và phương pháp tạo chuỗi trải PN. Thông qua phân tích, luận án cho thấy phương pháp tạo chuỗi trải MLS bằng LFSR sử dụng cho trải phổ chưa sử dụng hết toàn bộ các bộ chuỗi có thể có. Nhằm mục đích nâng cao tính chất bảo mật và chống thu chặn cho thông tin vô tuyến điện quân sự, luận án đề xuất một phương pháp tạo chuỗi PN từ mã cyclic cục bộ. Phương pháp tạo chuỗi trải này sẽ được đề xuất sử dụng trong các hệ thống khóa dịch mã tuần hoàn trình bày ở Chương 3.

CHƯƠNG 3: KỸ THUẬT KHÓA DỊCH MÃ TUẦN HOÀN SỬ DỤNG CHUỖI TRẢI TỪ MÃ CYCLIC CỤC BỘ

3.1 Giới thiệu

Khóa dịch mã tuần hoàn (CCSK) là một kỹ thuật trải phổ tương tự như kỹ thuật trải phổ chuỗi trực tiếp (DSSS). Điểm khác biệt cơ bản của CCSK là thay đổi dữ liệu đưa vào trải phổ. CCSK còn được chứng minh

có xác suất thu chặn thấp hơn so với DSSS. Hình 3-1 minh họa sơ đồ khối một hệ thống khóa dịch mã tuần hoàn.



Hình 3-1 Sơ đồ khối hệ thống khóa dịch mã tuần hoàn CCSK.

CCSK sử dụng một chuỗi cơ sở $\boldsymbol{c} = [c_1, c_2, \cdots, c_M]^T$ và các phiên bản dịch vòng của nó để biểu diễn các ký tự *B* bit. Các phần tử $c_m = \pm 1$ của $\boldsymbol{c}$ được gọi là các chip. Các chuỗi vòng của $\boldsymbol{c}$ được ký hiệu là $\boldsymbol{c}_0, \boldsymbol{c}_1, ..., \boldsymbol{c}_{M-1}$ với $\boldsymbol{c}_0 = \boldsymbol{c}$ và $\boldsymbol{c}_n$ là chuỗi dịch vòng thứ *n*. Để thực hiện điều chế CCSK, chuỗi bit dữ liệu b_i được nhóm thành các tổ hợp $k = \log_2 M$ bit. Các nhóm *k* bit dữ liệu nhị phân này tương ứng với các ký hiệu thập phân s_m. M ký hiệu thập phân s_m sẽ được ánh xạ tới một trong M chuỗi dịch vòng $\boldsymbol{c}_n$. Để giải mã CCSK máy thu thực hiện tính tương quan giữa chuỗi cơ bản ước lượng được $\tilde{\boldsymbol{c}}_n$ với chuỗi cơ sở dịch vòng $\boldsymbol{c}_n$ để ước lượng thống kê quyết định cho từng ký tự truyền. Tức là,

$$\tilde{s}_m = \left| \boldsymbol{c}_m^T \tilde{\boldsymbol{c}}_n \right|. \tag{3.4}$$

- Hệ thống CCSK đạt được phẩm chất BER tốt hơn so với hệ thống điều chế số BPSK ngay tại vùng E_b / N_0 thấp. Điều này có thể giải thích nhờ độ lợi phân tập thời gian đạt được khi kênh biến đổi theo thời gian.
- Phẩm chất BER trên kênh pha-đinh Rice với hệ số $\mathcal{K} = 50$ không phụ thuộc vào tần số Doppler. Điều này cho thấy được vai trò của tia trội đối với kênh chịu ảnh hưởng của pha-đinh.
- Khi tăng chiều dài chuỗi trải từ 8 chip (Hình 3-7) lên 32 chip (Hình 3-8) có thể cho phép cải thiện phẩm chất BER đáng kể nhờ độ lợi xử lý thu được của tín hiệu trải phổ.

3.6 Đánh giá phẩm chất CCSK trên kênh pha-đinh biến đổi nhanh sử dụng mã hóa/giải mã vi sai.

Trong phần trên CCSK đã cho thấy có thể đạt được phẩm chất tốt trên kênh pha-đinh biến đổi nhanh nhờ thu được độ lợi phân tập. Trên thực tế rất khó đạt được độ lợi phân tập này vì máy thu sử dụng tách tín hiệu kết hợp đòi hỏi phải biết được chính xác thông tin về kênh truyền. Các thuật toán tách tín hiệu không kết hợp có ưu điểm do không cần biết thông tin về kênh truyền. Vì vậy, luận án đề xuất một hệ thống tách tín hiệu không kết hợp trên cơ sở mã hóa/giải mã vi sai ở mức chip.

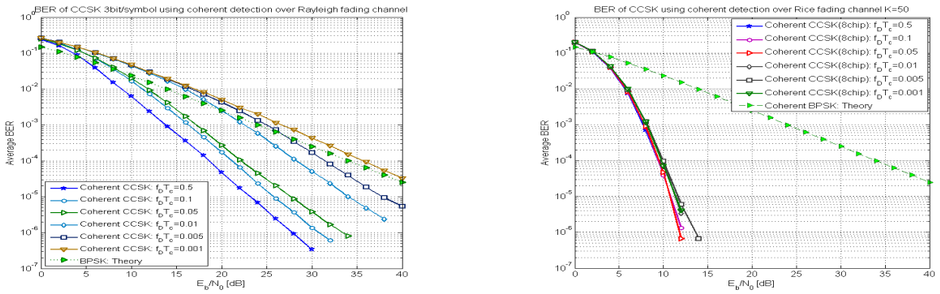
3.6.1 Nguyên lý khóa dịch mã tuần hoàn CCSK vi sai ở mức chip

Về cơ bản nguyên lý hoạt động tương tự như hệ thống CCSK ở Hình 3-1 ngoại trừ hai khối Mã hóa vi sai và Giải mã vi sai. Ở tuyến phát, chuỗi chip đầu ra c_ℓ từ bộ dịch tuần hoàn sẽ được mã hóa vi sai

$$\alpha_\ell = c_\ell c_{\ell-1}. \tag{3.53}$$

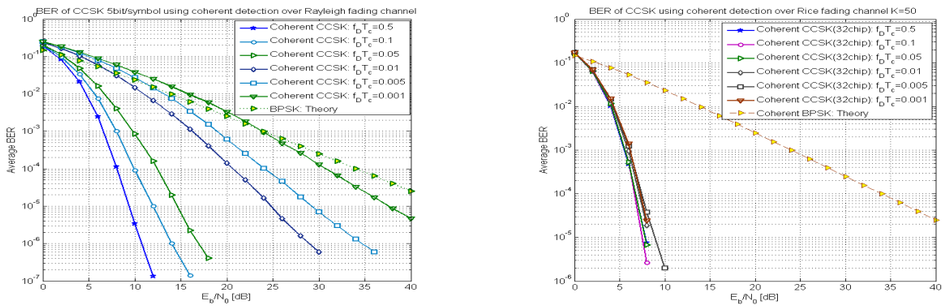
Kết quả mô phỏng cũng cho thấy độ dốc của đường đặc tính BER tăng dần ở vùng E_b / N_0 cao. Điều này có thể giải thích được thông qua độ lợi xử lý T_b / T_c của hệ thống trải phổ.

3.5 Đánh giá phẩm chất CCSK trên kênh pha-đinh sử dụng thu kết hợp



(a) Kênh pha-đinh Rayleigh (b) Kênh pha-đinh Rice (K=50)

Hình 3-7 Phẩm chất BER của CCSK trên kênh pha-đinh sử dụng chuỗi PN có độ dài 8 chip.



(a) Kênh pha-đinh Rayleigh (b) Kênh pha-đinh Rice (K=50)

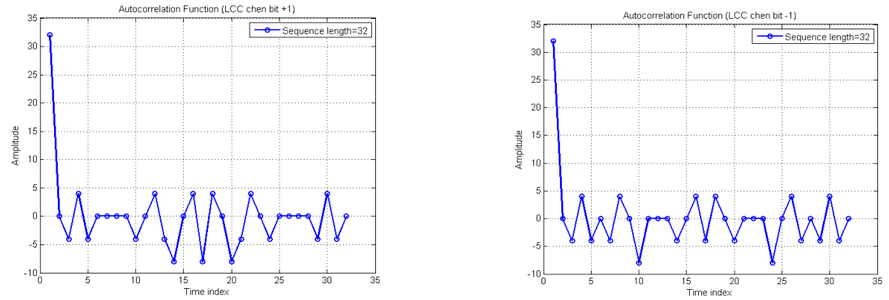
Hình 3-8 Phẩm chất BER của CCSK trên kênh pha-đinh sử dụng chuỗi PN có độ dài 32 chip.

Đánh giá hiệu quả của CCSK trên kênh pha-đinh Rayleigh và pha-đinh Rice với hệ số $\mathcal{K} = 50$. Để đánh giá ảnh hưởng của tính chất biến đổi của kênh sử dụng các tần số Doppler chuẩn hóa $f_D T_c$ khác nhau. Các chuỗi trải được lựa chọn có độ dài bằng 8 chip và 32 chip được tạo ra từ mã cyclic cục bộ.

với $m = 0,1,2,\ldots,M-1$. Từ đây, máy thu thực hiện phép quyết định sau nếu $\max(\tilde{s}_m) = s_p \rightarrow$ chọn k bit tương ứng với s_p để tìm các bit dữ liệu $\tilde{b}_i$.

3.2 Lựa chọn chuỗi trải PN tạo từ mã cyclic cục bộ

Hệ thống CCSK cũng có thể sử dụng chuỗi MLS để trải tín hiệu phát đi. Tuy nhiên, việc sử dụng chuỗi trải MLS sẽ hạn chế khả năng chống thu chặn nên sử dụng các chuỗi trải PN được tạo từ mã cyclic cục bộ như đã trình bày ở Chương 2 sẽ có ưu điểm hơn. Do chuỗi PN được tạo ra có số bit lẻ nên sẽ bổ sung thêm bit +1 hoặc -1 vào đầu chuỗi trải.



(a) Bổ sung bit +1 (b) Bổ sung bit -1

Hình 3-3 Hàm ACF của chuỗi c_0 32 chip mở rộng được tạo từ mã cyclic cục bộ.

Các đỉnh phụ của chuỗi trải đều nhận giá trị nhỏ (Hình 3-3), nên cho phép máy thu tương quan của hệ thống CCSK có thể tách chính xác được chuỗi bit phát từ tín hiệu CCSK nhận được.

3.3 Phân tích phẩm chất CCSK tạo từ LCC

3.3.1 Thuộc tính tương quan chéo

Tương quan chéo của chuỗi CCSK không trực giao được tính như sau

$$\mathcal{R}_\ell = \begin{cases} 32 & \ell = 0 \\ h_\ell & \ell = 1,2,\ldots,31. \end{cases} \tag{3.5}$$

Xác suất có điều kiện của lỗi symbol với $0 \le N \le 32$ thu được từ công thức

$$P_S = \sum_{J=0}^{32} P\left\{\text{lỗi symbol} \middle| N = J\right\} P\left\{N = J\right\} \quad (3.17)$$

3.3.2 Xác suất có điều kiện của lỗi symbol CCSK

Trên cơ sở thuộc tính tương quan chéo của CCSK, với các giá trị lỗi đưa ra $N = 7,8,...,32$ ta tính được xác suất lỗi trên Bảng 3-6.

Bảng 3-6 Xác suất có điều kiện lỗi symbol CCSK 32 chip

$N = J$	ξ_{UBJ_LCC} (đề xuất CCSK_LCC)	ξ_{UBJ_Kao} (Kao đề xuất [18,20])
0	0	0
1	0	0
⋮	⋮	⋮
6	0	0
7	0,0030	0,0015
8	0,0280	0,0207
9	0,1337	0,1166
10	0,4384	0,4187
11	1,0	1,0
⋮	⋮	⋮
32	1,0	1,0

3.3.3 Xác suất lỗi symbol của CCSK trên kênh AWGN

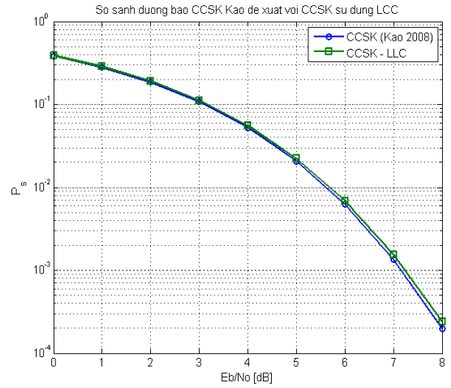
Công thức tính đường bao trên xác suất của lỗi symbol cho chuỗi 32 chip CCSK

$$P_s < \sum_{J=0}^{32} \xi_{UBJ\_\text{LCC}} \binom{32}{J} P_c^J \left(1 - P_c\right)^{32-J}. \quad (3.46)$$

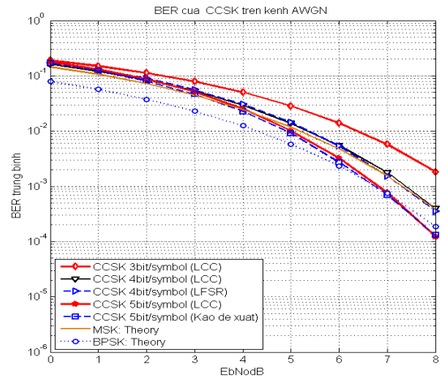
trong đó ξ_{UBJ_LCC} là xác suất có điều kiện của lỗi symbol CCSK. Nếu sử dụng điều chế BPSK để điều chế chip, phẩm chất của hệ thống được tính theo công thức

$$P_c = Q\left(\sqrt{\frac{10E_b}{32N_0}}\right) \quad (3.49)$$

Kết hợp công thức (3.46) và (3.49) ta vẽ được đường bao trên của CCSK sử dụng mã cyclic cục bộ thể hiện trên Hình 3-5.



Hình 3-5 Đường bao trên của chuỗi CCSK 32 chip sử dụng LCC.



Hình 3-6 Phẩm chất BER của CCSK trên kênh AWGN.

Nếu sử dụng chuỗi CCSK tạo ra từ các mã cyclic cục bộ thì phẩm chất kém hơn so với chuỗi CCSK mà Kao đề xuất là không đáng kể, thể hiện ở Hình 3-5. Vì vậy, ta có thể sử dụng chuỗi CCSK tạo ra từ LCC làm các chuỗi trải tăng tính bảo mật của hệ thống.

3.4 Mô phỏng đánh giá phẩm chất CCSK trên kênh AWGN

3.4.1 Tham số mô phỏng

Để so sánh phẩm chất của hệ thống CCSK sử dụng chuỗi trải được tạo từ mã cyclic cục bộ, tiến hành các mô phỏng Monte-Carlo và so sánh kết quả đã công bố của Kao C-H. Chuỗi dữ liệu truyền có độ dài 1.500.000 bit. Sử dụng điều chế số BPSK, tạp âm tác động lên hệ thống là tạp âm Gauss trắng cộng tính.

3.4.2 Phân tích kết quả

Kết quả mô phỏng trên Hình 3-6 cho thấy phẩm chất BER của hệ thống CCSK sử dụng chuỗi trải tạo từ mã cyclic cục bộ (LCC) hoàn toàn tương đương với trường hợp sử dụng chuỗi trải mà Kao đề xuất.