Analytical Modeling of Survivable Anycast Communication in Optical Networks

Yan Cui, Vinod M. Vokkarane

Analytical Modeling of Survivable Anycast Communication in Optical Networks

Yan Cui [1] and Vinod M. Vokkarane [2]

[1] University of Massachusetts Lowell, Lowell, MA 01854
[2] University of Massachusetts Lowell, Lowell, MA 01854
Yan_Cui@student.uml.edu
Vinod_Vokkarane@uml.edu

Abstract. Network resources are imperfect and vulnerable to failure from a wide variety of sources. Survivability is a well-researched field that focuses on strategies to prevent or reduce the harm inflicted when network elements fail. Solutions tend to either provision resources, such as backup paths, proactively so that traffic can be switched to the alternative route after a failure, or quickly find new resources to provision after failure event occurs. Current survivability solutions guarantee protection against these failures, but there is no mathematical model to calculate the network blocking probability for survivability solutions of anycast communication. In this paper, we developed new analytical models to calculate network-wide blocking performance for anycast survivability approaches. Performance results show that our models are accurate and are verified by extensive simulation results.

Keywords: Survivability, Analytical Model, WDM Networks, Anycast.

1 Introduction

In recent years, with rapid growth in demands on network connections, the optical network, acting as the foundation of network connectivity, have been becoming more and more indispensable and important to our daily life. Hence, failures in optical networks may cause catastrophic disasters. Those network failures happen on both network nodes and network links are common due to the human error, such as fiber cuts during construction accidents [1] and natural disasters. The arrival of Hurricane Sandy in New York and New Jersey in October 2012 resulted in the failure of three hundred Verizon facilities along the eastern seaboard [2]. Other unavoidable natural disasters, such as the catastrophic destruction brought about by 2011 Tohoku earthquake and tsunami in Japan [3], can occur, often without warning. Therefore, the ability of recovery of network connectivity, which is called network survivability [4], is of significance in the design of modern networks.

Regarding traffic engineering strategies, it can be beneficial to use different transmission techniques with respect to the characteristics of realized demands. Nowadays, the conventional transmission paradigm is unicast, i.e., data transmits from a source node to a destination node. However, the unicast paradigm cannot accommodate the novel distributed network applications, e.g., content distribution and Data Center (DC).

In the distributed network applications, available network services are provided by more than one network service providers (e.g., the DCs). In order to support these services, anycast could be applied which refers to the transmission of data from a source node to any one member in the candidate destination set [5]. The anycast client can establish a connection with any of the available DCs and selects the target DC based on different network performance criteria (e.g., DC response time, distance to DC, DC load, etc.). As a consequence, anycast is capable of improving network performance, remarkably reduce the network load and may also provide protection against the selected the target DC failure [6].

The designs of survivable networks are often modeled as the linear programming problem with graph theory, wherein, the nodes represent the network components (such as computers, routers, etc.), and edges represent the communication links between the components. Therefore, the survivable network design problem can be modeled as a problem of finding a subgraph satisfying certain connectivity constraints, or augmenting a given network to certain connectivity requirements [7]. In particular, the input is an undirected graph (or digraphs) with weights on the edges or nodes and prescribed demands on connectivity between nodes in the graph with the objective being the computation a subgraph of minimum weight that satisfies the connectivity demands.

There are mainly a drawback in the existing works on design of survivable networks, 1) authors are mainly focused on the design of optimal network survivability algorithms without considering the negative effects caused by new designed survivability algorithms. For instance, by selecting a subgraph for a pair of source and destination, there will be less available network resources for other traffics. This might cause severe network congestion when the amount of traffics is large.

In this work, we provide the theoretical analysis demonstrating the network-wide block rate with considering the survivability algorithms for anycast traffics. We assume two protection policies for anycast traffic networks. One is called survivable routing policy (SRP); The other is called survivable routing with relocation policy (SRRP). In the first scheme, two link-disjointed path are allocated to each pair of traffic source and destination. For efficient resource provision, in the second scheme, the Anycast connection is composed of two link disjointed routing paths between an anycast client and two same content DCs, wherein one path is used as the backup path just in case the primary path that carries the data fails.

The remainder of this paper is organized as follows: Section II introduces the network model and assumptions, and we describe the proposed blocking probability analytical model in Section III. Numerical evaluation and model verification are discussed in Section IV, and Section V concludes this paper.

2 Network Model and Assumptions

We consider a stochastic connection request arrival process and model connection arrivals in the network as a Poisson process. We also assume that the holding time of connection requests is exponentially distributed. In the analysis, the total offered load of the network is uniformly distributed between different anycast client.

We adopt the first-fit wavelength assignment (FF-WA) policy. In this scheme, all wavelengths are indexed and lowest indexed available wavelength is assigned before a higher indexed wavelength. We also assume that the resource provisioning and allocation for the dynamic connection request starts as soon as the request arrives into the network. The connection requests are holding-time-aware, each providing an exact duration.

Moreover, we assume that full wavelength conversion between all input and output links at all intermediate optical cross-connects is available. This provide the ability of fully making use of available wavelength spectrum for every link in a path.

2.1 Survivable Routing Policy (SRP)

We denote a anycast connection request as $R(s, D)$. Where s is anycast connection request node, and $D = (d_1, d_2, \dots, d_m)$ is a destination set and all candidate destinations are numbered. We assume that a source node s is randomly chosen from a node set and a candidate destination set is randomly chosen from the same node set except the source node for each incoming connection request.

For each source and candidate destination pair, we use Dijkstra's algorithm to find the optimal link-disjointed primary path and backup path. We denote the primary path as $p(s, d_{ip})$, and the backup path as $p(s, d_{ib})$, wherein i is the index of candidate destination. For example, Fig. 1 shows for the anycast client located at node 1, the destination set includes two destinations: node 2 and node 5. For the first destination node 2 , the primary path generated by Dijkstra's algorithm is $p(s, d_{1p})$ and the related link-disjointed backup path is $p(s, d_{1b})$. For the second destination node 5, the primary path and backup path are $p(s, d_{2p})$ and $p(s, d_{2b})$.

Anycast service requires selection of a destination for the candidate destinations. We use a first-fit destination selection (FF-DS) policy. In the FF-DS, all candidate destinations are numbered. Each destination will be checked one by one to verify if there are any available wavelengths for the incoming request. If at least one wavelength is available on each link along the primary and backup paths at a destination, the reservation is successful. Otherwise, the next destination will be checked. If there are no available wavelength on any link along all destinations, the connection request will be blocked. As an example a anycast client at node 1, the first destination node 2 will be checked first, followed by the second destination node 5. If there are no available wavelengths on any link all the two destinations, the anycast request will be blocked.

2.2 Survivable Routing with Relocation Policy (SRRP)

We denote an connection request as $R(s, \mathrm{D})$, where s is the anycast connection request node, $D = (d_p, d_b)$ and d_p is the selected target DC node, and d_b is backup data center node with same content. We assume that each node may be a source node s or a data center node d_p for the incoming connection request. We assume there are n DC nodes provide same content as backup choice. The backup data center node is generated randomly among of the n same DC nodes.

For each source – target DC- backup DC pair, we use Dijkstra's algorithm to find the optimal link-disjointed primary path and backup path. We denote the primary path

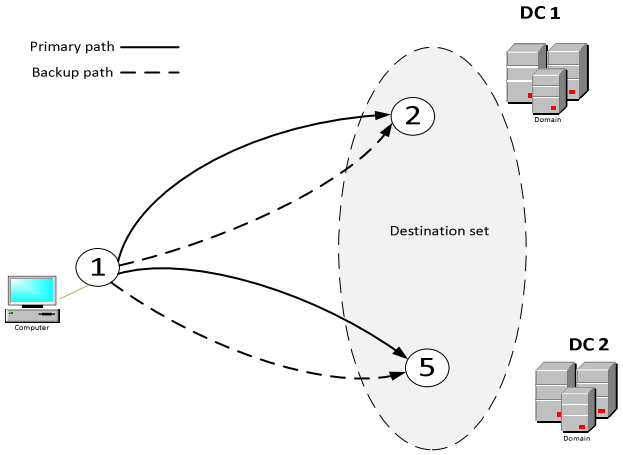


Fig .1. Anycast connection with primary and backup paths for each DC.

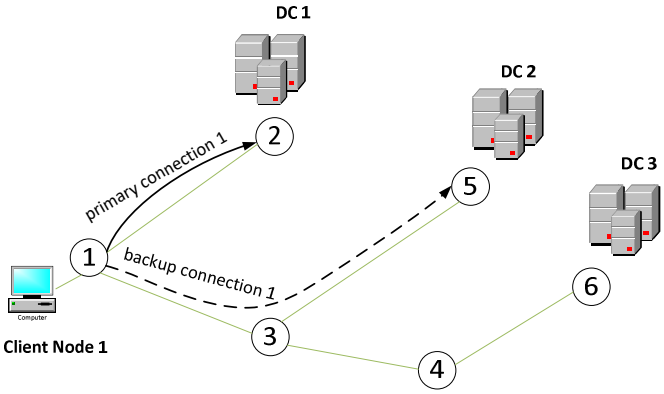


Fig .2. Anycast connection with primary and backup paths.

as $p(s, d_p)$, and the backup path as $p(s, d_b)$. For example, Fig. 2 shows for the anycast client located at node 1, the primary path generated by Dijkstra's algorithm is $p(n_1, n_2)$ and the related link-disjointed backup path is $p(n_1, n_5)$.

In order to cope with link failures, a connection needs to be allocated with a primary path and a backup path. The primary path $p(s, d_p)$ is the working path used to transfer its data from the source s to the destination d_p. The data is rerouted through the backup path in case of a failure on the primary path. We adopt dedicated path protection scheme to define the blocking problem for incoming connection request. When a connection request arrival at the network, the request tries to get resource allocation on the primary path and backup path, if currently there are available resource on each link traversed by primary path or backup path, we call this connection request is allocated successfully. Otherwise, the connection request will be blocked.

3 Analytical Blocking Model

There are two parts in this section. In the first part, we give the computation process of link arrival rates to calculate the link blocking probability. We present our theoretical model on how to calculate the average network blocking probability in the second part.

3.1 Computation of Link Arrival Rate

Survivable Routing Policy (SRP)

Link arrival rate when |D|= 1

This is called unicast traffic, when only one destination is included in destination set for incoming request. Since each node may be a source node or a candidate destination node, we can find that the total number of combinations of source-candidate destination pairs is $v \cdot (v-1)$, if the network has v nodes. Since the total offered load to the network is uniformly distributed among source-candidate destination set pairs, we can derive the arrival rate between a source and a destination as

$$\lambda^{s,D} = \lambda^{s,d} = \frac{\lambda}{v(v-1)} \tag{1}$$

We obtain the arrival rate λ^j for link j by combining the contributions of requests from all primary and backup paths that traverse such a link. Hence,

$$\lambda^j = \sum_{s,d|j \epsilon rp(s,d_p) \; or \; j \in p(s,d_b)} \lambda^{s,d}. \tag{2}$$

Link arrival rate when |D|>=2

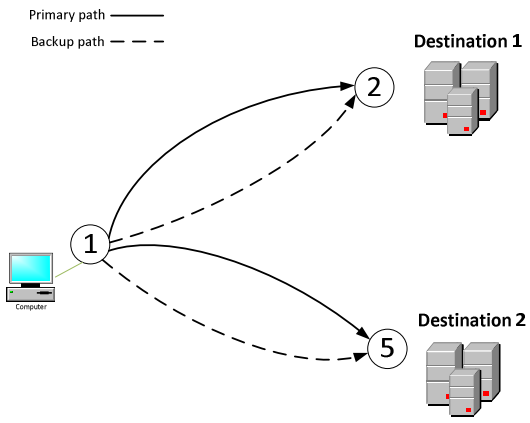
Each source-candidate destination set pair includes a source node and two destination nodes, which means the size of the route set is 2. As each node in an anycast network may be a source node or a destination node, if a network graph includes v nodes, the number of combinations of source-candidate destination set pairs is $v(v-1)(v-2)$. Since the total offered load to the network is uniformly distributed among source-candidate destination set pairs, we can derive the arrival rate of a route set between a source and candidate destination set as

$$\lambda^{s,D} = \frac{\lambda}{v \cdot (v-1)(v-2)} \tag{3}$$

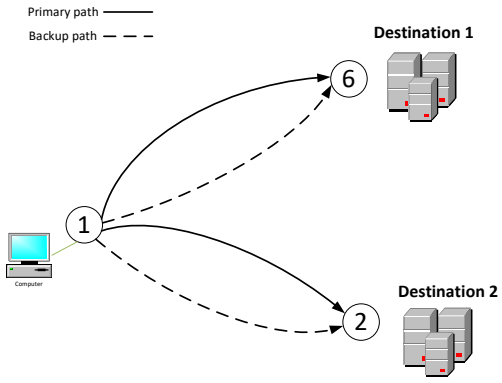
The request to the destination set will arrive at the first destination and attempt resource allocation, so the arrival rate of the first destination is the same as the arrival rate of the route set. However, if the request coming to first destination set is blocked, the request then arrives to the second destination and tries to receive resource allocation. So the contributed arrival rate to the second route is from the requests which are already blocked on the first destination.

In summary, we can derive the arrival rate of each source-destination pair by combining the contributions of requests that arrive at the destination set as

$$\lambda^{s,d} = \sum_{s,D} \lambda^{s,D} + \sum_{s,D} \lambda^{s,D} P^{sd^1}. \tag{4}$$



(a)



(b)

Fig .3. A source destination pair (1,2): (a) node 2 as first destination (b) node 2 as second one

In above equation, the first term is the sum of the arrival rate of source-candidate destination set pairs in which the destination d is the first destination in a destination set. The second term is the sum of the arrival rate of destination sets in which the d is the second destination. as shown in Fig. 3. Considering that the blocking probability P^{sd^1} that one source destination pair is blocked has already been computed in unicast network, we can compute the arrival rate of a source-candidate destination pair using the above equation. We can use Eq. (2) to calculate the link arrival rate after having computed the route arrival rate.

Survivable Routing with Relocation Policy (SRRP)

We denote the total mean arrival rate to the network as λ, the arrival rate for each primary-backup paths set as λ^{s,d_p,d_b}, the arrival rate of primary path between source s and destination d_p as λ^{s,d_p} and the arrival rate of backup path as λ^{s,d_b}. We will derive the link j arrival rate λ^j based on the connection request traversed by link j.

Since each node may be an anycast client node or a target DC node and the backup DC node is fixed based on the target DC node, we can find that the total number of combinations of client-DC pairs is $v \cdot (v-1)$, if the network has v nodes. Since the total offered load to the network is uniformly distributed among client-DC pairs, we can derive the arrival rate between a client node and DC node as

$$\lambda^{s,d_p,d_b} = \lambda^{s,d_p} = \lambda^{s,d_b} = \frac{\lambda}{v(v-1)}. \tag{5}$$

The connection request will go to primary path and backup path and try to get resource allocation. For a route (source-destination pair) in a network generated by route algorithm, as shown in Fig.4, the route may be as a primary path or as backup path to do the resource allocation. We denote a route in a network as $p(s,d)$ and the cumulated arrival rate going through this route as $\lambda^{s,d}$. We can get the arrival rate of a route (source-destination pair) generated by routing algorithm as

$$\lambda^{s,d} = \lambda^{s,d_p} + \lambda^{s,d_b} \tag{6}$$

We obtain the arrival rate λ^j for link j by combining the contributions of requests from all routes $p(s,d)$ that traverse such a link. Hence,

$$\lambda^j = \sum_{s,d|j\epsilon r(s,d)} \lambda^{s,d}. \tag{7}$$

3.2 Network-wide Blocking Model

The average generalized network blocking model is obtained in three steps. First, we provide a link blocking model based on Erlang-B model. We then present the primary and backup path set blocking computation. After having computed primary and backup path set blocking, we can calculate the average network blocking probability.

Link Blocking Analysis

If there is no available wavelength for incoming request on a link, the request is called blocked on this link.

We can model a link as a queuing system. We consider the number of wavelengths for each link to be equal and denoted as W and the average holding time of request is τ. We can calculate the blocking probability of link j, denoted as B_j, which is equal to the Erlang loss formula [9],

$$B^j = B(W, \lambda^j \tau) = \frac{\frac{(\lambda^j \tau)^W}{W!}}{\sum_{k=0}^{W} \frac{(\lambda^j \tau)^k}{k!}}. \tag{8}$$

In the above equation, λ^j represents the arrival rate of link j.

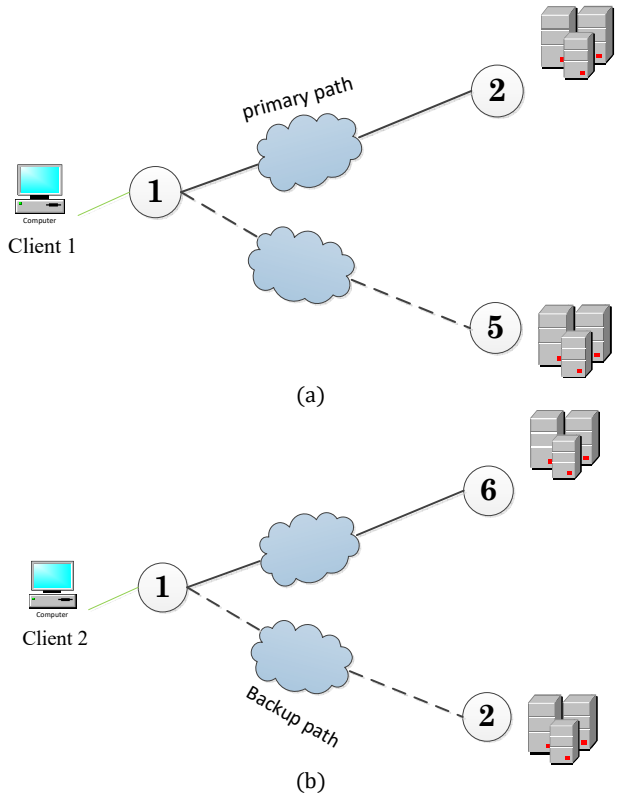


Fig .4. A path $p(n_1, n_2)$ generated by routing algorithm: (a) as a primary path (b) as backup path for different connection request.

Primary - backup Path Set Blocking Computation

Under SRP

- For Anycast$|D| = 1$

One destination node means only one pair of primary and backup paths. We can assume that the wavelength allocation on a path is independent between the links which are traversed by this path. With wavelength converters, different wavelength can be assigned on different links along a path. For survivability, there is at least one available wavelength on each link traversed by primary path and backup path for incoming request to get resource allocation. Considering link disjoint constrain, the probability that a connection request gets blocked which means at least one link along a primary path or backup path has no available wavelength when the connection request arrives to the network is equal to 1 minus the probability that the connection is not blocked in any of the corresponding link j along the primary path $p(s, d_p)$and backup path $p(s, d_b)$, Hence, we can derive the probability that a primary-backup set is blocked as

$$B_{s,D} = 1 - \prod_{\substack{j:j\in p(s,d_p) \\ or\ j\in p(s,d_b)}} (1 - B^j). \quad (9)$$

- For Anycast$|D| = 2$

If the candidate destination set size is two, there are one primary backup path for each destinations. We know there are no common link between primary and backup paths going to same destination. However common links probably happen between paths belongs to different destinations. We classify the links traversed by the all paths of this anycast traffic as three sets: set CL includes common links traversed by the first and second destinations; set L_1 includes links going to the first destination only; set L_2 includes links going to the second destination only. If any link belongs to CL has no available wavelength, the incoming request will be blocked, because the traffic cannot go the first or second destinations. We define this blocking probability as

$$B_1 = 1 - \prod_{j\in CL}(1 - B^j). \quad (10)$$

If all links belongs to CL has at least one available wavelength, but any link belongs to set L_1 and any link belongs to set L_2 has no available wavelength. The incoming traffic is still blocked. We define this blocking probability as

$$B_2 = \left(1 - \prod_{j\in L_2}(1 - B^j)\right)\left(1 - \prod_{j\in L_1}(1 - B^j)\right)\prod_{j\in CL}(1 - B^j). \quad (11)$$

In the above, the two cases are mutually exclusive, so we can sum the probability that each case happens to affect the primary-backup path set blocking probability:

$$B_{s,D} = B_1 + B_2. \quad (12)$$

Under SRRP

We can assume that the wavelength allocation on a route is independent between the links which are traversed by this route. With wavelength converters, different wavelength can be assigned on different links along a route. For survivability, there is at least one available wavelength on each link traversed by primary path and backup path for incoming request to get resource allocation. Considering link disjoint constrain, the probability that a connection request gets blocked which means at least one link along a primary path or backup path has no available wavelength when the connection request arrives to the network is equal to 1 minus the probability that the connection is not blocked in any of the corresponding link j along the primary path $p(s, d_p)$and backup path $p(s, d_b)$, Hence, we can derive the probability that a primary-backup set is blocked as

$$B_{s,d_p,d_b} = 1 - \prod_{\substack{j:j\in p(s,d_p) \\ or\ j\in p(s,d_b)}} (1 - B^j). \quad (13)$$

Network-wide Blocking probability

We can calculate the network wide blocking probability after having computed every individual primary-backup path set blocking probability, which is simply defined as

$$N = \frac{\sum_{s,d_p,d_b} \lambda^{s,d_p,d_b}\cdot\tau\cdot B_{s,d_p,d_b}}{\sum_{s,d_p,d_b} \lambda^{s,d_p,d_b}\cdot\tau}. \quad (14)$$

4 Numerical Results and Analysis

In this section, we assess the analytical blocking model proposed in Section III and compare its performance with simulation results on the 14-node National Science Foundation network (NSFnet) shown in Fig. 5.

In the simulations, we assume a Poisson arrival process with an average arrival rate of λ and an exponential distribution for request holding time with average holding time τ equal to 1. The total offered load is uniformly distributed among source-candidate destination set pairs. For a given simulation set, we change the arrival rate in order to generate the desired offered load ($\rho = \lambda\tau$). The resource provisioning and allocation for a connection request starts as soon as the call arrives into the network. We use the first-fit wavelength assignment and fixed route policy (Dijkstra's shortest path) to determine the link- disjointed primary and backup path for one source-destination pair or one source-target DC-backup DC pair. We use first-fit destination selection (FF-DS) policy for anycast requests to do the simulation. We assume 8 wavelengths on each link to do the simulation. The simulation results were averaged over 30 seeds of 10^6 connection demands each.

Reduced load [8] is a scientific method for the purpose of making theoretical model more close to reality. It is widely adopted in theoretical model of optical networks. To make our work valuable, we all involve reduced load in our analytical models.

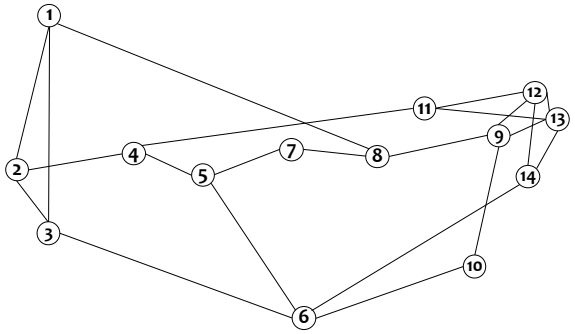


Fig .5. NSF network.

Fig. 6 shows the average network blocking probability performance as a function of different offered load for unicast traffic ($|D| = 1$) in survivability NSFnet. We can observe that the analytical results accurately match the simulation results. As expected, the blocking probability increases as the offered load increases. If the offered load is fixed, the blocking rate for unicast traffic with survivability is much higher than that unicast traffic without survivability algorithm. This is because two link-disjointed paths are provided for each source-destination pair in survivability networks, which needs much more network resource to allocate one single traffic, However the network resource provided are same.

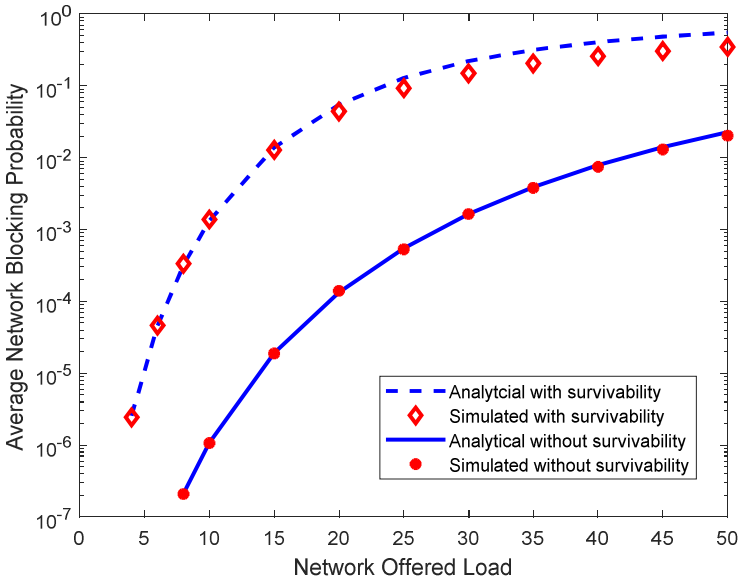


Fig .6. Network blocking comparison between uncast paradigm $|D| = 1$ without survivability and unicast paradigm with survivability.

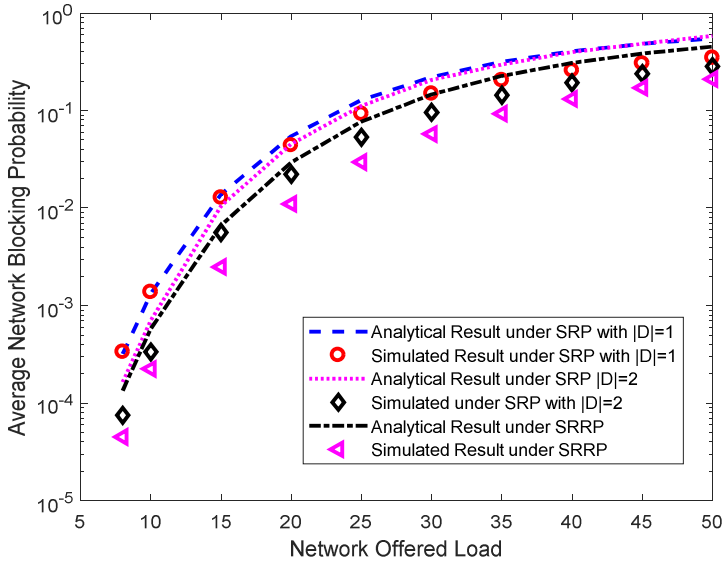


Fig .7. Network blocking probability under SRP and SRRP

Fig. 7 shows the average network blocking probability as a function of different offered load under SRP and under SRRP in NSFnet. We can observe that the analytical results accurately match the simulation results. It is worth noting that comparing the results between $|D| = 1$ and $|D| = 2$ under SRP for the NSFnet with same offered load, and same number of wavelengths on each link, the blocking probability on the latter is lower. This is because increasing the number of candidate destinations means increasing the size of the route set for anycast, providing more opportunities for a request to succeed in resource allocation based on FF-DS policy. To gain more insight in the efficiency of survivable routing with relocation scheme, We can observe that performance under survivable routing with relocation scheme are much better than that of under survivable routing for anycast ($|D| = 2$) paradigm, with same offered load.

5 Conclusion

We presented analytical models to compute network-wide blocking probability for anycast traffic paradigm in survivability optical WDM networks. Results demonstrate that our model provides good accuracy compared to simulation results. The models can be considered a useful design tool for anycast survivability optical WDM networks. For future work, we will work on analytical models for many-to-many traffic paradigms in survivability networks [7].

References

1. E. Modiano and A. Narula, "Survivable lightpath routing: A new approach to the design of WDM-based networks," IEEE J. Sel. Areas Com., vol. 20, no. 4, pp. 800–809, May. 2002.
2. A. Kwasinsk, "Hurricane sandy effects on communication systems," The University of Texas at Austin, Tech. Rep. PR-AK-0112-2012, Dec. 2012.
3. T. Adachi, Y. Ishiyama, Y. Asakura et al., "The restoration of telecom power damages by the Great East Japan Earthquake," in Telecommunications Energy Conference (INTELEC), 2011 IEEE 33rd International, Oct 2011, pp. 1–5.
4. R. J. Ellison, D. A. Fisher, R. C. Linger et al., "Survivable network systems: An emerging discipline," Carnegie-Mellon Software Engineering Institute, Tech. Rep. CMU/SEI-97-TR-013, 1999.
5.] K. Walkowiak and J. Rak, "Shared backup path protection for anycast and unicast flows using the node-link notation," in Proc. IEEE Int. Conf. Com. (ICC 2011), Kyoto, Japan, 5–9 Jun. 2011.
6. R. Goścień, K. Walkowiak, and M. Tornatore, ''Survivable multipath routing of anycast and unicast traffic in elastic optical networks,'' IEEE/OSA J. Opt. Com. Netw., vol. 8, no. 6, pp. 343–355, Jun. 2016.
7. D.A.P. Davis and V.M. Vokkarane, "Failure-Aware Protection for Many-to-Many Routing in Content Centric Networks," IEEE Transactions on Network Science and Engineering, Jan. 2019.
8. Y. Cui and V. M. Vokkarane, "Analytical blocking model for anycast RWA in optical WDM networks", IEEE/OSA Journal of Optical Communications and Networking, vol. 8, issue 10, pp. 787-799, 2016.