# ỨNG DỤNG KỸ THUẬT GIẢI MÃ ĐỐI NGẪU TRONG GIẢI MÃ LDPC

**Nguyễn Anh Tuấn[1*], Phạm Văn Ngọc[1], Phạm Xuân Nghĩa[2]**
*[1]Trường Đại học Công nghệ thông tin và truyền thông – ĐH Thái Nguyên*
*[2] Đại học Kỹ thuật Lê Quý Đôn*

TÓM TẮT

Bài báo trình bày cơ sở của phương pháp giải mã khối sử dụng kỹ thuật giải mã đối ngẫu, ứng dụng trên mã Haming, mã LDPC... Phương pháp này cho phép áp dụng kỹ thuật giải mã lặp đồng thời kết hợp với việc sử dụng các ma trận kiểm tra tương đương và kỹ thuật quyết định từ mã dựa vào trọng số syndrome khi thực hiện giải mã. Các kết quả mô phỏng thực hiện trên mô hình kênh Gauss và kênh pha đinh sử dụng thuật toán giải mã BPA-EH (Belief Propagation Algorithm based on Equivalent Parity Check Matrix *H*) cho kết quả cải thiện rõ rệt về độ lợi giải mã và rút ngắn được thời gian giải mã so với thuật toán BPA truyền thống.

**Từ khóa:** *Mã đối ngẫu, mã LDPC, ma trận kiểm tra, giải mã BPA, kênh Gauss, kênh pha đinh*

## ĐẶT VẤN ĐỀ

Mã kiểm tra chẵn lẻ mật độ thấp (LDPC-Low Density Parity Check) hiện nay được nghiên cứu nhiều và được chọn là mã dự phòng dài hạn cho các hệ thống thông tin di động thế hệ mới. Mã LDPC được biết đến cùng với các thuật toán giải mã truyền thống như: BPA, SPA, MPA... [1]. Các thuật toán này cho chất lượng giải mã khá tốt, tuy nhiên việc cải tiến nâng cao chất lượng giải mã vẫn là nội dung đang tiếp tục được nghiên cứu.

Với bản chất là một mã khối tuyến tính, cơ chế phát hiện và sửa sai của mã LDPC dựa vào đa thức kiểm tra $\boldsymbol{H}$. Mặt khác, với tính chất đối ngẫu của mã sửa sai, có thể áp dụng phương pháp giải mã đối ngẫu vào các thuật toán giải mã LDPC cho phép nâng cao hiệu quả giải mã.

## PHƯƠNG PHÁP GIẢI MÃ KHỐI DỰA TRÊN CÁC MÃ ĐỐI NGẪU

Xuất phát từ tính chất đối ngẫu của mã sửa sai mà bản chất của vấn đề này là với một mã khối tuyến tính, ma trận kiểm tra của mã này đóng vai trò là ma trận sinh của mã khối tuyến tính khác, mặt khác như ta đã biết, tính chất của ma trận kiểm tra và ma trận sinh của mã khối tuyến tính thể hiện như sau:

$$\boldsymbol{G} \times \boldsymbol{H}^T = \boldsymbol{0} \qquad (1)$$

Như vậy, có thể nói các từ mã trong bộ mã đối ngẫu trực giao với các từ mã tương ứng trong bộ mã gốc. Mặt khác mỗi bit kiểm tra đều mang một lượng thông tin về các bit tin, hay nói cách khác mỗi bit trong từ mã đối ngẫu $\boldsymbol{c}_j^{'} = (c_{j,0}^{'}, c_{j,1}^{'}, \ldots, c_{j,n-1}^{'})$ đều mang thông tin về các bit tin trong từ mã gốc $\boldsymbol{c} = (c_0, c_1, \ldots, c_{n-1})$. Trên cơ sở này hình thành nên phương pháp giải mã dựa trên mã đối ngẫu [2], [3]. Phương pháp giải mã này được mô tả như sau: Khi truyền từ mã $\boldsymbol{c}$ qua kênh, dưới tác động của nhiễu và tạp âm ta nhận được từ mã $\boldsymbol{r} = (r_0, r_1, \ldots, r_{n-1})$. Quá trình giải mã ở phía thu với từ mã đầu vào mềm là $\boldsymbol{r}$ ta phải tìm ra các bit $\hat{c}_m = c_m$ (trong đó $c_m$ là từ mã được truyền) với xác suất chính xác cao nhất. Ta ký hiệu $\omega = e^{\frac{2\pi}{p}\sqrt{-1}}$ là biểu diễn phức của nghiệm nguyên thủy $p$; $\delta_{ij} = 1$ nếu $i = j$ và $\delta_{ij} = 0$ với các trường hợp khác; $p_r(x)$ là xác xuất của $x$ và $p_r(x/y)$ là xác xuất có điều kiện của $x$ cho bởi $y$, nếu giá trị $s$ thuộc trường $GF(p)$ ta có $\hat{c}_m = s$ khi $A_m(s)$ đạt cực đại, với

* *Tel: 0912 998396, Email: natuan@ictu.edu.vn*

$$A_m(s)=\sum_{t=0}^{p-1}\omega^{-st}\sum_{j=1}^{p^{n-k}}\left[\prod_{l=0}^{n-1}\sum_{i=0}^{p-1}\omega^{i(c_{jl}^{'}+t\delta_{ml})}\Pr(r_l\mid i)\right] \quad (2)$$

Điều này đã được chứng minh trong [2], kết quả chứng minh khẳng định đối với mã nhị phân ($p=2$), điều kiện quyết định cứng (ở lần lặp cuối cùng) đối với bit $\hat{c}_m$ là $\hat{c}_m=0$ khi:

$$\sum_{j=1}^{2^{n-k}}\prod_{l=0}^{n-1}\left(\frac{1-\phi_l}{1+\phi_l}\right)^{c_{jl}^{'}\oplus\delta_{ml}}>0 \quad (3)$$

và $\hat{c}_m=1$ nếu (3) xảy ra theo chiều ngược lại, ở đây $\phi_l=\dfrac{\mathrm{P_r}(r_l\mid C_l=0)}{\mathrm{P_r}(r_l\mid C_l=1)}$.

Để làm rõ nội dung chứng minh trên ta xét một ví dụ cụ thể với mã Hamming (7, 4) với các bit mã nhận được ký hiệu là $\mathbf{r}=(r_0,r_1,\ldots,r_6)$, theo (3) điều kiện quyết định bit mã $\hat{c}_0$ là:

$$\hat{c}_0=0 \quad khi \quad \sum_{j=1}^{8}\prod_{l=0}^{6}\left(\frac{1-\phi_l}{1+\phi_l}\right)^{c_{jl}^{'}\oplus\delta_{0l}}>0 \quad (4)$$

Ta có ma trận kiểm tra của mã trên, cũng là ma trận sinh của mã đối ngẫu là:

$$\boldsymbol{H}=\begin{bmatrix}1&1&1&0&1&0&0\\0&1&1&1&0&1&0\\0&0&1&1&1&0&1\end{bmatrix}\begin{matrix}(a)\\(b)\\(c)\end{matrix}$$

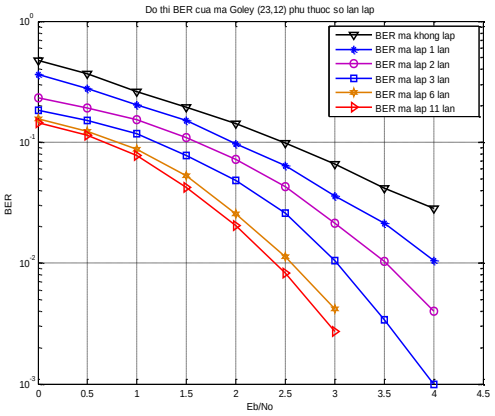
Như vậy các từ mã của bộ mã đối ngẫu (ở đây coi từ mã gồm tất cả các phần tử "0" là một từ mã trong bộ mã) là:

$$\mathbf{C}^{'}=\begin{array}{ccccccc}c_0&c_1&c_2&c_3&c_4&c_5&c_6\\0&0&0&0&0&0&0\\1&1&1&0&1&0&0&(a)\\0&1&1&1&0&1&0&(b)\\1&0&0&1&1&1&0&(a\oplus b)\\0&0&1&1&1&0&1&(c)\\1&1&0&1&0&0&1&(a\oplus c)\\0&1&0&0&1&1&1&(b\oplus c)\\1&0&1&0&0&1&1&(a\oplus b\oplus c)\end{array} \quad (5)$$

Đặt $\rho_\ell=(1-\phi_\ell)/(1+\phi_\ell)$ điều kiện quyết định đối với bít $\hat{c}_0$ là:

$$\hat{c}_0=0\ khi\ \rho_0+\rho_1\rho_2\rho_4+\rho_0\rho_1\rho_2\rho_3\rho_5+\\+\rho_3\rho_4\rho_5+\rho_0\rho_2\rho_3\rho_4\rho_6+\rho_1\rho_3\rho_6+\\+\rho_0\rho_1\rho_4\rho_5\rho_6+\rho_2\rho_5\rho_6>0. \quad (6)$$

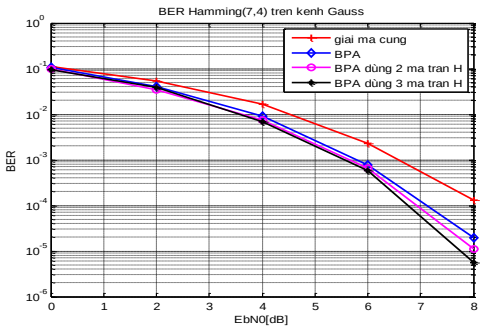
$\hat{c}_0=1$ khi (6) xảy ra theo chiều ngược lại.




**Hình 1.** *Sự phụ thuộc của chất lượng mã Golay (23, 12) vào số lần lặp*

Trong quá trình giải mã lặp, nếu ta tăng số lần lặp hoặc tăng số lượng từ mã đối ngẫu tham gia vào quá trình giải mã thì chất lượng mã sẽ được cải thiện đáng kể, điều này được minh chứng bởi kết quả đánh giá chất lượng của mã Golay (23, 12) trên Hình 1 [3].

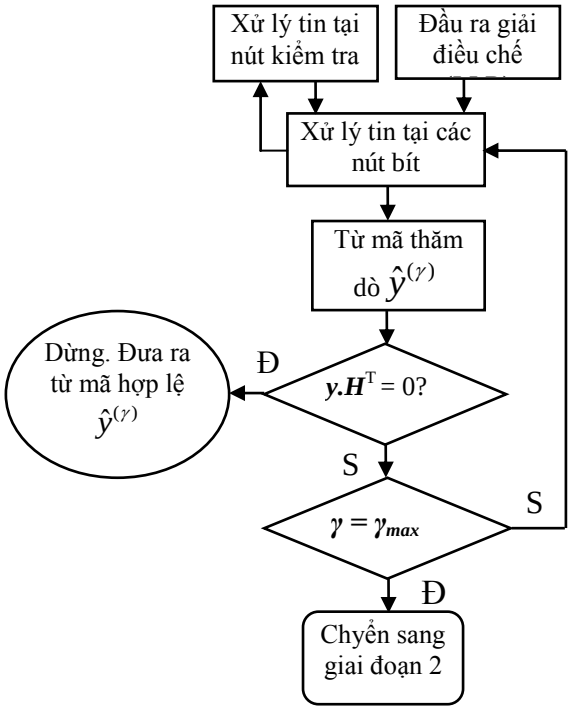
Mặt khác, đối với một mã khối tuyến tính, ma trận sinh được tạo thành từ các từ mã độc lập tuyến tính với nhau, như vậy với các từ mã của bộ mã đối ngẫu như trên sẽ có $c_{2^{n-k}}^{n-k}$ ma trận sinh tương đương nhau (tương ứng với số ma trận kiểm tra tương đương của mã gốc) được hình thành. Trong quá trình giải mã lặp thay vì sử dụng các từ mã đối ngẫu, ta sử dụng các ma trận kiểm tra tương đương này cũng cho chất lượng giải mã cải thiện đáng kể. Điều này được minh họa qua kết quả đánh giá chất lượng của mã Hamming (7, 4) trình bày trên Hình 2.




**Hình 2.** *Sự phụ thuộc của chất lượng mã Hamming (7, 4) vào số lượng ma trận kiểm tra trương đương*

ỨNG DỤNG GIẢI MÃ LDPC (LOW DENSITY PARITY CHECK) BẰNG THUẬT TOÁN BPA-EH VỚI MA TRẬN KIỂM TRA TƯƠNG ĐƯƠNG $H_e$

Ở giai đoạn 1, thuật toán BPA truyền thống (Belief Propagation Algorithm) được giải với số lần lặp cực đại là $\gamma_{max}$. Nếu kiểm tra thấy $\boldsymbol{c*H^T} = 0$ thì ta dừng và đưa ra từ mã. Nếu sau số lần lặp cực đại $\gamma_{max}$ mà $\boldsymbol{c*H^T} = 0$ không thỏa mãn ta chuyển sang giai đoạn 2 giải mã lại với các ma trận kiểm tra tương đương. Lưu đồ giải mã của thuật toán BPA-EH [4] giai đoạn 1 được trình bày trên hình 3.

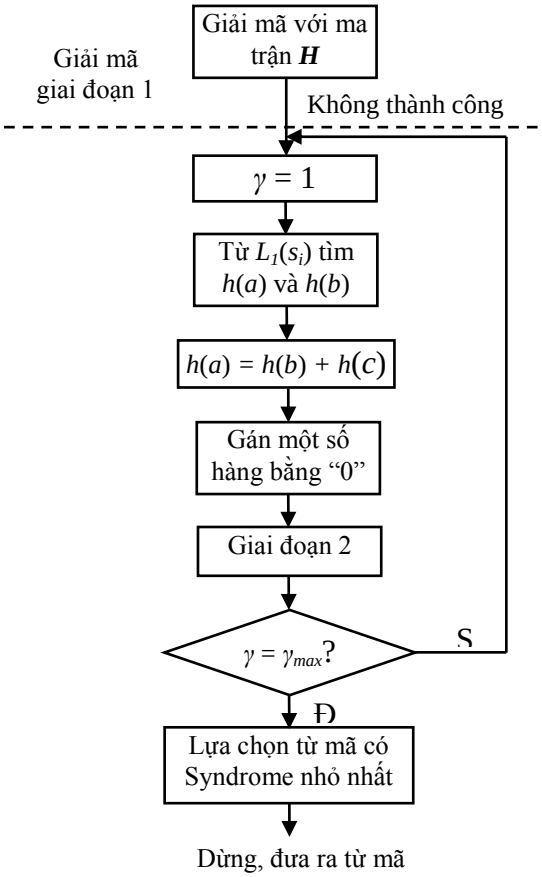



**Hình 3.** *Lưu đồ thuật toán BPA-EH giai đoạn 1*

Giai đoạn 2: Lưu đồ thuật toán của quá trình giải mã này được trình bày trên Hình 4.

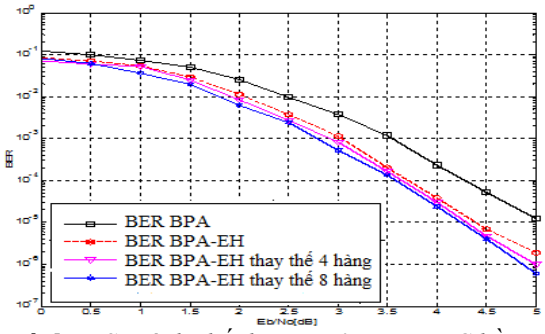
Từ giai đoạn 1, ta thu được giá trị $L(s_i)$, từ giá trị này ta tìm được hàng kém tin cậy $h(a)$, và hàng có độ tin cậy lớn nhất $h(b)$ [4], hàng $h(c)$ là các hàng còn lại khác hàng $h(a)$ và $h(b)$. Sau đó thực hiện thay thế hàng kém tin cậy $h(a) = h(b) + h(c)$. Ngoài việc thay thế hàng $h(a)$ ta còn thực hiện thay thế một số hàng ngoài 2 hàng $h(a)$ và $h(b)$ bằng các hàng toàn các phần tử "0", ở đây ta chọn các hàng có độ tin cậy kém hơn để thay thế.

Sau khi thực hiện thay thế một số hàng bằng véc tơ "0" ta nhận được ma trận kiểm tra tương đương $\boldsymbol{H_e}$ và thực hiện giải mã tương tự như giai đoạn 1. Như vậy với mỗi ma trận tương đương $\boldsymbol{H_e}$ ta sẽ nhận được 1 từ mã tương ứng, ở khâu quyết định cuối cùng sẽ chọn ra từ mã đầu ra là từ mã ứng với giá trị syndrome nhỏ nhất.



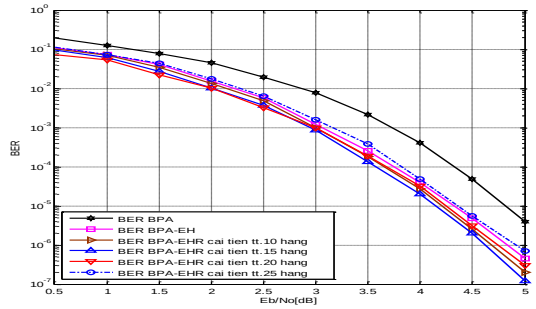

**Hình 4.** *Lưu đồ thuật toán BPA-EH cải tiến [5] giai đoạn 2*

Kết quả mô phỏng cho thấy, với bộ mã $\mathbf{C_1}$ sử dụng ma trận $\boldsymbol{H}_{48x96}$, khi thực hiện thuật toán giải mã BPA-EH cải tiến (thực hiện thay thế một số hàng của ma trận $\boldsymbol{H}_e$ bằng véc tơ "0") và BPA-EH thì chất lượng giải mã tương đương nhau thậm chí thuật toán giải mã BPA-EH cải tiến còn tốt hơn thuật toán giải mã BPA-EH đơn thuần khoảng 0,1 dB ở tỷ lệ lỗi bít $P_e = 10^{-4}$ . Thuật toán giải mã BPA-EH cải tiến mang lại độ lợi mã hóa khoảng 0.8 dB ở tỷ lệ lỗi bít $P_e = 10^{-4}$ so với thuật toán giải mã BPA truyền thống.




**Hình 5.** *So sánh chất lượng giải mã LDPC bằng thuật toán BPA, BPA-EH, BPA-EH cải tiến với ma trận $\boldsymbol{H}_{48x96}$, trên kênh AWGN*

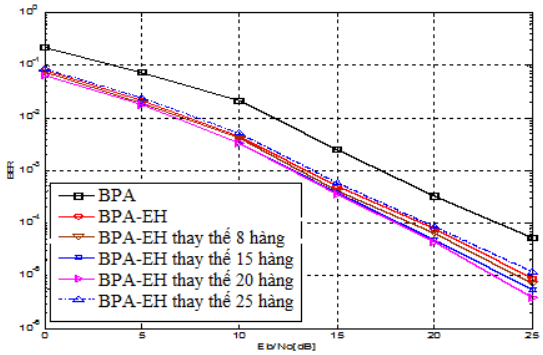
Kết quả giải mã đối với bộ mã $\mathbf{C_2}$ sử dụng ma trận $\boldsymbol{H}_{60x120}$ trên Hình 6 cũng cho kết quả tương tự như với bộ mã $\mathbf{C_1}$. Chất lượng giải mã khi sử dụng thuật toán giải mã BPA-EH cải tiến tương đương với thuật toán giải mã BPA-EH, thậm chí còn tốt hơn thuật toán giải mã BPA-EH khoảng 0,1 dB (ở $P_e = 10^{-4}$), nếu sử dụng thuật toán BPA-EH cần tỷ số $E_b/N_0$ = 3,8 dB, còn sử dụng BPA-EH cải tiến cần $E_b/N_0$ = 3,7 dB, điều đáng nói ở đây là thời gian giải mã của thuật toán này được cải thiện đáng kể.




**Hình 6.** *So sánh chất lượng giải mã LDPC bằng thuật toán BPA, BPA-EH, BPA-EH cải tiến với ma trận $\boldsymbol{H}_{60x120}$ trên kênh AWGN*

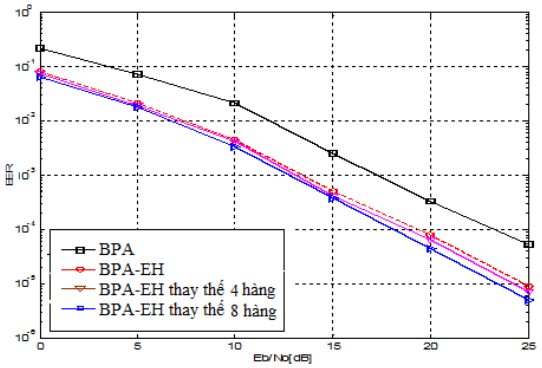
Đối với Hình 6 cho thấy, với bộ mã $\mathbf{C_2}$ sử dụng ma trận $\boldsymbol{H}_{120x240}$, khi thực hiện thuật toán giải mã BPA-EH cải tiến (thực hiện thay thế hết các chu kỳ "4" từ ma trận $\boldsymbol{H}_e$ của BPA-EH) và BPA-EH thì hiệu quả giải mã gần như nhau nhưng có lợi hơn về thời gian giải mã. Thuật toán giải mã BPA-EH cải tiến mang lại độ lợi mã hóa khoảng 0,8 dB ở tỷ lệ lỗi bít $P_e = 10^{-4}$ so với BPA truyền thống.

Trên Hình 7 so sánh chất lượng giải mã LDPC giữa các thuật toán BPA, BPA-EH và BPA-EH cải tiến. Từ đồ thị có thể thấy đối với một bộ mã LDPC xác định thì thuật toán BPA-EH cải tiến cho độ lợi tương đương, thậm chí tốt hơn thuật toán BPA-EH.




**Hình 7.** *So sánh chất lượng giải mã LDPC bằng thuật toán BPA, BPA-EH, BPA-EH cải tiến với ma trận $\boldsymbol{H}_{60x120}$, trên kênh pha-đinh*

Đánh giá chất lượng thuật toán BPA-EH, BPA-EH cải tiến trên kênh pha-đinh: Thực hiện mô phỏng thuật toán BPA-EH, BPA-EH cải tiến trên kênh pha-đinh Rayleigh, kết quả được chỉ ra trên Hình 8.




**Hình 8.** *So sánh chất lượng thuật toán BPA, BPA-EH, BPA-EH cải tiến với ma trận $\boldsymbol{H}_{60x120}$ trên kênh pha-đinh Rayleigh*

## KẾT LUẬN

Trong việc giải mã khối tuyến tính có thể áp dụng kỹ thuật giải mã đối ngẫu để tạo ra các ma trận kiểm tra tương đương trong quá trình giải mã lặp nhằm nâng cao hiệu quả sửa lỗi tại đầu thu. Các kỹ thuật này được thử nghiệm trên mã Haming và mã LDPC cho kết quả tốt.

Đối với thuật toán BPA-EH áp dụng với mã LDPC, việc sử dụng các ma trận kiểm tra tương đương $\boldsymbol{H_e}$ dựa trên nguyên tắc giải mã đối ngẫu cho phép nâng cao hiệu quả sửa lỗi mặc dù phải chấp nhận số phép tính nhiều hơn và thời gian giải mã dài hơn.

Đối với thuật toán BPA-EH cải tiến, bản thân việc thay thế các hàng có độ tin cậy kém trong ma trận $\boldsymbol{H}$ làm thay đổi trạng thái của tổ hợp các vị trí có độ tin cậy kém trong ma trận $\boldsymbol{H}$ ban đầu, từ đó làm tăng thêm thông tin sau các lần lặp dẫn đến tăng khả năng sửa lỗi. Việc thay thế một số hàng của ma trận kiểm tra tương đương $\boldsymbol{H_e}$ bằng véc tơ "0" cũng giúp làm giảm số phép tính và rút ngắn thời gian giải mã.

## TÀI LIỆU THAM KHẢO

1. R. Gallager (Jan 1962), "Low density parity check codes," IRE Trans. Information Theory, IT-8, pp. 21-28.

2. Carlos R.P. Hartman and Luther D. Rudolpho (1975),"An Optimum Symbol-by Symbol decoding rule for linear codes", Electrical Engineering and Computer Science Technical Reports, Syracuse University.

3. H. Greenbeger (1978), "An Iterative Algorithm for Decoding Block Codes Transmited Over a Memoryless Channel", Communications Systems Resech Section. DSN Progress Report 42-47.

4. Nguyen Tung Hung (2013), "A new decoding algorithm based on equivalent parity check matrix for LDPC codes", REV Journal on Electronics and Communications, Vol.3, No. 1-2, pp 73-76 .

5. Nguyễn Anh Tuấn, Phạm Xuân Nghĩa (8/2015), "Nghiên cứu giải mã LDPC sử dụng thuật toán BPA-EH cải tiến cho kênh pha-đinh", Tạp chí Khoa học và Kỹ thuật, Học viện Kỹ thuật Quân sự, tr.28-36.

## SUMMARY

## APPLICATIONS OF DECODING DUAL CODES TECHNICQUE IN LDPC DECODING

**Nguyen Anh Tuan[1*], Pham Van Ngoc[1], Pham Xuan Nghia[2]**

*[1]Univerity of Information and Communication Technology – TNU*

*[2]Le Quy Don Technical University*

This paper presents the basic of the decoding method using the dual decoding techniques, applications with the code Haming, code LDPC ... This approach allows the use of iterative decoding techniques combined with the use of the equyvalent matrix $\boldsymbol{H}$ and decision-making techniques based on the weight of the syndrome when decoding. Simulation results performed on a Gaussian channel model and fading channel using the BPA-EH algorithm (Belief Propagation Algorithm Based on Equivalent Parity Check Matrix H) result in significant improvements in decoding behavior and Shorten time decoding compared to traditional BPA algorithms.

**Keywords:** *Dual codes, LDPC code, Equivalent parity check matrix, BPA decoding, Gaussian hannels, fading channels*

***Ngày nhận bài: 04/01/2018; Ngày phản biện: 11/02/2018; Ngày duyệt đăng: 05/3/2018***

[*] *Tel: 0912 998396, Email: natuan@ictu.edu.vn*