FRADIR: A Novel Framework for Disaster Resilience

Alija Pašić*, Rita Girão-Silva†‡, Balázs Vass*, Teresa Gomes†‡, and Péter Babarczi*
*MTA-BME Future Internet Research Group, Budapest University of Technology and Economics (BME), Hungary
†Department of Electrical and Computer Engineering, University of Coimbra, Portugal
‡ Institute for Systems Engineering and Computers at Coimbra (INESC Coimbra), Portugal
{pasic, vb, babarczi}@tmit.bme.hu {rita, teresa}@deec.uc.pt

***Abstract*—In this paper we present a novel framework for disaster resilience, called FRADIR, which incorporates reliable network design, disaster failure modeling and protection routing in order to improve the availability of mission-critical applications. To the best of our knowledge, this is the first comprehensive framework which utilizes tools from all these fields in a joint design of disaster resilient connections. In particular, we introduce a new probabilistic regional failure model, which does not only take into account the distance from the epicenter of the failure, but includes the (improved) availability values of the network components into the model, too. Based on the failure list generated as the result of the availability-aware disaster failure model, dedicated protection approaches are used to route the connection requests. We demonstrate the concept and benefits of FRADIR through experimental results in two real-like network topologies. Our proof-of-concept implementation shows that with the interplay between protection routing, failure modeling and network update procedure the network performance in terms of blocking probability and average resource consumption can be significantly improved, which makes FRADIR a possible competitor to provide disaster resiliency in critical infrastructures.**

***Index Terms*—disaster resilience, probabilistic failure, regional failure, spine, general dedicated protection**

I. Introduction

On the dawn of the cloud era, communication networks emerged among the topmost critical infrastructures and allowed the proliferation of mission-critical applications such as telesurgery or stock market. These services clearly demand a higher reliability and/or availability of the underlying network infrastructure than e.g., web browsing. Hence, in order to satisfy the requirements of such critical communication services on which governments and people relay more and more, the often used simplification of single link failure resilience is not considered to be enough and these connections have to be resilient to (natural and man-made) disasters as well. Therefore, the disaster resilience of communications transport networks came into the spotlight in the last years [1]–[3].

Modeling disaster failures is a quite challenging task on its own, as it should satisfy the contradicting requirements of accuracy and simplicity at the same time. Serious network outages [4]–[6] are caused by challenges that cause failure events that take down almost every equipment in a physical region as a result of a disaster, such as weapons of mass destruction attacks, earthquakes, hurricanes, tsunamis, tornadoes, etc. For example, the 7.1-magnitude earthquake in Taiwan in Dec. 2006 caused simultaneous failures of six submarine links between Asia and North America [7], and hurricane Sandy in 2012 caused a power outage silencing 46% of the network in the New York area [8]. These failures are called *regional failures*, which are simultaneous failures of nodes/links located in specific affected geographic areas [4]–[6], and offer a good compromise between accuracy and the number of disaster failures to be considered in the network design.

Several works address how to improve the availability or reliability of transport networks against certain failure events (e.g., single link failures), such as reducing the mean time to repair (MTTR) of the links by optimized labor force allocation [9], while others use network design tools [10]–[13]. The *spine* concept was first presented in [14] to denote a highly available part of the network at the physical layer. Later, in [15] the authors seek to shield (make invulnerable) a set of links to ensure connectivity of the network against certain failures. Using these *network design* approaches against disaster failure events could be very inefficient (e.g., an excessive number of links have to be shielded). As for the *spine*-based approach, it should be leveraged by *protection routing approaches*, e.g., 1+1 protection.

In this paper we present a novel FRAmework for DIsaster Resilience (*FRADIR*), which brings together network design, failure modeling and protection routing in order to improve disaster resilience of mission-critical applications. In particular, FRADIR utilizes links with a higher availability, forming a spanning tree (the considered *spine*), to improve the connectivity between the communication end-points of critical services. Note that the edge availability values have an impact on the disaster failure modeling. Finally, based on the failure list (or Shared Risk Link Groups list) obtained by the regional failure model, dedicated protection approaches are used to provide a resilient communication infrastructure for the applications.

The rest of the paper is organized as follows. Section II provides related work and the background of the study. Section III introduces the concept of FRADIR in general, and the relation of the different concepts integrated in the framework are discussed, along with its potentials and its limits. Section IV presents the simulation results, while Section V concludes our work.

II. Background

A. Network Design

Some approaches use network design tools, in order to improve the reliability of transport networks. A connection between reliability and topological network design is established in [10], where the authors consider the diameter constrained reliability, i.e. the probability that specific nodes are within a specified number of hops, in the context of different topological network design problems. In [11], the authors deal with the problem of network design, given a network with capacity constraints. The model devised by the authors includes different patterns of failures that may affect the arcs of the network over time. Different link maintenance costs are considered and a strategy for selecting links for replacement, removal or addition in the case of failures is proposed. The authors in [12] formalize a network design problem aiming at improving the network reliability even if correlated attacks occur. This is accomplished by diversifying the devices used in the network and optimally placing them in the network topology. In [13], the authors tackle a problem of designing a minimum cost network topology subject to a predefined reliability constraint. The resolution approach is based on finding a sequence of spanning trees, in an order given by different greedy heuristics.

The *spine* is based on the idea that it is advantageous to improve the availability of the most resilient component in parallel systems, which is illustrated in [16]. This high availability sub-graph of the network would be used by the flows requiring stringent and demanding availability values. The *spine* allows a wider range of flow availabilities, with respect to 1+1 protection, as shown in [17].

A heuristic for the spine selection, based only on topological characteristics of the network is presented in [17]. More recently in [18] a heuristic resolution approach to select a suitable spine, using centrality measures that take the availability of the edges into account, was proposed.

A spine design optimization model formulation is presented in [16], which seeks to minimize the cost of upgrading links availability, ensuring the desired level of end-to-end availability for each WP, while guaranteeing a link disjoint protection or *backup path (BP)* exists. Results illustrate the advantages of the approach to support QoR classes in small transport networks [16]. To solve efficiently the problem in moderate sized networks heuristics may need to be used to try and reduce the optimality gap.

It should be noted that although in the works [16]–[19] a spanning tree was used for the spine topology, other network sub-graph could have been considered.

B. Modeling Regional Failures

In order to handle multiple link failures, the concept of *Shared Risk Link Groups (SRLGs)* was introduced. An SRLG consists of a set of links which are considered to have a significant probability of failing simultaneously, and thus for each SRLG there is a backup routing plan, as the network should be prepared for dealing with failures affecting the links in the SRLG.

Clearly, listing all possible sets of links as an SRLG is not an option, as it would mean exponentially many SRLGs to be prepared for. The list of SRLGs has to be defined carefully to cover the most important failure states while also having a manageable size. Protecting networks against regional failures is usually solved either by using geometric tools [4], [20]–[22] or by aggressively reducing the problem space by identifying candidate locations of failures [5], [6], [23], [24]. As it is more flexible, often a combinatorial geometric approach is followed and will be adopted in this paper.

C. Dedicated Protection Approaches

In transport networks, even the shortest disruptions may lead to a huge amount of data loss, which is unacceptable. To avoid this, *instantaneous recovery* is required in today's transport networks. The requirement of *instantaneous recovery* is fulfilled if the recovery time is less than 50 ms [25]. This means that when planning the recovery process, the main goal is usually to keep the recovery time under 50 ms, to ensure seamless operation even when a failure occurs.

In order to fulfill these requirements, *dedicated protection* is currently the most flexible [26] candidate for improving network survivability. In today's transport networks, the most widespread dedicated protection approach is the so called 1+1. With 1+1, the data is sent parallel on the disjoint WP and BP, providing instantaneous recovery against single link failures in a simple manner. In the single link and node failure scenario the solution for the 1+1 can be obtained with the Suurballe's algorithm [27] in polynomial-time. However, if multiple failures are considered, the problem becomes NP-complete [28]. Furthermore, note that if multiple failures are considered the 1+1 has a high blocking probability (i.e. there may not be SRLG-disjoint paths in the network) due to its rigid structure.

Several papers investigated how to efficiently generalize 1+1 protection in order to protect multiple link or node failures, such as [29]–[31], or failures that affect geographically larger areas [20], while others focused on improving bandwidth efficiency.

In [32], General Dedicated Protection (GDP) was introduced, which enables instantaneous failure recovery against arbitrary failure patterns listed in the SRLG list ($\mathcal{F}$) by generalizing the rigid SRLG-disjoint path structure of 1+1 to an arbitrary directed acyclic graph between the source and target nodes. More specifically GDP protects all protectable[1] failures $f \in \mathcal{F}$ by calculating a minimum cost path in every failure graph obtained by removing the failed edges of f and adds it to the solution. Hence, it provides an extremely high connection availability and instantaneous recovery even in sparse networks for the price of increased (but still moderate) bandwidth consumption. GDP minimizes the total bandwidth

[1]We call a failure $f \in \mathcal{F}$ *protectable* if the network topology remains $s-t$ connected after removing the links in f.

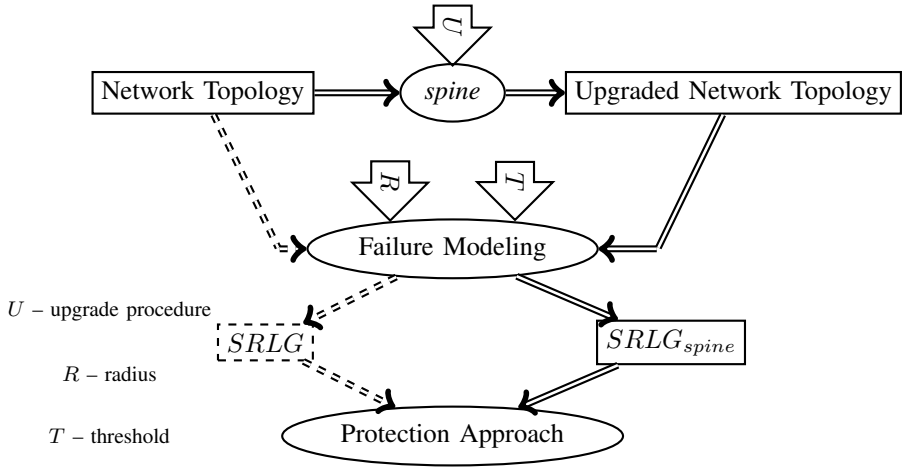


Fig. 1. The concept of FRADIR. Dashed lines represent the scenario without the *spine* topology upgrade, the full lines represents the scenario with the *spine* concept included.

cost and provides the optimal solution for the non-bifurcated scenario (called GDP-R), i.e., when the whole user data is sent along all links of the connection as in 1+1. It was shown that finding an optimal (non-bifurcated) GDP solution in terms of bandwidth cost is NP-complete [32].

III. FRADIR - Disaster Resilient Transport Networks

We argue that in order to create a truly disaster resilient network in an efficient manner it is not enough to focus separately on the network design, the failure generation modeling or the routing problem, but we have to address these problems jointly. FRADIR achieves this by integrating three already well established methods (*spine* [14], regional failure modeling [22] and GDP [32]) into a single framework. The basic concept of FRADIR is shown in Figure 1 and the process is described in Algorithm 1.

In a nutshell, in our FRADIR framework we use the *spine* concept [14] to compute a high availability structure (a spanning tree) in the topology (Algorithm 1 Step (1)). Recall that in the context of the *spine*-based approach the edges of that spanning tree are upgraded, i.e. their availability is increased by a certain amount. Next, we refine the model implemented in Section IV of [22] to take into account the unavailability values of the edges in the *spine*. In particular, as an intermediate step the concept of *Probabilistic SRLGs (PSRLGs)* is used, where every SRLG has an associated probability of failing. First we generate the list of PSRLGs according to the model implemented in [22], which is generating failing probabilities purely relying on the distances of edges from the epicenter of possible disasters. Next, the associated probabilities of failing are altered according to their unavailability values. We generate our list of SRLGs by selecting the PSRLGs with a failing probability higher than a pre-defined threshold (Algorithm 1 Step (2)). Finally, we use 1+1 and generalized dedicated protection approaches to route the connections based on this SRLG list (Algorithm 1 Step (3)). Note that in this paper we adopt GDP-R, the GDP version from [32] which assumes only forwarding packets for a fair comparison with 1+1 (i.e., network coding [32] is not allowed).

In this section first the network model is introduced (Section III-A), then in Section III-B the *spine* concept is detailed, along with its impact on the novel unavailability-based PSRLG generation in Section III-C.

Algorithm 1: The concept of FRADIR.

Input : Graph: $G = (V, E, c, A)$, Connection request: $D = (s, t, b)$, Parameters: ϵ, R, T

Output: $G' = (V, E, c, A')$, *Survivable Routing*

`// Network Design`

1 Run *spine* on $G = (V, E, c, A)$ according to [18]. Update link unavailability $U'(e) = U(e) \cdot (1 - \epsilon)$ for links in the *spine*, otherwise $U'(e) = U(e)$, creating $G' = (V, E, c, A')$, with $A' = 1 - U'$.

`// Failure Modeling`

2 Use the novel regional failure model described in Section III-C with parameters R and T on the updated network $G' = (V, E, c, A')$ (Step (1)) to generate the SRLG list $\mathcal{F}$.

`// Protection Approach`

3 Calculate the survivable routing for the connection request $D = (s, t, b)$ protecting all the failures listed in the SRLG list $\mathcal{F}$ created in Step (2).

A. Network Model

The network itself is represented with an undirected graph $G = (V, E, c, A)$ embedded in the plane $\mathbb{R}^2$, with node set V and edge set E, where the nodes V represent the OXCs (Optical Cross-Connects) and the undirected edges E represent the bidirectional fiber connections between the OXCs. Each node has a position given by coordinates in the plane (x, y) and for simplicity, edges are considered as straight line segments (intervals) in $\mathbb{R}^2$ between their endpoints. Each edge $e \in E$

has an availability value $A(e) \in [0,1]$, which is a function of the length of the edge, $\ell(e)$ [km], and is calculated as

$$A(e) = 1 - \frac{MTTR}{MTBF(e)} \tag{1}$$

where $MTTR = 24$ h (mean time to repair a failure) and $MTBF(e) = \frac{CC*365*24}{\ell(e)}$ h (mean time between failures). The parameter CC is the cable cut metric, which we assumed to be 450 km. All the edges have unit cost, i.e. $c(e) = 1, e \in E$. The cost function $c(e)$ corresponds to the cost of allocating a unit of demand (i.e. wavelength) on the given edge e.

B. Spine Design

Given a network i.e. a graph $G = (V, E, c, A)$ with the considered availability and cost values, a spine was obtained using the method described in [18] which maximizes the average availability of the WP for each demand. The unavailability of the links in this spine is reduced by multiplying it by a factor of $(1 - \epsilon)$ – this corresponds to the upgrade procedure U in the figure. Note that a more sophisticated approach for U, such as in [16], is only feasible in small instances and heuristics, adequate for coping with larger problems, have yet to be developed.

C. Unavailability-Based Regional Failure Model

As the next step we are using a new method for modeling regional failures to assess the benefits of the *spine*. As an input to the regional failure model we have graph G' (Algorithm 1 Step (2)), maximal radius of the failure $R \geq 0$ and the threshold $T \in [0,1]$. The output of the model is an SRLG list containing all the SRLGs with probability of failure above the given threshold. We emphasize that selecting a high threshold value leads to listing only some trivially probable SRLGs (e.g. non-spine single link failures), while a low T value results in listing almost every edge set that can be hit by a disk with radius at most R including highly improbable scenarios. The tuning of R and T allows to obtain the lowest number of probable SRLGs, still enabling to achieve the desired precision.

Our goal is to modify the model presented in [22] – which generates failing probabilities related to the distances of edges from the epicenter of disaster – to incorporate the *spine* concept. In other words, we modify the failing probability of each PSRLG based on the unavailability values of the edges it contains. This idea translates into reducing the probability of PSRLGs containing spine edges.

At the end, we take the list $\mathcal{F}$ of SRLGs having a failing probability higher than a threshold, as these SRLGs are considered to have the highest probability of failing after taking into account the unavailability values of the edges.

To be more precise, our model works as follows. Every disaster d has an epicenter $\mathcal{P}$ taking values $p \in \mathbb{R}^2$, with the shape overestimated by a circular disk with radius $\mathcal{R}$ taking values $r \in [0, R]$, where R is the maximum range of disasters we want to protect. We consider both $\mathcal{P}$ and $\mathcal{R}$ as random variables. Let $h(p)$ and $g(r)$ be the density function of the disaster epicenter and the disaster range, respectively. Every link $e \in E$ has an unavailability value $U(e) = 1 - A(e)$. Let $\overline{U}(e)$ be the normalized unavailability of the edges, where the $U(e)$ values are linearly scaled such that the average of the normalized unavailabilities is 1.

Let $I_{S,p,r}$ be the indicator variable which is 1 if the disk with center p and radius r hits all the edges of a set $S \subseteq E$, and 0 otherwise. With this notation, the probability of failing link set S is

$$P(S \text{ is hit}) = \int_{p \in \mathbb{R}^2} \int_{r \in [0,R]} I_{S,p,r} g(r) \mathrm{d}r \; h(p) \mathrm{d}p \prod_{e \in S} \overline{U}(e). \tag{2}$$

Due to the fact that usually we have some imprecision in the network data, a sufficiently fine discretization does not affect the precision of our results. We discretize the problem by defining a sufficiently fine resolution, say 1 km, and place a grid of 1 km $\times$ 1 km squares over the plane to assume that the values of the inner integrals (i.e. $\int_{r \in [0,R]} I_{S,p,r} g(r) \mathrm{d}r$) are almost identical for every p inside each grid cell c. This way, the whole integration problem boils down to a summation. As failure probability defined by Eq. (2) is almost identical to the one used in [22] (aside from factor $\prod_{e \in S} \overline{U}(e)$, which is not present there), detailing of the discretization is omitted here.

Besides the discretization, in our simulation we considered both h and g to have a uniform distribution, further simplifying the problem.

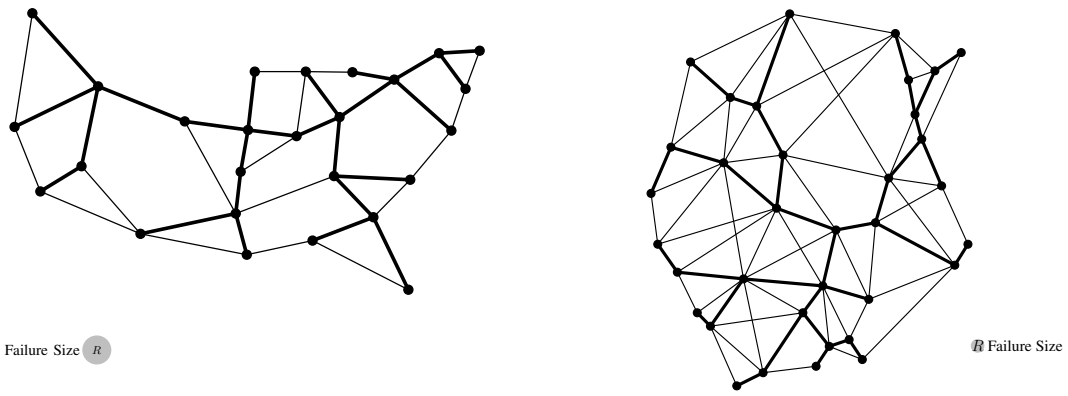
Including the unavailability values into the model yields a much more realistic approach, where the failure of the component does not only depend on the geographical distance from the disaster but also on the network component itself and its availability. Note that the availability itself depends on various factors (e.g. number of redundant components, frequency of maintenance, etc.).

IV. Experimental results

In this section we present our first experimental results (Tables I-IV) of the FRADIR framework obtained from two real world topologies [33], [34] shown in Figure 2. We compare the average capacity allocated per connection and the blocking probability of the protection approaches (1+1 protection[2] and GDP-R) with and without the upgraded availability values of the *spine* links. Several threshold values T and upgrade possibilities (corresponding to different values of ϵ) are investigated. The radius value R was fixed (50 km) assuming x-y coordinates in the gml files available at [33], [34] and the corresponding Euclidean distances. In the figures, the gray circle with R in the center is a scaled representation of distance $R = 50$ in each network.

Traffic demands are randomly generated (uniform distribution) and arrive one after the other, without any knowledge of future incoming requests. Each request is routed independently. Thus, as part of the routing problem input only a single

[2]The 1+1 is calculated with the two step approach. First the working path is calculated, then we try to calculate an SRLG-disjoint path. If it is not possible we block the connection.



(a) US (26 nodes, 42 edges, average nodal degree = 3.23) [33] (b) India (35 nodes, 80 edges, average nodal degree = 4.57) [34]

Fig. 2. The investigated networks. To visualize the size of the regional failure ($R = 50$) the radius is displayed as a gray circle. The edges in bold are in the spine.

connection request $D = (s, t, b)$ is given, which consists of the source node $s \in V$, destination node $t \in V$ and the number of bandwidth units b requested for data transmission. A total of 200 *connection requests* $D = (s, t, 1)$ were generated randomly. Note that the limited request number is a consequence of the very complex failure patterns in $\mathcal{F}$. With 200 demands it was possible to obtain the optimal solutions for GDP-R for our middle-size topologies in a reasonable time with the ILP presented in [32] (denoted simply as GDP in the tables of results).

In order to give a comprehensive overview, two scenarios were taken into account. First, all SRLGs generated by the probabilistic failure model are considered in $\mathcal{F}$ including the unprotectable SRLGs as well (i.e., the topology graph does not remain connected after failure f occurs, hence, this failure cannot be protected with any protection routing approach). A second scenario is investigated, where for each connection only the protectable SRLGs are included in the SRLG list, i.e., we prepare the protectable SRLG list $\mathcal{F}'_{s-t}$ for every $s-t$ pair by eliminating the unprotectable ones from $\mathcal{F}$. In this case the network remains $s - t$ connected $\forall f \in \mathcal{F}'_{s-t}$, thus, the GDP approach will always be able to find a disaster resilient subgraph for the connection. For clarity, in the SRLG column in Tables II and IV only the protectable SRLG number for the $s - t$ pair with the lowest number of SRLGs is shown.

One can observe that when the network is upgraded according to the *spine* concept, then all three important metrics i.e., the SRLG number, blocking probability and average capacity consumption, decrease. With the increase of ϵ the impact of the *spine* is more noticeable. Note that if $\epsilon = 1$, then we assume that the spine links are fully resilient, i.e., they do not fail in any case; hence, the network remains connected on the *spine* links all the time. Although it is not too realistic, we can use it as a benchmark.

A. Blocking Probability Analysis

We can observe that when the unprotectable SRLGs are included in the SRLG list (Tables I and III) and we do not upgrade the networks (i.e., without the *spine*) the blocking probability is extremely high, especially for the smaller and sparser US network. Of course the blocking probability depends on the threshold and radius applied in the failure model. If the threshold is higher the blocking probability decreases and of course if the radius is bigger the blocking probability increases. We see that even in this case (without considering the *spine*) the GDP significantly outperforms the 1+1 i.e., the blocking probability can be even 30% lower. In the protectable SRLG case (Tables II and IV) the difference is even more significant. Since the GDP is able to protect all protectable SRLGs the blocking probability is zero, and in the same cases the 1+1 still cannot protect more than 80% of the connections (even in Table IV with $T = 0.001$). In Table II the percentage of unprotected connections is significantly higher, as more than 88.5% of the connections are blocked by 1+1.

B. SRLG Analysis

In Tables I-IV we show that when using the *spine* concept to update the network, we can significantly reduce the number of SRLGs which fail with a larger probability than the predefined threshold. For example in Table I we see that the number of SRLGs decreases from 450 to 163 for $\epsilon = 0.7$ and $T = 0.0005$. Simultaneously the blocking probability from 1+1 decreases from 100% to 60% and for GDP from 87.5% to 38%.

We can also observe that the SRLG number in the protectable SRLG scenario is not significantly lower than in the unprotectable SRLG scenario e.g. when comparing Table I and Table II we see that without the *spine* the number drops from 450 to 435 and from 293 to 283 for $T = 0.0005$ and $T = 0.001$ respectively. When the *spine* is introduced the difference is even smaller: depending on ϵ and the threshold

the difference goes from 0 to 8 SRLGs. When the ϵ value is high enough the *spine* is able to make the critical links resilient, and the GDP is able to protect all the connections.

C. Resource Consumption Analysis

In Tables I-IV we show that the GDP has a better capacity efficiency than 1+1, in the investigated scenarios where their blocking probability is equal. This happens because of the flexible structure of GDP which avoids the deployment of lengthy disjoint backup paths to protect every failure. The GDP approach can reduce the bandwidth cost of 1+1 in most network scenarios with 1 unit per connection, which could lead to a significant capacity saving in transport networks with excessive number of connections.

Note that GDP contains 1+1 as a special case and always improves its resource consumption if both problems are solvable. The cases (e.g., Table II without the *spine*, and in some of the cases with the *spine*) when the GDP reserves more capacity than the 1+1 indicate that GDP was able to route additional connections in the network compared to 1+1, which were able to benefit from its flexible (although sometimes costly) structure.

V. Conclusions and Future Work

In this paper we presented FRADIR, a framework which utilizes already well established methods (*spine* [14], regional failure modeling [22] and GDP [32]) to create truly disaster resilient networks in an efficient manner. We showed the benefits of FRADIR through experimental results, and demonstrated that with the proper protection routing, disaster failure modeling and network update procedure we can significantly improve the network performance in terms of blocking probability and average resource consumption, while providing the required availability level for mission-critical applications.

In the future we plan to extend FRADIR with a feedback loop from the regional failure model to the network design phase, i.e., the probabilistic failure information can be utilized to enhance the efficiency of the *spine* design. Furthermore, in our proof-of-concept implementation the GDP minimizes the resource consumption oblivious to the location of the reliable *spine* links. In order to further improve the availability of the connection, GDP can be implemented by preferring the *spine* links, even if they yield a higher resource consumption in some cases.

Acknowledgments

This article is based on work from COST Action CA15127 RECODIS (Resilient communication services protecting end-user applications from disaster-based failures), supported by COST (European Cooperation in Science and Technology). A. Pašić, B. Vass, and P. Babarczi were partially supported by the High Speed Networks Laboratory (HSNLab) at the Budapest University of Technology and Economics, by the BME-Artificial Intelligence FIKP grant of EMMI (BME FIKP-MI/SC), and by the Hungarian Scientific Research Fund (grant No. OTKA K 124171). The work of R. Girão-Silva and T. Gomes was partially supported by Fundação para a Ciência e a Tecnologia (FCT) under project grant UID/MULTI/00308/2013 and was financially supported by FEDER Funds and National Funds through FCT under project CENTRO-01-0145-FEDER-029312. The work of P. Babarczi was partially supported by the Post-Doctoral Research Fellowship of the Alexander von Humboldt Foundation.

References

[1] J. Rak, D. Hutchison, E. Calle, T. Gomes, M. Gunkel, P. Smith, J. Tapolcai, S. Verbrugge, and L. Wosinska, "Recodis: Resilient communication services protecting end-user applications from disaster-based failures," in *Transparent Optical Networks (ICTON), 2016 18th International Conference on*. IEEE, 2016, pp. 1–4.

[2] T. Gomes, J. Tapolcai, C. Esposito, D. Hutchison, F. Kuipers, J. Rak, A. De Sousa, A. Iossifides, R. Travanca, J. André *et al.*, "A survey of strategies for communication networks to protect against large-scale natural disasters," in *Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop on*. IEEE, 2016, pp. 11–22.

[3] A. Mauthe, D. Hutchison, E. K. Cetinkaya, I. Ganchev, J. Rak, J. P. Sterbenz, M. Gunkelk, P. Smith, and T. Gomes, "Disaster-resilient communication networks: Principles and best practices," in *Resilient Networks Design and Modeling (RNDM), 2016 8th International Workshop on*. IEEE, 2016, pp. 1–10.

[4] S. Neumayer, G. Zussman, R. Cohen, and E. Modiano, "Assessing the vulnerability of the fiber infrastructure to disasters," *Networking, IEEE/ACM Transactions on*, vol. 19, no. 6, pp. 1610–1623, 2011.

[5] B. Mukherjee, M. Habib, and F. Dikbiyik, "Network adaptability from disaster disruptions and cascading failures," *Communications Magazine, IEEE*, vol. 52, no. 5, pp. 230–238, 2014.

[6] R. Souza Couto, S. Secci, M. Mitre Campista, K. Costa, and L. Maciel, "Network design requirements for disaster resilience in IaaS clouds," *Communications Magazine, IEEE*, vol. 52, no. 10, pp. 52–58, 2014.

[7] D. M. Masi, E. E. Smith, and M. J. Fischer, "Understanding and mitigating catastrophic disruption and attack," *Sigma Journal*, pp. 16–22, 2010.

[8] J. Heidemann, L. Quan, and Y. Pradkin, *A preliminary analysis of network outages during hurricane Sandy*. University of Southern California, Information Sciences Institute, 2012.

[9] H. Chang and P. Wang, "Upgrading service availability of optical networks: A labor force perspective," *International Journal of Communication Systems*, p. e3553, first published: 8 March 2018.

[10] F. Robledo, P. Romero, and M. Saravia, "On the interplay between topological network design and diameter constrained reliability," in *2016 12th International Conference on the Design of Reliable Communication Networks (DRCN)*, March 2016, pp. 106–108.

[11] D. Papadimitriou and B. Fortz, "Reliability-dependent combined network design and routing optimization," in *2014 6th International Workshop on Reliable Networks Design and Modeling (RNDM)*, Nov 2014, pp. 31–38.

[12] Y. Prieto, J. E. Pezoa, N. Boettcher, and S. K. Sobarzo, "Increasing network reliability to correlated failures through optimal multiculture design," in *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Oct 2017, pp. 1–6.

[13] B. Elshqeirat, S. Soh, S. Rai, and M. Lazarescu, "Topology design with minimal cost subject to network reliability constraint," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 118–131, March 2015.

[14] D. Tipper, "Resilient network design: challenges and future directions," *Telecommunication Systems*, vol. 56, no. 1, pp. 5–16, 2014.

[15] J. Zhang, E. Modiano, and D. Hay, "Enhancing network robustness via shielding," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2209–2222, Aug 2017.

[16] A. Alashaikh, D. Tipper, and T. Gomes, "Designing a high availability subnetwork to support availability differentiation," in *14th International Conference on the Design of Reliable Communication Networks (DRCN 2018)*, Paris, France, 19 February 2018.

[17] A. Alashaikh, T. Gomes, and D. Tipper, "The spine concept for improving network availability," *Computer Networks*, vol. 82, pp. 4–19, 2015.

TABLE I
US (26 NODES, 42 EDGES) – ALL SRLGS (UNPROTECTABLE SRLGS INCLUDED).

Without *spine*				With *spine*				
SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	ϵ
$R = 50; T = 0.0005$								
450	nan	12.92	100 87.5	163	8.94	8.57	60 38	0.7
				128	7.76	8.57	38 17	0.8
				109	7.99	8.87	35.5 17	0.85
				91	8.40	8.15	19 17	0.90
				71	8.22	6.96	0 0	0 .95
				61	7.64	4.615	0 0	1
$R = 50; T = 0.001$								
293	8.615	10.127	93.5 70.5	131	8.03	8.97	51 29	0.5
				96	8.19	8.71	31.5 17	0.7
				58	7.99	6.86	0 0	0.90
				50	7.58	4.87	0 0	0.95
				48	7.48	4.62	0 0	1

TABLE II
US (26 NODES, 42 EDGES) – PROTECTABLE SRLGS.

Without *spine*				With *spine*				
SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	ϵ
$R = 50; T = 0.0005$								
435	7	13.65	99.5 0	155	7.88	10	52 0	0.7
				123	7.94	9.39	38 0	0.8
				107	8.13	9	26 0	0.85
				89	8.63	8.25	2.5 0	0.9
				71	8.22	6.96	0 0	0.95
				61	7.64	4.62	0 0	1
$R = 50; T = 0.001$								
283	9	12	88.5 0	126	8.23	9.63	41 0	0.5
				94	8.34	8.77	19.5 0	0.7
				58	7.99	6.86	0 0	0.90
				50	7.58	4.87	0 0	0.95
				48	7.48	4.62	0 0	1

TABLE III
INDIA (35 NODES, 80 EDGES) – ALL SRLGS (UNPROTECTABLE SRLGS INCLUDED).

Without *spine*				With *spine*				
SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	ϵ
$R = 50; T = 0.0005$								
1126	7.92	8.16	69 40	501	7.49	7.09	9 9	0.8
				489	7.43	6.96	9 9	0.85
				471	7.34	6.29	0 0	0.9
				465	7.34	5.76	0 0	0 .95
				463	7.34	5.40	0 0	1
$R = 50; T = 0.001$								
410	7.85	7.57	22 18	243	7.245	6.25	0 0	0.8
				240	7.245	6.06	0 0	0.85
				237	7.25	5.72	0 0	0.90
				235	7.24	5.38	0 0	0.95
				235	7.24	5.38	0 0	1

TABLE IV
INDIA (35 NODES, 80 EDGES) – PROTECTABLE SRLGS.

Without *spine*				With *spine*				
SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	SRLG number	Average capacity 1+1	Average capacity GDP	Blocking prob. [%] 1+1 GDP	ϵ
$R = 50; T = 0.0005$								
1114	8.094	9.55	57.5 0	499	7.49	7.47	9 0	0.8
				488	7.40	7.02	6.5 0	0.85
				471	7.34	6.29	0 0	0.9
				465	7.34	5.76	0 0	0 .95
				463	7.34	5.40	0 0	1
$R = 50; T = 0.001$								
406	7.75	8.205	20 0	243	7.245	6.25	0 0	0.8
				240	7.25	6.06	0 0	0.85
				237	7.25	5.72	0 0	0.90
				235	7.24	5.38	0 0	0.95
				235	7.24	5.38	0 0	1

[18] R. Girão-Silva, L. Martins, T. Gomes, A. Alashaikh, and D. Tipper, "Improving network availability - a design perspective," in *Third International Congress on Information and Communication Technology (ICICT 2018)*, London, United Kingdom, February 27-28 2018, to appear in Springer Advances in Intelligent Systems and Computing, ISBN Number - 2194-5357 Series.

[19] A. Alashaikh, D. Tipper, and T. Gomes, "Exploring the logical layer to support differentiated resilience classes in multilayer networks," *Annals of Telecommunications*, vol. 73, no. 1, pp. 63–79, Feb 2018.

[20] P. K. Agarwal, A. Efrat, S. K. Ganjugunte, D. Hay, S. Sankararaman, and G. Zussman, "The resilience of WDM networks to probabilistic geographical failures," *IEEE/ACM Transactions on Networking*, vol. 21, no. 5, pp. 1525–1538, 2013.

[21] J. Tapolcai, L. Rónyai, B. Vass, and L. Gyimóthi, "List of shared risk link groups representing regional failures with limited size," in *Proc. IEEE INFOCOM*, Atlanta, USA, may 2017.

[22] J. Tapolcai, B. Vass, Z. Heszberger, J. Biró, D. Hay, F. A. Kuipers, and L. Rónyai, "A tractable stochastic model of correlated link failures caused by disasters," in *Proc. IEEE INFOCOM*, Honolulu, USA, Apr. 2018.

[23] F. Dikbiyik, M. Tornatore, and B. Mukherjee, "Minimizing the risk from disaster failures in optical backbone networks," *Journal of Lightwave Technology*, vol. 32, no. 18, pp. 3175–3183, 2014.

[24] X. Long, D. Tipper, and T. Gomes, "Measuring the survivability of networks to geographic correlated failures," *Optical Switching and Networking*, vol. 14, pp. 117–133, 2014.

[25] J. Vasseur, M. Pickavet, and P. Demeester, *Network recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publishers, 2004.

[26] W. Kellerer, A. Basta, P. Babarczi, A. Blenk, M. He, M. Klugel, and A. M. Alba, "How to measure network flexibility? A proposal for evaluating softwarized networks," *IEEE Communications Magazine*, vol. PP, no. 99, pp. 2–8, 2018.

[27] J. W. Suurballe, "Disjoint paths in a network," *Networks*, vol. 4, pp. 125–145, 1974.

[28] G. Ellinas, E. Bouillet, R. Ramamurthy, J.-F. Labourdette, S. Chaudhuri, and K. Bala, "Routing and restoration architectures in mesh optical networks," *Optical Networks Magazine*, vol. 4, no. 1, pp. 91–106, January/February 2003.

[29] P. Babarczi, J. Tapolcai, P.-H. Ho, and M. Médard, "Optimal Dedicated Protection Approach to Shared Risk Link Group Failures using Network Coding," in *Proc. IEEE ICC*, 2012, pp. 3084–3088.

[30] H. Luo, L. Li, and H. Yu, "Insights for segment protection in survivable WDM mesh networks with SRLG constraints," *Photonic Network Communications*, vol. 14, no. 3, pp. 361–368, 2007.

[31] P. Babarczi, J. Tapolcai, and P. Ho, "Availability-constrained Dedicated Segment Protection in circuit switched mesh networks," in *Workshop on Reliable Networks Design and Modeling (RNDM)*, 2009, pp. 1–6.

[32] P. Babarczi, A. Pasic, J. Tapolcai, F. Németh, and B. Ladóczki, "Instantaneous recovery of unicast connections in transport networks: Routing versus coding," *Elsevier Computer Networks*, vol. 82, pp. 68–80, 2015.

[33] "US Network," http://lendulet.tmit.bme.hu/~pasic/networks/, accessed: 2018-04-14.

[34] SNDlib, "Survivable fixed telecommunication network design library," http://sndlib.zib.de.