INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2015, VOL. 61, NO. 2, PP. 179–184
Manuscript received May 18, 2015; revised June 2015. DOI: 10.1515/eletel-2015-0023

Dynamic RSA Problem for Time-Varying Traffic in Spectrum Sliced Elastic Optical Path Network

Ireneusz Olszewski

***Abstract*—Service time-varying traffic flexible optical networks require a dynamic bandwidth allocation in order to follow the source transmission rate. The problem of service time-varying traffic, assuming that the set of connection requests is not known in advance, is considered in this work. Connection requests arrive randomly and have random durations. The considered dynamic RSA problem involves minimizing the probability of future connections blocking while maintaining spectrum continuity constraints and non-overlapping spectrum assignment constraints between spectrum-adjacent connections on the network links. The proposed algorithm determines the path with the required number of slots around the reference frequency for a connection request. An analysis of the network with time-varying traffic on the network connections was carried out on the basis of spectrum expansion/contraction schemes which allow to determine average blocking probability of the additional slot requests on these connections. The obtained results have been compared with those obtained by a well known algorithm that solves the dynamic RSA problem.**

***Keywords*—time-varying traffic, dynamic RSA problem, the optical path, the OFDM modulation**

I. INTRODUCTION

In traditional DWDM networks, rigid grid frequency leads to inefficient use of spectrum in the network if the traffic of a connection is not sufficient to fill the entire capacity of a given wave length. To eliminate these disadvantages in WDM networks, spectrum-sliced elastic optical path networks (SLICE) have been proposed. Orthogonal frequency modulation (OFDM) used in these networks allows to service connections with arbitrarily high data rate by dividing the transmitted data into several sub-carriers of low bit rates. Similarly to the problem of routing and wavelength assignment (RWA problem) in DWDM networks, the problem of routing and spectrum assignment (RSA problem) also appears in SLICE networks. This RSA problem can be considered as a static or dynamic case. In the static case the traffic matrix is *a priori* known in terms of the needed capacity. Routing and spectrum assignment for the connections being established is performed *off-line*. In turn, for the dynamic RSA problem a stream of connection requests is random and the set of connections and their duration are not known in advance. Routing and spectrum assignment for connections are performed *on-line*. In both cases sources transmission rates can be fixed or variable in time.

In [1] the formulated dynamic RSA problem takes into account the relationship between traffic bit rate and OFDM signal spectrum. Connection requests are random (Poisson) with exponential duration of the connections and the source transmission rate of this connections does not vary in time. The objective function minimizes the actual length of the path while the spectrum continuity constraints and non-overlapping spectrum for adjacent OFDM signal constraints play the role of constraints of the considered problem. Two different algorithms for solving the formulated problem, based on segment representation of the spectrum, have been proposed. In [2] the RSA problem is formulated for a known in advance set of demands as an integer linear programming task. Heuristic algorithm based on collision metrics has been proposed to solve this problem when the ILP solution is not achievable. In [3] a static problem of RSA, in which a set of connections is known in advance, has been formulated. The objective function minimizes the most utilized spectrum slot while maintaining non-overlapping spectrum for spectrum-adjacent connection constraints. To solve this RSA problem, several algorithms have been proposed from optimal and decomposition ILP algorithms to a sequential heuristic algorithm combined with appropriate ordering policies and simulated annealing meta-heuristic. In [4], the static RSA problem, where spectrum allocated to connections varies with time so as to follow the source transmission rate, has been considered. It should be noted, however, that in the considered problem (in [4]) the set of connection requests with the required number of slots is known in advance i.e. that the connections are only set up (long-lived connections).

In this paper, the dynamic RSA problem has been proposed in which the number of slots in the carried out connections varies dynamically according to the source transmission rate and the set of connection requests is not known in advance. Connection requests arrive randomly and duration of the connections is exponential. To solve this problem, an algorithm which finds a path and a reference frequency with the required number of slots so as to minimize the average blocking probability of additional slot requests has been proposed. An analysis of a network, in which the spectrum of connections varies dynamically, has been carried out using two expansion/contraction schemes, on the basis of which the blocking probability of additional slots has been determined. The obtained results have been compared with the results

I. Olszewski is with the Institute of Telecommunications, Faculty of Telecommunications, Informatics and Electrical Engineering, UTP University of Sciences and Technology, S. Kaliskiego 7, 85-789 Bydgoszcz, Poland (e-mail: ireneusz.olszewski@utp.edu.pl).

obtained using the MSP algorithm that solves the dynamic RSA problem assuming that the needed number of slots for each connection does not vary in time.

It should be noted that a further searching of algorithms for solving the dynamic RSA problem, in which a set of connections is not known in advance and required number of slots for the connections are variable in time, is still necessary.

The remaining part of this paper is as follows. The second part contains a formulation of the considered optimization problem. In the third part a network analysis method, where spectrum of the connections varies dynamically, is proposed. The fourth part describes the proposed algorithm, which solves the dynamic RSA problem. The fifth part presents the results while the sixth part contains a summary and conclusions.

II. THE FORMULATION OF THE OPTIMIZATION PROBLEM

Let the network be graph *G(N, E)*, where *N* is a set of nodes, and *E* is a set of unidirectional links *e*, such that the $e \in E$. *T* is a set of slots, numbered from 1 to $|T|$ for each network link. *R* is the symbol rate (in baud) for each OFDM sub-carrier, and *G* is a guard band (in slots) between adjacent OFDM signals. Further, let the incoming request between a pair of nodes *s*, $d \in N$ be for *C* units of bandwidth [in b/s]. The relationship between bit-rate *C* and signal spectrum *B* in the case of OFDM modulation, assuming that all of the sub-carriers have the same format with *m* bits per symbol, can be defined as [1]:

$$B = (\lceil C/2mR \rceil + 1)R \tag{1}$$

where: $n = \lceil C/2mR \rceil$ is the number of the sub-carriers that is equal to the number of required slots.

Connection requests with the required bandwidth arrive randomly and connection durations are exponential distribution. For a given request, the specified path *p* with the required number of slots $n_p = n_p^L + n_p^H$ around the reference frequency f_p is determined by the RSA algorithm. It should be noted that, for both static and dynamic RSA problems, an algorithm for finding path *p* must maintain the spectrum continuity constraints and non-overlapping spectrum-adjacent connection constraints for specified links of the network. The spectrum of link S_e can be represented as the sum of L_e sets of available slots: $S_e = \bigcup_l S_e^l = \bigcup_l (a_e^l, b_e^l)$, where: a_e^l is the first and b_e^l the last slot of *l*-set. On the other hand, the aggregated spectrum of path S_p is defined as the intersection of the spectrum of links S_e, such that $e \in p$, ie. $S_p = \bigcap_{e \in p} S_e$. Fulfillment of the spectrum continuity constraint ensures the required number of adjacent slots in set *l* of available slots of aggregated spectrum of path S_p^l, *l*=1..L_p, which means that $n_p + G \le |S_p^l|$. Increasing the required number of slots, e.g. by *G* = 1 slots results from the need to eliminate interference between the spectrum-adjacent connections on the network links. On the other hand, non-overlapping spectrum constraint makes it impossible for two spectrum-adjacent connections to use the same slots on link at the same time. It should be noted that in the case of connections serving dynamic traffic, where allocation of the required number of slots varies dynamically, the same slots may be shared by spectrum-adjacent connections. Figure 1 [4] shows an example of the spectrum slots occupancy on the two links *e* and *e'* belonging to connection *p*. Let *B(p,e)* and *U(p,e)* be the bottom and upper spectrum of spectrum-adjacent connections respectively to connection *p* on link *e*. Further, let $f_{B(p,e)}$ be the reference frequency, and let $n_{B(p,e)}^H$ be the number of upper spectrum slots of the connection bottom adjacent to connection *p* on link *e*. In turn, let $f_{U(p,e)}$ be the reference frequency and let $n_{U(p,e)}^L$ be number of lower spectrum slots of the connection upper adjacent to connection *p* on the same link.

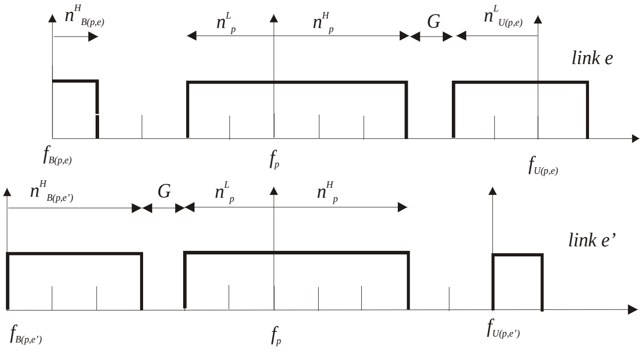

Fig. 1. Using the spectrum slots for connection *p* and spectrum-adjacent connections on link *e* and *e'* in a certain moment of time.

The connections serving time-varying traffic require a dynamic allocation of slots. In the case of traffic increase the spectrum of the connection can be increased by reservation of additional slots, whereas in the case of reducing the traffic the spectrum of the connection can be decremented by a release of certain slots. To determine the effect of time-varying traffic on the network blocking probability in [4], two schemes of increasing/decreasing the number of slots of the connection are proposed. In the first one, named as *Constant Spectrum Allocation* scheme (CSA), the slots for connection *p* may be occupied from reference frequency f_p to reference frequency $f_{U(p,e)}$ of upper spectrum-adjacent connection to connection *p* on link *e*. Thus, the range of variability of slots in this scheme is [4]:

$$0 \le n_p^H \le N_p^H \tag{2}$$

where: $$N_p^H = \min_{e \in p}\left(f_{U(p,e)}\right) - f_p - G \tag{2a}$$

It should be noted that for constant range of slots number variability n_p^H, ((N_p^H is not a function of the number of lower slots $n_{U(p,e)}^L$ of upper spectrum-adjacent connection to the connection *p*) no slots can be shared between spectrum-adjacent connections on the network links, and therefore, this scheme can be used only for comparison. Request of additional slots will be blocked when $n_p^H = N_p^H$. In the second scheme, named as *Dynamic high expansion-low contraction scheme*, when the transmission rate of connection *p* increases the additional slots are occupied first above frequency f_p until slots occupied by upper spectrum-adjacent connection to connection *p*, i.e. [4].

$$0 \le n_p^H \le N_p^H \tag{3}$$

where: $$N_p^H = \min_{e \in p}\left(f_{U(p,e)} - n_{U(p,e)}^L\right) - f_p - G \tag{3a}$$

In the absence of available slots above frequency f_p, free slots are occupied below frequency f_p , i.e. [4]

$$0 \le n_p^L \le N_p^L \tag{4}$$

where: $$N_p^L = f_p - \max_{e \in p}\left(f_{B(p,e)} + n_{B(p,e)}^H\right) - G \tag{4a}$$

In the absence of a free slot, a request of an additional slot will be blocked. It should be noted that the upper limit N_p^H for additional slots occupied above f_p is the function of the number of lower slots $n_{U(p,e)}^L$ belonging to the upper spectrum-adjacent connection to connection *p*. Moreover, the upper limit N_p^L for additional slots below $f_{p,}$ is the function of the number of upper slots belonging to the bottom spectrum-adjacent connection to connection *p*. It results from the fact that the slots belonging to connection *p*, located both above and below frequency f_p may be shared with slots belonging to the upper and bottom spectrum-adjacent connections respectively to connection *p*.

After a brief presentation of the schemes of use of free slots the problem analyzed in this paper can be defined as a RSA problem, where the streams of connection requests are random (Poisson) with exponential duration of the connections and the required number of slots of these connections varies dynamically in time so as to follow the source transmission rate.

The solution of this problem requires an algorithm that finds a path with the required number of slots around the reference frequency for an arriving connection request , taking into account the possibility of sharing slots, so as to minimize the average blocking probability of the additional slots request.

III. Network Analysis for Time-Varying Traffic

Before the final algorithm that solves the formulated optimization problem, a network analysis is presented on the assumption that the number of slots of the connections varies dynamically in time so as to follow the source transmission rate. Let us assume that the stream of connection requests is Poisson with parameter λ between each pair of nodes (for simplicity), and the duration of these connections is exponential with mean $1/\mu = 1$.Therefore, the average traffic (in bps) between each pair of nodes is $\rho \overline{C}$, where $\rho = \lambda/\mu$ is the traffic in Erl. The analysis of the network is carried out on the basis of Monte Carlo method. For a connection request with *C* units of bandwidth between a pair of nodes *s*, *d* the algorithm solving the dynamic RSA problem, which will be presented in the next section, finds path *p* with the required number of slots n_p around the reference frequency f_p. After obtaining the steady state of the network, an analysis of the network serving time-varying traffic is carried out. This analysis is performed by associating Poisson stream of additional slots requests of intensity λ_p with each connection *p* for the obtained network state. Requests of additional slots result from variability of the transmission rate of the connections. The duration of additional slots is exponential with mean $1/\mu_p = 1$. Then, the analysis is repeated 30 times for different states of the network obtained for the same load. An outline of the network analysis for both schemes of additional slots allocation is given in [5].

A. Network Analysis for CSA Scheme

In the case of the CSA scheme, the incoming request of an additional slot for connection *p* encounters $N_p^H - n_p^H$ slots above the reference frequency f_p , where N_p^H is determined by equation (2a). The blocking probability for this request can be determined based on the first Erlang function as $b_p = E_{1,\, N_p^H - n_p^H}(a_p)$, where $a_p = \lambda_p / \mu_p$. A request of additional slot will be blocked, when $n_p^H = N_p^H$. Knowing all connections in the network state and the blocking probability of an additional slot request for each of them, the average blocking probability of an additional slot request can be determined.

B. Network Analysis for DHL Scheme

In the case of DHL scheme the additional slots are occupied both above and below the reference frequency f_p. The incoming additional slot request encounters $N_p^H - n_p^H$ slots above frequency f_p. In order to simplify this model, it was assumed that all the connections in the network, with the exception of connection *p*, occupy the slots above the reference frequency. Hence, the blocking probability of additional slots requests above frequency f_p can be defined as $b_p^H = E_{1,\, N_p^H - n_p^H}(a_p)$, where $a_p = \lambda_p / \mu_p$. In the case of blocking this request, it will be directed to a free slot below frequency f_p. According to the above adopted assumption, the unoccupied slots on links $e \in p$ below f_p will be affected by the bottom spectrum-adjacent connections too, and therefore, each link $e \in p$ should be considered separately. The blocking probability of additional slot request below f_p can be defined as $b_{p,e}^L = E_{1,\, N_{p,e}^L - n_{p,e}^L}\left(a_p\left(b_p^H + 1\right)\right)$, where: $N_{p,e}^L = f_p - \left(f_{B(p,e)} + n_{B(p,e)}^H\right) - G$. The first component of argument $a_p b_p^H$ is the lost traffic above frequency f_p and the second component a_p is the traffic resulting from the additional slot requests generated by a bottom spectrum-adjacent connection to connection *p* on link *e*. Finally, the blocking probability of additional slot request on path *p* can be written as $b_p = b_p^H\left[1 - \prod_{e \in p}\left(1 - b_{p,e}^L\right)\right]$. Knowing all connections for a given state of the network and the blocking probability of additional slot requests for each of them, average blocking probability of additional slot requests can be determined.

IV. Solution of Dynamic RSA Problem

To solve the dynamic RSA problem a heuristic algorithm, called the Largest Segment Path algorithm (LSP) is proposed. The general rule of this algorithm is as follows: for each pair of nodes a set of *k* shortest paths, measured by number of lines is determined off-line. Paths in this set are sorted in ascending order. To determine a set of the shortest paths, the algorithm based on the Latin Multiplication [6] was used, with the computational complexity function equal to $O(|N|^4)$ when the algorithm determines all paths between each pair of nodes until Hamiltonian path (if any). For incoming requests between the pair of nodes *s, d* the aggregated spectrum S_p for each path *p = 1..k* is designated. Then, the spectra of these paths, starting with the shortest path, are searched for to find the largest set of available slots $S^{\max}$. Path *p* with largest $S^{\max}$, such that $|S^{\max}| \geq n_p + G$ is selected for implementation of the request. If the cardinality of the set of slots $|S^{\max}| > n_p + G$, then $fs = a^{\max} + 1$ will be the first slot for implementation of an arriving request, while the last slot $ls = fs + n_p + G - 1$. $a^{\max}$ is the first slot of the largest set of available slots $S^{\max}$. Moving the first slot (if possible) facilitates implementation of an additional slot for connection *p* or spectrum-adjacent connections. Whereas, when$|S^{\max}| = n_p + G$ then $fs = a^{\max}$ and $ls = fs + n_p + G - 1$. The required number of slots n_p is allocated above the reference frequency f_p ie.: $n_p^H = n_p$ and $n_p^L = 0$ (before introduction of traffic variations to connection *p*). In the absence of slots available for the connection the request is rejected. Below, the LSP Algorithm solving dynamic RSA problem is shown.

Input: Graf *G(N, E)*, designated set of *k* shortest paths, measured by number of links for each pair of nodes *s, d* . The connection request with *C* units of bandwidth (in b/s).

Output: Path *p* with required number of slots n_p around the reference frequency f_p

```
LSP algorithm;
{ On the basis of (1) determine the number of slots $n + G$}
for $p \leftarrow 1$ to $k$ do
    for each link $e \in p$ do
        $S_p \leftarrow S_p \cap S_e$ { spectrum aggregation }
    end for
end for
$S^{\max} \leftarrow \max_{p,l}\{S_p^l : p = 1,2...,k;\ l = 1,2,...L_e\}$;
if $|S^{\max}| \geq n_p + G$ then
    if $|S^{\max}| > n_p + G$ then
        $fs \leftarrow a^{\max} + 1$ ; { $a^{\max}$ is the first slot of the $S^{\max}$ }
    else $fs \leftarrow a^{\max}$;
        $ls \leftarrow fs + n_p + G - 1$; { $ls - fs + 1 = n_p = n_p^L + n_p^H$ }
    end if
else Blocking
end if
Return $p, f_p, n_p$;
```

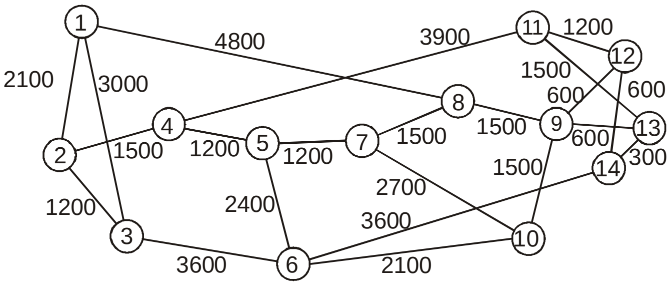

Fig. 2.Topological structure of the network

Assuming that the computational complexity of determining an aggregate spectrum of the path is $O(|N||T|)$ the computational complexity of the proposed algorithm is $O(k|N||T|)$.

V. The Obtained Results

The study of the proposed algorithm for the formulated dynamic RSA problem has been performed for the network shown in fig. 2 [1]. The network consists of 14 nodes connected by links and each of them includes *T* slots. The edges in the graph represent a pair of oppositely directed lines, while their weight determine the actual length. Assuming that each node may be an input and output node, 196 pairs of nodes can be distinguished in the network. The study of the network has been based on simulation using the Monte Carlo method. In the considered model it was assumed, for simplicity, that a stream of connection requests between each node pair *(s, d)* is a Poisson with parameter λ and the duration of the connection is an exponential with the average $1/\mu = 1$. Bandwidth of connection requests is distributed uniformly from 30 to 90 Gbps, with the mean equal to $\overline{C}$ = 60 Gbps. A network simulation was carried out for short-lived requests, i.e. that the requests are set up and disconnected. The results are recorded after obtaining the steady state of the model. To obtain averaged results, a simulation run has been repeated 30 times for each load of the network. In addition, it is assumed that the symbol rate *R* = 2.5 Gbaud and the number of bits per boud is *m*=2. The results were compared with results obtained by a well-known MSP algorithm, which provides the lowest probability of blocking from the algorithms presented in [1]. MSP algorithm solves the dynamic RSA problem i.e. the one where the connections have a constant bit rate. In fig. 3. the blocking probability of the connection requests (in logarithmic scale) depending on the offered traffic to the network (Tb/s) for both compared algorithms, assuming *T* = 350 slots on the each links of the network, has been shown. From the figure it follows that the proposed LSP algorithm provides blocking probability comparable to MSP algorithm for both 3 and 5 the paths for a large range of the traffic offered to the network. Thus, the following question arises: what is the optimal number of the searched paths in order to minimize the blocking probability of the connection requests, assuming that the largest segment in the aggregate spectra of these paths is occupied. Determination of the optimal *k* value is very difficult, as it is likely to be dependent on the network topology, the number of slots realized on the network links and the traffic between each pair of nodes. In [7], algorithm EDQR of choosing Label Switched Paths in IP/MPLS network from a designated off-line sequence of *k* paths for each pair of nodes, has been proposed. An upper bound for the optimal number of paths in this algorithm has been determined on the assumption that the optimum value of *k* may not depend on the distribution of the traffic and the offered traffic but depends only on the average link connectivity of the network and the number of possible paths. Basing on these assumptions and a further assumption that the network is a full mesh network, the upper bound for the optimal number of paths *k* is defined as:

$$k < 3.1 + 1.37\log_{10}(|N| - 2) \qquad (8)$$

It should be noted that the latter assumption is unrealistic from the point of view of the real network topology. In further consideration of this paper it is assumed that *k* = 3.

In order to verify the proposed algorithm under time-varying traffic, an analysis of a network based on an analytical and simulation model for each considered scheme of additional slots occupation, has been carried out. To make a reliable assessment of the obtained results, the schemes for allocating additional slots in both the analytical and the simulation model are used for the same network state. In order to estimate the obtained results, an analysis of the network was performed for 30 different states of the network under the same total load. The intensity of additional slot requests λ_p varies in the range from 0.1 to 1.0 ($1/\mu_p = 1$), which means that e.g. for, each connection of the network requests one additional slot. Taking into account the fact that the number of slots realized in different connections, determined according to formula (1), is from 3 to 9, the request for an additional slot for each connection increases the load from 11% to 33% (for the connection). In fig.4, blocking probability of additional slots depending on the intensity of the requests of additional slots for total load equal to 21.6 Tb/s, is shown. The figure indicates that the proposed LSP algorithm rejects definitely fewer additional slot requests then MSP algorithm. For example, for intensity equal to 0.1 for DHL scheme MSP algorithm rejects requests of additional slots with probability 0.356, while the proposed LSP algorithm rejects the requests of additional slots with a probability of 0.005. For loads up to 0.4 the blocking probabilities of additional slot requests for the proposed LSP algorithm is lower than the blocking probabilities of additional slot requests for MSP algorithm by more than one order of magnitude. In other cases, for the load above 0.4 the difference is very significant (several times) too.

The obtained results also indicate that in the case of DHL scheme, which takes into account sharing the same slots by different connections, the blocking probability of additional slot requests is significantly lower than for CSA scheme, for both compared algorithms. It is worth paying attention to the accuracy of the presented schemes in comparison with simulation models. Figure 4 shows that for smaller intensity of additional slot the accuracy of both schemes: CSA and DHL is good, however, as the intensity of additional slot increases above 0.4 the difference between analytical and simulation models increases.

Fig. 5 shows analogical dependences of the blocking probability of additional slots for both tested algorithms obtained for total load equal to 43.8 Tb/s. Fig. 4 and 5 show that for the whole range of intensity of additional slot requests MSP algorithm rejects additional slot requests with comparable probability regardless of the value of the total network load for both DHL and CSA schemes. In turn, for the proposed LSP algorithm, the probability of additional slots blocking for the same intensity of additional slot requests increases with the total network load.

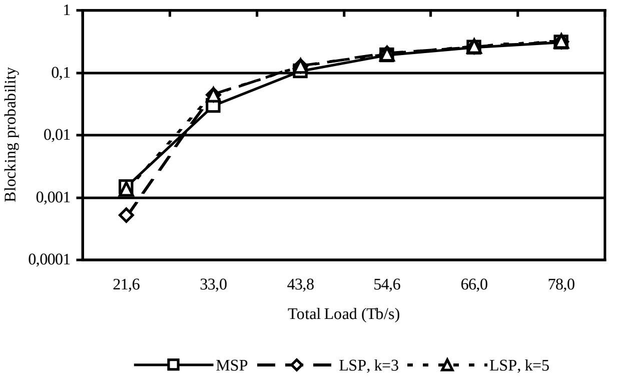

Fig. 3. Number of rejected connection requests depending on the traffic offered to the network (w Tb/s).

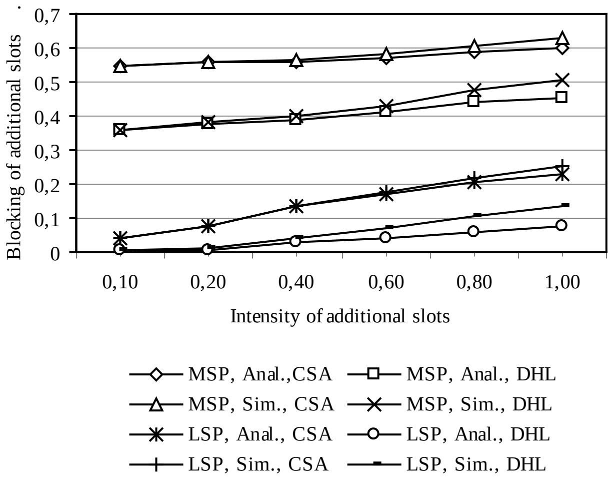

Fig. 4. The blocking probability of additional slots depending on the intensity of additional slot requests for total load equal to 21.6 Tb/s.

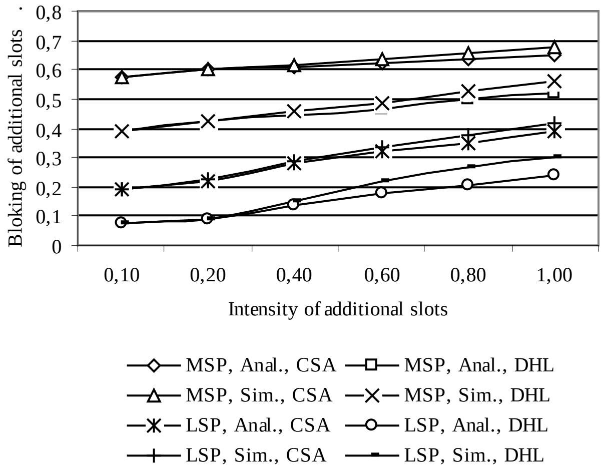

Fig. 5. The blocking probability of additional slots depending on the intensity of additional slot requests for total load equal to 43,8 Tb/s.

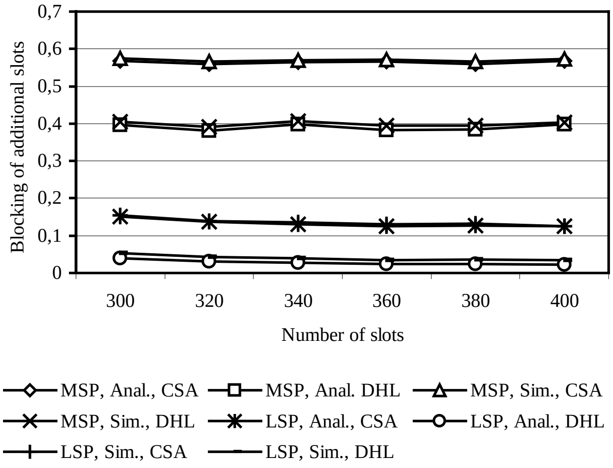

Fig. 6. The blocking probability of additional slot requests depending on the number of slots on each network link.

For example, for the network load equal to 43.8 Tb/s and an intensity equal to 0.1 the blocking probability of additional slot requests for DHL scheme is equal to 0.073, which is fourteen times greater than the blocking probability of additional slot requests for the network load equal to 21.6 Tb/s. While for the intensity equal to 0.4, the blocking probability of additional slot requests are equal to 0.038 for total network load equal to 21.6 Tb/s, and 0.153 for total network load equal to 43.8 Tb/s respectively. It means that the proposed algorithm correctly responds to the increase of the total network load, as opposed to the MSP algorithm.

In turn, fig. 6 shows the blocking probability of additional slots depending on the number of slots on the links of the network, for fixed intensity of additional slot request equal to 0.4. The figure shows that for the proposed algorithm, the blocking probability of additional slot requests decreases with an increase in the number of slots realized on network links which means that the algorithm has the ability to adapt.

VI. Summary and Conclusions

This paper considers the dynamic RSA problem, where the number of slots of the connections varies in time dynamically, so as to follow transmission rate of the sources. In addition, stream of connection requests and duration of the connections are random and are not known in advance.

To describe dynamic changes in the number of slots in the connections, two schemes have been used: the first one takes into account only permanent allocation of slots while the second takes into account the possibility of sharing the slots between spectrum-adjacent connections on the network links. To solve the dynamic RSA problem formulated in this paper an algorithm based on a sequence of the shortest paths, measured by the number of links, is proposed. The proposed algorithm implements the idea of the least loaded path in the set of paths, where the least loaded path is identified as the one for which the aggregate bandwidth has the largest segment enabling the connection realization. To verify whether the proposed algorithm solves the dynamic RSA problem, allocation of predetermined number of connections (short-live) has been carried out to obtain a certain state of the network. Then, a given state of the network random stream of additional slot requests is associated with each connection. To make a reliable assessment of the results, schemes of allocation of additional slots in both the analytical and simulation model are used for the same network state. The obtained results fully confirm that the proposed algorithm reduces (to some extent) the blocking probability of additional slot requests.

At the same time, these results indicate the need for further studies aimed at determining the performance of algorithms, for example prediction algorithms solving the dynamic RSA problem, where the incoming connection requests and the duration of the connections are random.

References

[1] X. Wan, N. Hua, X. Zeng, "Dynamic Routing and Spectrum Assignment in Spectrum –Flexible Transparent Optical Networks,"*J. Opt. Commun. Netw*, vol. 4, August 2012, pp. 603–613.

[2] M. Klinkowski, K. Walkowiak, "Routing and Spectrum Assignment in Spectrum Sliced Optical Path Network," IEEE Communications Letters, vol. 15, August 2011, pp. 884–886.

[3] K. Christodoulopoulos, I. Tomkos, A.E. Varvarigos, "Routing and Spectrum Allocation in OFDM-based Optical Networks with Elastic Bandwidth Allocation". *Telecommunications Conference (GLOBECOM 2010)*, 6-10 Dec. 2010.

[4] K. Christodoulopoulos I. Tomkos, A.E. Varvarigos, "Routing and Spectrum Allocation Policies for Time-Varying Traffic in Flexible Optical Networks," 16th International Conference, *Optical Network Design and Modeling (ONDM)*, 17-20 April 2012.

[5] I. Olszewski, "RSA Problem for Varying Traffic in Flexible Optical Networks,". *Image Processing & Communication*, vol 19, no.1, 2014.

[6] A. Kaufmann, "Graphs, Dynamic Programming and Finite Games," Academic Press, 1967, pp 270-280.

[7] Y. Man-Ching, J. Weijia, Ch. Chi-chung, "Efficient Distributed QoS Routing Protocol for MPLS Networks," *11th International Conference on Parallel and Distributed Systems*, 2005