International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Minimizing Routing Disruption along with Energy Saving and Risk Aware Mitigation for Routing Attacks in IP Networks

Varsha Gosavi[1], S. P. Pingat[2]

[1]PG Student, Computer Dept., SKNCOE, Sinhagad Road, Pune, India

[2]Professor, Computer Dept., SKANCOE, Sinhagad Road, Pune, India

Abstract: ***Today, the internet takes important role in communication infrastructure throughout the world. There is communication between two nodes which are connected to each other through the link in the wired connection. It is viewed that IP link failures occur in the internet. IP link failures are common in the internet for various causes such as internet backbone and disconnection of a link. These various causes can lead to millions of packet loss for several seconds. Therefore, quickly recovering from IP link failures is important for improving Internet availability and reliability. To avoid all these issues by taking help of Backup paths. In IP networks backup paths are commonly used for protecting IP links from failures. Backup path is nothing but the alternate path in the network while existing path is not available. With Probabilistically Correlated Failure (PCF) model, user chooses suitable backup paths for minimizing routing disruption. When link failures are occur, data is divided onto multiple backup paths which reduce the load of the network. Here proposed a technique of minimizing routing disruption with energy saving and avoid routing attacks via risk aware mitigation in IP networks***

Keywords: routing, failure, backup paths, IP networks

1. Introduction

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

Commonly in IP networks, a link or node failure occurs. In the internet there are several reasons of IP link failures like disconnection of a link and internet backbone. In IP networks when link failures occur, there is loss of data which is flowing currently through the link. So, rapidly recovering from IP link failures is important for enhancing Internet availability and reliability.

Currently backup paths are generally used to protect links from failures in IP networks. Backup path is nothing but alternate path in the network while existing path is not available. Backup path is generally used by ISP to protect their domains. When link failure is discovered, traffic originally crossing the link is rapidly shifted to the backup path of this link. In this way routing disruption is minimized.

Currently, IP network is built on the Wavelength Division Multiplexing (WDM) layered structure. In this layered structure, the IP layer topology (logical topology) is fixed on the optical layer topology (physical topology). Each logical link is mapped to a lightpaths in the optical layer. IP links are nothing but logical links. Fiber links are nothing but physical links. An IP link may be composed of multiple fiber links and multiple IP links may share a fiber link.

As shown in Figure 1 logical topology which contains five edges and four nodes. In fig. 1(a) v_1 uses a single backup path for protecting $e_{1,4}$ whose usable bandwidth is {1-0.6, 1-0.5} =0.4. When $e_{1,4}$ fails, the total load traffic will exceed its bandwidth, and therefore link overload occurs. This approach protects $e_{1,4}$ with the help of two backup paths. In Fig. 1(b) when $_{e1,4}$ fails the traffic load spilt onto the right one is 0.2 and that onto the left one is 0.4. IP link is protected by using multiple backup paths.

Here proposed to minimize routing interruption caused by IP link failures in IP networks. The basic idea is to protect each IP link with multiple reliable backup paths and considers the correlation between logical link failures. Here developed PCF model based on the topology mapping and failure probability of IP links (logical links) and fiber links (physical links). The PCF model proposed an algorithm to minimize the routing interruption by choosing N reliable backup paths to protect each IP links.

The main aim of proposed model is to minimize routing disruption of the whole network and achieves ensure packet delivery across IP networks. First of all system finds the shortest path between source and destination by using Dijksra's algorithm. After finding shortest path, system creates packet of entered message and send over the shortest path. There are two cases in system, first is link failure does not occur and second is link failure occurs. If there is link failure does not occur then packet is successfully delivered to destination node. If there is link failure occurs in IP network then packet will be divided and send through alternative paths i.e. backup paths calculated by this system. The system proposes an algorithm to find multiple reliable backup paths

with the help of PCF model. Then switch off the links which are not used for saving energy and find malicious node to avoid routing attacks using risk aware mitigation. Ultimately send the data from source to destination.

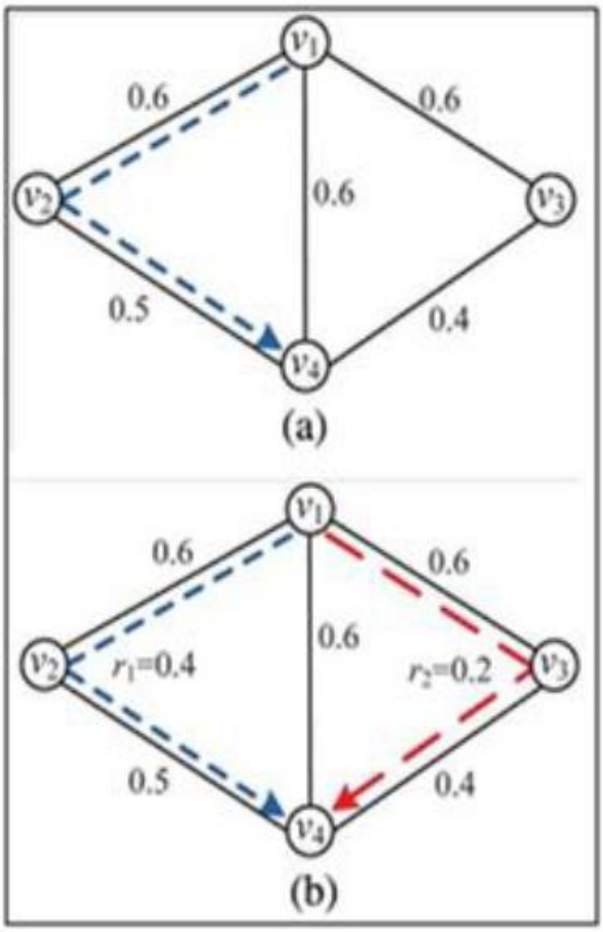

Figure 1: Logical Topology (a) Single backup path have not sufficient bandwidth.(b) The traffic is split on two backup paths [4].

2. Related Work

2.1 Survey

Amund Kvalbein *et.al* enhances a technique of Multiple Routing Configurations (MRC) model [5] which gives certainty of that link and node failures are fast recovered in failed IP networks. Multiple Routing Configurations (MRC) is built on the principle of storing additional information of routing in the routers and also it allows packet forwarding to move an alternate output link immediately in case of detection of failures. This technique gives surety recovery in all single failure scenarios, to manage both node and link failures by using a single mechanism instead of knowing the reasons of failures. It is connectionless technique and based on hop-by-hop forwarding only at destination. Multiple Routing Configurations (MRC) generates network configuration for the backup paths with the small set by using network mapping graph and links connected with it.

Qiang Zheng *et. al* proposed a scheme called Reactive Two-Phase Rerouting (RTR)[6] . This scheme is working for intra domain routing to quickly recovery from failures with shortest paths. The scheme name suggests two phases. In first phase, quickly recovery from failures and in second phase, finding the shortest recovery paths. Initial stage RTR forwards packets around the failure domain to collect failure details. In second stage, RTR finds shortest path and forwards packets through source routing. This scheme manages the network of any mapping for recovery and finding shortest path up to destination. Simulation of this scheme on the ISP topology shows that RTR can search the recovered shortest paths.

Shrinivas Kini *et. al* proposed an approach [7] for dual link failures recovery in IP networks. It based on the principle of re-routing of one failed link without knowledge of second failed link i.e. re-routing is independent of other link failure. This approach requires three protection addresses for each node in the network along with normal address and three protection graphs connected with them. Each protection graph is two edge connected. The network is recovered from first failure by tunneling the packets in dual link failure with the help of protection addresses and packet is routed. This approach 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 technique [8] for finding backup paths in advance effectively to reduce the response time. Generally backup paths are selected for the optional disjoint path from the primary path, backup paths are computed for all links. The backup paths are selected by two cases first, for all the links in the network may fail with identical probability and second for the links which are unprotected or shared links. All the links are not identically vulnerable to the failure in the network, even so it is not cost efficient to provide full protection scheme for all the links. In this proposal such a cost-effectives technique are proposed like, CENTER2 analyze failure characteristics which are based on the real world traces. In this approach propose a new critical-protection algorithm which is fast itself.

Matthew Johnston *et. al* proposed a mechanism [9] in that backup network is designed. The backup network provides protection from link failure. This mechanism handles random link failure with the help of backup network. The traffic is diverted using pre-planned backup path after link failure in the network. Backup networks provide protection against random failures. Backup network are low-cost. The backup networks have shortest backup paths. Here the design and capacity simulation of the backup network under random link failure is based on the robust optimization. Robust optimization finds a solution to a problem which is robust in an optimization parameters. Fig shows backup network shown as solid links and primary network shown as dotted link.

Eiji Oki *et. al* enhances a model [10] in which the disjoint path selection scheme is used for the networks of Generalized Multi-Protocol Label Switching (GMPLS) with the help of constraints of Shared Risk Link Group (SRLG). This mechanism also called as Weighted SRLG (WSRLG). The numbers of SRLG members are treated as the link cost during the execution of the shortest path algorithm. In

WSRLG a link which has less number of SRLG members are selected as the shortest path. This mechanism concludes with the WSRLG is best for choosing the disjoint paths over the conventional shortest path algorithm.

Lu Shen *et. al* enhances a model [11] which gives various types of services at optical layer of the network. The problem in the constraints of static provision is formulated and handles in various conditions of resources availability. SRLG-diverse path protection schemes are in the three classes such as shared dedicated and unprotected. In the unavailability of the sufficient resources the revenue maximum problem is formulated, whose aim is maximizing the total revenue value. In the availability of sufficient resources the capacity minimization problem is formulated.

Hyang-Won Lee *et. al* proposed a model [12] in which developed different schemes of routing to deal with numerous, potentially correlated , failure. Recovery from multiple failures can't achieve by guarantee till single failure managed with disjoint path protection. By considering probabilistic network failures developed a PSRLG framework for handling correlated failures and found by minimum joint failure probability.

2.2 Motivation

Routing is the processes of selecting best path for sending data packets from source to destination in the network. There are various techniques used to decide best path such as Dijksta's algorithm, Ant Colony optimization technique etc. In the internet there are various reasons of IP link failures such as internet backbone, disconnection of link for several seconds can lead to packets loss. In the network, there is situation like link failure which leads to loss of data. Therefore, rapidly recovery from link failures is important for enhancing internet availability and reliability. Backup paths provide protection for IP links from failures. Currently, backup paths are commonly used by Internet Service Providers (ISPs) to protect their domains. In this system there is a model which develop an algorithm to minimize routing interruption by selecting reliable backup paths. This system considers both reliability of backup paths and also bandwidth constraints.

3. Proposed Model

3.1 Model [2]

This system sends data from source to destination successfully by using shortest path or alternative backup paths. Loss of data during link failures can be recovered by using backup paths. Backup path is nothing but the alternate path in the network while existing path is not available.
Fig2. shows system architecture. At first, user selects shortest path by using Dijkstra's algorithm for sending data from source to destination successfully. When link is failure user can apply selectBP and selectBC algorithm for selecting multiple reliable backup paths in the network during sending data packets. User can be conserved energy by using energy conservation strategy in that user can switch off the links which are not used. During packet transmission verify malicious node avoid that attacks via risk aware mitigation. Ultimately user sends data from source to destination successfully.

In case of link failures: Initially user finds the nodes. With the help of this nodes create the network topology. User can choose his source and destination for sending data packets. According to Dijkstra's algorithm finds shortest path. When link failure occurs then apply two algorithms i.e. selectBP and selectBC. By using those algorithms system finds two reliable backup paths to protect each IP link from failures in IP networks. Then data packets are divided on two equal parts. When paths are fixed switch off the links which are not used for saving energy. Check is there malicious node. If there is malicious node then it avoids via risk aware mitigation. Finally system sends his data at destination through backup paths.

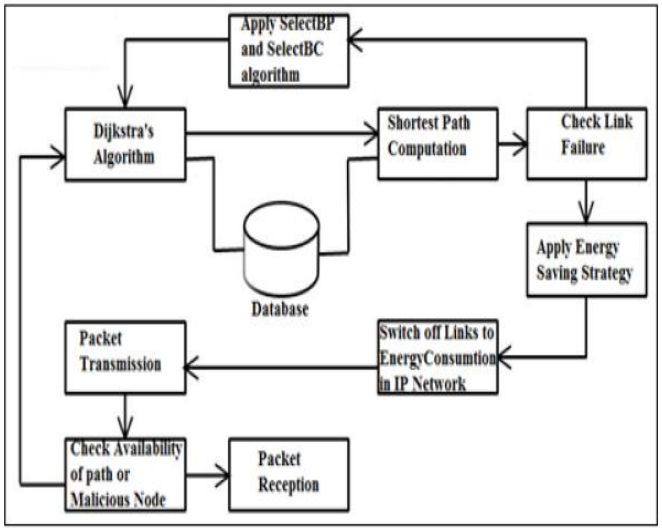

Figure 2: System Architecture [2]

In case of without link failure: Initially user finds the nodes. With the help of this nodes system creates network topology. User can choose his source and destination for sending data packets. According to Dijksra's algorithm finds shortest path. When paths are fixed switch off the links which are not used for saving energy. Check there is malicious node. If there is malicious node then it avoids that attack via risk aware mitigation. Finally system sends data at destination through backup paths.

3.2 Algorithm

Table Lookup capability Bypass Transformation (TLBT)
Input: ShortestPath sp, MultipleLinks ml, Energy Reduction Constant erc=100
Output : Reduce energy of used links and keep other links ideal
Step 1 : Identify ShortestPath sp
Step 2 : If sp == DirectLink link
Capacity = link.getCapacity-erc;
link.setLinkCapacity = Capacity;
Step 3 : Else If sp Contains MultipleLinks
For Each Link link : AllLinks {
For Each Link usedlink : MultipleLinks

```
If usedlink == link
Capacity = link.getLinkCapacity-erc;
link.setLinkCapacity = Capacity;

                    Else
Capacity = link.getLinkCapacity;
                    link.setLinkCapacity =
                Capacity;
}
```

Step 4 : Refresh link energy table with updated link capacities

Here,

DirectLink - represent direct path between source and destination node.

ShortestPath - Shortest path deriver by system.

Link - Link between two nodes.

MultipleLinks - List of link that are present in two shortest path derived by system.

Capacity - Represent current energy of links.

4. Result and Discussion

The main aim of proposed model is to minimize routing disruption of the whole network and achieves ensure packet delivery across IP networks. First of all system finds the shortest path between source and destination by using Dijksra's algorithm. After finding shortest path, system creates packet of entered message and send over the shortest path. There are two cases in system, first is link failure does not occur and second is link failure occurs. If there is link failure does not occur then packet is successfully delivered to destination node. If there is link failure occurs in IP network then packet will be divided and send through alternative paths i.e. backup paths calculated by this system. The system proposes an algorithm to find multiple reliable backup paths with the help of PCF model. Then switch off the links which are not used for saving energy and find malicious node to avoid routing attacks using risk aware mitigation. Ultimately send the data from source to destination.

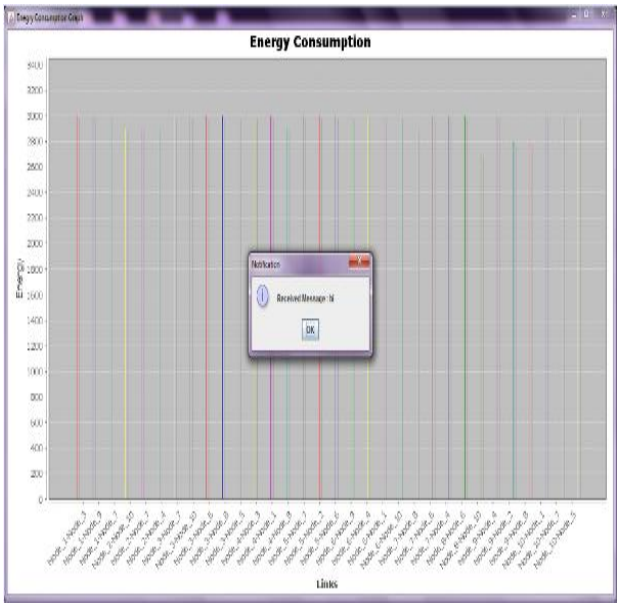

Figure 3: Links Vs Energy

The above graph shows Links Vs Energy. From the below graph it is observed that energy is conserved at the time receiving message. In the system topology, switch off the links which are unused for saving energy.

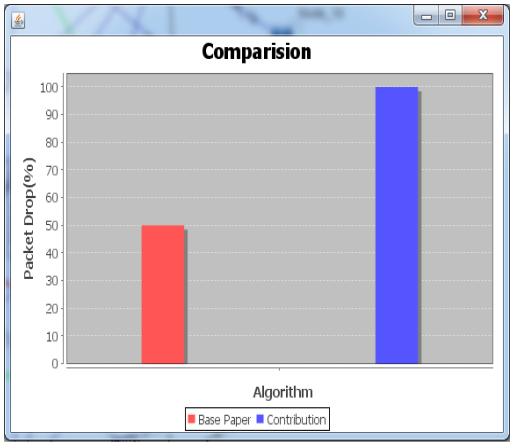

Figure 4: Comparison between existing topology and proposed system

The above graph shows comparison between existing topology and proposed system. In existing topology there is loss of packets. In proposed system there is no loss of packets.

5. Conclusion

This system is helpful for minimizing routing interruption caused by link failures in IP networks. Backup paths are generally used to protect IP links from failures. This system proposes an energy saving strategy which is based on energy conservation in that switch off the links which are unused. In IP networks, the system provides security against malicious node that means system avoids routing attacks.

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] Varsha Gosavi, Prof. S. P. Pingat, "Minimizing Routing Interruption through Backup Paths with Energy Saving and Routing Attacks in IP Networks", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 5, May 2015.*

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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