Routing and Spectrum Allocation Policies for Time-Varying Traffic in Flexible Optical Networks

[1]Konstantinos Christodoulopoulos, [2]Emmanouel (Manos) Varvarigos
1: Computer Science and Statistics Department, Trinity College Dublin, Ireland
2: Computer Engineering and Informatics Department, University of Patras, Greece

Abstract— **We consider the problem of serving dynamic traffic in a spectrum flexible optical network, where the spectrum allocated to an end-to-end connection varies dynamically with time so as to follow the required source transmission rate. In the proposed framework, each connection is assigned a route and is allocated a reference frequency over that route, using an appropriate Routing and Spectrum Allocation (RSA) algorithm, but the spectrum it utilizes around the reference frequency is allowed to expand and contract to match the source rate fluctuations. To perform this function, we propose two spectrum expansion/ contraction (SEC) policies and we develop models for calculating the network blocking probability for these policies. We then present an iterative RSA algorithm that takes into account the developed blocking models and identifies the routes and the reference frequency for the connections so as to minimize the average blocking of the network.**

Keywords- ***Spectrum-flexible networks, Optical OFDM, time-varying traffic, spectrum sharing, spectrum expansion/contraction policies, routing and spectrum allocation, blocking probability.***

I. INTRODUCTION

Increasing the capacity and improving the efficiency of optical transport networks has been an important research challenge for many years. To cope with traffic increases of almost 40% per year, research efforts have been devoted on advanced modulation formats and digital equalization in the electronic domain to enable per-channel bandwidths of 40 and 100 Gbps with improved transmission distance in traditional WDM systems. However, although wavelength routed WDM networks offer well-known advantages, their rigid and coarse granularity leads to inefficient capacity utilization, a problem expected to become more severe with the deployment of higher channel rate systems.

In order to address the issues of stranded and underutilized bandwidth, low agility, inefficient resource utilization due to over-provisioning, and wasted capital/operational expenses, a new networking approach is required. Optical Burst Switching (OBS) and Optical Packet Switching (OPS) utilize the time domain to enable the sharing of the network resources and statistical multiplexing gains. However, OPS can be viewed as long-term solution, since its enabling technologies are still maturing [1], while the few commercial OBS products for ring networks that were recently released have not yet found market success. In addition to the time domain, exploited in the OBS and OPS paradigms, the frequency is another domain that can be harvested to provide improved flexibility, granularity and efficiency for the optical networks. Typically, wavelength routed WDM networks, as well as OBS and OPS, operate over the ITU-T grid, that is a constant 50-GHz spaced grid. Taking a different approach, recent research efforts have focused on architectures that support variable spectrum connections to obtain flexibility and statistical multiplexing gains in the spectrum domain. *Spectrum-flexible*, *elastic*, *adaptive* or *gridless* are few terms used to describe these architectures [2]-[8].

The Spectrum-sLICed Elastic optical path network ("SLICE") [2]-[3] utilizes optical OFDM to enable spectrum-flexible transmissions. Optical OFDM distributes the data on several low data rate subcarriers (multi-carrier system). The spectrum of adjacent subcarriers can overlap, since they are orthogonally modulated, increasing spectral efficiency. A bandwidth-variable OFDM transponder generates an optical signal using just enough spectral resources with appropriately modulated subcarriers to serve the client demand. Another spectrum-flexible architecture called Flexible-WDM ("FWDM") is considered in [4]. To establish a connection in a spectrum-flexible network, every spectrum flexible optical-cross-connect (OXC), or flexible channel bandwidth OXC as referred to in [5], on the route allocates sufficient spectrum to create an appropriately sized end-to-end optical path. Standardization of a grid with granularity less than the 50 GHz currently used in WDM systems is under discussion in the ITU-T and the Optical Internetworking Forum (OIF).

The introduction of spectrum-flexible networks and non-constant spectrum connections pose new challenges on the networking level, since traditional algorithms designed for fixed-grid WDM systems are no longer applicable. In previous works, we have studied resource allocation in the planning (static) [7] and the operational (dynamic) [8] phases of a spectrum-flexible network. In the present paper we consider in detail the dynamic resource allocation problem in a spectrum-flexible optical network, extending our work in [8]. We assume that the requested rates carried by the connections vary dynamically with time and the network has to accommodate these changes in real time. The relatively few works that have studied the online problem in a spectrum-flexible network [3],[4], consider traffic changes as new connection requests and terminations. For example in [4], scenarios of establishing and releasing new connections of 10 up to 400 Gbps are considered. Given the high capacity that can be supported by a flexible optical transponder, relatively large periods of time will pass until an additional connection needs to be established or released, and so the time frame at which connection establishments or terminations happen is of the order of weeks or months. We adopt a different approach by focusing on the short- to medium-term traffic fluctuations that occur in reality. In our model, changes (usually smooth) in the requested rate happen dynamically, and have to be absorbed by the flexible transponders by changing their utilized spectrum in real time. This is done by expanding (if feasible) or contracting the continuous spectrum allocated to the existing connections.

We envision an elastic and dynamic spectrum flexible network where nodes communicate over adjustable-rate end-to-end connections, without establishing new or releasing old connections unless specifically required. The goal of this paper is to develop a framework for dynamic spectrum sharing among connections, propose basic sharing policies and examine the blocking performance of the resulting network. The proposed

framework can be employed in an OFDM or any other type of spectrum flexible optical network.

In the framework we propose, each connection is assigned a route and a reference frequency by a routing and spectrum allocation (RSA) algorithm. The connection is allowed to expand and contract the spectrum used around this reference frequency so as to follow the required transmission rate and absorb the traffic variations, according to what we call a *spectrum expansion/contraction* (*SEC*) policy. No spectrum overlapping among connections is allowed at any given instance, but the spectrum can be shared among connections at different time instants, yielding multiplexing gains similar to those obtained by the time-sharing of resources in an OBS or OPS network. A similar approach was followed in [6], where connections with negatively correlated rates were placed adjacent. The dynamic SEC policies we propose are more general, enabling the sharing of spectrum among more than just two adjacent connections. Moreover, our methods work for general and uncorrelated traffic. We propose and compare two SEC policies. The first is a simple Constant Spectrum Allocation (CSA) policy that defines the exclusive use of a set of spectrum slots to a connection. This policy, which is adaptive but offers no sharing and no statistical gains among connections, is compared to a Dynamic High Expansion-Low Contraction (DHL) policy that enables the dynamic sharing of spectrum slots among connections. We outline models for calculating the network blocking probability for both the CSA and the DHL policies.

We then present an iterative RSA algorithm that takes into account these blocking models and calculates the paths and reference frequencies that should be used, with the objective of minimizing the overall blocking in the network. In particular, the proposed RSA takes into account the load of each connection so as to identify the adequate slot distance from its upper spectrum- adjacent connections. Then the static RSA algorithm of [7] is used to find the paths and reference frequencies for the connections requiring the previously identified spectrum slots. If the solution found uses more spectrum slots than those supported by the network, we reduce the slots requirements of the connections, until we find a solution that can be supported by the network. We apply the blocking models of the utilized SEC policies to calculate the blocking performance of the network. Moreover, we search among different acceptable static RSA solutions to select the one that minimizes blocking. Our results show that the DHL policy significantly outperforms the CSA policy, by enabling the true sharing of spectrum between adjacent connections.

II. SPECTRUM-FLEXIBLE NETWORK AND DYNAMIC TRAFFIC

We consider a spectrum-flexible optical network, where the spectrum is divided into constant spectrum slots with granularity C in GHz finer than the typical 50-GHz grid used in WDM systems (C =12.5 or 6.25 GHz are discussed in the related standardization activities). The switching granularity of the nodes and the transponders is one slot. The network supports a restricted number of spectrum slots T, determined by the switching window of the OXCs. A spectrum slot is identified by its starting frequency $F\,C+F_0$, F=0,1,…,T-1, where F_0 is the lower frequency supported in the system. To simplify notation, we will use a quantized frequency axis and represent a slot with an integer F, F=0,1,…,T-1.

The traffic of the connections varies as a function of time. A connection is served by a specific path and a set of continuous

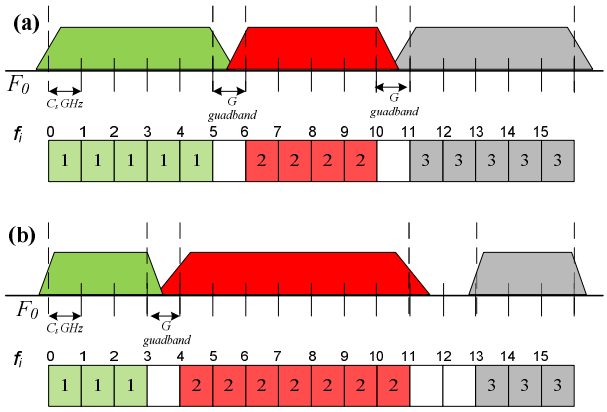

Fig. 1: Spectrum allocation of a link's bandwidth to variable rate connections. Two different time instances are displayed in (a) and (b). Spectrum guardabands, each consisting of G slots, separate the path flows so that they can be routed and received with acceptable BER.

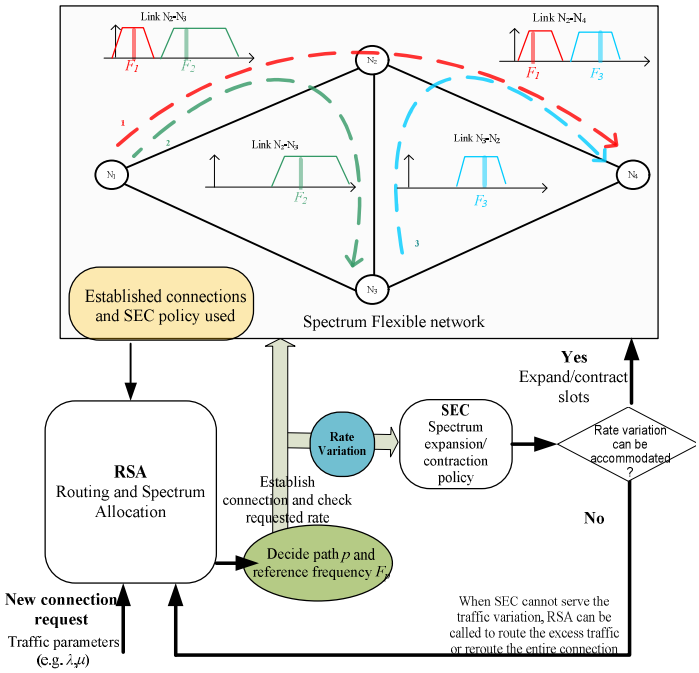

Fig. 2: Flow diagram for serving a connection request. RSA is used to determine the path and reference frequency and SEC policy takes care of traffic variations. When the SEC policy cannot accommodate a traffic variation, or if the rate exceeds the capability of the transponder, RSA can be triggered to set up an additional connection or reroute the existing connection.

spectrum slots on all the links of that path (satisfying the related spectrum continuity constraint), and it can dynamically increase/decrease the spectrum slots it utilizes around a specific reference frequency, so as to follow the variations in the requested traffic rate. Fig.1 presents an example of the utilization of a link in such a network for two different time instances. Between spectrum-adjacent connections, a spectrum guardband equal to G spectrum slots is used to enable the switching of these connections with low interference (G=1 slot in Fig. 1). The way connections adapt their utilized spectrum to their instantaneous traffic rate is called the *spectrum expansion/contraction* (*SEC*) policy.

Network performance does not only depend on the SEC policy used, but also on the arrangement of the connections in the space (routing) and frequency (spectrum allocation) domains. The role of the Routing and Spectrum Allocation (RSA) algorithm can be related to that of the SEC policy as follows. The RSA algorithm serves the connection requests, by assigning paths and reference frequencies to them so as to minimize the average network blocking, taking into account the specific SEC policy used. SEC policy is responsible for

accommodating the traffic variations of the connection. Fig. 2 presents the process of serving a connection. The RSA algorithm is also used when a connection needs additional spectrum slots on a regular basis, or when the requested rate exceeds the transponder capabilities. Then, RSA is called to route the excess traffic over a different spectrum-path, or reroute the entire connection (to save in guardbands).

The RSA algorithms proposed to date assign spectrum-paths to static (constant-rate) connections [2]-[4],[7] , but they can be extended to the case of time-varying traffic. In Section III we present an RSA algorithm that is based on [7] and uses blocking models obtained by our analysis and assigns paths and reference frequencies to the connections, so as to minimize the overall blocking in the network.

A. Spectrum-flexible framework for serving dynamic traffic

The optical network is represented as a graph (***V***,***E***), where ***V*** is the set of nodes and ***E*** the set of fiber links. We consider a connection that has been processed by the RSA algorithm and has been assigned a specific path p and a reference spectrum slot F_p, and utilizes n_p^H and n_p^L spectrum slots higher and lower than F_p, respectively. Therefore, a total of $n_p = n_p^L + n_p^H$ spectrum slots, starting from frequency slot F-n_p^L up to and including slot F_p+n_p^H , have been allocated to the connection on all the links of path p, so as to satisfy the *spectrum continuity constraint*. We will call F_p the *reference frequency* and not the starting frequency, since the connection can utilize spectrum slots lower than that. The total spectrum n_p (in slots) used by the connection is adjusted as a function of time to follow the traffic fluctuations, but no two connections can utilize the same spectrum slots over any link at any given time. This *non-overlapping spectrum assignment constraint* in spectrum-flexible optical networks corresponds to the single wavelength assignment constraint of traditional WDM networks. Fig. 3 presents the spectrum slot utilization of two links, l and l', on path p. We denote by $U(p,l)$ and by $B(p,l)$ the upper and bottom spectrum-adjacent connections, respectively, of the connection p on link l. We also denote by $F_{U(p,l)}$ and by $n_{U(p,l)}^L$ the reference frequency and the number of lower slots utilized by the upper spectrum-adjacent connection, and by $F_{B(p,l)}$ and $n_{B(sd,l)}^L$ the reference frequency and the number of higher slots utilized by the bottom spectrum-adjacent connection on link l. We also denote by G the guardband in spectrum slots used to enable the switching of the connections with low and acceptable interference (G=1 slot in Fig. 1 and 3).

According to the expansion policy, if the traffic of connection p increases, requiring the allocation of an additional spectrum slot to it, we increase either its higher or its lower spectrum slots. Similarly, the used policy decreases the higher or lower allocated slots when the transmission rate of the connection decreases. The non-overlapping spectrum assignment requirement constraints the number of higher and lower spectrum slots that can be utilized by the connection:

$$0 \le n_p^H \le \min_{l \in p}(F_{U(p,l)} - n_{U(p,l)}^L) - F_p - G\,,\ 0 \le n_p^L \le F_p - \max_{l \in p}(F_{B(p,l)} + n_{B(p,l)}^H) - G. \quad (1)$$

Blocking will occur when a connection requires an additional slot (due to an increase in its rate) and there are no available slots to accommodate it. In particular, for blocking to occur for p, an additional slot should be requested when,

$$n_p^H = \min_{l \in p}(F_{U(p,l)} - n_{U(p,l)}^L) - F_p - G, \quad \text{and} \quad (2)$$

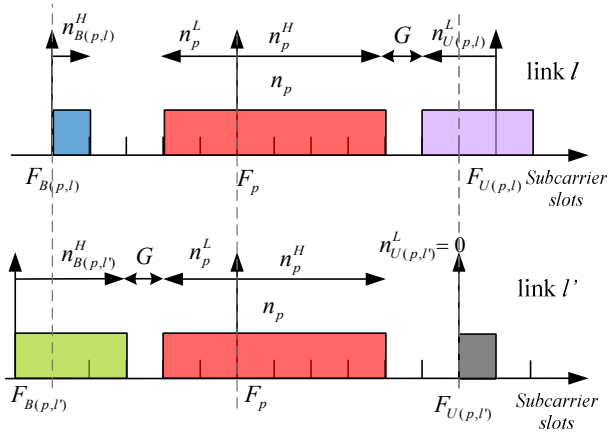

Fig. 3: Example of spectrum slot utilization on two links l and l'. The figure shows the slots allocated to connection p and its upper and bottom spectrum-adjacent connections $U(p,l)$, $U(p,l')$ and $B(p,l)$, $B(p,l')$ on l and l', respectively.

$$n_p^L = F_p - \max_{l \in p}(F_{B(p,l)} + n_{B(p,l)}^H) - G. \quad (3)$$

According to the flow diagram in Fig. 2, if blocking happens too frequently, meaning that the connection needs more spectrum resources than those it shares with its spectrum-adjacent connections, the RSA algorithm could be triggered to route the excess traffic or reroute the entire connection.

Under the proposed spectrum sharing framework, a connection shares the spectrum slots with its upper and bottom spectrum-adjacent connections. In general, spectrum sharing can be performed in different ways and the proposed framework can be extended to include additional rules. For example, we can allocate a number of slots exclusively to each connection and then use a policy for sharing the remaining slots. These options are not ruled out and are left for future studies.

The SEC policy that defines how the spectrum expands/ contracts affects significantly the network's operation and blocking performance. In the next subsection we present two such SEC policies.

B. Spectrum Expansion/Contraction (SEC) policies

1) Constant spectrum allocation (CSA) policy

In the first policy, each connection is assigned a path p and reference frequency F_p and has exclusive use of all spectrum slots higher than F_p, up to the reference frequency of its closer upper spectrum-adjacent connection. That is, connection p can expand and use n_p^H , $0 \le n_p^H \le N_p^H$, higher spectrum slots,

$$N_p^H = \min_{l \in p}(F_{U(p,l)}) - F_p - G. \quad (4)$$

This policy does not enable the sharing of spectrum slots among the connections and is proposed mainly for comparison purposes. In such a system, blocking will occur for connection p when it requires an additional slot, and it has already used up all its higher slots, that is, when $n_p^H = N_p^H$. This is a special case of the general bounding conditions described by Eq. (2) and (3), after setting n_p^L=0 for all connections.

2) Dynamic high expansion-low contraction (DHL) policy

We now present a *Dynamic High Expansion-Low Contraction* (DHL) spectrum expansion/contraction policy that enables the sharing of the spectrum among the connections. With DHL, a connection p wishing to increase its transmission rate, first uses its higher spectrum slots, increasing n_p^H until it

reaches a slot already occupied by an upper spectrum-adjacent connection on some link of p, that is, until the bounding condition of Eq. (2) is met. Then, if additional bandwidth is needed, it expands its lower slots, increasing n_p^L until it reaches a slot that is occupied by some bottom spectrum-adjacent connection on some link, that is, until the bounding condition of Eq. (3) is met. If the connection needs to increase further its rate and there is no higher or lower free slot space, blocking occurs (for the excess rate). Note that the DHL policy performs indirectly slot defragmentation, since it always searches first for free higher slots, even if lower spectrum slots have already been used by that connection, filling the free higher spectrum slots in every chance it gets. Note that spectrum defragmentation has been raised as an issue in other works [3].

When a connection decreases its spectrum slots due to a reduction in its rate, we first release lower spectrum slots and, if these have been reduced to zero, we release higher slots.

C. Analyzing the performance of the SEC policies

As already mentioned, each connection is assigned by the RSA algorithm a specific path p and a reference frequency F_p. The traffic rate of the connection, however, may fluctuate dynamically with time, and the same applies to the number of spectrum slots allocated to it to.

We analyzed the performance of the proposed framework assuming that the requested slots of connections follow a birth-death Markovian model. We also assumed that the additional slot requests are independent for different connections. If the slot requests of different connections were correlated, we could design an RSA algorithm that would take such correlation information into account, so as to obtain gains that may be more significant than those described in our results. We described the states of the network as a d-dimensional continuous time Markov chain, where $d=2\cdot|\boldsymbol{V}|\cdot(|\boldsymbol{V}|-1)$ and $|\boldsymbol{V}|$ is the number of nodes. This can be seen by noting that there are $|\boldsymbol{V}|\cdot(|\boldsymbol{V}|-1)$ possible connections in the network, and for each connection we need to record both the number of higher and lower utilized slots to characterize it. The set of feasible states of the system are described by Eq. (1) and the blocking states by Eq. (2) and (3). To calculate the average network blocking probability in addition to the traffic parameters, we need to know the utilized paths and the reference frequency slots selected by the RSA algorithm for all connections and the SEC policy used. The blocking states for a connection depend on the utilization of its bottom and upper spectrum-adjacent connections over all the links of the path it follows. In turn, the utilization of these connections depends on the utilization of their bottom and upper adjacent connections, and so on. Thus, the interdependence between the connections is rather complicated and cannot be simplified in the general case.

We carried out such an analysis for the proposed CSA and DHL policies. In particular, in the CSA policy no spectrum is shared among the connections, and the Markov chain describing the network state is greatly simplified. This is because the independence among the connections under the CSA policy, makes possible the decomposition of the d-dimensional Markov chain into separate 1-dimensional chains, each corresponding to an M/M/m/m queuing model and describing one connection. Thus, the blocking probability for new slot requests over p is given by the Erlang-B formula. This enabled us to provide models that calculate exactly the average blocking probability of a network under the CSA policy.

In the DHL policy the interdependence of the connections goes deep and the computation of the exact state probabilities is feasible only for small networks, and is intractable for more realistic situations. To address this problem, we developed an approximation model for calculating the probability that a new spectrum slot request over a specific p will be blocked. In the approximation system we assume that the connection p under study follows the DHL policy while all other connections expand their spectrum only towards their higher slots. The proposed approximation simplifies the interdependence among the connections. Since all other connection apart from p utilize only their higher spectrum slots, connection p is affected only by its q bottom spectrum-adjacent connections, and thus only q+1 dimensions play role in calculating the blocking of p. The remaining dimensions (other connections) do not affect connection p nor its bottom spectrum-adjacent connections. So the approximate system can be analyzed as a system that consists of q+1 independent queues, each described by a birth-and-death Markov chain [9]. The stationary distribution of the system can be expressed in product form and thus the approximate blocking probability of connection p can be calculated even for large networks.

III. Routing and Spectrum Allocation Algorithm

In the dynamic scenario with time-varying traffic rates considered in this study, the connections expand/contract their utilized spectrum so as to follow the traffic variations, in the way determined by the SEC policy used. As explained before, network performance does not only depend on the SEC policy, but also on the Routing and Spectrum Allocation (RSA) algorithm used, whose role is to assign the routes and reference frequencies within the available T slots (T is the number of slots supported in the system) so as to minimize the average blocking of the network.

To solve the dynamic (time-varying) RSA problem we transform it into a *static* RSA problem, solve the static problem, apply the blocking models presented above to calculate the network blocking of this RSA solution, and iteratively search for solutions with better blocking performance. The term *static* is used here to refer to the problem that takes as input a traffic matrix with specific number of required slots for all connections and solves the joint optimization problem for all connections.

To formulate the static problem, we initially assume that the CSA policy is used. The blocking performance of an RSA solution for the used SEC policy will be always better or equal to that of the CSA policy, since the latter is the simplest policy and does not permit the sharing of spectrum slots among connections. We assume we are given a blocking threshold B, that is considered acceptable (e.g., $B=10^{-6}$) and we use Erlang-B formula to calculate for each connection p the number N_p of spectrum slots for which the CSA blocking is acceptable. We use the set of N_p values for all connections as the traffic matrix in a *static* Routing and Spectrum Allocation (RSA) algorithm to find a path and a reference frequency slot for all connections. We denote by $T^* = \max_p(F_p + N_p)$ the highest slot allocated to a connection by the static algorithm. If the system can support T^* subcarriers slots ($T^*<T$), the algorithm finishes and we have found an acceptable solution with the CSA policy that does not require spectrum sharing at all (any policy that enables sharing will exhibit better performance). Note that finding a static RSA solution within T slots is NP-hard [7]. In this study we use the heuristic algorithm based on Simulated Annealing of [7] to obtain the static RSA solutions, which can be used to provide solutions in realistic cases. The

values N_p used as input to this static RSA algorithm correspond to the minimum distance of the reference frequency of connection p from its upper spectrum-adjacent connections [N_p^H in Eq. (4)]. If the RSA algorithm does not find a solution within T slots, we iteratively increase the related acceptable blocking threshold B and obtain new values for the number N_p of slots required by each p until we find acceptable solutions. A static RSA solution is acceptable if it utilizes less than the T slots supported by the system. After obtaining an acceptable static RSA solution we take into account the specific SEC policy used and apply the corresponding blocking model to calculate the average network blocking. However, we do not stop the first time we find an acceptable solution within T slots, but we search for different static RSA solutions with the same numbers $\boldsymbol{N}$ of required slots (using Simulated Annealing) or keep decreasing the numbers of required slots until we find K solutions that are acceptable. We select from the K solutions, the one with the lowest network blocking probability. Fig. 4 presents a block diagram of the proposed algorithm.

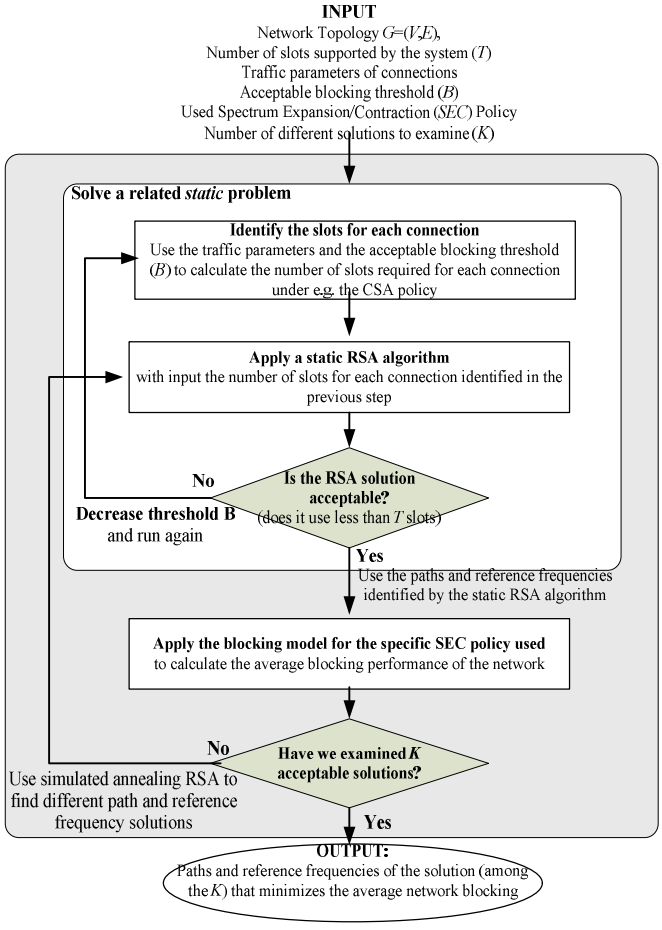

Fig. 4: Block diagram of the proposed algorithm to assign paths and reference frequencies to connection requests.

It is clear that the problem of finding the RSA solution that minimizes network blocking is very complicated. In the general case, the network blocking depends on the paths, the reference frequencies and ordering of the connections, on the expansion/contraction policy, and on the traffic parameters. Even for the simplest CSA policy, where there is no interdependence between connections and each connection can be treated separately, the blocking of a connection is given by the Erlang-B formula, which depends non-linearly on the traffic parameters of the connection. In addition to that, the static RSA problem is known to be NP-hard. The proposed algorithm solves the dynamic RSA problem indirectly. It solves a related static problem, considering the CSA policy, and then applies the blocking models developed for the particular SEC policy used to estimate the performance under dynamic traffic. In the future we plan to examine and analyze more sharing policies and also work on more sophisticated dynamic RSA algorithms that will incorporate more directly the policy blocking models in their formulations.

The proposed iterative RSA algorithm can be also used to serve new connections requests or tackle cases in which the SEC policy is not able to absorb the temporary traffic variations. Remember that the SEC policy is responsible to absorb short and mid-term traffic variations by adapting accordingly the utilized spectrum of the connection. When the average rate of a connection increases substantially and its blocking gets undesirably high, the RSA algorithm is triggered to establish a new connection for the excess traffic or reroute the whole connection (Fig. 2). To serve a new connection request with the proposed RSA algorithm we have two options. We either (i) allow the rerouting of existing connections, or (ii) do not allow the rerouting of existing connections. In case (i) we run the algorithm as described above to find new routes and reference frequency slots for the previously established connections and the new connection. In case (ii) we run the algorithm for only the new connection and fix the paths and reference slots of the already established connections. Assuming prioritized connections we can also have a solution in the middle, in which the new connection is allowed to reroute established connections with lower priorities and not connections with higher. Note that rerouting connections is also an indirect way to perform spectrum defragmentation. A periodic RSA rerouting process (performing full or partial rerouting) can be used to adjust the resources allocated to the connections, in terms of the spectrum space and their neighboring connections, to the long-term evolution of the traffic in the network.

IV. Performance Results

In this section we present performance evaluation results for serving traffic with time-varying rates in a spectrum-flexible network under the proposed spectrum sharing framework, for the SEC policies presented in Section II.B and the RSA algorithm described in Section III.

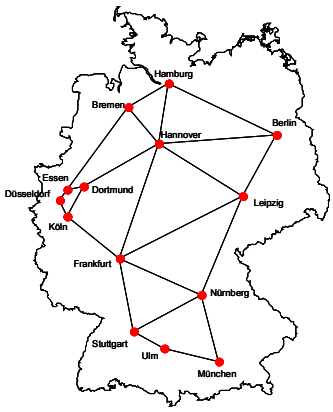

Fig 5: The generic DT network topology.

We performed experiments using a realistic topology based on the 14-node generic Deutche Telecom (DT) network (Fig. 5). We assumed that communication is performed among all source-destination pairs in the network. Spectrum slot requests for each source-destination pair p are generated according to a

Poison process of rate λ_p and their duration is exponentially distributed with mean $1/\mu_p$=1. The arrival rate λ_p for the slot requests of each connection p is drawn from an exponential distribution with mean λ. Thus, $\lambda \cdot |V| \cdot (|V|-1)$ is the total average network load in Erlangs, where $|V|$=14 in the specific case.

We graph the blocking performance of the CSA and DHL policies as calculated using the developed analytical models (exact for the CSA policy and approximate for the DHL policy). For the same traffic scenarios, we conducted full network simulation experiments and we also graph the corresponding blocking probability returned by the simulations. For comparison purposes, we also present the blocking performance of a network that does not follow the framework and SEC policies presented here, but supports the full sharing of all spectrum slots among the connections. This type of network can be viewed as a typical WDM network with spectrum slots corresponding to wavelengths, with the additional constraint of having to use spectrum guardbands between spectrum-adjacent connections. This reduces to a WDM network with $T/(1+G)$ wavelengths, where T is the number of spectrum slots supported in the network. We used the analytical models developed in [10] to compute the blocking of such a WDM network under the fixed alternate routing and random wavelength allocation RWA policy, and we also performed the related simulation experiments. We have set G=1 slot, which corresponds to the minimum guardband requirement; the performance of the WDM network for higher values of G is expected to be worse.

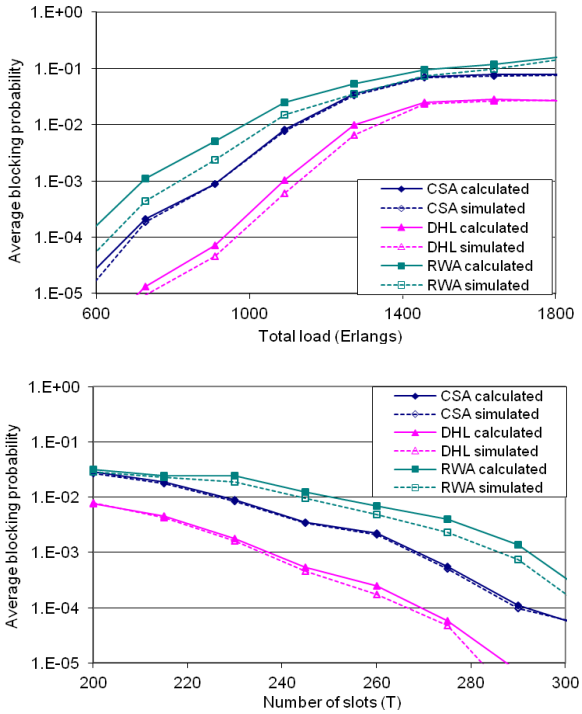

Fig. 6: Average blocking probability for the DT network as a function of (a) the total load, assuming T=250 slots and (b) the number of spectrum slots T, assuming 1000 Erlangs total load.

Fig. 6 presents the results obtained for the DT network. In Fig. 6a we graph the network blocking performance as a function of the total load (in Erlangs) assuming T=250. We observe that the proposed analytical models for calculating the blocking probabilities of the CSA and DHL policies are in very close agreement with the corresponding simulation results. The blocking model for the CSA policy, which reduces to the Erlang-B formula, does not involve any approximating assumptions, and thus we expected to have such a good accuracy. Our simulations show that the approximation model developed for the DHL policy is also very accurate. Recall that the DHL policy allows connections to also utilize their lower spectrum slots after they have utilized their higher slots, and therefore allows the full sharing of spectrum with the adjacent connections. The network blocking probability of the DHL policy is lower than that obtained for the CSA policy more than one order of magnitude. This is the gain that we obtain by enabling spectrum slot sharing among spectrum-adjacent connections, as done with the DHL policy. The performance of the WDM network and the corresponding RWA algorithms utilizing $T/2$ wavelengths (remember that G=1) is worse than the proposed solutions. The used analytical model for the RWA blocking [10] is very accurate for high traffic loads, but its accuracy deteriorates slightly for lower load values. Fig. 6b presents the performance of the network as a function of the number of spectrum slots T supported, assuming a total network load of 1000 Erlangs. Again we observe that the proposed DHL policy outperforms the CSA policy and that the WDM system exhibits the worse performance.

V. CONCLUSIONS

We considered the problem of serving dynamic traffic in a spectrum-flexible optical network where the spectrum allocated to a connection varies so as to follow its time-varying transmission rate. We presented a framework for serving dynamic traffic in such a network that assigns to each connection a route and a reference frequency. The connection is allowed to expand and contract the spectrum that it utilizes around this reference frequency. We proposed two spectrum expansion/contraction (SEC) policies and outlined our analytical models for computing the network blocking performance under these policies. We presented an iterative RSA algorithm that solves the static RSA problem and then applies the developed model to calculate the related network blocking performance. The performance of the network under the proposed framework was shown to be superior than that of a related WDM network that enables full sharing of slots among the connections with the additional requirement of having to use spectrum guardbands between the connections.

REFERENCES

[1] J. P. Jue, W. Yang, Y. Kim, Q. Zhang, "Optical packet and burst switched networks: a review", IET Communications, 3 (3), 2009.

[2] M. Jinno, et. al., "Spectrum-efficient and scalable elastic optical path network: architecture, benefits, and enabling technologies" IEEE Com. Mag., 47 (11), 2009.

[3] T. Takagi, H. Hasegawa, K. Sato, Y. Sone, B. Kozicki, Hirano, M. Jinno, "Dynamic Routing and Frequency Slot Assignment for Elastic Path Networks that Adopt Distance Adaptive Modulation", OFC 2011.

[4] A. Patel, P. Ji, J. P. Jue, T. Wang, "Routing, Wavelength Assignment, and Spectrum Allocation in Transparent Flexible Optical WDM (FWDM) Networks", Photonics in Switching, PDPWGI, 2010.

[5] S. Gringeri, B. Basch, V. Shukla, R. Egorov, T. Xia, "Flexible Architectures for Optical Transport Nodes and Networks", IEEE Com. Mag., 48(7), 2010.

[6] G. Shen, Q. Yang, S. You, W. Shao, "Maximizing time-dependent spectrum sharing between neighboring channels in CO-OFDM optical networks", ICTON 2011.

[7] K. Christodoulopoulos, I. Tomkos, E. Varvarigos, "Elastic Bandwidth Allocation in Flexible OFDM-based Optical Networks", IEEE/OSA Journal of Lightwave Technology, 29(9), 2011

[8] K. Christodoulopoulos, I. Tomkos, E. Varvarigos, "Dynamic Bandwidth Allocation in Flexible OFDM-based Networks", OFC, 2011

[9] D. Bertsekas, R. Gallager, "Data Networks", 2nd ed., Prentice Hall, 1992.

[10] A. Sridharan, K. Sivarajan, "Blocking in All-Optical Networks", IEEE/ACM Trans. on Netw., 12 (2), 2004.