Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Handling Routing Disruption in IP Network

Varsha Gosavi, Prof. S. P. Pingat
Department of Computer,
Smt. Kashibai Navale College of Engineering,
Pune (MH), India

Abstract— In the today's era communication through network is the best and fastest way of communication. In the case of wired connection there is the communication between two nodes which are connected through the link. The communication will takes place smoothly till the link is unbroken. So there is need of link protection to safeguard networks without fail. Link failures in speedy networks have always been an apprehension (concern) of supreme importance. A single link cut in the network may leads to insignificant loss of data flow. To avoid all these issues there is also an alternative for protection of smooth flow by providing backup paths. Backup path is nothing but the alternate path to be followed in network while existing is unavailable. In this paper the survey of issues related with the link state routing, link-failure handling techniques and reliability of the backup paths is discussed.

Keywords— backup path, failure recovery, IP network, link state routing, link failure

I. INTRODUCTION

In network communication the communication takes place between sources to destination through the media. The communication can be wired or wireless. In the wired communication there are actual links between the nodes of the topology. The flow of data passes through that links until these are intact. If there is the breakage of single link from the topology the flow is interrupted and hence communication network. Due to this disruption of the IP network there is the loss of the data which is flowing currently through the link.

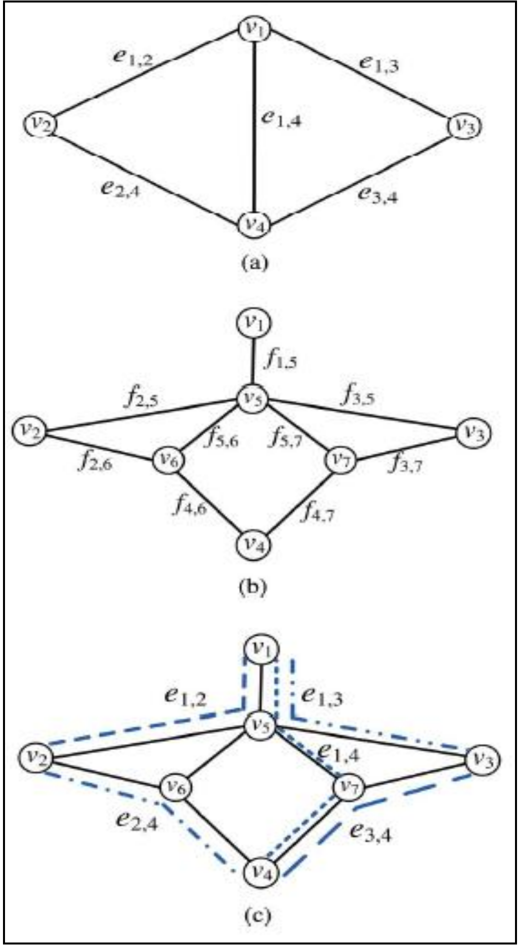

Fig. 1 Topology mapping of IP network (a) Logical Topology, (b) Physical Topology, (c) Mapping between the Logical and Physical Topology. [1]

To avoid all these losses by the link failure we have to find the alternative way for the recommencing of the flow. The link can be repaired, but for high bandwidth links the speed of flow is so high that the loss of data is so large. For the real time application such losses are dangerous. There should be high reliability and the high availability. So, another alternative is to provide the backup path for each link by which the flow can be switched to that path.

Currently in the IP network the whole connections done as per the wavelength division multiplexing (WDM) layered structure. So there are logical links in the network which are connected directly to the communicating nodes which are in between source to destination. IP network having layered IP topology in which logical links are implanted on the physical links. Logical links are nothing but the IP links and the physical links are nothing but the fiber links.

As shown in Fig. 1(a) the nodes in the communication are mapped by the logical topology. It shows $e_{i,j}$ as a logical link between node v_i and v_j. While mapping the actual communication between the nodes physical topology is used as shown in Fig. 1(b). It shows $f_{i,j}$ as a fiber link between node v_i and v_j. In the physical mapping there can be addition of nodes to divide the long links into the light-paths. These additional nodes are nothing but the physical devices induced into the network.

Link state routing is the method of routing in which each node of the network forms the map of its connectivity for communication with other nodes in the network. Every node calculates the best path for the destination from it in logical topology independently. All these best paths form the graph which is the combination of all best paths and forms the routing tables of each node. In link-state routing the nodes shares information between the nodes is in the form of connectivity only; unlike the distance vector routing method which shares the routing tables.

II. LITERATURE SURVEY

A. Related Work

As discussed above, in the recent world of internet it is become necessary that service should be with high availability, reliability and robustness. There is a large impact of unavailability off the network communication all the time due to failure of links. To achieve goal of recovering the flow of the network should be resumed as quickly as possible. Here discussed the various techniques of the IP network recovery and resumption of communication.

Amund Kvalbein et. al proposed a technique Multiple Routing Configurations (MRC) [4]. It gives surety that the node as well as link failures are fast recovered in failed IP network. MRC follows the principle of storing the additional information of routing in the routers. When there is the exposure of failure at some link the flow of data is instantaneously directed through the alternate output link. This technique is suitable for single link failure affairs for both link and nodes with the single mechanism instead of knowing the reason of failure. It is a connectionless technique and works on hop-by-hop forwarding. MRC forms network configuration for the backup with small set by using network mapping graph and links associated with it. By overall observations of simulations [4], MRC approaches performance of re-convergence of global OSPF.

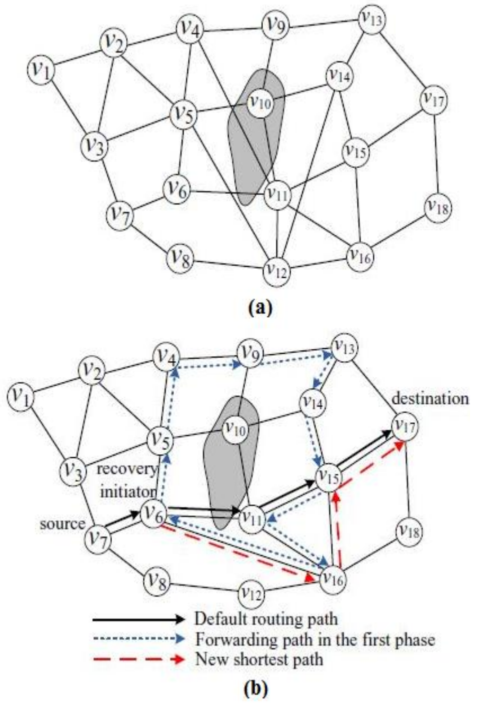

Fig. 2 a) Network with Failure(shaded region). b) Failure Handling with RTR [3].

Qiang Zheng *et. al* proposed a technique called Reactive Two-phase Rerouting (RTR) [3] as shown in Fig. 2. This approach works for intra-domain routing failure recovery. The technique name suggests two phases, quick recovery from failures and finding the shortest recovery paths. Initial stage contains the collection of failure details by forwarding the packets in failed network. Second stage contains the finding out shortest path for the destination from the current source and packets are forwarded through that path. Network of any mapping can be handled by this technique for the recovering and finding shortest path up to destination. Simulation [3] of this technique on the ISP topology shows that about 98.6% of failure paths are recovered with shortest path in the recovered network. As compared to previous techniques, network resources used for the irrecoverable paths of failed network is very less along with the better performance for recovering failed network.

Shrinivasa Kini *et. al* proposes a mechanism [5] for dual link failure recovery of networks. It works on the principle of re-routing of one failed link without knowledge of second failed link i.e. re-routing is independent of the other failed links. In this technique there are three protection addresses along with normal address for each node in the network and three protection graphs associated with them. In case of the protection graph, it is always two-edge connected with guarantee. In dual link failure the network is recovered from first failure by tunneling with the help of protection addresses and packet is routed. This proposal leads to the conclusion that three protection addresses for each node are sufficient for the dual link failure recovery.

M Hou *et. al* proposed a scheme [6] for finding backup paths in advance effectively to minimize the response time. Backup paths are chosen for the optional disjoint flow of packets for the primary paths of the network. The backup paths are chosen by two cases first, for all the links in the network communication and second, for the links which are not protected or shared links. In the network all links are not equally vulnerable to the failure; even though it's not cost effective to provide full protection scheme for all the links. In this proposal such a cost-effective schemes are proposed like, CERNET2 to analyze the failures from the real world traces. Here the selective protection scheme is followed because the failure probabilities are heavy-tail means the failure occurs due to the small set of links.

Matthew Johnston *et. al* proposed a scheme [7] for random link failure handling with the devoted backup network. After link failure in the network the traffic is diverted via pre-planned backup path. In finding out solution for the random link failures probabilistic survivability guarantees are provided to limit capacity over-provisioning. Here showed that the reliability of the primary network is gives stand to the optimal backup routing. In particular, when primary links becomes more failure resistant, the backup networks utilize optimally for additional resource sharing amongst available paths. Here the design and the capacity stipulation of the backup network are done based on the robust optimization.

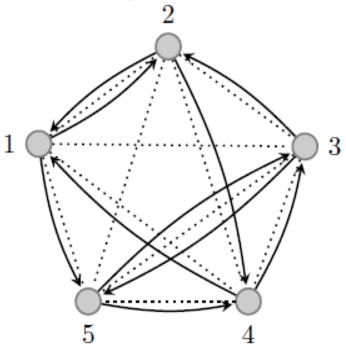

Fig. 3. Solid Link: Backup Network; Dotted Link: Primary Network[7]

Eiji Oki *et. al* proposes a model [8] in which the disjoint path selection mechanism is used for the networks of Generalized Multi-Protocol Switching (GMPLS) by using the constraints of Shared Risk Link Group (SRLG). This scheme also called as the Weighted-SRLG. At the time of execution of the shortest path algorithm the numbers of SRLG members are treated as the link cost. A link which has less number of SRLG members is selected as the shortest path always instead of some rare cases. This scheme concludes with the WSRLG is best for selection of disjoint paths over the conventional shortest path algorithm.

Lu Shen *et. al* proposed the model [9] mentioning the provision for services at optical layer of the network. The problems in the constraints of static provision is handled and formulated in different conditions of resource availability. SRLG-diverse path protection schemes are applied in the three classes as dedicated, shared and unprotected. A light path length constraints and revenue value associated with it is associated for each connection request. In the unavailability of the sufficient resources the revenue maximization problem is formulated for revenue value. When the resources are sufficient the capacity minimization problem is formulated.

Hyang-Won Lee *et. al* proposed a model [10] in which developed various schemes of routing to deal with numerous correlated, failures. Recovery from multiple failures can't achieve by guarantee till single link failure handled with disjoint path protection. In case of disasters or intentional attacks recovery mechanism is not that simple. By considering probabilistic network failures diverse routes have found by minimum joint failure probability and developed a Probabilistic Shared Risk Link Group (PSRLG) framework for handling correlated failures. By this framework, two paths containing minimum joint failure probability found to achieve optimal solutions.

As discussed above schemes in [4], [5], [6], [7] are based on the principle of independent logical link failure handling. Further schemes [8], [9] and [10] are contains the failure handling of the links by shared risk link group mechanism.

B. Related Work

As discussed in above section existing solutions of Link Failure Handling like independent model [4], [5], [6], [7] and Shared Risk Link Group (SRLG) model [8], [9], [10] does not correlate between IP link failures so results into failing to find reliable backup paths. It leads to the proposal of the cross-layer approach for minimizing routing disruption caused by IP link failures [1].

III. PROPOSAL OVERVIEW

For the proposal of the new model of cross layer approach base model from [1] is referred. In this developed a probabilistically correlated failure (PCF) model to measure the effect of IP link failure on the reliability of backup paths.

The proposal for the new model consists of the two objectives. First, to minimize routing interruption as well as handle routing attacks using risk aware mitigation mechanism and second, to achieve energy saving in IP networks.

IV. CONTRIBUTION

From all the above discussion it is highlighted that there is some limitations for the schemes of link failure handling like independent models, Shared Risk Link Group models. The overcome is achieved with the Cross Layer Approach. Also the technique Probabilistically Correlated Failure model is used to measure the impact of IP link failure on the reliability of backup paths which are used for the failure handling. By using this technique the routing attacks are handled and to minimize routing interruption.

ACKNOWLEDGMENT

For proposing this model referred the IEEE Transaction paper under the title “Cross-Layer Approach for Minimizing Routing Disruption in IP Networks” published in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 7, JULY 2014.

REFERENCES

[1] Qiang Zheng, Guohong Cao,Thomas F. La Porta, Ananthram Swami, “Cross-Layer Approach for Minimizing Routing Disruption in IP Networks”, *IEEE Transactions on Parallel and Distributed Systems, VOL. 25, NO. 7, July 2014.*

[2] Q. Zheng, J. Zhao, and G. Cao, A Cross-Layer Approach for IP Network Protection, in Proc. IEEE/IFIP DSN, 2012, pp. 1-12.

[3] Q. Zheng, G. Cao, T.L. Porta, and A. Swami, ‘‘Optimal Recovery from Large-Scale Failures in IP Networks,’’ *in Proc. IEEE ICDCS, 2012, pp. 295-304.*

[4] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, and O. Lysne, ‘‘Fast IP Network Recovery Using Multiple Routing Configurations,’’ *in Proc. IEEE INFOCOM, 2006, pp. 1-11.*

[5] S. Kini, S. Ramasubramanian, A. Kvalbein, and A.F. Hansen, ‘‘Fast Recovery from Dual Link Failures in IP Networks,’’ *in Proc. IEEE INFOCOM, 2009, pp. 1368-1376.*

[6] M. Hou, D. Wang, M. Xu, and J. Yang, ‘‘Selective Protection: A Cost-Efficient Backup Scheme for Link State Routing,’’ *in Proc. IEEE ICDCS, 2009, pp. 68-75.*

[7] M. Johnston, H.-W. Lee, and E. Modiano, ‘‘A Robust Optimization Approach to Backup Network Design with Random Failures,’’ *in Proc. IEEE INFOCOM, 2011, pp. 1512-1520.*

[8] E. Oki, N. Matsuura, K. Shiomoto, and N. Yamanaka, ‘‘A Disjoint Path Selection Scheme with Shared Risk Link Groups in GMPLS Networks,’’ *IEEE Commun. Lett., vol. 6, no. 9, pp. 406-408, Sept. 2002.*

[9] L. Shen, X. Yang, and B. Ramamurthy, ‘‘Shared Risk Link Group (SRLG)-Diverse Path Provisioning Under Hybrid Service Level Agreements in Wavelength-Routed Optical Mesh Networks,’’ *Proc. IEEE/ACM Trans. Netw., vol. 13, no. 4, pp. 918-931, Aug. 2005.*

[10] H.-W. Lee and E. Modiano, ‘‘Diverse Routing in Networks with Probabilistic Failures’’, *in Proc. IEEE INFOCOM, 2009, pp. 1035-1043.*