Volume 3, Issue 1 (2015) 164-167 ISSN 2347 - 3258
International Journal of Advance Research and Innovation

Alternate Path Selection in IP Networks using Bandwidth Optimization

A. Indira Devi *, N. Arthi
Department of Computer Science Engineering, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Anna University, Chennai, India

Article Info
Article history:
Received 21 January 2015
Received in revised form
15 February 2015
Accepted 28 February 2015
Available online 15 March 2015

Keywords
IP Link,
ISP,
Routing,
Backup Paths,
Failure,
Cross-layer

Abstract
Computer communication has been going through major changes throughout the last decades. Since TCP/IP was a protocol designed for wired networks, wireless transmission poses unique challenges to the well-defined and rigid protocol stack. Routing in ISP environment is challenging the clear path when the IP link was failure. In this paper, a Cross-layer approach is used to minimize routing disruption in IP networks. A model called probabilistically correlated failure (PCF) model was developed to quantify the impact of IP link failure on the reliability of backup paths. In PCF model, an algorithm is used to choose multiple reliable backup paths to protect each IP link. When an IP link fails, its traffic is split onto multiple backup paths to ensure that the rerouted traffic load on each IP link does not exceed the usable bandwidth. To evaluate this issue, the system has to be developed with real ISP service in particular network topology support. Entire path is initially used to select specific path, then backed up path are reused and tested by splitting entire bandwidth based on usage. The probability result will ensure the reliability and dedicated path of data transfer purpose. This kind of approach resolve the issue rose at high end data transaction application like VOIP, Video streaming etc.

1. Introduction

In recent years the Internet has been transformed from a special purpose network to a ubiquitous platform for a wide range of everyday communication services. The demands on Internet reliability and availability have increased accordingly. A disruption of a link in central parts of a network has the potential to affect hundreds of thousands of phone conversations or TCP connections, with obvious adverse effects. The ability to recover from failures has always been a central design goal in the Internet. IP networks are intrinsically robust, since IGP routing protocols like OSPF are designed to update the forwarding information based on the changed topology after a failure. This network-wide IP re convergence is a time consuming process, and a link or node failure is typically followed by a period of routing instability. During this period, packets may be dropped due to invalid routes.

This phenomenon has been studied in both IGP and BGP context, and has an adverse effect on real-time applications. Events leading to a re-convergence have been shown to occur frequently. Much effort has been devoted to optimizing the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation, but the convergence time is still too large for applications with real time demands

Proposed scheme guarantees recovery in all single failure scenarios, using a single mechanism to handle both link and node failures, and without knowing the root cause of the failure. MRC is strictly connectionless, and assumes only destination based hop-by-hop forwarding. MRC is based on keeping additional routing information in the routers, and allows packet forwarding to continue on an alternative output link immediately after the detection of a failure.

Corresponding Author,
E-mail address: indu.cutie@gmail.com

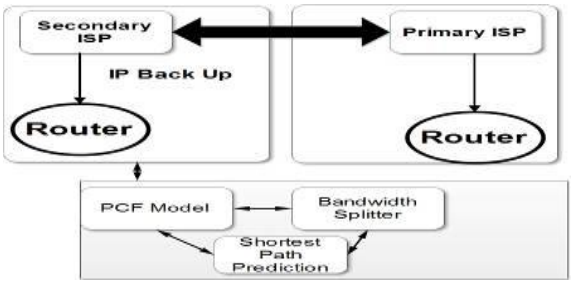

Fig: 1. Architectural Design for Selecting Backup Path

2. Existing System

Existing approaches mainly focus on choosing reliable backup paths to reduce the routing disruption caused by IP link failures. Logical link failures were considered as independent events and or modeled as a Shared Risk Link Group (SRLG). Link and Node failures will occur in IP networks. The slow convergence of routing protocols after a network failure becomes a growing problem. Packet loss or packet delay due to congestion. Time consumed to send the data is increased due to resending of lost data.

2.1 Disadvantages

The selected backup paths may be unreliable. They Consider backup path selection as a connectivity problem, but ignore the traffic load and bandwidth constraint of IP links. Logical link failures are not independent because of the topology mapping. Most prior works select single backup path for each logical link. Load Distribution failure and Congestion may occur.

3. Proposed System

The basic idea is to consider the correlation between IP link failures in backup path selection and protect each IP link with multiple reliable backup paths. A key observation is that the backup path for an IP link is used only when the

IP link fails. To develop a probabilistically correlated failure (PCF) model based on the topology mapping and the failure probability of fiber links and logical links. With the PCF model, an algorithm is proposed to select at most N reliable backup paths for each IP link and compute the rerouted traffic load on each backup path. A new scheme for handling link and node failures in IP networks was proposed. Multiple Routing Configurations (MRC) is a proactive and local protection mechanism that allows recovery in the range of milliseconds. MRC guarantees recovery from any single link or node failure, which constitutes a large majority of the failures experienced in a network. MRC makes no assumptions with respect to the root cause of failure, e.g., whether the packet forwarding is disrupted due to a failed link or a failed router. MRC is based on building a small set of backup routing configurations that is used to route recovered traffic on alternate paths after a failure Recovery in all single failure scenarios without knowing root cause of the failure Each and Every Node having Preconfigured Backup Path. That Backup path maintains the routing table. MRC assumes only destination of hop by hop forwarding.

3.1 Backup Path-Based IP Link Protection

In the current Internet, each router monitors the connectivity with its neighboring routers. When a logical link fails, only the two routers connected by it can detect the failure. Hence, a router may not have the overall information of failures in the network. Although the failed logical links can be identified within a few seconds [10], this waiting time translates to a lot of dropped packets on a high bandwidth optical link. As a result, a recovery approach cannot wait until finishing collecting the overall information of failures and then reroute traffic. Instead, backup paths are widely used to quickly reroute the traffic affected by failures. In backup path-based IP link protection, a router pre-computes backup paths for each of its logical links. On detecting a link failure, the router immediately switches the traffic originally sent on that logical link onto the corresponding backup paths. After the routing protocol converges to a new network topology, routing paths will not contain the failed logical link and the router has a reachable next hop for each destination. Therefore, the router stops using the backup path to reroute traffic. Moreover, routers re-compute backup paths based on the new network topology.

4. Probabilistically Correlated Failure Model

This section describes the probabilistically correlated failure (PCF) model.

4.1 Motivation

There are two types of IP link failures in the Internet, i.e., independent failures and correlated failures. Independent failures are unrelated. They occur for several reasons, such as hardware failures, configuration errors, and software bugs. Correlated failures are mainly caused by failures of fiber links carrying multiple logical links. When a logical link has a correlated failure, it implies that some other logical links sharing fiber links with it may also fail.

Since each router only monitors the connectivity with its neighboring routers, routers cannot determine whether a logical link failure is independent or correlated. The failure of ei;j implies that the logical links sharing at least one fiber link with ei;j may also fail with a certain probability. A PCF model was developed and it is based on the topology mapping and the failure probability of fiber links and logical links. The PCF model considers the probabilistic relation between logical link failures. The objective is to quantify the impact of a logical link failure on the failure probability of other logical links and backup paths. With the PCF model, propose an algorithm is proposed to choose reliable backup paths to minimize the routing disruption.

4.2 The PCF Model

The PCF model is built on three kinds of information, i.e., the topology mapping, failure probability of fiber links, and failure probability of logical links, all of which are already gathered by ISPs. ISPs configure their topology mapping, and thus they have this information. The failure probability of fiber links and logical links can be obtained with Internet measurement approaches [9] deployed at the optical and IP layers. A key observation is that the failure probability of the backup paths for logical link ei;j should be computed under the condition that ei;j fails, because the backup paths are used only when ei;j fails. A backup path is built on logical links, and a logical link is embedded on fiber links. Hence, we first compute the failure probability of fiber links under the condition that ei;j fails. Then, we compute the conditional failure probability of logical links and backup paths. The unconditional failure probability of logical link ei; j is denoted by pi,j €[0,1], which includes independent and correlated failures. However, it cannot reveal the correlation between logical link failures and thus we cannot directly use it to compute the conditional failure probability of backup paths. Unlike logical links, most fiber link failures are independent.

Assume that a fiber link fails independently with probability qm,n €[0,1]. In practice, we may obtain pi;j and qm;n based on previous logical link failures and fiber link failures. Let defined in Eq. (1) express the mapping between logical link ei;j and fiber link fm;n

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

A logical link is subject to failures and correlated failures are caused by the fiber links carrying multiple logical links. Let Fi;j be the set of fiber links shared by ei;j and other logical links. Fi;j is defined by Eq. (2). Suppose that a fiber link fm;n carries ei;j i.e, $\alpha_{m,n}^{i,j}$=1. If there is another logical link es;t that is also carried by fm;n, f(m,n)is in the set Fi;j

$$F_{i,j} = \left\{ f_{m,n} \middle| a_{m,n}^{i,j} a_{m,n}^{s,t} = 1, e_{i,j} \in E_L, \exists e_{s,t} \in E_L, \forall f_{m,n} \in F_p \right\} \quad (2)$$

5. Selection of Backup Path

An algorithm is used within the PCF model to select multiple backup paths to protect each IP link. This algorithm considers both reliability and bandwidth constraints. It aims at minimizing routing disruption by

choosing reliable backup paths and splitting the rerouted traffic onto them. It controls the rerouted traffic load to prevent causing logical link overload.

5.1 Motivation

This approach considers both reliability and bandwidth constraint. It protects each logical link with multiple backup paths and splits the rerouted traffic onto them, because there may be no individual backup path that has enough bandwidth for the rerouted traffic.

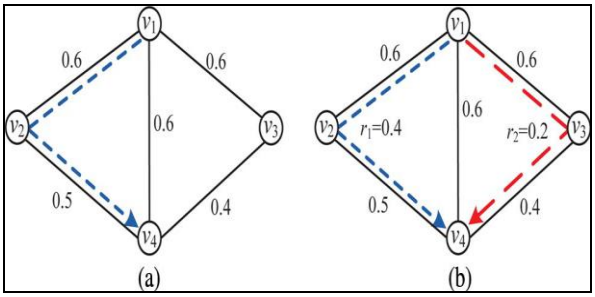

Fig: 2. Motivation for Protecting a Logical Link with Multiple Backup Paths

(a) Single backup path may not have enough bandwidth.
(b) The rerouted traffic is split on two backup paths.

5.2 Problem Definition

Both the reliability of backup paths and bandwidth constraint of logical links are considered in this approach. The objective is to minimize the routing disruption of the entire network, which was also the major objective in prior works. Furthermore, the rerouted traffic load on a logical link should not exceed its usable bandwidth to prevent logical link overload and interfering with normal traffic.

5.3 Algorithm

Algorithm 1 Select BP
Procedure
Initialize a priority queue *Q*
for each logical link $e_{i,j} \epsilon\ E_L$ do
$w_{i,j} \leftarrow p_{i,j} l_{i,j}$ the weight assigned to *wi,j*
$b_{i,j} \leftarrow c_{i,j} - l_{i,j}$ _ the usable bandwidth of *ei,j*
$n_{i,j} \leftarrow 0$ _ the number of backup paths for *ei,j*
$u_{i,j} \leftarrow l_{i,j}$ _ the unprotected traffic load of *ei,j*
ENQUEUE (*Q*, $e_{i,j}$)
end for
while *Q* _≠Ø do
$e_{i,j} \leftarrow$ the logical link in *Q* with the largest weight
$k \leftarrow n_{i,j} + 1$
$B_{i,j}^{k} \leftarrow$ run MaxWeightPath on G_L for $e_{i,j}$
if $B_{i,j}^{k}$ does not exist then
DEQUEUE(*Q*, $e_{i,j}$)
else $r_{i,j}^{k} \leftarrow$ the usable bandwidth of $B_{i,j}^{k}$
if $u_{i,j} < r_{i,j}^{k}$ then
$\leftarrow u_{i,j}$
end if
for each logical link $e_{s,t}$ on $B_{i,j}^{k}$ do
$b_{s,t} \leftarrow b_{s,t} - r_{i,j}^{k}$
if $b_{s,t} = 0$ then
$G_L \leftarrow G_L - e_{s,t}$ _ $e_{s,t}$does not have usable bandwidth
end if
end for
$\leftarrow c_{i,j} + 1$
$\leftarrow u_{i,j} - r_{i,j}^{k}$ _ update the unprotected traffic load
$w_{i,j} \leftarrow w_{i,j} - p_{i,j}\ r_{i,j}^{k} \left(1 - P\left(B_{i,j}^{k} | e_{i,j}\right)\right)$
if $c_{i,j} = N$ or $u_{i,j} = 0$ then
DEQUEUE (Q, $e_{i,j}$)
end if
end if

6. Related Work

There are two categories of existing works that are related to this approach.

6.1 Optimal Recovery and Backup Path

Quickly recovering IP networks from failures is critical to enhancing Internet robustness and availability. Due to their serious impact on network routing, large-scale failures have received increasing attention in recent years. Most prior works consider backup path selection as a connectivity problem and mainly focus on finding backup paths to bypass the failed IP links [3], [7].

However, they ignore the fact that a backup path may not have enough bandwidth. Consequently, the rerouted traffic may cause severe link overload on an IP backbone as observed by Iyer et al. [11]. A recent work [6] addresses the link overload problem in the backup path selection, but it aims at minimizing the bandwidth allocated to backup paths rather than minimizing routing disruption. All these methods use IP layer information for backup path selection, consider logical link failures as independent events, and select one backup path for each logical link. Different from these methods, PCF model is developed to reflect the probabilistic correlation between logical link failures, and split the rerouted traffic onto multiple backup paths to minimize routing disruption and avoid link overload.

6.2 IP Network Protection

Q.Zheng at 2012 [5] proposed a Model for IP network protection. The Model used [5] differs from PCF model in two ways. First, the PCF model considers both independent and correlated logical link failures, whereas the model in [5]

only considers correlated failures. Second, each logical link is protected by multiple backup paths in this paper, but protected by single backup path in [5]. Our approach is different from prior works in three aspects. First, it is based on a cross-layer design, which considers the correlation between logical and physical topologies. The proposed PCF model can reflect the probabilistic correlation between logical link failures. Second, we protect each logical link with multiple backup paths to effectively reroute traffic and avoid link overload, whereas most prior works select single backup path for each logical link. Third, our approach considers the traffic load and bandwidth constraint. It guarantees that the rerouted traffic load does not exceed the usable bandwidth, even when multiple logical links fail simultaneously.

References

[1] Q. Zheng, G. Cao, T. L. Porta, A. Swami, Optimal Recovery from Large-Scale Failures in IP Networks, in Proc. IEEE ICDCS, 2012, 295-304
[2] P. Francois, C. Filsfils, J. Evans, O. Bonaventure, Achieving Sub-Second IGP Convergence in Large IP Networks, ACM SIGCOMM Comput. Commun. Rev., 35(3), 2005, 35-44
[3] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing, O. Lysne, Fast IP Network Recovery Using Multiple Routing Configurations, in Proc. IEEE INFOCOM, 2006, 1-11
[4] E. Oki, N. Matsuura, K. Shiomoto, N. Yamanaka, A Disjoint Path Selection Scheme with Shared Risk Link Groups in GMPLS Networks, IEEE Commun. Lett., 6(9), 2002, 406-408
[5] Q. Zheng, J. Zhao, G. Cao, A Cross-Layer Approach for IP Network Protection, in Proc. IEEE/IFIP DSN, 2012, 1-12
[6] M. Johnston, H.-W. Lee, E. Modiano, A Robust Optimization Approach to Backup Network Design with Random Failures, in Proc. IEEE INFOCOM, 2011, 1512-1520
[7] M. Shand and S. Bryant, IP Fast Reroute Framework, RFC5714, 2010
[8] F. Giroire, A. Nucci, N. Taft, C. Diot, Increasing the Robustness of IP Backbones in the Absence of Optical Level Protection, in Proc. IEEE INFOCOM, 2003, 1-11
[9] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, Diot, Characterization of Failures in an Operational IP Backbone Network, IEEE/ACM Trans. Netw., 16(4), 2008, 49-762
[10] Q. Zheng, G. Cao, Minimizing Probing Cost and Achieving Identifiability in Probe Based Network Link Monitoring, IEEE Trans. Comput., 62(3), 2013, 510-523
[11] S. Iyer, S. Bhattacharyya, N. Taft, C. Diot, An Approach to Alleviate Link Overload as Observed on an IP Backbone, in Proc. IEEE INFOCOM, 2003, 406- 416

7. Conclusion

SRLG models ignore the correlation between the optical and IP layer topologies. It does not accurately reflect the correlation between logical link failures and may not select reliable backup paths. To resolve this, the cross-layer approach used to minimizing routing disruption caused by IP link failures, with bandwidth splitting and distribution. PCF model results the impact of every backed up path and it recover alternate on every route failure. This will cause to steadily maintain the bandwidth of end user network and prevent the unbalanced data rate in timing. This approach is more reliable than the existing approach. Thus a survey of cross layer approach for backup path selection in IP networks is prepared.