International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 05, May 2017
www.ijates.com
ijates
ISSN 2348 - 7550

CROSS LAYER NETWORK SURVIVABILITY IN CROSS-LAYER METRICES AND SHORTEST PATH IDENTIFICATION USIG ACO

G. Vijay Srinivasan[1] , Dr. M. Anand Kumar[2]

[1] *M.PhiL Research Scholar, Department of Computer Science*

Karpagam University.

[2]*Dr. M. Anand kumar, Associate Professor, Department of Information Technology*

Karpagam University.

ABSTRACT

In layered networks, a single failure at a lower layer may cause multiple failures in the upper layers. As a result, traditional schemes that protect against single failures may not be effective in cross-layer networks. A cross layer network with logical and physical topologies, the survivable logical topology routing problem is to route each link in the logical layer with a path in the physical topology between the end nodes of logical link such that the logical topology remains connected after a physical link fails. In this paper we introduce the problem of maximizing the connectivity of layered networks. We show that connectivity metrices in layered networks have significantly different meaning than these single-layer counter parts. Results that are fundamental to survivable single-layer network design, such as max-flow, min-cut theorem, are no longer applicable to the layered setting. We propose new metrices to measure connectivity in layered network's and analyze their properties. Using this formulation as a basic building block, we present unified MILP formulations to determine a survivable logical topology routing that also satisfies one of four cross-layer metrices: 1) Minimizing the number of logical links to be added to guarantee the existence of survivable logical topology routing; 2) Maximizing the capacity of the logical topology; 3) Maximizing the connectivity of the logical topology after a physical link failure and 4) Maximizing the minimum cross layer cut. After construction of physical and logical link we select number of optimal paths in the survivable network and also find maximum distance in the network layer using Ant colony Optimization (ACO). ACO is one of the bio-inspired mechanisms. ACO is a dynamic and reliable optimization. ACO algorithm reduces the energy consumption. ACO algorithm reduces the energy consumption. It optimizes the routing paths, providing an effective multi-path data transmission to obtain reliable communications in the case of no faults.

Keywords: *Cross layer networks, Cross-layer survivability, WDM optical networks, Ant Colony Optimization (ACO)*

I. INTRODUCTION

Modern communication networks are constructed using a layered approach. Such a network typically consists of an electronic packet switched network (such as IP); often this packet-switched network is built on top of one or more electronic circuit switched transport networks (e.g., ATM, SONET; sometimes neither or both); and these in turn are built upon a fiber network[1]. We examine this problem in the context of Wavelength Division Multiplexing

(WDM) based networks; although the concepts discussed are equally applicable to other layered architectures (e.g., IP over ATM, ATM over SONET, etc.).

In a WDM-based network the logical topology is defined by a set of nodes and lightpaths connecting the nodes, while the physical topology is defined by a set of nodes and the fibers connecting them. For example, an IP-overWDM network consists of IP routers that are connected using optical (WDM) lightpaths. These lightpaths are routed over the physical fiber topology. Networks often rely on the logical layer for providing protection and restoration services. However, even when the logical topology is designed to tolerate single logical link failures, once the logical topology is embedded on the physical topology, the logical topology may no longer be survivable to single physical link failures. This is because each physical fiber link may carry multiple lightpaths. Hence, the failure of a single fiber link can lead to the failure of multiple links in the logical topology, which may subsequently leave the logical topology disconnected.

In this paper, we focus on assessing cross-layer network reliability. An example of cross-layer network architecture is Internet Protocol over Wavelength Division Multiplexing networks, which is composed of logical and physical (lower-layer, WDM) networks. The demands of a link in the logical network are transmitted through a path connecting the corresponding node pair in the physical network. This logical-link to physical-path mapping is called cross-layer mapping. We will use logical, upper-layer, and IP networks interchangeably, as well as physical, lower layer, and WDM networks. We also refer to the topologies of the IP and WDM networks as logical and physical topologies, respectively.

In a logical topology, nodes and links represent IP routers and links connecting them, respectively. Similarly, physical nodes represent optical cross-connect (OXC) and optical adddrop multiplexer (OADM), while physical edges connecting them represent optical fibers. A lightpath is a cross-layer mapping of a logical link onto a path connecting corresponding physical nodes, through which transmission occurs on a single wavelength thereby bypassing opto-electro-optic (O-EO) conversions on the intermediate nodes of the path.

As a simple illustrative example, consider the physical and logical topologies shown in Figures 1(a) and (b). The lightpaths in the logical topology are routed over the physical topology in two different ways in Figures 2(c) and (d). In Figure 1(c), a failure of physical fiber (1, 5) would cause lightpaths (1, 5) and (3, 5) to fail. Consequently, node 5 will be disconnected from other nodes in the logical topology. On the other hand, in Figure 1(d), the logical topology will remain connected even if one of the fibers fails. The above example demonstrates that in a multi-layer network, a physical link failure can result in multiple logical link failures, and that the routing of the logical links on the physical topology has a big impact on the connectivity of the multi-layer network [1].

In contrast to the simplified example of Figure 1, real-life networks are highly intertwined and layered. However, due to the lack of general understanding of the issues in cross layer survivability, most existing protection and restoration mechanisms are based on principles that are applicable only to single-layer network environments, and are subject to cross layer issues as illustrated above.

To the best of our knowledge, this is the first paper that formally studies classical survivability theory in the context of layered networks. We show that standard survivability metrics, such as the minimum cut and maximum disjoint paths that have been widely used in characterizing the survivability properties of single-layer networks lose much of their meaning in the context of cross-layer architecture. In particular, the MaxFlow Min-Cut Theorem, which constitutes the foundations of network survivability theory and provides the mathematical justification of the

aforementioned metrics, no longer holds in the cross-layer context. Such a fundamental difference suggests that many basic issues of cross-layer survivability are largely not understood [3].

ACO is a part of swarm intelligence (also known as collective intelligence) which is inspired from the collective behavior of ants living in colonies in finding shortest path between nest and food source. The novelty of this foraging behavior of ants rises from the fact that the collective behavior of some unintelligent decentralized small entities results in intelligent outputs. ACO tries to mimic real ant actions to solve combinatorial optimization problems [4] .The ACO structure is composed of a set of agents also known as ants, randomly situated in the environment which is supposed to be a graph made up of nodes and arcs. According to agents' properties, these ants are capable of moving, sensing and acting in the environment. As ants take any random path a kind of chemical substance, known as pheromone which is detectable by other ants is laid on the trail. As pheromone accumulates when a path is used by multiple ants and as it evaporates by the time, and furthermore as ants tend to choose the path with higher amount of pheromone, the shortest path is selected. According to the extended Bridge Experiment (Goss et al., 1989) it is observed that path selection is biased towards the shortest path, since ants which follow the shortest path return to the nest earlier than ants on the longer path. The pheromone on the shorter path is therefore reinforced sooner than that on the longer path.

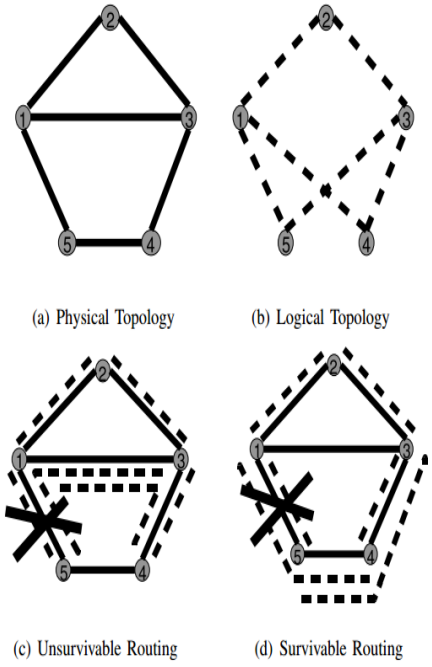


Fig. 1. Different lightpaths routings can affect survivability

II. EXISTING WORK

2.1 A Scalable approach for survivable topology

The survivable virtual topology routing problem is to route a virtual topology graph on a optical fiber physical topology such that the virtual topology remains connected when failures occur in the physical topology. In this work we study the problem of survivable virtual topology routing under single node/SRLG (Shared Risk Link Group) failure model. We prove that the survivable virtual topology routing problem under node/SRLG failures is NP-

complete. We present an improved integer linear programming (ILP) formulation for computing the survivable routing of a virtual topology graph. However, ILP is not scalable when the network size scales more than a few tens of nodes. In this work, we present sub-classes of graphs which more accurately model an actual network and for which a survivable routing can be easily computed solving an ILP. We successfully computed the survivable routing of virtual topologies belonging to these sub-classes against link/SRLG failures for topologies of size up to 24 nodes [5].

2.2 Survivable Virtual Topology Routing

Let us now discuss the SVTR problem. The physical topology is represented by Gp = (Vp, Ep) where Vp is the set of nodes in the physical topology and Ep is a set of bi-directional fiber links between nodes (i, j) ∈ Vp. A bidirectional fiber link is a pair of fiber links where each fiber is dedicated to carry data in a particular direction opposite to the other fiber. The SRLGs on the physical topology are defined by Rp = {ri|ri = {ei,1, ei,2,...ei,m}, $1 \leq j \leq m$,(ei,j ∈ Ep and that they share the same risk of simultaneous failure)} where ri is the i th SRLG and ei,j is the jth edge in the SRLG ri. Each link in the physical topology belongs to at least one SRLG in the set Rp. This assumption is based on the fact that every physical link passes through some conduit (at least one of its own) and is a possible source of failure. To model node failures using SRLG, all the links incident on the node are grouped into a single SRLG. The virtual or logical topology is a graph Gl = (Vl, El) where Vl ⊆ Vp and link (i, j) ∈ El represents logical bi-directional link between nodes i, j ∈ Vl. Not all the nodes in the physical topology need to be present in the virtual topology. Some of the nodes are just tapping points. A tapping point is a node in the network such that it is not a source or destination for any connection request.

To route a virtual topology on a physical topology, for each link in the virtual topology, we need to find a path/route in the physical topology. Both the fiber links in the physical topology and logical links in the virtual topology are bidirectional. We assume that both topologies are undirected and compute a route between the given pair of nodes. The direction is immaterial as the same path can be used to route the connection in both directions [7].

Given the physical topology Gp, the SRLG Rp and the virtual topology Gl we wish to determine a routing of the virtual topology such that in the event of failure of any single SRLG in the physical topology, the virtual topology is still connected. Such a routing is called SRLG survivable routing. In the rest of the document 'survivable' refers to 'SRLG survivable' unless specified explicitly. Let us illustrate the survivable virtual topology routing problem using Fig. 1. Fig. 2(a) shows a physical topology with SRLG. Links (a, b) and (b, f) belong to the SRLG r1 (indicated by dashed ovals). Similarly SRLG r2 and r3 containing two links each are shown in Fig. 2(a). Consider the virtual topology shown in Fig. 2(b). For each link in the virtual topology there are many different paths for routing the link on the physical topology. As shown in Fig. 2(b), the virtual link (b, e) is routed on the physical links labeled 3 and 6 in the physical topology. Similarly, the physical route of other virtual links is shown in Fig. 2(b). This routing is survivable against SRLG failures. If the link (b, e) of the virtual topology in Fig. 2(b) were routed on the links 1 and 5 (not shown in figure), then failure of SRLG r1 will result in the failure of the virtual links (a, b) and (b, e). Therefore routing the virtual link (b, e) on the links 1 and 5 results in a routing that is not survivable. Survivable routing of a virtual topology exists if there exists at least one routing of the virtual topology that is survivable. We call such a topology, survivable virtual topology. The routing of the virtual topology shown in Fig. 2(c) is not survivable. A thorough examination of all possible routings of the virtual topology in Fig. 1(c), will lead to the

conclusion that none of the routings of virtual topology in Fig. 2(c) on the physical topology Fig. 2(a) is survivable. Therefore a survivable routing of the virtual topology in Fig. 2(c) does not exist. Such a topology is called a non-survivable virtual topology [8].

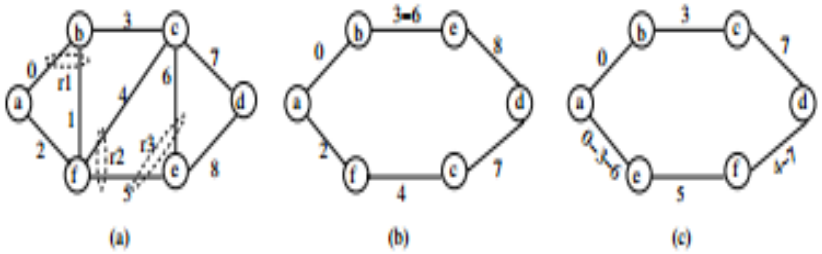


Fig. 2. (a). A 6-node physical topology with SRLG. (b). A survivable virtual topology and numbers adjacent to each virtual link show the routing. (c) A non-survivable virtual topology.

2.3 Drawbacks in scalable survivability

1. It will route in bidirectional. So the identification of the path/route is difficult.
2. The network node edges are disconnecting in some routing because the routing is performed virtually
3. It will not survivable in strong and weak condition.
4. Lot of Security issues in the existing model.

2.4 Security Issues and the proposed solutions

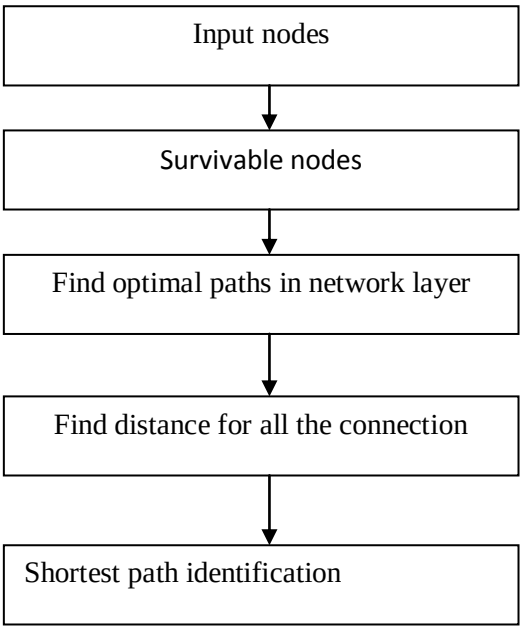
The perception of security is traditionally connected to exigencies of defending sensitive data from illegal access. But at the moment network security is often approached from a different perception. With the growing use of the Internet infrastructure for commercial applications, the demand for Quality of service is one of the emerging paradigms in Internet and seems to be the corner stone for more and more network services [2]. The paper [2] had included a layer called security layer between transport layer and the application layer. The work [6] proposed a new 512 bit block cipher named SF Block cipher. The proposed cipher is developed based on design principle known as Substitution permutation network [6]. The paper [10] analyzed several existing security algorithms to cope with the security issues. The work [14] proposed a new enhanced model for security which proved to be best suited for modern day applications.

III. PROPOSED WORK

3.1 Minimum logical topology augmentation for guaranteed weakly survivable routing

Given a cross-layer network, it is possible that the logical topology does not permit a weakly survivable routing. In such a case we need to add additional logical links to guarantee the existence of a weakly survivable routing. This augmentation problem was earlier considered in . In this section we now show how to enhance the WSR-MD algorithm to accommodate steps to augment the logical network with minimum number of additional links so that the augmented network admits a weakly survivable routing.

3.2 Flow diagram



IV. WEAKLY SURVIVABLE ROUTING UNDER CROSS-LAYER METRICS

In this section we develop MILP formulations to determine a survivable logical topology routing that maximizes one of three cross layer metrics.

A. Maximizing the After-failure Connectivity of the Logical Topology

The connectivity of a graph is the smallest number of edges whose removal disconnects the graph. Our interest is to find a survivable logical topology routing that maximizes the after-failure connectivity of the logical topology after a single physical link failure. This is equivalent to finding a survivable logical routing that maximizes the number of edges remaining in any cut of GL after any physical link failure.

B. Maximizing the Capacity of the Logical Topology

Given a routing that achieves a demand of on logical link (v, w). Let Ψ(s, t) be the maximum flow between any pair of nodes s, t ∈ VL while treating ρvw as the capacity of link (v, w) ∈ EL. Then we define the capacity of GL under the given routing as $\min_{s,t \in VL} \{\Psi(s, t)\}$. Our interest is to determine a survivable logical routing that maximizes logical capacity.

C. Maximizing the Min-Cross-Layer Cut

Given a logical topology routing R, the minimum crosslayer cut MCLC(R) of R is defined in [7] as the smallest number of physical link failures that will disconnect the logical topology. We wish to find a routing R that has the maximum value for MCLC(R). If this maximum value is greater than or equal to one, then that routing will be survivable.

V. HEURISTICS

To mitigate the computational complexity of these formulations, we present in this section heuristics for all the problems considered.

A. Heuristic for logical topology augmentation

The heuristic augments the given logical topology with additional links so that a survivable routing is guaranteed for the augmented logical topology. The routing corresponding to each logical link is also generated.

The heuristic first sorts all logical nodes by their degrees, and a datum node with the maximum degree is assigned and denoted as Δ. While there exists logical node v with degree ≥ 2, the heuristic assigns each logical node v with degree ≥ 2 a cost Cv=(degree of logical node) * (degree of corresponding physical node). The heuristic then selects the logical node with the largest Cv and chooses two of v's adjacent nodes v1 and v2 with the largest Cv1 and Cv2 . (v, v1) and (v, v2) are then mapped into disjoint paths in the physical topology. After that, v is removed from the logical topology. This procedure is repeated till no logical nodes with degree ≥ 2 are left. Next, the heuristic picks a node v from the remaining logical topology with degree = 1, i.e., an edge (u, v). An edge (u, v 0) parallel to (u, v) is then added and disjoint mappings for (u, v) and (u, v 0) in the physical topology are found. This procedure is executed until the elimination of all logical nodes with degree = 1. After the previous steps, if there exists nodes v with degree = 0, two parallel edges connecting v and Δ are added and they are mapped disjointly in the physical topology.

B) Heuristics for maximizing logical capacity

To guarantee survivability, the heuristic would still augment the logical topology with additional links. Steps 1-6 are the same as those in Algorithm 1. After selecting the candidate node Cv with degree ≥ 2 and the largest Cv, instead of mapping its adjacent nodes v1 and v2 with the largest Cv1 and Cv2 , the Cvi 's are included in a priority list. The heuristic selects two nodes at a time with the highest Cvi (in descending order), finds their disjoint mappings, and determines the minimal capacity of the routing. Among all the routings generated, the one that maximizes the minimal capacity is selected. This procedure is repeated till no logical node with degree ≥ 2 is left.

After a survivable routing is generated, to determine the maximal logical capacity, we first push the flow for all logical demands. This step is done by repeatedly pushing unit flow for each logical demand until the physical capacity cannot carry more logical demand. Here the physical edge capacity of an edge would be updated if the unit flow is routed through this edge. After the above step, the maximum flow is pushed for every logical node pair.

C) Heuristics for Maximizing the After-Failure Connectivity and the MCLC

Start with a spanning tree t, and map their links into paths using a shortest path algorithm At the end of this step all the physical edges that were not used in this mapping of the links in the tree are stored in a set CB(t).

Here a block refers to the set of co-tree edges with respect to a spanning tree edges. We have to make efforts that locks are not disjoint. We want them to overlap as much as possible so that an edge appears in more than one block. If this could be done then after a physical link failure several trees will remain connected increasing the connectivity of the logical network after a failure. W is a large number.

D) Maximizing After-Failure Connectivity

After finding mappings of all links in a tree ti the set CB(ti) is created. All the edges in CB(ti) are assigned a large W to discourage their selection for the mappings in the subsequent tree. This is to ensure that CB blocks for two

subsequent trees overlap as much as possible, This will guarantee that after the failure of an edge that is in two consecutive CB's at least two trees will remain resulting in increased after-failure connectivity.

E) Maximizing MCLC Value

In this heuristic all the edges that are used in the mapping of a logical link in a tree ti are assigned a large weight so that these edges are discouraged from entering the CB for ti . This is to create as large as a CB(ti) as possible. A larger CB means that multiple failures of the edge in CB will not disconnect the tree ti thereby increasing the MCLC value.

F) ACO for Shortest path identification

ANT COLONY OPTIMIZATION (ACO) Swarm Intelligence (SI) is the local interaction of many simple agents to achieve a global goal. SI is based on social insect metaphor for solving different types of problems.[15] Insects like ants, bees and termites live in colonies. Every single insect in a social insect colony seems to have its own agenda. The integration of all individual activities does not have any supervisor. In a social insect colony, a worker usually does not perform all tasks, but rather specializes in a set of tasks. This division of labour based on specialization is believed to be more efficient than if tasks were performed sequentially by unspecialized individuals. SI is emerged with collective intelligence of groups of simple agents. This approach emphasizes on distributedness, flexibility, robustness and direct or indirect communication among relatively simple agents. The agents are autonomous entities, both proactive and reactive and have capability to adapt, cooperate and move intelligently from one location to the other in the communication network. The basic idea of the ant colony optimization (ACO) meta-heuristic is taken from the food searching behavior of real ants. Ant agents can be divided into two sections:

G) Algorithm steps

Step 1: When the BS starts computing shortest path, it decides one destination node in WSN. An ant is created which will generate a path from BS to that destination node.

Step 2: Ant "k" at node "i" selects the next node "j" using formula in equation 1. Here "j" is one of the adjacent node of "i". An ant "k" has more probability to choose the node with larger values of k pij the next node selected is stored in memory of ant k denoted by (k M).

Step 3: If any ant visits the node which is already visited by the same ant then that ant Is discarded from path calculation.

Step 4: Step 2 and 3 are repeated until ant "k" finds its destination node or discarded.

Step 5: Step 1 to 4 is repeated for all ants.

Step 6: When all ants complete above procedure pheromone on the edge is updated which is given by equation 6.

$$\tau_{ij}(t) \leftarrow \tau_{ij}(t) + ((\frac{1}{\theta^{\Psi}}) \times (1 + (\frac{1}{j^{k}(t)^{\Omega}}))$$

Step 7: Then the evaporation of pheromone is calculated by equation 5.

Step 8: Now the path traversed by all ants is compared. The best optimal path is selected Among them by comparing the number of hops & distances. This optimal The path is then deleted from the graph. Again same

procedure is repeated, this time result will be a different optimal path than the previous one because that path is already deleted.

VI. EXPERIMENTAL RESULTS

The testing cases for both exact solution approaches (MILP formulations) and heuristics algorithms are as follows. First, we present the results for the minimizing logical network augmentation. Note that logical network augmentation is triggered only when cross-layer survivable route cannot be generated.

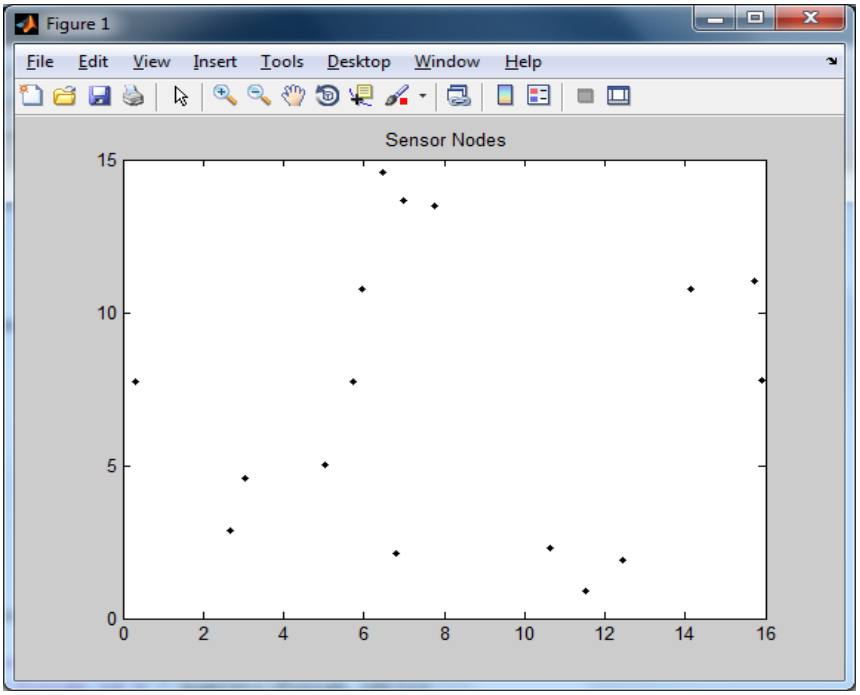


Fig.4 Number sensor nodes

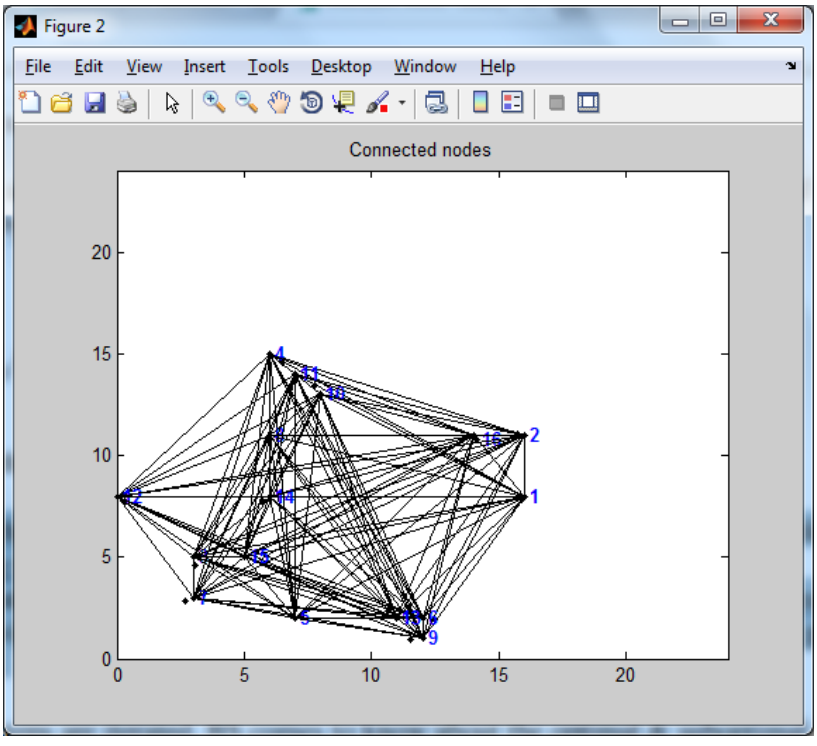


Fig.5 Connected nodes

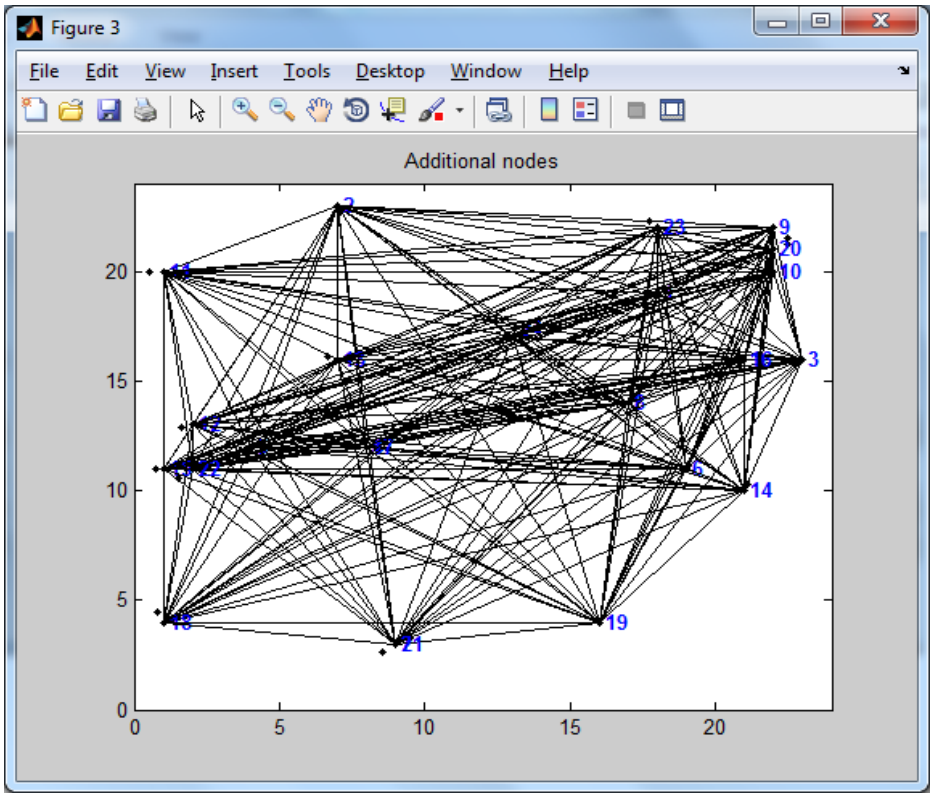


Fig.6 Additional nodes

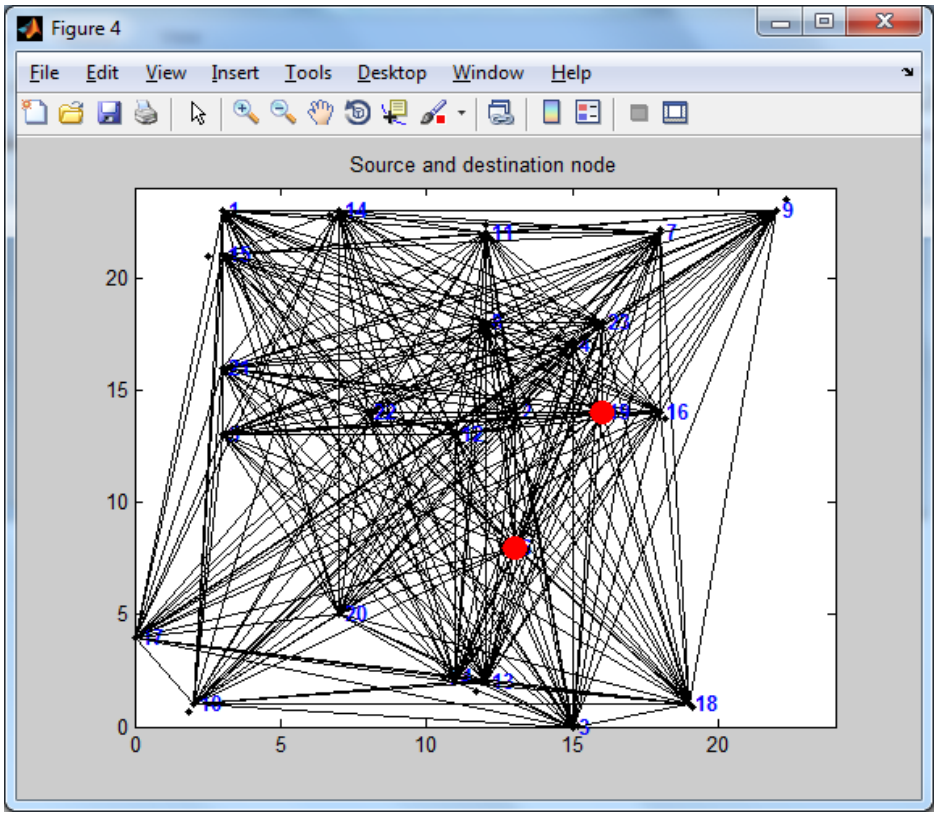


Fig.7 Source and destination nodes

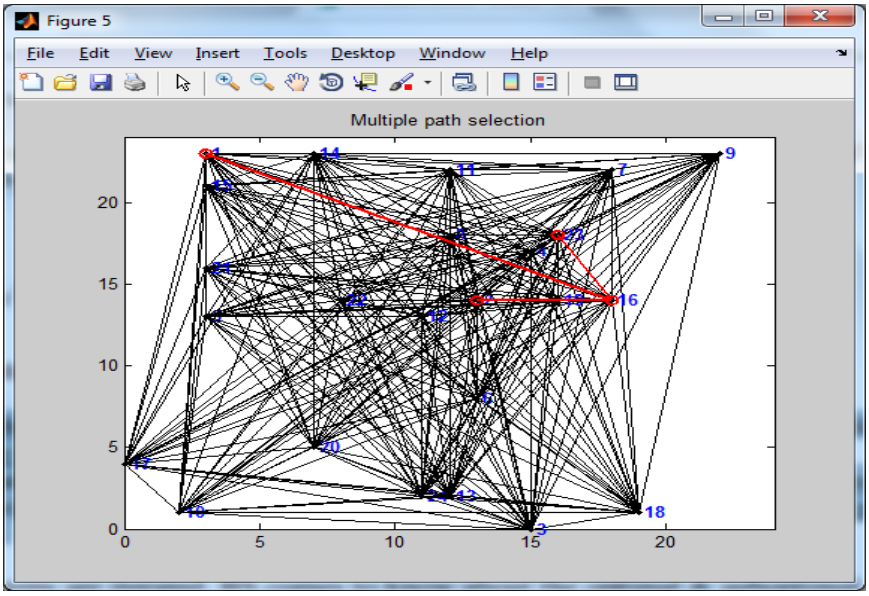


Fig.8 Multiple path selection

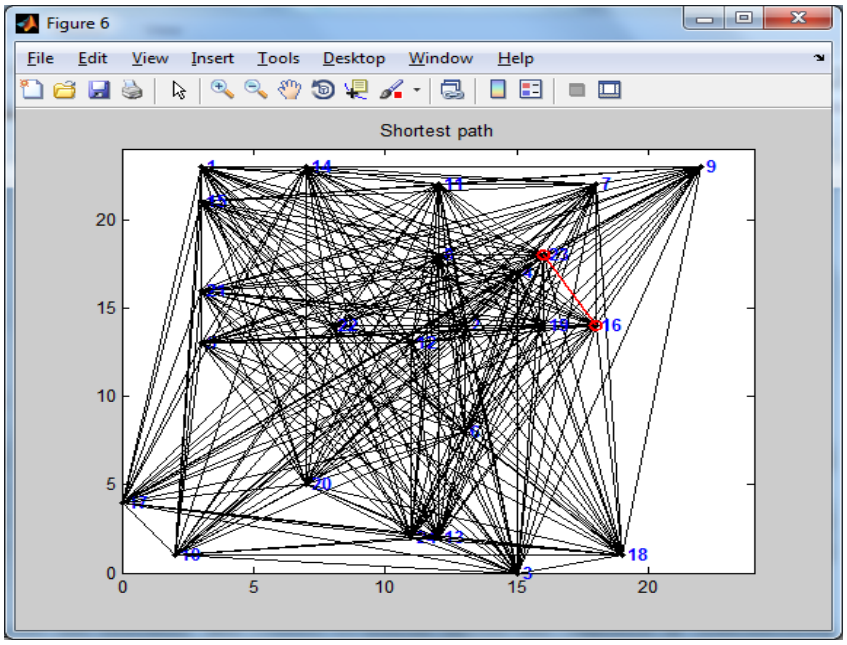


Fig.9 Shortest path

VII. CONCLUSION

In this paper we have presented a comprehensive treatment of mathematical programming frameworks for the survivable logical topology routing problem in capacitated cross-layer optical networks under multiple cross-layer evaluation metrics. We have enhanced the survivability routing formulation WSRMD given in Section III by developing MILP formulations for (1) minimum logical topology augmentation for guaranteed weakly survivable routing, (2) maximizing the afterfailure connectivity of the logical topology, (3) maximizing the capacity of logical topology, and (4) maximizing the minimum cross-layer cut. An interesting feature of our MILP formulations is that the optimization is carried out in a single stage, in contrast to previous approaches that consider logical sub graphs

obtained after each physical link failure. For example, see [7]. The contributions reported in this paper assume considerable significance in view of the increasing interest in network virtualization and topology abstraction incorporating survivability requirements.

VIII. REFERENCES

1. J. Sakaguchi, B. Puttnam, W. Klaus, Y. Awaji, N. Wada, A. Kanno, T. Kawanishi, K. Imamura, H. Inaba, K. Mukasa, R. Sugizaki, T. Kobayashi, and M. Watanabe, "305 Tb/s space division multiplexed transmission using homogeneous 19-core fiber," J. Lightwave Technol., vol. 31, no. 4, pp. 554– 562, Feb. 2013.
2. M. Anand Kumar, Dr. S. Karthikeyan (2011), "Security Model for TCP/IP Protocol Suite", Journal of Advances in Information Technology, 2[2], 87-91.
3. T. Lin, Z. Zhou, K. Thulasiraman, G. Xue, and S. Sahni, "Unified mathematical programming frameworks for survivable logical topology routing in IP-over-WDM optical networks," J. Opt. Commun. Netw., vol. 6, no. 2, pp. 190–203, 2014.
4. T. Lin, Z. Zhou, and K. Thulasiraman, "Logical topology survivability in IP-over-WDM networks: Survivable lightpath routing for maximum logical topology capacity and minimum spare capacity requirements," in Proc. Int. Workshop on the Design of Reliable Communication Networks (DRCN), Krakow, Poland, Oct. 2011, pp. 1–8.
5. K. Thulasiraman, T. Lin, M. Javed, and G. Xue, "Logical topology augmentation for guaranteed survivability under multiple failures in IP-over-WDM optical networks," Opt. Switching Netw., vol. 7, no. 4, pp. 206–214, 2010.
6. M. Anand Kumar and Dr. S. Karthikeyan 2012)," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", 4[11]:55-61.
7. C. Liu and L. Ruan, "A new survivable mapping problem in IP-over-WDM networks," IEEE J. Sel. Areas Commun., vol. 25, no. 3, pp. 25–34, 2007.
8. D. D.-J. Kan, A. Narula-Tam, and E. Modiano, "Lightpath routing and capacity assignment for survivable IP-over-WDM networks," in Proc. Int. Workshop on Design of Reliable Communication Networks (DRCN), Washington, DC, Oct. 2009, pp. 37–44.
9. K. Lee and E. Modiano, "Cross-layer survivability in WDMbased networks," in IEEE Int. Conf. on Computer Communications (IEEE INFOCOM), Rio de Janeiro, Brazil, Apr. 2009, pp. 1017–1025.
10. M. Anand Kumar and Dr. S. Karthikeyan (2012)," Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms" International Journal of Computer Network and Information Security", 4[2] : 22-28
11. A. Agrawal and R. E. Barlow, "A survey of network reliability and domination theory," Oper. Res., vol. 32, pp. 478–492, 1984.
12. A. Rosenthal and D. Frisque, "Transformations for simplifying network reliability calculations," Networks, vol. 7, pp. 97–111, 1977.
13. A. Shooman and A. Kershenbaum, "Exact graph-reduction algorithms for network reliability analysis," in IEEE Global Communications Conf. (IEEE GLOBECOM), Phoenix, AZ, Dec. 1991, pp. 1412–1420.
14. M. Anand Kumar.and Dr. S. Karthikeyan (2013)," An Enhanced Security for TCP/IP Protocol Suite" International. Journal of Computer Science and Mobile Computing , 2[11]:331-338.