Available online at www.sciencedirect.com
SCIENCE DIRECT
Int. J. Electron. Commun. (AEÜ) 60 (2006) 35–39
International Journal AEÜ of Electronics and Communications
www.elsevier.de/aeue

Optimal multi-topology routing for IP resilience

Matthias C. Scheffel, Claus G. Gruber, Thomas Schwabe*, Robert G. Prinz

Technische Universität München, Institute of Communication Networks, 80290 Munich, Germany

Dedicated to Professor Jörg Eberspächer on the occasion of his 60th birthday

Abstract

Multi-topology routing is a new strategy to provide traffic-engineering and resilience in IP networks. In case of network failures, affected traffic demands are routed in intact sub-topologies for which the routing information is predetermined. This paper investigates an optimal design of the topologies with respect to a shortest path protection routing. We formulate mathematical programs for global and local protection schemes and investigate a case study. Our results show that only very few topologies are necessary to provide an optimal protection configuration.

Keywords: IP resilience; Multi-topology routing; Resilient routing topologies; Linear programming

1. Introduction

Today's IP-based networks use either connection-less link-state protocols (e.g. OSPF [1] and IS–IS [2]) or connection-oriented approaches (e.g. MPLS [3]). Concerning traffic engineering and resilience possibilities, connection-oriented network approaches are superior to connection-less approaches since routes can be defined arbitrarily. However, extra effort and complexity is required to maintain the connection states.

A new connection-less routing mechanism with improved traffic-engineering and fast resilience mechanisms is provided by Multi-topology routing (MTR), that is currently in standardization process as an extension to OSPF [4] and IS–IS [5].

In this paper, we review and discuss the characteristics of the mentioned IP-based routing approaches and compare them with each other. Following this, we present an Integer Linear Programming approach to design optimal resilient routing layers in Section 3. The resulting protection configurations for different numbers of routing topologies are discussed in Section 4. Finally, Section 5 concludes this paper and summarizes the key findings.

2. IP-based routing approaches

2.1. Connectionless link-state routing

In connectionless link-state routing (CLR), the routers of an autonomous system maintain an own view of the topology and calculate shortest path trees to determine the next-hop outgoing interface for all known destinations. To enable traffic engineering, the link-metrics can be adapted to change the shortest paths. In case these link-weights are chosen in a sophisticated way, the traffic can be distributed evenly in the network and congestions are prevented. Failures of network elements are detected by the adjacent routers via hardware detection or liveliness protocols (e.g. bidirectional forwarding detection [6]). After flooding failure indication messages to all routers, the defect network elements are removed from their topology databases and failure-free routes are calculated. With this re-routing

* Corresponding author. Tel.: +49 89 289 23505; fax: +49 89 289 23523.
E-mail address: thomas.schwabe@tum.de (T. Schwabe).

1434-8411/$ - see front matter © 2005 Elsevier GmbH. All rights reserved.
doi:10.1016/j.aeue.2005.10.007

mechanism, routes are found as long as a physical connectivity exists.

However, link-state-based routing protocols have two main drawbacks:

(a) *Long convergence time*: Due to the distributed routing approach and the required flooding procedure, the reaction upon failures takes a long time. With standard timer-values, an OSPF network takes at least seconds to converge. Even with tuned timer-values, some hundreds of milliseconds are required for the flooding and the forwarding information base reconfiguration. This order of magnitude might be too high for some real-time traffic applications.

(b) *Limited traffic engineering possibilities*: In standard destination-based routing, traffic towards different destinations cannot be treated and routed differently. Additionally, all routes are calculated according to the same topology and link weights. Thus, choosing well-suited link weights is a complicated task [7] and the possibilities of traffic engineering are restricted.

2.2. Connection-oriented routing

In connection-oriented routing (COR), traffic is sent along pre-defined structures (e.g. paths, rings, trees). IP-packets are labeled at ingress routers (e.g. MPLS edge routers) and routed according to these labels. Since packets for different destinations can be aggregated to one label, the address space can be reduced and the forwarding process can be accelerated. Furthermore, as the routing structures can be defined arbitrarily and traffic for different destinations and/or sources can be routed differently, traffic-engineering is facilitated. Similar to traffic-engineering backup structures can be pre-defined and fast (local) detours around failed elements are possible (e.g. Cisco Fast Reroute, p-Cycles [8]). As a drawback, the structures have to be setup and maintained, which causes and additional management effort in the networks.

2.3. Multi-topology routing

MTR combines the idea of pre-planned backup structures with the connection-less approach of link-state-based routing. Packets are routed along a shortest-path tree that is calculated at each network router. However, instead of having only one topology, MTR maintains several topologies and shortest-path trees, respectively. An additional flag in the IP-header of a packet (e.g. TOS bits) defines on which of these topologies a packet is to be routed. An example of an MTR network with four topologies is given in Fig. 1.

In addition to the possibilities of traffic engineering, Hansen et al. [9] presented the idea to use these topologies as backup structures. In case of a network failure, packets that would traverse the affected area are relabeled onto a failure-free sub-topology. The 'Resilient Routing Topology' (RRT) concept can be divided into two variants. An example of the local and global variant of the RRT concept is illustrated in Fig. 2.

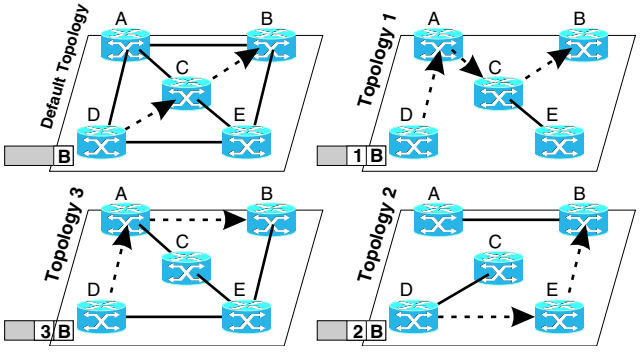

Fig. 1. Example of MTR with four topologies. Depending on the label, a packet is routed in a specific topology. The route of a packet from node D to B is represented by a dashed line.

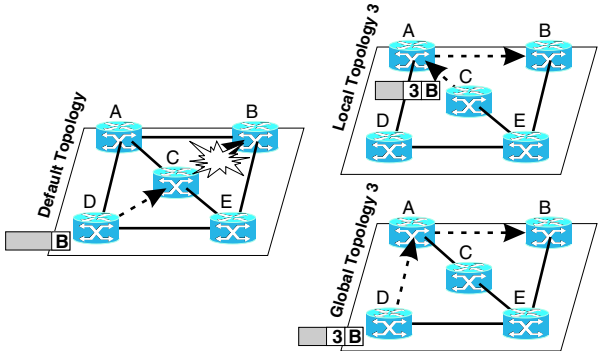

Fig. 2. Example of the local and global variant of RRT. *Local*: A packet is routed along the default topology and is relabeled at a router adjacent to a failure (path: D–C–A–B). *Global*: After signalization of the failure each router labels packets that would traverse the failing region to a failure-free sub-topology (path: D–A–B).

In contrast to CLR, the information about an outage is not flooded in 'Local RRT'. Instead of that, the routers adjacent to the failure relabel traversing packets to other sub-topologies. Thus, packets are locally detoured around a failing area.

The global variant of RRT is similar to the rerouting behavior of CLR. Information about a failure is flooded to all routers. However, a routing topology that does not include the failed elements was already pre-calculated and packets need only to be relabeled at source routers.

3. Multi-topology design

MPLS protection mechanisms like Local Link Protection (i.e. Cisco Fast Reroute) can be emulated with MTR when

using one RRT per failure pattern. However, the number of topologies and with it the routing table quantity can be reduced when a topology is used for multiple (and/or simultaneous) failure patterns. RRT topologies can be reduced further if topologies are generated for a sub-set of possible failures only. Thus, a fast reaction for the most likely failures is possible with RRT while a longer-lasting CLR rerouting can be applied for other failure patterns. Hansen et al. [9,10] presented a heuristic algorithm for creating RRT. A number of 3–6 topologies were sufficient to protect their example networks from single-element failures.

The design of suitable topologies in order to perform an optimal routing in case of a failure represents an optimization task. We develop mathematical models in terms of binary integer linear programs (BILPs) to calculate optimal topologies for global and local RRT using fixed link-weights. Our aim is to survive single link failures for a given number of topologies. The topologies are constructed such that the protection routing is optimized in terms of shortest path routing. We assume all link-metrics to be one and thus minimize the number of traversed edges (hops) that are required to reroute all the traffic demands affected by any single link failure.

3.1. Mathematical model for global RRT

The model is based on a bi-directed graph, i.e. adjacent nodes are connected by an edge and the counter-directed edge, respectively. In the following, we introduce the given data sets and functions.

- N: nodes n of the physical network.
- E: edges e of the physical network.
- D: demand relations d between two physical nodes.
- I: topology identifiers i.
- W_d: edges that are used for the primary routing in failure-free operation of demand relation d.
- $\text{source}(e), \text{source}(d) \in N$: returns the source node of an edge $e \in E$ or a demand relation $d \in D$.
- $\text{target}(e), \text{target}(d) \in N$: returns the target node of an edge $e \in E$ or a demand relation $d \in D$.
- $\text{reversal}(e) \in E$: returns the reverse edge of an edge $e \in E$.

The subsequent decision variables are to be determined. Only the number of topologies is know a priori, given by the set of identifiers. The structures of the individual topologies are computed by the rerouting process. If an edge fails, all affected traffic demands will be rerouted in another topology. The employed edges then determine the constitution of the alternative topology.

- $\text{ReroutFlow}_{d,f,e,i} \in \{0,1\}$: rerouted flow for demand relation $d \in D$ uses edge $e \in E$ in case of failure of edge $f \in W_d$ in topology with id $i \in I$
- $\text{TopProtFail}_{i,f} \in \{0,1\}$: topology with id i allows to protect a failure of edge f

Objective:

$$\text{Minimize} \sum_{\substack{d\in D\\ f\in W_d\\ e\in E\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} \tag{1}$$

Constraints:

$\forall d \in D,\ f \in W_d$:

$$\sum_{\substack{e\in E,\text{source}(e)\equiv\text{source}(d)\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} - \sum_{\substack{e\in E,\text{target}(e)\equiv\text{source}(d)\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} = 1, \tag{2}$$

$\forall d \in D,\ f \in W_d, i \in I, n \in N,$
$n \neq \text{source}(d) \cap n \neq \text{target}(d)$:

$$\sum_{\substack{e\in E,\text{source}(e)\equiv n\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} = \sum_{\substack{e\in E,\text{target}(e)\equiv n\\ i\in I}} \text{ReroutFlow}_{d,f,e,i}, \tag{3}$$

$\forall d \in D,\ f \in W_d$:

$$\sum_{\substack{e\in E,\text{target}(e)\equiv\text{target}(d)\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} - \sum_{\substack{e\in E,\text{source}(e)\equiv\text{target}(d)\\ i\in I}} \text{ReroutFlow}_{d,f,e,i} = 1, \tag{4}$$

$\forall d \in D,\ f \in W_d, e \in E, i \in I$:

$$\text{TopProtFail}_{i,f} + \text{TopProtFail}_{i,\text{reversal}(f)} \geqslant 2 \cdot \text{ReroutFlow}_{d,f,e,i} \tag{5}$$

$\forall d \in D,\ f \in W_d, e \in E, i \in I$:

$$\text{ReroutFlow}_{d,f,e,i} \leqslant 1 - \text{TopProtFail}_{i,e}. \tag{6}$$

The objective (1) optimizes the multitopology rerouting in terms of shortest path routing. It minimizes the overall number of hops for all rerouted flows considering all traffic demands and each single edge failure.

The primary routing used to satisfy the traffic demands in a failure-free network is determined in advance, based on the entire network topology. In case of a defect edge on this route, the demand has to be routed in another topology that does not contain the failed element. We cover the failure of the directed edges used by the primary path, solely. However, we assume that an edge outage involves the collapse of both transmission directions and take this into account when analyzing the rerouting. Constraint (2) launches a rerouting flow at the source node of each demand in one of the available topologies. The number of outgoing flows minus the number of incoming flows must be one. The continuity of the alternative routes is guaranteed in Eq. (3) for each topology. At any traversed node, the number of outgoing flows

must match the number of incoming flows. Potential loops are prevented by the objective, as the total hop number is minimized. Constraint (4) terminates the protection flows at the target node of the traffic demand. A topology will be able to protect the outage of an edge only if the edge is excluded from the topology.

Eq. (5) detects whether a certain topology is used to recover from an edge failure. For each traffic demand and each edge defect on its primary route, the potential edges of all topologies are considered. In case a rerouted flow traverses the edge, indicated by ProtFlow, the respective variable TopProtFail is set to one. Moreover, the variable for the counter-directed edge is also initialized, thus addressing bidirectional outages.

Valid topologies are ensured by Eq. (6). Once a topology is applied to survive a certain edge failure, this edge must be ruled out for the topology. Consequently, no rerouting flow can traverse the edge. The topologies are an inherent result of the rerouting configuration. A topology consists of all the employed edges that are indicated by the flow variables.

3.2. Mathematical model for local RRT

The mathematical program for the local protection mechanism can be derived from the global variant. The objective function and Eqs. (5)–(6) can be adopted. In order to redirect the traffic locally, the flow formulation (2)–(4) has to be replaced by the following equations:

$$\forall d \in D,\ f \in W_d:\quad \sum_{\substack{e\in E,\,\mathrm{source}(e)\equiv \mathrm{source}(f)\\ i\in I}} \mathrm{ReroutFlow}_{d,f,e,i} - \sum_{\substack{e\in E,\,\mathrm{target}(e)\equiv \mathrm{source}(f)\\ i\in I}} \mathrm{ReroutFlow}_{d,f,e,i} = 1, \tag{7}$$

$$\forall d \in D,\ f \in W_d, i \in I, n \in N,\ n \neq \mathrm{source}(f) \cap n \neq \mathrm{target}(d):\quad \sum_{\substack{e\in E,\,\mathrm{source}(e)\equiv n}} \mathrm{ReroutFlow}_{d,f,e,i} = \sum_{\substack{e\in E,\,\mathrm{target}(e)\equiv n}} \mathrm{ReroutFlow}_{d,f,e,i}, \tag{8}$$

$$\forall d \in D,\ f \in W_d:\quad \sum_{\substack{e\in E,\,\mathrm{target}(e)\equiv \mathrm{target}(d)\\ i\in I}} \mathrm{ReroutFlow}_{d,f,e,i} - \sum_{\substack{e\in E,\,\mathrm{source}(e)\equiv \mathrm{target}(d)\\ i\in I}} \mathrm{ReroutFlow}_{d,f,e,i} = 1. \tag{9}$$

In case a traffic flow is interrupted, it still follows the primary route up to the adjacent node of the defect edge. There, a rerouted flow is created in one topology by constraint (7). The continuity of the flow is guaranteed by Eq. (8). Finally, constraint (9) terminates the rerouted flow at the target node of the demand.

4. Case study

We investigate the mathematical programs for multi-topology protection routing for the pan-European COST 239 network [11] consisting of 11 nodes and 26 edges. It is assumed that there is one traffic demand between each node pair in the network. The performance of the protection configuration in terms of shortest hop routing is optimized for a given number of available routing topologies.

Fig. 3 shows the total number of rerouting hops subject to the topology quantity. The solid curve represents the global protection scheme and the local protection approach is marked by a dashed line. In both cases, the hop number was counted from the source to the target node of the traffic demand.

In order to compensate any single edge failure, each edge must be absent in at least one routing topology. Consequently, multi-topology protection routing requires at least two topologies. Topologies are formed so that the protection flows are routed as directly as possible while considering all failure scenarios. The more topologies are available, the better the structure can be adapted to minimize the routes of all protection flows. Our results show, that it is sufficient to have very few topologies to perform an efficient shortest hop routing. Only three and four topologies are required to achieve an optimal rerouting for global and local protection, respectively. A low number of topologies helps to keep the additional configuration overhead and hardware resource requirements for managing the multi-topology extension small. Global protection performs better than local protection because a new edge-disjoint protection path

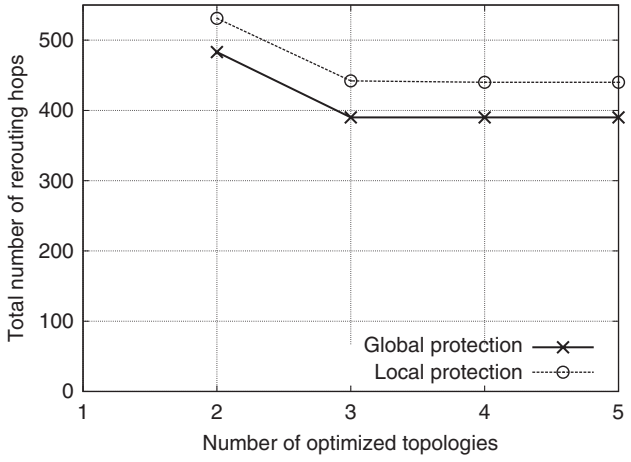

Fig. 3. Performance of global and local multi-topology rerouting. The overall number of hops required for the resilient routing in case of single edge failures is minimized for a varying number of available topologies.

can be selected from source to target node. Whereas for local protection, the alternative route is limited to follow the working route up to the node adjacent to the failed edge.

5. Conclusions

In this paper, we investigate multi-topology protection routing to provide IP resilience. The idea of 'Resilient Routing Topologies' combines the flexibility of traffic engineering in connection-oriented routing with the simplicity of connection-less link state-based routing. In case of a network element failure, affected data packets are labeled to another pre-defined routing topology that does not contain the defect area. The configuration of the routing table can be done in advance of any outage and very fast reaction upon failures can be performed. We formulate mathematical programs in order to create optimal topologies that enable an efficient rerouting with respect to minimal overall hop number for both variants of RRT. The global protection variant involves alternative routes from the demand source to the destination node and requires a signaling of a failure event within the network. The local protection scheme detours the primary routing at the nodes adjacent to the outage and thus does not necessitate any signaling. Our results show that only very few topologies are necessary to provide an optimal protection configuration. Global protection performs better than the local approach since the alternative route is not limited to traverse the node adjacent to the defect edge.

References

[1] Moy J. OSPF Version 2. RFC 2328, http://www.ietf.org: IETF, 1998.
[2] Callon R. Use of OSI IS–IS for routing in TCP/IP and dual environments. RFC 1195, http://www.ietf.org: IETF, 1990.
[3] Rosen E, Viswanathan A, Callon R. Multiprotocol label switching architecture. RFC 3031, http://www.ietf.org: IETF, 2001.
[4] Psenak P, Mirtorabi S, Roy A, Nguyen L, Pillay-Esnault P. Multi-topology (MT) routing in OSPF. Internet-Draft, draft-ietf-ospf-mt-04.txt, http://www.ietf.org: IETF, 2005.
[5] Przygienda T, Shen N, Sheth N. M-ISIS: multi topology (MT) routing in IS–IS. Internet-Draft, draft-ietf-isis-wg-multi-topology-10.txt, http://www.ietf.org: IETF, 2005.
[6] Katz D, Ward D. Bidirectional forwarding detection. Internet-Draft, draft-ietf-bfd-base-02.txt, http://www.ietf.org: IETF, 2005.
[7] Tomaszewiski A, Pioro M, Dzida M, Zagozdzon M. Optimization of administrative weights in IP networks using the branch-and-cut approach. International network optimization conference—INOC 2005, Lisbon, Portugal, 2005. p. B.2393–400.
[8] Grover W. Mesh-based survivable networks: options and strategies for optical, MPLS, SONET and ATM networking. 1st ed, Englewood Cliffs, NJ: Prentice-Hall, PTR; 2004.
[9] Hansen AF, Kvalbein A, Cicic T, Gjessing S, Lysne O, Jensen T, Osterbo ON. Fast, effective and stable IP recovery using resilient routing layers. The 19th international teletraffic congress (ITC19), 2005.
[10] Hansen AF, Kvalbein A, Cicic T, Gjessing S, Lysne O. Resilient routing layers for recovery in packet networks. International conference on dependable systems and networks (DSN 2005), 2005.
[11] Batchelor P. Ultra high capacity optical transmission networks. Final report of action COST 239, 1999.

Matthias C. Scheffel, Claus G. Gruber, Thomas Schwabe and Robert G. Prinz are members of the research staff of the Institute of Communication Networks (LKN) at the Technische Universität München (TUM), Germany.