

Multiple Backup Path Approach for Link Failure in IP Networks

S. Priyadharshini
PG Scholar, ECE

Muthayammal Engineering College,
Tamil Nadu, India.

V. Govindaraj
Assistant Professor ECE

Muthayammal Engineering College,
Tamil Nadu, India

M. Vignesh
Assistant Professor ECE

Muthayammal Engineering College
Tamil Nadu, India

Abstract- Backup paths are frequently used in IP networks to prevent from IP links failures. In existing systems such as the normally used independent model and dependent model do not precisely find the correspondence between IP link failures, and it cannot choose consistent backup paths. Then we propose a multiple back up path approach for link failure in IP link networks. We develop a probabilistically correlated failure (PCF) model to measure the collision of IP link failure on the dependability of backup paths. In proposed system a lightweight proactive source routing protocol can be used for the information exchange among neighboring nodes for updated network topology information. In Proactive Source routing protocol (PSR) which allows a node to have full-path information to all other nodes in the network. When an IP link fails, its travel is split onto multiple backup paths to certify that the rerouted traffic load on each IP link does not go beyond the usable bandwidth.

Key Terms: Routing, failures, route recovery, IP networks, multiple backup paths.

I INTRODUCTION

IP link failures are quite common in the Internet for various reasons. In high speed Internet Protocol networks like the Internet backbone, detachment of a link for several seconds can lead to millions of packets being dropped [1]. In this layered structure, the IP layer topology i.e., logical topology is embedded on the optical layer topology, and each IP link is mapped to a light path in the physical topology. An IP link consists of multiple fiber links, and a fiber link possibly distributed by multiple IP links. All the logical links will fail concurrently because of fiber link failure. Logical link failures were considered as dependent failures or modeled as a Shared Risk Link Group (SRLG) model. [2]. Reactive two-phase rerouting (RTR) approach is used it has two phases of works. In first phase RTR first forwards packets around the failure area to gather information on failure. In the second phase, RTR determines a new shortest path and forwards packets along it via source routing. [3]. A node re-routes a packet around the failed link without the knowledge of the second link failure. In this RTF and STF schemes are used for packet forwarding. [4]. In the Weighted – Shared risk link group (WSRLG) scheme binary search algorithm is used. The number of disjoint path is increased to 41% to overcome this problem modified binary search algorithm is used. Where

WSRLG control the weight of the SRLG factor by using a binary search algorithm, while fulfill the required number of disjoint paths between source and destination nodes. [5] A cross-layer approach for IP link protection. Based on the topology mapping, a correlated failure probability model can be developed to calculate the impact of IP link Failure on the dependability of backup paths. With this model, a heuristic algorithm and multiround algorithm can be proposed to choose the backup paths with minimum failure probability and it considers the bandwidth constraint in backup path selection. It aims at choosing backup paths to minimize the traffic disruption caused by link failures.[6].In this Routing Configurations recovery scheme is used for both the node and link failures.

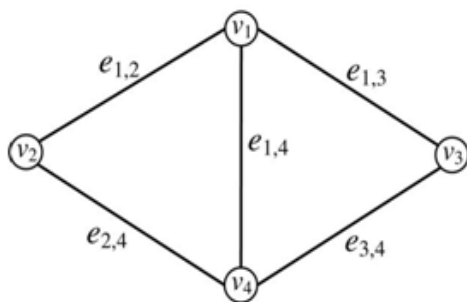
Due to the load distribution congestion can be occurred. MRC is used to overcome this problem.MRC is severely connectionless, and Presume only destination based hop-by-hop forwarding. It can be implemented with only Slight changes to existing systems. In Fig. 1, First while fiber link $f_{1,5}$ fails, then logical links $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ will fail jointly. This shows that the $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ are considered as independent failures. Second, sharing fiber links will cause logical links fails together in the same SRLG must be fail jointly. For example, $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ are in the similar SRLG method. While $e_{1,4}$ fails, it does not indicate that $e_{1,2}$ and $e_{1,3}$ must also fail. If the failure of $e_{1,4}$ is affected by fiber link $f_{4,7}$, $e_{1,2}$ and $e_{1,3}$ may exist. In up to date Internet measurements of [7], illustrate that independent failures and correlated failures coexist in the Internet. [9]. Failures are first differentiated based on patterns experiential at the IP-layer; in some cases, it is probable to additional deduce their probable basis, such as protection activities, router-related and optical layer obstacles.

Key sequential and spatial features of each class are examined and, when suitable, constraint using predictable distributions. Our results delegate that 20% of all failures occur during a period of scheduled protection activities of the unexpected failures, nearly 30% are joint by multiple links and are generally probable due to router-related and optical equipment- related inconvenience; whereas 70% change a single link at a time. In our categorization of failures make known the original and level of failures in the race of IP backbone. [8].A probabilistic outlook of network failures are

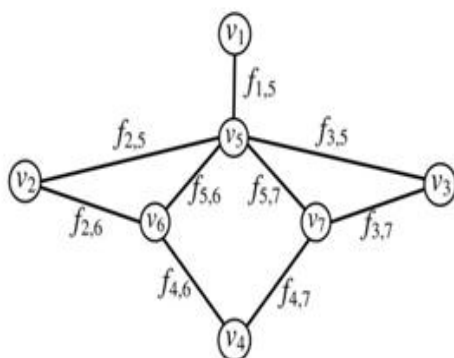
obtained where multiple failure consequence can occur concurrently, and expand algorithms for discovery of diverse routes with smallest amount of joint failure probability. Additionally, expand a narrative Probabilistic Shared Risk Link Group (PSRLG) framework for representing correlated failures.[10]. A backup path is chosen to be disjoint path from the main path, or in the network level, backup paths are deals with all links. The validity of this simple choice is based on 1) all the links may fail with equivalent probability; and 2) realize the high protection condition today, having links not defended or sharing links between the primary and backup paths immediately just look weird. Then vigilantly examine the functioning details and the overhead for common backup path schemes of the Internet at present. Originate an optimization problem where the routing performance should be definite and the backup cost should be diminished. This cost is exceptional as it occupies computation overhead.

When $e_{1,4}$ fails, it may be considered as independent or correlated failure due to shared fiber links. Consequently, $e_{1,2}$ and $e_{1,3}$ might be fail with a definite probability, i.e., failures of $e_{1,2}, e_{1,3}$, and $e_{1,4}$ links are probabilistically correlated. These features cannot be determined and has not been enquired in backup path selection.

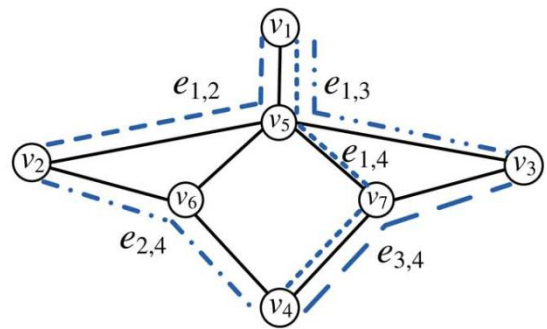
Fig.1. Mapping between the logical and physical topologies.



(a) Logical topology



(b) Physical topology



(c) Connected between the logical and fiber links.

New method is different from previous works in three aspects. First, it is based on a multiple backup path, which considers the connection between logical and physical topologies. The proposed PCF model can reveal the probabilistic correlation between logical link failures. Second, each logical link can be sheltered with multiple backup paths to productively reroute traffic and prevent from link overload, whereas most previous works select single backup path for each logical link. Third, our method considers the traffic load and bandwidth constraint. It assured that the rerouted traffic load does not exceed the usable bandwidth, yet when multiple logical links fail concurrently.

II. EXISTING SYSTEM

In existing system two methods are developed for link failures but it does not exactly find the connection between the IP link failure.[4].In first method Shared Risk Link Group (SRLG) model Binary search algorithm is used to find the path from a given network topology. It do not accurately reflect the correlation between IP link failures.[5].In second method correlated failure probability (CFP) model has two algorithms Heuristic algorithm and multi-round algorithm is used. The first algorithm concentrates on choosing the backup paths with smallest amount of failure probability. Then the second algorithm additionally believe that the bandwidth constraint and aims at minimizing the traffic disruption caused by failures. It causes low recovery rate.

III METHODOLOGY

3.1 The Pcf Model

The PCF model is built on three types of in formations, i.e., Topology mapping, failure possibility of fiber links, and failure possibility of logical links, all of which are already collected by ISPs. In real ISPs built their topology mapping and they have this information. The failure possibility of fiber links and logical links can be obtained with Internet measurement approaches [7], [8] arranged at the optical and IP layers. Observing mechanisms at the Optical layer can notice fiber link failure in SONET alarms. These sequences of logical link failures can be getting from routing updates. ISPs also maintain failure sequences, because they observe the optical and IP layers of their networks.

In carry out, it may get $p_{i,j}$ and $q_{m,n}$ based on preceding logical link and fiber link failures. Let $a_{m,n}^{i,j}$ distinct in Eq.(1) position the mapping between logical link $e_{i,j}$ and fiber link $f_{m,n}$

$$a_{m,n}^{i,j} = \begin{cases} 1 & \text{if } e_{i,j} \text{ is embedded on } f_{m,n} \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

$F_{i,j}$ is defined by Eq.(2) deduce that a fiber link $f_{m,n}$ holds $e_{i,j}$, i.e., $a_{m,n}^{i,j}$. If there is an one more logical link $e_{s,t}$ is also carried by $f_{m,n}$, $f_{m,n}$ is in the set $F_{i,j}$

$$F_{i,j} = \{f_{m,n} | a_{m,n}^{i,j} a_{m,n}^{s,t} = 1, e_{i,j} \in E_L, \exists e_{s,t} \in EL, \forall f_{M,n} \in F_P\} \quad (2)$$

As fiber link failures are independent, $p_{i,j}^c$ is work out by Eq.(3). If $e_{i,j}$ does not distribute a fiber link with other logical links, its correlated failure probability is 0

$$p_{i,j}^C = \begin{cases} 0 & \text{if } F_{i,j} = \emptyset \\ 1 - \prod_{f_{m,n} \in F_{i,j}} (1 - q_{m,n}) & \text{otherwise.} \end{cases} \quad (3)$$

If the independent failure probability of $e_{i,j}$ is $p_{i,j}^I$. The relation shown in Eq. (4), since failures of $e_{i,j}$ are moreover independent or correlated. In Lemma 1 shows that $p_{i,j}^I$ must be rigorously less than unity

$$P_{i,j} = 1 - (1 - p_{i,j}^I)(1 - P_{i,j}^C) \quad (4)$$

Lemma 1. $p_{i,j}^I \in [0, 1)$.

Proof. According to Eq. (4), $p_{i,j}^I = \frac{p_{i,j} - P_{i,j}^C}{1 - P_{i,j}^C}$. Since $q_{m,n} \in [0, 1)$

for each fiber link $q_{m,n}$, we have $p_{i,j}^C \in [0, 1)$. Together with $p_{i,j} \in [0, 1)$, we have $p_{i,j}^I < 1$. Therefore, $p_{i,j}^I \in [0, 1)$. \square

Case1: In $e_{i,j}$ is not implanted on $f_{m,n}$. It means that the breakdown of $e_{i,j}$ is not connect with $f_{m,n}$. Hence, $P(f_{m,n} | e_{i,j})$ is equal to $q_{m,n}$.

Case2: In $f_{m,n}$ just carries $e_{i,j}$, then a failure of $f_{m,n}$ conduct to an independent failure of $e_{i,j}$. In this case, $P(f_{m,n} | e_{i,j})$ is computed by Eq.(5), where $P(f_{m,n} | e_{i,j})$ is the probability of that $e_{i,j}$ has an independent failure. While it becomes failure, and $P(f_{m,n} | e_{i,j})$ is the probability of independent failure is happened by $f_{m,n}$

$$P(f_{m,n} | e_{i,j}) = P(e_{i,j}^I | e_{i,j}) * P(f_{m,n} | e_{i,j}^I) \quad (5)$$

In Eq.(6), $P(e_{i,j} | e_{i,j}^I)$ is the failure probability of $e_{i,j}$. when its independent failures occur, which is set to be 1. $P(e_{i,j} | e_{i,j}^I)$ is the independent failure probability of $e_{i,j}$,

$$\begin{aligned} P(e_{i,j}^I | e_{i,j}) &= \frac{P(e_{i,j} | e_{i,j}^I)}{P(e_{p,j})} \\ &= \frac{P(e_{i,j}^I)}{P(e_{i,j})} = \frac{P_{i,j}^I}{P_{i,j}} \end{aligned} \quad (6)$$

$$P(f_{m,n} | e_{i,j}^I) = \frac{P(e_{i,j}^I | f_{m,n}) P(f_{m,n})}{P(e_{i,j}^I)} = \frac{q_{m,n}}{P_{i,j}^I} \quad (7)$$

Where the conditional failure probability of $P(f_{m,n} | e_{i,j}^I)$ is given by Eq. (8), It is just defined for $e_{i,j}$ whose failure probability of $p_{i,j}$ is not 0. If $p_{i,j}$ is 0, $e_{i,j}$ certainly not fails, and they do not need to select backup paths for it

$$P(f_{m,n} | e_{i,j}) = \begin{cases} \frac{q_{m,n}}{p_{i,j}} & a_{m,n}^{i,j} = 0 \\ \frac{q_{m,n}}{p_{i,j}} & a_{m,n}^{i,j} = 1. \end{cases} \quad (8)$$

Lemma 2. If $f_{m,n}$ carries $e_{i,j}$ and $q_{m,n} > 0$, $P(f_{m,n} | e_{i,j}) > q_{m,n}$.

Proof. If $f_{m,n}$ carries $e_{i,j}$, the second case of Eq. (8) holds, i.e., $P(f_{m,n} | e_{i,j}) = \frac{q_{m,n}}{p_{i,j}}$. Since $q_{m,n} > 0$, the failure probability of $e_{i,j}$ is above 0. Since $p_{i,j} \in [0, 1)$, we have $p_{i,j} \in (0, 1)$. Therefore, $P(f_{m,n} | e_{i,j}) = \frac{q_{m,n}}{p_{i,j}} > q_{m,n}$. \square

$$P(e_{s,t}^C | e_{i,j}) = \begin{cases} 0 & \text{if } F_{s,t} = \emptyset \\ 1 - \prod_{f_{m,n} \in F_{s,t}} (1 - P(f_{m,n} | e_{i,j})) & \text{otherwise.} \end{cases} \quad (9)$$

Found on this, Eq. (10) computes the failure probability of $e_{s,t}$ below the condition that $e_{i,j}$ fails, which is denoted by

$$P(e_{s,t} | e_{i,j}) = 1 - (1 - P_{s,t}^I) (1 - P(e_{s,t}^C | e_{i,j})) \quad (10)$$

3.1.1 Algorithms

Evaluate our algorithms with Not-via [11] and PSRLG based Diverse Routing (DR) with disjointness constraint [8]. Then Not-via is an IP fast-rerouting (IPFRR) technique extensively organized in the Internet. DR employs a parameter p to identify the failure probability of logical links when the primary fiber link fails. Then put p to three typical values 0.2, 0.5, and 0.8. In extraction, compare our algorithms with five algorithms as follows.

- Not-via: Not-via is built as independent model.
- Not-via+SRLG: Not-via is built as SRLG model.
- DR (0.2): DR through its parameter p of 0.2.
- DR (0.5): DR through its parameter p of 0.5.
- DR (0.8): DR through its parameter p of 0.8.

3.2 Ad-Hoc Routing Protocol

An ad-hoc routing protocol is standard, that controls how nodes choose which way to route packets between computing devices in a mobile ad hoc network .In ad-hoc networks, nodes are not familiar with the topology of their networks. Alternatively, they have to determine it. The fundamental idea is that a new node may declare its presence and should listen for declaration broadcast by its neighbours. Each node learns about adjacent nodes and how to reach them, and may announce that it too, can arrive them. Note that in a extensive sense, ad hoc protocol can also be used accurately, that is, to denote an spontaneous and often protocol is established for a specific purpose.

3.2.1 Table-driven (Pro-active) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network.

3.2.2 On Demand (Reactive) routing protocol

This type of On-demand routing protocol finds a route by flooding the network with Route Request packets.

3.2.3 Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, can be employed on other wireless ad hoc networks. Where OLSR is a proactive link-state routing protocol, which uses hello packets and topology control (TC) messages to discover and then disseminate link state information is right through the mobile ad hoc network. Particular nodes use this topology information to process next hop destinations for all nodes in the network using shortest hop forwarding paths. Being a proactive protocol, OLSR uses power and network resources in order to propagate data about possibly idle routes. Whereas this is not difficulty for wired access points, and laptops, it makes OLSR inappropriate for sensor networks that try to sleep most of the time. In place of small scale wired access points with minimal CPU power, the open basis OLSR project illustrate that large scale mesh networks can run with OLSR on thousands of nodes with very little CPU power on 200 MHz embedded devices.

3.3 MANET

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized organization. Where Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks while, the arrangement of the network changes dynamically. This is mostly due to the mobility of the nodes. Where nodes in these networks employ the same random access wireless channel, work together in a friendly manner to appealing themselves in multihop forwarding. Where the nodes in the network are not only act as hosts but also act as routers that route data to/from other nodes in network. Then in mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and given that a destination node capacity will be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and destination. Inside a cell, a base station can attain all mobile nodes without routing via broadcast in regular wireless networks. In the system of ad-hoc networks, each node have to be able to forward data for other nodes in the networks. This creates supplementary problems with the length of the problems of dynamic topology which is unpredictable connectivity changes.

3.3.1 Mobile AD-HOC networks (MANET):

MANET means Mobile Adhoc network and it is the technology which is used to move vehicles as joint in network to make a transportable network. Participating vehicles become a wireless connection or router through MANET and it allow the vehicles almost to connect 100 to 300 meters to each other and in order to create a wide range network, other vehicles are connected to each other so the

mobile internet is prepared. It is invented that the first networks that will incorporate this technology are fire and police mobiles to interact with one another for security reasons.

Routing disruption: If a backup path does not enclose any overloaded logical link, For a failed logical link i.e., e_{ij} , the traffic rerouted by its improvement. Consider the overall traffic load of failed logical links is T and the recovered traffic load is T_r , then the routing distraction is defined as $T - T_r/T$. The optimal value is minimum means that no traffic is disrupted by failures.

Overload rate: In a test case, we count the logical links traversed by the rerouted traffic and indicate this number as L . We also calculate the overloaded ones between them. A logical link is overloaded if its capability is smaller than the traffic load on it, as well as its individual traffic and the rerouted traffic. Presume there are L_o overloaded logical links. The overload rate is distinct as L_o/L , and it accomplish the negative impact caused by the rerouted traffic.

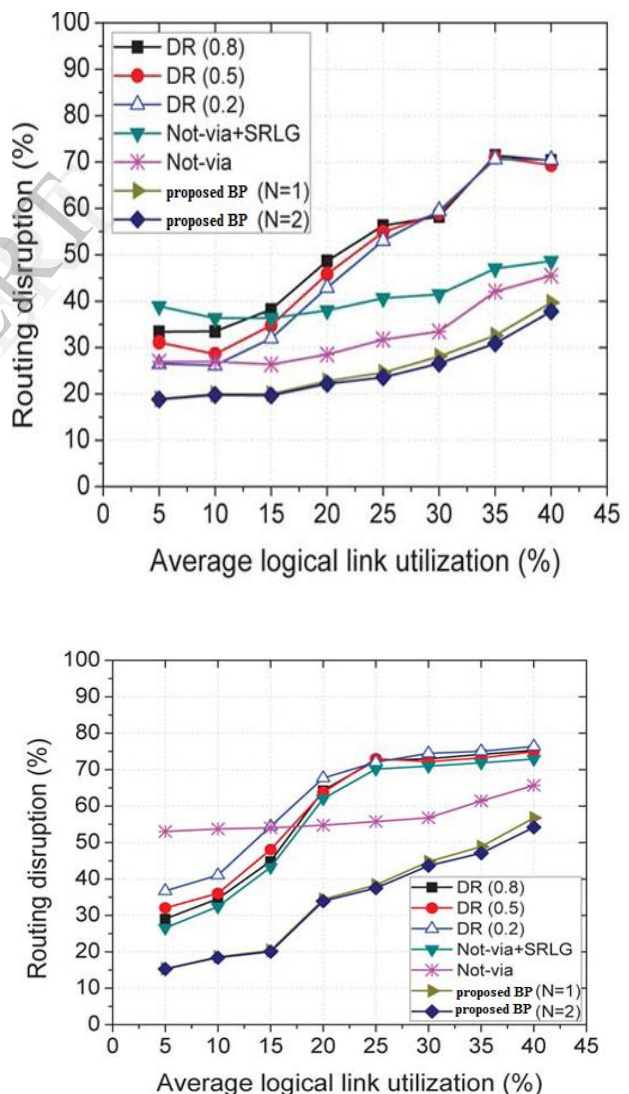


Fig.3.1 Average routing disruption under different logical link utilizations.

In fig.3.1 emphasize two important features of the simulation results. First, utilize more backup paths can minimize the routing disruption, particularly when the logical link consumption is high. The presentation of proposed BP does not differ much when $N \geq 2$ and therefore only show the result when $N = 1$ and $N = 2$. It denotes that two backup paths should be sufficient for defending a logical link. Second, proposed BP better than the other five algorithms beneath different logical link utilizations in each network.

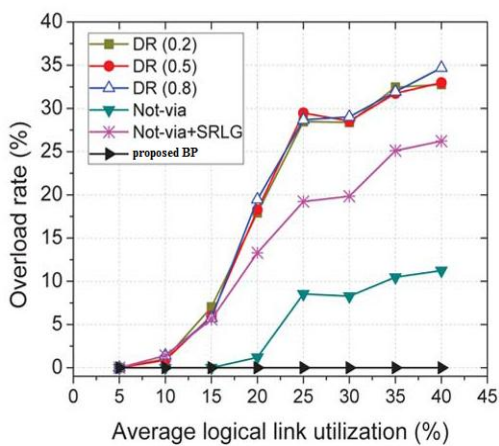
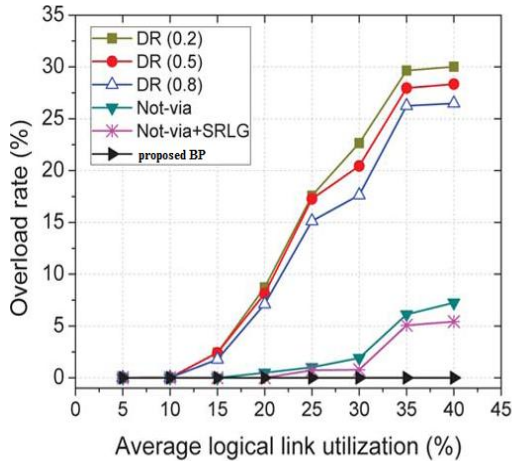


Fig.3.2 Overload rate under different logical link utilizations.

In fig.3.2 proposed BP keep away from logical link overload with two techniques, i.e., utilize logical links with functional bandwidth and managing the rerouted traffic load. Then other five algorithms have quite high overload rate when the logical link usage is higher than 20 percent. in the view of bandwidth constraint, the maximum logical link usage in proposed BP is 100 percent, which denote that proposed BP fully make use of the bandwidth and does not cause logical link overload. Then the other five algorithms that do not think about the bandwidth constraint and therefore some logical links may be worn by many backup paths at the uniform time. As a outcome, the maximum logical link employs in these algorithms is quite high.

IV RESULTS AND DISCUSSIONS

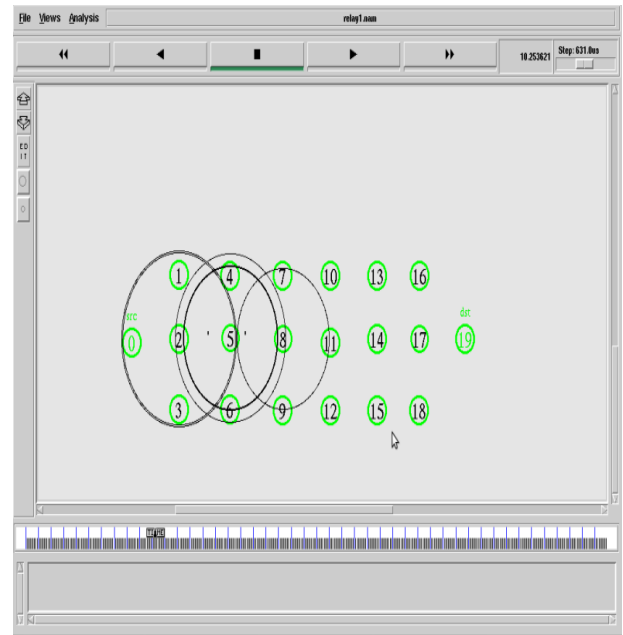


Fig 4.1 packet transfers from source to destination

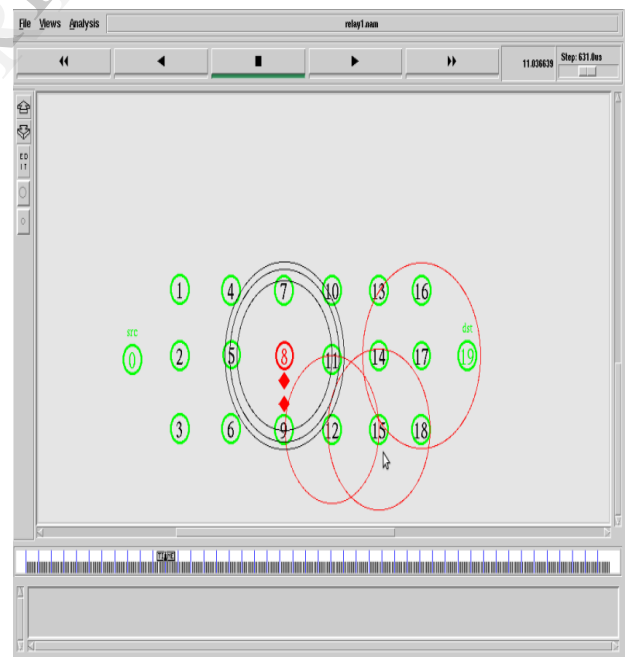


Fig 4.2 packet drops from node 8 due to link Failure.

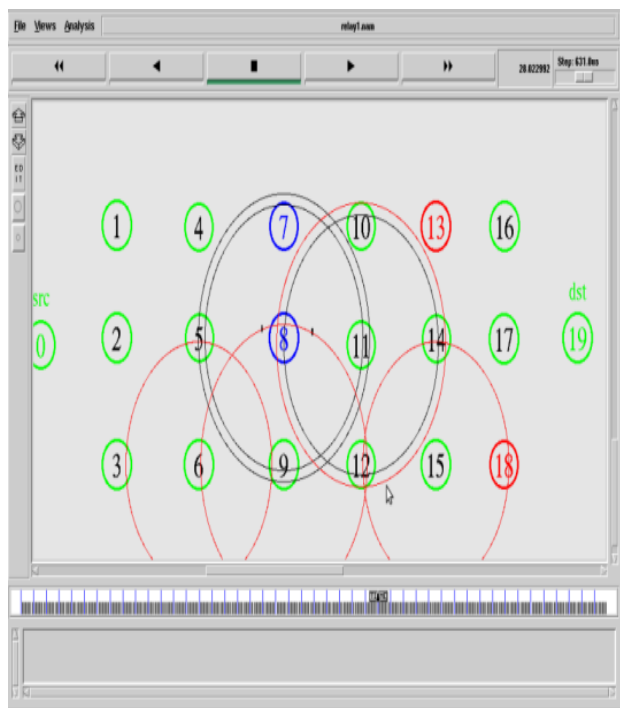
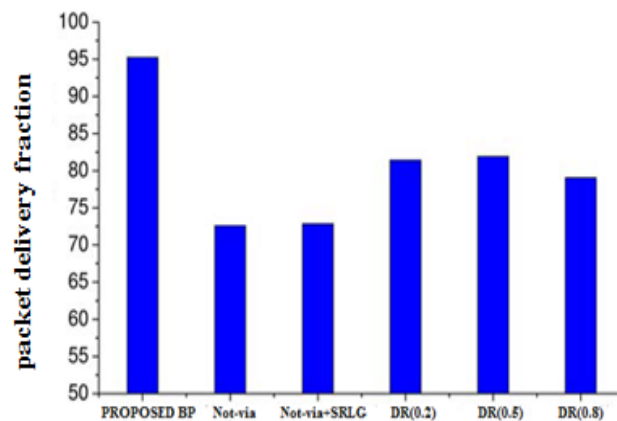


Fig 4.3 signal spanning for traffic rerouting



(a).packet delivery fraction

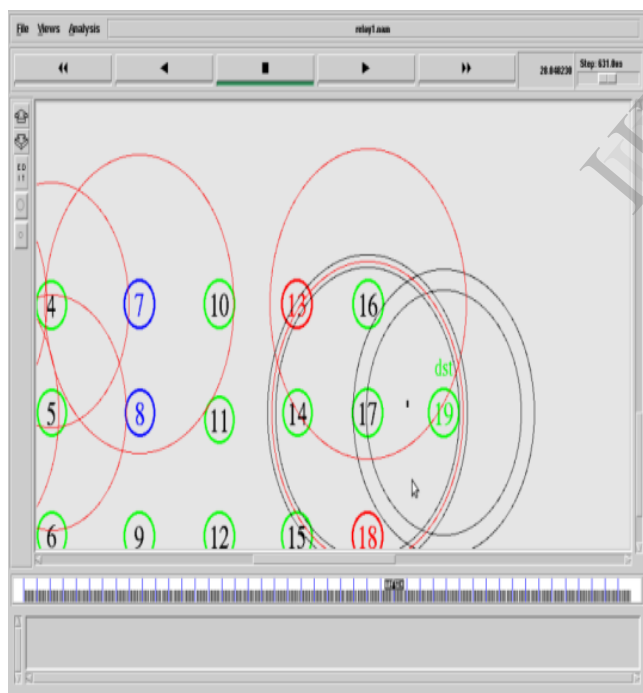
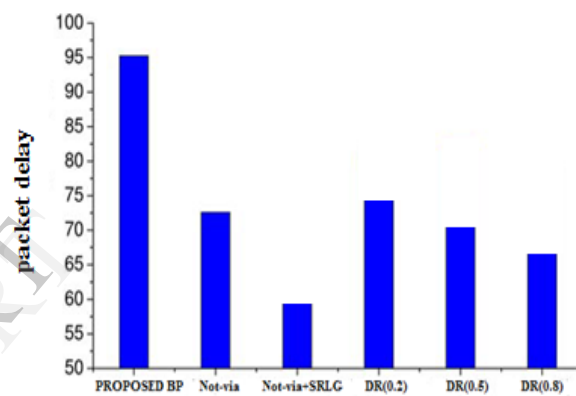
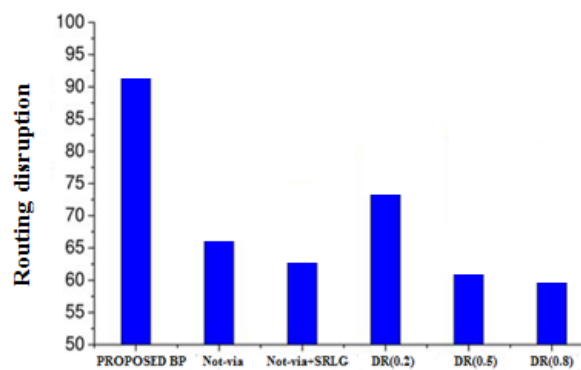


Fig 4.4 multiple backup path from source to destination



(b).packet delay



(c).Routing disruption

IV CONCLUSION

Multiple backup path approach for link failure in IP networks develop a probabilistically correlated failure (PCF) model to measure the impact of IP link failure on the dependability of backup paths. With this model, A lightweight proactive source routing (PSR) protocol is developed and it is used to minimize the routing disruption by choosing multiple reliable backup paths to protect each IP link. It ensures that the redirected traffic does not cause logical link overload, even when multiple logical links fail simultaneously.

REFERENCES

1. Qiang Zheng, Guohong Cao, F.Thomas ,La Porta, and Ananthram “Cross-Layer Approach for Minimizing Routing Disruption in IP Networks” vol. 25, no. 7, july 2014.
2. 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.
3. 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.
4. E. Oki, N. Matsuura, K. Shiimoto, 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.
5. Q. Zheng, J. Zhao, and G. Cao, “A cross-Layer Approach for IP Network Protection,” in Proc. IEEE/IFIP DSN, 2012, pp. 1-12.
6. 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.
7. A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot, “Characterization of Failures in an Operational IP Backbone Network,” IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 749-762, Aug. 2008.
8. H.-W. Lee and E. Modiano, “Diverse Routing in Networks with Probabilistic Failures,” in Proc. IEEE INFOCOM, 2009, pp. 1035-1043.
9. 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.
10. S. Bryant, M. Shand, and S. Previdi, “IP Fast Reroute Using Not-via Addresses”, Internet draft, 2011. [Online]. Available: <http://tools.ietf.org/html/draft-ietf-rtgwg-ipfrr-notvia-addresses-03>.