MÃ MẠNG TRÊN MỘT SỐ CẤU TRÚC ĐẠI SỐ

Phạm Long Âu[1], Nguyễn Bình[2],
Ngô Đức Thiện[2,*], Nguyễn Lê Cường[3]

Tóm tắt: *Mã mạng (network coding) là một kỹ thuật mạng, trong đó, dữ liệu truyền được mã hoá và giải mã để tăng lưu lượng mạng, giảm độ trễ và làm cho mạng ổn định hơn. Kỹ thuật mã mạng sử dụng phép toán học nào đó tác động lên dữ liệu với mục đích làm giảm thiểu số phiên truyền dẫn giữa nút nguồn và nút đích, tuy nhiên, nó sẽ đòi hỏi các nút trung gian và các nút đầu cuối phải xử lý nhiều hơn. Bài báo này trình bày ý tưởng xây dựng mã mạng dựng dựa trên một số cấu trúc đại số thông dụng như: các nhóm cộng trên đường cong elliptic; trên vành số* $\mathbb{Z}_p$; *vành đa thức, các nhóm nhân trên trường* $GF(p)$*; trường đa thức.*

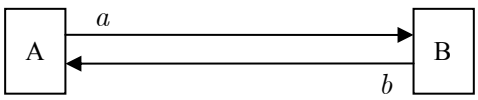
Từ khóa: Mã mạng, Vô tuyến hợp tác, Vành số, Vành đa thức, Trường hữu hạn, Đường cong elliptic.

1. MỞ ĐẦU

Năm 2000 một nhánh nghiên cứu rất thú vị được ra đời và càng lúc càng thu hút nhiều nhà nghiên cứu từ lý thuyết thông tin mã hóa đến mạng máy tính. Hướng nghiên cứu mới này là mã mạng (network coding). Khởi đầu từ bài báo của các tác giả R. Ahlswede, N. Cai, S. Y. Li & R. Young, "*Network information flow*" (IEEE. Trans on vol IT- 46, No. 4, pp 1204 - 1216, Jul 2000), cho đến nay mã mạng đã được nghiên cứu ứng dụng trong nhiều lĩnh vực, đặc biệt trong truyền thông vô tuyến, truyền thông multicast [3], truyền thông unicast [4], truyền thông broadcast [5], mạng phân phối nội dung (CDN) [6], mạng cảm biến không dây [7], hệ thống truyền video trực tuyến qua mạng ngang hàng P2P [9], hay hệ thống LTE [8],...

Mã mạng là một kỹ thuật toán học được sử dụng để nâng cao chất lượng, hiệu suất và khả năng mở rộng của mạng, cũng như khả năng chống lại các cuộc tấn công và nghe trộm. Thay vì chỉ đơn giản chuyển tiếp các gói thông tin nhận được như cách truyền thống, trong kỹ thuật mã mạng các nút của mạng sẽ kết hợp nhiều gói tin nhận được với nhau và tạo ra các gói mới để truyền. Kỹ thuật này đem lại một số lợi ích như tăng thông lượng, cải thiện độ tin cậy và tăng độ ổn định của mạng [10], [11].

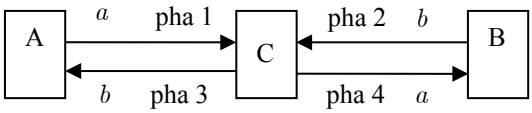
Xét mô hình truyền tin giữa hai nút mạng là A và B trong hình 1. Nếu A và B cách xa nhau, việc truyền thông tin tin cậy rất khó thực hiện được, kể cả khi ta dùng mã kênh.



Hình 1. *Mô hình truyền tin giữa 2 nút.*

Trên thực tế, ta có thể đảm bảo việc truyền tin tin cậy giữa A và B người ta có thể dùng hệ thống vô tuyến hợp tác (cooperative radio - CR) [1], [2]. Hệ thống này cho phép cung cấp tốc độ truyền dẫn cao hơn trên hệ thống truy nhập vô tuyến cũng như khả năng tạo vùng phủ rộng hơn.

Hệ thống CR sử dụng thêm một nút chuyển tiếp C (nằm giữa A và B), với quá trình truyền tin trải qua 4 pha như mô tả trong hình 2.



Hình 2. *Mô hình truyền tin vô tuyến hợp tác.*

Lưu ý: Các thông tin a (của A) cần truyền cho B và b (của B) cần truyền cho A được xem là các xâu bit (vector nhị phân n bit nằm trong không gian tuyến tính n chiều V_n).

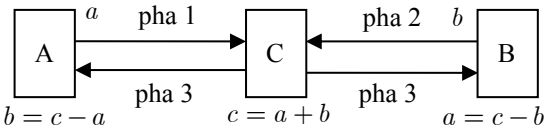
Để tăng hiệu quả của hệ thống CR này mà vẫn đảm bảo độ tin cậy cần thiết, vào năm 2000 Ahlswede [10] cùng một số nhà khoa học khác đã đưa ra ý tưởng dùng mã mạng như mô tả trong hình 3.

Với mô hình này, quá trình truyền tin giữa A và B chỉ còn lại 3 pha sau (thay vì 4 pha như thông thường).

- pha 1: A phát bản tin a cho C.
- pha 2: B phát bản tin b cho C.
- pha 3: C nhận được a, b và tạo ra $c = a + b$, sau đó, C phát quảng bá c cho A và B.

+ A nhận được c và tạo ra bản tin cần nhận là $b = c - a$.

+ B nhận được c và tạo ra bản tin cần nhận là $a = c - b$.



Hình 3. *Mô hình truyền tin sử dụng mã mạng.*

Nhận xét:

Cách thức liên lạc này vẫn đảm bảo độ tin cậy cần thiết những hiệu quả cao hơn nhờ giảm được một pha liên lạc.

C tạo ra thông tin quảng bá $c = a + b$ (sử dụng phần che giấu dữ liệu dùng mặt nạ cộng nhưng không thực hiện với mục đích bảo mật).

2. MÃ MẠNG TRÊN MỘT SỐ CẤU TRÚC ĐẠI SỐ

Dựa trên mô hình mã mạng như trong hình 3, trong phần này, chúng tôi đề xuất ý tưởng xây dựng mã mạng dựa trên một số cấu trúc đại số thông thường.

2.1. Mã mạng trên đường cong elliptic

Đường cong elliptic dạng Weierstrass trên $\mathbb{Z}_p$ với p nguyên tố được mô tả bởi phương trình sau [12]:

$$y^2 = x^3 + ax + b \bmod p \tag{1}$$

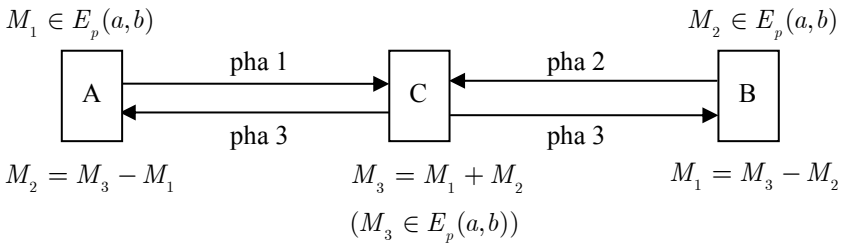
Với $a, b \in \mathbb{Z}_p^*$ (nhóm nhân trên $\mathbb{Z}_p$).

Chú ý: a và b ở đây là hệ số của đường cong elliptic trong biểu thức (1).

Điều kiện tồn tại nhóm cộng $E_p(a,b)$ trên đường cong elliptic này là khi và chỉ khi thỏa mãn điều kiện của định thức Δ như sau [12].

$$\Delta = (4a^3 + 27b^2) \bmod p \neq 0 \quad (2)$$

Nếu ta coi thông tin cần truyền là các điểm của nhóm cộng $E_p(a,b)$ trên đường cong elliptic, thì ý tưởng thực hiện mã mạng ta có thể xây dựng một hệ thống CR như sau:



Hình 4. *Mã mạng dựa trên đường cong elliptic.*

Nhận xét: Vì $E_p(a,b)$ là một nhóm cộng các điểm trên đường cong elliptic, nên với các điểm thông tin M_1 và M_2, hai bên liên lạc A và B luôn có thể xác định được các điểm đối: $-M_1; -M_2 \in E_p(a,b)$ và như vậy chúng luôn có thể tính được các thông tin cần nhận.

* *Ví dụ 1*: Chọn đường cong elliptic: $y^2 = x^3 + x + 1 \bmod 17$

Ta có: $a = 1$; $b = 1$; $p = 17$. Xét điều kiện tồn tại:

$$\Delta = (4a^3 + 27b^2) \bmod p = (4.1^3 + 27.1^2) \bmod 17 = 14 \neq 0$$

thỏa mãn điều kiện (2).

Nhóm cộng $E_{17}(1,1)$ xây dựng từ phần tử sinh $P(x,y) = P(0,1)$ như sau [12]:

$$\begin{aligned} E_{17}(1,1) = \{&P(0,1), 2P(13,1), 3P(4,16), 4P(9,12), 5P(16,4), 6P(10,12), 7P(6,6), \\ &8P(15,12), 9P(11,0), 10P(15,5), 11P(6,11), 12P(10,5), 13P(16,13), \\ &14P(9,5), 15P(4,1), 16P(13,16), 17P(0,16), 18P(0)\} \end{aligned}$$

Thông tin cần truyền giữa A và B là các điểm trên đường cong elliptic. Quá trình truyền tin giữa A và B sử dụng CR thực hiện như sau.

- pha 1: A phát bản tin $M_1 = 3P(4,16)$ cho C.

- pha 2: B phát bản tin $M_2 = 9P(11,0)$ cho C.

- pha 3: C nhận được M_1, M_2 và tạo ra: $M_3 = M_1 + M_2 = 12P(10,5)$, sau đó C phát quảng bá M_3 cho A và B.

+ A nhận được M_3 và tạo ra bản tin cần nhận là:

$$M_2 = M_3 - M_1 = 12P - 3P = 9P(11,0)$$

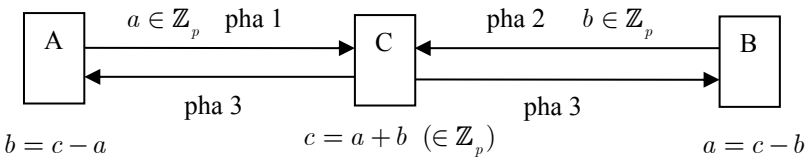
+ B nhận được M_3 và tạo ra bản tin cần nhận là:

$$M_1 = M_3 - M_2 = 12P - 9P = 3P(4,16)$$

Phép cộng các điểm trên đường cong elliptic được mô tả trong [12].

2.2. Mã mạng trên $\mathbb{Z}_p$

Tương tự, nếu ta coi thông tin cần truyền giữa A và B là các số nguyên nằm trong $\mathbb{Z}_p$ thì ta có thể xây dựng được CR với ý tưởng mã mạng như sau:



Hình 5. *Mã mạng dựa trên* $\mathbb{Z}_p$.

Nhận xét: Vì $\mathbb{Z}_p$ là nhóm cộng (theo modulo p) của các số nguyên a, b nên A và B hoàn toàn xác định được $-a$ và $-b$, và như vậy, A và B luôn có thể tính được thông tin cần nhận [13], [14].

* *Ví dụ 2*: Xét $p = 31 \to \mathbb{Z}_{31} = \{0,1,2,...,30\}$

- pha 1: A phát bản tin $a = 13$ cho C.
- pha 2: B phát bản tin $b = 25$ cho C.
- pha 3: C nhận được a, b và tạo ra: $c = (a+b) \bmod 31 = (13+25) \bmod 31 = 7$, sau đó, C phát quảng bá c cho A và B.

+ A nhận được $c = 7$ và tạo ra bản tin cần nhận là:

$$b = (c-a) \bmod p = (7-13) \bmod 31 = (7+18) \bmod 31 = 25$$

Chú ý: $-13 \bmod 31 \equiv 18 \bmod 31$

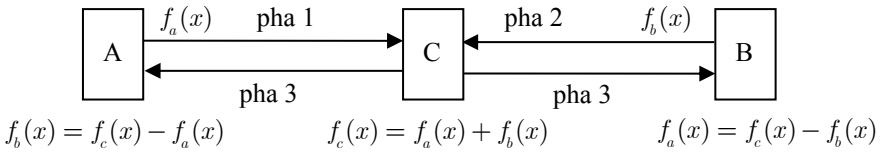
+ B nhận được $c = 7$ và tạo ra bản tin cần nhận là:

$$a = (c-b) \bmod p = (7-25) \bmod 31 = (7+6) \bmod 31 = 13$$

Chú ý: $-25 \bmod 31 \equiv 6 \bmod 31$

2.3. Mã mạng trên vành đa thức $\mathbb{Z}_2[x] / x^n + 1$

Nếu ta coi thông tin cần truyền giữa A và B là các đa thức $f_a(x)$ và $f_b(x)$ ($f_a(x), f_b(x) \in \mathbb{Z}_2[x] / x^n + 1$), khi đó ta có thể tạo được CR sử dụng mã mạng như hình 6 dưới đây.



Hình 6. *Mã mạng dựa trên* $\mathbb{Z}_2[x] / x^n + 1$.

Nhận xét: Vì các đa thức $f_a(x)$ và $f_b(x)$ là các phần tử trong nhóm cộng các đa thức (theo modulo x^n+1) nên luôn tồn tại các đa thức $-f_a(x)$ và $-f_b(x)$ [13] và như vậy A và B luôn có thể xác định được thông tin cần nhận của chúng.

* *Ví dụ 3*: Chọn $n=5$ xét vành đa thức $\mathbb{Z}_2[x]/x^5+1$.

- pha 1: A phát bản tin $f_a(x)=1+x+x^3$ cho C.

- pha 2: B phát bản tin $f_b(x)=1+x^3+x^4$ cho C.

- pha 3: C nhận được $f_a(x), f_b(x)$ và tạo ra

$$f_c(x)=f_a(x)+f_b(x)=1+x+x^3+1+x^3+x^4=x+x^4$$

sau đó, C phát quảng bá $f_c(x)=x+x^4$ cho A và B.

+ A nhận được $f_c(x)$ và tạo ra bản tin cần nhận là

$$f_b(x)=f_c(x)-f_a(x)=x+x^4-(1+x+x^3)=1+x^3+x^4$$

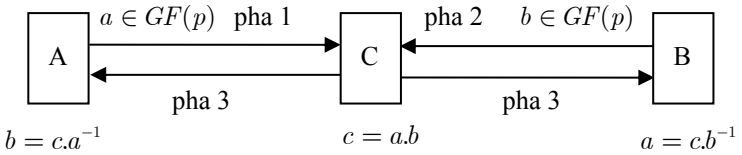
+ B nhận được $f_c(x)$ và tạo ra bản tin cần nhận là:

$$f_a(x)=f_c(x)-f_b(x)=x+x^4-(1+x^3+x^4)=1+x+x^3$$

2.4. Mã mạng sử dụng nhóm nhân

2.4.1. Mã mạng trên GF(p)

Với p là số nguyên tố, các thông tin là $a,b\in GF(p)$. Khi đó, ta có thể dùng mô hình CR với mã mạng như sau:



Hình 7. *Mã mạng dựa trên GF(p).*

Nhận xét: Vì $a,b\in GF(p)$ và $\mathbb{Z}_p^*=GF(p)\setminus\{0\}$ là một nhóm nhân cyclic cấp $p-1$, nên luôn tồn tại các phần tử nghịch đảo a^{-1} và b^{-1}. Như vậy, A và B luôn có thể tính được thông tin cần nhận [13], [14].

* *Ví dụ 4*: Xét $p=17\rightarrow\mathbb{Z}_{17}^*=\{1,2,3,...,16\}$

- pha 1: A phát bản tin $a=6$ cho C.
- pha 2: B phát bản tin $b=7$ cho C.
- pha 3: C nhận được a,b và tạo ra: $c=a.b=6.7\bmod 17=8$, sau đó C phát quảng bá c cho A và B.

+ A nhận được $c=8$ và tạo ra bản tin cần nhận là:

$$b=c.a^{-1}\bmod p=8.3\bmod 17=7\quad(a=6\rightarrow\ a^{-1}=3)$$

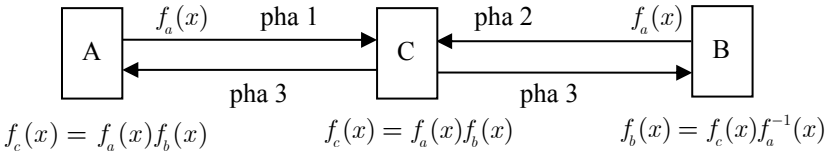
+ B nhận được $c=8$ và tạo ra bản tin cần nhận là:

$$a = c.b^{-1} \bmod p = 8.5 \bmod 17 = 6 \quad (b = 7 \rightarrow b^{-1} = 5)$$

Chú ý: các phép toán trên $GF(p)$ thực hiện theo modulo của p.

2.4.2. Mã mạng trên trường đa thức $\mathbb{Z}_2[x] / g(x)$

Giả sử $g(x)$ là một đa thức nguyên thủy bậc m trong phân tích của nhị thức $x^n + 1$ và khi đó $\mathbb{Z}_2[x] / g(x)$ là một trường các đa thức. Trong trường hợp này, ta coi thông tin cần truyền từ A tới B là đa thức $f_a(x)$ và từ B đến A là $f_b(x)$ với $\deg f_a(x) \le m-1$; $\deg f_b(x) \le m-1$, vì $f_a(x), f_b(x) \in \mathbb{Z}_2[x] / g(x)$ nên luôn tồn tại và tính được $f_a^{-1}(x)$ và $f_b^{-1}(x)$ (có thể tính theo thuật toán Euclide mở rộng). Vì vậy, ta có thể xây dựng CR với mã mạng như sau:



Hình 8. *Mã mạng dựa trên trường đa thức.*

Nhận xét: C tạo ra thông tin quảng bá $f_c(x) = f_a(x)f_b(x)$ (sử dụng phương pháp che giấu dữ liệu dùng mặt nạ nhân nhưng không dùng để bảo mật).

* *Ví dụ 5*: Chọn $n = 5$ ta có $x^5 + 1$ có phân tích như sau:

$x^5 + 1 = (1 + x)(1 + x + x^2 + x^3 + x^4) = g_1(x).g_2(x)$

Xét trường: $\mathbb{Z}_2[x] / g_2(x) \leftrightarrow \mathbb{Z}_2[x] / (1 + x + x^2 + x^3 + x^4)$

Với $m = \deg g_2(x) = 4$

Quá trình truyền tin:

- pha 1: A phát bản tin $f_a(x) = 1 + x + x^2$ cho C.
- pha 2: B phát bản tin $f_b(x) = 1 + x^2$ cho C.
- pha 3: C nhận được $f_a(x), f_b(x)$ và tạo ra $f_c(x)$

$$f_c(x) = f_a(x).f_b(x) \bmod g_2(x) = (1 + x + x^2)(1 + x^2) = x^2$$

sau đó, C phát quảng bá $f_c(x) = x^2$ cho A và B.

+ A nhận được $f_c(x)$ và tạo ra bản tin cần nhận là:

$$f_b(x) = f_c(x)f_a^{-1}(x) \bmod g_2(x) = x^2(1 + x^3) \bmod g_2(x) = 1 + x^2$$

+ B nhận được $f_c(x)$ và tạo ra bản tin cần nhận là:

$$f_a(x) = f_c(x)f_b^{-1}(x) \bmod g_2(x) = x^2(x + x^2) \bmod g_2(x) = 1 + x + x^2$$

Chú ý:

$+ f_a(x) = 1 + x + x^2 \leftrightarrow f_a^{-1}(x) = 1 + x^3$

+ $f_b(x) = 1 + x^2 \leftrightarrow f_b^{-1}(x) = x + x^2$

+ Các phép tính khi lấy modulo theo $g_2(x) = 1 + x + x^2 + x^3 + x^4$ ta coi: $x^4 = 1 + x + x^2 + x^3$.

3. KẾT LUẬN

Bài báo đưa ra một số ý tưởng xây dựng mã mạng trên năm cấu trúc đại số: trên đường cong elliptic; vành số $\mathbb{Z}_p$; vành đa thức; trường $GF(p)$ và trên trường đa thức.

Ngoài các cấu trúc trên, có thể mở rộng ý tưởng mã mạng trên cấu trúc đại số khác như vành ma trận…

Các nội dung trong bài báo mới chỉ là các đề xuất sử dụng một số cấu trúc đại số trong mã mạng hay vô tuyến hợp tác, hiệu quả của các vô tuyến hợp tác này như thế nào thì cần phải có các đánh giá và khảo sát trên từng cấu trúc đại số cụ thể.

TÀI LIỆU THAM KHẢO

[1]. A. Nosratinia, T. Hunter and A. Hedayat, "*Cooperative communication in wireless networks",* Communication Magazine, IEEE, vol. 42, Oct 2004, pp.74 – 80.

[2]. X. Tao, X. Xu, and Q. Cui, "*An overview of cooperative communications",* Communications Magazine, IEEE, vol. 50, June 2012, pp. 65-71.

[3]. T. Ho, M. Medard, R. Koetter, D. Karger, M. Effros, J. Shi, and B. Leong, "*A random linear network coding approach to multicast,"* IEEE Transactions on Information Theory, vol. 52, pp. 4413-4430, Oct, 2006.

[4]. N. Ratnakar, D. Traskov, and R. Koetter, "*Approaches to network coding for multiple unicast,"* in Communications, 2006 International Zurich Seminar on, pp.70-73, Oct 2006.

[5]. X. Wang, W. Guo, Y. Yang, and B. Wang, "*A secure broadcasting scheme with network coding,"* Communications letters, IEEE, vol. 17, pp.1435-1538, July 2013.

[6]. Q. Li, J.-S Lui, and D.-M Chiu, "*On the security and efficiency of content distribution via network coding,"* Dependable and secure computing, IEEE Transactions on, vol. 9, pp. 211-221, March 2012.

[7]. X. Yang, E. Dutkiewicz, Q. Cui, X. Tao, Y. Guo, and X. Huang, "*Compressed network coding for distributed storage in wireless sensor networks,"* in Communications and Information Technologies (ISCIT), 2012 International Symposium on, pp. 816-821, Oct 2012.

[8]. Cuong Cao Luu, Dung Van Ta, Quy Trong Nguyen, Sy Nguyen Quy, Hung Viet Nguyen, (Oct 15-17, 2014), "*Network coding for LTE-based cooperative communications",* the 2014 International Conference on Advanced Technologies for Communications (ATC), Hanoi, Vietnam.

[9]. F. de Asis Lopez-Fuentes and C. Cabrera Medina, "*Network coding for streaming video over p2p networks",* in Multimedia (ISM), 2013 IEEE International Symposium on, pp. 329-332, Dec. 2013.

[10]. R. Ahlswede, N. Cai, S. Y. Li & R. Young, "*Network information flow*". Information theory. IEEE. Trans on vol IT- 46, No. 4, pp 1204 - 1216, jul 2000.

[11]. R. W. Yeung and Z. Zhang, "*Distributed source coding for satellite communications*", IEEE Trans. Inform. Theory, vol. IT-45, pp. 1111–1120, 1999.

[12]. Jean-Yves Chouinard - ELG 5373, "*Secure Communications and Data Encryption, School of Information Technology and Engineering*", University of Ottawa, April 2002.

[13]. Rudolf Lidl, Harald Niederreiter, "*Finite Fields*", (Encylopedia of Mathematics and Its Appliaction; Volume 20. Section, Algebra), Addison-Wesley Publishing Company, 1983.

[14]. Nguyễn Chánh Tú, "*Lý thuyết trường và Galois*", Đại học Sư phạm Huế.

ABSTRACT

NETWORK CODING OVER SOME ALGEBRAIC STRUCTURES

Network coding is a networking technique in which transmitted data is encoded and decoded to increase network throughput, reduce delays and make the network more robust. Network coding techniques use some mathematical manipulations on the data to minimize the number of transmission sessions between the source node and the destination node, but this requires more processing at intermediary nodes and terminal nodes. This paper presents some ideals constructing network coding based on some common algebraic structures such as addition groups on elliptic curve; on number ring; on polynomial ring, multiplicative groups on $GF(p)$*; polynomial field.*

Keywords: Network coding, Cooperative radio, Number ring, Polynomial ring, Finite field, Elliptic curve.

Nhận bài ngày 20 tháng 12 năm 2017
Hoàn thiện ngày 08 tháng 3 năm 2018
Chấp nhận đăng ngày 10 tháng 4 năm 2018

Địa chỉ: [1] Cục Kỹ thuật nghiệp vụ II, Tổng cục An ninh, Bộ Công an;
[2] Học viện Công nghệ Bưu chính Viễn thông;
[3] Đại học Điện lực.
[*] Email: thiennd@ptit.edu.vn.