ĐỀ XUẤT GIẢI PHÁP GIẢI MÃ KÊNH ỨNG DỤNG CHO MÃ TÍCH

THE PROPOSED SOLUTION OF THE DECODER CHANNELS FOR PRODUCT CODES

Nguyễn Thị Hồng Nhung, Phạm Văn Nam

Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp

Đến Tòa soạn ngày 27/04/2022, chấp nhận đăng ngày 23/05/2022

Tóm tắt: Mạng cảm biến vô tuyến công nghiệp cần có các giải pháp mã kênh mạnh với các gói tin ngắn. Mã tích là họ mã kênh chỉ cần với chiều dài từ mã ngắn, đã đạt khả năng sửa lỗi rất tốt do có khoảng cách Hamming cực tiểu lớn. Vì quá trình giải mã phức tạp nên hiện nay mã tích vẫn chưa được đề xuất ứng dụng trong các hệ thống truyền tin. Với mong muốn khai thác khả năng kiểm soát lỗi của mã tích trong các ứng dụng truyền tin hiện đại, bài báo này dựa vào cơ sở lý thuyết giải mã tích, lựa chọn mã Hamming làm mã thành phần, đề xuất thuật toán giải mã lặp áp dụng phù hợp với mã tích cho chất lượng giải mã tốt với độ phức tạp chấp nhận được. Kết quả mô phỏng cho thấy, tại tỉ lệ lỗi bit (BER) 10^{-5}, yêu cầu về tỉ lệ công suất tín hiệu trên tạp âm chỉ cần 3,7 dB nếu sử dụng mã Hamming (31, 26) làm mã thành phần.

Từ khóa: Giải mã đối ngẫu, mã tích, mã Hamming, giải mã lặp, mã kênh.

Abstract: Industrial wireless sensor network requires strong channel codes with communication with short packages. Product codes are a family of channel codes which only require short codeword to achieve very good errror correction thanks to the minimum hamming distance. Due to the complex decoding process, product codes haven't yet been proprosed for application in communication systems. With the desire to exploit the error control ability of product codes in modern communication applications, this article which bases on the theory of product codes decoding and selects Hamming codes as component codes proposes interative decoding algorithms which is appropriately applied to the product codes with good decoding performance and acceptable complexity. Simulation results have shown that at the bit error rate (BER) of 10^{-5}, the requirement of signal to noise ratio is only 3,7 dB in case of using Hamming codes (31, 26) as the component codes.

Keywords: Dual codes decoder, Product codes, Hamming codes, iterative decoding, Channel codes.

1. ĐẶT VẤN ĐỀ

Ngày nay, hệ thống cơ sở hạ tầng phát triển không ngừng, mạng cảm biến vô tuyến đã và đang thể hiện những lợi thế hấp dẫn so với các hệ thống có dây truyền thống. Trong các môi trường khắc nghiệt, nhiễu lớn (như có nhiễu điện từ, có vật thể chuyển động và giao tiếp bị che chắn) dẫn đến lỗi truyền dẫn, làm ảnh hưởng đến chất lượng và thời gian xử lý thông tin. Các hệ thống cảm biến vô tuyến dễ dàng bị ảnh hưởng trong môi trường truyền tin này, đặc biệt là các mạng cảm biến vô tuyến công nghiệp có nguy cơ cao về lỗi truyền dẫn, có thể dẫn đến thiếu hoặc chậm trễ quá trình hoặc kiểm soát dữ liệu [2]. Lỗi truyền dẫn và bỏ lỡ quy trình hoặc thời hạn kiểm soát có thể dẫn đến tổn thất kinh tế nghiêm trọng và các vấn đề vi phạm an toàn. Để triển khai mạng

cảm biến vô tuyến công nghiệp, cần sử dụng kỹ thuật FEC với họ mã sửa lỗi có chiều dài ngắn với phương pháp giải mã hiệu quả nhằm đảm bảo truyền tin thời gian thực và đáng tin cậy.

Mã tích có khoảng cách mã lớn được xây dựng từ các mã thành phần có độ dài và khoảng cách mã nhỏ cho phép đạt chất lượng và độ phức tạp có thể so sánh với mã Turbo với số vòng lặp nhỏ hơn [3]. Có nhiều thuật toán giải mã mã tích đã được trình bày từ khi mã tích được biết đến. Các thuật toán này nhìn chung phân làm hai loại: Các thuật toán đơn giản cho chất lượng giải mã thấp và các thuật toán cho chất lượng giải mã cao nhưng có độ phức tạp cao [4], [5]. Giải mã Turbo có thể được áp dụng cho mã tích, sử dụng thuật toán cực đại hóa xác suất hậu nghiệm (MAP: Maximum a Posterior Probability) cho các mã thành phần. Đây là trở ngại lớn đối với việc sử dụng các mã khối tốt thay vì mã chập trong các hệ thống giải mã Turbo kết hợp, trừ các trường hợp rất hiếm, khi kích thước của mã rất nhỏ hoặc khi các mã cấu thành rất đơn giản. Để giải quyết vấn đề phức tạp của giải mã MAP mã thành phần, nhiều đề xuất có tiềm năng đã được thực hiện.

Thuật toán giải mã tối ưu được gọi là thuật toán Viterbi đầu ra mềm, gần giống với giải mã MAP, trên mã đối ngẫu, sử dụng các hàm phi tuyến dẫn đến độ phức tạp rất cao cho chất lượng kiểm soát lỗi lý tưởng. Vì vậy, theo các công trình đã công bố, phương pháp này chỉ dừng lại ở mức nghiên cứu lý thuyết và rất khó có thể áp dụng vào thực tế [6], [7].

Trong [8], [9], một biến thể nhằm giảm độ phức tạp cho việc giải mã MAP của các mã thành phần đã được đưa ra, cho chất lượng xấp xỉ tại [6]. Tuy nhiên phương pháp này sử dụng sự ước lượng gần đúng, không phải lúc nào cũng được giải thích hay trình bày bằng cơ sở lý thuyết, rất khó phân tích, nên việc cải thiện cũng như áp dụng cho các mã khác là không khả thi.

Nhìn chung, hiện nay chưa có nhiều phương pháp giải mã thực sự hiệu quả để có thể tận dụng khả năng sửa lỗi của mã tích.

Phương pháp giải mã đối ngẫu là phương pháp giải mã lặp bằng cách vét toàn bộ thông tin giải mã trong bộ mã đối ngẫu rất phù hợp các mã khối có độ dư nhỏ với độ phức tạp thấp [10]. Với các mã có độ dư nhỏ, vấn đề giải mã bằng mã đối ngẫu sẽ giảm được sự phức tạp mà vẫn đảm bảo thông tin giải mã như mã gốc, vì số lượng từ mã trong mã đối ngẫu của các mã này ít hơn nhiều so với mã gốc [11]. Như vậy, ý tưởng kết hợp ưu điểm về chất lượng kiểm soát lỗi cao của mã tích và tận dụng tính chất đối ngẫu của mã khối với phương pháp giải mã đối ngẫu cho mã thành phần mã tích là nội dung chính của trong bài báo [1]. Hướng nghiên cứu này tránh được giải mã MAP cho các mã thành phần. Hy vọng mã tích sẽ được đưa vào ứng dụng trong các hệ thống truyền tin số, đặc biệt là các hệ thống truyền tin yêu cầu thời gian thực. Với mong muốn tìm được phương pháp giải mã thực sự hiệu quả cho mã tích, bài báo này đã đề xuất được ý tưởng tích cực. Phần còn lại của bài báo có bố cục như sau: Mục 2 trình bày cơ sở lý thuyết thuật toán giải mã mới cho mã tích. Mục 3 đề xuất thuật toán giải mã lặp cải tiến cho mã tích trên cơ sở sử dụng phương pháp giải mã mềm cho mã đối ngẫu của các mã thành phần. Mục 4 trình bày các kết quả mô phỏng đánh giá chất lượng các thuật toán đề xuất cho các mã tích trên kênh Gauss và cuối cùng là phần Kết luận.

2. CƠ SỞ LÝ THUYẾT CỦA THUẬT TOÁN GIẢI MÃ CHO MÃ TÍCH

Cho **C** là mã khối tuyến tính với ma trận sinh **G** kích thước ($k \times n$), ma trận kiểm tra **H** kích thước (($n-k$)×n) và $\mathbf{c} = (c_1, c_2, ..., c_n)$ là từ mã;

trong đó n là chiều dài các bít mã, k là chiều dài các bít tin. Tín hiệu thu được là $\mathbf{y}=\mathbf{x}+\mathbf{w}$, trong đó $\mathbf{w}=(w_1,w_2,...,w_n)$ là vectơ tạp âm và $y_m=x_m+w_m$, $1\le m\le n$. . Cho $\mathbf{C}$' là mã đối ngẫu của $\mathbf{C}$, với $\mathbf{c}_j^{'}=(c_{j1}^{'},c_{j2}^{'},...,c_{jn}^{'})$ là từ mã đối ngẫu thứ j. Ký hiệu $P(y_m\,|\,\mathbf{i}),\mathbf{i}\in\{0,1\}$ là xác suất có điều kiện rằng thu được y_m khi bit mã $c_m=\mathbf{i}$ được gửi đi. Ký hiệu $\varphi_m=P(y_m\,|\,1)/P(y_m\,|\,0)$ là tỷ lệ hợp lẽ (Likelihood Ratio) của bit thứ m. Như vậy, $\varphi_m=\exp(-2y_m/\sigma^2)$. Theo [1]:

$$A_m(0)=\sum_{t=0}^{1}\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\sum_{i=0}^{1}(-1)^{\mathbf{i}(c_{jl}^{'}+t\delta_{ml})}P(y_m\,|\,\mathbf{i}) \tag{1}$$

$$A_m(1)=\sum_{t=0}^{1}(-1)^{t}\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\sum_{i=0}^{1}(-1)^{\mathbf{i}(c_{jl}^{'}+t\delta_{ml})}P(y_m\,|\,\mathbf{i}) \tag{2}$$

Ta có $A_m(0)=\lambda P(0\,|\,\mathbf{y})$ và $A_m(1)=\lambda P(1\,|\,\mathbf{y})$, với một hệ số xác định λ [1]. Nói cách khác, máy giải mã sẽ quyết định rằng bit c_m = 0 được gửi qua kênh khi và chỉ khi $A_m(0)>A_m(1)$ hay $A_m(0)-A_m(1)>0$.

Đầu vào của phép tính cho giải mã là giá trị tỷ lệ hợp lẽ xác suất hậu nghiệm φ_m và đầu ra của giải mã là hiệu

$$A_m(0)-A_m(1)=\lambda P(0\,|\,\mathbf{y})-\lambda P(1\,|\,\mathbf{y}).$$

Mà, giải mã mã tích là giải mã lần lượt cột-hàng (hàng-cột). Như vậy, để kế thừa được phương pháp giải mã của [10] cho mã tích, trong [1] đã biến đổi để đầu ra của tính toán trong bước giải mã hàng (cột) có thể làm đầu vào cho bước giải mã cột (hàng) sau. Theo [1]:

$$A_m(0)+A_m(1)=\lambda\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\left(\frac{1-\varphi_l}{1+\varphi_l}\right)^{c_{jl}^{'}} \tag{3}$$

$$A_m(0)-A_m(1)=\lambda\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\left(\frac{1-\varphi_l}{1+\varphi_l}\right)^{c_{jl}^{'}\oplus\delta_{ml}} \tag{4}$$

với $\delta_{ml}=1$ khi $m=l$ và $\delta_{ml}=0$ khi $m\ne l$.

Nên:

$$\frac{A_m(1)}{A_m(0)}=\frac{P(1\,|\,\mathbf{y})}{P(0\,|\,\mathbf{y})}=\frac{P(1\,|\,y_m)P(y_m\,|\,\mathbf{y})}{P(0\,|\,y_m)P(y_m\,|\,\mathbf{y})}$$

$$=\frac{P(y_m\,|\,1)P(1)}{P(y_m\,|\,0)P(0)}=\frac{P(y_m\,|\,1)}{P(y_m\,|\,0)}=\varphi_m,$$

với giả định rằng các bit 0 và 1 được gửi đi với xác suất như nhau.

Như vậy, cách tính các giá trị tỷ lệ hợp lẽ làm đầu vào mềm, đầu ra mềm cho bước giải mã hàng (cột) tiếp theo của mã tích là:

$$\varphi_m=\frac{A_m(1)}{A_m(0)}=\frac{B_2-B_1}{B_2+B_1} \tag{5}$$

với

$$B_2=\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\left(\frac{1-\varphi_l}{1+\varphi_l}\right)^{c_{jl}^{'}} \tag{6}$$

$$B_1=\sum_{j=1}^{2^{n-k}}\prod_{l=1}^{n}\left(\frac{1-\varphi_l}{1+\varphi_l}\right)^{c_{jl}^{'}\oplus\delta_{ml}}. \tag{7}$$

Công thức (5) là cơ sở lý thuyết cho phương pháp giải mã mã tích [1].

3. ĐỀ XUẤT THUẬT TOÁN GIẢI MÃ MỚI CHO MÃ TÍCH

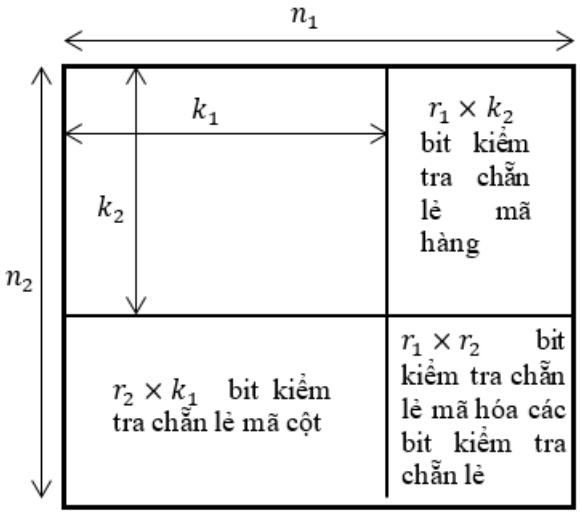
Xét mã tích $\mathbf{C}(n,k,d)$ có mã thành phần là hai mã khối tuyến tính $\mathbf{C}_1(n_1,k_1,d_1)$ và $\mathbf{C}_2(n_2,k_2,d_2)$, với ma trận sinh $\mathbf{G}_1$ kích thước $k_1\times n_1$ và ma trận sinh $\mathbf{G}_2$ kích thước $k_2\times n_2$, tương ứng. Đặt r_1,r_2 là chiều dài các bít kiểm tra trong bộ mã $\mathbf{C}_1,\mathbf{C}_2$ tương ứng.

Khi mã hóa, $k_1\times k_2$ bít thông tin được mã hóa thành $n_1\times n_2$ bít mã, tốc độ mã hóa là

$(k_1/n_1)(k_2/n_2)$ và khoảng cách Hamming tối thiểu là $(d_1 \times d_2)$, với d_1 và d_2 lần lượt là khoảng cách Hamming tối thiểu tương ứng của mã $\mathbf{C}_1$ và $\mathbf{C}_2$. Đầu vào bộ mã hóa là tin **u** (kích thước $k_2 \times k_1$), mã hóa bởi mã tích **C** có ma trận sinh **G**, được từ mã **c** (kích thước $n_2 \times n_1$). Từ mã **c** có thể được tạo ra bằng cách nhân một vector nhị phân chiều dài $k_1 k_2$ với ma trận sinh của **C** hoặc bằng cách sử dụng phương trình:

$$\mathbf{c} = \mathbf{G}_2^T \otimes \mathbf{u} \otimes \mathbf{G}_1 \quad (8)$$

với $\mathbf{G}_2^T$ là ma trận chuyển vị của ma trận sinh $\mathbf{G}_2$. Từ mã **c** được điều chế BPSK và được truyền qua kênh rời rạc không nhớ tạp âm Gauss với mật độ phổ công suất $2\sigma^2$.



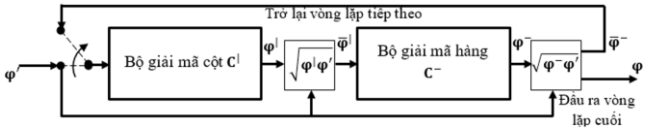
Hình 1. Cấu trúc mã tích

Cấu trúc mã tích (hình 1) cho thấy, mã tích chính là mã khối dài có thể được xây dựng bởi hai hay nhiều mã khối thành phần ngắn hơn. Mã tích có tỷ lệ mã hóa bằng tích các mã thành phần nên việc lựa chọn các mã thành phần là các mã khối có tỷ lệ mã hóa cao là ý tưởng hợp lý. Với các mã có tỷ lệ mã hóa cao, vấn đề giải mã bằng mã đối ngẫu sẽ giảm được sự phức tạp mà vẫn đảm bảo thông tin giải mã như mã gốc [10].

Nhằm đề xuất một phương pháp giải mã tích cho chất lượng tốt hơn, bài báo sẽ kế thừa ý tưởng phải tính đến ảnh hưởng của xác suất không đều của các bít từ mã trong [6] để cải tiến thuật toán giải mã DCAPC *(Dual codes Algorithm decoding of Product Codes)* được đưa ra trong [1]. DCAPC là thuật toán giải mã mềm được phát triển từ thuật toán giải mã tối ưu trong [10]. Để phát triển và ứng dụng thuật toán giải mã của các tác giả C.R.. Hartmann và Luther D. Rudolph cho mã tích, các tác giả trong [1] đã chứng minh và đưa ra công thức tính các giá trị tỷ lệ hợp lẽ làm đầu vào mềm, đầu ra mềm cho bước giải mã hàng (cột) tiếp theo. Các giá trị tỷ lệ hợp lẽ này được tính với giả thiết các bít 0 và 1 được gửi đi với xác suất như nhau.

Để đảm bảo tính ngẫu nhiên của các bít tin nhận được tại đầu vào bộ giải mã, ý tưởng trong bài báo này là: thông tin nhận được ban đầu đều được đưa vào các bước giải mã hàng (cột) tiếp theo. Phương pháp giải mã đề xuất trong bài báo này có thể được coi là phương pháp giải mã tối ưu cho mã tích. Vì, thông tin giải mã nhận được từ việc tính cả thông tin xác suất xuất hiện ngẫu nhiên của các bít từ mã tại đầu vào giải mã mỗi hàng (cột) và thông tin giải mã trong toàn bộ không gian mã đối ngẫu.

Gọi thuật toán giải mã này là thuật toán giải mã lặp mã đối ngẫu (IDDC: Iterative Decoding using Dual Codes). Bộ giải mã bao gồm hai bộ giải mã cột $\mathbf{C}^{|}$ và hàng $\mathbf{C}^{-}$ nối tiếp, quá trình giải mã được mô tả trên hình 2:



Hình 2. Phương pháp giải mã đối ngẫu tối ưu

Bộ giải mã tích nhận được tin

$\mathbf{y} = [y_{uv}, 1 \le v \le n_1, 1 \le u \le n_2]$ và hoạt động như sau:

Bộ giải mã cột (hàng) nhận thông tin đầu vào là ma trận $\boldsymbol{\varphi}'$ và chèn thêm các giá trị $\varphi'_{uv} = 1,\ k_2 + 1 \le u \le n_2,\ k_1 + 1 \le v \le n_1$, sau đó thực hiện vòng lặp thứ 1.

Bước 1: Tiến hành tính toán lại lần lượt giá trị từng cột (hàng) trong $\boldsymbol{\varphi}'$ để đưa ra ma trận $\varphi^{|}(n_2, n_1)$, với giá trị tương ứng cho bít mã thứ *m* trong một cột (hàng) bất kỳ:

$$\varphi_m^{|} = \frac{\sum_{j=1}^{2^{n_2-k_2}} \prod_{l=1}^{n_2} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{2jl}} - \sum_{j=1}^{2^{n_2-k_2}} \prod_{l=1}^{n_2} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{2jl} \oplus \delta_{ml}}}{\sum_{j=1}^{2^{n_2-k_2}} \prod_{l=1}^{n_2} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{2jl}} + \sum_{j=1}^{2^{n_2-k_2}} \prod_{l=1}^{n_2} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)} \quad (9)$$

Trong đó, $\oplus$ là phép cộng modulo 2; $\delta_{ml} = 1$ nếu $m = l$ và $\delta_{ml} = 0$ với các trường hợp khác; c'_{ajl} là bit thứ *l* của từ mã thứ *j* trong bộ mã đối ngẫu $\mathbf{C}'_a(n_a, r_a)$ của bộ mã gốc $\mathbf{C}_a(n_a, k_a)$; $a \in \{1, 2\}$; $\varphi'_m = P(y_m|1)/P(y_m|0)$.

Bước 2: Bộ giải mã hàng (cột) nhận trực tiếp thông tin giải mã tính toán được từ bước 1 là ma trận giá trị $\overline{\boldsymbol{\varphi}}^{|}$:

$$\overline{\boldsymbol{\varphi}}^{|} = \sqrt{\boldsymbol{\varphi}^{|}\boldsymbol{\varphi}'} \quad (10)$$

Tương tự bước 1, tiếp tục tính toán lại lần lượt giá trị từng hàng (cột) trong ma trận $\overline{\boldsymbol{\varphi}}^{|}$ để đưa ra ma trận $\boldsymbol{\varphi}^{-}$ với giá trị tương ứng cho bít mã thứ *m* trong một hàng (cột) bất kỳ:

$$\boldsymbol{\varphi}_m^{-} = \frac{\sum_{j=1}^{2^{n_1-k_1}} \prod_{l=1}^{n_1} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{1jl}} - \sum_{j=1}^{2^{n_1-k_1}} \prod_{l=1}^{n_1} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{1jl} \oplus \delta_{ml}}}{\sum_{j=1}^{2^{n_1-k_1}} \prod_{l=1}^{n_1} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{1jl}} + \sum_{j=1}^{2^{n_1-k_1}} \prod_{l=1}^{n_1} \left(\frac{1-\varphi'_l}{1+\varphi'_l}\right)^{c'_{1jl} \oplus \delta_{ml}}} \quad (11)$$

với, c'_{1jl} là bit thứ *l* của từ mã thứ *j* trong bộ mã đối ngẫu $\mathbf{C}'_1(n_1, r_1)$ của bộ mã gốc $\mathbf{C}_1(n_1, k_1)$. Tại đầu ra bộ giải mã thứ 2, cũng lấy giá trị trung bình nhân của ma trận giá trị $\boldsymbol{\varphi}_m^{-}$ với thông tin đầu vào ban đầu $\boldsymbol{\varphi}'$ theo công thức (10), được ma trận giá trị $\boldsymbol{\varphi}_m^{-}$ làm thông tin đầu vào cho vòng lặp tiếp theo. Quá trình giải mã được thực hiện cho đến vòng lặp cuối thì dừng lại.

Bước 3: Quyết định từ mã đầu ra dựa vào ma trận giá trị $\boldsymbol{\varphi}$ nhận được ở vòng lặp cuối.

$$\begin{cases} C_{ij} = 1 \text{ khi } \varphi_{ij} \ge 1 \\ C_{ij} = 1 \text{ khi } \varphi_{ij} < 1 \end{cases};$$

với C_{ij} là bít mã tương ứng trong từ mã tích $C(1 \le j \le n_1, 1 \le i \le n_2)$.

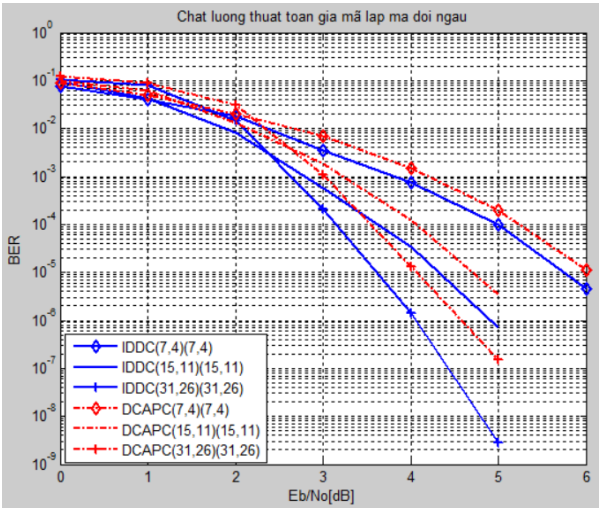
Như vậy, bài báo đã đưa ra đề xuất cải tiến so với thuật toán DCAPC [1] tại bước giải mã thứ 2. Ở đây, thông tin nhận được ban đầu đều được kết hợp với thông tin giải mã nhận được của bộ giải mã cột (hàng) để đưa vào bước giải mã hàng (cột) tiếp theo. Nghĩa là, tại đầu ra bộ giải mã cột (hàng), nhằm đảm bảo tính ngẫu nhiên của các bit từ mã, IDDC lấy giá trị trung bình nhân của ma trận $\boldsymbol{\varphi}^{|}$ với ma trận giá trị thông tin đầu vào ban đầu $\boldsymbol{\varphi}'$, làm đầu vào cho bước giải mã hàng (cột) tiếp theo.

4. ĐÁNH GIÁ CHẤT LƯỢNG THUẬT TOÁN ĐỀ XUẤT

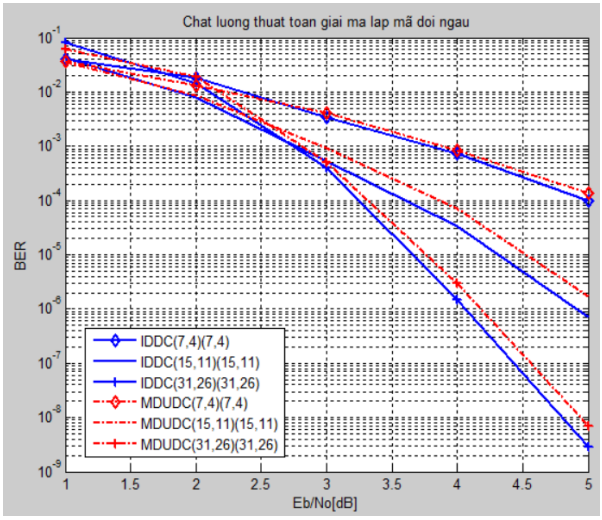
Để đánh giá thuật toán đề xuất chúng ta cần so sánh hiệu quả kiểm soát lỗi kênh của mã tích khi sử dụng thuật toán mới với thuật toán giải mã đối ngẫu mã tích (*DCAPC) và thuật toán MDUDC* đã được công bố [1].

Bài báo sử dụng kỹ thuật mô phỏng MonteCarlo nhằm khảo sát chất lượng thuật toán đề xuất trên kênh Gauss. Khả năng sửa lỗi của mã tích có các mã thành phần là các mã

thuộc họ mã Hamming (7,4); (15,11); (31,26) khi sử dụng thuật toán đề xuất, thu được kết quả chỉ sau hai lần lặp như Hình 3. Kết quả mô phỏng cho thấy, đối với mã thành phần là mã Hamming (31,26), chỉ cần tỉ lệ công suất tín hiệu trên tạp âm là 3,7 dB, thuật toán giải mã IDDC đã có thể đạt tỉ lệ lỗi bít là 10^{-5}. Dễ dàng thấy, thuật toán giải mã đề xuất cho tăng ích khoảng 0,3 dB đến 0,47 dB so với kết quả của DCAPC và 0,1 đến 0,2 dB so với kết quả của MDUDC tại tỉ lệ lỗi bit 10^{-5} [1]. Bảng 1 biểu thị sự đánh giá chi tiết về độ lợi giải mã của IDDC so với các thuật toán khác của các mã tích có mã thành phần với độ dài khác nhau.



Hình 3a. Chất lượng thuật toán giải mã IDDC



Hình 3b. Chất lượng thuật toán giải mã IDDC

Thuật toán IDDC sử dụng thông tin giải mã từ các từ mã thuộc mã đối ngẫu nhằm giảm bớt độ phức tạp. Như vậy, theo bảng 1, các mã thành phần có tỉ lệ mã hóa càng cao, thuật toán mới sẽ cho độ lợi nhiều hơn so với DCAPC. Còn khi so với thuật toán MDUDC, chất lượng giải mã cũng nhỉnh hơn, MDUDC có độ phức tạp quá cao, khó áp dụng thực tế [1].

Bảng 2 chỉ ra số lượng phép tính cần để giải mã mã tích với các mã thành phần là mã Hamming trong hai lần lặp khi sử dụng thuật toán IDDC. Rõ ràng, IDDC có độ phức tạp chấp nhận được là hàm tuyến tính $O(n,2^r)$. Điều này cũng cho thấy rằng, thuật toán đề xuất vẫn đảm bảo được tốc độ mã hóa cao, độ phức tạp tương đương nhưng đạt chất lượng giải mã tốt hơn so với thuật toán DCAPC [1].

Bảng 1. Độ lợi giải mã của IDDC khi so sánh với DCAPC và MDUDC tại $\mathrm{BER}=10^{-5}$

Mã tích	*Độ lợi so với DCAPC*	*Độ lợi so với MDUDC*
C(7,4)×(7,4)	0,3 dB	0,1 dB
C(15,11)×(15,11)	0,35 dB	0,2 dB
C(31,26)×(31,26)	0,47 dB	0,11 dB

Bảng 2. Độ phức tạp của thuật toán IDDC

Thuật toán	**IDDC**
Số phép tính nhân	$2n_1n_2\left[(n_1-1)2^{r_1}+(n_2-1)2^{r_2}+2\right]$
Số phép tính cộng	$2n_1n_2\left(2^{r_1}+2^{r_2}+2\right)$
Tổng số phép tính	$2n_1n_2\left(n_1 2^{r_1}+n_2 2^{r_2}+4\right)$

Với phương pháp giải mã này, ta có thể tính được độ phức tạp giải mã, kết quả tính toán mở ra tính khả thi khi hiện thực hóa thuật toán bằng các thiết bị phần cứng.

2. KẾT LUẬN

Từ cơ sở lý thuyết giải mã cho mã tích, bài báo đề xuất thuật toán giải mã mới IDDC. Thuật toán mới cho mã tích có cơ sở lý thuyết chắc chắn, sử dụng không gian mã đối ngẫu để giải mã, có độ phức tạp tính toán chấp nhận được đem lại độ lợi giải mã cao, phù hợp với các mã thành phần có mật độ cao và chiều dài ngắn. Kết quả nghiên cứu về thuật toán giải mã mới cho mã tích cho phép mở ra hướng mới về việc ứng dụng mã tích vào các hệ thống cảm biến vô tuyến yêu cầu thời gian thực, đồng thời có thể làm cơ sở để đề xuất các cải tiến mới cho các mã kênh nhằm kiểm soát lỗi đường truyền.

TÀI LIỆU THAM KHẢO

[1] Phạm Xuân Nghĩa, Nguyễn Thị Hồng Nhung, "Giải mã tích bằng giải mã quyết định mềm dùng mã đối ngẫu đảm bảo tính khả dụng", Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự, số 57, trang 11- 17, (2018).

[2] Kan Yu, "On reliable real time communication in industrial wireless sensor networks", Malardalen University, Sweden (2012).

[3] P. Elias, "Error-free coding", IEEE Transactions on Information Theory, vol. 4, pp. 29-37, (1954).

[4] A.J. Viterbi, "Convolutional codes and their performance in communication systems", IEEE Transactions on Communication Technology, COM- 19: 751-772, (1971).

[5] O. Al-Askary, "Iterative decoding of product codes", PhD Dissertation, Royal Institute of Technology, (2003).

[6] [J. Hagenauer, E. Offer and Lutz Papke, "Iterative decoding of binary block and convolutional codes", IEEE Transactions on Information Theory, vol. 42, pp. 429- 445, (1996).

[7] H. Nickl, J. Hagenauer and F. Burkert, "Approaching Shannon's capacity limit by 0.27 dB using Hamming codes in a 'turbs' decoding scheme", Proceedings of IEEE International Symposium on Information Theory, (1997).

[8] R.M. Pyndiah, "Near optimum decoding of product codes", IEEE Transactions on Communications, vol. 46, pp. 1003-1010, (1994).

[9] R.M. Pyndiah, "Near-optimum decoding of product codes: Block Turbo codes", IEEE Transactions on Communications, vol. 46, pp. 1003-1010, (1998).

[10] C.R.P. Hartmann, Luther D. Rudolph, "An optimum symbol-by-symbol decoding rule for linear codes", IEEE Transactions on Information Theory, vol. 22, pp. 514- 517, Sept., (1976).

[11] F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland Publishing Company, New York, USA, (1981).

[12] P. Robertson, E. Villebrun, P. Hoeher, "A comparison of optimal and sub-optimal MAP decoding algorithms operating in the log domain", Proceedings IEEE International Conference on Communications ICC '95, (2002)

Thông tin liên hệ: **Nguyễn Thị Hồng Nhung**

Điện thoại: 0945 616 629 - Email: nthnhung@uneti.edu.vn

Khoa Điện tử, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp.