NGHIÊN CỨU GIẢI PHÁP MÃ HÓA CHỐNG NHIỄU CHO NGÒI NỔ LASER CỦA TÊN LỬA PHÒNG KHÔNG

RESEARCH ENCODE TECHNICAL FOR LASER FUZE ON AIR DEFENSE MISSILES

Nguyễn Đức Thi[1,*], Nguyễn Trường Sơn[2], Trần Hoài Linh[3], Trần Xuân Tình[4], Trần Thuỷ Văn[5]

TÓM TẮT

Bài báo đề xuất một giải pháp xây dựng hệ thống chống nhiễu bằng phương pháp mã hóa xung thăm dò của ngòi nổ laser trên tên lửa phòng không tầm thấp. Phương pháp đề xuất được triển khai đánh giá trên phần mềm mô phỏng Matlab-Simulink. Kết quả mô phỏng cho thấy, kỹ thuật mã hoá cho phép nâng cao đáng kể tính chống nhiễu, giúp nâng cao độ tin cậy cho ngòi nổ laser.

***Từ khóa**: Tên lửa phòng không, ngòi nổ laser, mã hóa.*

ABSTRACT

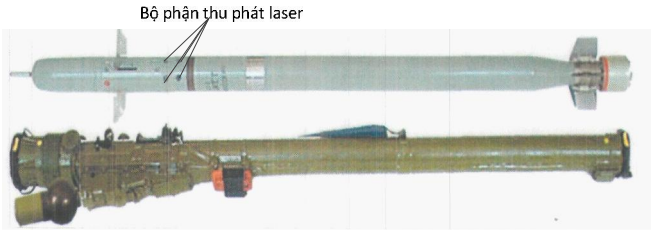
The paper proposes a solution to build an anti-jamming system by encoding the probe pulse of a laser fuse on a low-range air defense missile. The proposed method is evaluated on Matlab-Simulink simulation software. The simulation results show that the coding technique allows to significantly improve the anti-jamming properties, helping to improve the reliability of the laser fuse.

***Keywords:** Low-range missile, laser fuze, pseudo-random code.*

[1]Tổng cục Công nghiệp Quốc phòng
[2]Học viện Kỹ thuật Quân sự
[3]Trường Đại học Bách khoa Hà Nội
[4]Học viện Phòng không - Không quân
[5]Trường Đại học Công nghiệp Hà Nội
[*]Email: thi2306pro@gmail.com
Ngày nhận bài: 02/7/2020
Ngày nhận bài sửa sau phản biện: 15/8/2020
Ngày chấp nhận đăng: 18/8/2020

1. ĐẶT VẤN ĐỀ

Hiện nay, với tên lửa phòng không hiện đại, để tăng độ tin cậy, xác suất tiêu diệt mục tiêu, thì bên cạnh ngòi nổ thông thường còn có thêm ngòi nổ laser. Hình 1 là tên lửa IGLA-S 9M342 có bộ phận thu phát laser.

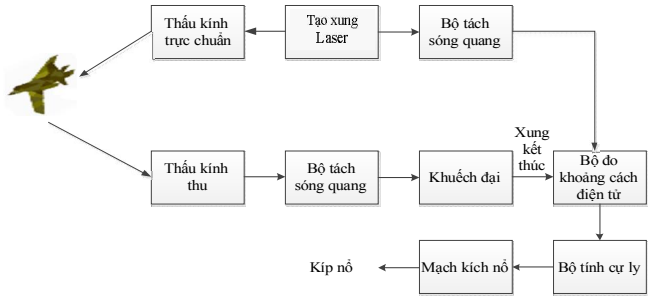


Hình 1. Tên lửa IGLA-S 9M342

Trong tác chiến, điều kiện làm việc của ngòi nổ laser rất phức tạp, nhiều dạng nhiễu tác động đến tuyến thu, phát trên ngòi nổ như: khói bụi đường truyền, ánh sáng mặt trời, các nguồn sáng phi tự nhiên, tán xạ do các bề mặt của đối tượng đã được xử lý, các nhiễu chủ động của đối phương gây ra,… Việc chống nhiễu cho ngòi nổ laser là bắt buộc, có thể áp dụng tổ hợp một số giải pháp chống nhiễu đồng thời. Trong đó việc ứng dụng kỹ thuật mã hóa xung phát laser đã được nhiều công trình nghiên cứu [3, 4, 5, 6], tuy nhiên thời gian xử lý thuật toán và khả năng bảo mật còn chưa được đề cập, khó có thể hiện thực hóa. Chính vì vậy, nhóm tác giả nghiên cứu đề xuất phương pháp mã hóa mới nhằm hoàn thiện khả năng chống nhiễu cho ngòi nổ laser, giảm thời gian xử lý để có thể áp dụng vào thực tế.

2. NGUYÊN LÝ HOẠT ĐỘNG CỦA NGÒI NỔ LASER

Về nguyên lý hoạt động của ngòi nổ laser tương tự như ngòi nổ vô tuyến nhưng khác là sử dụng tia laser để chiếu xạ mục tiêu, bằng cách: Chiếu xạ tới mục tiêu với một xung laser từ máy phát; Phát hiện tín hiệu laser phản xạ từ mục tiêu; Đo thời gian tia laser truyền từ máy phát tới mục tiêu và trở lại máy thu để tính khoảng cách từ ngòi nổ đến mục tiêu; Lựa chọn cự li và thời điểm thích hợp để kích nổ đầu nổ. Sơ đồ cấu trúc đơn giản của ngòi nổ laser như hình 2.



Hình 2. Sơ đồ cấu trúc đơn giản của ngòi nổ laser

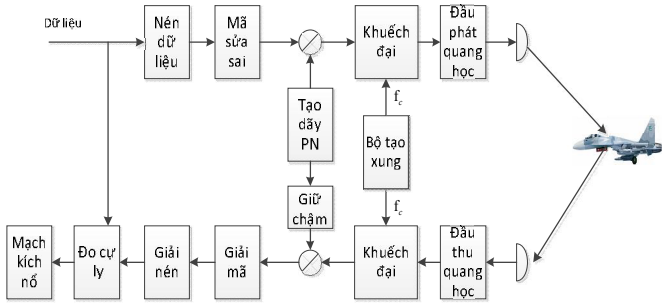
3. NÂNG CAO ĐỘ TIN CẬY CỦA NGÒI NỔ LASER BẰNG KỸ THUẬT MÃ HÓA

Hiện nay trên tên lửa phòng không tầm thấp đã có những giải pháp chống nhiễu như: đặt ngưỡng biên độ, đặt kính màu, chọn trường nhìn, đồng bộ thời gian làm việc, chọn đặc tuyến, tạo xung cửa. Tuy nhiên, các phương tiện tập kích đường không đã có những tiến bộ vượt bậc về khả

năng đối kháng và chống đối kháng, trong đó có cả hệ thống gây nhiễu hồng ngoại và laser. Chính vì vậy ngòi nổ sử dụng các phương pháp chống nhiễu truyền thống rất có thể bị gây nhiễu, giảm khả năng đánh trúng mục tiêu.

Do đó nhóm tác giả đề xuất phương pháp chống nhiễu bằng giải pháp mã hóa xung thăm dò của ngòi nổ laser. Bộ phận mã hóa tạo tín hiệu điện đã được mã hóa đưa đến điều khiển nguồn phát laser. Bộ phận thu sẽ so sánh tín hiệu thu về với quy luật mã hóa cho trước, nếu đúng quy luật sẽ tạo ra tín hiệu đưa sang cơ cấu bảo hiểm - kích nổ để kích nổ ngòi nổ.

Phương pháp mã hóa được sử dụng rộng rãi trong các hệ thống truyền thông vô tuyến, đặc biệt là trong các ứng dụng quân sự do khả năng chống nhiễu rất tốt [3, 4, 8]. Như đã đề cập, một trong các tiêu chí quan trọng nhất về chống nhiễu đối với ngòi nổ laser đó là: xử lý tin cậy, bảo mật và có thể triển khai được trên phần cứng, nhóm tác giả đề xuất một hệ thống mã hóa sửa lỗi dùng trên ngòi nổ laser như mô tả trong hình 3.



Hình 3. Sơ đồ chức năng hệ thống mã hóa dùng trên ngòi nổ laser

Trong hệ thống này, có hai thành phần chính là tuyến phát và tuyến thu. Tuyến phát có chức năng phát tín hiệu đã được mã hoá, tuyến thu có chức năng thu và giải mã tín hiệu có ích thu được phục vụ cho việc phát hiện mục tiêu và kích nổ đầu nổ. Chuỗi dữ liệu sau khi được số hóa thành chuỗi dữ liệu số (0, 1) sẽ được chèn vào các đoạn mã sửa sai và chuỗi mã hóa để tăng được độ tin cậy dữ liệu xử lý và đặc biệt nâng cao khả năng bảo mật. Bằng kỹ thuật này thì chuỗi dữ liệu được mã hóa để đưa lên kênh truyền sẽ được mở rộng phổ lên gấp nhiều lần tùy thuộc vào độ dài của chuỗi sửa lỗi và chuỗi mã hóa.

Nguyên lý hoạt động kênh phát: Chuỗi dữ liệu số hóa sau khi được chèn mã sửa lỗi và chuỗi mã hóa sẽ được đưa vào bộ khuếch đại công suất đầu phát laser. Các xung công suất phát sau đó được thực hiện dựa trên bộ tạo xung nhịp đồng bộ của khối xử lý laser.

Nguyên lý hoạt động kênh thu: Tín hiệu thu từ đầu vào kênh thu được khuếch đại lên mức tín hiệu trong dải hoạt động của đầu thu, sau đó kết hợp với bộ giữa chậm và chuỗi bit mã hóa và chuỗi sửa lỗi biết trước sẽ giải mã ra chuỗi dữ liệu phát đi. Bộ giữ chậm được tính toán dựa trên độ trễ tín hiệu giữa xung phát và xung thu do thời gian truyền sóng trên kênh truyền.

Bản chất các chuỗi giả ngẫu nhiên (chuỗi mã hóa) là các chuỗi số được tạo ra theo các hàm tiền định, sử dụng một giá trị khởi tạo ban đầu. Khi đã biết được giá trị ban đầu và hàm, ta có thể tái tạo lại được chuỗi đã sinh. Tuy nhiên, nếu không biết được các thông tin này, ta sẽ rất khó dự báo được các giá trị sẽ tiếp tục được sinh ra. Vì vậy đây được gọi là chuỗi giả ngẫu nhiên.

Để mã hóa tín hiệu, chỉ cần nhân bít dữ liệu cần mã với từng bít của chuỗi PN (số lượng bít tạo thành sẽ bằng chiều dài của chuỗi PN):

$$d_n \to s_n(1\ldots k) = d_n \odot \mathrm{PN}(1\ldots k) \quad (1)$$

Trong đó: $d_n = \begin{cases} 1 & \text{khi data bit} = 1 \\ -1 & \text{khi data bit} = 0 \end{cases}$

Để giải mã tín hiệu:

$$s_n(1\ldots k) \to \tilde{s}_n(1\ldots k) = s_n(1\ldots k) \odot \mathrm{PN}(1\ldots k) \quad (2)$$
$$\to d_n = \mathrm{sign}\left(\sum \tilde{s}_n(1\ldots k)\right)$$

Các bước hoạt động chính của quá trình mã hóa và giải mã được thực hiên như sau:

Nếu ngòi nổ sử dụng chuỗi giả ngẫu nhiên PN_A = [1 0 0 1 0 1] và đối phương sử dụng chuỗi giải ngẫu nhiên PN_B = [1 1 0 0 1 1]

- Ở tuyến phát, ngòi nổ phát đi chuỗi Data = [0 1 1] thì từng bước sẽ được thực hiện như sau:

1. Chuyển mức tín hiệu 0 → -1; 1 → 1:

$$\mathrm{Data} \to \mathrm{Data2} = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix}; \quad (3)$$
$$\mathrm{PN_A} \to \mathrm{PN_{A2}} = \begin{bmatrix} 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix}$$

2. Nhân từng bit với khóa giả ngẫu nhiên:

$$\mathrm{Data3} = \mathrm{Data2} \odot \mathrm{PN_{A2}} = \begin{bmatrix} -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 \end{bmatrix} \quad (4)$$

Các bit trong Data3 sẽ được truyền đi. Chú ý rằng số lượng bít đã bị tăng lên 6 lần (bằng độ dài bit của chuỗi giả ngẫu nhiên).

- Ở tuyến thu, thu nhận được tín hiệu sẽ tiến hành giải mã theo các bước sau:

1. Phân đoạn chuỗi nhận được thành các đoạn con có độ dài bằng độ dài của chuỗi giải ngẫu nhiên và nhân từng bít với chuỗi.

$$\mathrm{Data3} \to \mathrm{Data4} = \mathrm{Data3} \odot \mathrm{PN_{A2}} = \begin{bmatrix} -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (5)$$

2. Giải mã các hàng đã nhận:

$$\mathrm{Data4} \to \mathrm{Data5} = \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \quad (6)$$

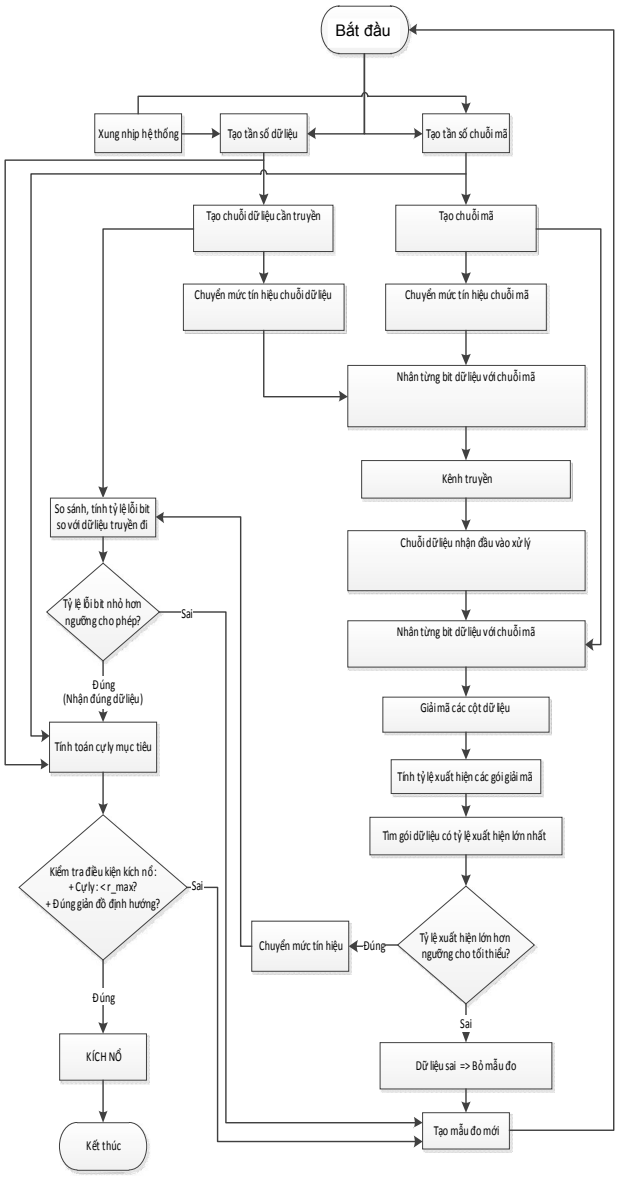
- Trong trường hợp đối phương muốn giải mã bản tin được kết quả như sau:

$$PN_B = [1\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1] \rightarrow PN_{B2} = [1\ \ 1\ \ -1\ \ -1\ \ 1\ \ 1] \quad (7)$$

$$Data3 \rightarrow Data4 = Data3 \odot PN_{B2} = \begin{bmatrix} -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix} \quad (8)$$

Như vậy, chuỗi Data4 không còn biểu thị được bit số liệu ban đầu. Tại các vị trí mã PN_A và mã PN_B khác nhau, giá trị bit bị đảo ngược. Nếu bên gửi sử dụng mã PN_A đủ dài thì xác suất để dò ra được chuỗi PN_B gần giống với PN_A sẽ rất thấp. Trong thực tế còn có thể sử dụng phương pháp sinh khóa liên tục, có nghĩa là mã PN_A được thay đổi liên tục trong quá trình hoạt động để hạn chế tối đa khả năng dò và phá mã của đối phương.

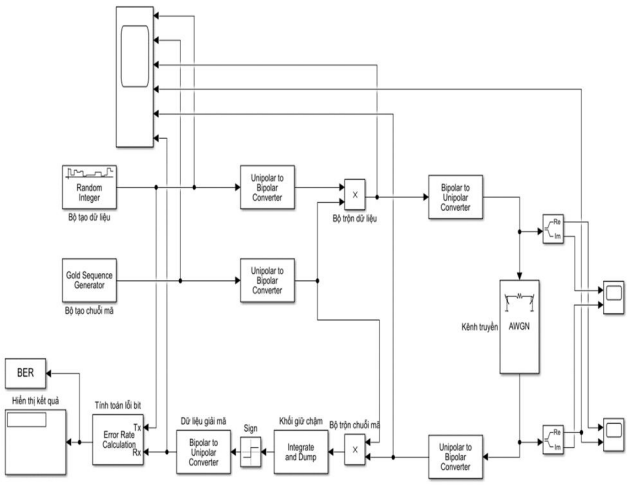
Lưu đồ thuật toán chống nhiễu bằng giải pháp mã hoá thể hiện trên hình 4.



Hình 4. Lưu đồ thuật toán chống nhiễu

4. KẾT QUẢ TÍNH TOÁN VÀ MÔ PHỎNG

Mô hình mô phỏng sử dụng các khối chức năng để thể hiện quá trình truyền và giải mã dữ liệu, các thành phần chính gồm: Bộ giả lập tạo dữ liệu truyền đi, bộ tạo mã ngẫu nhiên, bộ tổng hợp dữ liệu, kênh truyền, bộ giải điều chế, bộ giữ chậm tín hiệu kênh truyền, bộ giải mã, bộ so sánh dữ liệu phát và thu (hình 5).



Hình 5. Sơ đồ Matlab-Simulink của hệ thống sử dụng mã hóa

4.1. Tiến hành khảo sát, đánh giá khả năng kháng nhiễu

a) Dữ liệu mô phỏng

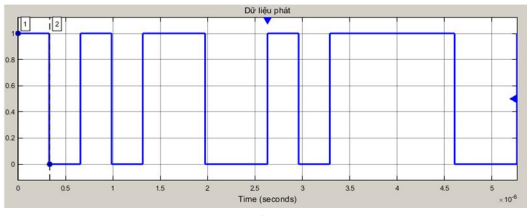
Bảng 1. Dữ liệu mô phỏng

STT	Thông số	Giá trị	Đơn vị
1	Tần số bộ tạo mã Gold	3	MHz
2	Độ dài mã Gold	31	Bit
3	Tần số dữ liệu phát	97,98	MHz
4	Số bit truyền đi	1024	Bit
5	Tỷ số Tín/ Nhiễu kênh truyền	4,5	dB

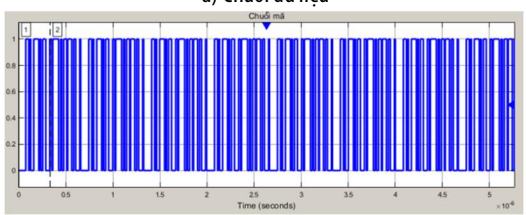
Bộ tạo mã chuỗi giả ngẫu nhiên: Sử dụng mã Gold, hai bộ m = 5 thanh ghi, độ dài mã là $N = 2^m - 1 = 31$ như bảng 1.

b) Kết quả và nhận xét

Chuỗi dữ liệu truyền đầu vào kênh phát và dữ liệu mã như hình 6.



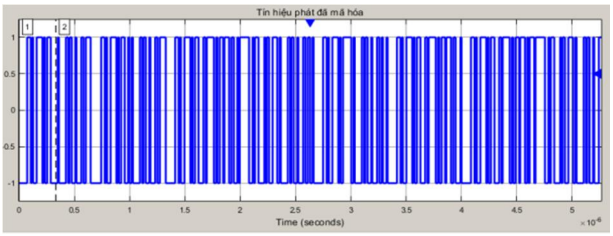
a) Chuỗi dữ liệu



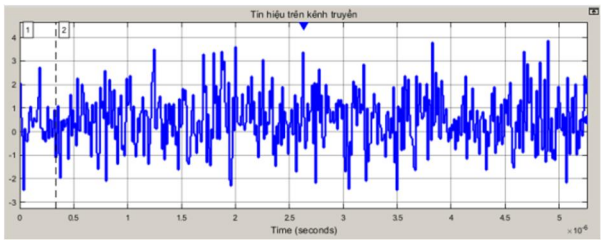
b) Chuỗi PN (Mã Gold)

Hình 6. Dạng xung dữ liệu truyền đi và mã Gold

Dữ liệu sau khi được mã hóa ở máy phát, kết hợp giả lập nhiễu trắng trên đường truyền và nhận được ở máy thu như hình 7.



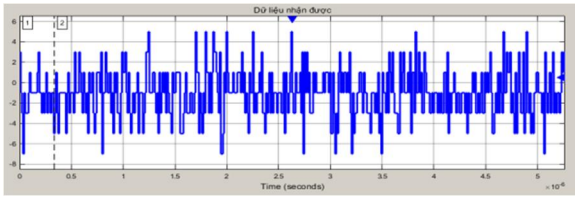
a) Chuỗi dữ liệu



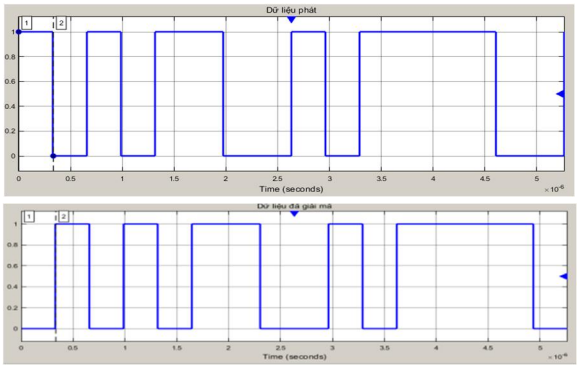
b)Chuỗi PN (Mã Gold)

Hình 7. Tín hiệu được mã hóa kết hợp nhiễu

Dữ liệu giải mã được như hình 8.



a) Tín hiệu tại kênh thu



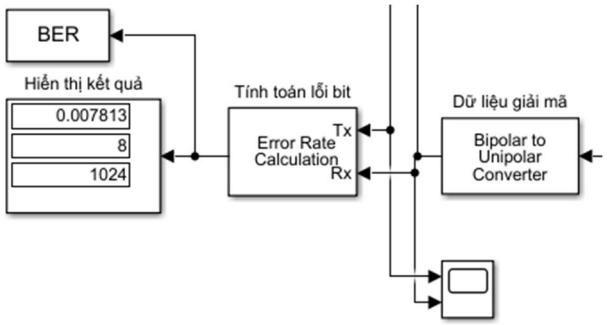
b) Chuỗi dữ liệu truyền đi và chuỗi dữ liệu giải mã

Hình 8. Dạng xung dữ liệu sau khi đã được giải điều chế chế ở máy thu

Thời gian giữ chậm giữa tín hiệu phát và thu: Kết quả mô phỏng cho thấy thời gian giữ chậm giữa 1 bit dữ liệu (31 bit mã) phát đi và thu về là 0,33us (tức tần số tạo mã 2,997MHz) thỏa mãn với các thông số tính toán, thiết kế.

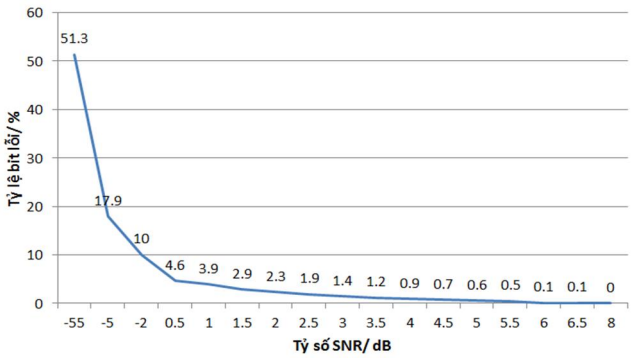
Về sai số phép đo cự ly: Thông tin cự ly sẽ xác định ngay sau khi truyền và nhận 1 bit mã. Tuy nhiên, để xác định được có phải là tín hiệu mục tiêu hay không, cần chờ nhận đủ 31 bit mã. Vì vậy, sai số phép đo được xác định bởi $\Delta D = \Delta D_1 + \Delta D_2$. Trong đó, ΔD_1 gây ra bởi độ trễ đáp ứng của đầu phát và thu laser khi truyền và nhận 1 bit mã, ΔD_2 gây ra bởi độ dịch chuyển của mục tiêu giữa 1 chu kỳ phát và thu 1 bit dữ liệu (31 bit mã). Với giả thiết tốc độ máy bay là 500m/s, tên lửa là 1200m/s, khi đó vận tốc tương đối của máy bay so với tên lửa $v_{tenlua\_muctieu}$ sẽ là: tối đa 1700m/s, tối thiểu là 700m/s. Khi đó ΔD = ~ 0,8m. Với sai số này, thoả mãn điều kiện yêu cầu đối với tên lửa phòng không có bán kính sát thương đến vài chục mét.

Về lỗi bit, trong 1024 bit dữ liệu truyền thì có 8 bit dữ liệu bị lỗi, tương ứng 0,7% tổng số bit truyền đi (hình 9). Đây là mức lỗi bit rất thấp.



Hình 9. Kết quả hiển thị lỗi bit trong mô phỏng

Để đánh giá được mức độ ảnh hưởng của nhiễu lên lỗi bit thực hiện khảo sát trên toàn dải nhiễu theo tỷ số SNR. Đồ thị biểu diễn bit lỗi tương ứng với mức nhiễu thể hiện trên hình 10.



Hình 10. Khảo sát lỗi bít khi thay đổi nền nhiễu

Khi tăng SNR thì số bit lỗi giảm dần, với SNR > 5,5dB thì tỷ số bit lỗi giảm dần về 0. Điều này chứng tỏ khả năng chống nhiễu tốt của phương pháp đề xuất.

4.2. Khảo sát, đánh giá tính bảo mật và phá mã

Khảo sát 2 trường hợp nguồn phá mã sử dụng bộ mã ngẫu nhiên 31bit và sử dụng chính mã Gold 31bit nhưng không biết chuỗi khởi tạo của mã, các điều kiện mô phỏng khác giống nhau (SNR 9dB). Kết quả khảo sát như bảng 2.

Bảng 2. Kết quả khảo sát

Số mẫu thử	Mã ngẫu nhiên (%)	Mã Gold (Không biết mã) (%)	Mã gold (Biết chính xác mã) (%)	Ghi chú
1	50,1	42	0	SNR 9dB
2	51,8	34,5	0	SNR 9dB
3	53,5	35,2	0	SNR 9dB
Trung bình	51,8	37,2	0	

Nhận xét: Trường hợp đối phương cũng sử dụng mã Gold. Tỷ lệ lỗi bit là 37% của 31 bit tương ứng với 11 bit lỗi, để dò ra mã đúng phải thử 2^11 lần nên không đủ thời gian do tên lửa đã tiếp tục di chuyển đến vị trí khác. Như vậy, đây là phương pháp có độ bảo mật rất cao. Nếu đối phương không biết mã dùng để mã hóa thì sẽ không thể tạo giả được chuỗi tín hiệu phản xạ từ mục tiêu về đầu thu laser. Như vậy, đây là phương pháp có độ bảo mật rất cao.

So với việc sử dụng các phương pháp mã hóa sửa lỗi khác như CRC, Hamming thì giải pháp này có một số ưu điểm đó là: Có thể thay đổi chuỗi PN được nên khả năng bị dò và phá chủ động sẽ khó hơn rất nhiều; Bộ mã và tạo mã đơn giản, dễ lập trình, dễ cài đặt tham số và triển khai trên phần cứng.

Để đảm bảo khả năng bảo mật và tỷ lệ lỗi bit nhỏ thì cần sử dụng chuỗi bit đủ lớn (8, 16, 32 hoặc 64 bit) tùy vào loại đầu nổ và yêu cầu cụ thể.

5. KẾT LUẬN

Việc ứng dụng kỹ thuật mã hoá trong các bộ thu - phát laser giúp tăng cường khả năng chống nhiễu và cho phép thu được các thông tin có ích một cách chính xác. Điều này giúp nâng cao chất lượng hoạt động của các ngòi nổ laser, giảm khả năng chế áp điện tử của đối phương. Phương pháp đề xuất được đánh giá trên phần mềm mô phỏng Matlab-Simulink và tiến tới thực nghiệm trên vi xử lý. Kết quả mô phỏng cho thấy, kỹ thuật mã hoá cho phép nâng cao đáng kể độ chính xác trong truyền và nhận tín hiệu, tỉ lệ lỗi do nhiễu gây ra là không đáng kể. Trên cơ sở các kết quả đạt được, có thể mở ra khả năng ứng dụng trong các ngòi nổ laser nhằm tăng độ tin cậy, cũng như nâng cao xác suất tiêu diệt mục tiêu cho các tên lửa phòng không hiện đại.

TÀI LIỆU THAM KHẢO

[1]. Krenev G.A., 2006. *Asymmetric response to precision weapons*. Voenizdat, Moscow.

[2]. Ove Steinvall, 2000. *Effects of target shape and reflection on laser radar cross sections.* Applied Optics Vol. 39, Issue 24, pp. 4381-4391

[3]. Kun Wang, Huimin Chen, 2011. *Analysis on the characteristics of pulsed laser proximity fuze's echo.* Proceedings Volume 8192, International Symposium on Photoelectronic Detection and Imaging 2011: Laser Sensing and Imaging; and Biological and Medical Applications of Photonics Sensing and Imaging; 819210. https://doi.org/10.1117/12.900186

[4]. Yan Xiaopeng, LI Ping, 2008. *Study on Detection Techniques for Laser Fuze using Pseudorandom Code*. Proceedings Volume 6824, Semiconductor Lasers and Applications III; 682418. https://doi.org/10.1117/12.756386.

[5]. Wen Zongping, 1996. *A study on laser Pseudorandom Code detection*. 8358th Institute, 3rd Academy, CASC Tianjin 300192.

[6]. Wang Wei, Deng Jia-hao, Huang Yan, Yin Jun 2003. *Laser Fuze Detection Technique Using the Pseudorandom Code*. Journal of Beijing Institute of Technology, 6/2003.

[7]. WEI Su-juan, Deng Jia-hao, Yao Xiu-juan, 2005. *Study on the Signal Processing Technique of Laser Fuzes*. Journal of Beijing Institute of Technology 3/2005.

[8]. Gong Jimin, 1989. *Proximity fuze phase-modulation by pseudo-random code.* Acta Armamentarii, 4/1989.

[9]. VK Arora, 2010. *Proximity Sensors Theory and Techniques.*

AUTHORS INFORMATION

Nguyen Duc Thi[1], Nguyen Truong Son[2], Tran Hoai Linh[3], Tran Xuan Tinh[4], Tran Thuy Van[5]

[1]General Department of Defense Industry

[2]Military Technical Institute

[3]Hanoi University of Technology

[4]Air Defense - Air Force Academy

[5]Hanoi University of Industry