International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012 pp-384-389 ISSN: 2249-6645

A Novel Approach for Link/Path Protection in Dual-Link Failures

1 Ashok kumar velpuri,2 Sreenivas velagapudi

1 Student, M.tech,Department of computer science and engineering,
K L University, Greenfields,Vaddeswaram,Guntur District,A.P,INDIA,Pincode:52250
2 Asst.prof, Department of computer science and engineering, K L University.

Abstract:

In every network we see the link failures are common, for this purpose networks having the scheme to protect their links against the link failures. Link protection helps fast recovery from link failures .Existing schemes either pre-reserve two backup paths for each demand or compute new backup paths for unprotected demands after the first link failure occurs. Both approaches require a large amount of backup capacity. In this paper, we propose a capacity efficient hybrid protection/restoration scheme for handling two-link failures. The protection component reserves backup capacity intelligently to ensure the majority of the affected demands can be restored using the pre-planned backup paths upon a two-link failure. A remarkable feature of our approach is that it is possible to trade off capacity for restorability by choosing a subset of double-link failures and designing backup paths using our algorithm for only those failure scenarios.

In this we use Backup link mutual exclusion(BLME), when the links fail simultaneously. The solution methodologies for BLME problem is 1).for mulating the backup path selection as an integer linear program;2)developing a polynomial time heuristic based on minimum cost path routing

Key Words: Optical networks, link protection, link failures, backup link mutual exclusion

I. INTRODUCTION

The growing transmission speed in the communication networks calls for efficient fault-tolerant network design. Current day's backbone networks use optical communication technology involving wavelength division multiplexing (WDM). One of the most gifted concepts for high capacity communication systems is wavelength division multiplexing (WDM). Each communication channel is allocated to a different frequency and multiplexed onto a single fiber. At
the destination wavelengths are spatially separated to different receiver locations. In this configuration the high carrier bandwidth is utilized to a greater level to transmit multiple optical signals through a single optical fiber.

Optical networks at present operate in a circuit switched way as optical header processing and buffering technologies are still in the in the early hours stages of research for wide-scale commercial deployment. Protecting the circuits or connections established in such networks against single-link failures may be achieved in different ways:

Path protection: Path protection is having the capability to

protect one or more peer-to-peer paths via a predetermined or pre-established backup tunnel. This is for all time peer-to-peer protection and is similar to the shadow PVC model often used in the ATM networks. The backup tunnel is link and node diverged from the primary tunnel, such that if any element (link or node) along the primary path fails, the head end reroutes the traffic onto the backup path. Many schemes for backup can be used, such as 1 to N or 1 to 1. In the 1-to-N scheme, there is one backup tunnel for N primary tunnels between the same pair of routers. The 1-to-1 back up implies that for every primary tunnel a backup tunnel exists. The number of backup tunnels needed for path protection is twice the number of primary tunnels. The past is referred to as failure independent path protection (FIPP) while the latter is referred to as failure-dependent path protection (FDPP).

Link protection*:* As clear by the name itself, link protection involves protecting against link failures. These days, links have become more reliable, but statistics still show that most unplanned failures in the network occur because of linkfailures. So, protecting against link failures is necessary in any network. To protect against link failures it can use multiple circuits or SONET APS protected circuits. This can result in expensive circuits. Because providing circuits is usually a recurring cost especially if the fiber circuit is not owned by the carrier you might want to reduce the operating cost by eliminating the redundant circuits if fast reroute of traffic can be done by using other paths in the network. Link protection enables you to send traffic to the next hop on a backup tunnel should the primary link fail. Off-course link protection does not work if the only means of reaching the next hop is through the primary link (singly connected cases). Link protection reduces the communication requirement as compared to path protection, so providing fast recovery. On the other hand, the downside of link protection is that its capacity requirement is higher than that of path protection, explicitly when protection is employed at the connection granularity [2].

Node protection: In link protection, the backup tunnel is always set up to the next hop node and the failure detection is performed based on loss of carrier or SONET alarms. In node protection, the mechanism described is similar to the link protection except that the backup tunnel is always set up to the node beyond the next hop that is, next-next hop. Upon detection of failure via a hello timeout, the point of local repair (PLR) node reroutes traffic onto the backup tunnel to the next-next-hop (nnhop). However, when MPLS packets emerge at the tail of the nnhop backup tunnel, they might not have the right labels for the merge point to carry the traffic further. To avoid discarding traffic at the tail of the backup tunnel, the head of the backup tunnel (also known as the point of local repair) swaps the primary tunnel label to the label expected by the merge point and then imposes the backup tunnel label. This ensures that the MPLS packets coming out of the backup tunnel carry the correct labels and hence are switched to the correct destination.

Algorithms for protection against link failures have traditionally considered single-link failures [3]–[5]. However, dual-link failures are becoming more and more important due to two reasons. First, links in the networks share resources such as conduits or ducts and the failure of such shared resources result in the failure of multiple links. Second, the average repair time for a failed link is in the order of a few hours to few days [6], and this repair time is satisfactorily long for a second failure to occur. Although algorithms developed for single-link failure resiliency is shown to cover a good percentage of dual-link failures [7]–[10], these cases often include links that are far away from each other. Considering the fact that these algorithms are not developed for dual-link failures, they may provide as an alternative to recover from independent dual-link failures. However, reliance on such approaches may not be preferable when the links close to one another in the network share resources, leading to correlated link failures.

Dual-link failures may be modeled as shared risk link group (SRLG) failures. A connection established in the network may be given a backup path under every possible SRLG failure. This approach assumes a precise knowledge of failure locations to re-configure the failed connections on their backup paths. An alternative is to protect the connections using link protection, where only the nodes adjacent to the failed link (and those involved in the backup path of the link) will perform the recovery. The focus of this paper is to protect end-to-end connections from dual-link failures using link protection.

II.DUAL-LINK FAILURE RESILIENCY WITH LINK PROTECTION

Assume that two links, *l* and *l*', failed one after the other (even if they happen together, assume that one failed first followed by the other) in a network. The backup path of the first failed link is analogous to a connection (at the granularity of a fiber) established between two nonadjacent nodes in the network with link removed. The connection is required to be protected against a single-link failure. Therefore, strategies developed for protecting connections against single link failures may be directly applied for dual-link ailures that employ link protection to recover from the first failure. Dual-link failure resiliency strategies are classified based on the nature in whichthe connections are recovered from first and second failures. The recovery from the first link failure is assumed to employ link protection strategy. Fig. 1 shows an example network where link 1-2 is protected by the backup path 1-3-4-2. The second protection strategy will refer to the manner in which the backup path of the first failed link is recovered.

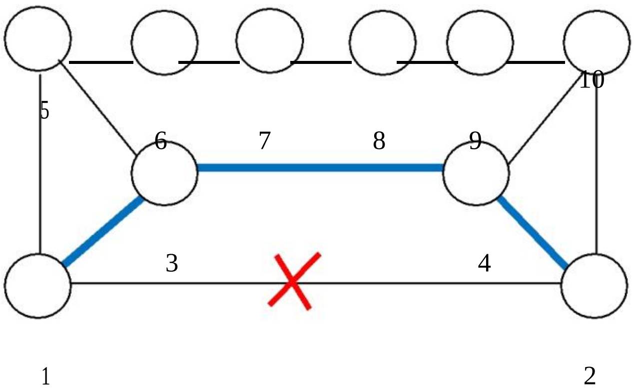


Fig. 1: Link 1-2 Protected by Backup Path 1-3-4-2 when Failed

Link Protection—Failure Independent Protection (LPFIP):
One approach to dual-link failure resiliency using link protection is to compute two link-disjoint backup paths for every link. Given a three-edge-connected network, there exists three link-disjoint paths between any two nodes [11]. Thus, for any two adjacent nodes, there exists two link-disjoint backup paths for the link connecting the two and *B'l* denote the two link-disjoint backups for link *Bl*. If any link in the backup path *Bl* fails, the backup path of will be reconfigured to *B'l*. Hence, the nodes connected to link *l* must have the knowledge of the failure in its backup paths (not necessarily the location).

Link Protection—Failure Dependent Protection (LPFDP):
For every second failure that affects the backup path, a backup path under dual-link failure is provided. This backup path is

computed by eliminating the two failed links from the network and computing shortest path between the specific node pairs. When a second link failure occurs, a failure notification must be sent to node specific node. It is fairly straight forward to see that the average backup path length under dual-link failures using LP-FDP will be lesser than that using LP-FIP. Every link is assigned one backup path for single link failure and multiple backup paths (depending on the number of links in the backup path for the single link failure) under dual-link failures.

Link Protection—Link Protection (LP-LP*):* Notification of the second failed link to different nodes for them to reconfigure their backup paths may result in a high recovery time. In order to avoid notification to the other nodes and reconfiguring at the end of the paths, link protection may be adopted to recover from the second link failure as well. Under this strategy, every link will have only one backup path (for all failure scenarios). In order for this strategy to work, the backup path under the second failure must not pass through the first failed link. This condition is referred to as the *backup link mutual exclusion* (BLME) constraint.

III. HEURISTIC APPROACH

As ILP solution times for large networks may be prohibitively high, a heuristic approach is also developed. The heuristic solution is based on iterative computation of minimum cost routing. The network is treated as an undirected graph G. A set of auxiliary graphs corresponding to failure of a link l G is created. In each auxiliary graph Zl the objective is to obtain a path between the nodes that were originally connected by link l. Let Pl denote the path selected in auxiliary graph Zl. If a link l' is a part of the path selected on graph Zl, then the path in graph Zl must avoid the use of link l. This is accomplished by imposing a cost on the links in the auxiliary graphs and having the path selection approach select the minimum cost path. Let Wll' denote the cost of link l' on graph Zl such that it indicates that graph Zl' contains link l and the two links l and l' may be unavailable simultaneously. Hence, the cost values are binary in nature.

The cost of a path in an auxiliary graph is the sum of the cost of links in it. At any given instant during the computation, the total cost of all the paths (T) is the sum of the cost of the paths across all auxiliary graphs. It may be observed that the total cost must be an even number, as every link l' in a path Pl that has a cost of 1 implies that link l in path Pl' would also have a cost of 1. For a given network, the minimum value of the total cost would then be two times the number of dual-link failure scenarios that would have the network scenarios that would disconnect the graph, then the termination condition for the heuristic is given by T= 2 T. disconnected. If T denotes the number of dual-link failure

Steps involved in the IMCP heuristic solution.

Iterative Minimum Cost Path (IMCP) Heuristic:

Step1. Obtain auxiliary graphs Zl for every l € Z as Zl =Z - {l} Note that every link l Z is bidirectional in nature.

Step 2. Initialize the path to be found in every graph Zl as an empty set Pl ← 0 , l€ Z

Step 3. Initialize the cost of all the links in every auxiliary graph to 0, Wll'← 0, l€ Z, l' Zl

Step 4. For every auxiliary graph Zl

1. Erase the old path and and update the cost in auxiliary graphs; ie, for every link l' € Pl update Wl'l ← 0, Pl ← 0

2. Recompute the least cost path Pl

3. If the link l' is present in this graph, then modify the cost of link l in auxiliary graph Zl, ie for every link l' Pl update Wl'l ← Pll'

Step 5.Compute the total cost of all path over all the auxiliary graphs ie T = Σ l Z Σ l' Pl Wll'

Step 6.If the total cost all the paths equals the threshold of 2T , where T is the number of dual link failure scenarios that would disconnect the graph, then it indicated the best possible solution has been obtained, ie T= 2 T, go to step 7, otherwise go to step 4.

Step 7:stop

IV. SYSTEM ANALYSIS

Existing System:

Algorithms for protection against link failures have traditionally considered Single-link failures. However, dual link failures are becoming increasingly important due to two reasons. First, links in the networks share resources such as conduits or ducts and the failure of such shared resources result in the failure of multiple links. Second, the average repair time for a failed link is in the order of a few hours to few days, and this repair time is sufficiently long for a second failure to occur. Algorithms developed for single-link failure resiliency is shown to cover a good percentage of dual-link failures, these cases often include links that are far away from each other. Considering the fact that these algorithms are not developed for dual-link failures, they may serve as an alternative to recover from independent dual-link failures.

Proposed System:
This paper formally classifies the approaches for providing dual-link failure resiliency. Recovery from a dual-link failure using an extension of link protection for single link failure results in a constraint, referred to as BLME constraint, whose satisfiability allows the network to recover from dual-link failures without the need for broadcasting the failure location to all nodes.

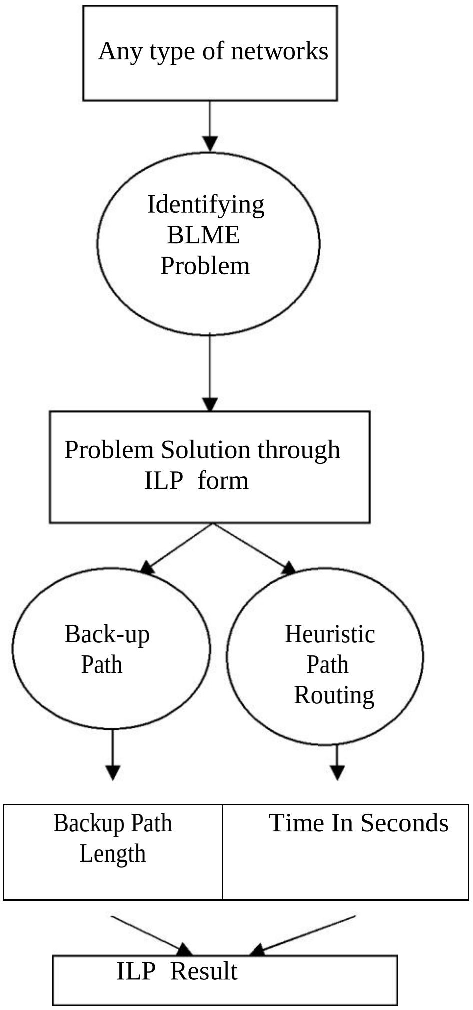


Fig. 2: Flow Diagram

This paper develops the necessary theory for deriving the sufficiency condition for a solution to exist, formulates the problem of finding backup paths for links satisfying the BLME constraint as an ILP, and further develops a polynomial time heuristic algorithm. The formulation and heuristic are applied to six different networks and the results are compared.

V. MODULE DESCRIPTION

Module 1:
containment hierarchy is a tree of components that has a top-
Component creation: To appear onscreen, every GUI component must be part of a *containment hierarchy*.

A level container as its root. Each GUI component can be contained only once. If a component is already in a container and try to add it to another container, the component will be removed from the first container and then added to the second.

Module 2:
Application of events and positioning of components

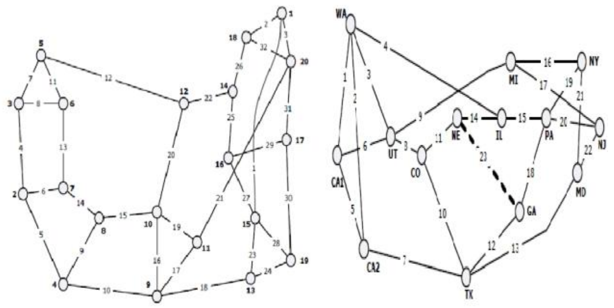
- Create the nodes in different positions and apply different colors.
- Create the distance between the nodes by applying stress.
- Apply different mouse events to the nodes.
- Using grouplayout of JFreechart all the nodes are positioned. By using virtual and horizontal position and parallel group, all the nodes are positioned.

Module 3:
Calculating TIS and BP length

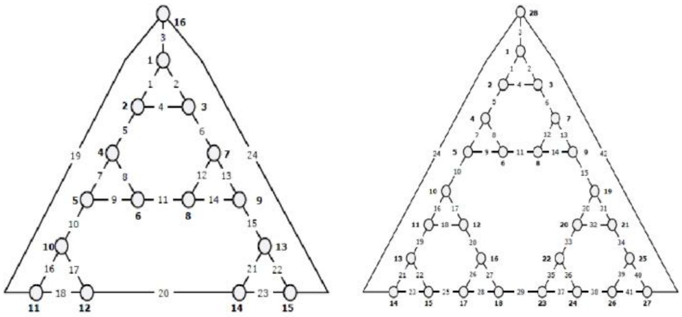
- By clicking any node, the data transfer to the next node and dual failure are shown in red color.
- For this dual failure, the backup path is shown in red color.

- The Time in seconds and BP length is displayed.

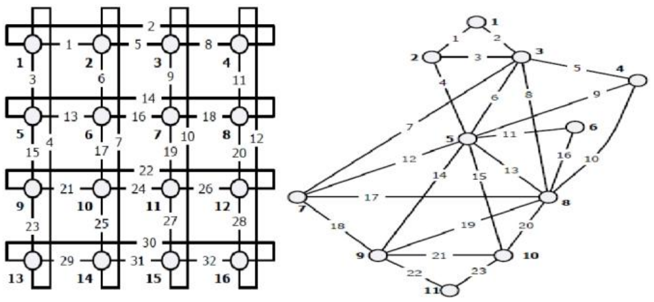
In this paper heuristic are applied only for six different types of networks [11] that are shown here.



(a) (b)



(b) (d)



(e) (f)

Fig. 3: Networks Considered for Performance Evaluation.

(a) ARPANET (20 nodes, 32 links). (b) NSFNET (14 nodes, 23 links). (c) Node-16 (16 nodes, 24 links). (d) Node-28 (28 nodes, 42 link nodes, 23 links).

CONCLUSION

This paper focuses on the approaches for providing dual-link failure resiliency. Recovery from a dual-link failure using an extensio constraint, referred to as BLME constraint, whose satisfiability allows the network to recover from dual-link failures without the need paper develops the necessary theory for deriving the sufficiency condition for a solution to exist, heuristic is shown to obtain a so guarantee, although such a solution may have longer average hop lengths compared with the optimal values. The heuristic produces a s the six scenarios. A maximum of 30 iterations were performed. While the objective of the heuristic is to obtain a feasible solution, it is n network scenario for any arbitrary two link failure scenario). The number of iterations required to arrive at the solution depends on auxiliary graphs are considered and the weights employed. Comparing the results of the heuristic to that of the ILP, it is observed tha average backup path lengths.

References:

[1] A. Chandak and S. Ramasubramanian, "Dual-link Failure Resiliency through Backup Link Mutual Exclusion," *in Proc. IEEE Int. Conf. Broadband Networks*, Boston, MA, Oct. 2008, pp. 258–267.

[2] J. Doucette and W. D. Grover, "Comparison of Mesh Protection and Restoration Schemes and the Dependency on Graph Connectivity," Hungary, Oct. 2001, pp. 121–128.

[3] M. Medard, S. G. Finn, and R. A. Barry, "WDM Loopback Recovery in Mesh Networks," *in Proc. IEEE INFOCOM*, 2008, pp. 752–759.

[4] S. S. Lumetta, M. Medard, and Y. C. Tseng, "Capacity Versus Robustness: A Tradeoff for Link Restoration in Mesh Networks," *J. Lightw. Technol.*, 18, No. 12, pp. 1765–1775, Dec. 2000.

[5] G. Ellinas, G. Halemariam, and T. Stern, "Protection Cycles in WDM Networks," *IEEE J. Sel. Areas Commun.*, 8, No. 10, pp. 1924–1937, Oct. 2000.

[6] W. D. Grover, *Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*. Upper Saddle River, NJ: Prentice-Hall, 2007. M. Fredrick, P. Datta, "Sub-graph Routing: A Novel Fault-tolerant Architecture for Sharedrisk Link Group Failures

[7] M. Clouqueur and W. D. Grover, "Mesh-restorable Networks with Complete Dual-failure Restorability and with Selectively Enhanced Dual-failure Restorability Properties," in *Proc. OPTICOMM*, 2002, pp. 1–12.

[8] J. Doucette and W. D. Grover, "Shared-risk Logical San Groups in Span-restorable Optical Networks:Analysis and Capacity Planning Model," *Photon. Netw. Commun.*, 9, No. 1, pp. 35–53, Jan. 2005.

[9] J. A. Bondy and U. S. R. Murthy, *Graph Theory With Applications*. New York: Elsevier, 2008.

[11] H. Choi, S. Subramaniam, and H. Choi, "On Double-link Failure Recovery in WDM Optical Networks," in *Proc. IEEE INFOCOM*, 2007, pp. 808–816.

[12] CPLEXSolver.[Online].Available:http://www.cplex.com

[13] H. Choi, S. Subramaniam, and H. Choi, "Loopback Recovery from Double-link Failures in Optical Mesh Networks," *IEEE/ACM Trans. Netw.*, 12, No. 6, pp. 1119– 1130, Dec. 2004.

[14] H. Choi, S. Subramaniam, and H.-A. Choi, "Loopback Recovery from Neighboring Double-link Failures in WDM Mesh Networks," *Inf. Sci. J.*, 149, No. 1, pp. 197– 209, Jan. 2003