ABOUT ONE METHOD OF IMPLEMENTING NETWORK CODING BASED ON POINTS ADDITIVE OPERATION ON ELLIPTIC CURVE

Phạm Long Âu[+], Ngô Đức Thiện[*]

+ PhD. student, Posts and Telecommunications Institute of Technology
[*] Posts and Telecommunications Institute of Technology

Abstract: Network coding is a network technique in which transmitted data are coded and decoded for the purpose of increasing network traffic, reducing latency and making the network more stable. Network coding technique uses some mathematical manipulations on the data to minimize the number of transmission sessions between the source nodes and the destination nodes, but it will require more computational proces-sing at intermediate nodes and terminal nodes. This article presents an idea for building a network coding model based on additive group of points on elliptic curve.

Keywords: Network coding, cooperative radio, elliptic curve, finite field.

I. INTRODUCTION

From the article by R. Ahlswede, N. Cai, SY Li & R. Young, "Network information flow" [1], so far the network coding has been studied in a wide range of applications, particularly in wireless communications, multicast communications [2], unicast communications [3], broadcast communications [4], distribution networks content (CDN) [5], wireless sensor network [6], LTE system [7], peer-to-peer video streaming system [8], or satellite information [9]…

Network coding is a mathematical technique used to improve the quality, performance of the networks, as well as the ability to resist attacks. Instead of simply forwarding packets received on the traditional way, in the network coding technique the nodes of the network will combine received packets and create new packets for transmission. This technique offers some benefits such as bandwidth expanded, reliability improved and network stability increased [1].

Tác giả liên hệ: Ngô Đức Thiện
Email: thiennd@ptit.edu.vn
Đến tòa soạn: 03/2019, chỉnh sửa: 04/2019, chấp nhận đăng: 05/2019.

Consider the wireless communication between the two nodes A and B of a network in figure 1. If A and B are far away, reliable communication is difficult, even if channel coding is used.

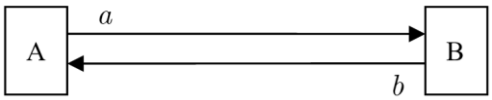

Fig. 1. Communication between two nodes A and B

In fact, to ensure reliable communication between A and B, we can use cooperative radio (CR) system [10], [11]. This system allows for higher transmission rates on radio access systems as well as greater coverage.

The CR system uses a forward node C (located between node A and node B), and operating with four phase transmissions, as described in figure 2.

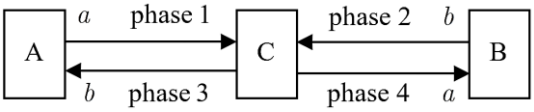

Fig. 2. Cooperative radio communnication model

Note: The message information a and b (of A and B, respectively) are considered to be bit strings (n - bit binary vector in n - dimensional linear space).

In order to increase the efficiency of this CR system and still retain the required reliability, in 2000 Ahlswede [1] and some scientists came up with the idea of using the network coding as depicted in figure 3.

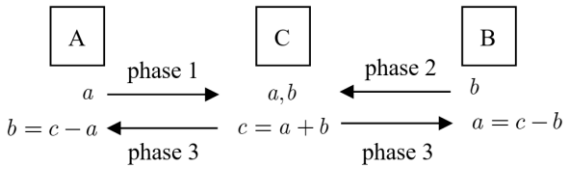

Fig. 3. Network coding communication model

With this model, the communication process between A and B has only three phases (instead of the usual four phases).

- Phase 1: A sends message a to C.

- Phase 2: B sends message b to C.

- Phase 3: C receives a,b and generates $c = a + b$ then C broadcasts c for A and B.

+ A decodes c to get back the message: $b = c - a$.

+ B decodes c to retrieve the message: $a = c - b$.

This technique not only ensures the reliability of communication but is more effective due to the reduction of a connection phase.

II. NETWORK CODING OVER ELLIPTIC CURVE

The elliptic curve (Weierstrass form) over finite fields is represented by following equation [12], [13]:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \quad (1)$$

Where $a,b \in \mathbf{Z}_p$ (restricted to $\bmod p$), p is a prime number.

a and b must satisfy the condition:

$$\mathrm{D} = (4a^3 + 27b^2) \bmod p \neq 0 \quad (2)$$

Now consider the set $E_p(a,b)$ consisting of all pairs of integers (x,y) that satisfy equation (1), together with a point at infinity O. The coefficients a, b and the variables x and y are all elements of $\mathbf{Z}_p$.

Set $E_p(a,b)$ also is an additive group and any point (or element) of $E_p(a,b)$ can be set as $P = (x_p,y_p)$, where x_p,y_p are x,y coordinates of P.

The rules for addition over $E_p(a,b)$ correspond to the algebraic technique described for elliptic curves defined over real numbers.

For all points $A,B \in E_p(a,b)$ we have [12], [13]:

1. $A + \mathrm{O} = A$
2. If $A = (x_a,y_a)$ then $A + (x_a,-y_a) = \mathrm{O}$. The point $(x_a,-y_a)$ is the negative of A, denoted as $-A$ (where $-y_a \bmod p = p - y_a \bmod p$).
3. If $A = (x_a,y_a)$ and $B = (x_b,y_b)$ with $A \neq -B$ then $C = A + B = (x_c,y_c)$ is determined by the following rules:

$$x_c = (l^2 - x_a - x_b) \bmod p \quad (3)$$

$$y_c = [l(x_a - x_c) - y_a] \bmod p \quad (4)$$

where

$$l = \begin{cases} \dfrac{3x_a^2 + a}{2y_a} \bmod p, & \text{if } A = B \\ \dfrac{y_b - y_a}{x_b - x_a} \bmod p, & \text{if } A \neq B \end{cases} \quad (5)$$

Note: a in (5) is coefficient a of equation (1).

4. Multiplication is defined as repeated addition; for example: $4A = A + A + A + A$.

By using additive operation of points in elliptic curve (EC), we can perform a network coding model as Fig. 4.

In Fig. 4, the messages that transmitted between A and B are the points on the EC. Of course, we need to transform those messages to EC points.

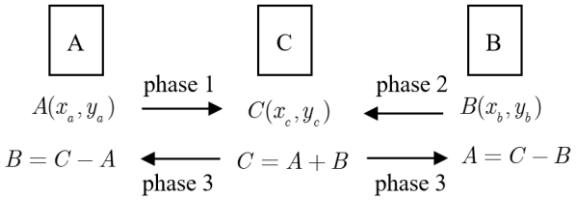

Fig. 4. Network coding model on EC

Suppose node A wants to send point $A = (x_a,y_a)$ to B, and B wants to send point $B = (x_b,y_b)$ to A. The transmission procedure is performed as follows:

Nodes A, B and C select an EC as (1) and a,b satisfy condition (2); and calculate $E_p(a,b)$.

Phase 1: A transmits point $A = (x_a,y_a)$ to C.

Phase 2: B transmits point $B = (x_b,y_b)$ to C.

Phase 3: Node C receives A,B and calculates:

$$C = A + B$$

and then C broadcasts point $C = (x_c,y_c)$ to both A and B.

Node A receives C and computes: $B = C - A$

Node B receives C and computes: $A = C - B$

III. A SMALL EXAMPLE

Consider $E_{13}(1,1)$ on EC:

$$y^2 \bmod 13 = (x^3 + x + 1) \bmod 13 \quad (7)$$

According to (1) we have $a = 1$; $b = 1$; $p = 13$ and:

$$\begin{aligned} \mathrm{D} &= (4.1^3 + 27.1^2) \bmod 13 \\ &= 31 \bmod 13 = 5 \neq 0 \end{aligned} \quad (8)$$

We see that D satisfies condition (2).

All elements of $E_{13}(1,1)$ can be calculated as follows.

Consider a set $Q_{13} = \{1,3,4,9,10,12\}$, this is a set of quadratic residue elements of $\mathbf{Z}_{13}^*$. We can get Q_{13} by doing power of two for all elements of $\mathbf{Z}_{13}^*$.

Table I. Quadratic residue elements of $\mathbf{Z}_{13}^*$

i	1	2	3	4	5	6	7	8	9	10	11	12
i^2	1	4	9	3	12	10	10	12	3	9	4	1

Each element of Q_{13} has two square roots:

$$\sqrt{1} = \{1,12\};\ \sqrt{3} = \{4,9\};\ \sqrt{4} = \{2,11\}$$
$$\sqrt{9} = \{3,10\};\ \sqrt{10} = \{6,7\};\ \sqrt{12} = \{5,8\}$$

Table II. Points value of $E_{13}(1,1)$

x	0	1	2	3	4	5	6	7	8	9	10	11	12
y^2	1	3	11	5	4	1	2	0	1	11	10	4	12
$y^2 \in Q_{13}$?	Y	Y	N	N	Y	Y	N	N	Y	N	Y	Y	Y
y_1	1	4			2	1		0	1		6	2	5
y_2	12	9			11	12		0	12		7	11	8

($Y = yes, N = no;\ \sqrt{y^2} = (y_1, y_2)$)

From table II, we have $E_{13}(1,1)$:

$$E_{13}(1,1) = \{(0,1),(0,12),(1,4),(1,9),(4,2),(4,11),$$
$$(5,1),(5,12),(7,0),(8,1),(8,12),(10,6),$$
$$(10,7),(11,2),(11,11),(12,5),(12,8),O\}$$

Where, $|E_{13}(1,1)| = 18$.

Note:

(a) In the table II, if $x = 7$ then $y = 0$, although $y = 0$ is not a quadratic residue element, but it has one square root, that is $\sqrt{0} = 0$.

(b) The point O has coordinates (¥ ,¥) and it is the point at infinity, which satisfy:

$$P + (-P) = O;\ (O, P \hat{I}\ E_{13}(1,1))$$

The message transmission procedure between node A and node B is performed as following steps:

Suppose: $A = (1,4)$; $B = (8,12)$.

Node C calculates $C = A + B$ (see (3), (4), (5)):

$$l = \frac{y_b - y_a}{x_b - x_a} \bmod p = \frac{12-4}{8-1} \bmod 13$$
$$= 8.7^{-1} \bmod 13 = 3$$

$$x_c = (l^2 - x_a - x_b) \bmod p$$
$$= (3^2 - 1 - 8) \bmod 13 = 0$$

$$y_c = [l(x_a - x_c) - y_a] \bmod p$$
$$= [3(1-0) - 4] \bmod 13$$
$$= -1 \bmod 13 = 12$$

Then C transits $C = (0,12)$ to both nodes A and B.

Note: in the multiplicative group $\mathbf{Z}_{13}^*$:

$$\mathbf{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\} \quad (9)$$

we have 7 pairs of inverse numbers [14]:

$$(1,1),(2,7),(3,9),(4,10),(5,8),(6,11),(12,12) \quad (10)$$

That mean $2 = 7^{-1}$ (of course $7 = 2^{-1}$), because $2.7 \bmod 13 = 1 \bmod 13$; $3 = 9^{-1} (9 = 3^{-1})$, etc.

Node A recovers message: $B = C + [-A]$.

According to the rules for addition over $E_p(a,b)$:

if $A = (1,4)$ then $-A = (1,-4)$ or $-A = (1,9)$

where $-4 \bmod 13 = 13 - 4 \bmod 13 = 9$.

According to (3), (4), (5), the coordinates (x_b, y_b) of point B can be computed as below:

$$l = \frac{9-12}{1-0} \bmod 13 = -3 \bmod 13 = 10$$

$$x_b = (l^2 - x_c - x_{-a}) \bmod p$$
$$= (10^2 - 0 - 1) \bmod 13 = 8$$

$$y_b = [l(x_c - x_b) - y_c] \bmod p$$
$$= [10(0-8) - 12] \bmod 13$$
$$= -92 \bmod 13 = 12$$

Node A restores accurate message $B = (8,12)$ that is sent from node B.

Node B recovers message: $A = C + [-B]$.

Because point $B = (8,12)$ so that $-B = (8,-12)$ or $-B = (8,1)$ ($-12 \bmod 13 = 1 \bmod 13$).

The coordinates (x_a, y_a) of point A can be calculated similarly:

$$l = \frac{y_{-b} - y_c}{x_{-b} - x_c} \bmod p = \frac{1-12}{8-0} \bmod 13$$
$$= -11.8^{-1} \bmod 13$$
$$= -11.5 \bmod 13 = 10$$

$$x_a = (l^2 - x_c - x_{-b}) \bmod p$$
$$= (10^2 - 0 - 8) \bmod 13 = 1$$

$$y_a = [l(x_c - x_a) - y_c] \bmod p$$
$$= [10(0 - 1) - 12] \bmod 13$$
$$= -22 \bmod 13 = 4$$

Node B restores accurate message: $A = (1, 4)$.

IV. CONCLUSION

In traditional network coding, transmitted data in the network are n - bit binary vectors. The data coding/decoding are performed by modulo 2 adding (XOR) these vectors together.

In the network coding model based on EC, the transmitted data are presented by the points in an additive group of EC. The data coding/decoding are performed by adding these points together.

The efficiency in reducing the number of transmission sessions of those two methods is the same, but is different in terms of algebraic structure.

This paper presents only another way to carry out network coding. For complete evaluations of this method, further research and analysis are needed.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

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

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

[12] Jean-Yves Chouinard - ELG 5373, "Secure communications and data encryption," School of Information Technology and Engineering, University of Ottawa, April 2002.

[13] William Stallings "Cryptography and Network Security Principles and Practice", Sixth edition, Pearson Education, Inc., 2014.

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

VỀ MỘT PHƯƠNG PHÁP XÂY DỰNG MÃ MẠNG DỰA VÀO PHÉP CỘNG CÁC ĐIỂM TRÊN ĐƯỜNG CONG ELLIPTIC

Tóm tắt: Mã hóa mạng là một kỹ thuật mạng trong đó dữ liệu truyền được mã hóa và giải mã nhằm mục đích tăng lưu lượng mạng, giảm độ trễ và làm cho mạng ổn định hơn. Kỹ thuật mã hóa mạng sử dụng một số thao tác toán học trên dữ liệu để giảm thiểu số lượng phiên truyền giữa các nút nguồn và các nút đích, nhưng vì thế nó sẽ cần xử lý tính toán nhiều hơn tại các nút trung gian cũng như các nút đầu cuối. Bài báo này trình bày một ý tưởng để xây dựng một mô hình mã hóa mạng dựa trên nhóm các điểm cộng trên đường cong elliptic.

Phạm Long Âu, Nhận học vị Thạc sỹ năm 2016. Hiện đang công tác tại Cục Kỹ thuật nghiệp vụ, Bộ Công an. Lĩnh vực nghiên cứu: Lý thuyết thông tin và mã hóa.

Ngô Đức Thiện, Nhận học vị Tiến sỹ năm 2010. Hiện công tác tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Lý thuyết thông tin và mã hóa, mật mã.