Optimization Letters manuscript No.
(will be inserted by the editor)

Sufficient Conditions for Protection Routing in IP Networks

János Tapolcai

Received: Sept. 2011

Abstract Providing fully distributed, fault tolerant, hop-by-hop routing is one of the key challenges for intra-domain IP networks. This can be achieved by storing two next-hops for each destination node in the forwarding table of the routers, and the packets are forwarded to primary next-hop (PNH), unless PNH is unreachable and secondary next-hop (SNH) is used instead. We follow the architecture by [4], where the routing tables are configured in a centralized way, while the forwarding and failure recovery is in a fully distributed way without relying on any encapsulation and signaling mechanisms for failure notification, to meet the standard IP forwarding paradigm. A network is protected if no single link of node failure results in forwarding loops. Kwong, Gao, Guerin and Zhang [4] conjectured that network node connectivity is not sufficient for a network to be protectable. In this paper we show that this conjecture is in contradiction with a conjuncture by Hasunuma [2, 3], and show that every four connected maximal planar graph and every underlying graph of a 2-connected line digraph has feasible protection routing.

Keywords IP Fast ReRoute (IPFRR), node-connectivity

1 Introduction

Hop-by-hop routing and IP protocol have become the dominant platform for telecom services [7, 10]. Commercial applications demand reducing the interruption in packet forwarding to sub-50ms in case of failures. As a solution for the problem, in [4] an intra-domain solution was proposed, where a centralized unit pre-computes a primary and an alternate next-hops for each router, where the traffic is instantly switched to the secondary next-hop (SNH) if the

Dept. of Telecommunications and Media Informatics,
Budapest University of Technology and Economics,
E-mail: tapolcai@tmit.bme.hu

primary next-hop (PNH) becomes unavailable. Therefore, forwarding and failure recovery are performed in a fully distributed way relaying on traditional IP forwarding without any encapsulation and signaling mechanisms for failure notification, similarly to O2 [11, 9], DIV-R [8], MARA [6], and LFA [1]. The key challenge is how to avoid forwarding loops in case of failures, when the traffic is forwarded on SNH at a single node. A network is protected if no single link of node failure results in forwarding loops. In this paper we investigate how dense should a topology be to become protected.

Kwong, et. al [4] showed that high edge connectivity is not sufficient for a network to be protected against every single link and node failure, and conjectured that high node connectivity is not sufficient either. In this paper we investigate the latter issue by applying the results and conjectures of Hasunuma [2, 3] to node connectivity. We show that the conjecture by Kwong, et. al is in contradiction with a conjecture by Hasunuma, besides we define a class of four-node-connected graphs with feasible protection routing.

2 Problem Formulation

We formulate the protection routing problem at the centralized routing entity. We assume that the network topology information and link bandwidths are available, and the packet forwarding is destination based (hop-by-hop) without reliance on packet marking or encapsulation.

2.1 Protection Routing

We model the network as an undirected graph $G = (V, E)$, with V the node set, E the link set. For a destination node $d \in V$ let $R_d = (V, E_d)$ be a *routing* for traffic destined to d, where $E_d \subseteq E$. R_d is a directed acyclic graph (DAG) rooted at d and defines a destination based routing. In R_d every node has at least one outgoing link except for d. Every outgoing link is called *primary link*, and the target node of every primary link is called *Primary Next Hop* (PNH). See also Fig.1 as an example.

The routing R_d towards node d can be modeled by a partial order. Define relation $\prec_d$ such that $x \prec_d s$, $x \neq s$ if there exists a path from node s to node x in R_d (i.e. there is a possible packet flight from s to d through x). Node s is *upstream* of node x if $x \prec_d s$, and conversely, node s is *downstream* of node x if $s \prec_d x$. Additionally, we denote by $x \succsim_d s$ the case when nodes x and s are not ordered with each other. Besides, the neighboring nodes of node n is denoted by $N_G(n)$. Next let us define link and protection[1].

Definition 1 A network $G = (V, E)$ is *protected* (with respect to node d) against single *link* failure $f \in E$, if there exists a routing R_d so that either

[1] In [4] the two definitions were merged into a more general definition on component failures.

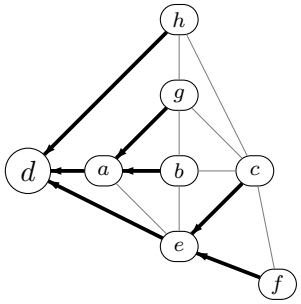


Fig. 1: A network G with a routing R_d drawn with solid thick arrows.

$f \notin R_d$; or $f = (x \leftarrow s) \in R_d$ and node s has a neighboring link $(s, k) \neq f$, such that

1. node k is not upstream of node s in R_d (i.e. $s \not\prec k$).
2. node k and all its downstream nodes (except d) have at least one PNH in $R_d \setminus f$.

On Fig. 1 every link is protected with the routing. Similarly we define node protection

Definition 2 The network $G = (V, E)$ is *protected* (with respect to node d) against single *node* failure $f \in V$, if there exists a routing R_d so that every node $s \in N_G(f)$ having primary link to f (i.e. $(f \leftarrow s) \in R_d$) has a neighboring node $k \neq f$ (i.e. $k \in N_G(s)$), such that

1. Node k is not upstream of node s in R_d (i.e. $s \not\prec k$).
2. Node k and all its downstream nodes (except d) have at least one PNH in $R_d \setminus N_G(f)$.

In both definitions node k is called Secondary Next Hop and denoted by $SNH_d(s)$. On Fig. 1 node e is not protected with the routing, because node f shall forward the packet to node c after the failure of e; however c has a PNH towards the failed node e.

Definition 3 A routing R_d is *protection routing* in network $G = (V, E)$ with respect to node d if every node and link failure is protected.

Definition 4 An undirected graph $G = (V, E)$ is *protectable* if a protection routing exists for all $d \in V$, otherwise the graph is *unprotectable*.

Note that G is protectable as it is shown on Fig. 3. In 2010 Kwong, et. al has showed [4], that the graph edge-connectivity is not a sufficient condition for a network to be protectable. Besides, for node connectivity, 2- and 3-node-connected unprotectable graphs were constructed, and for networks with higher node-connectivity the following conjecture was given:

Conjecture 1 ([4, Conjecture 4.1]) For any given $k \geq 4$, there exists a k-node-connected graph that is unprotectable.

In Section III. we show that this conjecture is in contradiction with a conjecture by Hasunuma from 2001.

2.2 Completely Independent Spanning Trees

Next we define the completely independent spanning trees problem and some general notations. Let T be a spanning tree in graph G. Let $T(s,t)$ denote the path in tree T between nodes s and t.

Definition 5 Let T^1 and T^2 be two spanning trees of an undirected graph G. We call them *completely independent spanning trees* if for any two nodes s and t the paths from s to d in T^1 and T^2 (i.e. $T^1(s,d)$ and $T^2(s,d)$) are node-disjoint apart from their end nodes.

In [2] Hasunuma showed that there are k completely independent spanning trees in the underlying graph of a k-connected line digraph and in [3] that there are two completely independent spanning trees in any 4-connected maximal planar graph.

Computing completely independent spanning trees is NP-hard [2]. According to our experiments for real size IP networks it can be done with ILP in reasonable time.

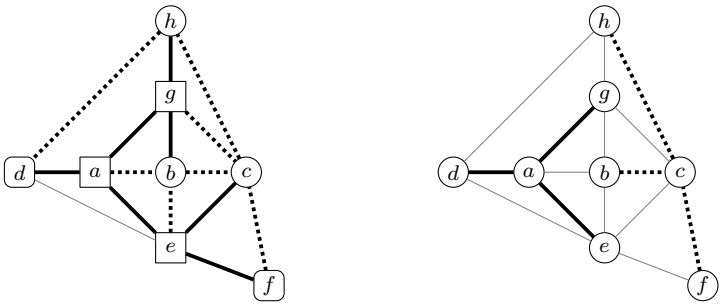
Completely independent spanning trees are special edge-disjoint spanning trees. On edge-disjoint spanning trees, Nash-Williams [5] showed that there are k edge-disjoint spanning trees in any $2k$-edge-connected graph. In 2001 [2, 3] Hasunuma gave a similar conjecture for node-disjoint graphs.

Conjecture 2 ([2], [3, Conjecture 2]) There are k completely independent spanning trees in any $2k$-connected graph.

The main contribution of this paper is to show that two completely independent spanning trees are sufficient for a network to be protected. As a result, both Conjecture 2 and Conjecture 1 cannot be true at the same time.

3 Sufficient Conditions for Protectable Graphs

In routing R_d if a node has multiple outgoing links the traffic is split evenly across them, which is favoured mainly for load balancing issues. As a result, between certain node-pairs the traffic is routed along multiple paths, called Equal-Cost Multi-Path (ECMP). In this section, for the sake of simplicity, we forbid ECMP and consider the case where routing R_d should be a tree instead of a DAG. Clearly, a d rooted tree is a special DAG, and thus with this new constraint the protection routing problem becomes harder to solve. In this case each node n has a single PNH, denoted by $PNH_d(n)$, and R_d is a d rooted spanning tree. An important observation is that when R_d is a spanning tree the second property of Definition 1 and 2 is not needed. In other words



(a) The circles are leaf nodes of T^1, the boxes are leaf nodes of T^2, and rounded boxes are leaf nodes in both trees.

(b) The two sub-trees: $\hat{T}^1$ is with solid thick lines, and $\hat{T}^2$ is with dashed lines.

Fig. 2: Two complete independent spanning trees, where T^1 is with solid thick lines, and T^2 is with dashed lines.

our task is to find a d rooted spanning tree R_d, such that each node s has a neighbor node k not upstream to the downstream adjacent node of s, except when the downstream adjacent node is the destination node d.

We call a degree one node of a tree as *leaf node*; otherwise it is an *internal node*. In [2] the following property of two completely independent spanning trees was proven.

Theorem 1 ([2, Theorem 2.1]) *Let T_1 and T_2 be two spanning trees in the graph G. Then T_1 and T_2 are completely independent if and only if T_1 and T_2 are edge-disjoint and for any vertex v of G there is at most one spanning tree T_i such that node v is an internal node of T_i.*

Fig. 2 shows an example of two completely independent spanning trees. According to Theorem 1 the nodes of the graph can be classified into the following three categories. Each node n is either

1. a leaf node in T_1, or
2. a leaf node in T_2, or
3. a leaf node both in T_1 and T_2.

Next we erase some leaf links from T^1 and T^2 to obtain two sub-trees, called skeletons.

Definition 6 For each node $n \in G$, we erase a leaf link from either T^1 or T^2. The resulting trees are called *skeletons* denoted by $\hat{T}^1$ for T^1 and $\hat{T}^2$ for T^2.

Note that according to Theorem 1 a node cannot be an internal node in both trees. Fig. 2(b) shows the skeletons $\hat{T}^1$ and $\hat{T}^2$ of the example on Fig. 2(a).

Observation 1 *Each skeleton is a connected sub-tree of graph G.*

Proof $\hat{T}^i$ is a sub-tree of T^i having every internal node and some leaf nodes.

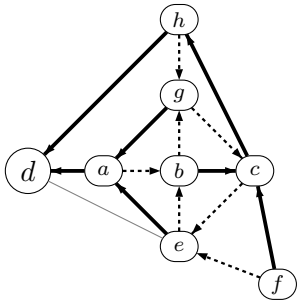


Fig. 3: Protection routing to node d, where PNH is drawn with solid thick arrows and SNH with dashed arrows.

Observation 2 *Each node $n \in V$ is a part of a skeleton and adjacent to a node in the other skeleton.*

Proof Completely independent spanning trees T^1 and T^2 cover every node of the graph twice, thus by erasing one (leaf) link form T^1 or T^2 each node remains covered by either $\hat{T}^1$ or $\hat{T}^2$ but not both. By symmetry let us assume node $n \in \hat{T}^1$. Since node n is a leaf node of T^2, node n is adjacent with an internal node of T^2 which is part of skeleton $\hat{T}^2$.

Theorem 2 *A graph with two completely independent spanning trees T^1 and T^2 is protectable.*

Proof We give a deterministic polynomial construction, which builds up a protection routing R_d from two completely independent spanning trees T^1 and T^2 respect to an arbitrary node d. First, we compute the skeletons of the two completely independent spanning trees T^1 and T^2, denoted by $\hat{T}^1$ and $\hat{T}^2$ respectively. By symmetry we assume node $d \in \hat{T}^1$. Let link e be the leaf link of T^2 adjacent to node d. Note that link e connects the two skeletons. The protection routing R_d contains the links of $\hat{T}^1$ and $\hat{T}^2$ and link e, and all the links are directed to node d. Fig. 3 shows the resulted protection routing of example Fig. 2.

To complete the proof we need to show that the network is protected by R_d. Clearly, R_d is a spanning tree because both $\hat{T}^1$ and $\hat{T}^2$ are connected subtree of graph G covering every node, and edge e connects the two skeletons. In R_d every node $u \in \hat{T}^1$ is routed to node d along links of skeleton $\hat{T}^1$ only, while each node $v \in \hat{T}^2$ is routed to node d along links of skeleton $\hat{T}^2$ and finally link e. Therefore, the routing from any node in $\hat{T}^1$ and any node in $\hat{T}^2$ are node- and link-disjoint (except for node d). By Observation 2 each node $s \neq d$ is adjacent with a node n form the other skeleton, which can be chosen as SNH, and concludes the proof.

Note that the proposed construction is much stronger than needed for protection routing, because (1) it guarantees that after a packet is sent to

SNH it will travel a fully disjoint route to the destination, compared to its original route. By the definition of protection routing the two routes may be overlapping, and should be disjoint from the failed neighboring link or node. Besides, (2) the proposed construction cannot take advantages of the possible ECMPs.

3.1 Corollaries

Corollary 1 *Conjecture 2 by Kwong et al. [4] and Conjecture 1 by Hasunuma [3] is in contradiction.*

Proof According to Conjecture 1 there are two completely independent spanning trees in any 4-node-connected graph. With two completely independent spanning trees by Theorem 2 a protection routing can be computed, which is in contradiction with Conjecture 2.

Corollary 2 *Every 4-connected maximal planar graph is protectable, and the protection routing can be calculated in linear time* $O(|E| + |V|)$.

Proof According to [3, Theorem 2] there are two completely independent spanning trees in any 4-connected maximal planar graph, which can be computed in linear time. With two completely independent spanning trees T^1 and T^2 by Theorem 2 a protection routing can be computed, by iterating through the nodes of the graph. Each step takes linear time.

Corollary 3 *Every underlying graph of a 2-connected line digraph is protectable.*

Proof It has been shown in [2] that there are k completely independent spanning trees in the underlying graph of a k-connected line digraph. With two completely independent spanning trees according to the construction of Theorem 2 protection routing can be built.

4 Conclusions

In this paper we investigated sufficient conditions for achieving protection routing in intra-domain IP networks. Kwong et al. propose a protection routing scheme in [4] and conjectured that node-connectivity of the topology graph is not sufficient for a network to be protectable. In this paper we show that this conjecture is in contradiction with a conjecture by Hasunuma [3]. Finally we show that every four-connected maximal planar graph, and every underlying graph of a 2-connected line digraph has protection routing.

Acknowledgements The work was supported by supported by the grant TÁMOP-4.2.2.B-10/1–2010-0009, the Magyary Zoltán post-doctoral program and by High Speed Network Laboratory (HSNLab).

References

1. Atlas A, Zinin A (2008) Basic specification for IP fast reroute: Loop-Free Alternates. RFC 5286
2. Hasunuma T (2001) Completely independent spanning trees in the underlying graph of a line digraph. Discrete Mathematics 234(1-3):149–157
3. Hasunuma T (2002) Completely independent spanning trees in maximal planar graphs. In: Graph-Theoretic Concepts in Computer Science, Springer, pp 235–245
4. Kwong KW, Gao L, Guerin R, Zhang ZL (2011) On the feasibility and efficacy of protection routing in ip networks. Networking, IEEE/ACM Transactions on 19(5):1543 –1556
5. Nash-Williams C (1961) Edge-disjoint spanning trees of finite graphs. Journal of the London Mathematical Society 1(1):445
6. Ohara Y, Imahori S, Van Meter R (2009) Mara: Maximum alternative routing algorithm. In: IEEE INFOCOM 2009, pp 298–306
7. Oliveira C, Pardalos P (2011) Mathematical Aspects of Network Routing Optimization, vol 53. Springer Verlag
8. Ray S, Guérin R, Kwong K, Sofia R (2010) Always acyclic distributed path computation. IEEE/ACM Transactions on Networking (ToN) 18(1):307–319
9. Reichert C, Glickmann Y, Magedanz T (2005) Two routing algorithms for failure protection in ip networks. In: IEEE Symposium on Computers and Communications (ISCC), pp 97–102
10. Resende M, Pardalos P (2006) Handbook of optimization in telecommunications, vol 10. Springer Verlag
11. Schollmeier G, Charzinski J, Kirstädter A, Reichert C, Schrodi K, Glickman Y, Winkler C (2003) Improving the resilience in ip networks. In: Workshop on High Performance Switching and Routing (HPSR), IEEE, pp 91–96