users have the right to choose their own route, or follow a predetermined route in the most efficient way. Thus, objects in traffic can travel in two ways, or according to a predetermined, pre-determined route; or follow an arbitrary route. We divide the objects of traffic in classes, depending on purposes and travel needs of those objects. For simplicity, we divide those objects into 2 classes, the first class is the objects participating in traffic according to the scheduled time (for example: Officials to work, students, students coming to school,...), the second class is the other travel and truck flows. On each class of objects participating in traffic, there are different ways to go. When traffic participants find their own unique route, they themselves form the flow of traffic on the network. This transportation network will be optimized according to the *Wardrop* 's variational principle. If we can predict the size of these objects between two points which are the source and target, predict form, which class, which route these objects follow, then we can make a plan and organize the optimal transport network of Hanoi city for the present and the future. Therefore, in this paper we present a mathematical model that predicts multi-class travel of traffic participants, combining the starting point (source) - the ending point (target) and the way to choose the mean of travel, the path of those objects. The solution to the problem helps us to plan as well as create an effective transport model, meeting the needs and requirements for the development of Hanoi city.

2. CONTENT

2.1. Mathematical model

Symbols:

l is the class of objects participating in traffic.

m is the way (type of travel) of objects participating in traffic.

d^{l}_{pqm} is the flow of people from starting area *p* to area ending *q* by way *m* of class *l*.

O^{l}_{p} is the total flow of guest of class *l* originating from area *p*.

D^{l}_{q} is the total flow of guest of class *l* go to from area *p*.

R_{pq} is the set of splicing routes go from area *p* to area *q*.

A is the way of the object to join the traffic without being bound to the route.

T is the way of the road participants according to a predetermined route.

$h^{l}_{r}, r \in R_{pq}$ is the flow of *(A)* of class *l* from area *p* to area *q* on route r of the network.

K_{pq} The fixed truck flow *(T)* from area p to area *q* is represented by h^{k}_{r} .

v^{l} is the number of people per vehicle, it denotes the relationship between the flow of people and the flow *(A)*.

In this article we only consider two ways of going (A) and (T) and they are considered to be operating independently on the network, so the total cost corresponding to each way is separate. The cost of taking *T* is the cost on the routes connecting the area *p* and area *q which* is fixed and shown by the timetable and fare schedule.

We consider the road network to be a set of points *(N)* and roads *(I)*; The Northern Delta region is divided into several provinces, denoted by *(Z).* The total cost of online travel is a weighted, linear function for the time passengers stay in the car, the time passengers spend outside the car of travel, the cost of money as well as the length of the routes (A) . The time passengers sit in the vehicle of each ramp of the road network is an increasing function of the total flow through itself. The time passengers spend outside the vehicle on the road network is the time of entry and exit at the starting and ending points. The monetary costs incurred on the road network are the ramp and parking fees at the end. The vehicle operating cost for a ramp is assumed to be a linear function of the time traveled on the ramp (in minutes) and the length of the ramp (in kilometers). Travel time and length of the distance are variables of the target function, they affect both: individual travel and operating costs related to (*A)* , the impact of these variables on The objective function is represented by the rating factor. The monetary cost of *(T)* is the fare of *(T)*. We define the variables related to cost as follows:

$t_a(f_a)$ is the time in the vehicle when the vehicle is traveling on the connecting road *a* of (*A), which* is the function of the total flow f_a *(minutes).*

k_a the fee for each vehicle (A) on the ramp a or parking fees at the end ramp *(thousand VND).*

s_a is the length of the connecting road a (Km).
$\delta_r^a = 1$ if road a is on route r and is zero in other cases.

$w_{pq,au}$ is the time to travel outside the vehicle by (A) from area p to area q (minutes).

$t_{pq,tr}$ is the time in vehicle of (T) from area p to area q (minutes).

$k_{pq,tr}$ the fare (T) from the area p to the area q (thousand VND).

$w_{pq,tr}$ is the time for going outside of vehicle (T) from area p to area q (minutes).
And other symbols:
$\gamma_1^l = 1$ is the coefficient corresponding to the travel time in (A), of class l.
γ_2^l is the coefficient corresponding to the monetary cost of (A), of class l.
γ_3^l is the coefficient corresponding to the time spent outside the car of (A), of class l.
γ_4^l is the coefficient corresponding to the travel distance of (A), of class l.
γ_5^l is the coefficient corresponding to the travel time in (T), of class l.
γ_6^l is the coefficient corresponding to the fare of (T), of class l.
γ_7^l is the coefficient corresponding to the time spent outside the car of (T), of class l.
γ_8^l is the coefficient corresponding to the waiting time for the transportation of class I

participants .

$\mu^l$is the cost-sensitive parameter of class l.

We have the following **mathematical model:**

$$minT(d,h) = \sum_a \int_0^{f_a} t_a(x)dx + \sum_{la} (\gamma_2^l f_a^l k_a + \gamma_4^l f_a^l s_a) + \sum_{lpq} \frac{\gamma_2^l}{v^l} . d_{pq,au}^l w_{pq,au}$$
$$+ \sum_{lpq} (\frac{d_{pq,tr}^l}{v^l} (\gamma_5^l t_{pq,tr} + \gamma_5^l t_{pq,tr} + \gamma_5^l t_{pq,tr} + \gamma_5^l)) + \sum_{lpqm} \frac{1}{\mu^1 v^1} d_{pqm}^l (lnd_{pqm}^l - 1)$$

With binding conditions:

$$\sum_{r \in R_{pq}} h_r^l = \frac{d_{pqau}^l}{v^l}; p,q \in Z; l \in L$$
$$\sum_{r \in R_{pq}} h_r^k = K_{pq}; p,q \in Z$$
$$\sum_{qm} d_{pqm}^l = 0_p^l; p \in Z; l \in L$$
$$\sum_{pm} d_{pqm}^l = D_q^l; q \in Z; l \in L$$
$$h_r^l \geq 0, r \in R_{pq}, p,q \in Z; l \in \mathrm{L}$$
$$h_r^k \geq 0, r \in R_{pq}, p,q \in Z$$

Here

$$f_a = \sum_l f_a^l + f_a^k = \sum_{lr} h_r^l \delta_r^a + \sum_{lr} h_r^k \delta_r^a \ , a \in A$$

The objective of the problem is to minimize the total cost of transport on the network. From the solution of the problem, we will know how to determine the capacity of the objects in traffic at both source and target points, from which the route and the type of route can be selected.

2.2. Preliminary solution

We construct the *Lagrange* function as follows:

$$L(d,h) = T(d,h) - \sum_{lpq} u_{pq}^l (\sum_{r \in R_{pq}} h_r^l - \frac{d_{pq,au}^l}{v^l}) - \sum_{pq} u_{pq}^k (\sum_{r \in R_{pq}} h_r^k - K_{pq})$$
$$- \sum_{lp} \alpha_p^l (\sum_{qm} d_{pqm}^l - 0_q^l) - \sum_{lq} \beta_q^l (\sum_{pm} d_{pqm}^l - D_q^l$$

Here $u_{pq}^l, u_{pq}^k, \alpha_p^l, \beta_q^l$ are the *Lagrange* agents with corresponding constraints.

Taking partial derivative according to the flow variable of *(A)* of *Lagrange* function, we achieve the following optimal conditions:

$$\sum_a t_a(f_a)\delta_r^a + \gamma_2^1 \sum_a k_a \delta_r^a + \gamma_4^1 \sum_a s_a \delta_r^a - u_{pq}^l \geq 0, pq \in Z; l \in L$$

$$h_r^l(\sum_a t_a(f_a)\delta_r^a + \gamma_2^1 \sum_a k_a \delta_r^a + \gamma_4^1 \sum_a s_a \delta_r^a - u_{pq}^l) = 0, pq \in Z; l \in L$$

Similarly, we also achieve the optimal condition for the flow (T).

We define the total cost of *(A)* of route *r* of class *l* as:

$$c_r^l = \left(\sum_a t_a(f_a)\delta_r^a + \gamma_2^1 \sum_a k_a \delta_r^a + \gamma_4^1 \sum_a s_a \delta_r^a\right)$$

If $h_r^l \geq 0, r \in R_{pq}, c_r^l = u_{pq}^l$. That means, if all the flow from p to q is positive flow of class l then the travel cost of the total flow of (A) is equal.

If $h_r^l = 0, r \in R_{pq}, c_r^l \geq u_{pq}^l$. That means, if the flow from p to q is flow 0 in class l, then the total travel cost of (A) is not less than the other flows. (These conditions derive from *Wardrop* 's variational principle).

The unit of overall cost of *(A)* is calculated in minutes of the vehicle on the road. Its corresponding coefficient is the number of minutes in the vehicle on the road per corresponding unit of variable (cents, number minutes outside the car, km,...). The monetary cost factor of *(A)* takes into account the occupancy, the length of the travel that adversely affects travel and the monetary cost of activity.

The coefficient of the time in the vehicle of the travel on the road in the target function is equal to 1.

The time spent on the ramp depends on the total coupling flow, applied for two ways *(A)* and (*T*), then take the partial derivative of the O-D variable of the *Lagrange* function, we obtain:

$$\textit{(A):} \quad \left(\frac{\gamma_3^l}{v^l}\right) w_{pq,au} + \left(\frac{1}{\mu^l v^l}\right) ln\ d_{pq,au}^l + \left(\frac{u_{pq}^l}{v^l}\right) - \alpha_p^l - \beta_q^l = 0, pq \in Z;\ l \in L$$

$$\textit{(T):} \quad \frac{1}{v^l}\gamma_5^l t_{pq,tr} + \gamma_6^l k_{pq,tr} + \gamma_7^l w_{pq,tr} + \gamma_8^l + \left(\frac{1}{u^l v^l}\right) ln\ d_{pq,au}^l - \alpha_p^l - \beta_q^l = 0, pq \in Z;\ l \in L$$

From the above two equations we have:

$$d_{pq,au}^l = \exp \mu^l v^l\ \ \alpha_p^l + \beta_q^l - \mu^l\ \ \gamma_3^l w_{pq,au} + u_{pq}^l$$

$$d_{pq,tr}^l = \exp \mu^l v^l\ \ \alpha_p^l + \beta_q^l - \mu^l\ \ \gamma_5^l t_{pq,tr} + \gamma_6^l k_{pq,tr} + \gamma_7^l w_{pq,tr} + \gamma_8^l$$

We put

$$c_{pq,au}^l = u_{pq}^l + \gamma_3^l w_{pq,au}^l$$

$$c_{pq,tr}^l = \gamma_5^l t_{pq,tr}^l + \gamma_6^l k_{pq,tr}^l + \gamma_5^l w_{pq,tr}^l + \gamma_8^l$$

Thence inferred:

$$d^l_{pq,au} = A^l_p O^l_p B^l_q D^l_q \exp -\mu^l c^l_{pq,au}$$

$$d^l_{pq,tr} = A^l_p O^l_p B^l_q D^l_q \exp -\mu^l c^l_{pq,tr}$$

The *Lagrange* factors are α^l_p, β^l_q; moreover, A^l_p, B^l_q are defined as:

$$1/\,A^l_p = \sum_q B^l_q D^l_q.\exp - \mu^l c^l_{pq,au} + \exp -\mu^l c^l_{pq,tr}$$

$$1/\,B^l_q = \sum_p A^l_p O^l_p.\exp - \mu^l c^l_{pq,au} + \exp -\mu^l c^l_{pq,tr}$$

3. CONCLUSION

The above text is a traffic forecasting problem model that can be applied to Hanoi City. Of course, there are other models related to this problem. Choosing which model is suitable for our processing ability and practical situation can only be solved on the basis of specific calculations. With the above model, this is a nonlinear planning problem with a very large number of variables, thoroughly solving this problem is still difficult. However, with the current development of computer technology, we hope to solve this problem thoroughly, and can create a good software to implement this model for traffic of Hanoi city.

REFERENCES

1. David Boyce , Hillel Bar-Gera (2003), Validation of multiclass urban travel forecasting models combining origin - destination, mode and route choices, *Journal of Regional Science*, 43.

2. Hillel Bar-Gera, David Boyce (2003), *Origin - based Algorithms for Combined Travel Forecasting Models*, Transportation Research Part B, 37, p. 405-422.

VỀ MỘT MÔ HÌNH DỰ BÁO GIAO THÔNG ĐA THÀNH PHẦN CHO THÀNH PHỐ HÀ NỘI

Tóm tắt: *Để giúp cho việc hoach định chiến lược phát triển mạng lưới giao thông nội đô và các vùng ngoại thành được tốt thì chúng ta phải dự báo được các thành phần tham gia giao thông của thành phố Hà Nội. Trong bài báo này, chúng tôi trình bày một mô hình dự báo giao thông đa thành phần, dự báo sự đi lại của nhiều lớp đối tượng tham gia giao thông. Việc nghiên cứu mô hình này có thể sẽ là hữu ích cho việc thiết lập và tổ chức mạng lưới giao thông liên quận huyện cho thành phố Hà Nội.*

Từ khóa: *Mô hình dự báo giao thông đa thành phần*

DEVELOPING RSA AND RABIN SIGNATURE SCHEMES IN CASE OF EXPONENT E=3

Hoang Thi Mai, Le Chi Chung, Ngo Van Than

Hanoi Metropolitan University, Hanoi University of Culture

Abstract: *The RSA and Rabin signature schemes are both developed based on the difficulty of the factorizing problem. While the exponent e in the RSA scheme has to satisfy gcd(e, ϕ(n)) = 1, in the Rabin scheme, e=2 and is always the divisor of ϕ(n). On solving the problem of constructing a signature scheme with low signature-verifying cost for digital transaction that require authentication of signature validity in a great deal, this study suggests a signature schemes base on the graphical model in case of exponent e= 3 and 3 is the divisor of ϕ(n). This scheme is similar to the Rabin scheme, with e=3 as the divisor of (p-1) and (q-1). With exponent e=3, the schemes have low signature-verifying cost, which meet the requirement of the problem above.*

Keywords: RSA Signature Scheme, Digital Signature Scheme, Rabin Signature Scheme, Cube Root Signature Scheme

Received: 19 March 2020

Accepted for publication: 20 April 2020

Email: htmai@hnmu.edu.vn

1. INTRODUCTION

In digital transactions, there are many activities that require authentication of signature validity in a great deal, such as the profile admission of public administration service; activities in which authentication is considered compulsory, such as inspecting digital certification. Therefore, in order to use digital signature efficiently, signature-verifying algorithm consuming little time needs to be applied.

Evaluating the digital signature systems that have been included as standard RSA (Rivest–Shamir–Adleman-the first public key cryptosystems), discrete logarithms (DL) and elliptic curves (EC) with input parameters of the same level of safety given in Figure 1 (cited from FIP 186-2 [1], NIST 800-56 [2] and presented by Darrel Hankerson in [3]), Lenstra and Verheul turned out that in case of a small exponent (e = 3), RSA was more efficient than EC and DL systems [4], [5].