Telecommun Syst (2015) 60:423–450
DOI 10.1007/s11235-015-9987-7

Future research directions in design of reliable communication systems

Jacek Rak · Mario Pickavet · Kishor S. Trivedi · Javier Alonso Lopez · Arie M. C. A. Koster · James P. G. Sterbenz · Egemen K. Çetinkaya · Teresa Gomes · Matthias Gunkel · Krzysztof Walkowiak · Dimitri Staessens

Published online: 27 March 2015
© The Author(s) 2015. This article is published with open access at Springerlink.com

Abstract In this position paper on reliable networks, we discuss new trends in the design of reliable communication systems. We focus on a wide range of research directions including protection against software failures as well as failures of communication systems equipment. In particular, we outline future research trends in software failure mitigation, reliability of wireless communications, robust optimization and network design, multilevel and multirealm network resilience, multiple criteria routing approaches in multilayer networks, resilience options of the fixed IP backbone network in the interplay with the optical layer survivability, reliability of cloud computing networks, and resiliency of software-defined networks. Described research directions are frequently enhanced with examples.

Keywords Network reliability · Software failures · Software-defined networks resiliency · Wireless communications reliability · Multilayer networks · Multilevel and multirealm network resilience · Multiple-criteria routing · Reliable cloud computing · Robust network design

1 Introduction

Despite numerous efforts to improve Quality of Service in communication networks in the presence of failures, it is not possible to provide 100 % of service availability. Since faults

J. Rak (✉)
Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Narutowicza 11/12, 80-233 Gdansk, Poland
e-mail: jrak@pg.gda.pl

M. Pickavet · D. Staessens
Ghent University - iMinds, Gaston Crommenlaan 8, 9050 Ghent, Belgium
e-mail: mario.pickavet@ugent.be

D. Staessens
e-mail: dimitri.staessens@ugent.be

K. S. Trivedi · J. A. Lopez
Electrical and Computer Engineering Department, Duke University, Durham, NC 27708-0291, USA
e-mail: ktrivedi@duke.edu

J. A. Lopez
Research Institute of Applied Sciences in Cybersecurity, University of Leon, 24004 León, Spain
e-mail: Javier.alonso@unileon.es

A. M. C. A. Koster
Lehrstuhl II für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
e-mail: koster@math2.rwth-aachen.de

J. P. G. Sterbenz · E. K. Çetinkaya
Electrical Engineering and Computer Science Department, Information and Telecommunication Technology Center, The University of Kansas, 154 Nichols Hall, Lawrence, KS, USA
email: jpgs@ittc.ku.edu
URL: http://www.ittc.ku.edu/resilinets

E. K. Çetinkaya
e-mail: ekc@ittc.ku.edu

J. P. G. Sterbenz
School of Computing and Communications, InfoLab21, Lancaster University, Lancaster, UK
e-mail: jpgs@comp.lancs.ac.uk

J. P. G. Sterbenz
Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong
e-mail: jpgs@comp.polyu.edu.hk

in communication systems are inevitable, construction of perfect communication systems, as well as full prevention against various challenges and threats is not possible [131]. However, by providing a proper defence, detection of unwanted events, remediation of negative effects, and recovery to normal operational state (e.g., by applying the $D^2R^2 + DR$ diagnose and refinement approach from [132] sketched in Fig. 1), a significant improvement in terms of *network resilience*, defined in [130,133] as the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation, can be achieved. According to [133], resilience itself includes survivability, fault tolerance, disruption tolerance, dependability, performability, as well as security.

In this position paper on reliable networks, we are particularly interested in *network reliability* defined in [7] as the continuity of correct service, being an important element of a *communication system dependability* (i.e., ability to avoid service failures that are more frequent and more severe than acceptable [7]). In particular, the aim of this paper is to outline the research directions in network reliability that are in our opinion of utmost importance, and point out important problems to be solved in the future.

Based on the general structure of communication systems that are expected to comply with ISO/OSI communication system model including seven layers: Physical (L1), Data Link (L2), Network (L3), Transport (L4), Session (L5), Presentation (L6), and Application (L7), we focus on a wide range of research directions in the area of communication systems reliability. Therefore we address not only issues concerning reliability of communications network infrastructure, but also point out problems related to software failures.

E. K. Çetinkaya
Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409, USA
email: cetinkayae@mst.edu

T. Gomes
Department of Electrical and Computer Engineering / INESC Coimbra University of Coimbra Coimbra, Portugal
email: teresa@deec.uc.pt

M. Gunkel
Deutsche Telekom, Fixed-Mobile Engineering Deutschland, Heinrich-Hertz-Strasse 3-7, Darmstadt, Germany
email: gunkelm@telekom.de

K. Walkowiak
Department of Systems and Computer Networks, Wroclaw University of Technology, Wroclaw, Poland
email: krzysztof.walkowiak@pwr.edu.pl

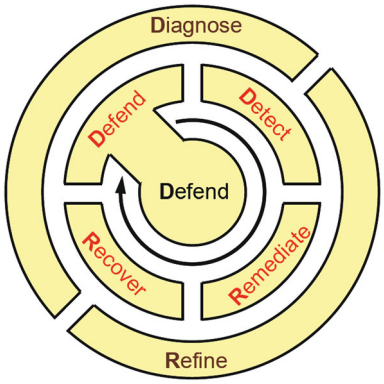


Fig. 1 Key components of the $D^2R^2 + DR$ strategy from [132]

In particular, Sect. 2 presents the up-to-date research directions related to software failure mitigation. Indeed following [53,108,110], about 40–50 % of communication systems failures are related with software. Despite applying, formal methods to reduce the probability of software failures, development of fault-free software seems hardly feasible. In Sect. 2, apart from presenting the classification of failures, the authors focus on the "Environmental diversity" concept to show the impact of the environment on failures, as well as indicate important open problems for future research.

In the next sections, we outline issues related to reliability of communication networks infrastructure. In general, this issue has received much attention so far in the literature with respect to wired networks. The respective approaches have been proposed for protection of communication paths, e.g., by means of alternate paths called *backup paths* (*BP*) being link/node disjoint with the primary paths (also called working or *active paths*—*AP*) being protected (see Fig. 2).

Alternate paths could be either installed in advance (*protection scheme*), or found dynamically after a failure (restoration scheme) [118]. Therefore, protection scheme guarantees full recovery with respect to the demanded capacity, while dynamic restoration provides backup paths only on the best-effort rule [140]. Concerning the scope of backup routes, the most important proposals include path, segment or link protection/restoration [102,111,118,137].

For network operators, the main aim is to provide the demanded service to customers while minimizing the total capacity and/or energy consumption. However, from the perspective of a user, it is often more important to provide fast recovery of flows affected by the failure [114].

Specific variants of algorithms to find communication paths are designed for protection of either static or dynamic traffic, i.e., with respect to volumes of traffic that do not change much over time (e.g., in core parts of the network), or are heavily time-dependent, accordingly.

Since the general problem of finding communication paths in capacity-constrained networks is *NP*-complete, efficient

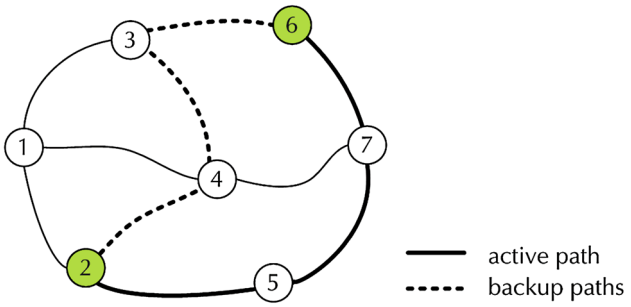


Fig. 2 Example active and backup paths

heuristic algorithms to find disjoint paths have been proposed (see e.g. [16]). In particular, due to time constraints, such heuristics seem to be the only solution in the case of dynamic traffic protection/restoration.

Available algorithms to find disjoint paths mostly refer to the case of *single-cost networks*, i.e., implying the same cost c_{ij} of link l_{ij} in all path computations (for both working and backup paths). However, this assumption is often not proper, e.g., in case of sharing the link capacity by several backup paths, where, the cost of a link in backup path computations is frequently the fraction of the respective cost used for working path computations. This is the example of the so-called *multi-cost networks* case, for which specific algorithms to find disjoint paths should be used, e.g., the k-Penalty algorithm from [113].

A large group of solutions refers to the case of *random failures*, i.e., failures of nodes/links having no mutual correlation. This assumption is often non-realistic, since characteristics of network elements themselves frequently have an impact on differentiated failure probabilities. Also, apart from failures that are random by nature, there is a large group of accidents being result of malicious human activities, referred to as *attacks*. The respective proposals of resistant-to-attack routing approaches can be found e.g., in [1,117].

The model of random failures is also not proper in case of modeling vulnerability of wireless networks owing to the observed spatial correlation of failures being result of e.g., natural disasters like heavy rain falls. In such case, available capacity of links significantly varies over time. We are convinced that this is a new research area that will receive much attention in the future. In particular, there is a need to provide reliable transmission schemes able to respond to *region failures*, i.e., simultaneous multiple failures occurring in bounded areas. The respective Sect. 3, first outlines characteristics of failures in wireless networks, and next shows two important directions of future research, i.e., providing the reliable transmission in Wireless Mesh Networks (WMNs) and in wireless mobile networks (here for the scenario of vehicle-to-vehicle communications in vehicular ad-hoc networks—VANETs). Section 4 in turn focuses on algorithmic aspects and future research directions in design of efficient methods to find communication paths.

In the next part of the paper, we focus on future directions with respect to resilience of multilayer networks. Recent communication networks are undoubtedly multilayer, i.e., composed of a stack of networks in client-server relationship. In general, in multilayer networks, the lower-layer network offers transport services to the higher-layer network [103]. The most promising architecture seems to the two-layer IP-over-Wavelength Division Multiplexing (WDM) structure with IP flows served directly by the WDM layer [96]. In general, protection/restoration approaches mentioned earlier in this section, can be easily adapted to provide protection of transmission in multilayer networks. However, in this case, it is important to define proper rules of cooperation between network layers to provide the multilayer resilience. This is a well-researched area, and the respective interworking strategies defining e.g., the sequence of network layers to perform recovery of affected flows, as well as a way of exchanging the respective information between the network layers, have been proposed e.g., in [32,38,39].

Observed evolution of end-user demands characteristics, implying the respective change of communication networks functionalities, brings out new challenges for the design of resilient multilayer networks, outlined in Sects. 5–7.

In particular, Sect. 5 extends the idea of multilayer network resilience towards resilience of multilevel and multi-realm networks—other concepts that are foreseen to gain attention in the future, especially in the case of multiple service providers interconnected in the Autonomous System.

Section 6 focuses on recent and future challenges of multiple-criteria routing schemes for multilayer networks. Unlike single-criteria models, in multiple criteria models, an explicit representation and mathematically-consistent treatment of the trade-off among multiple criteria in the objective functions can be achieved.

Section 7 points out problems related to deployment of multilayer networks in practice based on example challenges experienced by Deutsche Telekom. After focusing on practically operated real networks, and issues related to cost-aware approaches to multilayer network resilience, it presents the operator's concept of resilient IP-over-WDM network and pays special attention to Elastic Optical Networking, as a potential key element of architecture of future real multilayer networks.

Last two sections are particularly closely related to recent proposals of the architecture of Future Internet. The general idea behind these works is to design the architecture of Future Internet from scratch taking into consideration the best practices from the past. Leading research teams tend to design the Internet as a "hyper-network" consisting of networks of different types with special focus on parallel networks con-

cept, virtualization, new services, as well as architecture of data and control planes.

In particular, Sect. 8 includes the concept of *cloud computing* as one of the major solutions to reduce costs of deployment and provisioning of IT services in the future. Potential future research fields outlined in this section include: redundant data storage, issues related to energy consumption, or overload control. The last Sect. 9 refers to resiliency issues in Software-Defined Networks. Special focus is put on OpenFlow protocol, virtualization of network resources, as well as differentiated concepts of data and control plane resiliency.

2 Research directions in software failure mitigation

Our society′s pervasive dependence on computers and networks mandates that these systems be highly reliable. As per several surveys, underlying causes of the failures of the systems can be classified into three main categories: Hardware, Human, and Software. The proportions of failure causes have been evolving with software emerging as the main cause of system failures, representing between 40 and 50 % of the failures [53,108,110].

It seems to be tacitly assumed that the networks and telecommunication systems failures are mainly caused by hardware, though, some papers have revealed that the software is also one of the main causes of failures [35,76,92].

Despite many advances in formal methods, programming methodologies and testing techniques, developing fault-free software is an unaffordable task, if not unachievable. A good (and expensive) development process can reduce the number of residual faults to 1 per 10,000 lines of code [65]. It is clear that complex systems will be deployed with many faults. Hence, software fault tolerance during operation becomes a critical component to deal with the software faults and the consequent system failures. However, the software reliability literature has been focused on development, debugging, testing; neglecting the operational phase of the systems.

The authors of [78,95] propose the use of design diversity to deal with faults during operation. However, the practical applicability of design diversity has been limited by its excessive cost; it can only be justified in life-critical systems.

A question arises: is it possible to design affordable software fault tolerance to deal with failures during operation?

Traditionally, hardware transient failures have been mitigated by means of retry while hardware intermittent failures have been dealt with by rebooting or restarting the system. In recent years, transient or intermittent software failures, caused by underlying software faults, have also been mitigated by applying the same approaches. Based on this reasoning, we submit that a software fault tolerance approach based on retry, restart, reboot or fail-over to an identical software replica (not a diverse version) to deal with the failures caused by some types of software faults during operation is an affordable means of software fault tolerance.

Based on their characteristics, software faults can be classified into *Bohrbugs* (*BOHs*), *non-aging-related Mandelbugs* (*NAMs*), and *Aging-related bugs ARBs*) [52,54,57,58].

The term Bohrbug was coined by Gray [52] in 1985. It refers to faults that are easy to isolate, reproduce, and thus fix. By contrast, Mandelbug refers to those faults whose activation and/or error propagation is complex enough, resulting in a "non-deterministic" behavior.

Mandelbugs are intrinsically related to software complexity, as defined by Dörner [43, pp.38]. This complexity can be caused by:

1. a time lag between the fault activation and the occurrence of a failure; or
2. the influence of indirect factors, e.g.,
   (a) interactions of the software application with its system-internal environment (hardware, operating system, other applications); or
   (b) influence of the timing of inputs and operations (relative to each other, or in terms of the system runtime or calendar time); or
   (c) influence of the sequencing of operations; sequencing is considered influential, if the inputs could have been run in a different order and if at least one of the other orders would not have led to a failure.

A subtype of Mandelbug, called Aging-related bug, is responsible for the software aging phenomenon [55]. Software aging causes an increasing failure rate or progressive performance degradation. This phenomenon is especially evident in long-running applications [24]. In the case of the Aging-related bugs, software rejuvenation has been used as a proactive countermeasure. Software rejuvenation is based on stopping the application, cleaning its internal state and/or its environment, and restarting it. According to [56], the fraction of BOH, NAMs, ARBs across different types of software is found to be 61.4, 32.1, and 4.4 %, respectively.

Figure 3 summarizes the software fault classification and corresponding fault/failure mitigation approaches.

This classification of the software faults is not only theoretical, but is also relevant in practice: Each type of software fault requires different type of recovery approaches. The classification is relevant in developing effective software fault tolerance mechanisms, and if possible, determining the optimal times for preventive maintenance.

In [4], the nature of the times to flight software of different NASA/JPL missions was studied. Such an analysis of real TTF data can lead to better prediction of future failures, possible preventive maintenance schedules, better mitigation techniques and eventually better software designs.

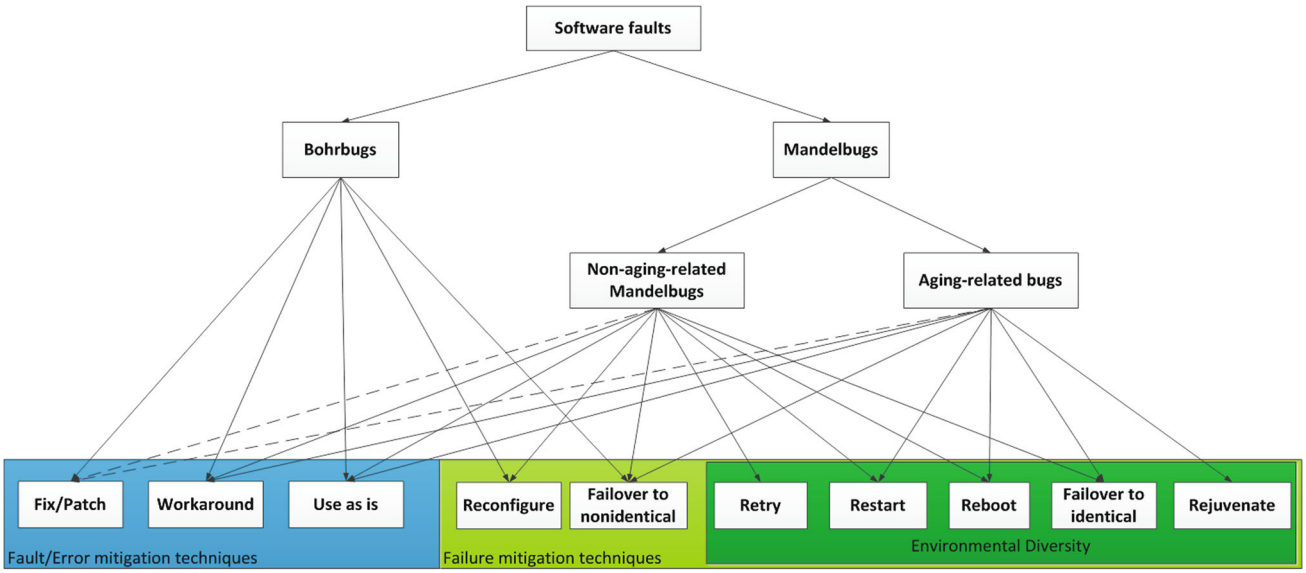


Fig. 3 Software fault/failure mitigation classification tree

Since the percentage of Mandelbugs in real-life software systems is not negligible, we advocate an affordable software fault tolerance via *Environmental diversity*. The underlying idea of Environmental diversity is that when we retry a previously faulty operation and it works, it is because of the environment where the operation was executed has changed enough to avoid the Mandelbug activation. The environment is understood as the resources of the operating system, other applications running concurrently and sharing the same resources, interleaving of operations, concurrency, or synchronization. The Environmental diversity idea is illustrated in Fig. 4.

In [5], we have discussed the different Environmental diversity approaches applied in 8 NASA/JPL missions. We found that the most used approach was fix and patch, as expected. However, a non-negligible fraction (approx. 11 %) of failures caused by NAMs was solved via Environmental diversity approaches (Retry, Reboot, Restart, and Failover to identical copy). While, only 1.6 % of failures caused by BOHs was fixed with these methods. This clearly shows the effectiveness of Environmental Diversity approach to deal with failures and their underlying faults during operations.

Summarizing, Environmental Diversity uses time redundancy over the expensive design diversity approach. Even though the term is relatively new, it has been applied in different systems [6,49,97,98,138,139] with successful and effective results.

Based on the above reasoning, we understand that the future of software fault tolerance lies in the implementation of these affordable solutions based on Environmental Diversity. These mechanisms will improve the availability of the systems at a reasonable cost without requiring reengineering the current or legacy applications and systems.

3 Reliability of wireless communications

Reliability of wireless communications is a relatively new research area. Compared to the number of results available in the literature concerning wired networks reliability issues, and, in particular, wired networks survivability (see e.g., [118,129,135,141]), there are only several respective proposals for wireless networks.

In general, reliability of wireless communications is harder to achieve mainly owing to problems related to time-dependent effective capacity of links. This capacity is frequently reduced (partially or completely) by disruptions of many kinds, the most important ones being e.g., channel fading, crosstalks, or weather-based factors. The problem becomes even more important for mobile wireless networks, where effective link capacity is also a function of time-varying distance between nodes.

We are convinced that reliability of wireless communications will remain an open research area in the forthcoming years. To justify this opinion, in this section, we provide an overview of current research results concerning wireless networks reliability, as well as indicate some future research topics.

In particular, in Sect. 3.1, we first concentrate on existing failure models and measures of fault tolerance proposed for wireless communications. After that, we present an overview of recent methods to provide reliability of communications for two different example scenarios of wireless communications, i.e., for Wireless Mesh Networks (with stationary nodes)—Sect. 3.2, and for Vehicular Ad-hoc Networks—VANETs (with mobile nodes)—Sect. 3.3, accordingly. In each case, we also discuss possible directions of future research.

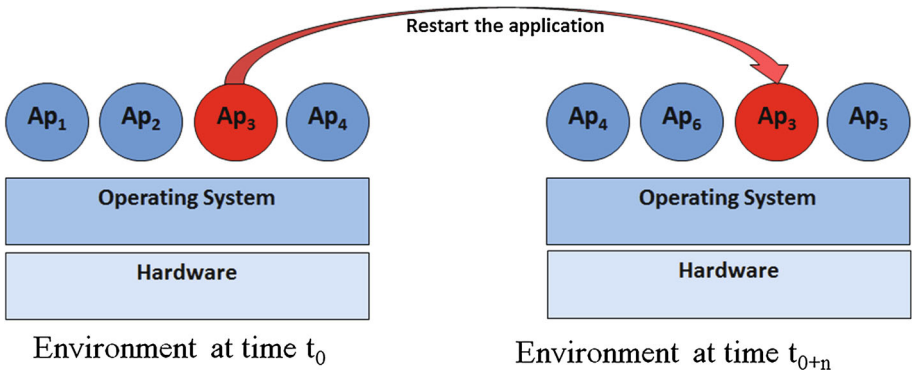


Fig. 4 Environmental diversity approach

3.1 Failure models and measures of fault tolerance

A large group of research papers present results for a model of isolated random failures [1]. In this model, failures of network elements have no mutual correlation. Such an assumption, even though realistic for wired networks, seems to be often inadequate for wireless communications. This is due to frequently observed spatial correlation between failures of wireless network elements being result of e.g., natural disasters (tornadoes, heavy rain falls), or malicious human activities (e.g., bomb explosions) [94].

Spatial correlation between failures in turn leads to the concept of a *region failure*, presented e.g., in [82,105,121], allowing for a simultaneous failure of several network elements located within a given area of a negative influence. Such a model seems to be appropriate for both node and link failures. In the latter case, it may imply either partial, or complete degradation of effective capacity of links.

Based on [121], the most common representation of a failure region is the geometrical one formed by a circular area of a given radius r. This is especially reasonable for natural disasters like earthquakes implying probability of failures of network elements proportional to their distance from the failure epicentre, as shown in Fig. 5.

Authors of most research papers on region failures assume that at a given time, failures are constrained to one region only. Results of modeling the simultaneous failures occurring in multiple regions can be found e.g., in [1,121].

Based on failure assumptions, known approaches to region failure modeling can be categorized as either *deterministic*-, or *probabilistic failure-based*. The first class (see e.g., [121, 150]) implies a failure with probability 1 of any network element located inside a given region, while in the latter one, probability of a network element failure is a monotonously decreasing function of distance between this node and the failure epicentre. In general, probabilistic models seem to be more suitable. However, they also have some limitations. For instance, in the model from [94], radius r of the circular failure region is assumed to be constant, which is in obvious contrast to reality. Another constraint remarkably limiting

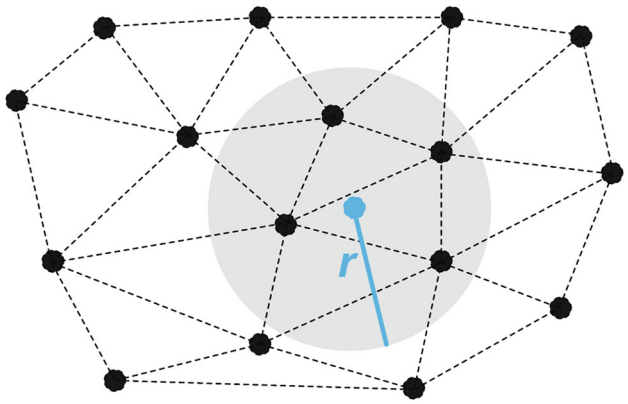


Fig. 5 Example of a region failure. The area of possible failures of network elements is represented here by a circle of a given radius r, centered at the failure epicentre

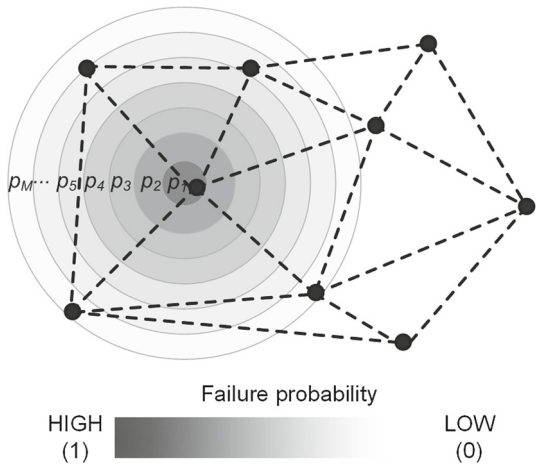


Fig. 6 Example region failure probabilities from [94]

application of this model in practice refers to probability p_i of node failures defined as a unique constant value in each ith area between two consecutive concentric annuluses, as given in Fig. 6. As a result, failure probability values are over-, or underestimated, accordingly.

Real failure scenarios together with topological characteristics of a network, have a direct implication on the resulting

level of network reliability. In order to evaluate the vulnerability of networks to random failures, average connectivity [11], distance connectivity [9], or path connectivity [61] measures can be used. The respective proposal of a wireless network reliability measure for a region failure scenario can be found in [122].

Scenarios of failures mentioned above can be found in the literature with respect to either stationary, or mobile nodes. In order to outline the current research directions for both cases, in the latter part of this section, we decided to focus on two example architectures of WMNs (with stationary nodes), and VANETs (concerning mobile nodes), accordingly. As written in Sects. 3.2 and 3.3, there is still a need to provide more realistic models of failures that would make the respective measures of wireless networks reliability more adequate.

3.2 Reliability of wireless mesh networks

Wireless Mesh Networks (WMNs) are typically formed by stationary routers forwarding the traffic generated by mobile/stationary users [64,70,99]. They are considered by many as an important alternative to wired local, or metropolitan networks. By offering at each link the transmission rates of 1–10 Gb/s owing to high-frequency wireless communications (e.g., utilizing the 71–86 GHz band [81]), and having a relatively low cost of deployment, WMNs gain a remarkable advantage over wired networks. This is especially important e.g., in dense rural areas, or other difficult locations including lakeland, upland, or mountain regions.

WMNs are also an important alternative to 3G (4G) operators not having their own wired network infrastructure. For them, WMNs seem to be one of few solutions to prevent from leasing the capacity from other network providers.

However, high-frequency wireless communications, apart from offering high-speed transmission capability in error-free scenarios, brings about significant efficiency problems under severe conditions. This especially refers to WMN links being very susceptible to weather disruptions. In particular, heavy rain falls often cause remarkable signal attenuation. As a result, effective capacity of a link may be partially, or even fully degraded. On the end-to-end transmission level, serious instability problems (e.g., route flapping) can be observed.

As stated in [72], since WMNs are formed by stationary nodes and do not encounter noticeable contention problems (if using highly directional antennas), they seem to have similar characteristics to wired networks, with the only clear exception being the link stability.

When modeling failures in WMNs, it seems reasonable to use the general idea of a region failure model. However, it is not proper to assume the circular representation of failure regions, since such areas (implied e.g., by location of heavy rain fall) can be of any form.

The real shape of regions of signal attenuation due to rain falls can be obtained e.g., by utilizing information from radar echo measurements. Such an idea was originally proposed by authors of [72], who suggested to apply periodic updates of routing algorithm characteristics based on predictions concerning future conditions of wireless mesh links. In particular, in [72], they introduced two algorithms (XL-OSPF and P-WARP) being extensions to Open Shortest Path First (OSPF) taking into consideration changing weather conditions. Both algorithms utilize formulas (1) and (2) from [36] defining the dependency of signal attenuation on the rain rate:

$$A(R_p, D) = \alpha R_p^{\beta}\left[\frac{e^{u\beta d}-1}{u\beta} - \frac{b^{\beta}e^{c\beta d}}{c\beta} + \frac{b^{\beta}e^{c\beta D}}{c\beta}\right] \quad (1)$$

$$d \le D \le 22.5\,\text{km}$$

$$A(R_p, D) = \alpha R_p^{\beta}\left[\frac{e^{u\beta D}-1}{u\beta}\right]; \quad 0 \le D \le d \quad (2)$$

where:

- A is the signal attenuation in dB,
- D is the length of the path over which the rain is observed,
- R_p is the rain rate in mm/h,
- α, β are the numerical constants taken from [36],
- $u = \frac{ln(be^{cd})}{d}$,
- $b = 2.3R_p^{-0.17}$
- $c = 0.026 - 0.03lnR_p$,
- $d = 3.8 - 0.6lnR_p$.

In particular, XL-OSPF introduces the link cost metric proportional to the observed bit error rate (BER) of the link. Unlike in XL-OSPF, link costs in P-WARP algorithm are estimated using weather-radar information to predict the future condition of links.

Both algorithms from [72] require modifications of routing algorithms, which may limit their applicability in practice. In order to avoid such difficulties, the author of [116] proposed to improve the WMN performance in the heavy rain scenario by means of applying the periodic updates of the network topology based on radar rain predictions. This proposal does not imply any updates to routing algorithms. Instead, as shown in Fig. 7, owing to dynamic antenna alignment features, some links have to be periodically created/deleted, if low/high level of signal attenuation is forecasted for them, accordingly.

Based on observations and results from [72–74,116], we may say that weather-based disruptions in Wireless Mesh Network is certainly a promising area for future research.

3.3 Reliability of VANET communications

Owing to the need to improve the public road safety, in recent years we have been observing a growing interest in inter-

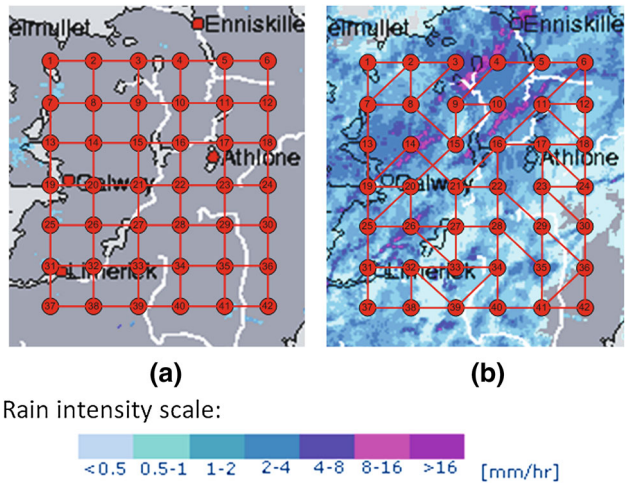


Fig. 7 Example topology of a WMNs **a** before, and **b** after applying the updates according to the proposal from [116]

vehicle wireless communication systems deployment. Apart from road safety issues (including accident warnings, lane change, or passing assistance, vehicle remote diagnosis, road warnings against low bridges, ice/oil on road), inter-vehicle communications (IVC) [51,70,149] may soon become an important solution for a large group of other problems related e.g., to traffic coordination issues, impact of transportation on environment (traffic light scheduling to reduce the travel time as well as environmental pollution), or travellers information support/infotainment [63,79,126]. However, some of these services (e.g., collision warning) require real-time communications. In such cases, messages arriving too late are no longer useful.

It is worth noting that IVC does not require utilization of a roadside infrastructure. In particular, VANETs are considered to be ad-hoc networks with multihop inter-vehicle communications (MIVC). The respective IEEE 802.11p and 1609 IVC standards have been recently ratified in the US, but in Europe they are still under preparation.

Compared to WMNs, reliability of VANET communications is harder to achieve owing to high mobility of nodes. Recent approaches from the literature to improve IVC communications include e.g., proposals to improve stability of links by utilizing information on vehicles mobility such as direction and velocity [104]. However, due to high mobility of vehicles, even if such features are included in the routing algorithm, the time needed to install the path is often still greater than the lifetime of a multi-hop path [18].

Multipath routing algorithms [69] transmitting information via several (frequently mutually disjoint) end-to-end paths certainly offer better fault tolerance. However, a failure of all alternate paths in VANETs is very probable. To overcome the above problems, the author of [115] proposed a new class-based multipath routing algorithm being extension to AODV routing approach. Unlike other approaches, this algorithm starts the process of finding a new alternate path immediately after detecting a failure of one of transmission paths between a given pair of end-nodes (other approaches start this process only after detecting failure of all alternate paths of a demand). A special metric is additionally introduced to improve the stability of each link.

Although being convincing, proposals from [18,23,69,104,115] can be seen as preliminary ones, and further research in this area seems to be necessary.

4 Robust optimization and network design

In the last decades, mathematical optimization has become an inevitable part of the planning process of communication networks. Graphs and algorithms play a vital role in modern communication networks. Without the mathematical theory and algorithms developed by researchers from discrete mathematics, algorithmics, mathematical optimization, and distributed computing, many services of the information society like (mobile) telephony, virtual private networks, broadband at home, wireless Internet access, and Phone over IP are unthinkable in their current form. At the heart of each of these are Integer Linear Programming (ILP) formulations to specify the planning task, and last but not least obtain cost-efficient solutions by use of ILP solvers.

Existing mathematical methods for network planning require a deterministic model of the problem at hand. Many factors in real applications are, however, non-deterministic. For example, the traffic volumes between nodes in a backbone network fluctuate heavily over time (see Fig. 8). Recently, robust optimization is a trendy topic for mathematicians. Where stochastic optimization [123] focuses on optimizing the expected objective value, robust optimization aims to find a solution that optimizes the worst case considered (to be specified below). In this contribution, we promote

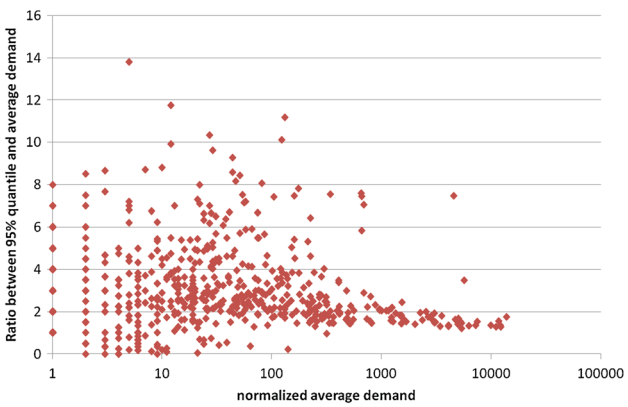


Fig. 8 Fluctuation in demands for all node pairs in a 50-node German backbone network

the adaption of this innovative methodology for the modeling and design of communication networks. First, we introduce the robust optimization approach, and afterwards, discuss its potential for telecommunication systems by the example of robust network design.

4.1 Robust optimization

A deterministic linear optimization problem can be written as $\max\{c^t x : Ax \leq b, x \geq 0\}$, where x is a vector of n variables, c the coefficients of the objective, and $Ax \leq b$ a system of m linear inequalities defining the constraints. In many optimization problems, the coefficients of c, A, and/or b are not deterministic, i.e., not known in advance. Hence, these values should be seen as random variables. Optimizing with, for example, expected values in c, A, and/or b may have two undesired side effects:

- the computed optimal solution x^* is not longer optimal (given the actual values of c), and
- the solution x^* is not valid for the actual values of A and b.

Assuming w.l.o.g. that the objective coefficients are certain, this issue can be addressed by solving a chance-constrained model instead:

$$\min c^t x \tag{3}$$

$$\text{s.t.} \mathcal{P}\left(A_i x \leq b_i\right) \geq 1 - \varepsilon_i \qquad \forall i = 1, \ldots, m \tag{4}$$

$$x \geq 0 \tag{5}$$

where A_i is the ith row of matrix A, b_i the ith component of vector b, and $\varepsilon_i > 0$ a small constant defining the probability that constraint i is violated by the optimal solution. Thus, we are looking for a solution that satisfies all constraints with high probability. Bertsimas and Sim have shown in [14,15] that in case all random variables are independent and have a symmetric distribution of the form $a_{ij} \in [\bar{a}_{ij} - \hat{a}_{ij}, \bar{a}_{ij} + \hat{a}_{ij}]$ (with $\bar{a}_{ij}$ the average and $\hat{a}_{ij}$ the maximum deviation), the chance-constrained model for a given ε can be solved by the defining an appropriate integer Γ and solving the following linear optimization problem:

$$\min c^t x \tag{6}$$

$$\text{s.t.} \sum_{j=1}^{n} \bar{a}_{ij} x_j + \max_{J \subseteq \{1,\ldots,n\}: \atop |J| \leq \Gamma} \sum_{j \in J} \hat{a}_{ij} x_j \leq b_i \quad \forall i = 1, \ldots, m \tag{7}$$

$$x \geq 0 \tag{8}$$

Thus, every linear inequality is extended with a term containing Γ largest deviations (of the product $\hat{a}_{ij} x_j$). This maximum causes the inequality being not linear anymore. It can be either linearized by defining a linear inequality for every subset of Γ elements of $\{1, \ldots, n\}$ (yielding an exponential number of inequalities), or by linear programming duality, see below. The level of robustness can be adjusted by varying the parameter Γ, the higher the value, the more robust the solution will be.

4.2 Robust network design

To show the potential of the mentioned approach, we describe its application for the classical network design problem, which is at the base of many technology-specific network planning problems. The so-called Γ-Robust Network Design Problem has been studied in detail in a series of papers by Koster et al., i.e., in [88–90]. The following description has been merely taken from Koster and Kutschka [87].

The *Γ-Robust Network Design Problem* can be described as follows. Let $G = (V, E)$ be an undirected graph representing the network topology. Let capacity be installable in batches of $C > 0$ on each of the links $e \in E$ with cost κ_e per batch. For every commodity k in a set K of point-to-point demands, a routing has to be defined from source $s^k \in V$ to target $t^k \in V$ such that the traffic volume d^k can be accommodated. The traffic volume d^k is uncertain with an unknown distribution but its realization is assumed to be in the interval $[0, \bar{d}^k + \hat{d}^k]$ where $\bar{d}^k$ denotes a default and $\hat{d}^k$ a deviation value for commodity $k \in K$. In addition, it is assumed that only $\Gamma \in \{0, 1, \ldots, |K|\}$ many demands deviate from their default values simultaneously. In worst case, the deviation equals $\hat{d}^k$.

The Γ-Robust Network Design Problem is to find a minimum cost installation of capacities such that a *routing template* exists which does not exceed the link capacities, if at most Γ commodities deviate from their default values simultaneously. A routing template is a set of multiple paths from s^k to t^k used according to a percentaged distribution of the flow.

Now, let x_e be the decision variable determining the number of batches (modules) installed on edge (link) $e \in E$. Let f_e^k be the decision variable determining the fraction of the (multi-)commodity flow of commodity $k \in K$ assigned to edge (link) $e \in E$. The capacity constraint for a link $e \in E$ now reads like in the general case:

$$\sum_{k \in K} \bar{d}^k f_e^k + \max_{Q \subseteq K, |Q| \leq \Gamma} \sum_{k \in Q} \hat{d}^k f_e^k \leq C x_e \tag{9}$$

Given a fixed flow f_e^k the maximum can be determined by an auxiliary integer program:

$$\max \sum_{k \in K} \hat{d}^k f_e^k z_e^k \tag{10}$$

$$\text{s.t.} \sum_{k \in K} z_e^k \leq \Gamma \tag{11}$$

$$z_e^k \in \{0, 1\} \tag{12}$$

Since the linear relaxation of this integer program is integral, the dual linear program is equivalent to it. In the dual, we have one variable π_e for the constraint that at most Γ many demands can be selected, and variables ρ_e^k for the inequalities $z_e^k \leq 1$ in the LP relaxation. Plugging this dual LP in the capacity constraint results in the following mixed integer programming formulation for Γ-robust network design:

$$\min \sum_{e \in E} \kappa_e x_e \tag{13}$$

$$\text{s.t.} \sum_{\substack{j \in V: \\ ij \in E}} (f_{ij}^k - f_{ji}^k) = \begin{cases} 1 & i = s^k \\ -1 & i = t^k \\ 0 & \text{otherwise} \end{cases} \quad \begin{matrix} \forall i \in V, \\ k \in K \end{matrix} \tag{14}$$

$$\Gamma \pi_e + \sum_{k \in K} \bar{d}^k f_e^k + \sum_{k \in K} \rho_e^k \leq C x_e \qquad \forall e \in E \tag{15}$$

$$\hat{d}^k f_e^k \leq \pi_e + \rho_e^k \qquad \begin{matrix} \forall e \in E, \\ k \in K \end{matrix} \tag{16}$$

$$f_e^k, x_e, \pi_e, \rho_e^k \geq 0 \tag{17}$$

$$x_e \in \mathbb{Z}^{|E|} \tag{18}$$

The objective (13) is to minimize the costs inflicted by installing capacities on links. For every node and commodity, the flow conservation is guaranteed by constraint (14). In contrast to the classical link capacity constraint, the Γ-robust capacity constraint (15) includes the dual variables π_e and ρ_e^k. The dual variables are connected to the deviation demand values $\hat{d}^k$ in Constraint (16). This constraint results from linear programming duality theory and is necessary to determine the correct bandwidth requirement in constraint (15). Constraints (17) and (18) are the nonnegativity respective integrality constraints.

Solving (13–18) results in a solution with optimal cost value depending on the value Γ. The *price of robustness* [15] measures the relative increase of the optimal cost value compared to $\Gamma = 0$. As the name suggests, robustness comes at a price, compared to a solution based on average values. In practice, however, network planners would calculate with far more conservative values than the average traffic volumes in order to guarantee robust networks. Therefore, it would be fairer to compare with $\Gamma = \infty$, i.e., the case where the network is designed for $\bar{d}^k + \hat{d}^k$ instead of $\bar{d}^k$. Figure 9 shows the results for four test instances and different values of Γ (see [90] for more details). For $\Gamma = 5$ about 10 % of the cost can be saved for all considered network instances. An analysis of the actual robustness (i.e., for actually observed traffic matrices) of the designs produced by this approach revealed that best possible values are already (almost) achieved for $\Gamma = 5$.

4.3 Further remarks

The above discussion is just one example of a problem where robust optimization can improve current practice. The robust approach of Bertsimas and Sim from [15] can be applied in many more cases, including the real optimization of future communication systems. Two examples are given in [12] by Belotti et al. and in [44] by Duhovniko et al., but many more applications are possible.

One drawback of robust optimization compared to traditional deterministic optimization is the increasing size of the integer linear programs to be solved. Every uncertain constraint requires extra variables and constraints. Fortunately, these are continuous variables instead of discrete variables. In some cases it may be beneficial to avoid these extra variables by separating the exponentially-sized set of constraints resulting from a straightforward linearization (see Fischetti and Monaci [48]) or to project the polyhedron to a subspace of the original variables (see the work of Claßen et al. [28]). In addition, the derivation of additional valid inequalities can be considered (see Koster et al. [90]).

Robust optimization as it is presented in this contribution is conceptually a one stage optimization problem: a single solution is found for all considered scenarios. In network design, for example, it might be possible to adapt the flow according to the actual traffic volumes, but the capacity installation has to be carried out in advance. In such a case a two stage approach would be more beneficial. Ben-Ameur [13] and Poss and Raack [112] describe such robust approaches yielding a routing that is neither static nor completely dynamic. An alternative concept is *recoverable robustness* [93] where limited changes towards the actual values are allowed. This concept has only be applied so far towards classical combinatorial optimization problems like shortest path [20] and knapsack [21,22].

5 Multilevel and multirealm network challenges and resilience

Real communication networks are complex multilevel graphs [62,101,132]. Understanding the resilience properties of the network requires modelling this complex structure *as a whole* such that challenges can be applied to model the impact on user services. Resilience is the ability of the network to provide and maintain service in the face of challenges to the network [133]. *Resilience* subsumes survivability (tolerance of correlated failures from large-scale disasters and attacks), disruption tolerance (for weakly connected channels, mobil-

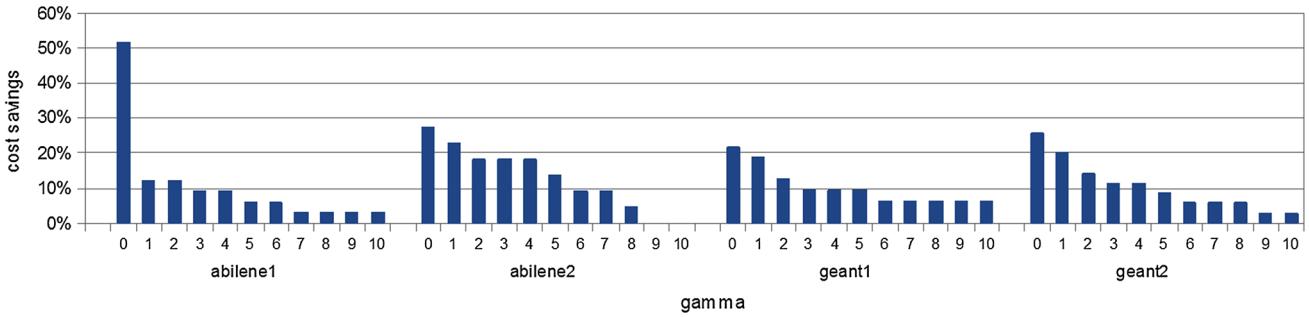


Fig. 9 Cost savings of robust ABILENE and GÉANT network design compared to classical network design with peak demand values (i.e., corresponding to Γ-Robust Network Design with $\Gamma = |K|$)

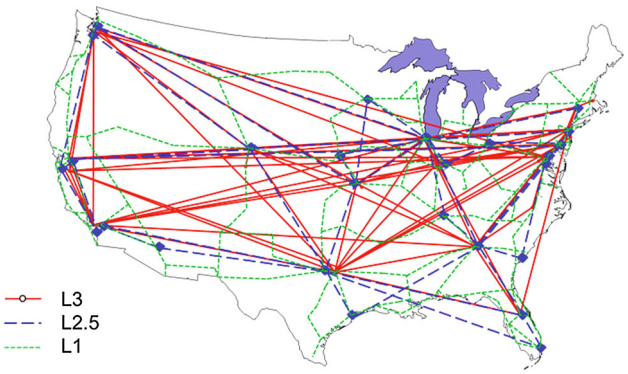


Fig. 10 Multilevel ISP network

ity, unpredictable delay, and energy constraints), dependability (including reliability and availability), and performability (that measures degraded performance of a complex system when some of its subsystems fail).

5.1 Multilevel network structure

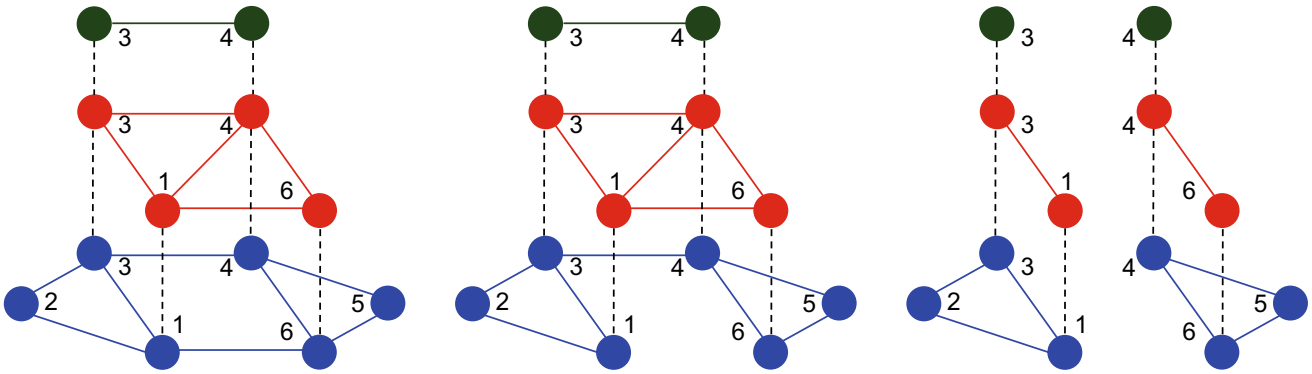
From an operational and protocol point of view, networks can be represented by a multilevel graph, as shown in Fig. 10; this example is for the US Sprint service provider [91]. The lowest level L1 consists of the physical *infrastructure* in which the graph edges are fiber, copper, or wireless links, and the vertices are switches, cross-connects, or multiplexors. This level is grid-like in its topology and degree distribution. Each level up is a graph that consists of a subset of the vertices and an arbitrary edge set. For example, the router topology L3 consists of vertices that are IP routers at some of the physical infrastructure nodes, and a set of IP virtual links between the routers. This level is a mesh-like overlay on the grid-like underlay. There may be a virtual link level L2.5 in-between for traffic engineering using MPLS. These three levels are shown for the Sprint network in Fig. 10. Above this, the end-to-end transport graph represents all transport flows, and application level and social-network level flows can be constructed.

Traditional Internet analysis has largely been conducted on the IP (layer 3) graph (e.g., [3]). However, an understanding of resilience (including survivability and dependability) requires multilevel representation and modelling, in which failures and challenges are applied to the proper level, with the impact on service measured at the proper level above. For example, a large-scale disaster or terrorist attack must be modelled as failures at the physical infrastructure level, with the vertex and edge deletions propagated upward to the IP level and further to the application level to understand the impact on service to the user. Similarly, a malware attack against the IP infrastructure needs to be modelled as failures in the network level graph [26].

This can be analytically modelled as a *multilevel graph* [27], as shown in Fig. 11a consisting of multiple graphs, one for each level, arranged such that for any pair of levels, the set of all nodes in the higher level is a subset of the set of all nodes in the lower level, and such that nodes that are not connected in a lower level are not connected in a higher level. Thus when a link is removed at the bottom (typically physical) level, this does not impact the connectivity of the higher level graphs if dynamic routing is utilised as shown in Fig. 11b. However, as shown in Fig. 11c, the removal of links (1, 6) and (3, 4) in the lowest level partitions the graph and necessitates their removal in the above levels as well. Thus we can model the impact of challenges to the physical infrastructure on higher-level services by understanding the resilience properties induced on the higher level graph that delivers these services.

5.2 Multirealm network structure

The multilevel graph described in the last subsection would be accurate if there were only one service provider. In reality, the Internet is composed of many service providers interconnected as an AS (autonomous system) graph. While AS graphs have been modelled (e.g., [47]), this interconnection is more complex when viewed as a level above the router graph. Each AS vertex is a single multilevel service-provider graph, but the peering interconnection consists of links between



(a) Connected multilevel network **(b)** Disconnected multilevel network **(c)** Partitioned multilevel network

Fig. 11 Multilevel graph example

the edge routers of each AS, as shown in the top two levels of Fig. 12. We refer to any policy, trust, or mechanism boundary, as a realm [17]. This includes, but is not limited to AS boundaries. Thus, the modeling of the interrealm graph consists not only of the realm-graph adjacency matrix, but also of the specific peering edges between the multilevel provider graphs. This significantly increases the complexity of modelling Future Internet resilience, but is necessary to adequately capture the complexity of the modern Internet.

We can then extend the multilevel analytical graph model described in the last subsection to a multirealm graph model. This is done by first constructing the multirealm graph of providers (or autonomous systems—AS). In this graph, each vertex corresponds to a multilevel provider graph. This provides the adjacency of the provider graphs, but we additionally need to capture the peering points. Thus, the peering vertices (corresponding to border routers) in the top level of each provider graph are the neighbours of the interprovider edges that connect them.

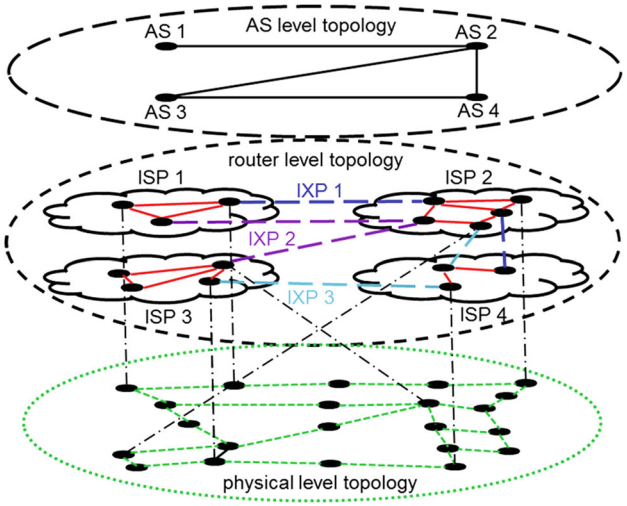


Fig. 12 Multirealm multilevel topology

5.3 Challenge taxonomy and modelling

Given a network topology graph, its resilience can only be predicted by applying a challenge and measuring its robustness, either analytically, through simulation, or experimentation on a large-scale testbed [131]. This requires a threat model and an understanding of potential challenges that could disrupt the network.

A key part of this understanding is to develop a rigorous taxonomy of challenges [25], along the lines of fault [17] and survivability [131] taxonomies. This section briefly introduces the ResiliNets challenge taxonomy.

Challenges can be categorized in 11 dimensions, some of which have sub-categories.

- **cause** is natural (terrestrial, meteorological, cosmological), human-made (social, political, business and economical, or terrorism), or based on a dependency (independent infrastructure, lower-level failure, or cascading failure),
- **target** is either direct or collateral damage,
- **objective** is malicious, selfish, or non-malicious,
- **intent** is deliberate or non-deliberate,
- **capability** is accidental or due to incompetence,
- **dimension** is hardware, software, protocols, or traffic,
- **domain** is wired or wireless,
- **scope** is nodes, links, or area (fixed or evolving),
- **significance** is catastrophic, major, or minor,
- **persistence** is long-lived, short-lived, or transient,
- **repetition** is single, multiple, or adaptive.

As an example, a large-scale blackout impacting the network can be classified as, cause: interdependent infrastructure, target: collateral, objective: non-malicious, intent: non-deliberate, capability: incompetence, dimension: hardware, domain: wired and wireless, scope: area, significance: major,

persistence: short-lived, repetition: single. The goal of this taxonomy is to classify past and potential challenges in each of these 11 dimensions to understand what resilience mechanisms should be deployed and how robust the network will be to these challenges.

This permits the construction of a challenge correlation table that categorises know past challenges, including attacks and large scale disasters in each of the 11 taxonomy dimensions. This can then be used to understand how the network is likely to respond to particular threats and help increase the resilience to these future challenges.

6 Multiple-criteria routing approaches in multilayer networks—highlights of issues and challenges

Routing between two end points in a network requires finding a path between those end points satisfying certain quality of service (QoS) related constraints, and usually seeking to optimize some metrics. It is advantageous that routing methods in modern telecommunication networks may take into account multiple, often conflicting objectives related to Quality of Service (QoS) or cost/revenue metrics. A recent example can be found in [146] where results show that there is a tradeoff between power minimization and blocking probability. The authors of [146] propose a weighted power-aware lightpath routing (WPA-LR) approach where a parameter $\alpha \in [0, 1]$ is used such that if α is equal to 0, WPA-LR becomes a pure power minimization approach, while for values of close to 1 WPA-LR will provision connection requests favoring shorter routes. They evaluate the power consumption and blocking, for increasing traffic load and different selected values of α. In our view, the resolution of this type of routing problem could greatly benefit from a bi-criteria approach.

6.1 Multiple-criteria approaches

Single objective approaches, which seek the optimization of one metric/function alone while other metrics are usually represented as constraints, have inherent limitations. Hence there are potential advantages in the development of explicit multiple-criteria models (that is models where one seeks the simultaneous optimization of several metrics/objective functions) for dealing with various routing problems.

In fact, multiple criteria models enable an explicit representation and mathematically consistent treatment of the trade-off among the different metrics, taken as objective functions considered as conflicting criteria. Note that in models involving explicitly multiple and conflicting criteria, the concept of optimal solution (that is usually infeasible), is replaced by the concept of non-dominated solutions. A non-dominated solution is a feasible solution such that no improvement in any criterion is possible without sacrificing at least one of the other criteria. The aim of a multiple criteria optimization model is, in general, the calculation of non-dominated solutions and the selection of one of them, considered as a "good" compromise solution for the specific problem under analysis. A state of art review of multiple criteria models in telecommunication network design, namely routing models is in the book chapter [30]. An overview on multiple criteria routing models in telecommunication networks with a case study is in [31]. Key methodological and modeling issues in this area and a meta-model for hierarchical multiple criteria network-wide routing optimization in multiprotocol label switching (MPLS) networks are discussed in [37] while a proposal of a systematic conceptual framework for multiple criteria routing in QoS-IP networks, is given in [147]. Also in [147] diverse aspects of multiple-criteria routing in QoS IP networks to be taken into account in future developments of network engineering, are discussed.

Routing algorithms are often based on shortest path routing, assigning a length (or cost) to each network link, and then finding the shortest length paths (where weights may also be considered for each link in each candidate path [147]). Non-dominated solutions (paths) can be calculated by optimizing a scalar function which is a convex combination of the considered n objective functions. After transforming the multiple criteria problem into the weighted-sum scalar problem, only non-dominated supported solutions can be computed. These are the solutions belonging to the boundary of the convex hull of the non-dominated solution set in the n-dimensional objective function space [134]. This is illustrated in Fig. 13, where solutions 1, 2, 3 and 4 are supported non-dominated solutions and the duality gaps are marked in gray, where the unsupported solutions 5, 6, 7, 8 and 9 are marked. In [34] an interactive bi-objective shortest path approach is proposed for searching for unsupported non-dominated solutions and in [29] a reference point approach to determine unsupported non-dominated solutions in multiple criteria integer linear programming is proposed.

In [50] a bicriteria model for calculating topological paths, corresponding to supported and unsupported non-dominated solutions, is described; after the selection of the topological path, wavelengths are assigned to the links, completely defining the lightpath. This model was extended in [127], for considering dedicated path protection.

6.2 Multilayer networks

There has been an effort to reduce the number of intervening layers in order to simplify network operation and management of communication networks. This resulted in the IP over WDM architecture, enabled by an optical transport network. However this simplification raised new challenges, namely regarding multi-vendor compatibility, as well as the complexity of requiring network resiliency at the optical layer.

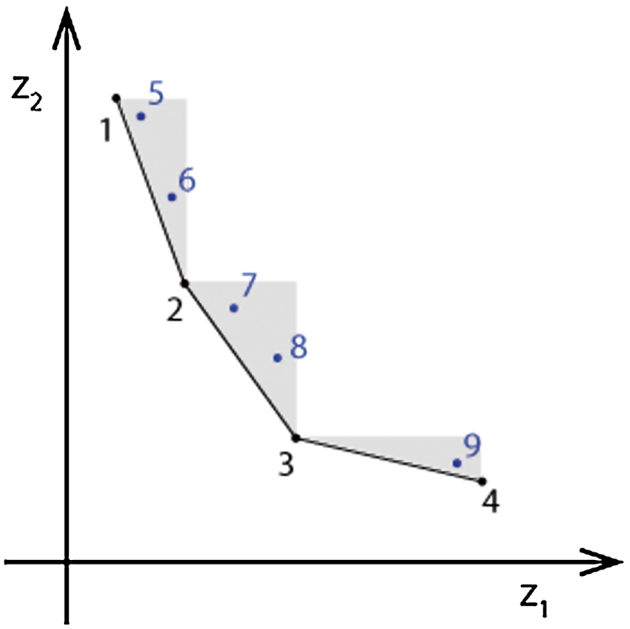


Fig. 13 Two objective functions z_1 and z_2, supported and unsupported non-dominated solutions

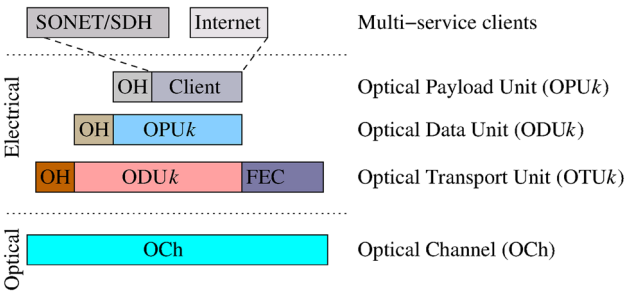


Fig. 14 Building an OTN container

The Optical Transport Network (OTN) was initially developed by the ITU-T as the core transport for SDH, and later extended to support Ethernet and IP [71]. The OTN supports the transport of diverse client signals, is agnostic to client signal types, capable of efficiently transporting variable bandwidth granularities, and incorporates forward error correction (FEC) which significantly increases the distance transmission without the need for the 3R (re-amplification, re-shaping, re-timing). In OTN, at the digital layer, the client traffic flows are mapped into optical data units (ODUs). The ODUs are then mapped into an optical transport unit (OTU) where the FEC is added and the signal is ready to be carried in an optical channel (OCh)—see Fig. 14. The granularity of the multiplexing hierarchy defined by ODUk is 1.25 Gb/s, 2.5 GB/s, 10 Gb/s, 10.4 Gb/s, 40 Gb/s, 100 Gb/s, k = 0, 1, 2, 2e, 3, 4. A flexible container was also defined, designated ODUFLex, which was developed to accommodate signals of different speeds (variable and constant bit rates). Lower order ODUs can then be multiplexed in higher-order ODU (with higher rate), to allow a better use of the network bandwidth. This also allows sub-wavelength networking capabilities [59].

The OTN technology [71] is required by today's telecommunications, to cope with growths of bandwidth, and emerging services [148]. It has operations, administration, maintenance, and provisioning (OAM&P) capabilities per wavelength [59], which were missing in previous transport technologies. The flexibility of the WDM layer was improved with the introduction of reconfigurable optical add-drop multiplexers (ROADM). ROADM is a device which allows optical signals (assigned to wavelengths) to be added, dropped or bypassed (switched) in a reconfigurable manner.

Multiprotocol label switching [8,120] is used in IP networks to create tunnels—label switched paths (LSPs)—and ensure QoS for traffic flows. MPLS fast reroute ensures very fast service recovery [109]. Recently MPLS Transport Profile (MPLS-TP) [106] has been proposed, which is simultaneously a subset and an extension of MPLS. The objectives of MPLS-TP according to [19] are to enable MPLS to be deployed in a transport network and to be operated in a similar manner to existing transport technologies and also to enable MPLS support of packet transport services with a similar degree of predictability to that found in existing transport networks. MPLS-TP has the efficiency of MPLS and the reliability and OAM capabilities of existing transport networks.

In the IP/MPLS over WDM model, wavelengths can be routed and switched between the source and destination points, using all-optical ROADMS, thence achieving the features of a full dynamic wavelength routed network.

In the IP-over-OTN-over-WDM model, the OTN switching capability is exploited in order to bypass many of the IP layer routers, thus reducing the amount of router capacity (and power consumption). It also allows traffic grooming at sub-wavelength level, which results in a more efficient bandwidth utilization. The network architecture may also be IP/MPLS-over-MPLS-TP-over-OTN-over-WDM, in order to further improve the efficiency of bandwidth utilization, through a higher level of traffic grooming. The MPSL-TP switch is capable of identifying the LSPs carried in the ODUs, and will be capable of switching them for a better use of the ODUs bandwidth, resulting in network with better bandwidth performance. In [80] an optimization design model for protection in IP/MPLS-over-OTN-over-WDM networks is presented, which takes into account the technological constraints in each layer.

The use of MPLS-TP combined with OTN is expected to save capital expenditure (CAPEX) and lower operational expenditure (OPEX) [107]: at the IP/MPLS layer it saves CAPEX by requiring less router hardware and lowers OPEX by reducing power consumption; at the DWDM layer it reduces the need for new wavelengths (and fibers) due to sub-lambda grooming. However, the cost of a node equipped with

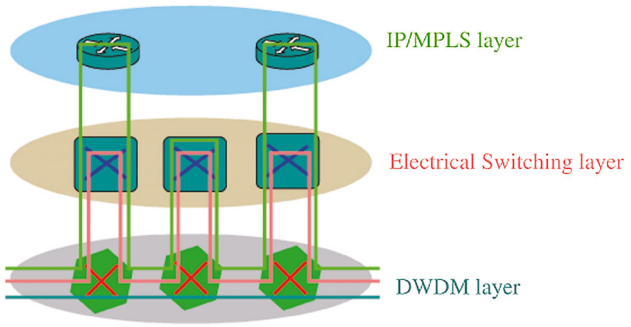


Fig. 15 Incorporating MPLS-TP in the tranport layer [107]

MPLS-TP is higher. Hence the introduction of MPLS-TP requires a careful evaluation at an economic level and routing (with protection) optimization to ensure that the potential advantages of MPLS-TP are fully exploited. Figure 15 illustrates that the deployment of MPLS-TP within the OTN switch, allows intermediate sites to have reduced or no router traffic [107].

The cost of packet layer topologies and the advantage of OTN switching are analyzed in [46]. In [40] a study was carried out comparing three scenarios for WDM and switching architectures, with 100 Gb/s technology. The authors concluded that the introduction of OTN switching increases wavelength efficiency and enables the deployment of fewer 100 Gb/s wavelengths. Morover, although MPLS-TP was not considered, as the cost of introducing this layer is mainly related to a new software function in the OTN nodes [107], these results seem to indicate that incorporating MPLS-TP, while adding an extra layer to the network architecture, is likely to be a promising approach.

6.3 Multiple criteria models in multilayer networks

Routing optimization using multiple-criteria approaches is especially interesting in the network management plane, as part of a decision support system. A multiple-criteria optimization model for routing with protection, could make it clear the trade-offs among various instances/metrics resulting from the different routing and protection options in each layer. The non-dominated solutions (the whole set or a selected sub-set) obtained at a lower layer could then be ranked or filtered at the next upper layer.

The applicability of a multiple-criteria approach for routing with protection in multilayer networks will depend, among other factors, on the required time response. A multiple-criteria approach for routing with protection in an IP/MPLS over MPLS-TP over OTN over DWDM, could involve the following issues:

- formulating a multiple-criteria routing model and solving the associated multiple criteria optimization problem at the WDM layer. For example, the use of an energy-aware routing with protection, seeking to minimize power consumption and global blocking [146], while complying with Quality of Transmission. The solution of multiple-criteria optimization for this problem would be a set of non-dominated virtual lightpaths,
- with MPLS-TP over OTN, for each virtual lightpath topology option from the first step, there will be different routing (at transport level) and sub-wavelength grooming possibilities. The resolution of the resulting decision problem at this layer could also benefit from a multiple-criteria approach.

A challenging issue in this area is to explore the development of hierarchical multiple criteria routing models integrating, in an articulated manner the type of problems addressed in the previous points. Conceptual analysis and methodological proposals on hierarchical models in the context of multiple criteria routing approaches in MPLS and QoS IP networks can be found in [37,147].

We believe that this is an area where both from a methodological and application perspectives interesting challenges lay ahead, taking into account on the one hand the great complexity of problem involved and on the other hand the possible impacts in terms of network performance/cost improvements.

7 Resilience considerations of an IP backbone network in the interplay with an agile optical layer

Multi-layer (ML) networking is already discussed for many years now. However, despite of a huge amount of publications it has not been widely deployed in real networks. However, recently it gains more and more attention in the communications industry due to newly achieved feasibility of connected with the expectations of further cost reduction and superior network performance.

7.1 General technology trend in the communications industry: cost reduction by multi-layer optimization within real network implementations

Picking up the general technology trend, we recommend the following guidelines for future research directions with high practical relevance:

- *consider real, practically operated networks*
  In addition to artificial networks′ topologies derived by software generation it is also recommendable to concentrate on real networks. For example, Deutsche Telekom (DT) is willing to share a reasonable topology for its future national router network. A generic end-to-end traf-

fic profile can also be provided together with typical failure probabilities for, e.g., a cut of fiber pair per km.

– *do cost-aware resilience research*
Generally, reliability and availability modeling should always take cost issues into account. This does not necessarily mean that any work not directly dealing with economics is out of scope. Indeed, conceptually work and new ideas are highly appreciated. But it is always mandatory having economics issues in mind in order to achieve a competitive cost scaling of any new resilience scheme. A recent collaborative capital expenditure model was accepted for near-term publication [119].

This detailed model is a key requirement to evaluate multilayer metro and core network architectures and their resilience approaches. It is based on IP/MPLS, MPLS-TP, OTN and WDM technology and was developed by researchers from system vendors and network operators within the framework of the European FP7 project STRONGEST [66]. Besides current equipment and corresponding prices for the different layers L0 to L3, it also contains predictions for technology evolution and pricing until 2018.

– *consider multilayer architectures*
Traditionally, there has been competition between different departments at all operators. Recently this has changed. Indeed, previously competing departments have been merged for good reasons. Closer integration of packet and optical transport network layers helps network operators to reduce both, capital and operational expenditures. Therefore, it is now the right time to reconsider previous multilayer concepts under current technology capabilities and updated cost structures. There has not been a full coverage of studies on resiliency option for ML optimized networks. Presumably, there is now enough room for accordingly updated multilayer architectures, latest interworking options, and further improved resilience schemes.

7.2 Upcoming topics to be considered in detail

– **IP-over-Optics** The direct interworking of the router layer and the optical transport layer beneath is usually called as IP-over-Optics or IP-over-DWDM, basically both meaning the same. It offers the opportunity for a smarter multilayer resilience scheme overcoming the traditional over-dimensioning of packet networks. In this sense, reliability-aware ML network design and optimization is the key enabler for huge overall cost savings as has been demonstrated recently [60]. The cost saving potential stems from the reduced number of line interfaces enabled by a higher interface utilization. A new service-differentiated multilayer resilience scheme combines traditional IP protection for high-priority traffic with optical restoration for the best-effort share of the total traffic. Today, this low-priority traffic dominates the entire traffic volume.

All key technological ingredients are available today: first, flexible optical transmission at 100G with coherent reception technology being much more flexible and allowing a more dynamic mode of service provisioning and operation, second, a ML GMPLS control plane aware of topological modification on the optical layer, e.g., in reaction to a fiber failure. Especially, the control plane interworking must be aware of shared risk groups unintentionally induced by optical rerouting.

While all this is comparably mature today and even field tests are on the way serving as a proof-of-concept, some key technological questions are still unsolved. For example, how the optimum topology looks like, i.e., whether or not the two associated WDM rails should be interconnected (see Fig. 16 for more details). Furthermore, the detailed interworking of the control planes on the router and optical layer side is to be addressed. Finally, the overall network availability for all service classes needs to be carefully evaluated (Fig. 17).

– *Elastic Optical Networking*
A second hot research topic is the Elastic Optical Networking (EON). This research field is also known as flexgrid / flexreach / flexrate networking. The EON architecture is based on Bandwidth Variable Transponders

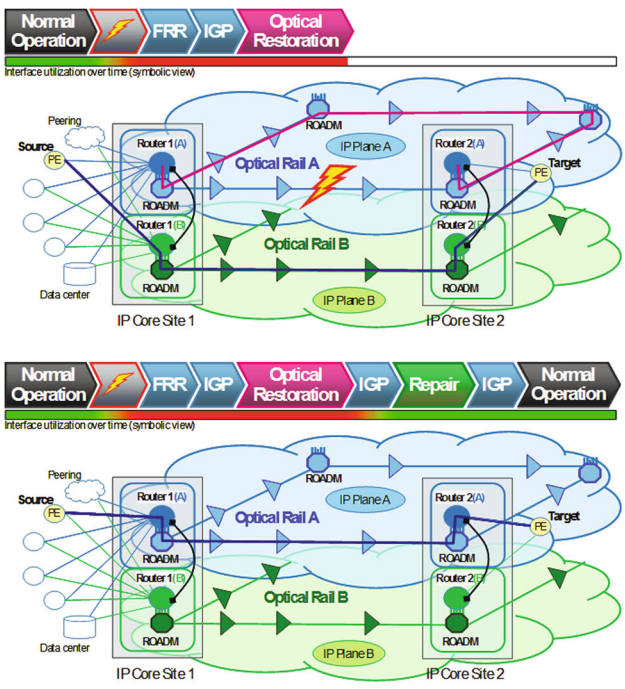


Fig. 16 Schematic of an IP-over-Optics network with A-/B-Plane design and how the optical restoration is embedded into a ML resilience scheme

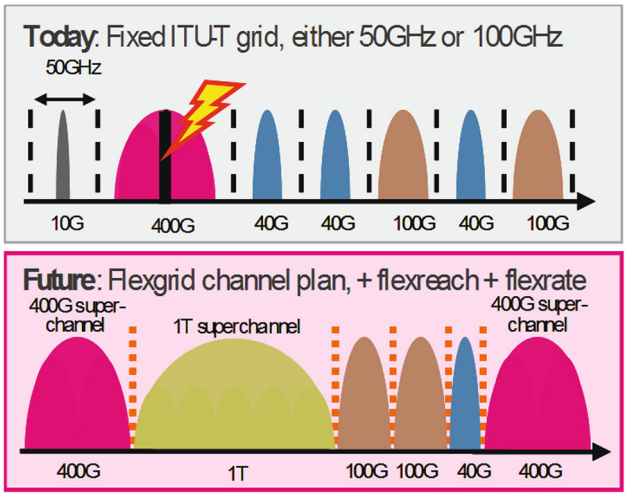


Fig. 17 A fundamental paradigm change is going on from static fixed-grid networking towards a fully flexible optical transport network incorporating flexible reach and flexible rate functionalities

(BVT), and flexgrid optical switching technologies, capable of fulfilling the requirements in terms of capacity and dynamicity of future core networks. This is required as traffic demand is increasing dramatically, year on year, with typical growth figures of between 30 and 60 % for Internet based traffic. Such traffic increase is impacting on both network costs and power consumption. Moreover, traffic is not only increasing but might also become more dynamic, both in time and direction. For these reasons, transport network evolution from current static DWDM systems towards elastic optical networks, based on flexgrid transmission and switching technologies, could significantly increase both transport network scalability and flexibility. Further benefits come again from multilayer interworking mechanisms enabling electronic switching technologies (IP/MPLS, OTN, etc) to directly control the BVTs for optical bandwidth optimization purposes.

Within a new European FP7 project named IDEALIST [67] this approach is evaluated both from a theoretical and conceptual view as well as from an industrial perspective emphasizing economic issues. EON feasibility studies and experimental implementation and demonstration of prototypes will be key project activities.

Besides the industrial focus of IDEALIST and also some early papers on *Routing-and-Spectrum Allocation* (RSA) Algorithms with Dedicated Path Protection [84], there is still a broad band of yet unsolved questions open concerning flexgrid-based resilience.

One of the anticipated early door-openers of commercial EON deployments is their superior flexible reaction capability to network failures. Today an optical interface needs to stay entirely out of service when its restored physical lightpath exceeds the maximum distance for the given fixed line rate. In the future EON framework, the line rate will be flexibly controlled. Therefore it might get realistic to reduce the line rate by modulation depth adaption such that the wavelength just covers the physical path. Of course, the original traffic throughput is reduced, but higher network layers like the IP layer might still take advantage of this type of ML resilience. This approach balancing reach against capacity needs to be thoroughly investigated. A study should cover both cases, a single optical layer, and a multilayer consideration, respectively. Many more resilience-related questions with a big impact on practical flexgrid networking are expected to enter the stage over time.

8 Cloud computing: new challenges for reliable networks design

Cloud computing seems to be an emerging and promising IT technology, especially attractive to business customers. This follows mainly from the fact that cloud computing can significantly reduce costs of deployment and provisioning of various IT services. The general idea behind the cloud computing is based on having large pools of computer systems sharing an IT infrastructure [68]. Gartner[1] defines cloud computing as *a style of computing where massively scalable IT-related capabilities are provided "as a service" using Internet technologies to multiple external customers*. Cloud computing emerged as a mature IT solution around 2007 and since that time the topic has exploded in huge attention within both industry and academia. In this section, we would like to briefly present the main aspects of cloud computing idea and examine how the advent of cloud computing impacts the research in the topic of reliable networks design [142,151].

8.1 Cloud computing

The most important factors in development of cloud computing are: "dot-com boom" which started an explosion of interest in outsourcing IT services; popularity, maturity and scalability of the Internet; appearance of large data-centres of commodity hardware developed by companies such as Google, Amazon and Microsoft [142]. In the literature, a large number of definitions related to cloud computing can be found. However, the most common elements recurring in most of the definitions are: network access and distributed computing resources. In recent years, these two elements have been gaining much attention in many areas of industry parallel to overwhelming popularity of Internet and growing need to process a huge amount of data. The concept of

[1] http://www.gartner.com.

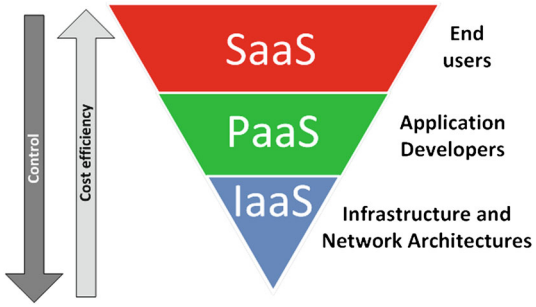


Fig. 18 Models of providing services in cloud computing

cloud computing combining both flexible network access and scalable distributed computing perfectly responses to a large number of business and research challenges.

There are three fundamental models of providing services in cloud computing [42,151] (Fig. 18):

- *Infrastructure as a service* (**IaaS**). In this model, a customer outsources from the provider the equipment used to support operations, including storage, hardware, servers, virtual machines and networking components. The provider is the owner of the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS include: Amazon EC2, Windows Azure Virtual Machines.
- *Platform as a service* (**PaaS**). In this model, a customer rents virtualized servers and associated services (e.g., operating system, programming language execution environment, database, web server) for running existing applications or developing and testing new ones. Examples include Google App Engine and Microsoft Windows Azure Compute.
- *Software as a service* (**SaaS**). In this model, applications are hosted by service providers and made available to customers over a network, typically the Internet [77]. The customers do not manage the cloud infrastructure and platform on which the application is running, what in a consequence reduces the requirement to install and run the application on the customer's own hardware simplifying maintenance and support. Examples include Google Apps and Microsoft Office 365.

The SaaS model seems to become an increasingly dominant model in parallel with development of technologies that support Web services and service-oriented architecture (SOA). Moreover, this model is the simplest one from business point of view.

The main advantages of cloud computing systems are [142,151]:

- cost and energy consumption reduction—development of dedicated data centers on one hand enables savings in CAPEX costs following from large scale of the systems and on the other hand deployment of specialized solutions shall reduce OPEX costs including energy expenditures,
- high scalability, as customers are provided with on demand resource that can be acquired without substantial investment costs,
- easy access, since services provided in the cloud model are mostly based on web solutions and are easily accessible through a variety of devices with the Internet connectivity,
- possibility to create new markets, particularly in areas like business intelligence with beforehand needed significant IT investment,
- reduced demand for skilled labor as IT skills shortages exist in many developed markets.

8.2 Cloud computing and networks

As pointed out above, the computer network is an indispensable element of the cloud computing model. Therefore, the unprecedented development of cloud computing triggers the need to make a critical review of currently used networks from the perspective of cloud computing needs. According to [33], current transport networks are not efficiently designed for requirements of cloud environments. First of all, existing networks are mostly focused on unicast (one-to-one) traffic, while different types of applications running on cloud computing systems lead to new traffic patterns including anycast (one-to-one-of-many) flows. Second, flexibility and scalability of cloud computing environments naturally implies dynamic changes of traffic demand, what may affect the traditional planning and dimensioning rules of network operators. Third, concentration of processing in relatively small number of sites (i.e., data centers) means that the volume of traffic on network links adjacent to these sites can become very large, thus network technologies supporting high capacity may be required.

To answer all these challenges, the authors of [33] propose an idea of a *cloud-ready* network that is prepared to support cloud computing services. The cloud-ready network is based on three technological concepts:

- flexible transport network, that can provide the required capacity on demand,
- multilayer oriented network management, that can handle the network traffic demand in an economical way,
- set of cross-strata capabilities, that can provide a combined optimization of both the computing resources and the network.

For a more comprehensive discussion on the topic a cloud-ready network refer to [33].

The authors of [2] mention that in some cases according to the needs of users such as on-demand availability with very small latency requirements, the cloud computing environment can use a *mist computing architecture*, i.e., cloud resources (computing and storage) are distributed in the network in more extent than in classical cloud model. Another motivation behind the misty model follows from the energy consumption limitations. Data centers and generally supercomputers grow very quickly, however in the near future the growth will probably slow down due to problems with providing sufficient energy supply.

According to [86], an exaflops-class supercomputer obtained by simply scaling Blue Waters up 100 times, would need 1.5 GW of power, what is more than 0.1 percent of the total U.S. power grid. The main consequences of the misty model from the network perspective is that resources are more scattered and thus additional effort should be made to provide effective allocation of these resources and optimization of corresponding network flows.

8.3 Cloud computing and reliable networks design

In this section, we present a discussion on the new directions in research on reliable networks design following from the emergence of cloud computing with a special focus on optimization aspects.

First, we center around the new traffic patterns generated by cloud and mist computing systems. As underlined above, anycasting defined as one-to-one-of-many transmission ideally fits to the traffic patterns generated by cloud computing systems, especially in the mist model. Anycasting, has recently become popular according to deployment of various network services, including Content Delivery Networks (CDNs), peer-to-peer systems (P2P), video streaming, and others. Anycast flows can significantly reduce the network load, compared to the unicast flows. Furthermore, since the user can select the source (destination) of data among many replica sites, anycasting also improves the network resilience [143]. As a consequence of the growing importance of anycasting in the context of cloud computing, new static and dynamic optimization problems appear in order to provide high reliability for the networks. Some initial works have been conducted in this field, e.g., [41,117,145].

In Figs. 19 and 20, we show two scenarios related to anycasting and cloud computing. Figure 19 displays a classical cloud computing setup with two data centers (clouds) and the user can use any of them, i.e., *A* can serve as a working data center and *B* can be a backup data center. Figure 20 presents a corresponding configuration, however cloud *B* is spread into smaller data centers using the mist model. In such a case, more backup data centers (and more backup connections) are available in the network, what improves the reliability.

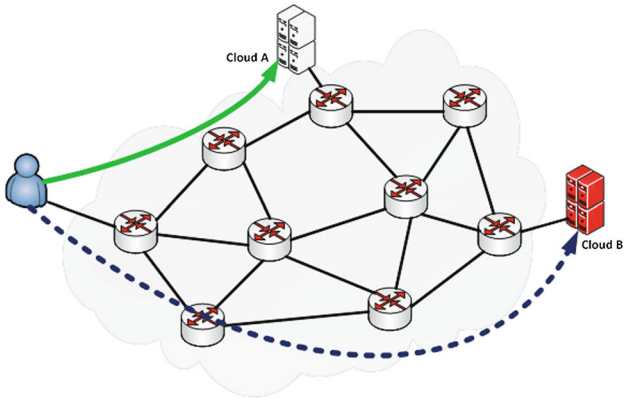


Fig. 19 Survivable anycasting in cloud computing (cloud model)

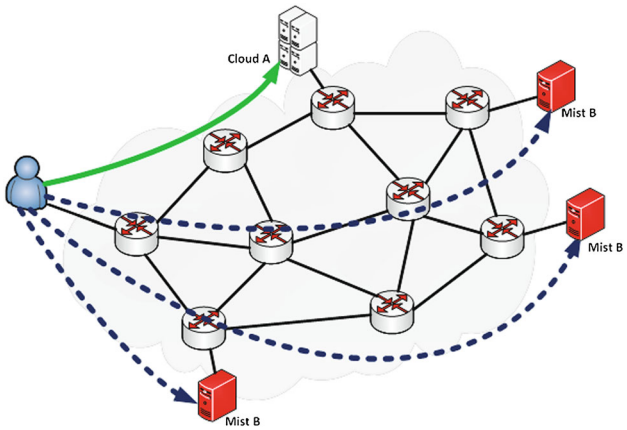


Fig. 20 Survivable anycasting in cloud computing (mist model)

To provide effective communication with data centers multicasting and peer-to-peer transmissions should be also considered in the reliability context. In [144], the authors described both static and dynamic approaches to optimization of survivable P2P multicasting systems. Another new traffic pattern that arises from cloud computing is many-to-many transmission, where there are many sources and destinations of the data transmission. The optimization of many-to-many flows is generally a novel topic, especially in the context of survivability constraints.

According to the Moore′s law and parallel with the evolution of IT services, the overall network traffic grows quickly. Moreover, the concept of cloud computing assumes aggregation of IT processing in a relatively small number of specialized data centers. Thus, there is a growing need for an introduction of an efficient and scalable transport platform for links of 100 Gb/s and beyond. A recent proposal to answer this challenge is the idea of EON that utilizes the spectrum resources more efficiently compared to DWDM and provides more flexibility [75,83]. Since the operation of EON differs significantly from the currently used optical technologies,

many new aspects and problems including survivability and optimization must be considered by the research community in the context of EON. So far, in the literature there have been proposed relatively few works addressing the survivability of EON, e.g., [45,84].

The cloud computing concept has many business advantages as described above. However, the outsourcing of computing and storage resources outside the location of a company or organization means that the access to the Internet is even more critical than in traditional local server model. Therefore, reliability context of access networks should be also highlighted as an another research direction. Obviously, a large number of technological and organizational issues can be addressed here, however we want to draw our attention of multi-homing architecture, i.e., each node is connected to the Internet by a number of separate and disjoint access links. Such an architecture provides high reliability but requires novel optimization approaches. For some information related to survivable dual homing (a special case of multi homing) in overlay networks refer to [85].

Further potential research fields in reliable networks design in the cloud computing context mentioned only briefly are:

- redundant data storage (e.g., backups),
- energy consumption issues,
- analysis and monitoring (e.g., new points of vulnerability),
- overload control,
- availability and reliability challenges following from complexity of cloud systems, e.g., high-availability requirements, automatic failure detection, reporting and recovery mechanisms, etc.

9 Resiliency in software-defined networks

In this section, we consider resiliency of Software-Defined Networking (SDN). SDN is an approach to networking which allows network operators to optimize network behavior by directly configuring the packet forwarding hardware according to user defined rules. At the heart of a software-defined network is a controller, which means that SDN is logically centralized. We will consider three aspects: how to handle failures in the data network, how to maintain connectivity with the controller, and some aspects of virtualization.

The goal of SDN is to provide open user-controlled management of the forwarding hardware of a set of network elements. The OpenFlow protocol was designed particularly to deploy and test experimental protocols in the production quality campus network Stanford used every day, instead of in a separated lab environment [100]. If operators want to be able to program the behavior of high speed networking elements such as IP routers or Ethernet switches for their custom needs, they require direct programming of the forwarding hardware. Modern routers/switches contain a proprietary FIB (Forwarding Information Base), which is implemented in hardware.

OpenFlow provides control of forwarding hardware by providing a standardized abstraction of the FIB called a Flow Table. An OpenFlow switch is a network element implementing an instance of the (abstract) Flow Table that has a secure channel to the OpenFlow controller. The OpenFlow controller manages the OpenFlow switches over the OpenFlow protocol. The OpenFlow protocol supports messages to add, delete and modify flow entries in the Flow Table. A flow entry consists of (1) a matching structure (for the packet header) which defines the flow, (2) an action which defines how the matching packets should be processed, and (3) per-flow statistics which keep track of the number of packets, the number of bytes, and the time elapsed since the last packet matched for this particular flow.

Incoming packets processed by OpenFlow switches are compared against the flow entries in the Flow Table. If a matching flow entry is found, the predefined actions for that entry are performed on the matched packet. If no match is found, the packet can be dropped or forwarded to the controller over the secure channel. If the packet is forwarded to the controller, it determines how the packet should be handled; either by returning this specific packet to the switch and stating which port it should be forwarded to or by adding valid flow entries in the switch [136].

9.1 Data plane resiliency

Carrier-grade networks have a strict requirement that the data plane should recover from single failures within a 50 ms interval. Because of the centralized nature of OpenFlow, reactive approaches to failure recovery (such as restoration) put considerable stress on the controller momentarily after the failure because it has to reconfigure all affected flows in the network and therefore update a lot of entries in the Flow Tables. Proactive solutions (such as path protection), where the recovery actions are taken in the switches themselves without contacting the controller, do not suffer from centralized control. It is shown that restoration is not able to achieve fast failure recovery of a large number of flows within 50 ms but protection has no scalability issues and can achieve recovery within 50 ms in a large-scale network serving many flows [124].

9.2 Control plane resiliency

Because OpenFlow is a logically centralized architecture, reliability of the control plane is of the utmost importance. The constraints on control plane recovery, such as the allowed recovery time (seconds or milliseconds?) and the behavior of the switches during recovery (keep the current state infor-

mation or not?) are currently unknown. Other open questions are the order in which the switches must be reconnected and whether the recovery is the responsibility of the switch or the controller.

The most efficient way to build a resilient control network for a Software Defined Network still requires a lot of investigation, and a number of research directions are presented here.

One can provide two controllers, each in a separate control network (Fig. 21) and when connection to one controller is lost, the switch uses the backup controller and network. This is a (potentially) very fast, but expensive solution. Moreover one has to maintain a consistent state between the master and redundant controllers.

A switched control network (e.g., Ethernet-based) with multiple controllers may be cheaper, but has slower recovery (e.g., STP/RSTP). Providing more advanced methods for resiliency in this network will again drive the cost upwards.

Another option is to try to restore the connection to the controller by routing the affected control traffic over the data network. When a switch loses its connection to the OpenFlow controller, it sends its control traffic to a neighboring switch which is unaffected by the failure and can relay the messages to the controller. This through-the-data-plane solution is an intermediate step towards full in-band control.

In an in-band control network, the controller is integrated into the data network and the connections between OpenFlow switches and controller pass through the other OpenFlow switches (Fig. 22).

In-band control has a number of advantages because there is no separate network. Apart from the obvious savings in equipment and the associated cost reduction, any resilience mechanism implemented for failures in the data network can also recover (at least some) control traffic. The main advantage, however, is that the controller can be in control of its own control network and take additional recovery actions when needed. The main drawback of in-band control is the additional management complexity.

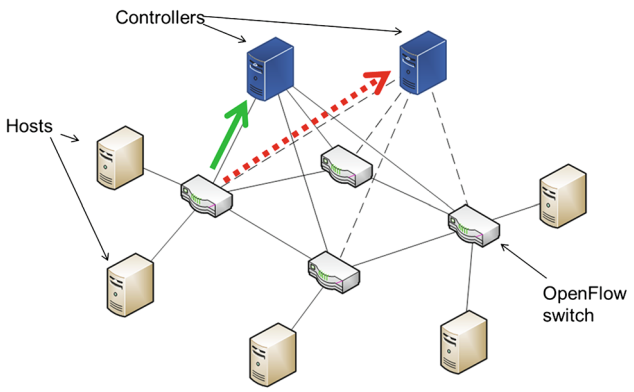


Fig. 21 Separate out-of-band control networks

9.3 Virtualization

SDN provides a framework that allows a number of ways to virtualize a network. Through network virtualization, multiple isolated logical networks each with potentially different addressing and forwarding mechanisms can share the same physical infrastructure (IaaS). Therefore, it can be an efficient way for improving network resource utilization, separation of traffic between different entities, and simplifying network management.

The most essential part of any virtualization solution is some kind of translation / hypervisor unit that translates names, addresses and other network identifiers between the real physical network and the different virtual views (Fig. 23). As with computer virtualization hypervisors, there are many different options for how and where to implement it, but it has to be somewhere between the application logic and the physical fast-path hardware. One of the first and best known virtualization methods for OpenFlow was FlowVisor [125] but other options have been investigated [128].

Providing efficient resiliency in a virtualized environment brings about some additional challenges. Some aspects, such as link failures and virtual machine failures have been investigated. Recovery actions can be the responsibility of the physical network provider, the virtual network operator, or

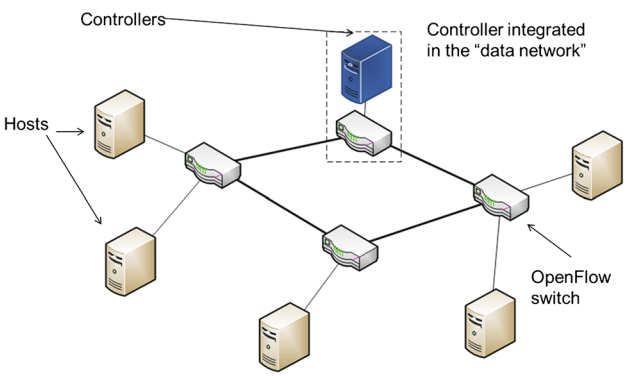


Fig. 22 In-band control

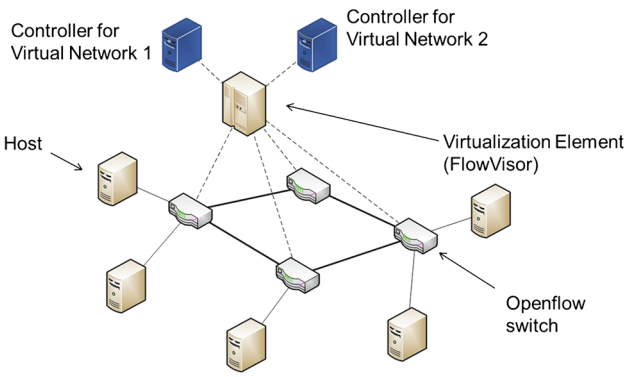


Fig. 23 Virtualization using FlowVisor

both [10]. However, failures of the virtualization mechanism (e.g. the FlowVisor) can be very difficult to recover from, especially if the state information in the virtualization elements is lost. Protecting the virtualization element means that constant synchronization will be required which may induce large costs.

In summary, in order to make Software Defined Networks resilient, we need to experimentally determine the impact of failures in the control network to determine the recovery requirements for the controller and control network. Furthermore, the impact of failures or misconfigurations of the virtualization system in an IaaS scenario must be investigated, and also how to propagate errors from the physical (both control and data) networks to the virtualized networks on top.

10 Conclusions

As communication networks become more and more important in our daily professional and private life, service failures should be avoided at all times and even a brief outage can have large economical consequences. Hence, network reliability is indispensable and represents a key research topic. This paper presents some key challenges in the domain of reliable communication networks. It is clear that reliability is required on many fronts: reliable software, reliable protocols with inherent recovery schemes, interaction between technologies via multilayer recovery, novel architectures for the Future Internet, etc. Clear insight in these domains and their mutual interaction is important to further enhance the research efforts in this field.

Acknowledgments The work of Jacek Rak has been supported in part by the Polish Ministry of Science and Higher Education under the Grant N N519 581038. The work of Arie M.C.A. Koster was supported by the Federal Ministry of Education and Research (BMBF Grant 05M10PAA, project ROBUKOM Robust Communication Networks, http://www.robukom.de). The work of James P.G. Sterbenz and Egemen K. Çetinkaya was based on research performed in the ResiliNets group at the University of Kansas (US) and Lancaster University (UK), and is funded in part by NSF FIND (Future Internet Design) Program under Grant CNS-0626918 (Postmodern Internet Architecture), by NSF Grant CNS-1050226 (Multilayer Network Resilience Analysis and Experimentation on GENI), and by the EU FP7 FIRE Programme ResumeNet project (Grant agreement No. 224619). The work of Teresa Gomes has been partially supported by programme COMPETE of the EC Community Support Framework III and co-sponsored by the EC fund FEDER, Project FCT PTDC/EEA-TEL/101884/2008, and by FCT under Project Grant Pest-OE/EEI/UI308/2014. The work of Matthias Gunkel has been partially supported by STRONGEST, an Integrated Project funded by the European Commission through the 7th ICT framework program FP7/2007-2013 under Grant agreement No. 247674. The work of Krzysztof Walkowiak was supported by the Polish National Science Centre under the Grant N N519 650440.

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

References

1. Agarwal, P. K., et al. (2010). Network vulnerability to single, multiple and probabilistic physical attacks. In *Proceedings of the Military Communications Conference, MILCOM 2010* (pp. 1824–1829). IEEE.
2. Ahlgren, B., Aranda, P. A., Chemouil, P., Oueslati, S., Correia, L. M., Karl, H., et al. (2011). Content, connectivity, and cloud: Ingredients for the network of the future. *IEEE Communications Magazine*, *49*(7), 62–70.
3. Alderson, D., Li, L., Willinger, W., & Doyle, J. C. (2005). Understanding Internet topology: Principles, models, and validation. *IEEE/ACM Transactions on Networking*, *13*(6), 1205–1218.
4. Alonso, J., Grottke, M., Nikora, A. P., & Trivedi, K. S. (2012). The nature of the times to flight software failure during space missions. In *Proceedings of the 23rd IEEE International Symposium on Software Reliability Engineering (ISSRE 2012)*. IEEE.
5. Alonso, J., Grottke, M., Nikora, A. P., & Trivedi K. S. (2013). An empirical investigation of fault repairs and mitigations in space mission system software, In *Proceedings of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN 2013), (pp. 1–8).
6. Alonso, J., Silva, L., Andrzejak, A., Silva, P., & Torres, J. (2007). High-available grid services through the use of virtualized clustering. In *Proceedings of the 8th IEEE/ACM International Conference on Grid Computing (GRID 2007)* (pp. 34–41). IEEE.
7. Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, Carl. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11–13.
8. Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., & Swallow, G. (2001). RSVP-TE: Extensions to RSVP for LSP tunnels. *IETF RFC 3209*.
9. Balbuena, M. C., Carmona, A., & Fiol, M. A. (1998). Distance connectivity in graphs and digraphs. *Journal of Graph Theory*, *22*(4), 281–292.
10. Barla, I. B., et al. (2011). Analysis of resilience in virtual networks. In *Proceedings of the 11th Würzburg Workshop on IP, Euroview 2011* (pp. 1–2).
11. Beineke, L. W., Oellermann, O. R., & Pippert, R. E. (2002). The average connectivity of a graph. *Discrete Mathematics*, *252*(1–3), 31–45.
12. Belotti, P., Kompella, K., Ceuppens, L., & Noronha, L. (2011). Transport networks at a crossroads: The roles of MPLS and OTN in packet transport networks. In *Proceedings of the Optical Fiber Communication—-National Fiber Optic Engineers Conference (OFC/NFOEC)*, 2011.
13. Ben-Ameur, W. (2011). Between fully dynamic routing and robust stable routing. In *Proceedings of the DRCN 2007–6th International Workshop Design Reliable Communication Networks* (pp. 1–6).
14. Bertsimas, D., & Sim, M. (2003). Robust discrete optimization and network flows. *Mathematical Programming*, *98*, 49–71.
15. Bertsimas, D., & Sim, M. (2004). The price of robustness. *Operations Research*, *52*(1), 35–53.
16. Bhandari, R. (1999). *Survivable Networks: Algorithms for Diverse Routing*. Philip Drive Norwell, MA: Kluwer.
17. Bhattacharjee, B., Calvert, K., Griffioen, J., Spring, N., & Sterbenz, J. P. G. (2006). *On power-law relationships of the Internet topology*. NSF-FIND proposal, ITTC Technical Report ITTC-FY2006-TR-45030-01 (2006). Lawrence, KS: The University of Kansas.
18. Blum, J., Eskandarian, A., & Hoffman, L. (2004). Challenges of intervehicle ad-hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *5*(4), 347–351.

19. Bocci, M., Bryant, S., Frost, D., Levrau, L., & Berger, L. (2010). A framework for MPLS in transport networks. I*ETF RFC 5921*.
20. Büsing, C. (2012). Recoverable robust shortest path problems. *Networks*, *59*(1), 181–189.
21. Büsing, C., Koster, A. M. C. A., & Kutschka, M. (2011). Recoverable robust knapsacks: Γ-scenarios. In *Proceedings of the INOC 2011–5th International Network Optimization Conference*. Lecture Notes on Computer Science, (vol. 6701, pp. 583–588). Berlin: Springer.
22. Büsing, C., Koster, A. M. C. A., & Kutschka, M. (2011). Recoverable robust knapsacks: The discrete scenario case. *Optimization Letters*, *5*(3), 379–392.
23. Casaca, A., Silva, T., Grilo, A., Nunes, M., Presutto, F., & Rebelo, I. (2007). The use of wireless networks for the surveillance and control of cooperative vehicles in an airport. *Telecommunication Systems*, *36*(1–3), 141–151. doi:10.1007/s11235-007-9063-z.
24. Castelli, V., Harper, R. E., Heidelberger, P., Hunter, S. W., Trivedi, K. S., Vaidyanathan, K., et al. (2001). Proactive management of software aging. *IBM Journal of Research & Development*, *45*(2), 311–332.
25. Çetinkaya, E.K., & Sterbenz, J.P.G. (2013). A taxonomy of network challenges. In *Proceedings of the 9th IEEE/IFIP International Conference on Design of Reliable Communication Networks (DRCN)*, Budapest (pp. 322–330).
26. Çetinkaya, E. K., Broyles, D., Dandekar, A., Srinivasan, S., & Sterbenz, J. P. G. (2011). Modelling communication network challenges for future internet resilience, survivability and disruption tolerance: A simulation-based approach. Telecommunication Systems, *52*(2), 751–766. doi:10.1007/s11235-011-9575-4.
27. Çetinkaya, E. K., Peck, A. M., & Sterbenz, J. P. G. (2013). Flow robustness of multilevel networks. In *Proceedings of the 9th IEEE/IFIP International Conference on Design of Reliable Communication Networks (DRCN)*, Budapest (pp. 274–281).
28. Claßen, G., Koster, A. M. C. A., & Schmeink, A. (2013). A robust optimisation model and cutting planes for the planning of energy-efficient wireless networks. *Computers & Operations Research*, *40*(1), 80–90.
29. Clímaco, J., & Pascoal, M. (2012). *A new method to determine unsupported non-dominated solutions in multicriteria integer linear programming: A reference point approach*. Technical Report 3/2012. Coimbra: INESC Coimbra.
30. Clímaco, J., & Craveirinha, J. (2005). Multiple criteria decision analysis: State of the art surveys. *Multicriteria analysis in telecommunication planning and design—problems and issues* (pp. 899–951)., International Series in Operations Research & Management Science New York: Springer.
31. Clímaco, J., Craveirinha, J., & Pascoal, M. (2007). Advances in Multiple Criteria Decision Making and Human Systems Management: Knowledge and Wisdom. *Multicriteria routing models in telecommunication networks: Overview and a case study* (pp. 17–46). Amsterdam: IOS Press.
32. Colle, D., et al. (2002). Data-centric optical networks and their survivability. *IEEE Journal on Selected Areas in Communications*, *20*(1), 6–20.
33. Contreras, L. M., Lopez, V., De Dios, O. G., Tovar, A., Munoz, F., Azanon, A., et al. (2012). Toward cloud-ready transport networks. *IEEE Communications Magazine*, *50*(9), 48–55.
34. Coutinho-Rodrigues, J. M., Clímaco, J., & Current, J. R. (1999). An interactive bi-objective shortest path approach: Searching for unsupported nondominated solutions. *Computers & Operations Research*, *26*(8), 789–798.
35. Cramp, R., Vouk, M. A., & Jones, W. (1992). On operational availability of a large software-based telecommunications system. In *Proceedings of the International Symposium on Software Reliability Engineering ISSRE*. IEEE.
36. Crane, R. (1980). Prediction of attenuation by rain. *IEEE Transactions on Communications*, *28*(9), 1717–1733.
37. Craveirinha, J., Girão-Silva, R., & Clímaco, J. (2008). A metamodel for multiobjective routing in MPLS networks. *Central European Journal of Operations Research*, *16*(1), 79–105.
38. De Maesschalck, S., et al. (2002). Intelligent optical networking for multilayer survivability. *IEEE Communications Magazine*, *40*(1), 42–99.
39. Demeester, P., et al. (1999). Resilience in multilayer networks. *IEEE Communications Magazine*, *37*(8), 70–76.
40. Deore, A., Turkcu, O., Ahuja, A., Hand, S. J., & Melle, S. (2012). Total cost of ownership of WDM and switching architectures for next-generation 100Gb/s networks. *IEEE Communications Magazine*, *50*(11), 179–187.
41. Develder, C., et al. (2011). Survivable optical grid dimensioning anycast routing with server and network failure protection. In *Proceedings of the IEEE International Conference on Communications—ICC* (pp. 1–5). IEEE.
42. Develder, C., De Leenheer, M., Dhoedt, B., Pickavet, M., Colle, D., De Turck, F., et al. (2012). Optical networks for grid and cloud computing applications. *Proceedings of the IEEE*, *100*(5), 1149–1167.
43. Dörner, D. (1997). *The logic of failure: Recognizing and avoiding error in complex situations*. Cambridge: Perseus Books.
44. Duhovniko, S., Koster, A. M. C. A., Kutschka, M., Rambach, F., & Schupke, D. (2013). Γ-robust network design for mixed-line-rate-planning of optical networks. In *Proceedings of the Optical Fiber Communication—National Fiber Optic Engineers Conference (OFC/NFOEC)*. IEEE.
45. Eira, A., et al. (2012). Optimized design of shared restoration in flexible-grid transparent optical networks. In *Proceedings of the Optical Fiber Communications, OFC*.
46. Engel, T., Autenrieth, A., & Bischoff, J.-C. (2009). Packet layer topologies of cost optimized transport networks. In *Proceedings of the ONDM 2009–13th Conference on Optical Network Design and Modeling* (pp. 1–7). IEEE.
47. Faloutsos, M., Faloutsos, P., & Faloutsos, C. (1999). On power-law relationships of the Internet topology. In *Proceedings of the ACM SIGCOMM, 1999* (pp. 251–262).
48. Fischetti, M., & Monaci, M. (2012). Cutting plane versus compact formulations for uncertain (integer) linear programs. *Mathematical Programming Computation*, *4*, 239–273.
49. Garg, S., Huang, Y., Kintala, C. M. R., Trivedi, K. S., & Yajnik, S. (1999). Performance and reliability evaluation of passive replication schemes in application level fault tolerance. In *Proceedings of the FTCS 1999—Twenty-Ninth International Symposium on Fault-Tolerant Computing* (vol. 322). IEEE.
50. Gomes, T., Craveirinha, J., Clímaco, J., & Simões, C. (2009). A bicriteria routing model for multi-fibre WDM networks. *Photonic Network Communications*, *18*(3), 287–299. doi:10.1007/s11107-009-0192-z.
51. Gozalvez, J., Sepulcre, M., & Bauza, R. (2012). Impact of the radio channel modelling on the performance of VANET communication protocols. *Telecommunication Systems*, *50*(3), 149–167. doi:10.1007/s11235-010-9396-x.
52. Gray, J. (1985). Why do computers stop and what can be done about it? In Tandem Computers, Technical Report 85.7, PN 87614.
53. Gray, J. (1986). Why do computers stop and what can be done about it? In *Proceedings of the SRDS86—5th Symposium on Reliability in Distributed Software and Database Systems, Los Alamitos, CA* (pp. 1–1).
54. Grottke, M., & Trivedi, K. S. (2005). A classification of software faults. In *Proceedings of the Sixteenth International IEEE Symposium on Software Reliability Engineering* (pp. 4.19–4.20). IEEE.

55. Grottke, M., Matias, R., & Trivedi, K. S. (2008). The fundamentals of software aging. In *Proceedings of the 1st International Workshop on Software Aging and Rejuvantion* (pp. 1–6).
56. Grottke, M., Nikora, A. P., & Trivedi, K. S. (2010). An empirical investigation of fault types in space mission system software. In *Proceedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (pp. 447–456). IEEE.
57. Grottke, M., & Trivedi, K. S. (2005). Fighting bugs: remove, retry, replicate, and rejuvenate. *Journal of the Reliability Engineering Association of Japan*, *27*(7), 425–438.
58. Grottke, M., & Trivedi, K. S. (2007). Software faults, software aging and software rejuvenation. *IEEE Computer*, *40*(2), 107–109.
59. Gumaste, A., & Krishnaswamy, N. (2010). Proliferation of the optical transport network: A use case based study. *IEEE Communications Magazine*, *48*(9), 54–61.
60. Gunkel, M., Autenrieth, A., Neugirg, M., & Elbers, J.-P. (2012). Advanced multilayer resilience scheme with optical restoration for IP-over-DWDM core networks: How multilayer survivability might improve network economics in the future. In *Proceedings of the RNDM 2012–4th International Workshop on Reliable Networks Design and Modeling* (pp. 10–15).
61. Guo, Y. (1997). Path connectivity in local tournaments. *Discrete Mathematics*, *167–168*, 353–372.
62. Haddadi, H., Rio, M., Iannaccone, G., & Moore, A. (2008). Network topologies: Inference, modeling, and generation. *IEEE Communications Surveys & Tutorials*, *10*(2), 48–69.
63. Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad-hoc networks. *IEEE Communications Magazine*, *46*(6), 164–171.
64. He, Y., & Perkins, D. (June 2011). Achieving seamless handoffs via backhaul support in Wireless Mesh Networks. *Telecommunication Systems*. doi:10.1007/s11235-011-9474-8.
65. Holzmann, G. J. (2007). Conquering complexity. *IEEE Computer*, *40*(12), 111–113.
66. Homepage of the European FP7 project. Scalable, Tunable and Resilient Optical Networks Guaranteeing Extremely-high Speed Transport (STRONGEST). http://www.ict-strongest.eu/. Accessed 27 Nov 2012.
67. Homepage of the European FP7 project. Industry-Driven Elastic and Adaptive Lambda Infrastructure for Service and Transport Networks (IDEALIST) http://www.ict-idealist.eu/. Accessed 29 Nov 2012.
68. Hu, J., Deng, J., & Wu, J. (October 2011). A green private cloud architecture with global collaboration. *Telecommunication Systems*. doi:10.1007/s11235-011-9639-5.
69. Huang, X., & Fang, Y. (2009). Performance study of node-disjoint multipath routing in vehicular ad-hoc networks. *IEEE Transactions on Vehicular Technology*, *58*(4), 1942–1950.
70. Iannone, L., & Fdida, S. (2006). Evaluating a cross-layer approach for routing in wireless mesh networks. *Telecommunication Systems*, *31*(2–3), 173–193. doi:10.1007/s11235-010-9400-5.
71. ITU-T. (2009). Network node interface for the optical transport network (OTN). Rec. G.709/Y.1331.
72. Jabbar, A., et al. (2009). Performance comparison of weather disruption-tolerant cross-layer routing algorithms. In *Proceedings of the IEEE INFOCOM 2009* (pp. 1143–1151).
73. Jabbar, A., Rohrer, J.P., Oberthaler, A., Çetinkaya, E.K., Frost, V.S., & Sterbenz, J.P.G. (2009). Performance comparison of weather disruption-tolerant cross-layer routing algorithms. In *Proceedings of 28th IEEE Conference on Computer Communications (INFOCOM 2009)*, Rio de Janeiro, (pp. 1143–1151).
74. Jabbar, A., Raman, B., Frost, V.S., & Sterbenz, J.P.G. (2009). Weather disruption-tolerant self-optimising millimeter mesh networks, In *Third International IFIP/IEEE Workshop on Self-Organizing Systems (IWSOS 2008)*, Vienna, LNCS 5343, Springer, Heidelberg, (pp. 242–255).
75. Jinno, M., et al. (2010). Distance-adaptive spectrum resource allocation in spectrum-sliced elastic optical path network. *IEEE Communications Magazine*, *48*(8), 138–145.
76. Kaaniche, M., & Kanoun, K. (1996). Reliability of a commercial telecommunications system. In *Proceedings of the International Symposium on Software Reliability Engineering (ISSRE)*. IEEE.
77. Kang, J., Lee, J., Hwang, C., & Chang, H. (September 2011). The study on a convergence security service for manufacturing industries. *Telecommunication Systems*. doi:10.1007/s11235-011-9651-9.
78. Kanoun, K. (2001). Real-world design diversity: A case study on cost. *IEEE Software*, *18*(4), 29–33.
79. Karagiannis, G., et al. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards, and solutions. *IEEE Communications Surveys and Tutorials*, *13*(4), 584–616.
80. Katib, I., & Medhi, D. (2011). A network protection design model and a study of three-layer networks with IP/MPLS, OTN, and DWDM. In *Proceedings of the DRCN 2011—8th International Workshop on the Design of Reliable Communication Networks* (pp. 17–24).
81. Khan, J. A., & Alnuweiri, H. M. (2005). Traffic engineering with distributed dynamic channel allocation in BFWA mesh networks at millimeter wave band. In *Proceedings of the 14th IEEE Workshop on Local and Metropolitan Area Networks* (pp. 1–6). IEEE.
82. Kim, K., & Venkatasabramanian, N. (2010). Assessing the impact of geographically correlated failures on overlay-based data dissemination. In *Proceedings of the IEEE GLOBECOM 2010* (pp. 1–5).
83. Klinkowski, M., & Walkowiak, K. (2011). Routing and spectrum assignment in spectrum sliced elastic optical path network. *IEEE Communications Letters*, *15*(8), 884–886.
84. Klinkowski, M., & Walkowiak, K. (2012). Offline RSA algorithms for elastic optical networks with dedicated path protection consideration. In *Proceedings of the RNDM 2012—4th International Workshop on Reliable Networks Design and Modeling* (pp. 25–31).
85. Kmiecik, W., & Walkowiak, K. (2011). Survivable P2P multicasting flow assignment in dual homing networks. In *Proceedings of the RNDM 2011—3rd International Workshop on Reliable Networks Design and Modeling* (pp. 157–163).
86. Kogge, P. (2011). The tops in flops. *IEEE Spectrum*, *48*(2), 48–54.
87. Koster, A. M. C. A., & Kutschka, M. (2011). Network design under demand uncertainties: A case study on the Abilene and GÉANT network data. In *Proceedings of the 12th ITG-Fachtagung Photonische Netze* (pp. 154–161).
88. Koster, A. M. C. A., Kutschka, M., & Raack, C. (2010). Towards robust network design using integer linear programming techniques. In *Proceedings of the NGI 2010—Next Generation Internet* (pp. 1–8).
89. Koster, A. M. C. A., Kutschka, M., & Raack, C. (2011). On the robustness of optimal network designs. In *Proceedings of the IEEE ICC—IEEE International Conference on Communications* (pp. 1–5). IEEE.
90. Koster, A. M. C. A., Kutschka, M., & Raack, C. (2013). Robust network design: Formulations, valid inequalities, and computations. *Networks*, *61*(2), 128–149.
91. KU TopView ResiliNets Topology Map Viewer, 2011. http://www.ittc.ku.edu/resilinets/maps/. Accessed 21 Nov 2012.
92. Kyas, O. (2001). *Network Troubleshooting*. Palo Alto California, Agilent Technologies.

93. Liebchen, C., Lübbecke, M. E., Möhring, R., & Stiller, S. (2009). The concept of recoverable robustness, linear programming recovery, and railway applications. *Lecture Notes on Computer Science* (vol. 5868, pp. 1–27). Berlin: Springer.
94. Liu, J., et al. (2011). Reliability assessment for wireless mesh networks under probabilistic region failure model. *IEEE Transactions on Vehicular Technology, 60*(5), 2253–2264.
95. Lyu, M. R., Chen, J., & Avizienis, A. (1994). Experience in metrics and measurements for N-version programming. *International Journal of Reliability, Quality and Safety Engineering*. doi:10.1142/S0218539394000052.
96. Maier, G., & Pattavina, A. (2013). Deflection routing in IP optical networks. *Telecommunication Systems*, *52*(1), 51–60. doi:10.1007/s11235-011-9442-3.
97. Marshall, E. (1992). Fatal error: How patriot overlooked a scud. *Science*, *255*(5050), 1347.
98. Matias, R, Jr, Trivedi, K. S., & Maciel, P. R. M. (2010). Using accelerated life tests to estimate time to software aging failure. In *Proceedings of the IEEE International Symposium on Software Reliability Engineering* (pp. 211–219).
99. Matos, R., Sargento, S., Hummel, K. A., Hess, A., Tutschku, K., & de Meer, H. (2012). Context-based wireless mesh networks: A case for network virtualization. *Telecommunication Systems*, *51*(4), 259–272. doi:10.1007/s11235-011-9434-3.
100. McKeown, N., et al. (2008). OpenFlow: Enabling innovation in campus networks. In *Proceedings of the SIGCOMM, Review* (vol. 38(2), pp. 69–74).
101. Medhi, D., & Tipper, D. (2000). Multi-layered network survivability models, analysis, architecture, framework and implementation: An overview. In *Proceedings of the DISCEX 2000—DARPA Information Survivability Conference and Exposition* (pp. 173–186).
102. Molisz, W., & Rak, J. (2005). Region protection/restoration scheme in survivable networks. *Lecture Notes in Computer Science*, *3685*, 442–447.
103. Molisz, W., & Rak, J. (2008). A novel class-based protection algorithm providing fast service recovery in IP/WDM networks. *Lecture Notes in Computer Science*, *4982*, 338–345.
104. Naumov, V., & Gross, T. (2007). Connectivity-aware routing in vehicular ad-hoc networks. In *Proceedings of the International Conference on Computer Communications—INFOCOM 2007* (pp. 1919–1927).
105. Neumayer, S., & Modiano, E. (2010). Network reliability with geographically correlated failures. In *Proceedings of the IEEE International Conference on Computer Communications INFOCOM 2010* (pp. 1–9).
106. Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., & Ueno, S. (2009). Requirements of an MPLS transport profile. *IETF RFC 5654*.
107. Nokia Siemens Networks. (2011). Optical transport network switching: Creating efficient and cost-effective optical transport networks. White Paper.
108. Oppenheimer, D., Ganapathi, A., & Patterson, D. A. (2003). Why do internet services fail, and what can be done about it? In *Proceedings of the 4th USENIX Symposium on Internet Technologies and Systems (USITS03)*.
109. Pan, P., Swallow, G., Atlas, A. (2005). Fast reroute extensions to RSVP-TE for LSP tunnels, RFC 4090. http://www.rfc-editor.org/info/rfc4090. Accessed 23 Nov 2012.
110. Peret, S., & Narasimham, P. (2005). Causes of failure in web applications. TR CMU-PDL-05-109. Pittsburgh, PA: Carnegie Mellon University.
111. Pióro, M., & Medhi, D. (2004). *Flow and capacity design in communication and computer Networks*. Burlington, MA: Morgan Kaufmann.
112. Poss, M., Raack, C. (2011). Affine recourse for the robust network design problem: Between static and dynamic routing. *Networks, 61*(2), 180–198.
113. Rak, J. (2010). *k*-Penalty: A novel approach to find *k*-disjoint paths with differentiated path costs. *IEEE Communication Letters*, *14*(4), 354–356.
114. Rak, J. (2012). Fast service recovery under shared protection in WDM networks. *IEEE/OSA Journal of Lightwave Technology*, *30*(1), 84–85.
115. Rak, J. (2013). Providing differentiated levels of service availability in VANET communications. *IEEE Communication Letters*, *17*(7), 1380–1383.
116. Rak, J. (2015). A new approach to design of weather disruption-tolerant wireless mesh networks. *Telecommunication Systems*. doi:10.1007/s11235-015-0003-z.
117. Rak, J., & Walkowiak, K. (2013). Reliable anycast and unicast routing: Protection against attacks. *Telecommunication Systems*, *52*(2), 889–906. doi:10.1007/s11235-011-9583-4.
118. Ramamurthy, S., Sahasrabuddhe, L., & Mukherjee, B. (2003). Survivable WDM mesh networks. *IEEE Journal of Lightwave Technology*, *21*(4), 870–883.
119. Rambach, F., Konrad, B., Dembeck, L., Gebhard, U., Gunkel, M., Quagliotti, M., Serra, L., López, V. A multi-layer cost model for metro/core networks. Accepted for publication in the Journal of Optical Communications and Networking. http://www.opticsinfobase.org/jocn. Accessed 18 Nov 2012.
120. Rosen, E., Viswanathan, A., & Callon, R. (2001). Multiprotocol label switching architecture. *IETF RFC 3031*.
121. Sen, A., Murthy, S., & Banerjee, S. (2009). Region-based connectivity: A new paradigm for design of fault-tolerant networks. In *Proceedings of the 15th International Conference on High Performance Switching and Routing (HPSR09)* (pp. 1–7).
122. Sen, A., Shen, B. H., Zhou, L., & Hao, B. (2006). Fault-tolerance in sensor networks: A new evaluation metric. In *Proceedings of the IEEE International Conference on Computer Communications—INFOCOM06* (pp. 1–12).
123. Sen, S. (2011). *Stochastic mixed-integer programming algorithms: Beyond Benders' decomposition*., Wiley Encyclopaedia of Operations Research and Management Science New York, NY: Wiley.
124. Sharma, S., et al. (2012). OpenFlow: Meeting carrier-grade recovery requirements. *Computer Communications*. Amsterdam: Elsevier. doi:10.1016/j.comcom.2012.09.011.
125. Sherwood, R., et al. (2009). FlowVisor: A network virtualization layer. Technical report openflow-tr-2009-1-flowvisor. http://www.openflow.org. Accessed 26 Nov 2012.
126. Sichitiu, M. L., & Kihl, M. (2008). Inter-vehicle communication systems: A survey. *IEEE Communications Surveys and Tutorials*, *10*(2), 88–105.
127. Simões, C., Gomes, T., Craveirinha, J., and Clímaco J. (2010). Performance analysis of a bi-objective model for routing with protection in WDM networks. *Journal of Telecommunications and Information Technology*, (3), 25–35. http://www.nit.eu/czasopisma/JTIT/2010/3/25.pdf. Accessed 27 Nov 2012.
128. Sköldström, P., et al. (2012). Network virtualization and resource allocation in OpenFlow-based wide area networks. In *Proceedings of the IEEE International Conference on Communications (ICC)* (pp. 6622–6626). IEEE.
129. Somani, A. (2006). *Survivability and traffic grooming in WDM optical networks*. Cambridge: Cambridge University Press.
130. Sterbenz, J. P. G., & Hutchison, D. (2006). ResiliNets: Multilevel resilient and survivable networking initiative wiki. http://wiki.ittc.ku.edu/resilinets. Accessed 23 Nov 2012.
131. Sterbenz, J. P. G., Çetinkaya, E. K., Hameed, M. A., Jabbar, A., Shi, Q., & Rohrer, J. P. (December 2011). Evaluation of network resilience, survivability, and disruption tolerance: analy-

sis, topology generation, simulation, and experimentation (invited paper). *Telecommunication Systems*, *52*(2), 705–736. doi:10.1007/s11235-011-9573-6.
132. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2014). Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance (invited paper). *Telecommunication Systems*, *56*(1), 17–31. doi:10.1007/s11235-013-9816-9.
133. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., et al. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks: Special Issue on Resilient and Survivable Networks (COMNET)*, *54*(8), 1245–1265.
134. Steuer, R. E. (1986). *Multiple criteria optimization: Theory, computation and application*. Hoboken, NJ: Wiley.
135. Tapolcai, J., Ho, P.-H., Verchere, D., Cinkler, T., & Haque, A. (2008). A new shared segment protection method for survivable networks with guaranteed recovery time. *IEEE Transactions on Reliability*, *57*(2), 272–282.
136. The OpenFlow Switch Specification 1.3.0, June 2012. http://www.opennetworking.org/. Accessed 28 Nov 2012.
137. Trivedi, K. S., & Xia, R. (2015). Quantification of system survivability. *Telecommunication Systems*. doi:10.1007/s11235-015-9988-6.
138. Trivedi, K., Mansharamani, R., Seong Kim, D., Grottke, M., & Nambiar, M. (2011). Recovery from failures due to mandelbugs in IT systems. In *Proceedings of the IEEE 16th Pacific Rim International Symposium on Dependable Computing (PRDC'11)* (pp. 224–233). IEEE.
139. Trivedi, K., Wang, D., Hunt, J., Rindos, A., Smith, W. E., & Vashaw, B. (2008). Availability modeling of SIP protocol on IBM WebSphere. In *Proceedings of the IEEE Pacific Rim Dependability Conference* (pp. 323–330). IEEE.
140. Truong, D.-L., & Jaumard, B. (2008). Recent progress in dynamic routing for shared protection in multidomain networks. *IEEE Communications Magazine*, *46*(6), 112–119.
141. Vasseur, J.-P., Pickavet, M., & Demeester, P. (2004). *Network recovery*. Burlington, MA: Morgan Kaufmann.
142. Venters, W., & Whitley, A. (2012). A critical review of cloud computing: Researching desires and realities. *Journal of Information Technology*, *27*, 179–197.
143. Walkowiak, K. (2010). Anycasting in connection-oriented computer networks: Models, algorithms and results. *International Journal of Applied Mathematics and Computer Science*, *1*(20), 207–220.
144. Walkowiak, K., & Przewoźniczek, M. (2011). Modeling and optimization of survivable P2P multicasting. *Computer Communications*, *34*(12), 1410–1424.
145. Walkowiak, K., & Rak, J. (2013). Simultaneous optimization of unicast and anycast flows and replica location in survivable optical networks. *Telecommunication Systems*, *52*(2), 1043–1055. doi:10.1007/s11235-011-9611-4.
146. Wiatr, P., Monti, P., & Wosinska, L. (2012). Power savings versus network performance in dynamically provisioned WDM networks. *IEEE Communications Magazine*, *50*(5), 48–55.
147. Wierzbicki, A. P., & Burakowski, W. (2011). A conceptual framework for multiple-criteria routing in QoS IP networks. *International Transactions in Operational Research*, *18*(3), 377–399.
148. Xia, T. J., Gringeri, S., & Tomizawa, M. (2012). High-capacity optical transport networks. *IEEE Communications Magazine*, *50*(11), 170–178.
149. Zeadally, S., Hunt, R., Chen, Y-Sh, Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems*, *50*(4), 214–241. doi:10.1007/s11235-010-9400-5.
150. Zhang, D., Gogi, S. A., Broyles, D. S., Çetinkaya, E. K., & Sterbenz, J. P. G. (2012). Modelling attacks and challenges to wireless networks. In *Proceedings of the 4th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)* (pp. 806–812).
151. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7–18.

Jacek Rak holds Ph.D. degree in computer science received with distinction in 2009 from Gdansk University of Technology (GUT), Poland. He is currently an Assistant Professor at the Department of Computer Communications at GUT. His main research areas include: routing, design, and analysis of communication networks with special focus on reliability. He is the author/co-author of over 60 publications, including around 20 publications in journals. Dr. Rak has been involved in many projects related to optimization of reliable computer networks. He has also served as a TPC member of numerous international conferences on communications, e.g., IEEE ICC, IEEE GLOBECOM, DRCN, and journals, including IEEE Trans. on Networking, IEEE Communications Letters, or IEEE Trans. on Multimedia. He was the TPC Co-chair of ICUMT 2011&2012, NETWORKS 2010, Publication Chair of BCFIC 2011&2012, NETWORKS 2010&2012, and Workshops Chair of ITST'13. Between 2012 and 2014, he served as a member of the Editorial Board of Telecommunication Systems (Springer). Dr. Rak is currently the Vice Chair of IFIP TC6 WG 6.10, a senior member of IEEE, Steering Committee Member of NETWORKS and ICUMT conferences, as well as the founder and the General Chair of International Workshop on Reliable Networks Design and Modeling (RNDM).

Mario Pickavet received an M.Sc. and Ph.D. degree in electrical engineering, specialized in telecommunications, from Ghent University in 1996 and 1999, respectively. Since 2000, he is professor at Ghent University where he is teaching courses on discrete mathematics, multimedia networks and network modeling. He is co-leading the research cluster on Network Modeling, Design and Evaluation (NetMoDeL) covering 4 research topics: Fixed internet architectures and optical networks, techno-economic studies, green-ICT and design of network algorithms (DNA). In this context, he is currently involved in several European and national projects. He has published about 300 international publications, both in journals (Proc. of the IEEE, IEEE JSAC, IEEE Comm. Mag., Journal of Lightwave Technology, ...) and in proceedings of conferences. He is co-author of the book 'Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS'.

Kishor S. Trivedi holds the Hudson Chair in the Department of Electrical and Computer Engineering at Duke University, Durham, NC. He has been on the Duke faculty since 1975. He is the author of a well known text entitled, Probability and Statistics with Reliability, Queuing and Computer Science Applications, published by Prentice-Hall; a thoroughly revised second edition (including its Indian edition) of this book has been published by John Wiley. He has also published two other books entitled, Performance and Reliability Analysis of Computer Systems, published by Kluwer Academic Publishers and Queueing Networks and Markov Chains, John Wiley. He is a Fellow of the Institute of Electrical and Electronics Engineers. He is a Golden Core Member of IEEE Computer Society. He has published over 490 articles and has supervised 44 Ph.D. dissertations. He is the recipient of IEEE Computer Society Technical Achievement Award for his research on Software Aging and Rejuvenation. His research interests in are in reliability, availability, performance and survivability of computer and communication systems and in software dependability. He works closely with industry in carrying our reliability/availability analysis, providing short courses on reliability, availability, and in the development and dissemination of software packages such as SHARPE, SREPT and SPNP.

Javier Alonso Lopez received the master's degree in Computer Science in 2004 and the Ph.D. degree from the Technical University of Catalonia (Universitat Politecnica de Catalunya, UPC) in 2011. From 2006 to 2011, he held an assistant lecturer position in the Computer Architecture Department of UPC. From 2011 to 2014 he held a Postdoctoral Associate position under the mentoring of Professor K.S. Trivedi, in the Electrical and Computer Engineering Department, Duke University, Durham, NC. Currently, Dr. Alonso is the Acting Research Director at the Research Institute of Applied Sciences in Cybersecurity - University of Leon, Spain. He also helds a visiting Assistant Professor position at Duke University, USA. Dr. Alonso has published papers about different aspects of software engineering with special interest on dependability, high availability, performance, software security and software aging in premier conferences and journals. He has also served as a reviewer for IEEE Transactions on Computers, IEEE Transactions on Dependability and Security Computing, Performance Evaluation, and Cluster Computing, and several international conferences. He is or has been involved in NASA, JPL/NASA, NEC, NATO, Huawei, WiPro funded projects.

Arie M. C. A. Koster is since April 2009 Professor of Mathematics at RWTH Aachen University. He received his M.Sc. degree in Technical Mathematics (1995) from Delft University of Technology, The Netherlands, and his Ph.D. degree in Mathematics of Operations Research (1999) from Maastricht University, The Netherlands. The title of his doctoral thesis is "Frequency Assignment—Models and Algorithms". From 1999 to 2007 he was a senior researcher with the Department of Optimization at Zuse Institute Berlin, working on both the application of discrete optimization to telecommunication network optimization and algorithmic graph theory. From 2007 to 2009, he was an Assistant Professor at Warwick Business School and the Centre for Discrete Mathematics and its Applications (DIMAP) of the University of Warwick, United Kingdom. At RWTH Aachen University his research currently focuses on robust optimization and its applications. He coordinated from 2010 to 2013, the BMBF-project ROBUKOM—Robust Communication Networks.

James P. G. Sterbenz is Professor of Electrical Engineering & Computer Science and on staff at the Information & Telecommunication Technology Center at The University of Kansas, and is a Visiting Professor of Computing and Communication in InfoLab 21 at Lancaster University 1408 in the UK, and an Adjunct Professor of Computing at The Hong Kong Polytechnic University. He has previously held senior staff and research management positions at BBN Technologies, GTE Laboratories, and IBM Research. His research interests include resilient, survivable, and disruption tolerant networking, future Internet architectures, active and programmable networks, and high-speed networking and components. He is director of the ResiliNets Research Group, currently PI in the NSF-funded FIND and GENI programs, the EU-funded FIRE ResumeNet project, leads the GpENI international programmable network testbed project, and leads a US DoD project in highly-mobile ad hoc disruption-tolerant networking. He received a doctorate in computer science from Washington University in 1991. He has been program chair for IEEE GI, GBN, and HotI; IFIP IWSOS, PfHSN, and IWAN; and is on the editorial board of IEEE Network. He is principal author of the book High-Speed Networking: A Systematic Approach to High-Bandwidth Low-Latency Communication.

Egemen K. Çetinkaya is an Assistant Professor in the Electrical and Computer Engineering Department at Missouri University of Science and Technology. He received his Ph.D. in Electrical Engineering from the University of Kansas in 2013. He received his B.S. degree in Electronics Engineering from Uludağ University (Bursa, Turkey) in 1999 and the M.S. degree in Electrical Engineering from University of Missouri–Rolla in 2001. He held positions as a support, system, and design engineer at Sprint from 2001 until 2008. His research interests are in resilient networks. He is a senior member of the IEEE, Communications Society, a member of ACM SIGCOMM and Sigma Xi.

Teresa Gomes is an Assistant Professor in telecommunications at the Department of Electrical and Computer Engineering of the Faculty of Sciences and Technology of the University of Coimbra, Portugal, since 1998, and a researcher at the INESC Coimbra. She obtained a M.Sc. in computer science (1989) and a Ph.D. in Electrical Engineering—Telecommunications and Electronics (1998), both at the University of Coimbra. She is the author/co-author of more than 50 technical publications in international journals and conference proceedings, and one european patent. Her main present interests include routing, protection and reliability analysis models and algorithms for optical, MPLS and GMPLS networks, and multilayer routing optimization.

Matthias Gunkel was born in 1966. He received his Ph.D. in communications engineering from Darmstadt University of Technology in 1997. After 2 years working for Virtual Photonics Inc., Berlin, as project manager for photonic software engineering, he joined Deutsche Telekom in 1999. Within DT he is now with Fixed-Mobile Engineering Deutschland" (FMED) in Darmstadt, Germany, DTs network engineering centre being responsible for all kinds of technology introduced within DT group. As Senior Transport Network Architect, Dr. Gunkel is responsible for high-speed optical transport technology and future network architectures. Currently, Matthias leads DT-internal strategic activities investigating IP plus Optical architectures. Key question is how to achieve higher router interface utilization than today by the application of 100G coherent technology together with a cost-efficient multilayer resilience concept.

Krzysztof Walkowiak was born in 1973. He received the Ph.D. degree and the D.Sc. (habilitation) degree in computer science from the Wroclaw University of Technology, Poland, in 2000 and 2008, respectively. Currently, he is an Associate Professor at the Department of Systems and Computer Networks, Faculty of Electronics, Wroclaw University of Technology. His research interest is mainly focused on modeling and optimization of computer networks including: content-oriented networks; survivable networks; elastic optical networks; distributed computing systems. Prof. Walkowiak has been involved in many research projects related to optimization of computer networks. He received the Best Paper Award in the International Workshop on Design of Reliable Communication Networks (DRCN 2009). Moreover, he has been consulting projects for large companies in Poland including Ernst and Young, Skanska, TP SA, PZU, PKO BP. Prof. Walkowiak published more than 160 scientific papers. He serves as a reviewer for many international journals and he is actively involved in many international conferences. Prof. Walkowiak is a member of IEEE and ComSoc.

Dimitri Staessens received his M.Sc. Degree in numerical computer science in 2004 from Ghent University, Belgium. Since 2005 he has been working at the "Internet Based Communications Networks and Services group" and finished a Ph.D. on survivability of optical networks in 2012. This work led to over 30 publications and was performed in European projects such as NOBEL, DICONET, and NoE's e-photon/One and BONE. His current interests are in the control and management of networks, Software Defined Networking and future network architectures.