Minimizing Routing Interruption through Backup Paths with Energy Saving and Routing Attacks in IP Networks

Varsha Gosavi, Prof. S. P. Pingat

***Abstract*— Today, the internet is one of the most powerful tools in communication throughout the world. In wired connection there is communication between two nodes which are connected to each other through the link. It is observed that IP link failures occur in the internet. There are various reasons of IP link failures in the internet such as internet backbone and disconnection of a link for several seconds can lead to millions of packet loss. Hence quickly recovering from IP link failures is important for improving internet reliability and availability. To avoid all these issues by using backup paths. Backup paths are commonly used for protecting IP links from failures in IP networks. Backup path is an alternate path in the network while exiting is unavailable. With the probabilistically correlated failure (PCF) model, user chooses reliable backup paths for minimizing routing interruption. When link fails, its data is split onto multiple backup paths which reduce the load of the network. Here proposed a technique of minimizing routing interruption with energy saving and avoid routing attacks using risk aware mitigation in IP networks.**

Keywords — Routing, failures, recovery, IP networks, backup paths

I. INTRODUCTION

Internet takes important role in our daily life for many online services such as online transactions, online shopping and for other e-commerce applications. The internet has become most powerful tools and widely used infrastructure for a large range of communication and other services. When network became failure at that time internet goes from slow convergence of routing protocols. The most important aim in the internet is the ability to regain from failures.

Generally in IP networks, a link or node failure occurs. In the internet there are many causes of IP link failures like internet backbone and disconnection of a link. When a link fails in IP networks, there is loss of data which is flowing currently through the link. Thus, quickly recovering from IP link failures is important to enhance internet reliability and availability. Currently backup paths are commonly used to protect links from failures in IP network. Backup path is an alternate path in a network while exiting path is unavailable. Backup path is widely used by Internet Service Providers (ISPs) to protect their domain. When a link failure is found, traffic originally crossing the link is quickly shifted to the backup path of this link. In this way routing interruption is minimized.

Now, in the IP networks whole connections are based on the Wavelength Division Multiplexing (WDM) layered structure. In the network there are logical links which are connected straightforwardly to the communicating nodes which are in between source and destination. In this layered structure the logical topology is fixed on the physical topology. Physical links are nothing but fiber links. Logical links are nothing but IP links. A logical link may be composed of multiple fiber links and multiple logical links may share a fiber link.

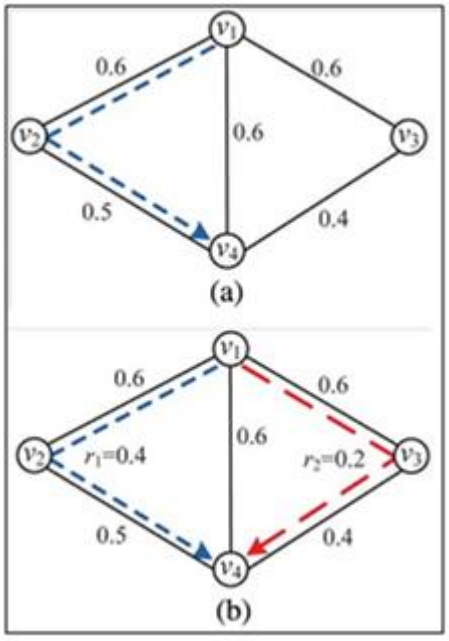

Fig. 1 Logical Topology. (a) Single backup path have not enough bandwidth. (b) The rerouted traffic is split on two backup paths [3].

Fig.1 shows logical topology. There are five nodes and five edges in that topology. In Fig. 1(a) v_1 utilizes a single backup path for protecting $e_{1,4,}$ whose usable bandwidth is min{1-0.6, 1-0.5}=0.4. The total load traffic will exceed its bandwidth after $e_{1,4}$ fails and therefore link overload occurs. With the help of two backup paths to protect $e_{1,4.}$ In Fig. 1(b) the traffic load divided onto the left one is 0.4 after $e_{1,4}$ fails and that onto the right one is 0.2. Using multiple backup paths, IP link is protected.

Here proposed to minimize routing disruption caused by IP link failures. The basic idea is to defend each IP link with multiple reliable backup paths and considers the correlation between logical link failures. Here developed probabilistically correlated failure (PCF) model based on the topology mapping and failure probability of logical links and physical links. The PCF model presented an algorithm to select N reliable backup paths for each IP links.

The objective of proposed model is to minimize routing interruption of the whole network and achieves ensure packet delivery across IP networks. First of all system search the shortest path between source to destination with the help of Dijkstra's algorithm. Then system creates packet of entered message and send over the shortest path. There are two cases in that system, first is link failure occurs and second is link failure does not occur. If there is not link failure the packet will send to destination successfully. If there is link failure occur then packet will be divided and send through backup paths calculated by our system. That means system proposes an algorithm to find more reliable backup paths with the help of PCF model. Then switch off links which are unused for saving energy and find malicious node to avoid routing attacks.

II. LITERATURE SURVEY

A. Survey

Amund Kvalbein *et. al* proposed a Multiple Routing Configurations(MRC) model [4]. It gives certainty of that link as well as node failures are fast recovered in failed IP network. MRC is based on the principle of storing the additional information of routing in the routers. When there is unprotected of failure at some link the flow of data is immediately moved through the alternate output link. This technique is suitable for all single link failure scenarios, to manage both link and node failures using a single mechanism instead of knowing the causes of failures. It works on hop-by-hop forwarding and is connectionless technique. MRC forms a small set of backup network configuration by using network graph and links associated with it.

Qiang Zheng *et. al* proposed an approach called Reactive Two-phase Rerouting(RTR) [5]. This approach works for intra domain routing to rapidly recovery from failures with the shortest recovery paths. The approach name suggests two phases. In first phase, RTR forwards packets around the failure area to collect failure details. In second phase, RTR computes the shortest path and forwards packets through source routing. This approach handles the network of any mapping for recovering and selecting shortest path up to destination. Simulation of this approach based on ISP topology show that RTR can discover the recovered shortest paths.

Shrinivas Kini *et. al* proposed a scheme [6] for dual link failure recovery of networks. It works on the principle of rerouting of one failed link without knowing the second link failure i.e. rerouting is not dependent of other failed links. This technique needs three protection addresses for each node in the network along with normal address and three protection graphs joined with them. Each protection graph is always two-edge connected with guarantee. In dual link failure the network is recovered by tunneling the packets from first failure with the help of protection addresses and packet is routed. This proposal leads to the conclusion that three protection addresses for every node are sufficient for the dual link failure recovery.

M. Hou *et. al* enhances a technique [7] for finding backup paths in advance effectively to minimize the response time. Usually backup paths are chosen most disjoint path from the primary path, backup paths are computed for each and every links. There are two cases for choosing backup paths first, for all the links in the network may fail with equal probability and second, for the links which are not protected or shared links. All the links are not equally vulnerable to the failure in the network, even though it is not cost effective to provide full protection scheme for all the links. In this proposal cost may not be effective, CERNET2 analyze the failures from the real world traces. In this mechanism propose a novel critical-protection algorithm which is fast itself.

Matthew Johnston *et. al* proposed a technique [8] for random link failure handling with the help of backup network. Here backup network is designed. The traffic is rerouted via pre-planned backup path after link failure in the network. Backup networks are a low-cost and which are provided protection against random failures. Backup networks consist of shortest backup paths. When primary links become more failure resistant, the backup networks use ideally for additional resource sharing amongst available paths. Here the design of backup network under random link failures is done based on the robust optimization.

Eiji Oki *et. al* enhances a model [9] in which the disjoint path selection mechanism with the constraints of SRLG for the networks of Generalized Multi-Protocol Label Switching (GMPLS). This mechanism is also known as Weighted SRLG (WSRLG) mechanism. At the time of execution of shortest path algorithm the number of SRLG members are describe to a link as part of the link cost. In WSRLG, a link which has many SRLG members are hardly selected as the shortest path. This mechanism concludes that the SRLG is best for selection of disjoint paths over the conventional shortest path algorithm.

Lu Shen *et. al* proposed the model [10] which gives different types of services at option layer of the network. The problems in the constraints of static provision is managed and expressed in different terms of resource availability. SRLG-diverse path protection schemes have 3 classes such as dedicated, shared and unprotected. When the network resources are enough the capacity minimization problem is formulated with the objective of minimizing the number of usable wavelength-links. When network resources are not enough, then revenue maximization problem is formulated for revenue value.

Hyang-Won Lee *et. al* enhances a model [11] in which developed different routing schemes to deal with numerous, correlated, failures. Recovery from multiple failures is not

ISSN: 2278 – 1323

assured till single link-failure handled with disjoint path protection. By taking probabilistic picture of network failures where multiple failures events can occur at the same time and developed a Probabilistic Shared Risk Link Group (PSRLG) framework for handling correlated failures.

B. Motivation

Routing is the process of choosing best path for sending data packets from source to destination in the network. There are different techniques are used to choose best path such as Ant colony optimization technique, Dijkstra's algorithm etc. There is link failure occurs in the network which leads to the loss of data. So quickly recovering from link failures is vital to enhance internet reliability and availability. Backup paths are used to protect IP links from failures. At this moment backup paths are widely used by ISP to protect their domain. In this system there is a model which develop an algorithm to reduce routing interruption by choosing reliable backup paths. That model is Probabilistically Correlated Failure (PCF). This system considers both bandwidth constraints and reliability of backup paths.

III. PROPOSED MODEL

A. Model[2]

The proposed system sends the data from source to destination successfully. Loss of data during link failures can be retrieved by using backup paths. Backup paths are nothing but alternative ways to send data from source to destination in the IP networks.

Fig. 2 shows the architecture of the system. Initially user selects shortest path using Dijkstra's algorithm for sending data packets from source to destination successfully. User applies selectBP and selectBC algorithm when link is failure for sending multiple reliable backup paths in the network during sending data packets. User can be saved energy by using energy saving strategy in that user can switch off the links which are unusable. At the time of packet transmission, checks malicious node and avoid that attacks via risk aware mitigation. At last user sends data from source to destination properly.

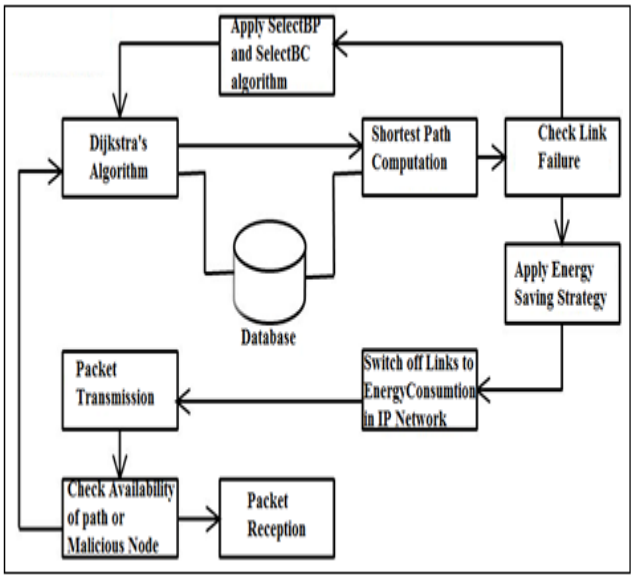

Fig. 2 System Architecture [2]

In case of link failure: First of all user searches the nodes. If there are a large number of nodes then build the network topology. User can choose his source and destination. After that he chooses shortest path according to the Dijksrta's algorithm. When there is link failure then apply two algorithms i.e. selectBP and selectBC. User finds two reliable backup paths by using those algorithms to protect each IP link. Then split the data packets on two equal parts. When paths are fixed switch off the links which are not usable for saving energy. And also verify is there any malicious node. If there is malicious node then avoid that's attack using risk aware mitigation. At last user sends his data at destination properly.

In case of without link failure: First of all user searches the nodes. If there are a large number of nodes then build the network topology. User can choose his source and destination. After that he chooses shortest path according to Dijkstra's algorithm. When paths are fixed switch off the links which are not usable for saving energy. And also verify is there any malicious node then avoid that attacks using risk aware mitigation. At last user sends his data at destination properly.

B. Algorithm

Table 1.Table of Notations

Symbols	Representation
Q	Priority Queue
$w(v_i)$	Weight of node v_i
v_i	Node of v_i
v_j	Node of v_j
v_m	Node of v_m

Input: Number of Nodes
Output: Construct backup paths

1. for each node consider the failure Probability from v_m to v_i.
2. visit (v_i) ← 0 flag to denote if vi is visited
3. prev (v_i) ← NULL previous node of v_i
4. end for
5. Initialize priority queue Q,
6. while Q = null do
7. extract the node vi with Minimum Probability from Q
8. if w(v_i) = ∞ then
9. break
10. end if
11. select not visited node v_i
12. for each neighbor of vi with visit (v_j) = 0 do
13. check for path from neighbors
14. if neighbor v_j minimum Probability select
15. else discard node
16. back to pervious node v_i
17. end if
18. end for
19. end while
20. Construct path

IV. Results and Discussion

The objective of proposed model is to minimize routing interruption of the whole network and achieves ensure packet delivery across IP networks. First of all system search the shortest path between source to destination with the help of Dijkstra's algorithm. Then system creates packet of entered message and send over the shortest path. There are two cases in that system, first is link failure occurs and second is link failure does not occur. If there is not link failure the packet will send to destination successfully. If there is link failure occur then packet will be divided and send through backup paths calculated by our system. That means system proposes an algorithm to find more reliable backup paths with the help of PCF model. Then switch off links which are unused for saving energy and find malicious node to avoid routing attacks.

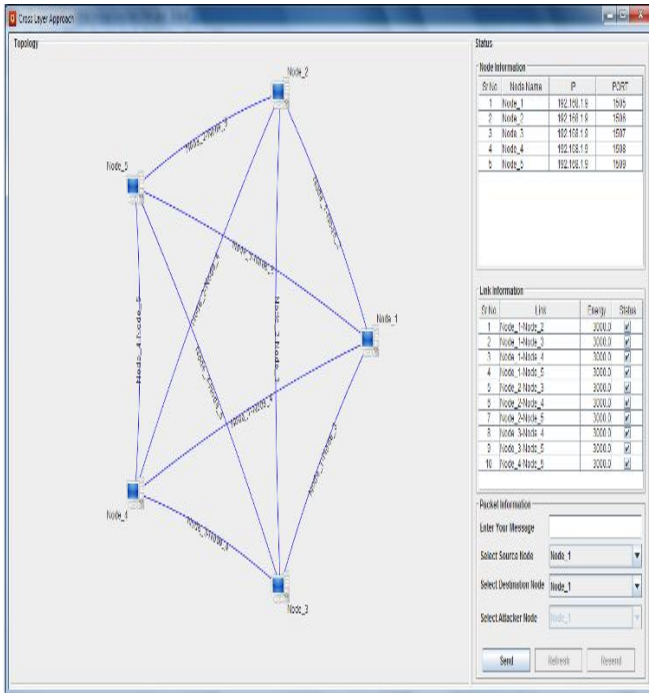

Fig. 3 Main GUI of system

In Fig.3 shows main GUI of the system. There are 5 nodes and 10 edges. In Fig.4 shows message sends after link failure using backup paths. In that topology node1 is source and node2 is destination. Link of red color is failure link in between source to destination hence send the message using two backup paths i.e.path1 is node1-node3-node2 and path2 is node1-node4-node2.

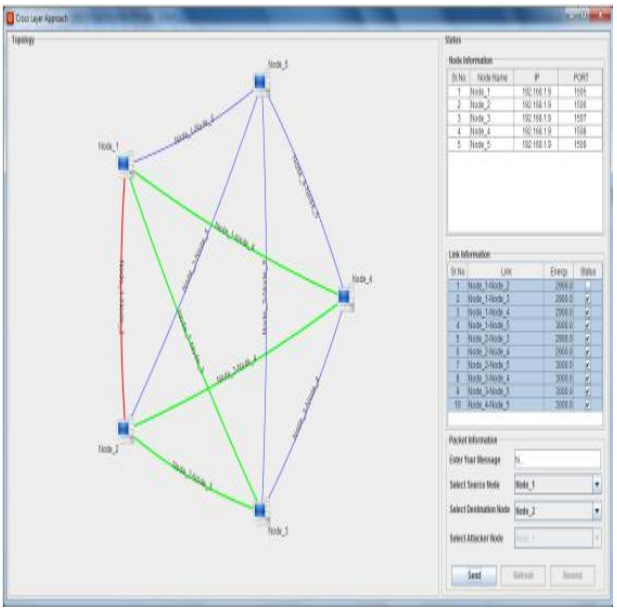

Fig. 4 Message send after link failure using backup paths.

ISSN: 2278 – 1323

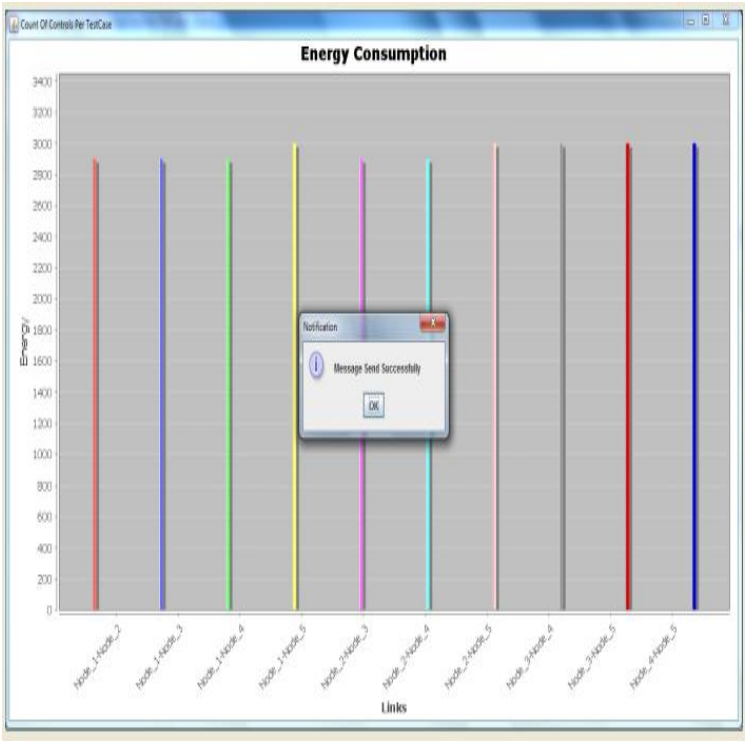

Fig. 5 Links Vs Energy

The above graph shows Links Vs Energy. From the above graph it is observed that energy is conserved during sending message. In that topology , switch off the links which are not used for saving energy.

V. CONCLUSION

This paper proposes the system which is useful for minimizing routing disruption caused by link failures in IP networks. Backup paths are widely used for protecting IP links from failures in the network. This system proposes an energy conservation which is based on the energy saving strategy in that switch off the links which are not used. In the network, the system provides security against malicious node i.e. the system avoids routing attacks.

The system can be made more specialize to manage node failures in IP networks through localized on demand Link State Routing. This Advanced future proposal heads to the increasing the scope of system from link to the node in IP networks.

REFERENCES

[1] Varsha Gosavi, Prof. S. P. Pingat, "Survey of Handling Routing Disruption in IP Network", in *International Journal of Advanced Research in Computer Science and Software Engineering* **,** Volume 4, Issue 11, November 2014 .

[2] Varsha Gosavi, Prof. S. P. Pingat, "Minimizing Routing Interruption with Energy Saving and Risk Aware Mitigation for Routing Attacks in IP Networks", *Proceedings of Fourth Post Graduate Conference of Computer Engineering, cPGCON 2015*.

[3] 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*.

[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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

