Chapter 1
Introduction

Communication networks have become essential for everyday operation of our society [1]. In particular, the Internet, considered as an indispensable part of the critical information infrastructure for a number of personal and business applications, is now expected to be *always available* [25]. Availability of network services has thus become an important element of Service Level Agreements (SLAs) between service providers and customers. Any disruption of end-to-end routing, even lasting for a short time, commonly induces serious economic losses, as well as remarkably affects reputation of the network provider.

Huge amount of content exchanged in the core part of a communication infrastructure requires high-capacity storage, processing, and transmission capabilities. Therefore, in case of failures of network nodes/links, thousands of flows may be affected and significant amount of data (measured in terms of terabits) may be lost [22]. For instance, an OC-48 optical link downtime equal to 10 s causes about 3 million packets of the average size of 1 kB to be dropped [25].

Table 1.1 shows border requirements on Quality of Service (QoS), as identified for Internet Protocol (IP) networks by International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) in Y.1540 and Y.1541 recommendations for different service classes expressed in terms of IP packet Loss Ratio (IPLR), IP packet Error Ratio (IPER), IP packet Transfer Delay (IPTD), and IP packet Delay Variation (IPDV).

As discussed in [5], SLAs commonly include requirements on:

– high network availability (e.g., of 99.99 %, or higher – like 99.999 % availability for telemonitoring, or telesurgery applications, also called the "five nines" property [23]),
– short time of service recovery after a failure. In particular, for stringent services, it is necessary to provide service recovery time below 50 ms [32] (which is compliant with the respective value of IPDV parameter for service classes 0 and 1 from Table 1.1).

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications and Networks, DOI 10.1007/978-3-319-22333-9_1

Table 1.1 Values of QoS parameters for different ITU-T service classes based on [29]

Class of service	Examples of applications	IPLR	IPER	IPTD	IPDV
Class 0	Real-time, jitter-sensitive, highly interactive	1×10^{-3}	1×10^{-4}	100 ms	50 ms
Class 1	Real-time, jitter-sensitive, interactive	1×10^{-3}	1×10^{-4}	400 ms	50 ms
Class 2	Transaction data, highly interactive	1×10^{-3}	1×10^{-4}	100 ms	*ND*
Class 3	Transaction data, interactive	1×10^{-3}	1×10^{-4}	400 ms	*ND*
Class 4	Low loss only (e.g., short transactions, bulk data, video streaming)	1×10^{-3}	1×10^{-4}	1 s	*ND*
Class 5	Traditional applications of default IP networks	*ND*	*ND*	*ND*	*ND*

ND not defined

Failures of nodes and links interrupting the normal functioning of communication networks are fairly common due to various reasons. Following [18], 20 % of failures in wired networks emerge from scheduled maintenance activities (for instance updates of the network architecture). Among the other (unplanned) failures, 70 % of them are failures of single links caused by unintentional cuts, e.g., due to dig-ups by third parties affecting links located underground. Quite often, such *random failures* simultaneously affect more than one link at a time (especially if several links, buried together in a duct, are cut at the same time).

The remaining 30 % of unplanned failures of links/nodes mostly refer to *disaster-based failures* identified in [8, 10, 22] as following from:

- natural disasters including e.g., earthquakes, floods, or fires,
- malicious attacks aimed to bring out severe losses at minimum cost (often causing failures of high-degree nodes, or high-capacity links serving most of the traffic),
- technology-related disasters implied by technological issues, such as Northeast Power Grid Blackout in the US.

They are all reported to affect more than one network element. Half of them are in turn related with links not connected to the same node [18]. Besides, the risk of large-scale failures due to natural disasters (or human-made disasters) is rising.

Disaster-based failures are far more dynamic and broader in scope than classical random failures. They commonly result in simultaneous failures of network elements located in specific geographic areas [13]. For instance, every year tens of hurricanes worldwide are responsible for power outages disrupting communications on a massive scale for a long time (10 days, on average) [10]. Hurricane Katrina that caused severe losses in Louisiana and Mississippi in Southeastern US in August 2005 [30] is only one of them.

Earthquakes are the reasons for even greater destructions due to long times of manual repair actions. A notable example – the 7.1-magnitude earthquake in December 2006 in Southern Taiwan resulted in simultaneous failures of seven submarine links visibly affecting the Internet connectivity between Asia and

North America for weeks. As a result, international communications to China, Taiwan, Hong Kong, Korea, and Japan immediately became not possible [30]. Similarly, the Greatest Japan Earthquake of 9.0 magnitude on March 11, 2011, caused a wide-scale damage to undersea cables, and impacted about 1500 telecom switching offices due to power outages [8].

Another important reason for disruptions of network nodes and links bounded in specific geographical areas refers to intentional human activities, e.g., bombing, use of weapons of mass destruction (WMD) attacks [1], as well as electromagnetic pulse (EMP) attacks. Such activities can obviously remarkably affect the ability of a network to fulfill the QoS requirements.

Based on the occurrence of disaster symptoms, disasters can be classified as predictable (e.g., hurricanes, or floods) and non-predictable (e.g., earthquakes) [24]. The general observation is that disaster-based failures are often cascading meaning that the initial failure of a certain network element (e.g., due to the earthquake) can next trigger the correlated failures in other parts of the network (e.g., due to power outages after the earthquake) [8].

Apart from failures characterized by long times of manual repair actions, about 50 % of failures are identified as transient (i.e., short-lived) and last less than a minute [25]. This refers, for example, to disruptions of communication paths observed in IP networks where routing protocols (e.g., Open Shortest Path First – OSPF) are able to reroute the traffic reactively upon the occurrence of a failure.

Other important scenarios of relatively short-lasting failures are attributed to wireless networks. For instance, Wireless Mesh Networks (WMNs) with stationary nodes connected by high-frequency wireless links often encounter time-varying weather-based disruptions partially or completely degrading the available link capacity (e.g., as a result of a heavy rain storm) [15]. In mobile Vehicular Ad-hoc NETworks (VANETs), lifetime of communication links (and thus also availability of links and end-to-end communication paths) is commonly measured in seconds due to high mobility of vehicles [16, 21].

Since failures cannot be completely eliminated, in order to reduce their negative impact on end-to-end routing, various redundancy techniques have been proposed so far to network routing to assure that a proper *alternate* (*backup*) *path* is available to redirect the traffic upon the failure affecting the *primary* (*working*) *path*. This is to assure *network resilience* against failures of links/nodes, defined in [30] as the ability of a network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. Traditionally, in order to provide protection against failures of single links/nodes, any backup path should not have common transit links/nodes with the primary path being protected.

In any failure scenario, in order to limit the service interruption time, it is important not only to reduce the time to redirect the affected traffic onto the alternate path (i.e., recovery switching actions optionally including calculation of alternate paths after the failure), but also focus on other steps of the recovery procedure shown in Fig. 1.1, commonly consisting of fault detection, fault localization, fault notification, and recovery switching [6, 22].

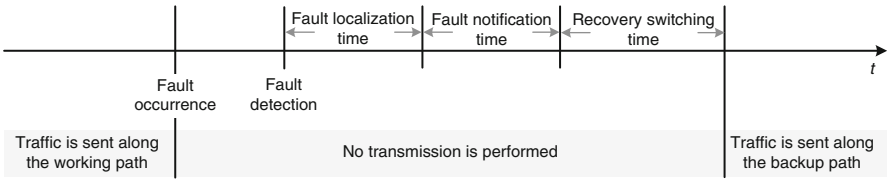

Fig. 1.1 Typical elements of a service recovery procedure

It is worth noting that network resilience has been recently identified as a separate aspect of quality provisioning, referred to as *Quality of Resilience* (*QoR*), focusing on QoS measures related to network resilience [6, 7]. Its emergency is justified by its importance to the society, as well as follows from a wide range of techniques providing differentiated Quality of Service to end users [29].

1.1 Motivations and Objectives of This Book

Issues of resilient routing have been extensively studied for scenarios of random failures related to single and multiple links/nodes mostly for wavelength division multiplexing (WDM) and IP-based wired network architectures. Example techniques available in the literature refer to end-to-end resilience [3, 26], dedicated protection [4, 28], shared protection [12, 31], multi-layer and multi-domain network resilience [11, 27], fault localization [17, 34], service resilience differentiation [6], or fast restoration issues [2, 19], as discussed in detail in Chap. 2 of this book.

However, protection against disaster-based correlated multiple failures is a topic that has not been paid much attention in the literature so far [13]. In particular, the role of network preparedness to predictable disasters such as heavy precipitation/floods, hurricanes, or earthquakes is expected to become more crucial in the nearest future owing to the observed increasing frequency of such phenomena. Communication networks need to be also adapted for resilient functioning in the disaster-prone environment characterized by the increased probability of droughts and fires (being result of the global warming) [24].

Since catastrophic failures can be caused not only by forces of nature but be also implication of human-made cyber attacks, terrorist attacks, or use of weapons of mass destruction, a proper understanding of disaster-based disruptions and cascading failures is of utmost importance [9]. It seems necessary to provide the networks with self-organizing capabilities to reduce the impact of disruptions on end-to-end routing as much as possible. If a disaster can be predicted beforehand, the network can be prepared in advance for it. In particular, this would mean e.g., re-allocation of network resources, re-dissemination of data, and updates of routing schemes.

Emerging new architectures of communication networks pose new challenges to resilient routing. In particular, the idea of the Future Internet (FI) is becoming content-centric, which raises the need to design new techniques of resilient routing providing content connectivity (the concept of Content Delivery Networks – CDNs, also known as content-aware networking/content-oriented networking (CAN/CON) paradigm, as opposed to the common network connectivity rule [33]). Other important issues of FI resilient communications that need extensive research are related to cloud computing/communications [14], or software-defined networking (SDN) [20].

Resilient routing schemes available in the literature are dedicated mostly to wired networks (e.g., IP-based, optical). In the case of wireless networks where fault-tolerant end-to-end communications is even harder to achieve due to time-varying characteristics of wireless links and nodes mobility, still too little has been done to improve their resilience. For instance, as mentioned before, Wireless Mesh Networks encounter link availability problems related to high frequency communications under heavy rain falls. This topic has been only marginally addressed so far with very few solutions proposed (see e.g., [15]).

Another important example refers to the concept of Vehicular Ad-hoc Networks, which is now seen by car manufacturers as a promising solution to a number of issues concerning public safety aspects (exchange of messages between vehicles in case of accidents, or bad weather conditions), traffic coordination (e.g., traffic light management to help the drivers move in the green phase), or infotainment (on-board information and entertainment services such as Internet access). Independent of the service type, urgent research issues are related with stability of end-to-end wireless communication paths over VANET links.

The objective of this book is to address the up-to-date issues of end-to-end resilient routing with special focus on:

- analysis of challenges commonly leading to failures of network elements,
- overview of available techniques of resilient routing,
- open problems of end-to-end resilient routing in emerging future architectures of communication networks, in particular related to the concept of the Future Internet, as well as wireless networks.

For each considered network architecture, new approaches proposed by the author are described and followed by evaluation of their characteristics.

The book is targeted at researchers and practitioners from both academia and industry interested in issues of end-to-end resilient routing related to contemporary and future architectures of communication networks. It can be also useful for third-level research students.

1.2 Content Organization

The remaining part of this book is structured into four main chapters as follows.

Chapter 2 outlines the state-of-the-art principles of communication networks resilience. It starts with a detailed analysis of challenges responsible for faults of network links and nodes. A number of resilience disciplines described next in Chap. 2 (including survivability, fault tolerance, traffic tolerance, and disruption tolerance) have emerged, as they result from diversity of discussed challenges leading to differentiated failure scenarios. Analysis of these disciplines is followed by a description of measurable characteristics of network resilience, including attributes of network dependability (such as reliability, or availability), security, and performability.

Later part of Chap. 2 presents an overview of existing resilient routing mechanisms that are based on utilization of alternate paths. Special focus is put on analysis of alternate path resource reservation techniques classified, e.g., based on backup path setup methods, scope of a recovery procedure, or usage of network resources. The chapter is concluded by a discussion on resilience issues in multi-domain and multi-layer communication environments, as well as identification of open problems.

Chapters 3, 4, and 5 present three differentiated scenarios related to resilient routing issues of emerging communication network architectures. In particular, in Chap. 3, we investigate resilience of Future Internet communications. This is an open issue, since current Internet, originally designed around 40 years ago, still remains in common use. Many research teams are now working in parallel to define the foundations of the new Internet. As already mentioned, among a number of Future Internet concepts worked out so far, a significant part of them focus on content (information) connectivity rather than on network connectivity – i.e., the basis for Content Delivery Networks. In terms of resilience, it translates into possibility to provide access to content not only under random failures of network nodes hosting the content, but also in the face of malicious human activities or disaster-based failures.

Chapter 3 starts with a detailed analysis of current Internet challenges, as well as design goals for the Future Internet architecture in particular related to FI resilience. To support differentiated requirements, the concept of virtualization is described that allows for the deployment of Parallel Internet (PI) architectures utilizing common network resources. Later part of Chap. 3 presents our four original contributions. The first one is the scheme of resource provisioning for the Future Internet architecture defined in terms of three Integer Linear Programming (ILP) models that allows for fair allocation of network resources (link capacities and processing power of nodes) to Parallel Internets using the concept of virtualization.

Next three proposals refer to resilience of content-oriented networking. First two of them are to provide resilient routing against random failures under the assumption that the same information can be replicated and accessible at several replica servers. In particular, anycast routing concept is extended here to provide protection against failures of destination nodes (which is not possible for the common unicast transmission scheme). Introduced ILP models as well as heuristic algorithms are designed for two variants of dedicated and shared protection, accordingly. Chapter 3 is concluded by a proposal of a new anycast routing technique aimed at

achieving the substantial reduction of a number of affected end-to-end flows being result of malicious activities targeted at high-degree nodes.

Protection against disaster-based failures is extensively addressed in Chap. 4 presenting the respective solutions for Wireless Mesh Networks commonly formed by stationary mesh routers inter-connected by wireless links. High-frequency communications (e.g., using the 71–86 GHz band) is the reason for vulnerability of WMNs to weather-based disruptions, in particular to intensive precipitation. Therefore, heavy rain falls may seriously reduce (or even completely degrade) the available link capacity. Since rain falls usually occur in certain regions, and thus simultaneously affect multiple WMN links located inside a given region, the considered case is a good example of region-based disruptions leading to correlated failures.

Apart from highlighting the threats to end-to-end resilient routing in WMNs, Chap. 4 includes two original contributions. The first one is a set of measures of WMN resilience to region-based disruptions, i.e., region failure survivability function – RFS, *p*-fractile region survivability function – PFRS, and the expected percentage of total flow delivered after a region failure (EPFD). The respective methodology of calculating these measures is described and is followed by analysis of their characteristics. Results of evaluation show that the introduced measures give adequate and consistent information, as well as can be used to compare vulnerability of different WMNs to region-based disruptions.

The second proposal described in Chap. 4 is related with a new transmission scheme that allows to prepare the WMN topology in advance to the forecasted heavy rain falls. By using the dynamic antenna alignment features (functionality offered by a number of WMN equipment vendors), the network can update "a priori" configuration of its links to reduce the extent of losses under heavy rain falls. This means automatic creation (or deletion) of WMN links in certain areas, if low (or high) signal attenuation is forecasted based on radar echo rain maps. Results of simulations obtained for real scenarios of rain falls show that the proposed approach is able to provide a significant reduction of signal attenuation, compared to the reference scheme of not changing the alignment of WMN antennas.

The last communications scenario is related with resilience of end-to-end routing in VANETs and presented in Chap. 5. This novel concept of wireless mobile networks organized in ad-hoc manner encounters link availability problems due to high mobility of vehicles. The problem becomes even more difficult, if stability of end-to-end multi-hop paths is concerned. Currently, there are practically no proposals in the literature addressing this issue.

In Chap. 5, we describe our two approaches to resilient end-to-end routing in VANETs that help to remarkably increase the lifetime of end-to-end communication paths. The first one is designed to provide differentiated protection paths based on investigated classes of service. In particular, it adjusts the number of utilized disjoint paths to meet the requirements on end-to-end communications availability. Simulations results show that due to: (1) multipath routing, (2) use of a novel metric of link costs based on link stability information, as well as (3) calculation of the alternate path immediately after detecting the interruption of a single transmission path, our scheme is able to maintain the end-to-end connectivity in a failure-prone environment.

The second scheme proposed in Chap. 5 extends the concept of anypath routing to improve probability of end-to-end message delivery, as well as utilizes a new metric of link costs to select stable links in message forwarding decisions. This approach is also one of the few available to improve the lifetime of the main communication path.

Chapter 5 is followed by general conclusions, also including comments on open research issues.

References

1. Agarwal, P.K., Efrat, A., Ganjugunte, S.K., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. IEEE/ACM Trans. Networking **21**(5), 1525–1538 (2013)
2. Alicherry, M., Bhatia, R.: Simple pre-provisioning scheme to enable fast restoration. IEEE/ACM Trans. Networking **15**(2), 400–412 (2007)
3. Autenrieth, A., Kirstadter, A.: Engineering end-to-end IP resilience using resilience-differentiated QoS. IEEE Commun. Mag. **40**(1), 50–57 (2002)
4. Azodolmolky, S., Klinkowski, M., Pointurier, Y., Angelou, M., Careglio, D., Sole-Pareta, J., Tomkos, I.: A novel offline physical layer impairments aware RWA algorithm with dedicated path protection consideration. IEEE/OSA J. Lightwave Technol. **28**(20), 3029–3040 (2010)
5. Bonaventure, O., Filsfils, C., Francois, P.: Achieving sub-50 milliseconds recovery upon BGP peering link failures. IEEE/ACM Trans. Networking **15**(5), 1123–1135 (2007)
6. Chołda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J.: A survey of resilience differentiation frameworks in communication networks. IEEE Commun. Surv. Tutorials **9**(4), 32–55 (2007)
7. Chołda, P., Tapolcai, J., Cinkler, T., Wajda, K., Jajszczyk, A.: Quality of Resilience as a network reliability characterization tool. IEEE Netw. **23**(2), 11–19 (2009)
8. Dikbiyik, F., Tornatore, M., Mukherjee, B.: Minimizing the risk from disaster failures in optical backbone networks. IEEE/OSA J. Lightwave Technol. **32**(18), 3175–3183 (2014)
9. Dinh, T.N., Thai, M.T.: Network under joint node and link attacks: vulnerability assessment method and analysis. IEEE/ACM Trans. Networking **23(3)**, 1001–1011 (2014)
10. Goścień, R., Walkowiak, K., Klinkowski, M., Rak, J.: Protection in elastic optical networks. IEEE Network, 1–15 (to appear in 2016)
11. Gunkel, M., Autenrieth, A., Neugirg, M., Elbers, J.: Advanced multilayer resilience scheme with optical restoration for IP-over-DWDM core networks. In: Proceedings of the 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT'12), pp. 657–662 (2012)
12. Guo, L., Cao, J., Yu, H., Li, L.: Path-based routing provisioning with mixed shared protection in WDM mesh networks. IEEE/OSA J. Lightwave Technol. **24**(3), 1129–1141 (2006)
13. Habib, M.F., Tornatore, M., De Leenheer, M., Dikbiyik, F., Mukherjee, B.: Design of disaster-resilient optical datacenter networks. IEEE/OSA J. Lightwave Technol. **30**(16), 2563–2573 (2012)
14. Harter, I.B.B., Hoffmann, M., Schupke, D.A., Carle, G.: Scalable resilient virtual network design algorithms for cloud services. In: Proceedings of the 6th International Workshop on Reliable Networks Design and Modeling (RNDM'14), pp. 123–130 (2014)
15. Jabbar, A., Rohrer, J.P., Oberthaler, A., Cetinkaya, E.K., Frost, V., Sterbenz, J.P.G.: Performance comparison of weather disruption-tolerant cross-layer routing algorithms. In: Proc. 28th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'09), pp. 1143–1151 (2009)

16. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., Weil, T.: Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards, and solutions. IEEE Commun. Surv. Tutorials **13**(4), 584–616 (2011)
17. Khair, M., Kantarci, B., Zheng, J., Mouftah, H.T.: Performance optimization for fault localization in all-optical networks. In: Proceedings of the 5th International Conference on Broadband Communications, Networks and Systems (BROADNETS'08), pp. 531–535 (2008)
18. Kini, S., Ramasubramanian, S., Kvalbein, A., Hansen, A.F.: Fast recovery from dual-link or single-node failures in IP networks using tunneling. IEEE/ACM Trans. Networking **18**(6), 1988–1999 (2010)
19. Kodialam, M., Lakshman, T.V., Sengupta, S.: Guaranteed performance routing of unpredictable traffic with fast path restoration. IEEE/ACM Trans. Networking **17**(5), 1427–1438 (2009)
20. Kreutz, D., Ramos, F.M.V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**(1), 14–76 (2015)
21. Li, F., Wang, Y.: Routing in vehicular ad hoc networks: a survey. IEEE Veh. Technol. Mag. **2**(2), 12–22 (2007)
22. Mas, C., Tomkos, I., Tonguz, O.K.: Failure location algorithm for transparent optical networks. IEEE J. Sel. Areas Commun. **23**(8), 1508–1519 (2005)
23. Menth, M., Martin, R.: Network resilience through multi-topology routing. In: Proc. of the 5th International Workshop on Design of Reliable Communication Networks (DRCN'05), pp. 271–277 (2005)
24. Mukherjee, B., Habib, M.F., Dikbiyik, F.: Network adaptability from disaster disruptions and cascading failures. IEEE Commun. Mag. **52**(5), 230–238 (2014)
25. Nelakuditi, S., Lee, S., Yu, Y., Zhang, Z.-L., Chuah, C.-N.: Fast local rerouting for handling transient link failures. IEEE/ACM Trans. Networking **15**(2), 359–372 (2007)
26. Pandi, A., Tacca, M., Fumagalli, A.: A threshold based on-line RWA algorithm with end-to-end reliability guarantees. In: Proc. International Conference on Optical Networks Design and Modeling (ONDM'05), pp. 447–453 (2005)
27. Schupke, D.A.: Multilayer and multidomain resilience in optical networks. Proc. IEEE **100**(5), 1140–1148 (2012)
28. Soproni, P., Babarczi, P., Tapolcai, J., Cinkler, T., Ho, P.H.: A meta-heuristic approach for non-bifurcated dedicated protection in WDM optical networks. In: Proc. 8th International Workshop on Design of Reliable Communication Networks (DRCN'11), pp. 110–117 (2011)
29. Stankiewicz, R., Chołda, P., Jajszczyk, A.: QoX: what is it really? IEEE Commun. Mag. **49**(4), 148–158 (2011)
30. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schoeller, M., Smith, P.: Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Comput. Netw. **54**(8), 1245–1265 (2010). Elsevier
31. Tapolcai, J., Ho, P.-H., Verchere, D., Cinkler, T., Haque, A.: A new shared segment protection method for survivable networks with guaranteed recovery time. IEEE Trans. Reliab. **57**(2), 272–282 (2008)
32. Vasseur, J.P., Pickavet, M., Demeester, P.: Network Recovery: Protection and Restoration of Optical, SONET-SDH, and MPLS. Morgan Kaufmann, San Francisco (2004)
33. Wang, Y., Ma, Ch., Li, X., Zhao, Y., Zhang, Y.: Node protection method with content-connectivity against disaster in disaster recovery center networks. In: Proceedings of the 13th International Conference on Optical Communications and Networks (ICOCN'14), pp. 1–4 (2014)
34. Wu, B., Ho, P.-H., Yeung, K.L., Tapolcai, J., Mouftah, H.T.: Optical layer monitoring schemes for fast link failure localization in all-optical networks. IEEE Commun. Surv. Tutorials **13**(1), 114–125 (2011)