Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

An Optimized Method of Packet Loss Rate under Backup Path Protection in OBS Network

To cite this article: Aodong Meng *et al* 2021 *J. Phys.: Conf. Ser.* **1746** 012064

An Optimized Method of Packet Loss Rate under Backup Path Protection in OBS Network

Aodong Meng[1,2,*], Yucheng Chen[1,2], Jiahao Dai[1,2] and Yongqun Chen[1,2]

[1]Science and Technology on Communication Information Security Control Laboratory, Jiaxing, China
[2]No.36 Research Institute of CETC, Jiaxing, China

*Corresponding author email: 1906251174@qq.com

Abstract. In order to calculate the packet loss rate in OBS network, this paper proposes a method, which performs good in both accuracy and rapidity, based on Erlang B formula to estimate the packet loss probability in OBS network using backup path protection mechanism. This method can be used to optimize the design of OBS network protocol, and it also provides an accurate and efficient approximate calculation method of packet loss rate in OBS network and can be conductive to the study of using copy transmission to enhance the network survivability. Based on the formula of Erlang B, this paper briefly introduces the derivation process and principle of this method. The basic experimental principles of simulation and estimation processes are designed in this paper, and the experimental results of the proposed method under a typical network topology (ARPA network) with no protection mechanism and 1 and 2 backup paths protection mechanisms are analyzed to verify its rapidity and accuracy. The results of experiments show the accuracy and efficiency of this method.

1. Introduction

In 1997, Qiao Chunming [1] and Jonathan Turner [2] respectively proposed new technologies for optical burst switching (OBS) for transitioning between circuit switching and packet switching technologies. Optical switching technologies can be divided into optical line switching (OCS), optical packet switching (OPS), optical burst switching (OBS), and optical multi-protocol label switching (OMPLS) technologies [3-6]. Compared with other technologies, optical burst switching has better resource allocation and resource utilization performance, which overcomes the disadvantages of optical packet switching in optical switch technology and optical buffer technology, and will be an important transition technology in the development of the Internet.

Survivability is one of the research focuses in OBS networks [7], and the research purpose is that data packets can still be transmitted when a link failure occurs. Thus, we can send multiple copies to the destination node through other paths while sending burst packets, namely the backup path protection mechanism [8]. This can significantly increase the probability of successful transmission of burst packets in the case of a small number of link failures. However, after the extra burst packet copy enters the OBS network, it will increase the actual load, increase the packet loss rate in the network, and reduce the quality of service (QoS) of the network. The approximate calculation of the packet loss rate of the OBS network using the backup path protection mechanism is very important for the optimization of the theoretical scheme and the design of the actual OBS network protocol.

2. Approximate Calculation Algorithm Principle

In this section, this paper briefly introduces and analyzes the calculation formula of Erlang B. Based on this, the approximate calculation algorithm formula of the OBS network packet loss rate proposed in this article is derived.

2.1. ErlangB Formula

We can define: in the optical burst network, the probability of causing the packet transmission process to fail, referred to as the packet loss rate, is usually expressed by *B*. We specify A as the load of all burst packets, and A' as the load of burst packets that are successfully carried out during the packet transfer process, referred to as the completion load; C_0 is the number of times that the packet transfer process is successfully performed in unit time; t_0 is the average time that the channel is occupied by each burst transmission process. In summary, it is easy to get the formula of the completed load: A' $=C_0*T_0$. The corresponding packet loss rate can be expressed as: B=$\frac{A-A'}{A}$*100%. $A-A'$ is the lost load. Therefore, we can get the Erlang B formula [9, 10] to solve the packet loss rate. The formula is as follows.

$$\mathrm{B}=P_n=\frac{A^N/n!}{\sum_{k=0}^{n}A^k/k!} \tag{1}$$

A represents the intensity of the traffic that flows into the service, that is, the load; n represents the system capacity or the number of circuits. The application of the Erlang B formula is based on two assumptions [11]:

(1) The number of users is much larger than the total number of channels actually provided in the switching system.

(2) The user will not initiate the burst packet transfer process again after the request is rejected due to blocking.

Based on these two assumptions, we can consider that the burst arrival of users obeys the Poisson distribution, so the probability of k burst packets occupying the channel at the same time can be expressed by the following formula:

$$\mathrm{P(k)}=\frac{\left(\frac{\lambda}{\mu}\right)^k/k!}{\sum_{i=0}^{N}\left(\frac{\lambda}{\mu}\right)^i/i!} \tag{2}$$

Where λ represents the average number of times a user's burst packet arrives per unit time; T is the average hold time of the channel occupied by the burst packet; μ=1/T, often referred to as the average leave rate; N represents the number of channels of the switching system. When all channels in the system are occupied, the system is considered to be blocked. Thus, the probability that all channels in the system are simultaneously occupied can be expressed as:

$$\mathrm{B}=\mathrm{P(N)}=\frac{(\lambda/\mu)^N/N!}{\sum_{i=0}^{N}(\lambda/\mu)^i/i!} \tag{3}$$

Comparing Eq. (3) and Eq. (1), it is easy to get A=λ/μ= λ*T, which represents the average load. It should be noted that the load A actually includes the load generated by the burst packets that have been served and the load generated by the burst packets that are rejected due to link blocking. The formula for calculating the load generated by a burst packet whose transmission request is satisfied is as follows:

$$A'=\mathrm{E\{k\}}=\sum_{k=0}^{N}\mathrm{kP}(k)=\frac{\sum_{k=0}^{N}k*A^k/k!}{\sum_{i=0}^{N}A^i/i!}=\frac{A*\sum_{k=0}^{N-1}A^k/k!}{\sum_{i=0}^{N}A^i/i!}=\mathrm{A(1\text{-}B)} \tag{4}$$

It can be seen that A' represents the load actually provided by the *N* channels, and the load of the burst packets that are blocked can be expressed by $A * B$.

This formula is also a formula that is frequently used in this paper. It may be calculated multiple times based on the network topology.

2.2. Algorithm for Approximate Calculation of Packet Loss Rate in OBS Networks

In this section, this paper describes the principle of the approximate algorithm for the packet loss rate of OBS networks under the backup path protection mechanism based on the Erlang B formula.

First we take the protection mechanism using one backup path as an example. For each source node-destination node pair *m*, the load of the basic path is specified as ρ_m^{pri}, and the load of the protection path is specified as ρ_m^{pro}, assuming that they are independent of each other. And we assume here that these links are independent of each other, and the transmission process on each link satisfies Poisson distribution.

Therefore, for the total load a_j of a link *j*, we can use the following formula to calculate:

$$a_j = \sum_{m\in\beta} I'\left(j, U_m^{\text{pri}}\right)\rho_m^{\text{pri}} \prod_{i\in E}\left(1 - I\left(i, j, U_m^{\text{pri}}\right)b_i\right) + \\ \sum_{m\in\beta} I'(j, U_m^{\text{pro}})\,\rho_m^{\text{pro}} \prod_{i\in E}(1 - I(i, j, U_m^{\text{pro}})b_i) \tag{5}$$

E represents a set of links; *U* represents a path table, which refers to each link that a path passes through; *I (i, j, U)* is 1 when the links *i* and *j* belong to the path table U and the link *i* precedes the link *j*, otherwise 0. $I'(j,U)$ is 1 when the link *j* belongs to the path table *U*, otherwise 0.

After the total load of each link is obtained, the blocking rate for a certain link *i* can be calculated using the Erlang B formula:

$$b_i = \frac{a_i^C/C!}{\sum_{n=0}^{C} a_i^n/n!} \tag{6}$$

C is the total number of channels on link *i*.

Then, the formula for calculating the packet loss ratio of the SD pair is:

$$B_m^p = (1 - \prod_{j\in U_m^{\text{pri}}}(1 - b_j))(1 - \prod_{i\in U_m^{\text{pro}}}(1 - b_i)) \tag{7}$$

Then the average packet loss rate of this network is:

$$B_{\text{network}} = \sum_{m\in\beta} B_m^p \tag{8}$$

The above is the formula using a single backup path in protection mechanism. If the network uses multiple backup paths in protection mechanism, the basic principle of the formula remains unchanged, but the protection path part needs to be expanded. For example, if two backup paths are used in protection mechanisms, the link load calculation formula is:

$$a_j = \sum_{m\in\beta} I'\left(j, U_m^{pri}\right)\rho_m^{pri} \prod_{i\in E}\left(1 - I\left(i, j, U_m^{pri}\right)b_i\right) + \\ \sum_{m\in\beta} I'\left(j, U_m^{pro1}\right)\rho_m^{pro1} \prod_{i\in E}\left(1 - I\left(i, j, U_m^{pro1}\right)b_i\right) + \\ \sum_{m\in\beta} I'\left(j, U_m^{pro2}\right)\rho_m^{pro2} \prod_{i\in E}\left(1 - I\left(i, j, U_m^{pro2}\right)b_i\right) \tag{9}$$

The calculation formula of the packet loss rate of a single link and the average packet loss rate of the network is unchanged, while the calculation formula of the packet loss rate of the burst packets using the two backup paths in protection mechanism is:

$$B_m^p = (1 - \prod_{j\epsilon U_m^{pri}}\left(1 - b_j\right))(1 - \prod_{i\epsilon U_m^{pro1}}(1 - b_i))\,(1 - \prod_{i\epsilon U_m^{pro2}}(1 - b_i)) \tag{10}$$

The calculation formula of the packet loss rate under the protection mechanism using more backup paths can be deduced by analogy.

3. Experiment

The experiments in this paper include two parts: simulation and algorithm estimation. Next, we use the protection mechanism with one backup path as an example to describe the principle of simulation and algorithm estimation. The descriptions of the principles of simulation and algorithm estimation are as follows in Section 3.1 and 3.2.

3.1. Principle of Simulation

(1) First, after the network structure is constructed and the path information is recorded, it is determined whether the network is completely empty, that is, whether all links in the network are idle.
If the above conditions are met, only incoming packets may occur at this time. The total number of incoming packets on the network and the number of existing packets waiting for service in the network are updated, and related information is recorded.
(2) If the condition (1) is not satisfied, a random number X ($0 \le X \le 1$) needs to be generated to compare with the probability calculation formula $p = \lambda / (\lambda + \mu * Q)$ (where Q represents the total number of burst packets currently waiting for service in the network, and the other parameters are the same as those defined in Section 2.1) to determine whether a packet-in or packet-out process occurs at this time.
(a) If $X \le p$, the judgment result is the packet entering process. After updating the relevant information of the packet, read the path table to determine the link that the burst packet should first enter, and determine if there is an idle channel in the link:
If all channels of the link are found to be occupied, it is determined that packet loss has occurred at this time, and the packet loss rate needs to be updated.
If it is found that there is an idle channel in the link, it is similar to packet loading process in (1), and then record the corresponding burst packet and network condition information;
(b) If $X > p$, the judgment result is a packet out process, and one of the burst packets waiting for service in the current network needs to be randomly selected for packet out. Read the information of the burst packet for judgment. If the judgment result is that the current burst packet is located on the last hop, the next action of the burst packet should be leaving the network, and the relevant information parameters should be recorded.
If the judgment result is that the current burst packet still needs to continue the transmission process, read the relevant information of the burst packet, and read the path table to get the sequence number of the link that the packet will enter next. The following process is similar to (2)(a);
The above process needs to be repeated for many times (it is performed for 10^6 times in this paper) to achieve the effect of experimental simulation;
(3) After the loop process above is completed a predetermined number of times, the network packet loss and the total number of network packets are extracted, and the packet loss rate is calculated according to the following formula: Packet loss rate = Number of network packets lost / The total number of network packet. The simulation process ends.
In the packet entering process in (1) and (2)(a), the source and destination of the packet are generated randomly (but they should not be the same node). This paper uses Dijkstra algorithm [12,13] to find the shortest path in the simulation part of the experiment.

3.2. Principle of Algorithm Estimation

(1) First, after the network structure is constructed and the path information is recorded, each record parameter is initialized and the initial link blocking rate value is specified.
(2) Calculate the total initial load of each link according to formula (5).
(3) Calculate the blocking rate of each link according to formula (6), and determine whether the accuracy of the single link blocking rate meets the requirements (in this paper, the error of each link blocking rate is summed and the result meets the requirements when the sum is less than 10^{-15}).
If the requirements are not met, the initial blocking rate of each link is updated to the current calculated value and the process returns to (2).
If the requirements are met, the total packet loss rate of each SD pair and the network is calculated according to formulas (7) and (8), and the algorithm estimation process ends. In this paper, the high accuracy and efficiency of the estimation algorithm proposed in this paper are verified in three cases (no protection mechanism, and protection mechanism using 1 and 2 backup paths).

3.3. Analysis of Results

In this paper, ARPA network topology is selected for experiment. In this paper, there are two reverse independent links between two connected nodes in the topology, and one link contains 10 channels.

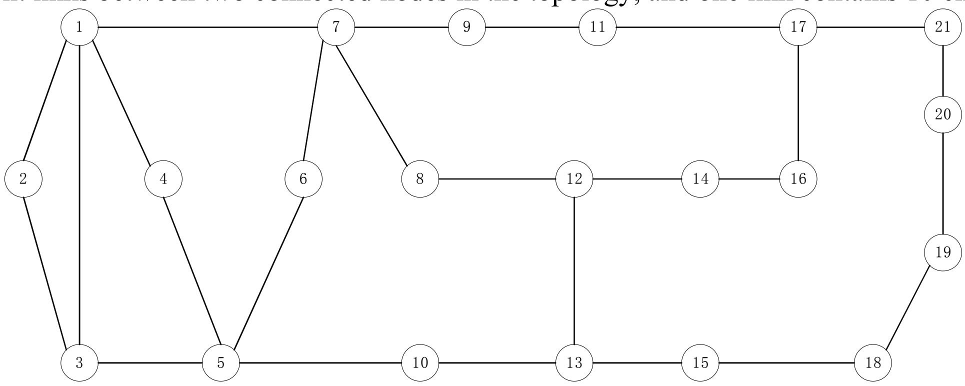

Figure 1. ARPA network topology.

This paper verifies the high accuracy and efficiency of the estimation algorithm proposed in the three cases (no protection mechanism, and protection mechanism using 1 and 2 backup paths) of the above network topology. As a comparison, the experiment of no protection mechanism is performed in order to make the experimental results more comprehensive. We performed experiments on a set of specified total network loads. The experimental results in each case of network topology include an experimental data table and two experimental data graphs. The table records the simulation results and the estimated results of packet loss rate and the time consumed. The experimental data graph compared the above results. Due to the large span of the experimental results under different network total load, the ordinates are plotted on the graph in logarithm for observation and comparison. The loss rate is calculated according to the principle in Section 3.1 and Section 3.2.

The experimental results of network with no protection mechanism are as follows:

Table 1. The experimental result of network with no protection mechanism

Total network load	Simulation packet loss rate	Simulation time (s)	Estimated packet loss rate	Estimation time (s)
20	6.70E-05	5.940171	9.61E-05	0.019914
30	0.002	5.993149	0.0019	0.02047
40	0.0109	6.213463	0.0112	0.022506
50	0.0325	6.433759	0.0347	0.023754
60	0.068	6.261841	0.0724	0.027979
70	0.1133	6.601606	0.1186	0.028648
80	0.1608	6.31979	0.1675	0.03096
90	0.211	6.806833	0.2154	0.033538
100	0.2524	6.408433	0.2606	0.035459
110	0.2977	6.719234	0.3023	0.038858
120	0.3353	6.207093	0.3406	0.042227

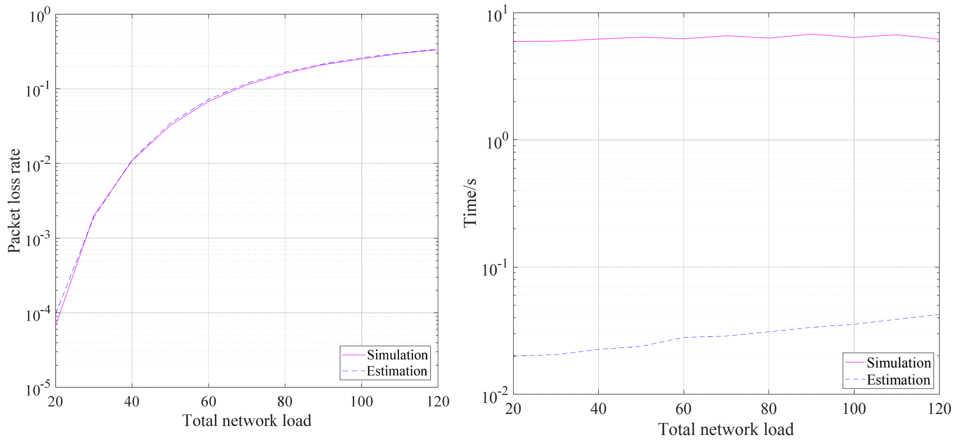

Figure 2. The experimental result graphs of network with no protection mechanism

The experimental results of network with protection mechanism using 1 backup path are as follows:

Table 2. The experimental results of network with protection mechanism using 1 backup path

Total network load	Simulation packet loss rate	Simulation time (s)	Estimated packet loss rate	Estimation time (s)
20	0.0032	7.41407	0.0033	0.034704
30	0.042	7.680619	0.0444	0.068792
40	0.1218	7.560794	0.126	0.082585
50	0.2123	8.07267	0.2158	0.144401
60	0.2936	8.187993	0.2984	0.16371
70	0.3635	7.769653	0.3698	0.201429
80	0.4243	7.70521	0.4306	0.225679
90	0.4789	7.846779	0.4822	0.228273
100	0.5227	7.96452	0.5262	0.219173
110	0.5618	7.775833	0.564	0.225177
120	0.5932	7.608299	0.5966	0.232031

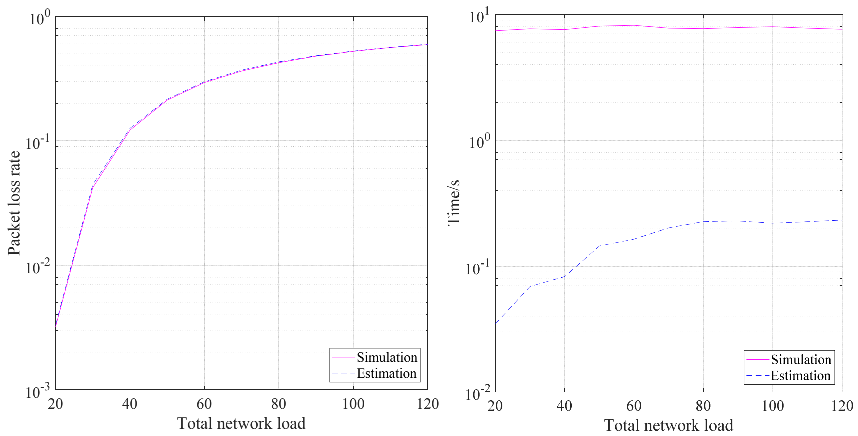

Figure 3. The experimental result graphs of network with protection mechanism using 1 backup path

The experimental results of network with protection mechanism using 2 backup paths are as follows:

Table 3. The experimental results of network with protection mechanism using 2 backup paths

Total network load	Simulation packet loss rate	Simulation time (s)	Estimated packet loss rate	Estimation time (s)
20	0.0033	7.522046	0.0034	0.039501
30	0.0434	7.818592	0.0447	0.053572
40	0.1219	8.221438	0.1266	0.093317
50	0.2101	8.218726	0.2166	0.178769
60	0.2941	8.167579	0.2992	0.192024
70	0.3645	8.30299	0.3707	0.254183
80	0.4275	8.130542	0.4315	0.25565
90	0.4783	8.175803	0.4831	0.259517
100	0.5211	8.279601	0.5271	0.257845
110	0.5609	8.305944	0.5648	0.26074
120	0.5953	8.504412	0.5974	0.250109

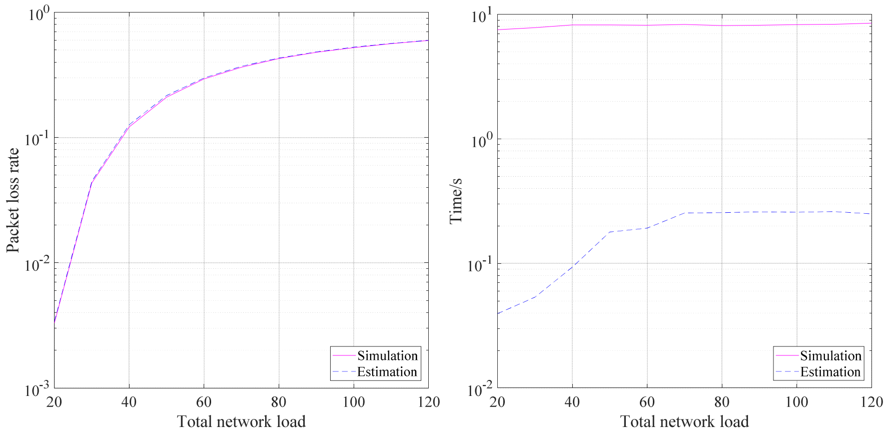

Figure 4. The experimental result graphs of network with protection mechanism using 2 backup paths

From the above experimental results we can get:

1) The calculation result of algorithm estimation proposed by this paper is close to the simulation results of corresponding network packet loss rate, and the algorithm running time is obviously much shorter than the simulation time, indicating that the approximate algorithm in this paper has good accuracy and rapidity;

2) As shown in the graph of consumption time, with the increase of the total network load, the simulation time changes little, while the algorithm estimation time shows an obvious trend of gradual increase, but it is still far less than the simulation time in general.

3) By comparing experimental data under different conditions of the topology, we found that:

a) When compared with no protection mechanism, the packet loss rate of the network with backup path protection mechanism is significantly higher. This is because after the use of the backup path for all packages, although the resistance ability of the network to the sudden failure of a link is improved, the actual data in the network is also significantly increased, which aggravates the network load and increases the packet loss rate. So in actual application, the important data can be transmitted with backup path protection mechanism, and the ordinary data can be transmitted in the normal way. Therefore, the network improves its resistance to sudden link fault as well as reduces the actual load in the network, enhances the overall performance of the network;

b) Compared with the unprotected mechanism, the experimental simulation time and algorithm estimation time of the backup path mechanism are significantly increased. This is because at this time, in addition to the main path, there are backup paths in the network. The principle of algorithm is more complicated, so the increase in time consumption is normal.

4. Conclusion

This paper presents a fast and accurate method that can be applied to approximate the packet loss probability in OBS networks using backup path protection mechanisms. After introducing the simulation process and the methods used in the estimation algorithm, this paper evaluates the accuracy and speed of the proposed estimation algorithm in three cases (no protection mechanism, and protection mechanism using 1 and 2 backup paths) of a typical network topology. The results show that the estimation algorithm proposed in this paper has good accuracy and efficiency. This method can provide a reference in the design and optimization process of OBS network protocol, and can also perform fast approximate calculation in the study of the survivability of OBS network.

In future work, further research may be considered in the following points:

(1) It can be considered to apply the experimental simulation and approximate calculation algorithm in this paper to some larger and more complex network topologies in future work in order to further improve the approximate calculation algorithm.

(2) It is possible to consider the case of adding sudden link failures and different protection mechanisms for important and ordinary data in the experiment to further verify and improve the approximate calculation algorithm in this paper.

References

[1] Qiao C, Yoo M. Optical burst switching (OBS) - A new paradigm for an Optical Internet[J]. Journal of High Speed Networks, 1999, 8(1):69-84.

[2] Turner J S. Terabit Burst Switching[J]. Journal of High Speed Networks, 1999, 8(1):3-16.

[3] Ohno H, Hasegawa H, Sato K I. A dynamic and quasi-centralized RWA method for optical fast circuit switching networks employing route pre-prioritization[J]. Optical Switching and Networking, 2011, 8(4):242-248.

[4] Huang Y C, Yoshida Y, Kitayama K I, et al. OPS/Agile-OCS Data Center Network With Flow Management [J]. Journal of Optical Communications and Networking, 2015, 7(12):1109.

[5] Huang Y C, Yoshida Y, Ibrahim S, et al. Novel virtual OCS in OPS data center networks [J]. Photonic Network Communications, 2016, 31(3):448-456.

[6] Wen Y G, Zhang Y, Chen L K. On Architecture and Limitation of Optical Multiprotocol Label Switching (MPLS) Networks Using Optical-Orthogonal-Code (OOC)/Wavelength Label[J]. Optical Fiber Technology: Materials, Devices and Systems, 2002, 8(1):43-70.

[7] Alam M S, Alsharif S, Panati P. Performance evaluation of throughput in optical burst switching[J]. International Journal of Communication Systems, 2015, 24(3):398-414.

[8] Oh S, Kim Y, Yoo M, et al. Survivability in the optical internet using the optical burst switch [J]. Etri Journal, 2002, 24(2):117–130.

[9] Hernandez J A , Aracil J , Pedro L D , et al. Analysis of Blocking Probability of Data Bursts With Continuous-Time Variable Offsets in Single-Wavelength OBS Switches[J]. Journal of Lightwave Technology, 2008, 26(12):1559-1568.

[10] Zeng G. Two common properties of the erlang-B function, erlang-C function, and Engset blocking function[J]. Mathematical and Computer Modelling, 2003, 37(12-13):1287-1296.

[11] Schneps-Schneppe M, Sedols J. On Erlang B-formula and ERT method extension[C]. Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on. IEEE, 2010.

[12] Idri A, Oukarfi M, Boulmakoul A, et al. A distributed approach for shortest path algorithm in dynamic multimodal transportation networks[J]. Transportation Research Procedia, 2017, 27:294-300.

[13] Jasika N , Alispahic N , Elma A , et al. Dijkstra's shortest path algorithm serial and parallel execution performance analysis[C]. 2012 Proceedings of the 35th International Convention MIPRO. IEEE, 2012.