www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12550-12556

Cross-Layer Approach for Minimizing Routing Disruption with Load Balancing in IP Networks

Mr. Mahalingesh Honnalli[1] , Mr. Santosh S. Dewar[2]

[1]PG Scholar, Dept. of CS Dr. P. G. Halakatti College of engineering & Technology, Vijayapur, Karnataka, India.

[2]Asssistant Professor, Dept. of CS Dr. P. G. Halakatti College of engineering & Technology, Vijayapur, Karnataka, India

Abstract: In IP networks Backup paths are widely used to protect IP links from failures. Still, existing solutions such as the commonly used independent model and Shared Risk Link Group (SRLG) model will not exactly redirect the correlation between IP link failures, and which may not choose reliable backup paths. We propose a cross-layer approach for minimizing routing disruption caused by IP link failures. We develop a probabilistically correlated failure (PCF) model to quantify the impact of IP link failure on the reliability of backup paths. With this model, we propose an algorithm to pick several reliable backup paths to defend each IP link. If an IP link fails, its traffic is divided into several backup paths to ensure that the rerouted traffic load on each IP link does not exceed the usable bandwidth. Experimental results show that two backup paths are adequate for protecting a logical link. Compared with existing works, the backup paths selected by our approach are at least 18 percent more reliable and the routing disruption is reduced by at least 22 percent. Unlike prior works, the proposed approach prevents the rerouted traffic from interfering with normal traffic.

Keywords - Routing, failures, cross-layer, recovery.

1. INTRODUCTION

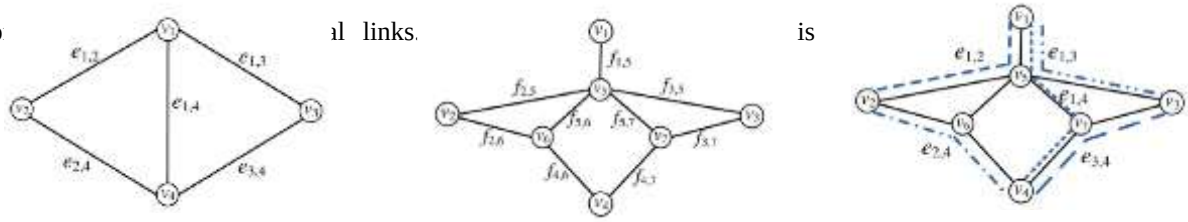
The Internet has evolved into a platform with applications having strict demands on robustness and availability, like trading systems, online games, telephony, and video conferencing. For these applications, even short service disruptions caused by routing convergence can lead to intolerable

performance degradations. In these schemes, backup next-hops are prepared before a failure occurs, and the discovering router handles a component failure locally without signaling to the rest of the network.

The IP link failures are fairly common in the Internet for various reasons. In high speed IP networks like the Internet backbone, disconnection of a link for several seconds can lead to millions of packets being dropped[1]. Therefore, quickly recovering from IP link failures is important for enhancing Internet reliability and availability, and has received much attention in recent years. Currently, backup path-based protection [2] [3] widely used by Internet Service Providers to protect their domains. In the approach, backup paths are pre-computed, configured, and stored in routers. When a link failure is detected, traffic, originally traversing the link is immediately switched to the backup path of this link. Through this, the routing disruption duration is reduced to the failure detection time which is typically less than 50ms [4].

The IP backbone networks are primarily built on the Wavelength Division Multiplexing infrastructure[5]. In the Backup path-based protection is primarily used for intra domain routing, which is really deployed by ISPs to protect their domains. Similarly, our approach is also for intra domain routing. ISP's instrument their networks heavily and have the network topology, link capacity, and traffic demands which are used in our approach. The IP over WDM network under study has a logical topology and a physical topology, which are commonly modeled as two undirected graphs. Each logical link is mapped on the physical topology as a light path, a path over the fiber links. Hence a logical link is embedded on fiber

links, o ıl links. is network



(a) Logical Topology (b) Physical Topology (c) Mapping between the Logical and fiber links

Fig 1 Example of the Mapping between the logical and physical topologies in IP over WD networks

configuration, and thus is known to us. Unlike logical link states, the topology mapping is quite stable and does not frequently change. When the network administrator adjusts the topology mapping, the topology mapping information at routers can also be updated. In this layered structure, the IP layer topology (logical topology) is embedded on the optical layer topology (physical topology), and each IP link (logical link) is mapped to a light path in the physical topology. An IP link may consist of multiple fiber links, and a fiber link may be shared by multiple IP links. When a fiber link fails, all the logical links embedded on it fail simultaneously.

When a fiber link fails, all the logical links embedded on it fail simultaneously. Fig. 1 shows an example of the topology mapping in IP-over-WDM networks. The logical topology in Fig. 1a is embedded on the physical topology shown in Fig. 1b, in which nodes v_5, v_6, andv_7 are optical layer devices and hence do not appear in the logical topology. Logical links are mapped to light paths as shown in Fig. 1c. For example, $e_{1,4}$ shares a fiber link $f_{1,5}$ with $e_{1,3}$ and shares fiber link $f_{4,7}$ with $e_{3,4}$

2 PRELIMINARIES

This section introduces backup path-based IP link protection and a model of IP-over-WDM networks.

2.1 Backup Path-Based IP Link Protection

On today's Internet, every router monitors the connectivity with its neighboring routers. In a network when a logical link failure occurs only the two routers connected by it can detect the failure. So, a router will not have the overall information about failures in the network. Even though the failed logical links can be identified within a few seconds [1], 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 recomputed backup paths based on the new network topology. Backup paths can be implemented with Multi-Protocol Label Switching which is widely supported in the current Internet. Each backup path is configured as a Label-Switched Path (LSP) and the rerouted traffic can be split on backup paths.

2.2 Model of IP-over-WDM Networks

Backup path-based protection is primarily used for intra domain routing, which is really deployed by ISPs to protect their domains. Similarly, our approach is also for intra domain routing. ISP's instrument their networks heavily and have the network topology, link capacity, and traffic demands which are used in our approach. The IP-over-WDM network under study has a logical topology and a physical topology, which are commonly modeled as two undirected graphs.

The topology mapping is established during network configuration, and this is known to us. Unlike logical link states, the topology mapping is quite stable and does not frequently change. When the network administrator adjusts the

topology mapping, the topology mapping information at routers can also be updated.

3.PROBABILISTICALLY CORRELATED FAILURE MODEL

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

3.1 Motivation

Recent measurements [8], [9] show that there are two types of IP link failures on 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 $e_{i,j}$ implies that the logical links sharing at least one fiber link with $e_{i,j}$ may also fail with a certain probability. Therefore, backup path selection approaches should consider this probabilistic correlation between logical link failures. However, the traditional independent and SRLG [6][7] models take the correlation between logical link failures as a non-or-all relation.

The independent model considers that logical links only has independent failures and thus it usually underestimates the failure probability of logical links; whereas the SRLG model considers that logical links only have correlated failures and usually overestimates the failure probability. PCF model developed 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, we propose an algorithm to choose reliable backup paths to minimize the routing disruption.

3.2 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 by Internet measurement approaches [8], [9] deployed at the optical and IP layers. Monitoring mechanisms at the optical layer can detect fiber link failures through SONET alarms. The information about logical link failures can be extracted from routing updates. ISPs also maintain failure information, because they monitor the optical and IP layers of their networks.

3.3 BLOCK DIAGRAM

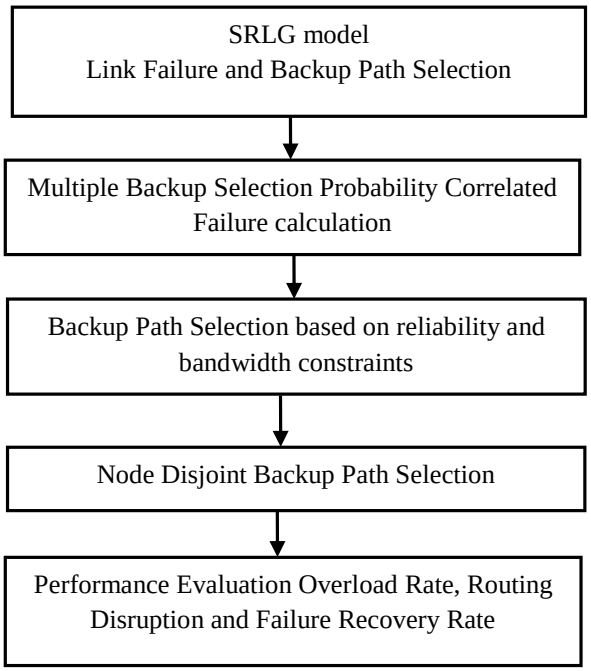


Fig.2 Block diagram of the proposed model

4. MODULES

In this methodology we have five modules as explained below

4.1 SRLG Model

SRLG works assume that once an SRLG failure event occurs, all of its associated links fail simultaneously. Here, generalize the notion of an SRLG to account for probabilistic link failures. This generalized notion allows us to model correlated failures that may result from a natural or man-made

disaster. For example, in the event of a natural disaster, some, but not necessarily all, of the links in the vicinity of the disaster may be affected. Such failures cannot be described using a deterministic failure model, and this raises the need for a systematic approach to dealing with correlated probabilistic link failures. This address issue by modeling SRLG events probabilistically so that upon an SRLG failure event, links belonging to that SRLG fail with some probability not necessarily one.

4.2 Backup Path Selection

In this layered structure, the IP layer topology that means logical topology is embedded on the optical layer topology that means physical topology, and each IP link, that means the logical link is mapped to a light path in the physical topology. An IP link may consist of multiple fiber links, and a fiber link may be shared by multiple IP links. When a fiber link fails, all the logical links embedded on it fail simultaneously.

There are two types of IP link failures on the Internet, that is independent failures and correlated failures. Independent failures are unrelated. This failure occurs 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. When a link failure is detected, traffic originally traversing the link is immediately switched to the backup path of this link. Through this, the routing disruption duration is reduced to the failure detection time. Each router only monitors the connectivity with its neighboring routers, routers cannot determine whether a logical link failure is independent or correlated. But we are calculating the correlation, probability of link failure.

The failure of logical links implies that the logical links sharing at least one fiber link with logical link may also fail with a certain probability. Therefore, backup path selection approaches should consider this probabilistic correlation between logical link failures. As show In fig 3.

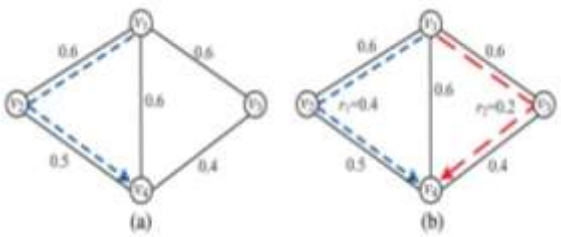


Fig.3 Motivation for protecting a logical link with multiple backup paths.
(a)Single backup path may not have enough bandwidth.
(b)The rerouted traffic is split on two backup paths.

4.3 Reliable Backup Selection Using Probability Correlated Failure

A PCF model 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.

A backup path is built on logical links, and a logical link is embedded on fiber links. Hence, first compute the failure probability of fiber links under the condition that logical link fails. Then, compute the conditional failure probability of logical links and backup paths. The unconditional failure probability of logical link is denoted by $p_{i,j}$ probability of 0 and 1 which includes correlated failures.

The probability that logical link has correlated failures with other logical links. If logical link does not share a fiber link with other logical links, its correlated failure probability is 0. Otherwise

$$P_{i,j}^{C} = \begin{cases} 0 & if\ F_{i,j} = \emptyset \\ 1 - \prod f_{m,n} \in F_{i,j}\left(1 - q_{m,,n}\right) & otherwise \end{cases}$$

Where: $e_{i,j}$ is represent the logical link

$F_{m,n}$ represent the fiber link

$F_{i,j}$ Fiber link shared by the logical link by other logical links.

Let $a^{i,j}{}_{m,n}$ is the mapping between logical link $e_{i,j}$ and fiber link $f_{m,n}$

The correlated probability of logical link

$$\mathbf{P_{i,j} = 1 - (1-P^{C}{}_{i,j})}$$

The PCF model to select multiple backup paths to protect each IP link. The 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. Furthermore, it controls the rerouted traffic load to prevent causing logical link overload.

The routing disruption based on the PCF model. Under normal conditions, the traffic load on $e_{i,j}$ is $l_{i,j}$ which satisfies the traffic load less than or equal to capacity of logical link. The logical link overloaded if the rerouted traffic load on it exceeds the $c_{i,j}$ - $l_{i,j}$. Therefore, the traffic disruption of $e_{i;j}$ is the mathematical expectation of the disrupted traffic load.

$$\boldsymbol{D_{i,j} = p_{i,j}\left\{\sum_{k=1}^{N} P\left(B_{i,j}^{k}\middle|e_{i,j}\right) r_{i,j}^{k} + l_{i,j} - \sum_{k=1}^{N} r_{i,j}^{k}\right.}$$

Where: $c_{i,j}$ is denoted as capacity of logical link

$l_{i,j}$ represent the traffic load of logical link

$B^{k}_{i,j}$ denoted as Kth backup path

$r^{k}_{i,j}$ denoted as reserved bandwidth

$D_{i,j}$ represent the disrupted traffic load

The routing disruption of the entire network is then defined as

$$\boldsymbol{D = \sum_{e_{i,j} \in E_L} D_{i,j.}}$$

D is denoted as traffic disruption in entire network

To select at most N backup paths for each logical link and compute the rerouted traffic load for each backup path, such that the routing disruption of the entire network is minimized and the rerouted traffic load on each logical link does not exceed its usable bandwidth. The basic idea is to select backup paths one by one until there is no usable bandwidth or no logical link can have more backup paths. It is used to $D_{i;j}$ defined as the weight of $e_{i,j}$. In each round, the algorithm Select back up path picks out the logical link with the largest weight, and then selects a backup path for logical link and determines the rerouted traffic load. Suppose logical link already has k - 1 backup paths. Adding one more backup path reduces traffic disruption $D_{i;j}$.

$$\Delta_{i,j} = p_{i,j}\, r^{k}_{i,j}\, (1 - P(B^{k}_{i,j} \mid e_{i,j}))$$

To choose $B^{k}_{i,j}$ and determine $r^{k}_{i,j}$ to maximize $D_{i,j}$. The basic idea is similar to calculates the shortest path.

4.4. Node Disjoint Backup Path Selection

The cross layer approach for minimizing routing disruption is an extension to the SRLG for computing multiple loop free and link disjoint paths. The cross layer approach computes multiple backup path loop free and link disjoint paths. To ensure loop freedom and node only accepts an alternate path to the destination if it has a lower hop count then the advertised hop count for that destination. Multiple backup path routing can balance the load better than the single path routing in IP networks, where the first selective shortest paths are used for routing. This is possible only for the networks having a huge number of nodes between any source-destination pair of nodes. It is infeasible to build such a system it is economical for discovering and maintaining a large number of paths. The load-balancing approach is a multiple backup path using link failure concepts of IP networks. For a better load balanced network distributed multiple backup path load splitting strategies need to be designed. Load balancing is a methodology to distribute workload across multiple backup paths, to achieve minimize traffic overload, and minimize the routing disruption.

4.5. Performance Evaluation

Routing Disruption

For a failed logical link, if a backup path does not contain any failed or overloaded logical link, the traffic rerouted by it is recovered. Suppose the overall traffic load of failed logical links is T and the recovered traffic load is Tr.

The routing disruption is defined

$$Routing\ \ Disruption = \frac{T - Tr}{T}$$

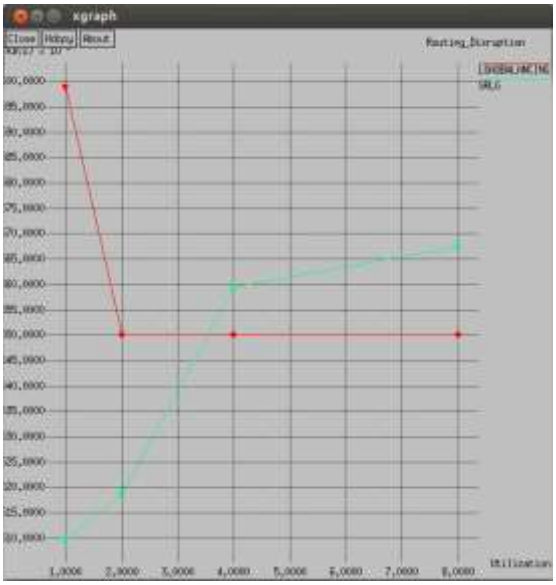


Fig 4 shows the routing disruption is better than that of the existing system

Overload Rate

The ratio of count the logical links traversed by the rerouted traffic denoted as L to overloaded logical links denoted as Lo.

The overload rate is defined as

$$Overload\ Rate\ = \frac{L_0}{L}$$

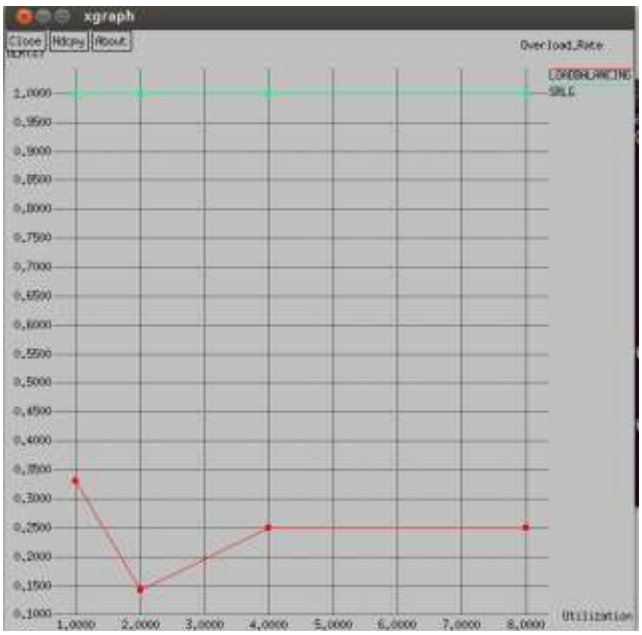


Fig 5 Shows the over load rate is high when compared to the existing system SRLG

Failure Recovery Rate

Failure Recovery Rate is defined as the percentage of recovered logical link failures.

Failure Recovery Rate

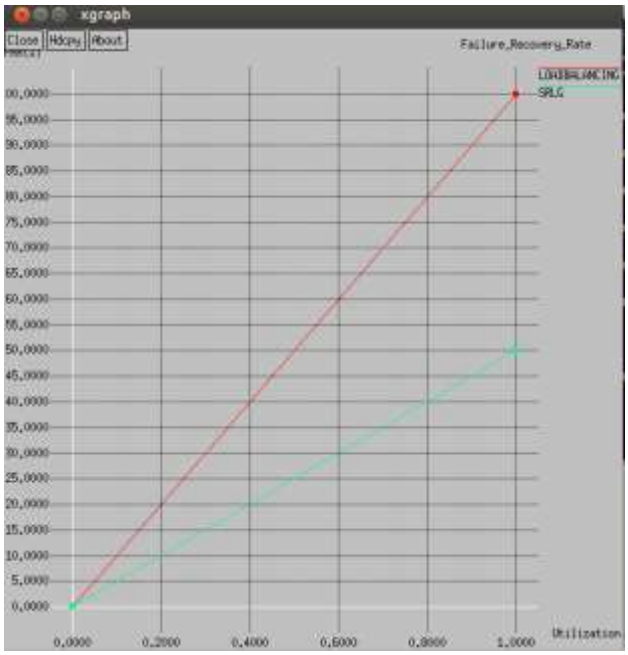


Fig 6 Shows the percentage of failure recovery rate is better than the SRLG system

CONCLUSION

The commonly used independent and SRLG models ignore the correlation between the optical and IP layer topologies. As a result, they do not accurately reflect the correlation between logical link failures and may not select reliable backup paths. The proposed system is a cross-layer approach for minimizing routing disruption caused by IP link failures it develop a probabilistically correlated failure (PCF) model to quantify the impact of IP link failure on the reliability of backup paths. With this model, to minimize the routing disruption by choosing multiple reliable backup paths to protect each IP link. The proposed approach ensures that the rerouted traffic does not cause logical link overload, even when multiple logical links fail simultaneously. It evaluates the proposed approach using real ISP networks with both optical and IP layer topologies. Experimental results show that two backup paths are adequate for protecting a logical link. The load-balancing approach is a multiple backup path used to link failure concepts of IP networks. For a better load balanced network distributed multiple backup path load splitting strategies need to be designed. Load balancing is a

methodology to distributed workload across multiple backup paths, it achieved to minimize traffic overload, and minimize the routing disruption.

REFERENCE

[1] 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.

[2] A. Bremler-Barr, Y. Afek, H. Kaplan, E. Cohen, and M. Merritt,‘‘Restoration by Path Concatenation: Fast Recovery of MPLs Paths,’’in Proc. ACM PODC, 2001, pp. 43-52.

[3] V. Sharma and F. Hellstrand, Framework for MPLS-Based Recovery, RFC 3469, 2003.

[4] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure, ‘‘Achieving Sub-Second IGP Convergence in Large IP Networks,’’ ACM
SIGCOMM Comput. Commun. Rev., vol. 35, no. 3, pp. 35-44,July 2005.

[5] F. Giroire, A. Nucci, N. Taft, and C. Diot, ‘‘Increasing the Robustness of IP Backbones in the Absence of Optical Level Protection,’’ in Proc. IEEE INFOCOM, 2003, pp. 1-11.

[6] 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.

[7] 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.

[8] 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.

[9] D. Turner, K. Levchenko, A.C. Snoeren, and S. Savage,‘‘California Fault Lines: Understanding the Causes and Impact of Network Failures,’’ in Proc. ACMSIGCOMM, 2010, pp. 315-326.

[10] Q. Zheng and G. Cao, ‘‘Minimizing Probing Cost and Achieving Identifiability in Probe Based Network Link Monitoring,’’ IEEETrans. Comput., vol. 62, no. 3, pp. 510-523, Mar. 2013.