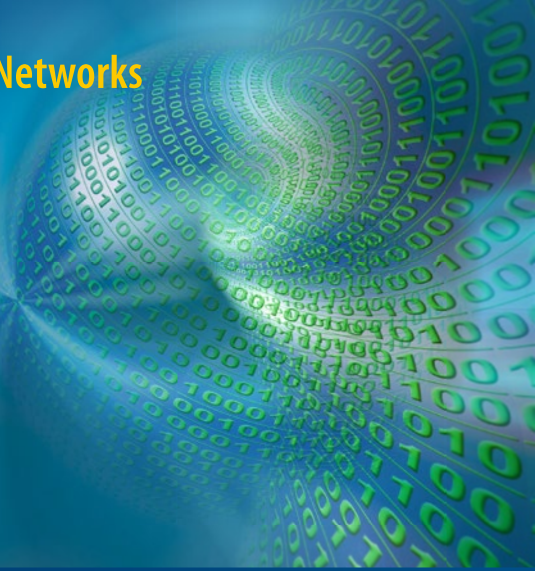
Computer Communications and Networks



Jacek Rak

# Resilient Routing in Communication Networks

Springer

# Computer Communications and Networks

**Series editor**
A.J. Sammes
Centre for Forensic Computing
Cranfield University, Shrivenham campus
Swindon, UK

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Jacek Rak

# Resilient Routing in Communication Networks

Springer

Jacek Rak
Faculty of Electronics, Telecommunications,
and Informatics
Gdansk University of Technology
Gdansk, Poland

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-22332-2 ISBN 978-3-319-22333-9 (eBook)
DOI 10.1007/978-3-319-22333-9

Library of Congress Control Number: 2015945628

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

*To the memory of*
*my grandfather Jan Rak*

# Preface

Since the introduction of the Internet in the 1970s of the past century, the concept of global communications has notably changed our daily activities. Communication networks, providing access to products and services at any time and location, have become the key elements of a critical infrastructure our everyday life depends on. Therefore, they are expected to offer uninterrupted service in the presence of various challenges. However, as their effective capacity is predicted to increase to accommodate the more-or-less exponentially growing demand volumes, the cost of failures of network elements is forecasted to rise as well.

Communication networks resilience is undoubtedly a complex issue. For any network architecture, a proper understanding of network challenges, including natural threats, as well as malicious human activities, is thus a necessity to introduce the appropriate preventive mechanisms related to end-to-end communications resilience – the topic addressed in this book.

The target audience includes researchers and professionals in the area of resilience and dependability of current and emerging communication technologies. The content can be also valuable for advanced-level students interested in this research area.

A significant part of work presented here has been carried out in the Department of Computer Communications of the Faculty of Electronics, Telecommunications, and Informatics of Gdansk University of Technology, Poland, as well as during my visits to a number of research centres over the years 2010–2015. In particular, a remarkable share of the content of this book is the implication of discussions during my scholarships, scientific visits, invited lectures, and seminar talks at: Concordia University, Montreal, Canada (Concordia Research Chair Optimization of Communication Networks lead by Brigitte Jaumard); Osaka University, Japan (Photonic Networks Laboratory lead by Ken-ichi Kitayama); National Institute of Information and Communications Technology (NICT) Tokyo, Japan; Ghent University-iMinds (lead by Piet Demeester); Technical University of Munich (Chair of Communication Networks lead by Wolfgang Kellerer); and Halmstad University, Sweden (CERES centre with the leadership of Magnus Jonsson).

A notable part of my works has been done in co-operation with many great researchers, in particular (without the intention of forgetting anyone): Javier Alonso Lopez (University of Leon, Spain), Piotr Chołda (AGH University of Science and Technology, Poland), Tibor Cinkler (Budapest University of Technology and Economics, Hungary), Egemen K. Çetinkaya (The University of Kansas, US/Missouri University of Science and Technology, US), Georgios Ellinas (University of Cyprus), Teresa Gomes (University of Coimbra, Portugal), Róża Goścień (Wrocław University of Technology, Poland), Janusz Gozdecki (AGH University of Science and Technology, Poland), Matthias Gunkel (Deutsche Telekom, Germany), Brigitte Jaumard (Concordia University, Canada), Mirosław Kantor (AGH University of Science and Technology, Poland/University of Luxembourg), Mirosław Klinkowski (National Institute of Telecommunications, Poland), Arie Koster (RWTH Aachen, Germany), Yevgeni Koucheryavy (Tampere University of Technology, Finland), Wojciech Molisz (Gdansk University of Technology, Poland), Hussein Mouftah (Ottawa University, Canada), Krzysztof Walkowiak (Wrocław University of Technology, Poland), Dimitri Papadimitriou (Alcatel-Lucent Bell Labs, Belgium), Mario Pickavet (Ghent University-iMinds, Belgium), Michał Pióro (Warsaw University of Technology, Poland/Lund University, Sweden), Gangxiang Shen (Soochow University, China), Peter Soproni (Budapest University of Technology and Economics, Hungary), Dimitri Staessens (Ghent University-iMinds, Belgium), James P.G. Sterbenz (The University of Kansas, US/Lancaster University, UK/The Hong Kong Polytechnic University, Hong Kong), David Tipper (Pittsburgh University, US), Kishor Trivedi (Duke University, US), Alexey Vinel (Halmstad University, Sweden), Krzysztof Wajda (AGH University of Science and Technology, Poland), Rolland Wessäly (atesio GmbH, Germany), Jozef Wozniak (Gdansk University of Technology, Poland), and Wen-De Zhong (Nanyang Technological University, Singapore).

Gdansk, Poland Jacek Rak

# Contents

# List of Symbols

$A$ Set of directed arcs used to represent the network links

$A_{nn}$ Node-to-node incidence matrix

$a_h$ Directed arc

$BC(n)$ Betweenness centrality coefficient for node $n$

$b_h$ Amount of capacity to be reserved at arc $a_h$ for backup paths under backup capacity sharing

$b_{h,g}$ Total capacity needed for backup paths at arc $a_h$ in the case of shared protection provided for working paths traversing the failed arc $a_g$

$b_{r,h,g}$ Binary variable to indicate whether for $r$-th demand the failed primary path traverses arc $a_g$ and the corresponding backup path traverses arc $a_h$

$c_h$ Total capacity of arc $a_h$

$c_h(t)$ Capacity of arc $a_h$ available at time $t$

$\overline{c_h}$ Unused capacity of arc $a_h$

$\breve{c}_{m,h}$ The lower bound on capacity required at arc $a_h$ for $m$-th instance of Parallel Internet

$c_r$ Minimal residual capacity along links of the calculated path of $r$-th demand

$\overline{c_r}$ Capacity to be reserved for $r$-th demand along links traversed by the respective path

$D$ Set of demands

$D_m$ Set of demands for $m$-th instance of Parallel Internet

$D^{AN}$ Set of anycast demands

$D^{DS}$ Set of anycast downstream demands

$D_{nn}$ Node-to-node matrix of demanded capacities (for end-to-end flows)

$D^{UN}$ Set of unicast demands

$D^{US}$ Set of anycast upstream demands

$d_r$ Volume of the $r$-th demand

$d_{r,m}$ Volume of $r$-th demand from $m$-th instance of Parallel Internet

| | |
|---|---|
| $EPFD\left(\hat{\hat{r}}\right)$ | Expected percentage of total flow delivered after a failure |
| $F[\psi]$ | Auxiliary function providing information on the frequency a given percentage $\psi$ of flows ($\psi\in\{0,1,\ldots, 100\}$) is successfully delivered after region failures |
| $f$ | Total flow transported before occurrence of a failure (in a normal state) |
| $\hat{f}$ | The aggregate flow restored after a region failure |
| $G$ | Arbitrarily chosen large value |
| $(i, J)$ | VANET hyperlink between vehicle $i$ and the set of forwarding vehicles $J$ |
| $J$ | Set of forwarding vehicles in VANET anypath communications |
| $k$ | Degree of a network node |
| $L$ | Set of transmission channels |
| $N$ | Set of network nodes |
| $n$ | Network node |
| $N\backslash T$ | Set of edge nodes |
| $PFRS(p)$ | $p$-fractile region survivability |
| $P\left(\hat{\hat{r}}_n\right)$ | Probability of node $n$ failure in a region failure scenario |
| $P(\delta)$ | Probability of occurrence of a failure scenario $\delta$ |
| $p$ | Probability of successful delivery of flows after a region failure |
| $p_h$ | The upper bound on transmission delay along arc $a_h$ |
| $p_{i,J}$ | Probability of delivering the packet from vehicle $i$ to at least one node from forwarding vehicles $J$ |
| $p_{i,j}$ | Layer 2 probability of packet delivery via VANET link $(i, j)$ |
| $p_{m,r}$ | The upper bound on end-to-end transmission delay for $r$-th demand from $m$-th instance of Parallel Internet |
| $p(r_{i,j})$ | Probability density function of inter-vehicle distance |
| $p_{\Psi}(\psi)$ | Probability density function of percentage $\psi$ of flows surviving the region failure |
| $p_{\Psi}\left(\psi, \hat{\hat{r}}\right)$ | Probability density function of $\Psi$ defined for region failures of radius $\hat{\hat{r}}$ |
| $P_i(t)$ | Probability that a system is in state $i$ at time $t$ |
| $RFS(\psi)$ | Region failure survivability function |
| $R_p$ | Rain rate in mm/h |
| $r$ | Index of a demand |
| $r_{i,j}$ | Distance between nodes $i$ and $j$ |
| $\hat{\hat{r}}$ | Radius of a failure region |
| $\hat{\hat{r}}_{\max}$ | Maximum analyzed radius of a failure region |
| $\hat{\hat{r}}_n$ | Distance between node $n$ and the failure epicentre |
| $s_h$ | Length of arc $a_h$ |
| $sh_h^{(r)}$ | Capacity reserved so far at $a_h$ that may be shared with respect to backup path of $r$-th demand (continuous) |
| $S_{\boldsymbol{i}}(t_0, \Delta t)$ | Movement vector of vehicle $i$ in time interval $(t_0, t_0+\Delta t)$ |
| $s_i^x(t_0, \Delta t)$ | Movement of vehicle $i$ in time interval $(t_0, t_0+\Delta t)$ along X axis |

| | |
|---|---|
| $s_i^y(t_0, \Delta t)$ | Movement of vehicle $i$ in time interval $(t_0, t_0+\Delta t)$ along Y axis |
| $s_{i,j}$ | Stability index of a VANET link $(i, j)$ |
| $sp(p, q)$ | Number of the shortest paths between nodes $p$ and $q$ (of the same minimal length) |
| $sp_n(p, q)$ | Number of the shortest paths between nodes $p$ and $q$ (of the same minimal length) traversing node $n$ |
| $s_r$ | Source node of $r$-th demand |
| $s_{r,m}$ | Source node of $r$-th demand from $m$-th instance of Parallel Internet |
| $T$ | Set of transit nodes |
| $\breve{T}$ | Lifetime of a network |
| $t_r$ | Destination node of $r$-th demand |
| $t_{r,m}$ | Destination node of $r$-th demand from $m$-th instance of Parallel Internet |
| $u_n$ | Binary variable to indicate that node $n$ is a replica node |
| $\boldsymbol{v_i}(t)$ | Velocity vector of vehicle $i$ at time $t$ |
| $v_i^x(t)$ | Velocity of vehicle $i$ at time $t$ along X axis |
| $v_i^y(t)$ | Velocity of vehicle $i$ at time $t$ along Y axis |
| $v_{r,m,h}$ | Binary variable used to indicate whether arc $a_h$ is forwarding the traffic referring to $r$-th demand of $m$-th instance of Parallel Internet |
| $v_{r,n}$ | Binary variable to indicate whether a replica server located at node $n$ is selected as a backup replica of $r$-th anycast demand |
| $w_{i,j}$ | Probability of node $j$ being the forwarding node of a packet received from vehicle $i$ |
| $W$ | Set of states in which the system is considered as available |
| $x^l_{r,h}$ | Binary variable to determine if $l$-th channel is assigned for $r$-th demand path at arc $a_h = (i, j)$; 0 otherwise |
| $x_{r,h}$ | Binary variable indicating utilization of arc $a_h$ by a working path of $r$-th demand |
| $(\bar{x}_n, \bar{y}_n)$ | X and Y axis coordinates of node $n$ |
| $\left(\widehat{\bar{x}}, \widehat{\bar{y}}\right)$ | X and Y axis coordinates of the failure epicentre |
| $x_{m,h}$ | Capacity assigned for $m$-th instance of Parallel Internet at arc $a_h$ (in MFlops) |
| $y_{r,h}$ | Binary variable indicating utilization of arc $a_h$ by a backup path of $r$-th demand |
| $z_{r,m,h}$ | Capacity assigned at arc $a_h$ for $r$-th demand of $m$-th instance of Parallel Internet |
| $\Gamma(N, A)$ | Graph representing a directed network |
| $\gamma$ | Exponent in power law distribution of node degrees |
| $\gamma\left(\breve{T}\right)$ | Link cost function based on signal attenuation ratio at time $t \in \breve{T}$ |
| $\delta$ | Region failure scenario given by the set of non-operational nodes after the outage |
| $\zeta_h$ | Cost per unit flow of each commodity on arc $a_h$ for backup paths (if different from $\xi_h$) |

| | |
|---|---|
| $\eta_i$ | $i$-th disjoint path |
| $\mathit{\Theta}$ | Length of the path over which the rain is observed |
| $\theta_{m,h}$ | Consumption of node processing power measured per unit capacity for $m$-th instance of Parallel Internet defined for outgoing arc $a_h$ |
| $\kappa_{r,n}$ | Binary variable to indicate if a replica server located at node $n$ is selected as a working replica of $r$-th anycast demand |
| $\mathit{\Xi}$ | Matrix of arc costs |
| $\xi_h$ | Cost per unit flow of each commodity at arc $a_h$ |
| $\widetilde{\pi}_n$ | Probability of existence of a VANET path consisting of $k_n$ links |
| $\rho_h$ | Probability that two vehicles are connected by a wireless link $a_h$ at any time |
| $\rho_{m,h}$ | Consumption of node processing power measured per unit capacity for $m$-th instance of Parallel Internet defined for incoming arc $a_h$ |
| $\sigma_J$ | Cost of a VANET anypath from set $J$ to the destination node |
| $\sigma_{i,J}$ | Cost of a VANET hyperlink $(i, J)$ |
| $\sigma_{i,t}$ | Cost of a VANET path between nodes $i$ and $t$ |
| $\tau$ | Time interval between two consecutive updates of a WMN topology |
| $\tau(r)$ | Index of a demand associated with $r$-th demand |
| $\mathit{\Phi}_i(t)$ | Position vector of vehicle $i$ at time $t$ |
| $\vartheta\left(\breve{T}\right)$ | Function determining existence of links at time $t \in \breve{T}$ |
| $\varphi(\boldsymbol{x})$ | Objective function |
| $\phi_n$ | Aggregate processing power at node $n$ |
| $\chi_{r,n}$ | Binary variable to indicate that node $n$ is the closest replica for anycast $r$-th demand |
| $\mathit{\Psi}(\delta)$ | Random variable referring to the percentage $\psi$ of flows delivered in scenario $\delta$ |
| $\widetilde{\mathit{\Psi}}_m$ | Probability of multipath VANET transmission availability (by means of $m$ paths) |
| $\psi$ | Percentage of flows surviving the region failures |
| $\mathit{\Omega}$ | Signal attenuation in dB |
| $\omega_h$ | Estimated signal attenuation for arc $a_h$ |
| $\omega_h(t)$ | Estimated signal attenuation for arc $a_h$ at time $t$ |
| $\wp_{m,n}$ | Amount of resources reserved to process flows from $m$-th instance of Parallel Internet at node $n$ |

# Acronyms

| | |
|---|---|
| 3G | Third generation |
| 4G | Fourth generation |
| ADM | Add-Drop Multiplexer |
| AODV | Ad-hoc On demand Distance Vector |
| APF | Active Path First |
| APS | Automatic Protection Switching |
| ATM | Asynchronous Transfer Mode |
| BC | Betweenness centrality |
| BER | Bit Error Rate |
| BLSR | Bi-directional Line Switched Ring |
| C2C-CC | Car-to-Car Communications Consortium |
| CAM | Cooperative Awareness Message |
| CAN | Content-Aware Networking |
| CCH | Control Channel |
| CCN | Content-Centric Networking |
| CDN | Content Delivery Network |
| CoS | Class of Service |
| CON | Content-Oriented Networking |
| CPU | Central Processing Unit |
| DDoS | Distributed Denial of Service |
| DNS | Domain Name System |
| DSRC | Dedicated Short Range Communications |
| DSS | Data Stream Switching |
| DWDM | Dense Wavelength Division Multiplexing |
| EMP | Electromagnetic Pulse (attack) |
| ETSI | European Telecommunications Standards Institute |
| FCC | Federal Communications Commission |
| FI | Future Internet |
| FIA | Future Internet Assembly |

| | |
|---|---|
| FIT | Failures in time |
| Gb/s | Gigabit per second |
| GHz | Gigahertz |
| GMPLS | Generalized Multiprotocol Label Switching |
| GPS | Global Positioning System |
| HTTP | Hypertext Transfer Protocol |
| ICN | Information-Centric Networking |
| IETF | Internet Engineering Task Force |
| IFIP | International Federation for Information Processing |
| ILP | Integer Linear Programming |
| InP | Infrastructure Provider |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPDV | IP packet Delay Variation |
| IPER | IP packet Error Ratio |
| IPLR | IP packet Loss Ratio |
| IPTD | IP packet Transfer Delay |
| IPv6 | Internet Protocol version 6 |
| ISP | Internet Service Provider |
| ITU-T | International Telecommunication Union – Telecommunication Standardization Sector |
| IVC | Inter-Vehicular Communications |
| LOS | Line of Sight |
| LP | Linear Programming |
| LSA | Link State Advertisement |
| LSP | Label Switched Path |
| MAC | Media Access Control |
| Mb/s | Megabit per second |
| MDT | Mean Downtime |
| MFlop | Mega Floating-point operations |
| MIMO | Multiple-input multiple-output |
| MIVC | Multi-hop Inter-Vehicular Communications |
| MPLS | Multiprotocol Label Switching |
| MTBF | Mean Time Between Failures |
| MTBI | Mean Time Between Interruptions |
| MTFF | Mean Time to First Failure |
| MTRS | Mean Time to Restore Service |
| MTTF | Mean Time to Failure |
| MTTR | Mean Time to Repair/Recovery |
| MUT | Mean Uptime |
| NDO | Named Data Object |
| NNI | Network-Network Interface |
| NVE | Network Virtualization Environment |
| OBU | On-Board Unit |
| OSPF | Open Shortest Path First |

| | |
|---|---|
| OXC | Optical Cross Connect |
| P2P | Peer-to-peer |
| PDR | Packet Delivery Ratio |
| PER | Packet Error Rate |
| PHY | Physical Layer |
| PIA | Percent of IP service Availability |
| PIU | Percent of IP service Unavailability |
| PLR | Packet Loss Ratio |
| POI | Point of Interest |
| PWCE | Protected Working Capacity Envelope |
| QoR | Quality of Resilience |
| QoS | Quality of Service |
| RFC | Request for Comments |
| RREP | Route Response |
| RREQ | Route Request |
| RSU | Road-Side Unit |
| SCH | Service Channel |
| SDH | Synchronous Digital Hierarchy |
| SDN | Software-Defined Networking |
| SIVC | Single-hop Inter-Vehicular Communications |
| SLA | Service Level Agreement |
| SLB | Service Loss Block |
| SNR | Signal-to-Noise Ratio |
| SONET | Synchronous Optical Network |
| SP | Service Provider |
| SRLG | Shared Risk Link Group |
| TCP | Transmission Control Protocol |
| TDM | Time Division Multiplexing |
| UNI | User-Network Interface |
| UPSR | Unidirectional Path-Switched Ring |
| V2I | Vehicle-to-Infrastructure |
| V2V | Vehicle-to-Vehicle |
| VANET | Vehicular Ad-hoc NETwork |
| VLAN | Virtual Local Area Network |
| VN | Virtual Network |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| VRU | Vulnerable Road User |
| VSCC | Vehicle Safety Communications Consortium |
| WDM | Wavelength Division Multiplexing |
| WMD | Weapons of Mass Destruction |
| WMN | Wireless Mesh Network |
| WSN | Wireless Sensor Network |

# 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 | $1 \times 10^{-3}$ | $1 \times 10^{-4}$ | 100 ms | 50 ms |
| Class 1 | Real-time, jitter-sensitive, interactive | $1 \times 10^{-3}$ | $1 \times 10^{-4}$ | 400 ms | 50 ms |
| Class 2 | Transaction data, highly interactive | $1 \times 10^{-3}$ | $1 \times 10^{-4}$ | 100 ms | *ND* |
| Class 3 | Transaction data, interactive | $1 \times 10^{-3}$ | $1 \times 10^{-4}$ | 400 ms | *ND* |
| Class 4 | Low loss only (e.g., short transactions, bulk data, video streaming) | $1 \times 10^{-3}$ | $1 \times 10^{-4}$ | 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].

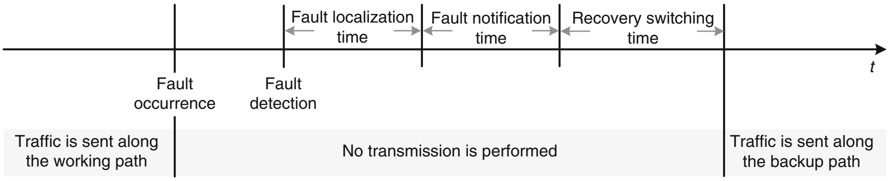

Fault localization time
Fault notification time
Recovery switching time
t
Fault occurrence
Fault detection
Traffic is sent along the working path
No transmission is performed
Traffic is sent along the backup path

**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)

# Chapter 2
# Principles of Communication Networks Resilience

Faults of communication network elements are inevitable. As indicated in the previous chapter, they may occur as a consequence of various challenges, including forces of nature (e.g., hurricanes, earthquakes), human errors (e.g., cable cuts), or malicious attacks, just to mention a few. Despite a visible diversity of their characteristics, they share a common feature: there is no way to eliminate them.

Our daily routines, becoming more and more dependent on communication networks services, are responsible for the exponential growth of exchanged information. As a consequence, emerging failures of network links (or nodes) bring about significant data and revenue losses. With the continuously observed extension of communication networks reach toward supporting almost all activities of our society, the negative consequences of failures are only expected to increase.

Majority of routing disruptions in communication networks follow from accidental faults of links/switching devices [27, 36], including, e.g., cable cuts by street works (mostly dig-ups), underwater cable damages by fishing vessels, or power supply faults. Following [22], failures of single links play the major role in wide-area networks covering about 70 % of all failure events. In long-haul networks, for every 10 km of a fiber link, a cable cut occurs once every 12 years [60].

Link failures can sometimes last several days/weeks and thus be responsible for a remarkable degradation of the network performance. The problem gets more complicated in wireless networks due to time dependency of link characteristics on various factors, also including weather-based disruptions. However, in local area networks with wired links, the share of node failures over all failures is commonly greater due to possibility to provide a better physical protection of shorter links. Localization of faults followed by necessary repairs of links (or nodes) can take hours to days, implying severe disruptions to network-dependent services.

Therefore, there is a justified need to develop the network mechanisms of automatic reconfiguration, in particular being responsible for restoration of network services until faults of network elements are physically repaired. Without any built-in mechanism to provide recovery of the affected traffic, a significant part of

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications and Networks, DOI 10.1007/978-3-319-22333-9_2

a network may shortly become useless from the clients perspective. This in turn brings us to the topic of network resilience addressed in detail in this chapter.

The remaining part of this chapter is organized in the following way. In order to deal with faults of network elements, it is necessary to analyze first the challenges responsible for their occurrence. This is the main aim of Sect. 2.1 presenting classification of challenges, followed by spatial and temporal analysis of their influence, and analysis of their correlation with various challenge categories.

However, diversity of challenge characteristics makes the task of real-time challenge identification rather complex, and often requiring a multi-stage approach, as described in the later part of Sect. 2.1. It is also crucial to identify the intermediate events occurring before any service failure, i.e., faults and errors referring to network elements, which is indispensable to provide the real-time response of network recovery mechanisms.

Diversity of communication network technologies, as well as of challenges bringing about differentiated failure scenarios, is the reason for existence of a number of network resilience disciplines described in detail in Sect. 2.2 referring to network design approaches to provide service continuity (in particular including survivability, fault tolerance, traffic tolerance, and disruption tolerance mechanisms). Analysis of communication networks resilience can be in turn performed using measurable characteristics, i.e., attributes of network dependability (such as reliability and availability), security, or performability – all related to the perceived service quality, and included in recommendations of International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) and Internet Engineering Task Force (IETF), as described later in Sect. 2.2.

Since the main aim of this book is to focus on design of end-to-end resilient routing schemes, the core part of this chapter (i.e., Sect. 2.3) presents an overview of resilient routing mechanisms available in the literature mainly based on the utilization of alternate paths to deliver the traffic in case of faults of network elements affecting the primary transmission paths. In particular, the appropriate signalling procedure described in the first part of Sect. 2.3, including fault detection, fault localization, and isolation followed by fault notification messages, is required to redirect the affected traffic onto the alternate paths.

As given in Sect. 2.3.1, recent service recovery techniques have been mostly designed for topologies of mesh networks and originated from the respective ones proposed for ring-based optical networks. Independent of network characteristics, alternate paths, although providing automatic recovery after faults, always require additional network resources (commonly related to link capacities).

Section 2.3.2 presents classification of alternate paths resource reservation mechanisms based on numerous criteria, the most important ones including: backup path setup methods, scope of a recovery procedure, as well as usage of network resources. Special focus is put on presentation of techniques of sharing the alternate paths resources to decrease the amount of link capacity required to install the alternate paths. In general, a trade-off can be observed between the resulting ratio of additional resources and the time needed to activate the alternate paths. Presentation of the main techniques of alternate paths computation is also extended by a discussion on the resulting computational complexity.

Providing resilience of end-to-end transmission often implies problems related to multi-domain routing, i.e., routing across multiple domains each one determined based on geographical scope or ownership, as stated in the later part of Sect. 2.3.2, where, due to confidentiality aspects, precise routing information is not shared among domains. The final part of Sect. 2.3.2 refers to resilience of multilayer networks – a general scheme for contemporary wide-area networks, allowing for existence of the upper-layer virtual links provided by the physical lower-layer paths. Important aspects of this complex scheme refer, e.g., to the sequence of layers according to which the recovery procedures are executed.

Final part of this chapter (Sect. 2.4) outlines three selected up-to-date topics discussed in detail in Chaps. 3, 4, and 5. They include resilience aspects of:

1. The Future Internet architecture being now investigated as a remedy for numerous efficiency problems related to the exponential increase of network traffic, evolving characteristics of applications, as well as emerging new solutions (e.g., Content Delivery Networks – CDN).
2. Wireless Mesh Networks (WMNs) with stationary nodes and wireless high-capacity links between them (established using directional antennas), being a promising alternative to fiber-optic architecture of metropolitan area networks (especially in urban scenarios where the cost of wired installations is almost prohibitive), but encountering resilience problems related, e.g., to weather-based disruptions.
3. Vehicular Ad-hoc Networks (VANETs) seen by car manufacturers as an important solution to improve the vehicular traffic safety (for example, by warnings sent in case of accidents, low bridges, ice, or oil on road), as well as to reduce the impact of vehicles on environmental pollution (e.g., traffic light scheduling to help the driver move in the green phase), but encountering availability problems referring to nodes mobility.

## 2.1 Network Challenges

Communication networks are subject to a large group of challenges, recognition of which is crucial for network design and planning. Following [9], a *challenge* can be defined as a characteristic/condition that may occur as an event affecting the normal operation of a network. Major challenges for communication networks are shown in Fig. 2.1.

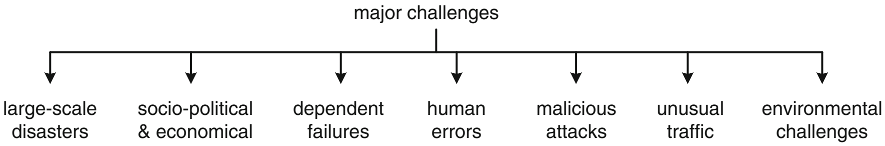


**Fig. 2.1** Major challenges identified in [9]

*Large-Scale Disasters* can be caused by forces of nature (referred to as *natural disasters*) including earthquakes (e.g., the 2006 Taiwan earthquake [37], the 2008 Wenchuan earthquake [61], the 2011 Japan earthquake [74], etc.), or hurricanes (for instance Katrina [14]) bringing about significant disruptions of communication links, as well as communication hardware (nodes). Apart from terrestrial or meteorological causes, natural disasters can be also result of cosmological events including, e.g. geomagnetic storms [34]. Other source of large-scale disasters is human activity. Such *human-made disasters* can be caused by either malicious actions, or follow from ignoring early warnings in operation of a system.

*Socio-Political and Economical Challenges* include deliberate activities (also acts of terrorism) aimed at disrupting the network normal operation, e.g., as a response to political decisions or simply to achieve advantage on economical markets.

*Dependent Failures* refer to challenges that may result in a cascade of failures, for instance after a failure of a system (or its part) offering service to another system [9]. Examples include power grids providing power supply for the Internet.

*Human Errors* are implied by non-malicious human activities. They include, e.g., misconfiguration errors being result of human incompetence. As a consequence, communication networks may even encounter catastrophic failures.

*Malicious Attacks* is another group of challenges referring to deliberate actions designed to cause as much disruption as possible, commonly by being targeted at the most important software/hardware elements of the network infrastructure.

*Unusual Traffic* can be a problem, if its volume exceeds the limits (i.e., the upper bound) assumed during the network design phase. Such extra traffic can be inserted into the network, e.g., after occurrence of a catastrophic event not necessarily disrupting the network infrastructure itself, but resulting in a significant increase of a number of simultaneous requests to get information (often by an order of magnitude greater, as in the case of 9/11 terrorist attack in New York).

*Environmental Challenges* are in turn dependent on communication environment characteristics. They are related, e.g., to mobility aspects in wireless ad-hoc networks (and in particular to time-dependent characteristics of wireless links).

Regardless of the challenge, the most important aspects refer to characteristics measurable in space and in time. As shown in Table 2.1, the impact of a disruption on a communication network performance can be different from the original scope/duration of a challenge. For instance, an attack being a challenge related to a single node may influence the performance of the entire network.

According to [3, 9], any network challenge can be categorized based on detailed criteria including *cause* (natural, human-made, or challenge-dependent), *boundaries* (internal, or external), *target* (direct, or collateral), *objective* (non-malicious, selfish, or malicious), *intent* (non-deliberate, or deliberate), *capability* (accidental, or incompetence), *dimension* (hardware, software, protocols, or traffic), *domain* (medium, mobility, delay, or energy), *scope* (nodes, links, or area), *significance*

**Table 2.1** Spatial and temporal characteristics of challenges based on [9]

| | Spatial region | | Duration | |
|---|---|---|---|---|
| Examples of challenges | Challenge | Impact | Challenge | Impact |
| Earthquake | 100 s km$^2$ | 100 s km$^2$ | Seconds | Days+ |
| Fire | 100 s m$^2$ | 10 s km$^2$ | Hours | Days |
| Hurricane | 100 s km$^2$ | 100 s km$^2$ | Hours | Days+ |
| Malicious attack | Node | Global | Hours | Hours |
| Misconfiguration | Node | Global | Seconds | Minutes |
| Pandemic | Global | Global | Days | Months |
| Policy-related | N/A | Regional/global | N/A | Years |
| Power blackout | 100 s km$^2$ | Regional | Minutes | Hours |
| Solar storm | 1000 s km$^2$ | 1000 s km$^2$ | Minutes | Days+ |
| Terrorism | 100 s m$^2$ | Global | Hours | Hours+ |

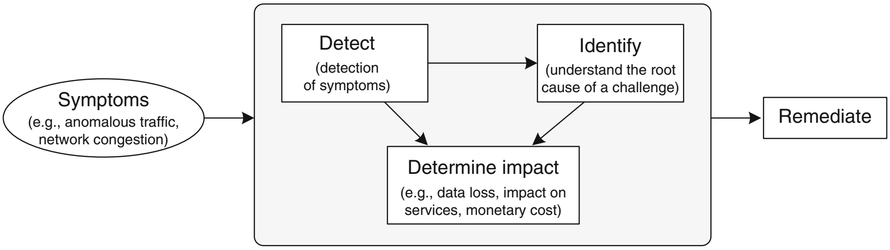

Symptoms
(e.g., anomalous traffic, network congestion)
Detect
(detection of symptoms)
Identify
(understand the root cause of a challenge)
Determine impact
(e.g., data loss, impact on services, monetary cost)
Remediate

**Fig. 2.2** Aspects of challenge identification from [20]

(minor, major, or catastrophic), *persistence* (short-lived, long-lived, or transient), and *repetition* (single, multiple, or adaptive).

A detailed correlation of these challenge categories with major challenges listed in Fig. 2.1 (following from the respective one proposed in [3] for computer systems by International Federation for Information Processing (IFIP) Working Group 10.4) can be found in [9].

Real-time identification of challenges is often a difficult task, especially when they share a number of symptoms. For instance, the observed increased traffic can be implication of a Distributed Denial of Service (DDoS) attack attempt, or simply the legitimate overload caused by flash crowds.

For a proper recognition of challenges, a multi-stage approach (Fig. 2.2) is often necessary [20]. It includes detection of challenge symptoms (i.e., that may lead to recognition of a challenge onset), identification of the root cause of a challenge, and determination of a potential impact on the system. However, in order to be cost-efficient, any remediation action should be preceded by the assessment of the challenge impact versus the cost of remediation [20]. Challenge detection mechanisms, typically invoked in a distributed manner, should be as lightweight as possible in order not to use resources unnecessarily (which is a key requirement for resource-limited networks), and not to disturb the network normal operation [20].

If a network is not provided with built-in mechanisms to defend against challenges (if appropriate mechanisms are not applied, e.g., due to high cost), as well as in the face of new/unknown challenges, any such occurring challenge can afterward trigger a *fault*, i.e., a flaw being either an accidental design flaw (for instance a software bug), or an intentional flaw not eliminated for instance due to the cost constraints of the system.

A fault needs to be *detected* in real-time either in the physical layer (e.g., due to loss of signal, loss of modulation, or loss of clock) by means of signal degradation recognition (e.g., increased Bit Error Rate – BER), or Quality of Service deterioration (indicated by decreased throughput, or increased transmission delay). After fault detection, it is important to *localize* the point of fault to distribute *fault notifications* necessary to remediate the negative effects of the fault on the network performance [11, 20]. Full return of a communication network to its normal operational state can be achieved later in time, only if the root causes of the fault are eliminated.

For any challenge, apart from evaluating its impact on communication network performance, it is important to identify the probability of a challenge occurrence (*challenge_prob*), as well as probability *fail_prob* that a particular challenge will result in a fault (since not all challenges necessarily lead to faults). These two measures combined with information on the challenge *impact* can be used to derive the measure of network resources *exposure* to disruptions from [66], as given in Eq. 2.1.

$$exposure = (challenge\_prob \times fail\_prob) \times impact \tag{2.1}$$

A fault, if not properly dealt with, can next cause an *error*, defined as a deviation between the observed value/state and its specified (correct) value/state. If the error propagates, it may result in a *service failure* (or shortly *failure*) [5, 40, 67, 69, 72].

The four mentioned events form the "challenge → fault → error → failure" chain [69].

Challenges leading to failures of network links/nodes often imply severe disruptions to routing of demands. The resulting problem of communication paths unavailability is additionally escalated owing to the continuous exponential increase of the volume of transmitted information. Since failures of communication paths are inevitable simply due to inability to prevent from a significant subset of challenges, appropriate modifications to routing schemes are necessary to make end-to-end communications feasible in the face of the challenges occurrence.

## 2.2 Resilience Disciplines

There are a number of resilience disciplines proposed in the literature (see e.g., [40, 41], or [43]). However, the most comprehensive one seems to be by Sterbenz et al. from [69]. Following [68, 69], *network resilience* can be defined as the ability

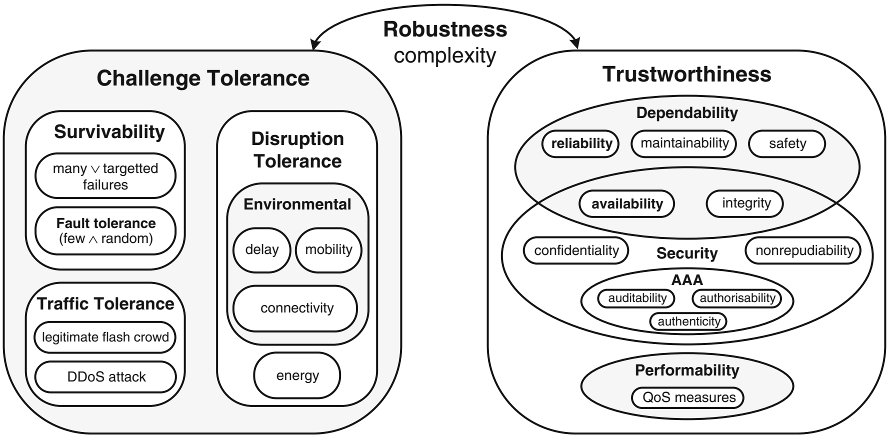


**Fig. 2.3** Classification of resilience disciplines from [69]

of a network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation. Since faults and challenges are inevitable, network resilience should be viewed as one of the most important characteristics of communication networks design.

A detailed classification of resilience disciplines is given in Fig. 2.3. According to [69], resilience disciplines can be classified into two main categories, namely: *challenge tolerance* focusing on network design approaches to provide service continuity in the presence of challenges and *trustworthiness* describing measurable characteristics of analyzed communication systems. The relation between these two, referred to as *robustness*, is the indicator of performance of a network under perturbative conditions.

The first of the two considered resilience disciplines can be further decomposed into: *survivability* (including *fault tolerance*) – referring to communication networks infrastructure, *disruption tolerance* for communication paths resistance to disruptions, and *traffic tolerance* for various challenges related to traffic (e.g., additional volume that is injected into the network).

*Survivability* is typically defined as the capability of a system to fulfill its mission in a timely manner, in the presence of threats including attacks or natural disasters [69]. Another definition from [27] relates survivability with the ability of a network to recover the affected traffic in failure environments and to provide different services continuously. In [36], survivability is in turn defined as the ability of a network to continue the service in the presence of failures, while in [10] it is referred to as the ability of automatically reacting to both physical and software faults by redirecting the traffic from the affected routes to ones which are operating properly.

The scope of survivability is thus broader than of fault tolerance and comprises issues of correlated failures for unbounded networks [50], including e.g., failures due to malicious human activities (attacks) [15], or failures of large parts of a communication network infrastructure [1, 51]. Compared to fault tolerance, apart from redundancy required to provide service recovery, survivability additionally requires *diversity* [45, 68] assuring that the same flaw does not affect multiple elements of a communication system under multiple correlated failures.

Quantification of network survivability is more complex than of fault tolerance. One of possible ways considering simultaneous failures is to utilize multidimensional Markov chains [28], while in [46], a network survivability function (i.e., a probability function of the percentage of total flow delivered after a failure) and survivability attributes have been proposed for evaluation of survivability of any telecommunication network.

*Fault Tolerance* is the ability of a communication system to cope with faults being result of events other than service failures [72]. It uses redundancy to provide compensation for random and uncorrelated failures of system components. However, fault tolerance is not sufficient to provide recovery after multiple correlated failures, and therefore, it is considered as a subset of survivability.

*Disruption Tolerance* is defined in [69] as the ability of a system to tolerate disruptions in connectivity among its components. This connectivity is evaluated in terms of communication paths characteristics, and may be affected due to environmental challenges including, e.g., weak and episodic channel connectivity, nodes mobility, unpredictably long delay, and energy/power challenges [35].

Disruptions of end-to-end connectivity may arise due to:

– dynamic behavior of a network (as e.g., in VANETs [64]),
– large delays not tolerated by traditional network protocols (as e.g., in satellite communications [8]),
– energy constraints limiting the operational time of network nodes (as e.g., in Wireless Sensor Networks – WSNs [44]).

*Traffic Tolerance* is the last fundamental discipline of challenge tolerance, and, following [69], refers to the ability of a system to tolerate the unpredictable traffic load. Traffic can be considered as a challenge, if its volume raises unexpectedly far beyond the network design assumptions for the normal operational state. Example scenarios include either legitimate activities such as flash crowd [18] following natural disasters like earthquakes implying the need to get the relevant information [33], or e.g., malicious actions like DDoS attacks [21].

*Trustworthiness* is defined in terms of measurable characteristics of service delivery as the assurance that the communication system will perform as expected [4]. It comprises three disciplines, namely: dependability, security, and performability.

*Dependability* discipline is used to quantify the level of service reliance and is mainly composed of *reliability* and *availability* [5]. Following [69], *reliability*, being a measure of *service continuity*, is defined in Eq. 2.2 as the probability that a system/service remains operable in a given time frame (0, *t*).

$$R(t) = \Pr(\text{no failure in } [0, t]) \tag{2.2}$$

As stated in [10], reliability function $R(t)$ is most commonly modeled by a negative exponential distribution of failure times (see Eq. 2.3).

$$R(t) = e^{-\frac{t}{\text{MTFF}}} \tag{2.3}$$

where MTFF is the mean (average) time to first failure.

*Availability* ($A$) of a communication system at time $t$ is typically defined as the readiness for its usage, as given in Eq. 2.4.

$$A(t) = \sum_{i \in W} P_i(t) \tag{2.4}$$

where

$W$ is the set of states in which the system is operating correctly
$P_i(t)$ is the probability that a system is in state $i$ at time $t$

Following [69], it can be estimated by the availability indicator from Eq. 2.5.

$$A = \frac{\text{MTTF}}{\text{MTBF}} = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}} \tag{2.5}$$

where

MTTF is the mean time to failure, i.e., the measure of *service continuity* being the length of a time period during which the service is not interrupted [11], to be derived as the expected value of the failure density function
MTBF is the mean time between consecutive failures
MTTR is the mean time to repair – the expected value of the repair density function

Since network operators can only control recovery parameters rather than service continuity characteristics, adjusting service availability characteristics to the needs of the customer can be done by controlling the MTTR parameter only.

Reliability is of utmost importance for applications being session/connection-oriented requiring relatively long value of MTTF. Availability is in turn an appropriate measure for transactional services (e.g., Hypertext Transfer Protocol – HTTP) performing individual operations in a short time. For such services, as long as MTTR is relatively short, it is less important whether the system fails frequently, or not. Availability is also typically used to assess the resilience of communication networks for practical reasons [11]. Other dependability characteristics include:

*Maintainability*, i.e., predisposition of a system to updates/evolution.

*Safety* – a measure of a system dependability under catastrophic failures, in particular referring to the effect rather than the cause of a failure, as for example in the context of cyber attacks [40, 52, 69]. Any system is commonly considered to be safe, if it is harmless for normal functioning of the environment.

*Integrity* being the absence of improper (unauthorized) system alterations [5].

Another important aspect is *security* being the ability of a system to protect itself from various unauthorized activities (e.g., access or updates based on the respective security policies). Security has joint properties of *availability* and *integrity* with dependability, as well as individual characteristics including *authenticity*, *authorisability*, *auditability*, as well as *confidentiality* and *nonrepudiability* [5].

*Performability* is the discipline that is used to provide measures on performance of a system compared with the respective Quality of Service requirements following from service specifications in terms of delay, jitter, throughput/goodput, and packet delivery ratio [69].

Tables 2.2 and 2.3 present selected sets of resilience characteristics, as identified by ITU-T and IETF for communication networks. From the client perspective, the most important resilience characteristics are those that are related to the perceived service quality, referred to as the *Quality of Resilience* (QoR) features, being the QoS characteristics related to resilience observed by the end users [11].

On the contrary, network operators are mainly interested in characteristics concerning operational and implementation aspects (known as the operation-related features) influencing the cost of solutions. Since objectives of these two groups are obviously in contrast to each other, a detailed assessment is necessary to verify whether the offered quality meets the client requirements, and if, at the same time, it is profitable for the network operator.

It is worth noting the remarkable difference between QoS and QoR characteristics concerning the time needed to obtain the results. Unlike QoS features being short-term by nature, most of resilience measures are long-term [12]. Therefore, resilience can be evaluated in long term only based on end-to-end transmission characteristics. Additionally, unlike QoS measures, QoR characteristics often cannot be derived precisely, since in many cases, they are not perceived by end users directly. For instance, increased transmission delay/packet losses may be result of either congestion, or a network element failure.

## 2.3 Existing Approaches to Provide Resilient Routing

In Sects. 2.3.1 and 2.3.2, we present known approaches to resilient routing originally proposed for wired networks with special focus on disruption tolerance with respect to a single network layer. In order to maintain service continuity after failures, spare capacity (mostly related to link bandwidth) is commonly reserved in the network to provide possibility to reroute the traffic along the *alternate path* (also called *backup* or *protection path*), when the *primary* (*working*) *path* fails [29]. In general, the greater is the capacity to be protected, the more significant is the task to protect the network from failures.

**Table 2.2** Selected resilience metrics defined by ITU-T based on [12]

| Recommendations of International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) | | |
|---|---|---|
| ID | Area | Metric |
| E.800<br>E.802<br>E.820<br>E.850<br>E.855<br>E.860<br>E.862<br>E.880 | General (e.g., Internet access), telephone network | Instantaneous availability/unavailability – probability defined for a network element of being in an "up"/"down" state at a given instant of time |
| | | Mean time between failures (MTBF) – mean value of time duration between two consecutive failures of a repaired element |
| | | Mean time between interruptions (MTBI) – mean value of time duration measured between the end of one interruption and the beginning of the next one |
| | | Mean time to failure (MTTF) – mean value of time duration for a network element measured from the instant its state changes from "down" to "up" until the next failure |
| | | Mean time to recovery (MTTR) – mean value of time duration when a network element is in a "down" state due to a failure |
| | | Mean up time (MUT)/mean down time (MDT) – interval during which an element is in an "up"/ "down" state |
| | | *p*-fractile repair time |
| | | Probability of fault coverage |
| | | Reliability function R($t$) – probability that a network element can perform as expected under given conditions for a specified time interval |
| | | Retainability: measure of probability that a service will continue to be provided |
| | | Failure/repair rate $\lambda(t)/\mu(t)$ |
| G.911 | Fiber optic systems | Failures in time (FIT) – a number of failures occurred per $10^9$ device hours |
| | | Median life – a value on a lognormal probability plot of time to failure at which 50 % of the devices fail earlier and 50 % of the devices fail later |
| | | Standard deviation – a value of a standard deviation concerning the natural logarithms of the time to failure |
| | | Availability (A), MTBF, MTTR, unavailability (U), $\lambda(t)$ |
| M.60<br>M.3342 | General | Mean time to restore service (MTRS) – similar to MTTR but here related to the service level |
| | | A, MTBF, MTTR, R($t$), retainability |
| Y.1540<br>Y.1541<br>Y.1542 | IP | IP packet loss ratio (IPLR) – the total number of lost IP packets to the total number of transmitted IP packets in a given population of interest |
| | | Percent of IP service (un)availability (PIU/PIA) – percentage of total time of IP service categorized as (un)available based on the availability function of IP service |
| | | Service availability – a portion of total scheduled service time for an IP service classified as "available" |

(continued)

**Table 2.2** (continued)

| Recommendations of International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) | | |
|---|---|---|
| ID | Area | Metric |
| Y.1561 | MPLS (Multiprotocol Label Switching) | Packet loss ratio (PLR) – analogous to IPLR |
| | | Recovery time – time needed for recovery actions at MPLS layer calculated based on the number of successive time intervals of consecutive SLB outcomes at ingress node |
| | | Severe loss block (SLB) outcome – an event occurring at an ingress node for a block of packets if the ratio of lost packets at an egress node exceeds the upper bound |
| | | Service availability, PIU, PIA – defined similarly as in Y.1540, but here related to SLB |
| Y.1562 | Higher layer protocols | Service availability – in Y.1562 related to the transfer delay and success ratio of service |

**Table 2.3** Selected resilience metrics defined by IETF based on [12]

| Recommendations of Internet Engineering Task Force (IETF) in Requests for Comments (RFCs) | | |
|---|---|---|
| ID | Area | Metric |
| 2330 | IP | Packet loss rate (PLR) – similar to IPLR |
| 3386 | Multi-layer networks | Protection switching time – time interval between the network fault occurrence until the completion of protection-switching actions |
| | | Restoration time – time interval from the network fault occurrence until the complete restoration of the affected traffic, exhaustion of spare resources, or existence of no more extra traffic |
| 3469<br>4378 | MPLS | Availability – the percentage of time that a service is operating |
| | | Full restoration time – time necessary to switch the traffic onto links/paths meant to handle the traffic in recovery scenarios |
| | | Number of concurrent faults – number of faults a selected recovery scheme can cover |
| | | Recovery time – time needed for activation of an MPLS backup path (and resumption of affected traffic flows) after a fault |
| | | Setup vulnerability – measure of time when the primary path is left unprotected during recovery paths computations /setup |
| 3945<br>4427<br>4428 | GMPLS (Generalized Multiprotocol Label Switching) | Recovery ratio – fraction of the restored traffic bandwidth divided by the overall traffic bandwidth to be protected |
| | | Recovery time (down time) |

In this book, we define *resilient routing* as a routing scheme that is able to provide the continuity of service in the presence of disruptions.

Following [10, 63], and as previously mentioned in Chap. 1, after occurrence of a failure, the recovery process is initiated with *detection* of a failure. It can be recognized, e.g., by IP-MPLS mechanisms like `MPLS LSP ping` or `MPLS LSP traceroute` [39] (sent along Label Switched Paths – LSPs), which are, however, time-consuming. Another option is to determine the failure based on the `Loss of Light`, or `Loss of Clock` events.

Fault detection should be followed by *fault localization* and *isolation* (i.e., determination of the faulty node/link), which is necessary to stop further transmission of information via the affected element that should be repaired [10].

*Fault Notification* messages are sent to network nodes responsible for further recovery actions. At this stage, the two processes typically initiated are the repair process and the recovery process. The first one is related with repair of the faulty element, while recovery process is to identify the affected traffic, localize the failure, and determine the alternate path over which traffic is next *redirected*.

Both processes are assumed to terminate with *normalization*, i.e., recognition of the repaired element and return to the normal operational state. Concerning routing, this would generally mean return to transmission paths that were in use before the failure (since recovery paths are typically non-optimal, e.g., with respect to the resource usage).

The ideal *recovery time* (i.e., the time needed to switch the traffic to backup paths) should not be greater than 50 ms, since a disruption lasting up to 50 ms is seen by the higher layers as a transmission error only. Any disruption longer than 50 ms results at least in packet losses, or unavailability of service [60]. A detailed classification of time outages from [22] is given in Table 2.4.

Although utilization of protection paths to provide automatic switchover seems rather intuitive, the question how to implement efficient recovery schemes, being not only capacity-efficient, but also scalable and including multiple criteria of QoS, especially in heterogeneous mesh network environments, is a difficult task.

In general, characteristics of any recovery method strongly influence the values of service recovery time [10]. In the later part of this section, we will highlight the most important recovery techniques with special focus on restoration time characteristics, as well as its relation with the resource efficiency objective.

A fundamental classification of resilience mechanisms based on the structure of communication networks divides existing approaches into ring- and mesh-based. The former one refers to architectures introduced about three decades ago including, e.g., Synchronous Optical Networks/Synchronous Digital Hierarchy (SONET/SDH) [65] and early architectures of ring Dense Wavelength Division Multiplexing (DWDM) networks [49]. Based on flow direction, *ring networks* may be classified as unidirectional, or bidirectional, accordingly. As shown in Fig. 2.4, both working and backup routes in ring networks are organized in rings.

**Table 2.4** Impacts of outage time from [22]

| Target range | Duration | Main effects |
|---|---|---|
| Protection switching | ≤50 ms | No outage logged; recovery of Transmission Control Protocol (TCP) after one errored frame; no TCP fallback; no impact at all for most TCP sessions |
| 1st type outage | >50 ms<br>≤200 ms | <5 % voiceband disconnects; signaling system switchovers |
| 2nd type outage | >200 ms<br>≤2 s | Common upper bound on distributed mesh restoration time; TCP/IP protocol back-off |
| 3rd type outage | >2 s<br>≤10 s | Disconnections of all switched circuit services; disconnections of private lines; TCP sessions time-outs; Hello protocol affection; web page "not available" errors |
| 4th type outage | >10 s<br>≤5 min | All calls and data sessions terminated; timeouts of TCP/IP application layer programs; users making attempts of mass redials; link state advertisements (LSAs) sent by routers referring to failed links; updates of topology and resynchronization network-wide |
| Undesirable outage | >5 min<br>≤30 min | Massive reattempts causing heavy load of switches; noticeable Internet "brownout"; minor societal/business effects |
| Unacceptable outage | >30 min | Major societal impacts (societal risks: travel booking, impact on all markets); headline news; regulatory reporting often required; lawsuits; SLA clauses triggered |

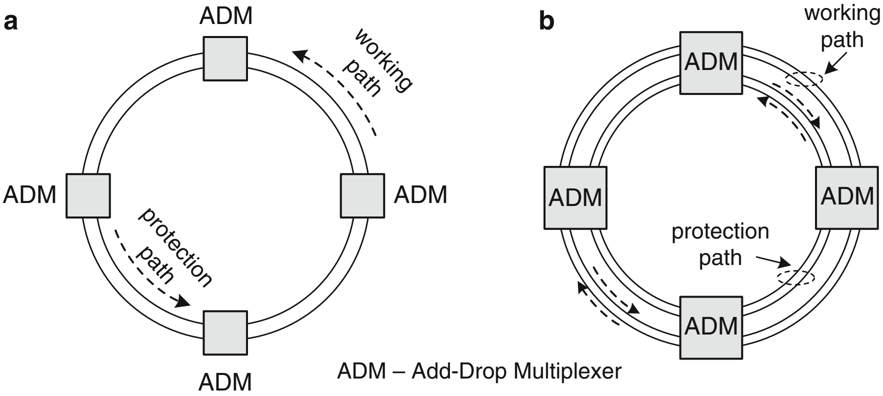


**Fig. 2.4** Example of Unidirectional Path-Switched Ring (UPSR) and Bi-directional Line Switched Ring (BLSR) with Add-Drop Multiplexers (ADMs)

Backup rings can be thus viewed as a preplanned protection scheme providing a very short recovery switching time. However, the disadvantage is the high ratio of network *redundancy* (being the ratio of protection capacity to working capacity) of exactly 100 % [29].

### 2.3.1 Resilient Routing in Mesh Networks

In contemporary networks often characterized by a mesh topology [26], transmission paths are of end-to-end type, i.e., they do not form ring structures. As opposed to networks from the past engineered to offer a single type of service only (either voice, or data), current communication networks are also expected to provide a variety of services (e.g., real-time services, as well as bulk data transfer) to support a wide range of applications having differentiated requirements with respect to resilience, as well as quality of transmission, as shown in Fig. 2.5.

This differentiation can also follow from different usage of the same application [11]. In other words, the same application can thus have differentiated requirements depending on how the users utilize it. For instance, even in the case of a classic telephone service, requirements on service availability for a company would be much higher than those addressed by a home user.

Designing a communication network always meeting the highest requirements over the entire range of services (i.e., prepared to provide the highest level of service) would be extremely costly and unreasonable. Such over-provisioning is particularly expensive in wireless and access networks where bandwidth is limited (compared e.g., to optical DWDM long-haul networks) [11].

Therefore, proper *resilience differentiation* (e.g., as discussed in [47, 56]) is crucial in client-operator relations as an important element of Service Level Agreements. The operator, interested in maximizing the profit, is looking for cost-efficient resilience mechanisms tailored to specific QoR requirements. Willingness of clients to pay for the service is also differentiated. In particular, clients expect the lowest possible price for the service able to support characteristics of applications, but with only a marginal regard to network mechanisms the operator would deploy to support these applications. Utilization of multiple resilience mechanisms in the network may thus enable both clients and operators to increase their profit.

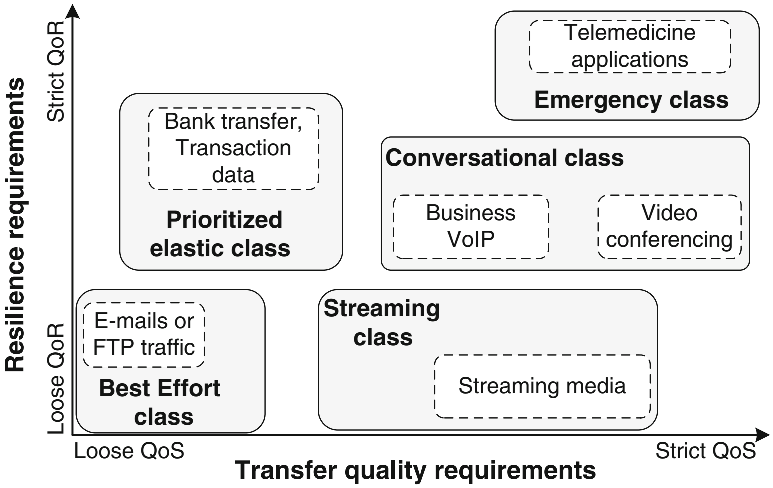


**Fig. 2.5** Transfer quality vs. resilience requirements from [73]

## 2.3.2 Backup Path Resources Reservation Schemes in Mesh Networks

This section presents a brief overview of the most important resilience mechanisms proposed in the literature to provide fault-tolerant routing. Resilience differentiation can be obtained by combining several of them in a single network. Figure 2.6 outlines the most important classifications of resilience mechanisms for mesh networks, characterized in detail later in this section.

### Backup Path Setup Method

Concerning backup path setup methodologies, recovery paths can be:

- installed in a preplanned way (i.e., in advance when finding the primary paths) – often referred to as the *preplanned protection* in the literature [27],
- determined dynamically (reactively) after the occurrence of a failure (known as *dynamic restoration*).

The former case, historically derived from the Automatic Protection Switching (APS) [11], enables fast recovery of each failed transmission path (since backup paths are established in advance).

Dynamic restoration with its origins in IP networking [10] is in turn better in terms of efficiency of network resource utilization (backup paths are installed here only when necessary, i.e., after a failure, and can reuse link capacities of failed transmission paths). However, it inherits all disadvantages characteristic to dynamic IP routing, in particular the time-consuming recovery switching, path instabilities, and risk of loops creation. It also does not guarantee recovery due to unpredictable amount of spare resources available after a failure [13].

In general, in order to provide 100% of restorability for working data flows, any backup path should not only be characterized by the same capacity as the corresponding working path, but it should also be link/node-disjoint (i.e., have no common links/transit nodes) with the working path – Fig. 2.7. The latter

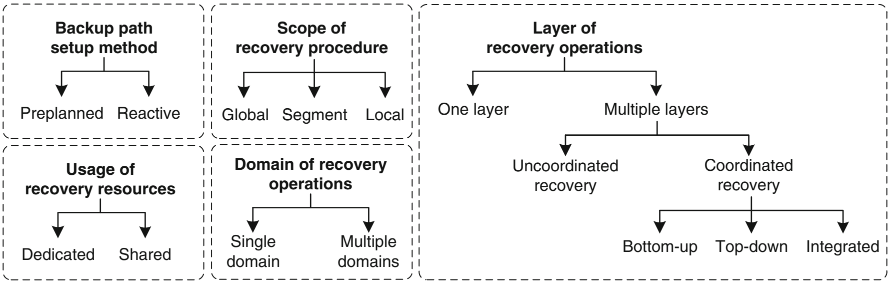


**Fig. 2.6** Major classifications of resilience mechanisms

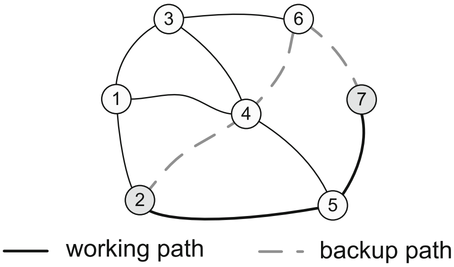


**Fig. 2.7** Example of end-to-end node-disjoint pair of paths between nodes 2 and 7

requirement is to guarantee that any failure of a link/node affecting the working path will also not disrupt the respective backup path [29].

This disjointedness is thus to assure that the two considered paths (i.e., working and backup path) of a demand do not use resources of network elements belonging to the same *Shared Risk Link Group* (*SRLG*) defined in [27, 29] as the set of network elements, being either links, nodes, physical devices, or a mix of these, subject to a common risk of failure. Following [29], any working path is said to be *SRLG-disjoint* with the respective backup path, if both paths are not involved in any common SRLG.

### Scope of Recovery Procedure

Considering the scope of recovery, apart from *global protection* (assuming utilization of a single end-to-end backup path protecting the entire working path of a demand) – Fig. 2.8a, *local protection* may be applied with backup paths used to redirect the affected traffic over the failed link/node, as given in Fig. 2.8b [10]. The intermediate solution called *segment protection* [48] provides existence of backup paths each one protecting a given segment of a working path (consisting of several consecutive network elements), e.g., as in Fig. 2.8c.

### Usage of Recovery Resources

When analyzing the schemes of spare resources utilization, two solutions should be outlined, namely dedicated and shared protection. In a *dedicated protection* scheme, resources (link capacities) of any backup path are reserved to protect a single working path only. This technique is very costly but enables fast recovery of the affected traffic. Additionally, if preplanned protection is applied, backup paths may be either used in parallel with working paths in the normal operational state (i.e., the $1+1$ scheme of transmitting the signal simultaneously along both paths), or activated only for short time-periods to redirect the traffic influenced by the failure (known as the 1:1 protection scheme). In the latter case, backup capacity can be used by best-effort traffic under normal operation [27].

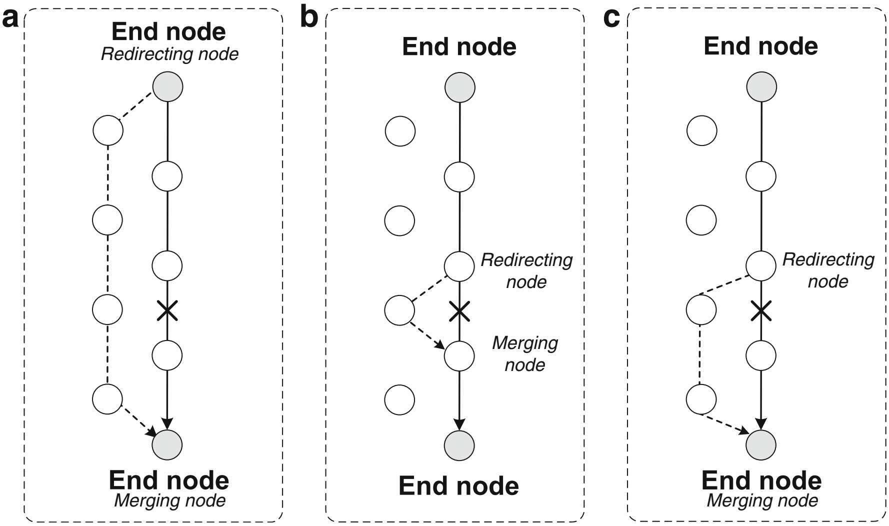


**Fig. 2.8** Examples of: (**a**) global, (**b**) local, and (**c**) segment recovery schemes

The problem of providing the resilient routing for a set of demands by backup paths being SRLG-disjoint with the respective working paths in capacity-constrained networks was shown to be *NP*-complete in [60], which implies that the use of combinatorial approaches is necessary. For instance, the optimal solution to the example problem to find the working and backup path pairs to provide protection against a single node failure for a set of demands, for which the total cost of working and protection paths given by Eq. 2.6 is minimized, can be determined by solving the respective ILP problem. As presented in our work [48], formulation of this problem should include flow conservation constraints (Eq. 2.7), constraints on total link capacity formula (2.8), constraints to ensure nodal disjointedness for each pair of working and backup paths formulas (2.9) and (2.10), and constraints on allowed values (Eq. 2.11).

However, for a single demand $r$, the problem of finding the pair of working and protection paths of the minimal joint cost of both paths can be achieved in polynomial time by Surballe's algorithm [70, 71], or its modification – Bhandari's approach [6, 7]. In each of them, a single end-to-end path can be calculated using Dijkstra's algorithm [16].[1]

[1] Algorithms [6] and [70] are also suitable to calculate the set of $k$ end-to-end node-(link-)disjoint paths with the lowest overall cost, necessary if protection against *multiple failures* (i.e., a simultaneous failure of multiple network elements) is required, e.g., as in [57]. Such a scenario can occur for instance if several network links are buried together in a duct that is cut by a third party.

### Indices

$\Gamma(N, A)$ directed graph, where $N$ and $A$ are the sets of network nodes $n$ and directed arcs $a_h$, accordingly; each network link is represented by two opposite arcs $a_h = (i, j)$ and $a_{h'} = (j, i)$; $|N|$ and $|A|$ are the numbers of network nodes and arcs, accordingly

$D$ set of demands; $|D|$ is the number of demands

$r$ demand number; $1 < r \leq |N| \cdot (|N| - 1)$

### Constants

$c_h$ total capacity of arc $a_h$

$d_r$ capacity requested for a working and a backup path of demand $r$

$s_r$ ($t_r$) source (destination) node of $r$-th demand; $r = 1, 2, \ldots, |D|$

$\xi_h$ cost per unit flow of each commodity on arc $a_h$

### Variables

$x_{r,h}(y_{r,h})$ 0-1 binary variables indicating utilization of arc $a_h = (i, j)$ by a working (backup) path of $r$-th demand

### Objective

It is to minimize the total cost of a solution defined by formula (2.6):

$$\varphi(\mathbf{x}) = \sum_{r \in D} \sum_{h \in A} \xi_h d_r \left( x_{r,h} + y_{r,h} \right) \tag{2.6}$$

### Constraints

1. To provide flow conservation rules (Kirchhoff's law):

$$\sum_{\substack{h \in \{h : a_h \equiv (n, j) \in A; \\ j = 1, 2, \ldots, |N|; j \neq n\}}} x_{r,h} - \sum_{\substack{h \in \{h : a_h \equiv (i, n) \in A; \\ i = 1, 2, \ldots, |N|; i \neq n\}}} x_{r,h} = \begin{cases} 1, & \text{if} \quad n = s_r \\ -1, & \text{if} \quad n = t_r \\ 0, & \text{otherwise} \end{cases} \tag{2.7}$$

where

$a_h = (i, n)$: arc incident into node $n$
$a_h = (n, j)$: arc incident out of node $n$; $r \in D$

Equations for backup paths are similar to (2.7) with $x^{l}_{r,h}$ replaced by $y^{l}_{r,h}$.

2. On total capacity available at network links:

$$\sum_{r \in D} \left(x_{r,h} + y_{r,h}\right) \cdot d_r \leq \ c_h; \quad h \in A \tag{2.8}$$

3. On nodal disjointedness of working and backup paths of a demand:

$$\left.\begin{array}{l} \sum\limits_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} \left(x_{r,h} + y_{r,h}\right) \leq 1 \\ \sum\limits_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} \left(x_{r,h} + y_{r,h}\right) \leq 1 \end{array}\right\} \begin{array}{l} \text{where :} \\ n \neq s_r; n \neq t_r \left(\text{i.e., for} \right. \\ \left.\text{transit nodes}\right), \text{if both} \\ \text{paths consist of at least} \\ \text{two arcs;} \quad r \in D \end{array} \tag{2.9 and 2.10}$$

4. On allowed values of variables:

$$x_{r,h} \in \{0; 1\}; \quad y_{r,h} \in \{0; 1\}; \quad r \in D; \quad h \in A \tag{2.11}$$

The disadvantage of a dedicated protection scheme is that, even though it provides the fastest recovery, it implies high additional cost of over 100 % due to the ratio of network redundancy exceeding 100 % (since backup paths typically traverse more links than the corresponding working paths). Therefore, to limit the cost of a solution, the concept of *shared protection* was proposed in which link capacities can be mutually shared by several backup paths. According to [42], shared protection approach is able to limit the redundancy ratio to the level of 35–70 %.

If flows are required to be 100 % restorable, sharing the link capacities by several backup paths is feasible, only if the respective parts of working paths (i.e., being protected by these backup paths) are mutually disjoint, meaning that they do not share the same risk of failure (i.e., if they do not belong to a common SRLG) [29].

In resilient routing schemes, capacity of any link is classified into: (1) *working capacity* (i.e., used by existing working paths), (2) *spare capacity* (denoting capacity already reserved for backup paths), and (3) *free capacity* not used by any path (i.e., that can be allocated for either working, or backup paths) [29].

As shown in Fig. 2.9, under backup capacity sharing, the spare capacity of any link is further divided into two classes: *shareable* and *non-shareable*. The former one comprises backup capacity reserved for other backup paths that may be shared by the backup path to be established (i.e., when the respective part of a working path of an incoming demand is SRLG-disjoint with parts of all other working paths being protected by backup paths using this shareable capacity). The latter case refers to the capacity already reserved for backup paths that cannot be shared.

Following [29, 54, 75], when finding a backup path in a backup capacity sharing scenario, the cost $\zeta_h$ of arc $a_h$ is commonly defined as given in Eq. 2.12. According to this metric, the cost of a backup path link is thus determined only by the extra capacity that has to be reserved for a given backup path. Otherwise, if there is no need to reserve the extra capacity at $a_h$ for this backup path (i.e., if the requested capacity is not greater than the shareable backup capacity at $a_h$), then $\zeta_h$ is set to $\varepsilon$. Links with sharable capacity are thus preferred in backup path computations.

$$\zeta_h = \begin{cases} \varepsilon & \text{if} \quad d_r \leq sh_h^{(r)} \\ \left(d_r - sh_h^{(r)}\right) \cdot \xi_h & \text{if} \quad d_r > sh_h^{(r)} \text{ and } \overline{c_h} \geq d_r - sh_h^{(r)} \\ \infty & \text{otherwise} \end{cases} \tag{2.12}$$

where

$d_r$ is the capacity requested for $r$-th demand
$\overline{c_h}$ is the unused capacity of arc $a_h = (i, j)$
$\xi_h$ is a unitary cost of arc $a_h$ in working path computations
${sh_h}^{(r)}$ is the capacity reserved so far at $a_h$ that may be shared with respect to the backup path of $r$-th demand

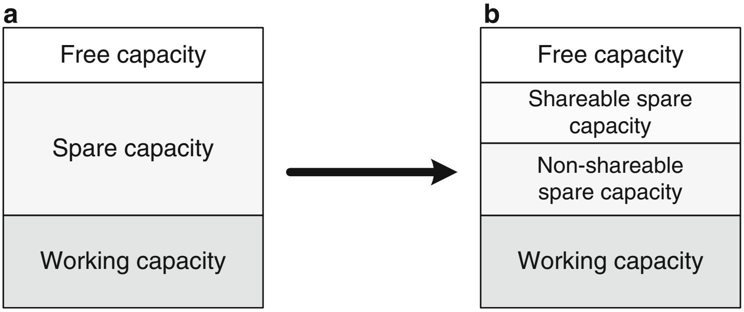


**Fig. 2.9** Example link capacity classification under: (**a**) dedicated, (**b**) shared protection

Since the problem of resilient routing with shared backup paths is an extension to the conventional problem of resilient routing defined by formulas (2.6–2.11), it is also *NP*-complete. In order to find the optimal solution, several updates to the model defined by formulas (2.6–2.11) are necessary. In particular, the objective function (Eq. 2.6) has to be replaced with Eq. 2.13.

$$\varphi(\mathbf{x}) = \sum_{r \in D} \sum_{h \in A} \xi_h d_r x_{r,h} \quad + \sum_{h \in A} \xi_h b_h \tag{2.13}$$

where

$b_h$ is an additional variable determining how much extra capacity has to be reserved for backup paths at arc $a_h$ (therefore related with metric $\xi_h$)

It is also necessary to introduce an additional binary variable $b_{r,h,g}$ to indicate whether for $r$-th demand the failed primary path traverses arc $a_g$, and the corresponding backup path traverses arc $a_h$, as well as a continuous variable $b_{h,g}$ denoting the total capacity needed for backup paths at arc $a_h$ in the case of shared protection provided for working paths traversing the failed arc $a_g$.

The set of constraints formulas (2.7–2.11) has to be extended with formulas (2.14–2.17) responsible for appropriate sharing of backup path capacities. In particular, formula (2.14) assures that in the case both variables of left-hand side are equal to 1 (which implies that a given working path traverses the failed arc $a_g$ while the corresponding backup path traverses arc $a_h$), then variable $b_{r,h,g}$ must be also equal to 1 (i.e., it must indicate this relation).

Formula (2.15) in turn guarantees that if at least one of variables $x_{r,g}$ and $y_{r,h}$ is equal to 0 (i.e., if arcs $a_g$ and $a_h$ are not used in parallel by the respective working and backup paths of demand $r$), then $b_{r,h,g}$ should be equal to 0 – in order not to indicate the mentioned relation. Equation 2.16 provides arc spare capacity constraints (i.e., the amount of spare capacity required at $a_h$ in a particular scenario of arc $a_g$ failure), while formula (2.17) is to provide constraints on the maximum amount of spare capacity needed to be reserved at $a_h$ for all failure scenarios.

$$x_{r,g} + y_{r,h} \leq 1 + b_{r,h,g}; \quad r \in D; \quad h \in A; \quad g \in A; \quad g \neq h \tag{2.14}$$

$$2b_{r,h,g} \leq x_{r,g} + y_{r,h}; \quad r \in D; \quad h \in A; \quad g \in A; \quad g \neq h \tag{2.15}$$

$$b_{h,g} = \sum_{r \in D} d_r b_{r,h,g}; \quad h \in A; \quad g \in A; \quad g \neq h \tag{2.16}$$

$$b_{h,g} \leq b_h; \quad h \in A; \quad g \in A; \quad g \neq h \tag{2.17}$$

Considering heuristic approaches to determine the resilient routing with shared protection, the Active Path First (APF) technique described in [30, 31] is typically used. In this two-step scheme, a working path of a demand is found first and is followed by calculation of a backup path for the topology of a residual network (i.e., with arcs traversed by the working path excluded). Numerous variants of this method have been proposed in the literature aimed at, e.g., determining the working path links in a way to get the most benefits from backup capacity sharing in the second phase [77].

However, if a backup path sharing scheme incorporates the shareability factor into the cost of a backup path link (e.g., as shown in formula (2.12) and in fact in Eq. 2.13), such backup paths occur to be non-optimal with respect to their length. As we showed in [54], in this case backup paths may be even 40–50 % longer, compared with the results for a dedicated protection approach. For instance, for the example scenario from [54] given in Fig. 2.10, the path (2, 1, 3, 4, 7) with the total cost of $10 + 3\varepsilon$ is chosen to be the backup path for the working path, even though there is a much shorter candidate path (2, 4, 7) but of the total cost of 27.

Due to the three-way handshake procedure of backup path activation [59] including sending the `LINK/NODE FAIL` message along the working path links followed by the exchange of `SETUP` and `CONFIRM` messages along the backup path, the total time of service restoration is mainly determined by message propagation delay along the backup path. Therefore, for the classical backup path sharing scheme, improved capacity efficiency comes at a price of the increased service restoration time. In general, there is a tradeoff between capacity efficiency and recovery time, i.e., the larger is the segment of the working path being protected by a given backup path, the better capacity efficiency can be obtained, but for the price of longer recovery times. A detailed analysis of service recovery time for various recovery schemes is presented in [10].

To overcome this problem, our approach introduced in [54] assumes that both working and backup paths are first determined based on the same metric of link costs (i.e., reflecting the lengths of links only). In order not to increase the length of backup paths, backup path sharing is then performed "a posteriori" by finding the solution to the problem of vertex coloring of the respective graph of conflicts for each network link individually (i.e., to perform capacity sharing for the established backup paths to comply with SRLG constraints concerning the respective working paths). After applying our capacity sharing solution, backup paths traverse the same links, as under dedicated protection.

In the literature, the term *multi-cost network* is used to represent a scheme with differentiated costs assigned to network links in computations of multiple end-to-end disjoint paths of the same demand (e.g., as in the case of a typical backup path sharing scheme using differentiated costs $\xi_h$ and $\zeta_h$ of arcs $a_h$ for working and backup paths, accordingly). On the contrary, in the scheme of a *single-cost network*, the same cost $\xi_h$ of arc $a_h$ is assigned to network links in computations of all disjoint paths of a given demand (e.g., as in [54]).

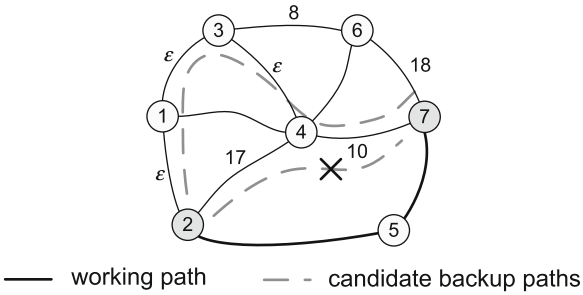


**Fig. 2.10** Example candidate backup paths (backup path sharing scenario)

The problem to find multiple end-to-end disjoint paths for the multi-cost network scheme was shown to be *NP*-complete even for a single demand [76]. Therefore, in order to provide a time-efficient solution, there is a need to use the suboptimal heuristic approach, e.g., as proposed by us in [55].

*Protection Cycles* (or shortly *p*-cycles) originally introduced in [25] are pre-configured ring-like structures defined for mesh networks to provide backup detours for a set of working paths. Similar to ring networks, *p*-cycles can protect segments of working paths traversing the respective *p*-cycle (referred to as the *on-cycle spans*), as in the case of working paths W1, W2, W3 that share a common *p*-cycle in Fig. 2.11. However, unlike in ring networks, *p*-cycles can be also used to protect working paths straddling the protection cycle (i.e., not having any common link with the *p*-cycle), as the example working path W4 from Fig. 2.11. This additional feature results in improved capacity efficiency of *p*-cycles, which is comparable to the one for shared backup path protection [2]. In general, a single *p*-cycle can protect multiple on-cycle and straddling spans, if all these spans are SRLG-disjoint.

In the event of a failure, only two switching actions (like in ring networks) are necessary to redirect the traffic onto the protection path provided by the *p*-cycle (i.e., at the end nodes of the failed span). Therefore, *p*-cycles combine the best characteristics of mesh-based and ring-based protection methods, i.e., ring-like service restoration speed with mesh-like capacity efficiency.

Following [36], *p*-cycles are often selected either from the set of all distinct cycles for a given network graph, or from a reasonably large set of candidate cycles.

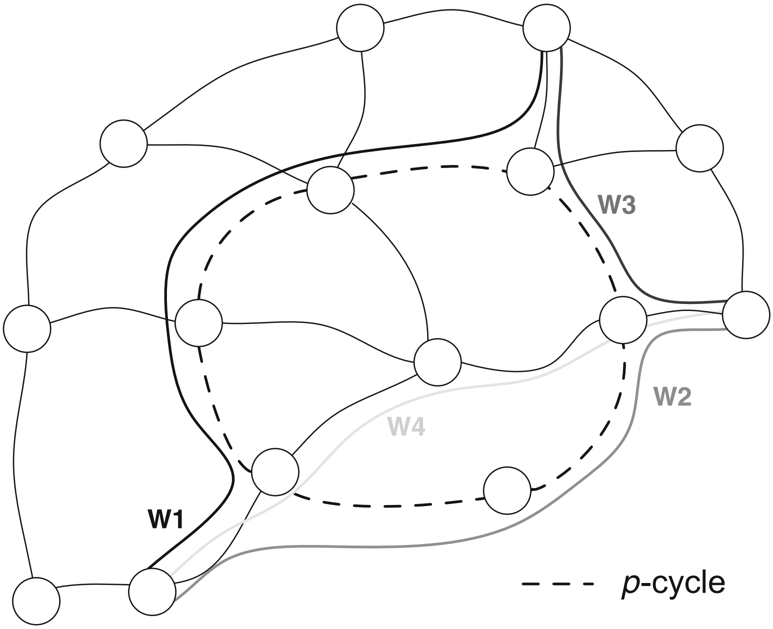


**Fig. 2.11** Example *p*-cycle

Regarding combinatorial optimization issues, three approaches have been widely used [2]: optimization of only spare capacity, joint optimization of working and spare capacity, and the concept of protected working capacity envelope (PWCE) from [23] assuming routing of demands based on information on already established *p*-cycles.

Protection cycles have been widely adapted to many networking scenarios, including, e.g., path protecting *p*-cycles [32, 38], node-encircling *p*-cycles [17], Hamiltonian *p*-cycles [62], flow *p*-cycles [24], or multicast provisioning [19, 78].

### Domain of Recovery Operations

End-to-end routing between distant locations frequently needs to be provided over multiple network domains, each one defined based on administrative/geographical scope, or network provider ownership and commonly identified with an autonomous system [10]. In the context of end-to-end routing, *multi-domain routing* encounters problems related to availability of precise routing information (i.e., following from topological characteristics of domains), which, due to confidentiality aspects, is generally not shared [63].

Another problem refers to the lack of exchanged information concerning physical deployment of links in different domains related to SRLG disjointedness. For instance, as given in Fig. 2.12, even though it may seem that end-to-end routing by means of two separate paths over several domains meets the requirements of nodal disjointedness, in practice links from different domains (for instance links `B1-B3` and `C2-C3` from Fig. 2.12) may be deployed in the same duct, e.g., physically routed over the same bridge, which raises the risk of a simultaneous failure of both of them. Therefore, the application of *inter-domain recovery* techniques (i.e., joint actions taken in multiple domains to recover from failure) is often unrealistic.

### Layer of Recovery Operations

Internet IP traffic is mostly carried over optical networks (e.g., in the backbone). It means that a certain kind of communication networks layering is applied there.

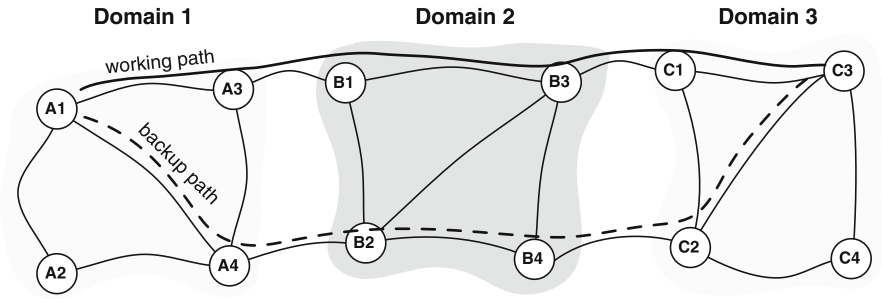


**Fig. 2.12** Example scenario of multi-domain routing

Indeed, IP links are frequently virtual, meaning that they are provided, e.g., by the optical multi-hop paths. Therefore, the resulting IP virtual topology is commonly formed over the underlying optical transport network.

This simple scenario mentions only two layers: i.e., the upper IP layer (frequently enhanced with Multiprotocol Label Switching (MPLS) functionality towards QoS provisioning, often referred to as IP-MPLS), and the lower Wavelength Division Multiplexing (WDM) [10]. In this case, IP-MPLS routers are connected to ports of the lower-layer Optical Cross Connects (OXCs). OXCs themselves are in turn interconnected in a physical mesh topology via multiwavelength optical links.

As shown in the example Fig. 2.13, a working IP-layer path for a demand between nodes R1 and R4 consists of a direct virtual link (R1, R4) that is provided in the WDM layer by a lightpath (O1, O2, O4). For this demand, the backup IP-layer path consists of two links (R1, R3) and (R3, R4), each one provided by a separate lightpath.

In general, this concept can be extended to the case of networks consisting of more than two layers with client-server relationship between each neighboring pair of layers (including, e.g., SONET/SDH between IP-MPLS and WDM layers) [10]. The automated control of multilayer networks has been standardized in the Generalized Multiprotocol Label Switching (GMPLS) framework including all necessary entities for use by routing and signaling protocols, in particular the User-Network Interface (UNI) and the Network-Network Interface (NNI).

Considering the issue of interoperation between layers, following [10, 63], three main schemes may be distinguished, namely:

- the *overlay model* assuming that routing is performed in each layer separately (i.e., no routing information is shared between network layers),
- the *peer* (also called *integrated*) *model* allowing for sharing of routing information between network layers,
- the *augmented* (or *hybrid*) *model* being the extension to the overlay model that makes information about nodes reachability available at the UNIs.

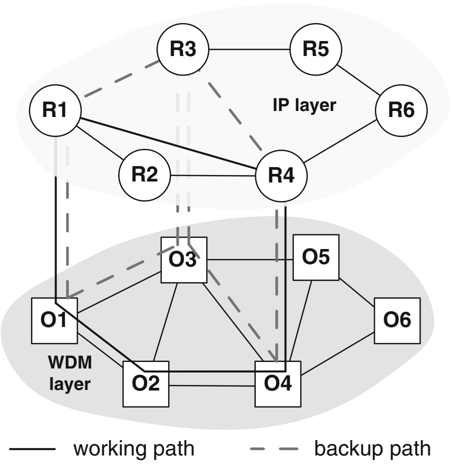


**Fig. 2.13** Example scenario of a multi-layer routing

In such a multi-layer scheme, recovery actions after failures become even more complex. In general, due to the observed *grooming* of lower-rate traffic from the upper layers into the higher-rate paths of the lower layers using time division multiplexing (TDM) [53, 58], granularity of traffic switching becomes coarser from higher to lower layers. Therefore, more recovery actions are necessary to be performed in the higher layers (i.e., restoration of many low-rate flows) than in the lower layers (where recovery is fast due to performing the recovery actions with respect to the aggregate flows). Besides, recovery time in the upper layers may be additionally increased as a result of a significant number of recovery actions to be performed.

Concerning the order of layers in which recovery actions are performed, based on [10] the following escalation strategies can be distinguished:

- *bottom-up* where recovery actions are initiated in the lowermost layer and are next propagated toward the upper layers. A clear advantage of this technique is to perform the recovery actions at an appropriate granularity. In particular, it means that handling the coarsest granularity actions in the lowermost layer is followed by recovery actions in the upper layers only with respect to flows that could not be restored at the lower layer (e.g., a failure of the end node of the lower-layer path),
- *top-down* where recovery is started in the uppermost layer. Such an approach, although allowing for a better differentiation of recovery actions concerning multiple classes of traffic, requires more complex signaling (since lower layers have no direct means to detect if the upper layer was not successful in restoring the affected traffic).

If recovery actions are available in multiple layers, then it is also important to provide the appropriate inter-layer coordination, including determination of the sequence of layers according to which recovery actions are performed.

Such coordination between network layers is necessary to prevent from multiple reactions of different layers to the same failure. This can be obtained, e.g., by the *hold-off timer* mechanism [63] used to postpone the recovery actions in the higher layer to give the lower layer time for recovery of the affected traffic. After that, recovery actions are triggered in the higher layer for all the affected traffic that could not be restored in the lower layer.

Another proposal is to use the *recovery tokens* that help shorten the time of initializing the recovery actions in the higher layer. In this case, as soon as the lower layer finishes the recovery process, it sends a signal to the higher layer to start the recovery actions there.

Due to the client-server relationship, a failure of a higher-layer node (e.g., of an IP-MPLS router) cannot be restored in the lower layer. However, the reverse, i.e., recovery of a failure occurring in the lower layer (of a lower-layer link/node) is possible in the higher layer.

In order to perform the recovery actions, each layer has to estimate the spare capacity that is necessary for rerouting of flows after failures. In particular, IP-MPLS layer is commonly responsible for handling the router failures (e.g., a failure of a router `R3` from Fig. 2.13 that cannot be dealt with by the lower layer), while the lower (optical) layer is expected to handle failures of fibers/transit OXCs. Backup resources may be shared between network layers forming the *common pool* of resources [63] in a way that the respective protection paths from different layers do not share the risk of being activated at the same time.

## 2.4 Open Issues Addressed in This Book

Although resilient routing in communication networks seems to be a well-researched topic with a number of important contributions in this field published in the literature over the last two decades, there are still a number of open issues. First of all, majority of proposed solutions is related with wired networks where capacity of links does not change over time. Secondly, proposed solutions are dedicated to current (or former) architectures, and only few research results are available addressing issues of resilient routing for new architectures of communication networks, e.g., adjusted to emerging transmission schemes such as content delivery networking, as well as responding to challenges such as large-scale disasters or attacks.

The objective of the next three chapters of this book is to highlight selected up-to-date problems of resilient routing and introduce the respective solutions for important emerging architectures of communication networks, in particular for:

1. The architecture of the *Future Internet*. Current Internet, designed over 40 years ago, is more and more facing the efficiency problems owing to the exponential increase of the traffic volume, as well as altering requirements of applications becoming more stringent with respect to Quality of Service attributes including bandwidth, latency, jitter, and packet losses. Evolving characteristics of applications, as well as emerging solutions (e.g., content delivery networking), imply differentiation of application requirements to the extent not met before and make resilient routing even more complex to achieve.

   Majority of research teams from all over the world currently pursuing their Future Internet concepts are convinced that the best approach is to make the new Internet a kind of a “hyper-network”, i.e., composed of different types of networks. Special focus is put on new functionalities such as virtualization, parallelization, redesign of data and control planes, or development of new services, all monitored by Future Internet Assembly (FIA), European Telecommunications Standards Institute (ETSI), and ITU-T.

   To address these problems, Chap. 3 of this book is to introduce new schemes of resilient routing with special focus on resilient anycasting, fast service recovery, as well as resistance to large-scale disasters and attacks.
2. Wireless Mesh Networks (WMNs) that seem to be a promising alternative to fiber-optic metropolitan area networks due to the significantly lower costs of deployment and maintenance especially in urban areas. WMNs with stationary nodes interconnected via wireless links can offer transmission rates of 1-10 Gb/s owing to millimeter-wave communications via wireless links utilizing the 71-86 GHz band. Unfortunately, millimeter-wave communications often encounters resilience problems related to weather-based disruptions, in particular caused by heavy rain falls. In such a scenario, available capacity of any

WMN link located in the area of a heavy rain fall may be seriously degraded (or even a complete link failure may be observed).

Contrary to wired networks, degradation of effective capacity of WMN links is temporal, and the network typically returns to its normal operational state after the challenge has passed. However, since duration of a challenge (e.g., duration of a rainfall) is seldom short, it is necessary to introduce solutions to provide resilient routing under challenging conditions. This issue is addressed in detail in Chap. 4 presenting the respective reliability measures for WMNs under region failures, as well as describing possible solutions to the weather-resistant routing problem.

3. Vehicular Ad-hoc Networks (VANETs) where inter-vehicle links face availability problems related not only with time-dependent link capacity fluctuations due to external factors, but also owing to mobility of network nodes. The problem of an end-to-end communication path existence is very challenging there. VANETs are seen by car manufacturers as an important solution to improve the vehicular traffic safety (for instance by warnings sent in case of accidents, low bridges, ice, or oil on road), as well as to reduce the impact of vehicles on environmental pollution (e.g., traffic light scheduling to help the driver move in the green phase). In all mentioned scenarios, fast end-to-end data dissemination is a necessity, since any such information shortly becomes useless.

In Chap. 5, we focus on end-to-end path availability and introduce the respective algorithms to provide resilient routing over “stable” wireless paths, i.e., end-to-end paths with estimated long duration (availability) time.

## References

1. Agarwal, P.K., Efrat, A., Ganjugunte, S., Hay, D., Sankararaman, S., Zussman, G.: The resilience of WDM networks to probabilistic geographical failures. In: Proc. 30th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM’11), pp. 1521–1529 (2011)
2. Asthana, R., Singh, Y.N., Grover, W.: *p*-cycles: an overview. IEEE Commun. Surv. Tutorials **12**(1), 97–111 (2010)
3. Avizienis, A., Laprie, J.-C., Randell, B.: Dependability and its threats: a taxonomy. In: Jacquart, R. (ed.) Building the information society, vol. 156, IFIP International Federation for Information Processing, pp. 91–120. Springer, New York (2004)
4. Avizienis, A., Laprie, J. C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. Technical Research Report TR2004-47, Institute for Systems Research, The University of Maryland (2004)
5. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. Dependable and Secure Comput. **1**(1), 11–33 (2004)
6. Bhandari, R.: Optimal physical diversity algorithms and survivable networks. In: Proc. 2nd IEEE Symposium on Computers and Communications (ISCC’97), pp. 433–441 (1997)
7. Bhandari, R.: Survivable Networks: Algorithms for Diverse Routing. Kluwer Academic, Boston (1999)
8. Caini, C., Cruickshank, H., Farrell, S., Marchese, M.: Delay- and disruption-tolerant networking (DTN): an alternative solution for future satellite networking applications. Proc. IEEE **99**(11), 1980–1997 (2011)

9. Cetinkaya, E.K., Sterbenz, J.P.G.: A taxonomy of network challenges. In: Proc. 9th International Conference on Design of Reliable Communication Networks (DRCN'13), pp. 322–330 (2013)
10. Chołda, P., Jajszczyk, A.: Recovery and its quality in multilayer networks. IEEE/OSA J. Lightwave Technol. **28**(4), 372–389 (2010)
11. Chołda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J., Jajszczyk, A.: A survey of resilience differentiation frameworks in communication networks. IEEE Commun. Surv. Tutorials **9**(4), 32–55 (2007)
12. 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)
13. Colle, D., De Maesschalck, S., Develder, C., Van Heuven, P., Groebbens, A., Cheyns, J., Lievens, U., Pickavet, M., Lagasse, P., Demeester, P.: Data-centric optical networks and their survivability. IEEE J. Sel. Areas Commun. **20**(1), 6–20 (2002)
14. Cowie, J., Popescu, A., Underwood, T.: Impact of Hurricane Katrina on Internet Infrastructure, Technical Report, Renesys (2005)
15. Cucurull, J., Asplund, M., Nadjm-Tehrani, S., Santoro, T.: Surviving attacks in challenged networks. IEEE Trans. Dependable and Secure Comput. **9**(6), 917–929 (2012)
16. Dijkstra, E.W.: A note on two problems in connexion with graphs. Numer. Math. **1**, 269–271 (1959)
17. Doucette, J., Giese, P., Grover, W.D.: Combined node and span protection strategies with node-encircling *p*-cycles. In: Proc. 5th International Workshop on Design of Reliable Communication Networks (DRCN'05), pp. 213–221 (2005)
18. Fangming, L., Bo, L., Lili, Z., Baochun, L., Hai, J., Xiaofei, L.: Flash crowd in P2P live streaming systems: fundamental characteristics and design implications. IEEE Trans. Parallel. Distrib. Syst. **23**(7), 1227–1239 (2012)
19. Feng, T., Ruan, L., Zhang, W.: Intelligent *p*-Cycle protection for multicast sessions in WDM networks. In: Proc. IEEE International Conference on Communications (IEEE ICC'08), pp. 5165–5169 (2008)
20. Fry, M., Fischer, M., Karaliopoulos, M., Smith, P., Hutchison, D.: Challenge identification for network resilience. In: Proc. 6th EURO-NF Conference on Next Generation Internet (NGI'10), pp. 1–8 (2010)
21. Geva, M., Herzberg, A., Gev, Y.: Bandwidth Distributed Denial of Service: attacks and defences. IEEE Secur. Priv. **12**(1), 54–61 (2014)
22. Grover, W.D.: Mesh-based Survivable Networks. Options and Strategies for Optical, MPLS, SONET, and ATM Networks. Prentice Hall PTR, Upper Saddle River (2004)
23. Grover, W.D.: The protected working capacity envelope concept: an alternate paradigm for automated service provisioning. IEEE Commun. Mag. **42**(1), 62–69 (2004)
24. Grover, W.D., Shen, G.: Extending the *p*-cycle concept to path-segment protection. In: Proc. IEEE International Conference on Communications (IEEE ICC'03), 2, pp. 1314–1319 (2003)
25. Grover, W.D., Stamatelakis, D.: Cycle-oriented distributed preconfiguration: ring-speed with mesh-like capacity for self-planning network restoration. In: Proc. IEEE International Conference on Communications (IEEE ICC'98), pp. 537–543 (1998)
26. Haddadi, H., Rio, M., Iannaccone, G., Moore, A., Mortier, R.: Network topologies: inference, modeling, and generation. IEEE Commun. Surv. Tutorials **10**(2), 48–69 (2008)
27. Haider, A., Harris, R.: Recovery techniques in Next Generation Networks. IEEE Commun. Surv. Tutorials **9**(3), 2–17 (2004)
28. Heegaard, P.E., Trivedi, K.S.: Network survivability modeling. Comput. Netw. **53**(8), 1215–1234 (2009)
29. Ho, P.-H.: State of the art progress in developing survivable routing schemes in mesh WDM networks. IEEE Commun. Surv. Tutorials **6**(4), 2–16 (2004)
30. Ho, P.-H., Tapolcai, J., Cinkler, T.: Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels. IEEE/ACM Trans. Networking **12**(6), 1105–1118 (2004)

31. Ho, P.-H., Tapolcai, J., Mouftah, H.: On achieving optimal survivable routing for shared protection in survivable Next-Generation Internet. IEEE Trans. Reliab. **53**(2), 216–225 (2004)
32. Jaumard, B., Rocha, C., Baloukov, D., Grover, W.D.: A column generation approach for design of networks using path-protecting *p*-cycles. In: Proc. 6th International Workshop on Design of Reliable Communication Networks (DRCN'07), pp. 1–8 (2007)
33. Jung, J., Krishnamurthy, B., Rabinovich, M.: Flash crowds and denial of service attacks: characterization and implication for CDNs and web sites. In: Proc. 11th International Conference on World Wide Web (WWW'02), pp. 293–304 (2002)
34. Kappenman, J.: A perfect storm of planetary proportions. IEEE Spect. Mag. **49**(2), 26–31 (2012)
35. Khabbaz, M.J., Assi, C.M., Fawaz, W.F.: Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. IEEE Commun. Surv. Tutorials **14**(2), 607–640 (2012)
36. Kiaei, M.S., Assi, C., Jaumard, B.: A survey on the *p*-cycle protection method. IEEE Commun. Surv. Tutorials **11**(3), 53–70 (2009)
37. Kitamura, Y., Lee, Y., Sakiyama, R., Okamura, K.: Experience with restoration of Asia Pacific network failures from Taiwan earthquake. IEICE Trans. Commun. **E90-B**(11), 3095–3103 (2007)
38. Kodian, A., Grover, W.D.: Failure-independent path-protecting *p*-cycles: efficient and simple fully preconnected optical-path protection. IEEE/OSA J. Lightwave Technol. **23**(10), 3241–3259 (2005)
39. Kompella, K., Swallow, G.: Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures, IETF RFC 4379 (2006)
40. Laprie, J.C.: Dependability: Basic Concepts and Terminology. IFIP Working Group 10.4 – Dependable Computing and Fault Tolerance, Springer-Verlag Wien (1994)
41. Laprie, J.-C.: Resilience for the scalability of dependability. In: Proc. Fourth IEEE International Symposium on Network Computing and Applications, pp. 5–6 (2005)
42. Liu, Y., Tipper, D., Siripongwutikorn, P.: Approximating optimal spare capacity allocation by successive survivable routing. IEEE/ACM Trans. Networking **13**(1), 198–211 (2005)
43. Maruyama, H., Legaspi, R., Minami, K., Yamagata, Y.: General resilience: taxonomy and strategies. In: Proc. 2014 International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE'14), pp. 1–8 (2014)
44. Mingsen, X., Wen-Zhan, S., Deukhyoun, H., Jong-Hoon, K., Byeong-Sam, K.: ECPC: preserve downtime data persistence in disruptive sensor networks. In: Proc. IEEE Mobile Ad-Hoc and Sensor Systems (MASS'13), pp. 281–289 (2013)
45. Misseri, X., Gojmerac, I., Rougier, J.-L.: IDRD: enabling inter-domain route diversity. In: Proc. IEEE International Conference on Communications (IEEE ICC'13), pp. 3536–3541 (2013)
46. Molisz, W.: Survivability function: a measure of disaster-based routing performance. IEEE J. Sel. Areas Commun. **22**(9), 1876–1883 (2004)
47. Molisz, W., Rak, J.: A novel class-based protection algorithm providing fast service recovery in IP/WDM networks. Lect. Notes Comput. Sci. **4982**, 338–345 (2008)
48. Molisz, W., Rak, J.: Region protection/restoration scheme in survivable networks. Lect. Notes Comput. Sci. **3685**, 442–447 (2005)
49. Mukherjee, B.: Optical WDM Networks. Springer, New York (2006)
50. Mukherjee, B., Habib, M.F., Dikbiyik, F.: Network adaptability from disaster disruptions and cascading failures. IEEE Commun. Mag. **52**(5), 230–238 (2014)
51. Neumayer, S., Zussman, G., Cohen, R., Modiano, E.: Assessing the vulnerability of the fiber infrastructure to disasters. IEEE/ACM Trans. Networking **19**(6), 1610–1623 (2011)
52. Nicol, D.M., Sanders, W.H., Trivedi, K.S.: Model-based evaluation: from dependability to security. IEEE Trans. Dependable and Secure Comput. **1**(1), 48–65 (2004)

53. Rak, J.: Fast service recovery under shared protection at connection level in WDM grooming networks. In: Proc. 22nd IEEE International Symposium on Computer and Information Sciences (ISCIS'07), pp. 1–6 (2007)
54. Rak, J.: Fast service recovery under shared protection in WDM networks. IEEE/OSA J. Lightwave Technol. **30**(1), 84–95 (2012)
55. Rak, J.: *k*-Penalty: a novel approach to find *k*-disjoint paths with differentiated path costs. IEEE Commun. Lett. **14**(4), 354–356 (2010)
56. Rak, J.: Priority-enabled optimization of resource utilization in fault-tolerant optical transport networks. Lect. Notes Comput. Sci. **4208**, 863–873 (2006)
57. Rak, J., Molisz, W.: A new approach to provide the differentiated levels of network survivability under a double node failure. In: Proc. 11th International Conference on Transparent Optical Networks (ICTON'09), pp. 1–4 (2009)
58. Rak, J., Molisz, W.: Fast service restoration under shared protection at lightpath level in survivable WDM mesh grooming networks. Commun. Comput. Inf. Sci. **1**, 362–377 (2007)
59. Ramamurthy, S., Mukherjee, B.: Survivable WDM mesh networks, Part II – Restoration. In: Proc. IEEE Integrated Circuits Conference, pp. 2023–2030 (1999)
60. Ramamurthy, B., Sahasrabuddhe, L., Mukherjee, B.: Survivable WDM mesh networks. IEEE/OSA J. Lightwave Technol. **21**(4), 870–883 (2003)
61. Ran, Y.: Considerations and suggestions on improvement of communication network disaster countermeasures after the Wenchuan earthquake. IEEE Commun. Mag. **49**(1), 44–47 (2011)
62. Sack, A., Grover, W.D.: Hamiltonian *p*-cycles for fiber-level protection in semi-homogeneous, homogeneous, and optical networks. IEEE Netw. **18**(2), 49–56 (2004)
63. Schupke, D.: Multilayer and multidomain resilience in optical networks. Proc. IEEE **100**(5), 1140–1148 (2012)
64. Sichitiu, M.L., Kihl, M.: Inter-vehicle communication systems: a survey. IEEE Commun. Surv. Tutorials **10**(2), 88–105 (2008)
65. Siller, C.A., Shafi, M.: Synchronous Networking. IEEE Press, IEEE Communications Society, New York (1996)
66. Smith, P., Hutchison, D., Sterbenz, J.P.G., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, M., Plattner, B.: Network resilience: a systematic approach. IEEE Commun. Mag. **49**(7), 88–97 (2011)
67. Steinder, M., Sethi, A.: A survey of fault localization techniques in computer networks. Sci. Comput. Program. **53**(2), 165–194 (2004)
68. Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., Qian, S., Rohrer, J.P.: Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. Telecommun. Syst. **52**(2), 705–736 (2013)
69. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: strategies, principles, and survey of disciplines. Comput. Netw. **54**(8), 1245–1265 (2010)
70. Suurballe, J.W.: Disjoint paths in a network. Networks **4**(2), 125–145 (1974)
71. Suurballe, J.W., Tarjan, R.E.: A quick method for finding shortest pairs of disjoint paths. Networks **14**(2), 325–336 (1984)
72. T1A1.2 Working Group: Reliability-related metrics and terminology for network elements in evolving communication networks. American National Standard for Telecommunications T1. R1.524-2004, Alliance for Telecommunications Industry Solutions – ATIS (2004)
73. Tapolcai, J., Chołda, P., Cinkler, T., Wajda, K., Jajszczyk, A., Autenrieth, A., Bodamer, S., Colle, D., Ferraris, G., Lonsethagen, H., Svinnset, I.-E., Verchere, D.: Quality of resilience (QoR): NOBEL approach to the multi-service resilience characterization. In: Proc. 2nd International Conference on Broadband Networks (BROADNETS'05), 2, pp. 1328–1337 (2005)
74. Urushidani, S., Aoki, M., Fukuda, K., Abe, S., Nakamura, M., Koibuchi, M., Ji, Y., Yamada, S.: Highly available network design and resource management of SINET4. Telecommun. Syst. **56**(1), 33–47 (2014)

75. Xiong, Y., Xu, D., Qiao, C.: Achieving fast and bandwidth-efficient shared-path protection. IEEE/OSA J. Lightwave Technol. **21**(2), 365–371 (2003)
76. Xu, D., Chen, Y., Xiong, Y., Qiao, C., He, X.: On the complexity of and algorithms for finding the shortest path with a disjoint counterpart. IEEE/ACM Trans. Networking **14**(1), 147–158 (2006)
77. Xu, D., Qiao, C., Xiong, Y.: An ultra-fast shared path protection scheme – Distributed partial information management – Part II. In: Proc. 10th IEEE International Conference on Network Protocols (IEEE ICNP'02), pp. 344–353 (2002)
78. Zhang, F., Zhong, W.: Performance evaluation of *p*-cycle based protection models for provisioning of dynamic multicast sessions in WDM networks. Photon. Netw. Commun. **16**(2), 127–138 (2008)

# Chapter 3
# Resilience of Future Internet Communications

Over the last 40 years, we have been observing a gradual evolution of the Internet from an academic network towards a widespread commercial architecture. Indeed, current Internet, designed in the 1970s by Vinton G. Cerf and Robert E. Kahn [14] as a network of networks, evolved from its predecessor – the ARPANET academic network connecting computing sites at universities across the US [43].

Internet was originally meant to be a computer communication network of datagram orientation only (i.e., mainly for conservative data traffic usage). Afterward, it has been progressively adapted to meet the evolving diverse expectations of end users with respect to services and applications of daily use to enhance the quality of life [9]. In particular, owing to the observed convergence of telecommunications, media, and information technology, Internet is now becoming an integrated system enabling accessing, distributing, processing, storing, and managing the content [60].

However, the main architectural changes to the Internet architecture have been mostly the "last minute" fixes/updates, while important modifications have recently become practically infeasible [61]. Besides, current Internet has already reached its limits where even minor improvements do not have much chance to succeed. Therefore, a comprehensive transformation of the Internet from a simple "host-to-host" packets exchange environment towards a complex networking paradigm built around the content and end users instead of network nodes is inevitable [55]. Following [60], major challenges driving the research efforts toward the *Internet of the Future* include:

- identification of a large set of network nodes,
- scalability and efficiency of network and mobility management,
- Quality of Service,
- security,
- performance reliability,
- energy efficiency.

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications and Networks, DOI 10.1007/978-3-319-22333-9_3

Since without doubt future knowledge society will be built on Internet communications base, any limitations referring to the efficiency of Internet must be defeated. Otherwise, end users may not be able to fully benefit from a number of emerging technologies, e.g., advanced wireless/mobile communications, broadband optical networking, huge storage capacity, or innovative techniques including sensors and energy sources [60].

All these demands have driven the research community to design the respective Future Internet (FI) solutions within various research activities intensively supported in the last decade for instance by the European Commission [25], National Science Foundation in the US [52], and others. As a result, one/two Future Internet Assemblies [53] have been organized every year since 2008 to discuss the outcomes of numerous ongoing FI research projects, as well as to summarize their achievements in the respective FIA books (see for instance [8, 23, 67]).

Apart from the European activities in this area, including e.g., 4WARD [63], FIRE [27], GEANT2 [30], or IIP [29], there have been also other important initiatives from the US (e.g., FIA [28], FIND [52, 54], GENI [34], MobilityFirst [48], or NDN [49]), Japan (e.g., AKARI [3]), and China (e.g., CERNET [15]).

It is worth noting that there is no standardized/publicly accepted definition for the Future Internet. Instead, it is mostly described by a set of relevant capabilities not existing in the current Internet architecture. As discussed in [8, 23, 24, 55, 56, 61], the list of desired functionalities of the Future Internet architecture includes the following:

– *content-oriented networking* being an opposite solution to the conventional host-to-host information delivery, as primary utilization of the Internet gradually evolves into data/content distribution. A widely observable trend is to design the architecture of the Future Internet "around people" instead of around machines [55], implying the need to update the IP layer to provision content distribution, and making information (rather than conventional IP addresses) the primary search goal,
– *cloud computing/communications*. Combining data centres and computation possibilities into the cloud to form a "computing utility" available over the Internet is seen as an efficient solution to provide the global-scale resource and computation capabilities,
– *novel human-computer interaction techniques* driven by the availability of cheap sensor technology that may soon revolutionize the way humans interact with computers (i.e., via human gestures, as well as displays integrated with objects of everyday use),
– real-time access to huge-scale multimedia content (known as the *Big Data* paradigm), e.g., to 3D and cognitive content, virtual, and augmented world,
– *users acting as service providers*, e.g., selling photos, or operating as stream broadcasters. Other examples include inter-vehicular communications (as discussed in Chap. 5 of this book), where a system installed in a vehicle may automatically inform other vehicles about accidents, ice on road, etc.,

- *personalized services* including personalized (or context-aware) search results, person-(group-)oriented services targeting specific interest groups,
- *mobility-centric orientation enabling ubiquitous access to information anytime and anywhere*. Due to the observed shift from stationary (PC-based) computing to mobile computing, as well as the convergence of heterogeneous networks, mobility is now one of the key functionalities of the Future Internet. It should be thus considered as a norm, rather than an exception,
- *interconnection of devices, sensors*, etc. (known as the Internet of Things – *IoT* concept) into networks of diverse physical objects, such as vehicles, mobile phones, etc.,
- *networks programmability* offered by virtualized software-defined networks with network control functions being directly programmable and decoupled from forwarding [62], [73],
- *security* mechanisms forming an inherent part of the FI architecture (as opposed to functioning as an additional overlay in the current Internet), which is justified from both technical and economical reasons,
- *energy efficiency*. Gradual growth of Internet traffic volume brings about increasing energy consumption by networking equipment to accommodate the demands. One of solutions to save the energy may be switching off the devices, or putting them into the sleep mode in inactive periods,
- *availability and disruption-tolerance*. The Internet is viewed as an important element of a critical infrastructure (similar to e.g., fresh water supplies, or power grids). Therefore, architecture of the Future Internet should be also resistant to disruptions of any kind, providing the alternate means for content distribution/processing in the face of failures, as well as guaranteeing fast recovery of affected network elements.

Another classification of FI main research areas from [60] is presented in Fig. 3.1. In particular, issues of Future Internet resilience are included in areas #2 (Future Internet modeling, analysis, and design) and #3 (Future Internet network architectures), accordingly.

In order to support these functionalities, one of possible ways proposed by the research community is the so-called *clean-slate* concept, in which applying certain solutions may be done under the assumption that other parts of the architecture remain unchanged [26, 55]. Therefore, deploying a number of clean-slate solutions may not necessarily lead to a new architecture of the Internet. Besides, redesign of the Internet architecture should utilize the best practices from the past, as well as be evolvable and flexible for the purpose of accommodating the future demands [55].

In the clean-slate paradigm, there are practically no restrictions on the architectural design of the Future Internet. However, since today's Internet is connecting billions of nodes and supporting millions of applications, even though the new architecture is expected to be revolutionary, its application should be done on an evolutionary basis. In particular, "new technology" nodes should be able to communicate over the existing infrastructure. Researchers are convinced that the Future Internet has to be designed in a dynamic and modular way that allows for further adaptive changes [9].

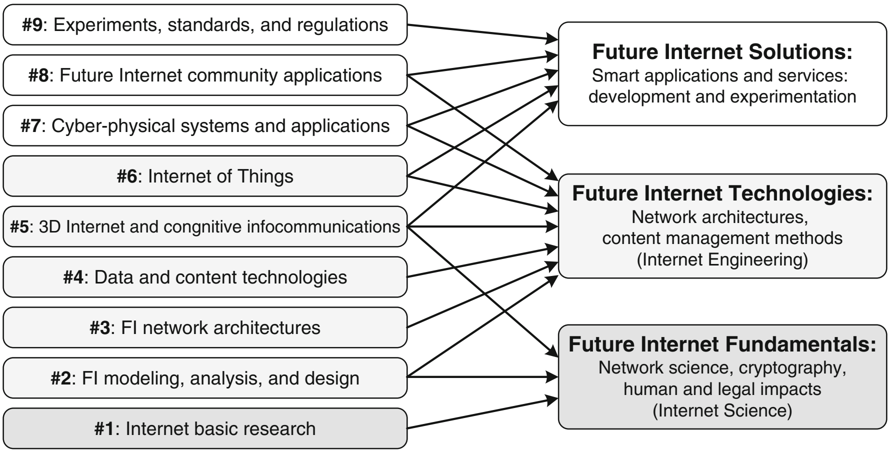

**#9**: Experiments, standards, and regulations
**#8**: Future Internet community applications
**#7**: Cyber-physical systems and applications
**#6**: Internet of Things
**#5**: 3D Internet and congnitive infocommunications
**#4**: Data and content technologies
**#3**: FI network architectures
**#2**: FI modeling, analysis, and design
**#1**: Internet basic research
**Future Internet Solutions:** Smart applications and services: development and experimentation
**Future Internet Technologies:** Network architectures, content management methods (Internet Engineering)
**Future Internet Fundamentals:** Network science, cryptography, human and legal impacts (Internet Science)

**Fig. 3.1** Future Internet research areas in relation to their goals from [60]

In the remaining part of this chapter, we will discuss in detail the key research topics and requirements for the FI architecture (Sect. 3.1), present our solutions to network resource provisioning necessary to provide network resilience (Sect. 3.2), and describe in Sect. 3.3 three proposals to improve resilience of content-oriented FI networking. The chapter is summarized in Sect. 3.4.

## 3.1 Key Research Topics and Requirements for the Future Internet Architecture

Considering the architectural requirements on the Future Internet, a distinction between providers of a network infrastructure (i.e., physical resources) and providers of network services becomes apparent and justifies the need of *virtual networks* implementation. Such a scheme allowing to lease the physical network resources (e.g., node processing power, link capacity, etc.) to deploy the end-to-end services, as well as having a certain control on the usage of these leased resources (being one of the main foundations of virtual local area networks – VLANs, virtual private networks – VPNs, or overlay networks [18]), has now evolved with respect to the Future Internet architecture into the *virtualization* scheme [11, 68].

Following [64], *network virtualization* benefits from decoupling the single role of common *Internet service providers* (*ISPs*) into two independent entities: *infrastructure providers* (*InPs*) managing the physical infrastructure of networks, and *service providers* (*SPs*) offering the end-to-end services via *virtual networks* (*VNs*) created and managed by them based on aggregating resources from multiple InPs.[1] In such a virtualized networking scheme, the set of multiple heterogeneous network

[1] In general, the idea of identifying the separate roles of InPs and SPs is not new (it has been proposed for the *information society* paradigm before).

architectures owned by different service providers that can be utilized to form a virtual network by the InP is often referred to as the *network virtualization environment* (*NVE*) [18], as presented in Fig. 3.2.

Virtual network is the basic entity in any NVE. It consists of *virtual nodes* (hosted on a given physical node) linked together by *virtual links* typically provided by paths in the physical network utilizing the respective resources from the physical layer (mainly link capacities and processing power of transit physical nodes). Therefore, end users can benefit in the NVE from multiple virtual networks managed by different SPs for a number of services.

Following [18], network virtualization implies:

- *coexistence* of many virtual networks of different SPs utilizing physical resources from at least one InP [6],
- *inheritance* allowing child VNs inherit the architectural attributes of their parent VNs [43],
- *recursion* being a parent–child relationship for virtual networks (see Fig. 3.2) creating the VN hierarchy (i.e., VNs built on top of other VNs), often referred to as *nesting* [45],
- *revisitation* enabling hosting multiple virtual nodes from a given VN by a single physical node [64].

Network virtualization leading to transformation into logical networks built on top of the existing physical network infrastructure can be thus viewed as an evolved form of the overlay networking concept. Similar to the original idea of overlays, deployment of new network virtualization environments does not require changes

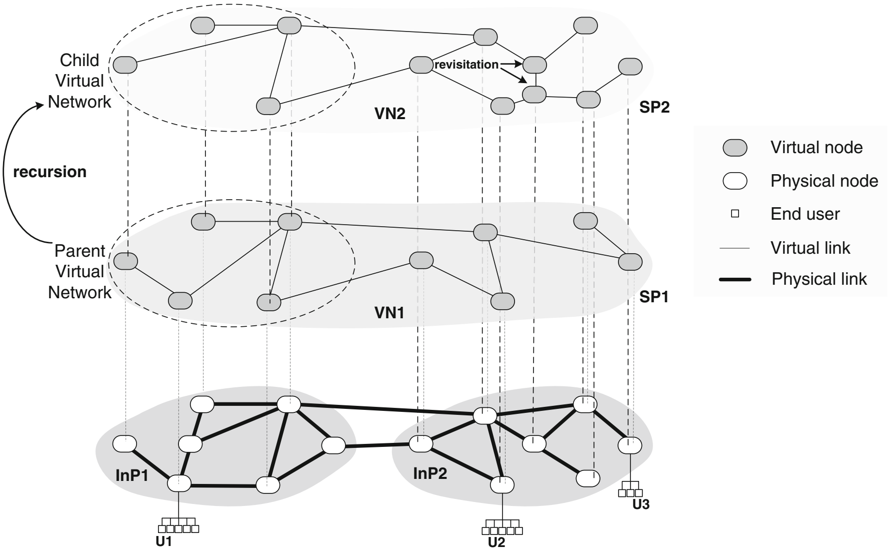


**Fig. 3.2** Example network virtualization environment (NVE) with virtual network VN1 created on top of InP1 and InP2 resources, and VN2 additionally implementing partial parent-child relationship with VN1

to the underlying physical network once it is set up to support network virtualization [18]. Therefore, virtualization is expected to be a scalable scheme able to offer relatively easy and inexpensive means to configure communication environments for end-to-end services.

A proper evaluation of Future Internet solutions requires utilization of *large-scale testbeds* [55]. However, a number of ongoing (and completed) projects related to FI architectures use either small testbeds (e.g., of a national scale), multiple heterogeneous testbeds (e.g., multiple testbeds with differentiated schemes deployed), or simply infrastructure of the current Internet, as well as testbeds of previous research project not related to FI architectures.

In a network virtualization environment, a proper reservation of physical network resources is necessary for provisioning the end-to-end services by service providers to meet the stringent requirements related to Quality of Service. As such, it is also an important element to support the resilient routing (for instance by efficient reservation of network resources for the purpose of alternate paths establishment) in the face of differentiated challenges and should be considered as an important part of any Future Internet architecture.

Therefore, in the following Sect. 3.2, we will highlight the concept of network resource provisioning for virtualization environments proposed in the example framework of one of major European research projects on Future Internet architecture by researchers from Polish technical universities and research centres in 2010–2013, called Future Internet Engineering [29]. In particular, solutions to the network resource provisioning problem implemented in "System IIP" – the core part of the designed FI architecture, allow for automatic reservation of physical network resources for co-existing virtual networks of differentiated transmission types.

The respective network resource provisioning module implemented by us for System IIP includes three Integer Linear Programming models introduced to obtain the optimal solutions to the respective network resource provisioning problems. This module, being an important part of the management system, is to be utilized periodically to update the resource provisioning solutions to respond to changes of end-to-end demands over time.

## 3.2 Network Resource Provisioning Concepts in the "System IIP" Future Internet Architecture

Among a number of completed and ongoing projects related to the Future Internet architecture design, the Polish initiative called Future Internet Engineering resulted in the four-layer architecture of the so-called System IIP, comprising in the bottom-up order: L1 – physical infrastructure layer, L2 – virtualization layer, L3 –Parallel Internets layer, and L4 – virtual networks layer [12, 13]. This architecture, characterized by the ability to adjust its properties based on the required transmission scheme, was designed to provide co-existence of

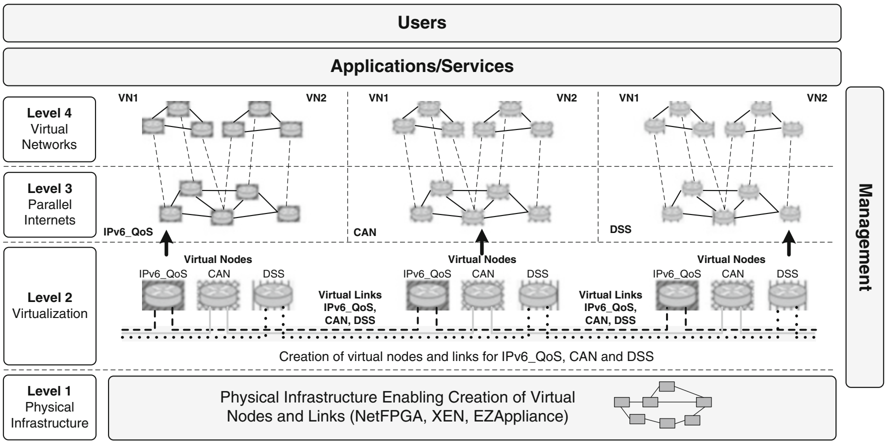


**Fig. 3.3** Architecture of System IIP from [12]

differentiated types of Parallel Internets (PIs) within one physical infrastructure, including IPv6 with Quality of Service (IPv6_QoS), Content-Aware Network (CAN), and Data Stream Switching (DSS), as shown in Fig. 3.3.

In this section, we focus on the Future Internet resource provisioning issues, in particular concerning architectural aspects of L1/L2 resource provisioning module implemented by us in the System IIP architecture. Allocation of requested resources is provided here periodically in a static way. Therefore, before each consecutive update of the network resource provisioning solution, a traffic matrix is prepared in advance. Additional constraints (for example on link propagation delay with respect to given PIs) may be also introduced.

The objective of the network resource provisioning module is to assign elementary resources (such as link capacity, or node processing power) to three investigated Parallel Internets and to the management system enabling virtualization of nodes and links [16, 20]. The following three schemes aimed at providing the optimal solution to the respective Linear Programming (LP) problems were implemented in the System IIP architecture, as described in [36].

## Model 1: Formulation of Link Bandwidth Utilization Optimization Problem Respecting Basic Requirements on Routing (LBUO)

### Indices

$\Gamma(N, A)$ Directed network, where $N$ and $A$ are the sets of network nodes and directed arcs, accordingly; each network link is represented by two opposite arcs $a_h = (i, j)$ and $a_{h'} = (j, i)$; $|N|$ and $|A|$ are the numbers of network nodes and arcs, accordingly

$T$ Set of transit (forwarding) nodes

$N\backslash T$ Set of edge nodes

$M$ Set of instances of Parallel Internets (here referring to IPv6_QoS, CAN, and DSS Internets, accordingly; $|M| = 3$)

$D_m$ Set of demands $r$ for each $m$-th Parallel Internet, $r = 1, 2, \ldots, |D_m|$

### Constants

$c_h$ Total capacity available at arc $a_h$

$\breve{c}_{m,h}$ The lower bound on capacity (i.e., fraction of link capacity) required at arc $a_h$ for $m$-th instance of PI

$d_{r,m}$ Volume of demand $r$ from $m$-th instance of PI

$s_{r,m}$ Source node of demand $r$ from $m$-th instance of PI

$t_{r,m}$ Destination node of demand $r$ from $m$-th instance of PI

### Variables

$x_{m,h} \geq 0$ Capacity assigned for $m$-th PI at arc $a_h$

$z_{r,m,h} \geq 0$ Capacity assigned for demand $r$ of $m$-th PI at arc $a_h$

### Objective

It is to minimize the total bandwidth consumption for delivering the traffic defined by formula (3.1):

$$\varphi(\mathbf{x}) = \sum_{m \in M} \sum_{h \in A} x_{m,h} \tag{3.1}$$

### Constraints

1. To assure that the amount of flow leaving node $n$ via arc $a_h$ for $m$-th Parallel Internet is the same as the amount of flow received at the other end of arc $a_h = (i, j)$:

$$\sum_{n: a_h \equiv (i,n) \in A} x_{m,h} = \sum_{n: a_h \equiv (n,j) \in A} x_{m,h}; \quad m \in M; \quad h : a_h = (i, j) \in A \tag{3.2}$$

2. To provide flow conservation rules at transit nodes for total capacities assigned to each $m$-th PI:

$$\sum_{\substack{h \in \{h : a_h \equiv (t,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} x_{m,h} = \sum_{\substack{h \in \{h : a_h \equiv (i,t) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} x_{m,h}; \quad m \in M; \quad t \in T \tag{3.3}$$

3. On the lower bound on the aggregate capacity assigned to $m$-th PI at arc $a_h$:

$$x_{m,h} \geq \overset{\smile}{c}_{m,h} c_h; \quad m \in M; \quad h \in A \tag{3.4}$$

4. On the upper bound on the total flow passing via network links for all PIs:

$$\sum_{m \in M} x_{m,h} \leq c_h; \quad h \in A \tag{3.5}$$

5. To provide flow conservation rules for demands $r$ of each $m$-th PI:

$$\sum_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} z_{r,m,h} - \sum_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} z_{r,m,h} = \begin{cases} d_{r,m}, & if \quad n = s_{r,m} \\ -d_{r,m}, & if \quad n = t_{r,m} \\ 0, & \text{in other cases} \end{cases} ; r \in D_m; \quad m \in M; \quad n \in N \tag{3.6}$$

6. To guarantee that the aggregate flow transported via arc $a_h$ for all demands of $m$-th PI does not exceed the capacity reserved for this PI at arc $a_h$:

$$\sum_{r \in D_m} z_{r,m,h} \leq x_{m,h}; \quad m \in M; \quad h \in A \tag{3.7}$$

We also implemented another objective function aimed at maximizing the total residual (free) capacity at all arcs, as given in Eq. 3.8. This objective is suitable when determining the capacity assignment in a way to increase the residual capacity margin (necessary, e.g., to apply the resilience schemes based on backup paths).

$$\varphi(\mathbf{x}) = \sum_{h \in A} \left( c_h - \sum_{m \in M} x_{m,h} \right) \tag{3.8}$$

The next model implemented in System IIP is an extension to the LBUO model by additional constraints referring to node resource optimization issues. Therefore, it also includes constraints on node resources (here related to node processing power).

## Model 2: Extension of LBUO Model Including Basic Requirements on Node Resource Utilization Optimization Issue (LBNR)

**Indices** the same as in LBUO model

**Constants**
Compared to the LBUO model, the list of constants is additionally extended by the following:

$\theta_{m,h}$ ($\rho_{m,h}$) Consumption of node processing power measured per unit capacity for $m$-th PI defined for outgoing (incoming) arc $a_h$
$\phi_n$ Aggregate processing power at node $n$

**Variables**
The list of variables is the same as in LBUO model and additionally includes the following:

$\wp_{m,n} \geq 0$ Amount of resources reserved to process flows from $m$-th PI at node $n$ (in MFlops)

**Objective**
It is to minimize the total processing power to deliver the traffic defined by formula (3.9):

$$\varphi(\mathbf{x}) = \sum_{m\in M}\sum_{n\in N}\wp_{m,n} \tag{3.9}$$

**Constraints**
The set of constraints includes formulas (3.2–3.7) and is additionally extended by constraint (3.10) referring to calculation of node $n$ processing power utilization related to the portion of capacity reserved for each $m$-th PI, and formula (3.11) providing the upper bound on the total processing power available at node $n$ for the purpose of serving all demands.

$$\wp_{m,n} = \sum_{\substack{h\in\{h:a_h\equiv(n,j)\in A;\\ j=1,2,\ldots,|N|;j\neq n\}}} \theta_{m,h}x_{m,h} + \sum_{\substack{h\in\{h:a_h\equiv(i,n)\in A;\\ i=1,2,\ldots,|N|;i\neq n\}}} \rho_{m,h}x_{m,h}; \quad m\in M;\ n\in N \tag{3.10}$$

$$\sum_{m\in M}\wp_{m,n} \leq \phi_n; \qquad n\in N \tag{3.11}$$

The last of the three network resource provisioning models implemented in System IIP includes additional constraints on the maximum allowed transmission delay for delay-sensitive streams. In this model, any potential path is verified with respect to its end-to-end delay defined as the sum of delays along all network arcs $a_h$ forming the path. Therefore, in this case any valid solution must consist of paths compliant with upper bounds on end-to-end delay.

## Model 3: Extension of LBNR Model Including Additional Constraints on End-to-end Delay (LBDC)

**Indices** The same as in LBUO model

**Constants**
Compared to LBUO and LBNR models, the list of constants is additionally extended by:

$p_h$ Upper bound on transmission delay along arc $a_h$
$p_{m,r}$ Upper bound on end-to-end transmission delay for demand $r$ from $m$-th Parallel Internet
$G$ Arbitrarily chosen large value

**Variables**
The list of variables is the same as in LBNR model and additionally includes the following:

$v_{r,m,h}$ Equals 1, if arc $a_h$ is used to forward the traffic referring to demand $r$ of $m$-th PI; 0 otherwise

**Objective**
The same as in LBUO model (i.e., Eq. 3.1)

**Constraints**
The set of constraints includes formulas (3.2–3.7, 3.10, and 3.11), and is extended by formula (3.12) to guarantee that the end-to-end transmission delay for any demand $r$ from $m$-th Parallel Internet does not exceed a predefined upper bound, as well as formula (3.13) combined with constant $G$ necessary to bind the respective binary variable $v_{r,m,h}$ with the continuous variable $z_{r,m,h}$.

$$\sum_{h \in A} v_{r,m,h} p_h \leq p_{m,r}; \qquad r \in D_m; \quad m \in M \tag{3.12}$$

$$z_{r,m,h} \leq v_{r,m,h} G; \qquad r \in D_m; \quad m \in M; \quad h \in A \tag{3.13}$$

In general, all three problems were proved to be $NP$-complete in [37]. Therefore, for larger problem instances, it is necessary to use one of suboptimal heuristic approaches, e.g., the one we proposed in [37].

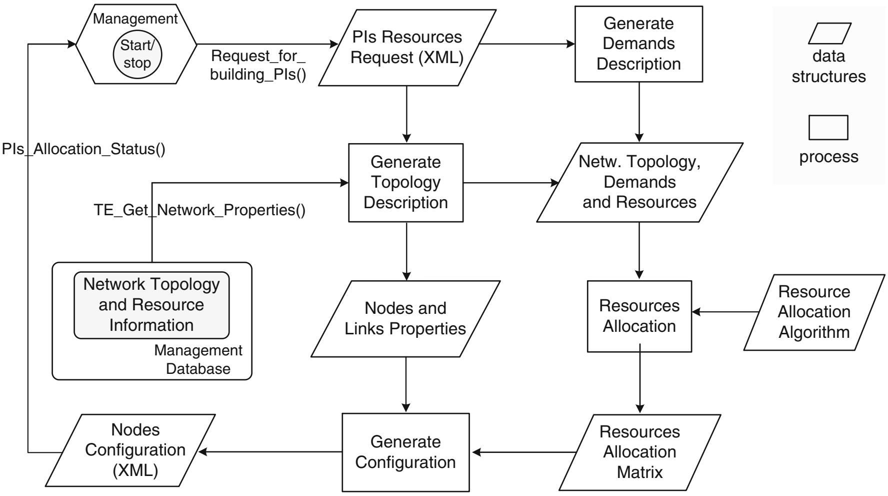

Management
Start/stop
Request_for_building_PIs()
PIs Resources Request (XML)
Generate Demands Description
data structures
process
PIs_Allocation_Status()
Generate Topology Description
Netw. Topology, Demands and Resources
TE_Get_Network_Properties()
Network Topology and Resource Information
Management Database
Nodes and Links Properties
Resources Allocation
Resource Allocation Algorithm
Nodes Configuration (XML)
Generate Configuration
Resources Allocation Matrix

**Fig. 3.4** Functional diagram of network resource provisioning module in System IIP architecture from [37]

Owing to utilization of the implemented network resource provisioning module with respect to the core network (i.e., characterized by little fluctuations of the aggregate flows over time), it is reasonable to activate the resource provisioning procedure once every several hours/days. Figure 3.4 presents a functional diagram of the network resource provisioning module in the System IIP architecture.

Three introduced Linear Programming models of network resource provisioning implemented by us in System IIP have been validated for the real large-scale testbed deployed in IIP project and passed all necessary tests. Similar approaches to determine the optimal solution to the network resource provisioning problem are often applied in the design of resilient network architectures with the aim to decide not only on resource provisioning with respect to the primary communication paths, but also concerning backup routes, as discussed in detail in Sect. 3.3 for the information-centric networking concept (the paradigm of one of PIs addressed in this chapter).

## 3.3 Fault Tolerance of Content-Oriented Networking

Owing to the remarkable increase of the Internet traffic in recent years (even four times between 2010 and 2015, following [1]), as well as further predictions of expected exponential increase (mainly attributed to the exchange of various forms of objects, including video, music, and other documents), Future Internet architecture should be characterized by built-in efficient and scalable techniques of content distribution. Indeed, contrary to conventional host-centric communications based on named hosts, currently widely discussed *content-oriented networking* (*CON*) concept (often referred to as *data-oriented networking* [32, 44], or *information-centric networking* (*ICN*) [5, 66, 74]) to provide access to *named data objects* (*NDOs*) [1, 51], focuses on objects of practically any kind that people wish to store and access as the main elements to be addressed. Although the idea itself is not new (see e.g., solutions of peer-to-peer information exchange from [17, 31]), there is no such a built-in mechanism available for the current Internet.

Following [1], an NDO – the main abstraction in information-centric networking does not depend on location, storage method, etc. Therefore, its name is considered as an identity regardless of its physical location. Naming an object in information-centric networking is thus as important as issues of naming a host in a conventional scheme. Object names should be unique since they are used for identification independent of their location.

Several copies of an NDO stored in the Internet should thus be equivalent. It means that any node that holds a copy of an object should be able to provide it to the requesting node, if a node with the original NDO is not available (for instance due to the node failure, or a failure of a transit link/node of a communication path). It is important to assure a reliable distribution of content in a failure-prone environment, especially with sparse connectivity, or high-speed mobility [19].

Considering routing issues, there are several approaches to retrieve information from source nodes of the content. Among them, it is important to mention the approach implemented in Data-oriented Network Architecture project [44], where content is published into the network by the sources. Nodes hosting the data have to register themselves at "resolution handlers" that next forward the requests to them from the requesting nodes. Data is further delivered from the source node:

- via the reverse path of a request,
- as information cached at one of transit nodes (some nodes can use cache memory to act as sources of object copies once they have forwarded the content to the requesting nodes),
- over a shorter (i.e., a more direct) route.

Under *content-centric networking* (*CCN*), content is published at original nodes [32]. Therefore, routing is needed to disseminate information about location of the content around the network.

In general, the considered scheme allowing for serving the content by one of many potential servers, each one storing a copy (also called a replica) of the original object is referred to as *anycasting* in the literature [38]. This paradigm will be investigated in detail in the later part of this section, where we focus on improving the resilience of information-centric networking and present our approaches from [59, 71, 72] to provide protection against failures of network elements by means of alternate paths to such a replicated content.

### 3.3.1 The Concept of Survivable Anycasting

Anycasting – a one-to-one-of-many transmission technique [47] commonly utilized by a number of services including Content Delivery Networks (CDNs), Domain Name System (DNS), peer-to-peer (P2P) systems, or video streaming, due to possibility to retrieve the content from one of many locations, decreases the overall network load as well as latency, compared to the common unicast (i.e., one-to-one) transmission. Anycasting can also provide survivability of stored information, since, unlike in unicasting, in the case of a failure of a node hosting the content, information can be retrieved from another replica server (as e.g., in Fig. 3.5) [70].

Our proposal from [72] presented here aims at optimizing routing of anycast and unicast flows with special focus on assuring survivability of the affected traffic. Such a joint optimization scheme is reasonable due to the co-existence of these transmission types in contemporary networks. For instance, the growing popularity of content delivery networking [65, 75] is responsible for 20 % share of Internet traffic currently served by the Akamai system [2].

In case of anycast traffic, in order to provide survivability against single failures of end nodes, the content has to be stored in parallel at two different replica servers accessible by means of node-disjoint paths [69]. For unicast traffic, a conventional end-to-end path protection scheme can be used. The novelty of our approach, compared to other results available in the literature (e.g., [7, 22, 46, 49, 69]), is in application of a single backup path method aimed at providing 100 % protection for both anycast and unicast demands.

In this section, we present an optimization model to provide protection against single link failures (i.e., establishing link-disjoint paths), as well as failures

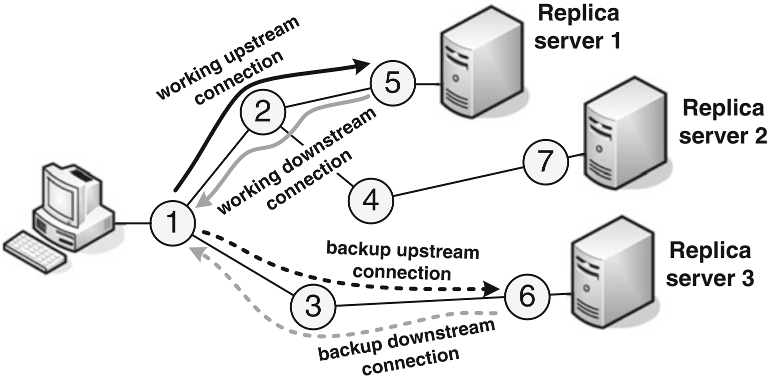

Replica server 1
Replica server 2
Replica server 3
working upstream connection
working downstream connection
backup upstream connection
backup downstream connection
1
2
3
4
5
6
7

**Fig. 3.5** An example of survivable anycast routing with a backup path leading to another replica server

of replica nodes (by utilization of different primary and backup replicas). The model is related to the physical infrastructure of optical networks, which can be well justified by common utilization of WDM technology in backbone networks.[2] Therefore, in this section, we consider a directed network $\Gamma(N, A)$, where $N$ is a set of nodes, and $A$ is a set of directed arcs. Each arc $a_h \in A$ is characterized by cost $\xi_h$ (referring to the length of arc $a_h$) and offers $\Lambda$ unidirectional channels, each of a standard capacity. Replica servers are located at nodes selected in advance in the network planning phase.

All network flows are modeled as non-bifurcated multicommodity flows. In this model, we assume that for each demand $r$, the requested capacity is equal to the capacity of a single WDM channel (i.e., $d_r = 1$). In anycast communications, we have upstream and downstream demands (referring to sets $D^{US}$ and $D^{DS}$, accordingly). Each anycast demand $r$ is related to a given client node (being the source $s_r$ / destination $t_r$ node of the upstream/downstream demand, respectively).

Each anycast upstream (downstream) demand $r \in D^{US}$ ($D^{DS}$) has to be associated with the respective downstream (upstream) anycast demand (denoted as $\tau(r)$) referring to the same client node. As shown in Fig. 3.5, both associated anycast demands $r$ and $\tau(r)$ must be related with the same replica node. Since all replica servers located in the network are assumed to provide the same content, working and backup paths can lead to any two of them. The proposed ILP model is defined as follows:

### Indices

| | |
|---|---|
| $N$ | Set of network nodes |
| $n$ | Network node |
| $A$ | Set of arcs representing directed links |
| $h$ | Arc index |
| $D$ | Set of demands |
| $D^{UN}$ ($D^{AN}$) | Set of unicast (anycast) demands |
| $D^{DS}$ ($D^{US}$) | Set of anycast downstream (upstream) demands |
| $r$ | Demand index |
| $\tau(r)$ | Index of a demand associated with demand $r$ |

### Constants

$s_r$ ($t_r$) Source (destination) node of $r$-th demand. For dowstream anycast demands, we are given only the destination nodes $t_r$, while for upstream anycast demands only source nodes $s_r$ are defined

$c_h$ Capacity of arc $a_h$, here given by the number $\Lambda$ of unidirectional optical channels

[2] This approach can be easily adapted for other networking solutions (e.g., for overlay anycasting by replacing the term "optical channel capacity" with capacity of a virtual link).

$\xi_h$ Cost (length) of arc $a_h$

$u_n$ Equals 1, if node $n$ is a replica node; 0 otherwise

$\chi_{r,n}$ Equals 1, if node $n$ is the closest replica for anycast demand $r$; 0 otherwise

### Variables

$x_{r,h}$ Equals 1, if arc $a_h$ is used by the working path of $r$-th demand; 0 otherwise

$y_{r,h}$ Equals 1, if arc $a_h$ is used by the backup path of $r$-th demand; 0 otherwise

$\kappa_{r,n}$ Equals 1, if a replica server located at node $n$ is selected as a working replica of $r$-th anycast demand; 0 otherwise

$v_{r,n}$ Equals 1, if a replica server located at node $n$ is selected as a backup replica of $r$-th anycast demand; 0 otherwise

### Objective

It is to minimize the total cost of delivery of flows by means of working and backup paths given by formula (3.14).

$$\varphi(\mathbf{x}) = \sum_{r\in D}\sum_{h\in A}\xi_h\left(x_{r,h}+y_{r,h}\right) \tag{3.14}$$

### Constraints

1. To provide flow conservation rules of working paths of unicast demands:

$$\sum_{\substack{h\in\{h:\,a_h\equiv(n,j)\in A;\\ j\in N;\,j\neq n\}}} x_{r,h} \quad - \sum_{\substack{h\in\{h:\,a_h\equiv(i,n)\in A;\\ i\in N;\,i\neq n\}}} x_{r,h} = \begin{cases} 1, & if\ \ n=s_r\\ -1, & if\ \ n=t_r\ ;\\ 0, & otherwise \end{cases} \quad r\in D^{UN};\quad n\in N \tag{3.15}$$

2. To provide flow conservation rules of backup paths of unicast demands:

$$\sum_{\substack{h\in\{h:\,a_h\equiv(n,j)\in A;\\ j\in N;\,j\neq n\}}} y_{r,h} \quad - \sum_{\substack{h\in\{h:\,a_h\equiv(i,n)\in A;\\ i\in N;\,i\neq n\}}} y_{r,h} = \begin{cases} 1, & if\ \ n=s_r\\ -1, & if\ \ n=t_r\ ;\\ 0, & otherwise \end{cases} \quad r\in D^{UN};\quad n\in N \tag{3.16}$$

3. To provide flow conservation rules of working paths of anycast downstream demands:

$$\sum_{\substack{h\in\{h:\,a_h\equiv(n,j)\in A;\\ j\in N;\,j\neq n\}}} x_{r,h} \quad - \sum_{\substack{h\in\{h:\,a_h\equiv(i,n)\in A;\\ i\in N;\,i\neq n\}}} x_{r,h} = \begin{cases} -1, & if\ \ n=t_r\\ \kappa_{r,n}, & if\ \ n\neq t_r \end{cases}; \quad r\in D^{DS};n\in N \tag{3.17}$$

4. To provide flow conservation rules of backup paths of anycast downstream demands:

$$\sum_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j \in N; j \neq n\}}} y_{r,h} - \sum_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i \in N; i \neq n\}}} y_{r,h} = \begin{cases} -1, & \mathit{if} \quad n = t_r \\ \nu_{r,n}, & \mathit{if} \quad n \neq t_r \end{cases}; \quad r \in D^{DS}; n \in N \tag{3.18}$$

5. To provide flow conservation rules of working paths of anycast upstream demands:

$$\sum_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j \in N; j \neq n\}}} x_{r,h} - \sum_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i \in N; i \neq n\}}} x_{r,h} = \begin{cases} 1, & \mathit{if} \quad n = s_r \\ -\kappa_{r,n}, & \mathit{if} \quad n \neq s_r \end{cases}; \quad r \in D^{US}; n \in N \tag{3.19}$$

6. To provide flow conservation rules of backup paths of anycast upstream demands:

$$\sum_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j \in N; j \neq n\}}} y_{r,h} - \sum_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i \in N; i \neq n\}}} y_{r,h} = \begin{cases} 1, & \mathit{if} \quad n = s_r \\ -\nu_{r,n}, & \mathit{if} \quad n \neq s_r \end{cases}; \quad r \in D^{US}; n \in N \tag{3.20}$$

7. To provide proper selection of replica nodes:

$$\kappa_{r,n} \leq u_n; \quad r \in D^{AN}; n \in N \tag{3.21}$$

$$\nu_{r,n} \leq u_n; \quad r \in D^{AN}; n \in N \tag{3.22}$$

8. To guarantee that the associated upstream and downstream anycast demands use the same corresponding replica node for working paths:

$$\kappa_{r,n} = \kappa_{\tau(r),n}; \quad r \in D^{DS}; n \in N \tag{3.23}$$

9. To guarantee that the associated upstream and downstream anycast demands use the same corresponding replica node for backup paths:

$$\nu_{r,n} = \nu_{\tau(r),n}; \quad r \in D^{DS}; n \in N \tag{3.24}$$

10. To provide that exactly one node is selected as the working replica node for each anycast demand:

$$\sum_{n \in N} \kappa_{r,n} = 1; \quad r \in D^{AN} \tag{3.25}$$

11. To assure that exactly one node is selected as the backup replica node for each anycast demand:

$$\sum_{n \in N} v_{r,n} = 1; \quad r \in D^{AN} \tag{3.26}$$

12. On finite arc capacity:

$$\sum_{r \in D} \left(x_{r,h} + y_{r,h}\right) \leq c_h; \quad h \in A \tag{3.27}$$

13. To provide link disjointedness of working and backup paths of anycast demands:

$$\left(x_{r,h} + y_{r,h}\right) \leq 1; \quad r \in D; \quad h \in A \tag{3.28}$$

14. To guarantee link disjointedness of the respective working path and backup path of the associated anycast demand:

$$\left(x_{\tau(r),h} + y_{\tau(r),h}\right) \leq 1; \quad r \in D^{AN}; \quad h \in A \tag{3.29}$$

The objective is to minimize the overall cost of the flow (formula (3.14)) subject to constraints (3.15–3.29). In the model given by formulas (3.14–3.29), there is no constraint referring to the physical separation of working and backup replica servers (i.e., they may be hosted at either the same, or different nodes). Therefore, the model (3.14–3.29) is called Any Replica (AR) here.

Our investigations are also extended by:

- an additional constraint (3.30) to provide disjointedness of working and backup replica servers (forming the Disjoint Replica (DR) model defined by formulas (3.14–3.30),
- constraint (3.31) to assure that for each anycast demand, working and backup replica servers are hosted by the same node (Common Replica (CR) model given by formulas (3.14–3.29, and 3.31)),

- constraint (3.32) to assure that working and backup replica servers are located in the nearest vicinity for each anycast demand – forming the Nearest Replica (NR) model [42] by formulas (3.14–3.29, and 3.32).

$$\sum_{n \in N} (\kappa_{r,n} + \nu_{r,n}) \leq 1; \quad r \in D^{AN} \tag{3.30}$$

$$\kappa_{r,n} = \nu_{r,n}; \quad r \in D^{AN}; n \in N \tag{3.31}$$

$$\kappa_{r,n} = \nu_{r,n} = \chi_{r,n}; \quad r \in D^{AN}; n \in N \tag{3.32}$$

### Simulation Results and Conclusions

Verification of characteristics of four introduced models focusing on evaluation of the total network cost (defined as given in formula (3.14)), and values of computational time, was performed for four example networks, namely: the NSF Network, COST 239 Network, Italian Network, and US Long-Distance Network from Fig. 3.6. All links were assumed to have $\Lambda = 160$ channels of equal capacity. Nodes had a full wavelength conversion capability (i.e., at each transit node, flows arriving at any wavelength $\lambda_i$ of the incoming link could be switched onto any wavelength $\lambda_o$ of the outgoing link).

Two scenarios referring to the number of replica servers were investigated, i.e., 2 and 4, as shown in Table 3.1 with replica servers located at nodes of a relatively high degree (i.e., defined as the number of neighboring nodes).

The set of anycast demands ($D^{AN}$) contained all network nodes, while the set of unicast demands ($D^{UN}$) included the respective number of randomly chosen pairs of nodes (with node indices following the uniform distribution) such that the anycast ratio (i.e., the number of anycast demands $|D^{AN}|$ divided by the total number of demands $|D|$ was equal to 30 %).

In each simulation determined by: replica model, number of replica servers, and network topology, computations were performed for 50 different sets of demands $D$ generated randomly (following the uniform distribution of node indices). Analysis of multiple scenarios of network load, replica servers count, and other extensions of our ILP model is given in [72].

Table 3.2 presents results referring to the average execution time for each analyzed topology and replica model. As shown in Table 3.2, all four models are characterized by comparable values of the average execution time. The only exception is for CR model, for which the average execution time is about two times greater than for the other models. The reason for this is in additional constraint (3.31) including variables for both working and backup replicas.

Figures 3.7 and 3.8 present the average network costs calculated based on formula (3.14), as well as their relation with the number of available replica servers.

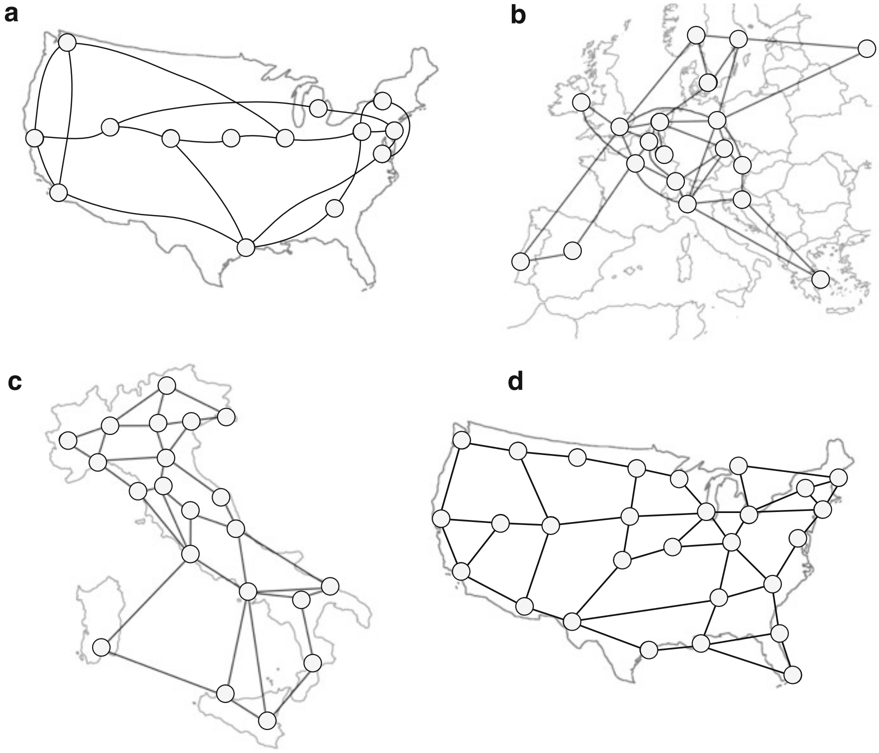


**Fig. 3.6** Network topologies used in analysis: (**a**) NSF Network, (**b**) COST 239 Network, (**c**) Italian Network, and (**d**) US Long-Distance Network

**Table 3.1** Locations of replica servers (node indices)

| Network | 2 replicas | 4 replicas |
|---|---|---|
| NSF | 6, 10 | 4, 5, 6, 10 |
| COST 239 | 2, 14 | 2, 3, 9, 14 |
| Italian | 6, 17 | 6, 7, 11, 17 |
| US Long-Distance | 14, 17 | 7, 14, 17, 23 |

**Table 3.2** Average execution time

| | Model | | | |
|---|---|---|---|---|
| Network | DR [s] | CR [s] | NR [s] | AR [s] |
| NSF | 0.41 | 2.80 | 0.43 | 0.43 |
| COST 239 | 1.38 | 2.53 | 1.44 | 1.41 |
| Italian | 1.69 | 3.98 | 1.68 | 1.67 |
| US Long-Distance | 3.34 | 5.55 | 3.37 | 3.40 |

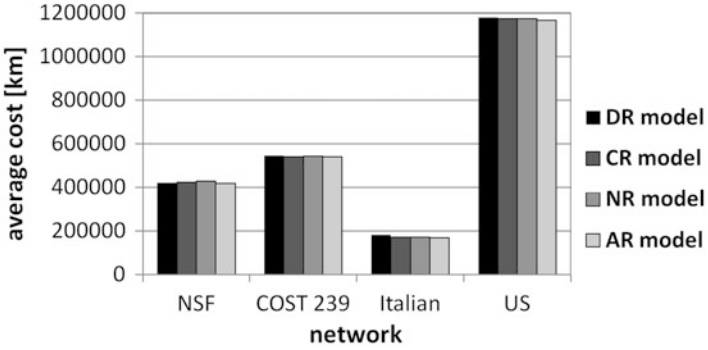


**Fig. 3.7** Average network cost for 2 replica servers

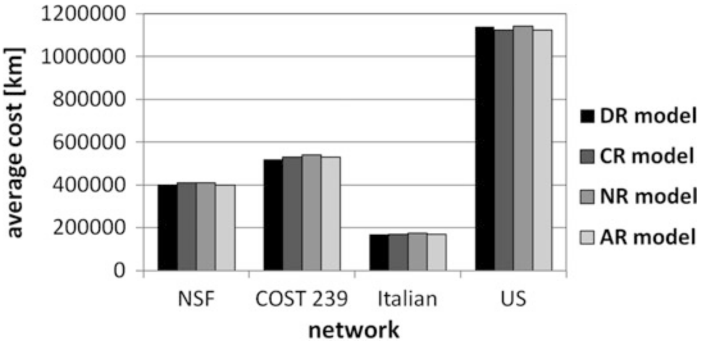


**Fig. 3.8** Average network cost for 4 replica servers

Independent of the replica model, increasing the number of replica servers decreases the overall cost of a network (as a consequence of the observed decrease of the average total length of established paths). Indeed, when increasing the number of available replica servers, the average minimal distance between replica servers and client nodes becomes smaller.

Regarding characteristics of analyzed models, AR approach outperforms the other ones. This is due to its flexibility (i.e., it does not impose additional constraints on replica servers selection). For the other models, their performance depends on network characteristics and the number of available replica servers.

As discussed in Chap. 2 of this book, providing preplanned protection against failures by means of alternate paths increases the cost of the original solution (i.e., the one without backup paths) by over 100 %, since backup paths are commonly longer than the corresponding working paths. Therefore, in order to reduce the overall cost of a solution, the concept of survivable anycast and unicast routing will be extended in the next section by sharing the backup path capacities.

### 3.3.2 *Shared Protection for Survivable Anycasting*

As discussed in Chap. 2, in order to decrease the ratio of network redundancy necessary to provide 100 % protection of flows after failures of nodes (or links), one may apply the concept of sharing the backup paths resources (i.e., link capacities) under condition that the respective working paths being protected are mutually node-(link-)disjoint [4, 40]. In this section, we present our proposal from [71] of sharing the backup path resources for routing of anycast and unicast demands with protection against a single link failure.

So far, the concept of backup path sharing has been investigated mainly for the case of unicast traffic protection [39, 40, 41, 57]. Considering backup path resource sharing for survivable anycast routing (as shown in example Fig. 3.9), recent models to find the optimal solution available in the literature have been formulated using only the Link-Path formulation (i.e., with a limited number of pre-defined candidate backup paths) [33]. This in fact leads to suboptimal results, since in Link-Path formulation, not all possible backup paths are analyzed.

In this section, we introduce the Integer Linear Programming formulation of the backup path sharing problem defined using the Node-Link notation enabling for investigation of all possible backup paths, and, consequently allowing to reach the optimal results. This model, being an extension of the respective one from Sect. 3.3.1, is defined as follows.

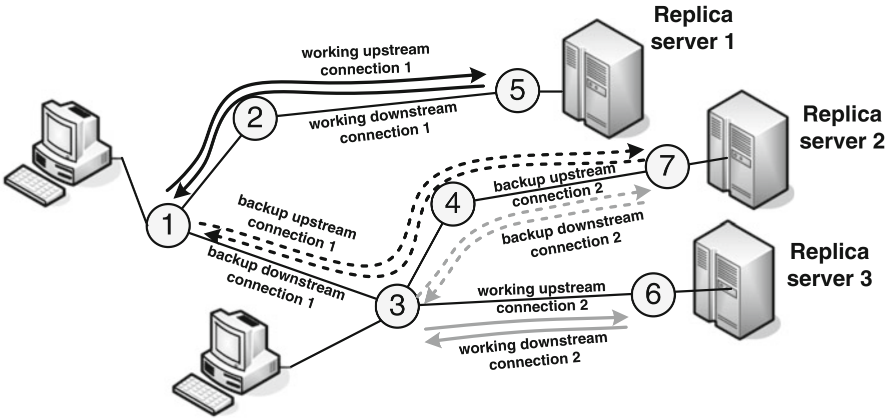

Replica server 1
Replica server 2
Replica server 3
working upstream connection 1
working downstream connection 1
backup upstream connection 2
backup downstream connection 2
backup upstream connection 1
backup downstream connection 1
working upstream connection 2
working downstream connection 2
1
2
3
4
5
6
7

**Fig. 3.9** Example of survivable anycast routing with different backup replica servers. Sharing the backup path capacities may be performed at links (3, 4) and (4, 7)

### Indices

The set of indices is the same as in Sect. 3.3.1 and extended by the following:

$d_r$ Volume (capacity) of demand $r$

### Variables

The set of variables is the same as in Sect. 3.3.1 and extended by the following:

$b_{r,h,g}$ Is equal to 1, if after a failure of arc $a_g$, the channel of arc $a_h$ is used by a backup path of $r$-th demand, 0 otherwise

$b_{h,g}$ Spare capacity required at arc $a_h$ in the case of link $a_g$ failure (integer value)

$b_h$ Aggregate spare capacity to be reserved for backup paths at arc $a_h$ (integer value) to provide protection against a failure of each single link

### Objective

It is to minimize the total cost of delivery of flows by means of working and backup paths given by formula (3.33).

$$\varphi(\mathbf{x}) = \sum_{r \in D} \sum_{h \in A} \xi_h d_r x_{r,h} + \sum_{h \in A} \xi_h b_h \tag{3.33}$$

### Constraints

1. To provide: flow conservation rules of working and backup paths of unicast demands; flow conservation rules for downstream and upstream anycast demands: formulas (3.15–3.20)
2. To provide proper selection of replica nodes: formulas (3.21–3.22)
3. To assure that the associated upstream and downstream demands use the same corresponding replica node for working and backup paths: formulas (3.23–3.24)
4. To guarantee that exactly one node is selected as a working and backup replica node for each anycast demand: formulas (3.25–3.26)
5. On finite arc capacity:

$$\sum_{r \in D} d_r x_{r,h} + b_h \le \Lambda; \quad h \in A \tag{3.34}$$

6. To provide link disjointedness of working and backup paths: formulas (3.27–3.28)
7. To obtain shared protection with respect to the considered backup paths:

$$\begin{gathered} x_{r,g} + y_{r,h} \le 1 + b_{r,h,g} \\ r \in D; \quad h \in A; \quad g \in A; \quad g \ne h \end{gathered} \tag{3.35}$$

$$\begin{gathered} 2b_{r,h,g} \le x_{r,g} + y_{r,h} \\ r \in D; \quad h \in A; \quad g \in A; \quad g \ne h \end{gathered} \tag{3.36}$$

8. To provide bounds on arc spare capacity:

$$b_{h,g} = \sum_{r \in D} d_r b_{r,h,g} \qquad h \in A; \quad g \in A; \quad g \neq h \tag{3.37}$$

$$b_{h,g} \leq b_h \qquad h \in A; \quad g \in A; \quad g \neq h \tag{3.38}$$

9. To assure location of working and backup replica servers at the nearest nodes: formula (3.32)

   If we replace formula (3.38) with the following formula (3.39), we obtain the model without shared protection, since $b_h$ is then defined simply as the sum of backup capacities over all link failures.

$$b_h = \sum_{g \in A} b_{h,g} \tag{3.39}$$

To summarize, the above formulas can be used to obtain four following models investigated in detail in the later part of this section:

- SBPP-AR: Any Replica model; shared protection: additional formulas (3.33), (3.15–3.20), (3.23–3.28), (3.34–3.38),
- SBPP-NR: Nearest Replica model; shared protection: formulas (3.33), (3.15–3.20), (3.23–3.28), (3.32), (3.34–3.38),
- noSBPP-AR: Any Replica model; dedicated protection: formulas (3.33), (3.15–3.20), (3.23–3.28), (3.34–3.37), (3.39),
- noSBPP-NR: Nearest Replica model; dedicated protection: formulas (3.33), (3.15–3.20), (3.23–3.28), (3.32), (3.34–3.37), (3.39).

### Simulation Results and Conclusions

The aim of numerical experiments was to evaluate the efficiency of the introduced shared protection schemes in terms of: (1) the total cost of a solution; (2) length and hop-count of established paths, all as a function of the anycast ratio (defined as the proportion of anycast traffic to the total traffic – i.e., anycast and unicast); (3) the number of replica servers available in the network (2 or 3) – as given in Table. 3.3, and (4) two analyzed scenarios (AR and NR) of replica server locations.

Considering the anycast ratio, we investigated the values from the set (10 %, 20 %, . . ., 80 %). Twenty four different demand sets (comprising three demand sets per each anycast ratio value) were generated randomly (using the uniform distribution function of indices of demand nodes). The numbers of anycast and unicast demands per each demand set were in ranges 8–28 and 7–44, accordingly. In order to obtain a given value of anycast ratio, demand volumes $d_r$ were selected from range 1–9. Two cases of replica servers count (2 and 3, accordingly), and four analyzed variants of our ILP model in total gave 192 different experiments, all performed for the analyzed NSF network from Fig. 3.6a.

Experiments were also prepared to evaluate the performance of shared backup capacity models in comparison to schemes without backup capacity sharing. Therefore, the first set of results, presented in Fig. 3.10, refers to the average overall cost of solutions (based on formula (3.33)) in terms of ratios $cost^{\mathrm{SBPP}}/cost^{\mathrm{noSBPP}}$ as a function of the anycast ratio parameter. The average value of this coefficient (obtained for all experiments) was 0.64, which means that shared backup path approaches outperformed the respective "no-sharing" ones by 36 %. As shown in Fig. 3.10, the difference between the analyzed approaches decreases with the increase of the anycast ratio parameter, since under anycasting, one of end nodes of a demand is also related with one of replica servers located at a limited number of network nodes. This in turn limits the possibility of backup path sharing (following the general backup capacity sharing rule).

As shown in Fig. 3.10, increasing the number of replica servers (here from 2 to 3) also reduces the gap between SBPP and noSBPP models, since with the increase of the number of replica servers, working paths become shorter (due to the physical location of replica servers closer to the client nodes). Therefore, with the increase of

**Table 3.3** Locations of replica servers (node indices)

| 2 replica servers | 3 replica servers |
|---|---|
| 6, 10 | 4, 6, 10 |

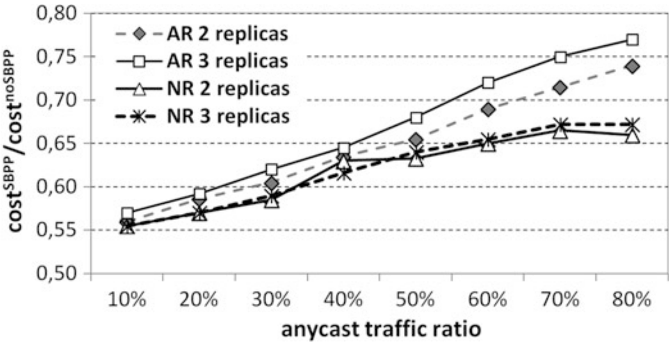


**Fig. 3.10** Average cost ratios between SBPP and noSBPP solutions

the number of replica servers, the average path hop count decreases, which implies fewer possibilities of backup capacity sharing.

Table 3.4 presents the average ratios between SBPP and noSBPP models for all analyzed parameters. In general, there is no visible impact of the scenario of replica server location on the presented ratios independent of analyzed metrics. Considering the cost metric, the Any Replica (AR) model is characterized by lower values of the cost difference (expressed by larger values of the SBPP/noSBPP ratio), since AR, being more flexible than the Nearest Replica (NR) scheme, is able to benefit from switching the traffic to another replica server after the failure (not possible for the NR model implying location of working and backup replicas of a demand at the same closest network node).

Characteristics of the capacity utilization metric are similar, i.e., with the increase of the anycast traffic ratio, as well as the number of replicas, the difference between SBPP and noSBPP scenarios (42 %, on average), becomes less visible.

The most important result refers to the average length of backup paths, which is about 70–100 % greater for SBPP schemes, compared to noSBPP approaches for both anycast and unicast demands. This is due to the backup path cost included in the objective function (Eq. 3.33) reflecting only the extra capacity that has to be reserved for backup paths (i.e., the fraction of backup capacity without possibility of sharing). Therefore, links with sharable backup capacity are preferred in backup path computations. Backup paths may thus traverse many links of “zero” cost, which increases their hop count.

As shown in Fig. 3.11, with the increase of the anycast traffic ratio, the 3 replica/2 replica ratio considering cost and capacity parameters decreases, implying the growth of the difference of cost and capacity parameters. This is a natural consequence of adding a new replica server leading to more efficient results in terms of reduction of the average path length (observed with the increase of the anycast traffic ratio). Obtained results confirm the remarkable capacity efficiency of our shared protection scheme at a price of the increased length of backup paths.

**Table 3.4** Average ratios between SBPP and noSBPP schemes

| Number of replica servers | 2 | 3 | 2 | 3 |
|---|---|---|---|---|
| Replica scenario | AR | AR | NR | NR |
| Cost | 0.65 | 0.67 | 0.62 | 0.62 |
| Capacity utilization | 0.60 | 0.61 | 0.56 | 0.57 |
| Anycast working path length | 1.01 | 1.06 | 1.01 | 1.03 |
| Anycast backup path length | 2.00 | 2.09 | 1.79 | 1.91 |
| Anycast working path hops | 1.00 | 1.00 | 1.01 | 1.02 |
| Anycast backup path hops | 1.54 | 1.60 | 1.43 | 1.56 |
| Unicast working path length | 1.01 | 1.01 | 1.01 | 1.05 |
| Unicast backup path length | 1.71 | 1.68 | 1.78 | 1.86 |
| Unicast working path hops | 1.01 | 1.01 | 1.00 | 1.03 |
| Unicast backup path hops | 1.49 | 1.43 | 1.53 | 1.55 |

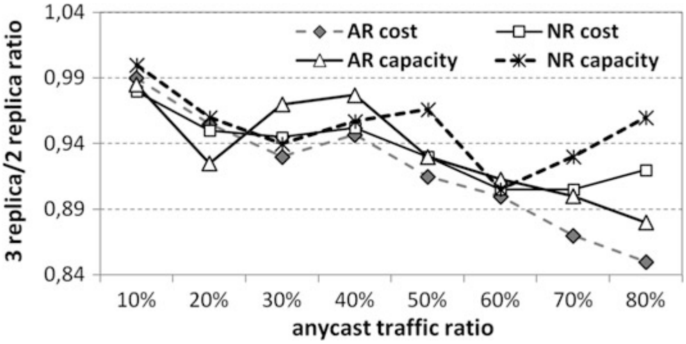


**Fig. 3.11** Average ratios of results between 3 and 2 replica servers

### 3.3.3 *Protection of Information-Centric Communications Against Intentional Failures*

Majority of proposals available in the literature are related with protection against random failures being implication of hardware faults, software defects, or simply human errors, all typically characterized by uniform distribution function of failure probabilities (i.e., failure probabilities independent of network element characteristics). Only a few papers address the issue of protection against failures resulting from malicious activities, referred to as *attacks*, typically affecting the most important network elements (i.e., nodes/links of relatively high degree/capacity switching/storing large amount of data). The problem is of utmost importance, since attacking such elements frequently causes severe losses (which is actually the main aim of attackers).

Such differentiation of severity of attack outcomes can be observed especially for networks of irregular topology (obtained as a result of an uncontrolled network growth), for which the node degree distribution does not comply with the uniform law. Following the Barabási and Albert rule of *preferential attachment* of new nodes from [10], when adding a node to the network, it is more probable to link it with an existing one of high rather than low degree, as given in formula (3.40). In case of such an uncontrolled growth, network topologies commonly gradually evolve towards irregular ones (as illustrated in Fig. 3.12) with asymptotic power law degree distribution of node degrees $k$ given by formula (3.41) [10]. Examples include, e.g., topology of the Internet with $\gamma = 2.22$ [76].

$$\Pi(n) = \frac{\deg(n)}{\sum_j \deg(j)} \tag{3.40}$$

$$P(k) \sim k^{-\gamma} \tag{3.41}$$

It is important to notice that under the conventional shortest path routing, many shortest paths traverse such high degree nodes (also called *central nodes*) and are at

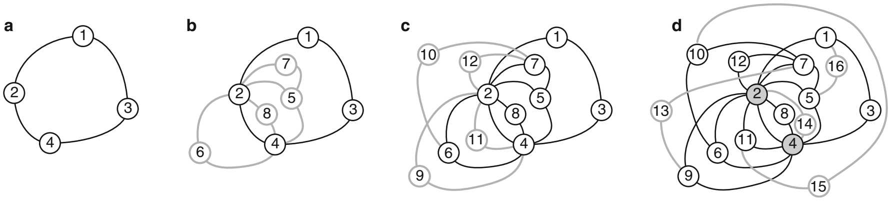


**Fig. 3.12** Example evolution of a network topology (steps b-d) following the preferential attachment rule

high risk of being affected by an attacker. Therefore, shortest path routing does not seem to be a proper solution for networks of dynamically evolving topologies. This is especially true for the current Internet owned by multiple providers without any common policy on topology evolution. It is thus crucial to provide Future Internet with routing mechanisms preventing communication paths from attacks.

In this section, we describe our approach from [59] called "resistant-to-attacks" (RA) designed to protect anycast and unicast flows against malicious activities targeted at network nodes. It uses path protection scheme to assure protection of each working path by a dedicated backup path against a single node failure. To reduce the impact of attacks, in our approach:

- working paths are established using a dedicated metric of link cost (different than the conventional metric of distance applied by us in backup path computations only) to make them omit nodes of high degree,
- replica servers are located at low-degree nodes to reduce the losses resulting from attacks.

Vulnerability of communication paths to attack-based disruptions changes as the network topology is subject to evolution over time. Therefore, it is crucial to introduce a routing scheme that dynamically adjusts its properties in response to changes of the network topology. In order to address this objective, in working path computations we propose to use the metric of link costs based on *betweenness centrality* (*BC*) coefficient [35] defined for any node $n$ as given in formula (3.42), providing a proper estimation of a node centrality ratio, and thus being an important indicator of node vulnerability to attacks.

$$BC(n) = \sum_{p \neq q} \frac{sp_n(p,q)}{sp(p,q)} \tag{3.42}$$

where

$sp_n(p,q)$ is the number of the shortest paths between nodes $p$ and $q$ (of the same minimal length) traversing node $n$

$sp(p,q)$ is the number of the shortest paths between nodes $p$ and $q$ (of the same minimal length)

In particular, we define the cost $\xi_h$ of arc $a_h$ in working path computations as the average value of the normalized betweenness centrality parameter ($BC^*$) of nodes $i$ and $j$ incident to arc $a_h$, as given in formula (3.43). Since the cost of any link incident to a high-degree node should be high as well, working paths calculated based on costs (3.43) are thus expected not to traverse such central nodes (as e.g., nodes `6, 11, 17` in Fig. 3.13), and, as a result, be less vulnerable to attack-based disruptions.

$$\xi_h = \xi_{i,j} = \frac{BC^*(i) + BC^*(j)}{2} \tag{3.43}$$

where

$$BC^*(n) = \frac{BC(n)}{\max_i(BC(i))} \tag{3.44}$$

For the purpose of backup path computations, cost $\zeta_h$ of any network arc $a_h$ is defined here by formula (3.44) as the normalized length of this arc.

$$\zeta_h = \frac{s_h}{\max_i(s_i)} \tag{3.45}$$

Backup paths are thus established as the shortest ones. Although they are allowed to transit high-degree nodes (as shown in Fig. 3.13), they are used in

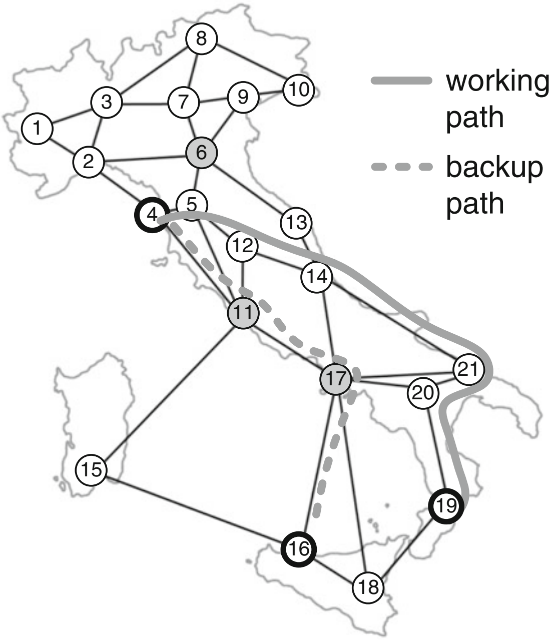


**Fig. 3.13** Example anycast routing following the proposed approach; Italian network from Fig. 3.6c

relatively short time periods (for a temporary recovery until the time of manual repair of failed elements).

Similar to Sects. 3.3.1–3.3.2, under anycast routing, working and backup paths may lead to different replica servers to provide protection against a failure of a replica node (Fig. 3.13).

The ILP model necessary to find the solution to our optimization problem is the same as the Disjoint Replica model from Sect. 3.3.1 defined by formulas (3.14–3.30) with the only one exception for the objective function (3.14) here replaced with formula (3.46).

$$\min \quad \varphi(\mathbf{x}) = \sum_{r \in D} \sum_{h \in A} \xi_h x_{r,h} + \sum_{r \in D} \sum_{h \in A} \zeta_h y_{r,h} \tag{3.46}$$

However, the considered problem defined by formulas (3.15–3.30) and (3.46) is $NP$-complete due to $NP$-completeness of a simpler task to find $|D|$ working paths only (i.e., without protection) in capacity-constrained networks [50]. Therefore, for larger problem instances, it is necessary to use a heuristic approach to obtain the suboptimal results in a reasonable time. As stated in [58], in the case of multi-cost networks (i.e., when for any link, different link costs are assigned to working and backup path links – as considered in this section), the problem is $NP$-complete even for a single demand.

The heuristic scheme from Fig. 3.14, proposed for the general case of establishing the set of $k$ end-to-end node-disjoint paths for a given demand, is similar to the Active Path First (APF) approach [58]. For each demand, after initialization Steps 1–3, it first tries to calculate the working path using any algorithm of the shortest path computation (e.g., Dijkstra's from [21]). However, in backup paths computations, contrary to the APF scheme, in our approach in order to provide nodal disjointedness of transmission paths, the costs of the respective *forbidden arcs* traversed by the working path are increased by a large value (instead of being set to infinity). This update is to prevent from entering into the *trap problem* (i.e., the case when the algorithm fails to establish the next disjoint path of a demand, even though it would be feasible for a given topology).

In particular, in the case of establishing $k$ end-to-end node-disjoint paths, before finding the next disjoint path $j$, for each previously calculated path $\eta_i$, the cost of any forbidden arc is first increased by the total cost of path $\eta_i$ calculated based on the matrix of backup link costs $\Xi^j$ (Step 4). However, after finding the next path ($\eta_j$) of a demand in Step 5 and detecting that more than one of already calculated paths of a demand traverse a given arc $a_h$, the cost of such a *conflicting arc* is permanently increased by the total cost of path $\eta_j$ in all matrices $\Xi^i$ (calculated based on arc costs from $\Xi^i$), and the execution starts from the beginning (Step 6).

After several possible conflicts, the method is expected to terminate successfully (as shown later in this section). The time complexity of our scheme depends on complexity of the base approach of path computations. If Dijkstra's algorithm from

**INPUT**

- A demand (with index $r$) to determine the set of $k$ end-to-end node-disjoint paths (each unicast demand is determined by a pair of nodes ($s_r$, $t_r$), while each anycast demand is given by a client node $s_r$ to be connected to working and backup replica servers located at different nodes)
- Matrices $\Xi^1$, $\Xi^2$, ..., $\Xi^k$ of arc costs $\xi_h^1$, $\xi_h^2$,..., $\xi_h^k$ (defined for computations of consecutive disjoint paths of $r$-th demand)
- The upper bound *it_upper* on the number of allowed conflicts

**OUTPUT** The set $\{\eta_1, \eta_2, ..., \eta_k\}$ of $k$ end-to-end node-disjoint paths

| VARIABLES | | |
|---|---|---|
| | $\Xi^{tmp}$ | auxiliary matrix of arc costs $\xi_h^{tmp}$ |
| | $j$ | index of the current path |
| | $ic$ | conflict counter |

```
Step 1  Set $ic := 1$.
Step 2  Set $j := 1$.
Step 3  For each network arc $a_h$, set $\xi_h^{tmp} := \xi_h^j$.
Step 4  For each path $\eta_i$ from the set of previously found $j-1$ paths of a demand and for each arc $a_h$, if
        $a_h$ is a forbidden arc* of path $\eta_i$, then increase the arc cost $\xi_h^{tmp}$ by the total cost $\xi^i$ of $\eta_i$ in $\Xi_j$.
Step 5  Find path $\eta_j$ using the Dijkstra's algorithm and the costs matrix $\Xi^{tmp}$.
Step 6  If $\eta_j$ is not disjoint with the previously found $j-1$ paths of $r$-th demand then:
            Step 6.1  Increase the costs $\xi_h^i$ of each conflicting arc** $a_h$ of $\eta_j$ by the total cost $\xi^j$ of $\eta_j$ in
                      all matrices $\Xi^i$. After that, delete the found paths.
            Step 6.2  Set $ic := ic + 1$.
            Step 6.3  if $ic > it\_upper$ then
                          terminate and reject the demand,
                      else go to Step 2.
        else increment $j$.
Step 7  If $j > k$ then terminate and return the found set of paths
            else go to Step 3.
```

* In case of required nodal disjointedness of the set of $k$ end-to-end paths of a demand, a forbidden arc of $\eta_i$ is an arc that is incident to any transit node of $\eta_i$

** In case of required nodal disjointedness of the set of $k$ end-to-end paths of a demand, arc $a_h$ is a conflicting arc of a given path $\eta_j$, if it is incident to any common transit node of $\eta_j$ also used by any other of previous $j$-1 paths

**Fig. 3.14** Heuristic approach to find the set of $k$ end-to-end node-disjoint paths

[21] is utilized for this purpose, the overall complexity is bounded from above by $O(|N|^2)$, where $|N|$ is the number of network nodes.

This scheme is used here to find $k = 2$ end-to-end node-disjoint paths.

## Simulation Results and Conclusions

Characteristics of the proposed RA approach referring to link capacity utilization ratio, length of working and backup paths, total number of connections broken due to attacks, as well as time of connection restoration were evaluated by means of simulations, and compared with the reference results of the common approach to establish working and backup paths using the metric of distance (here called "non-resistant-to-attacks" – NA approach).

Time of connection restoration was calculated based on [50]. Experiments were performed using CPLEX 11.0 solver (to obtain the ILP-based optimal results), as well as the heuristic method from Fig. 3.14 for topologies of two irregular networks shown in Fig. 3.15 (achieved using the Barabási-Albert approach of topology generation [10]). Concerning anycast and unicast demands:

- demanded capacity was assumed to be unitary (equal to the channel capacity),
- 100 % of the requested capacity was required to be available for each demand after failures of single nodes,
- working paths were protected by dedicated backup paths (i.e., with no sharing of link capacities reserved for backup paths).

Three scenarios of network load were investigated. In each case, the analyzed sets of demands $D^{AN}$ comprised all network nodes. However, concerning unicast demands, the analyzed sizes of demand sets were adjusted in a way to receive three ratios of anycast demands ($|D^{AN}|/|D|$) equal to 10 %, 20 %, and 30 %. Any pair of demand end-nodes was always chosen randomly using the uniform distribution function of node indices. Considering the number of replica servers available in the network, we investigated three cases of 2, 3, and 4 replica servers hosted by nodes of the highest (common NA model), and the lowest (our RA model) degree, accordingly.

A single simulation comprised 50 different sets of demands for a given network topology, and the number of available replica servers. Probability of node failures was proportional to the values of the normalized betweenness centrality coefficient defined for network nodes by Eq. 3.44.

One of objectives of simulations was to evaluate the efficiency of our heuristic method in comparison with the results of ILP modeling. This analysis is presented

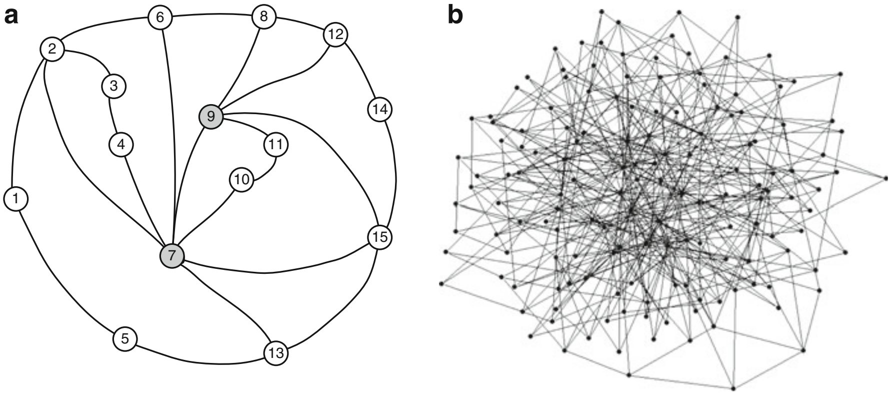


**Fig. 3.15** Network topologies used in simulations: (**a**) ASF Network, (**b**): BA-150 Network

in Fig. 3.16 for ASF network from Fig. 3.15a (with assumed $\Lambda = 40$ channels available at each network link) in terms of the total link capacity per connection necessary to serve the demands as a function of the network load (Fig. 3.16) and the number of replica servers (Fig. 3.17).

The results show that the amount of capacity necessary to serve the demands (per connection) for the heuristic approach was similar to the optimal ILP solution. In some cases, our technique required even less capacity (up to 2.49 % less). However, this was an implication of inconsistency of the proposed formula (3.46) with the hop count metric. In general, our RA scheme required about 10 % more capacity than the reference NA algorithm.

The next set of experiments was aimed at evaluating characteristics of the proposed approach related to working and backup path length, the total number of connections broken due to attacks, as well as the average time of connection restoration. Due to the size of the investigated network (BA-150 network from Fig. 3.15b with 3 replica servers and $\Lambda = 160$ channels available at each link), evaluation was feasible for the heuristic approach only.

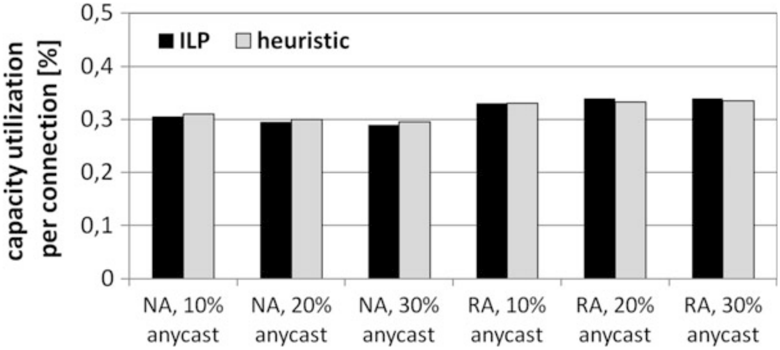


**Fig. 3.16** Ratios of total link capacity utilization per connection for ASF network from Fig. 3.15a achieved for different network loads (number of replica servers: 2)

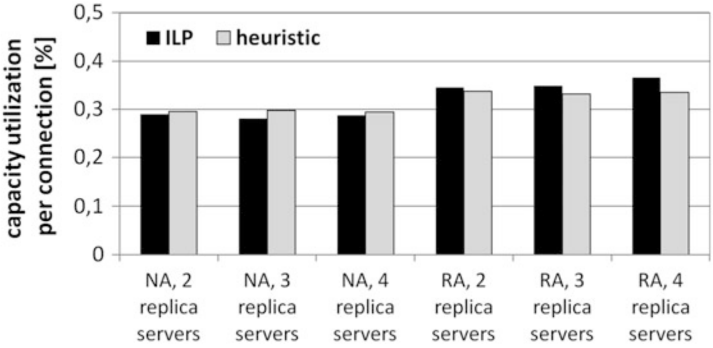


**Fig. 3.17** Ratios of total link capacity utilization per connection for ASF network from Fig. 3.15a achieved for different numbers of replica servers (anycast ratio: 30 %)

For our RA approach, the average length of working paths was up to 2.26 times greater, compared to the common NA scheme (due to the fact that RA working paths tried to omit high-degree nodes). On the contrary, RA backup paths were about 25 % shorter than the respective NA ones (Fig. 3.18).

Since RA working paths were established in a way to omit nodes of high degree, characteristics referring to the number of connections broken due to attacks from Fig. 3.19 show a significant advantage of our scheme (i.e., a 7.47-fold advantage), compared to the reference NA approach. Finally, the achieved average values of service restoration time (which due to the three-way handshake procedure commonly depend on lengths of working and backup paths [50]) were similar for both approaches (see Fig. 3.20).

To conclude, the proposed approach to establish working paths in a way to omit nodes of high degree results in a remarkable decrease of a number of connections affected after attacks at a price of only insignificant increase of the length of

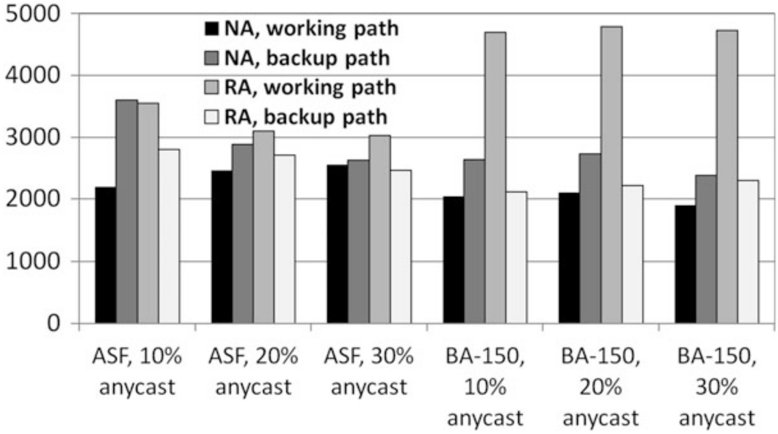


**Fig. 3.18** Average length of paths

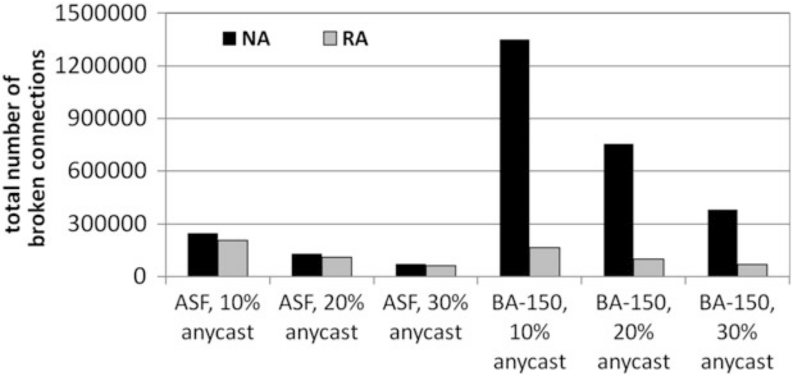


**Fig. 3.19** Total number of broken connections

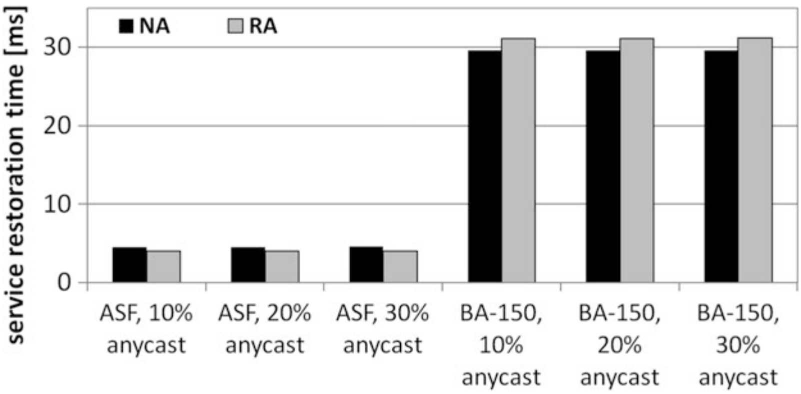


**Fig. 3.20** Average service restoration time

working paths. Dynamic properties of our scheme make it a suitable solution at any stage of a network evolution.

A detailed analysis of our approach characteristics, including e.g., presentation of 95 % confidence intervals for the analyzed parameters, is available in [59].

## 3.4 Summary

Diversity of Future Internet desired functionalities, routing paradigms, as well as challenges threatening the normal operation of any global network, altogether make resilience of FI communications a complex issue. Considered by many as an important part of a critical infrastructure expected to offer the uninterrupted service anytime and anywhere, Future Internet needs to be provided with efficient solutions to assure service continuity under both random and intentional failures.

To address this issue, in this chapter we first presented the efficient solutions to routing and network resource provisioning problems deployed by us in one of European research projects on Future Internet architecture, called Future Internet Engineering. Next, we focused on resilience of content-oriented networking (being an important paradigm for the Future Internet) and introduced three new concepts of survivable routing of unicast and anycast flows for: (1) dedicated, and (2) shared protection under random failures of nodes/links, as well as (3) dedicated protection of flows under attack-based disruptions.

Obtained results confirmed efficiency of our techniques in assuring the uninterrupted routing of FI demands in differentiated scenarios, including dedicated protection (Sect. 3.3.1), shared protection (Sect. 3.3.2 with the achieved 36 % reduction of redundancy ratio, compared to the case of dedicated protection) in random failure scenarios, as well as a significant improvement in terms of the number of connections broken due to attacks (characterized by a remarkable 7.47-fold advantage over the conventional routing scheme, as shown in Sect. 3.3.3).

## References

1. Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutcher, D., Ohlman, B.: A survey of information-centric networking. IEEE Commun. Mag. **50**(7), 26–36 (2012)
2. Akamai project: http://www.akamai.com. Accessed on 8 Mar. 2015
3. Akari architecture design project: http://www.nict.go.jp/en/photonic_nw/archi/akari/akari-top_e.html. Accessed on 8 Mar. 2015
4. Ali, M.: Shareability in optical networks: beyond bandwidth optimization. IEEE Opt. Commun. **42**(2), s11–s15 (2004)
5. Al-Naday, M.F., Reed, M.J., Trossen, D., Yang, K.: Information resilience: source recovery in an information-centric network. IEEE Netw. **28**(3), 36–42 (2014)
6. Anderson, T., Peterson, L., Shenker, S., Turner, J.: Overcoming the Internet impasse through virtualization. IEEE Comput. **38**(4), 34–41 (2005)
7. Awerbuch, B., Brinkmann, A., Scheideler, C.: Anycasting in adversarial systems: routing and admission control. Lect. Notes Comput. Sci., Springer. **2719**, 1153–1168 (2003)
8. Álvarez, F., Cleary, F., Daras, P., Domingue, J., Galis, A., Garcia, A., Gavras, A., Karnourskos, S., Krco, S., Li, M.-S., Lotz, V., Müller, H., Salvadori, E., Sassen, A.-M., Schaffers, H., Stiller, B., Tselentis, G., Turkama, P., Zahariadis, T. (eds.): The Future Internet – Future Internet Assembly (FIA 2012): From Promises to Reality, Aalborg, 9–11 May, 2012. Lect. Notes Comput. Sci., Springer. **7281** (2012)
9. Balasubramaniam, S., Leibniz, K., Lio, P., Botvich, D., Murata, M.: Biological principles for Future Internet architecture design. IEEE Commun. Mag. **49**(7), 44–52 (2011)
10. Barabási, A.-L., Albert, R.: Emergence of scaling in random networks. Science **286**, 509–512 (1999)
11. Botero, J.F., Hesselbach, X., Fischer, A., de Meer, H.: Optimal mapping of virtual networks with hidden hops. Telecommun. Syst. **51**(4), 273–282 (2012)
12. Burakowski, W.: Role of network virtualization in designing Future Internet. In: Proc. 15th Telecommunications Network Strategy and Planning Symposium (Networks’12), pp. 1–3 (2012)
13. Burakowski, W., et al.: IIP System specification level 1 and 2, POIG IIP project deliverable (2011)
14. Cerf, V.G.: The day the Internet age began. Nature **461**(7268), 1202–1203 (2009)
15. China Education and Research Network: http://www.edu.cn/english/. Accessed on 24 Nov. 2014
16. Chołda, P., Gozdecki, J., Kantor, M., Wielgosz, M., Pach, A.R., Wajda, K., Rak, J.: Provisioning concepts of the IIP Initiative. In: Proc. 13th International Conference on Transparent Optical Networks (ICTON’11), pp. 1–4 (2011)
17. Chou, H.-Z., Wang, S.-C., Kuo, S.-Y., Chen, I.-Y., Yuan, S.-Y.: Randomised and distributed methods for reliable peer-to-peer data communication in wireless ad hoc networks. IET Commun. **1**(5), 915–923 (2007)
18. Chowdhury, N.M., Boutaba, R.: Network virtualization: state of the art and research challenges. IEEE Commun. Mag. **47**(7), 20–26 (2009)
19. D’Ambrosio, M., Fasano, P., Marchisio, M., Vercellone, V., Ullio, M.: Providing data dissemination services in the Future Internet. In: Proc. IEEE Global Communications Conference (IEEE GLOBECOM’08), pp. 1–6 (2008)
20. Dedecker, P., Hoebeke, J., Moerman, I., Moreau, J., Demeester, P.: Network virtualization as an integrated solution for emergency communication. Telecommun. Syst. **52**(4), 1859–1876 (2013)
21. Dijkstra, E.: A note on two problems in connexion with graphs. Numer. Math. **1**, 269–271 (1959)
22. Din, D.: Anycast routing and wavelength assignment problem on WDM network. IEICE Trans. Commun. **E88-B**(10), 3941–3951 (2005)

23. Domingue, J., Galis, A., Gavras, A., Zahariadis, T., Lambert, D., Cleary, F., Daras, P., Krco, S., Müller, H., Li, M.-S., Schaffers, H., Lotz, V., Alvarez, F., Stiller, B., Karnouskos, S., Avessta, S., Nilsson, M. (eds.): The Future Internet – Future Internet Assembly 2011: Achievements and Technological Promises. Lect. Notes Comput. Sci., Springer, Berlin. **6656** (2011)
24. European Commission: Council decision establishing the specific program implementing HORIZON 2020 – the framework programme for research and innovation (2014–2020). Brussels, 2011. Work Programme 5.i. Leadership in technologies. Draft Discussion Doc. pp. 86–86 (2013)
25. European Commission: http://ec.europa.eu. Accessed on 21 Nov. 2014
26. Feldmann, A.: Internet clean-slate design: what and why? ACM SIGCOMM Comput. Commun. Rev. **37**(3), 59–64 (2007)
27. FIRE: Future Internet Research and Experimentation: http://cordis.europa.eu/fp7/ict/fire/. Accessed on 24 Nov. 2014
28. Future Internet Assembly: http://www.future-internet.eu/home/future-internet-assembly.html. Accessed on 20 Nov. 2014
29. Future Internet Engineering (IIP) Initiative: http://www.iip.net.pl. Accessed on 24 Nov. 2014
30. GEANT2 project: http://www.geant2.net/. Accessed on 24 Nov. 2014
31. Gedik, B., Liu, L.: A scalable peer-to-peer architecture for distributed information monitoring applications. IEEE Trans. Comput. **54**(6), 767–782 (2005)
32. Ghodsi, A., Koponen, T., Rajahalme, J., Sarolahti, P., Shenker, S.: Naming in content-oriented architectures. In: Proc. ACM SIGCOMM'11 Workshop on Information-Centric Networking, pp. 1–6 (2011)
33. Gładysz, J., Walkowiak, K.: Optimization of survivable networks with simultaneous unicast and anycast flows. In: Proc. RNDM'09 @ International Conference on Ultra Modern Telecommunications & Workshops (ICUMT'09), pp. 1–6 (2009)
34. Global Environment for Network Innovations (GENI) Project: http://www.geni.net/. Accessed on 24 Nov. 2014
35. Goh, K.-I., Oh, E.S., Jeong, H., Kahng, B., Kim, D.: Classification of scale free networks. arXiv:cond-mat/0205232, v2 (2002)
36. Gozdecki, J., Kantor, M., Wajda, K., Rak, J.: A flexible provisioning module optimizing utilization of resources for the Future Internet IIP initiative. In: Proc. 15th International Telecommunications Network Strategy and Planning Symposium (NETWORKS'12), pp. 1–6 (2012)
37. Gozdecki, J., Kantor, M., Wajda, K., Rak, J.: Methods of network resource provisioning for the Future Internet IIP initiative. Telecommunication Systems (2015). doi:10.1007/s11235-015-9997-5
38. 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 (2011)
39. Ho, P.-H., Mouftah, H.T.: A framework for service-guaranteed shared protection in WDM mesh networks. IEEE Commun. Mag. **40**(2), 97–103 (2002)
40. Ho, P.-H., Tapolcai, J., Cinkler, T.: Segment shared protection in mesh communications networks with bandwidth guaranteed tunnels. IEEE/ACM Trans. Networking **12**(6), 1105–1118 (2004)
41. Ho, P.-H., Tapolcai, J., Mouftah, H.T.: Diverse routing for shared protection in survivable optical networks. In: Proc. IEEE Global Communications Conference (IEEE GLOBECOM'03), vol. 5, pp. 2519–2523 (2003)
42. Hofmann, M., Beaumont, L.: Content Networking: Architecture, Protocols, and Practice. Morgan Kaufmann, San Francisco (2005)
43. IEEE Communications Society: A Brief History of Communications, 2nd edition, IEEE, Piscataway (2012)

44. Koponen, T., Chawla, M., Chun, B.-G., Ermolinskiy, A., Kim, K.H., Shenker, S., Stoica, I.: A data-oriented (and beyond) network architecture. In: Proc. ACM Annual Conference of the Special Interest Group on Data Communication (ACM SIGCOMM'07), pp. 181–192 (2007)
45. Kounavis, M.E., Campbell, A.T., Chou, S., Modoux, F., Vicente, J., Zhuang, H.: The Genesis Kernel: a programming system for spawning network architectures. IEEE J. Sel. Areas Commun. **19**(3), 511–526 (2001)
46. Low, C.P., Tan, C.L.: On anycast routing with bandwidth constraint. Comput. Commun. **26**(14), 1541–1550 (2003)
47. Metz, C.: IP anycast point-to-(any) point communication. IEEE Internet Comput. **6**(2), 94–98 (2002)
48. MobilityFirst Future Internet Architecture Project: http://mobilityfirst.winlab.rutgers.edu/. Accessed on 24 Nov 2014
49. Molisz, W., Rak, J.: Region protection/restoration scheme in survivable networks. Lect. Notes Comput. Sci., Springer. **3685**, 442–447 (2005)
50. Mukherjee, B.: Optical WDM Networks. Springer, New York (2006)
51. Named Data Networking project: http://www.named-data.net. Accessed on 24 Nov. 2014
52. National Science Foundation: http://www.nsf.gov. Accessed on 24 Nov. 2014
53. NSF Future Internet Architecture Project: http://www.nets-fia.net. Accessed on 24 Nov. 2014
54. NSF NeTS FIND Initiative: http://www.nets-find.net. Accessed on 24 Nov. 2014
55. Pan, J., Paul, S., Jain, R.: A survey of the research on future internet architectures. IEEE Commun. Mag. **49**(7), 26–36 (2011)
56. Petcu, D., Galis, A, Karnouskos, S.: The Future Internet cloud: computing networking and mobility. Introduction to chapter on computing and mobile clouds. In: The Future Internet – FIA 2013: validated results and new horizons, pp. xiii–xv (2013)
57. Rak, J.: Fast service recovery under shared protection in WDM networks. IEEE/OSA J. Lightwave Technol. **30**(1), 84–95 (2012)
58. Rak, J.: *k*-Penalty: a novel approach to find *k*-disjoint paths with differentiated path costs. IEEE Commun. Lett. **14**(4), 354–356 (2010)
59. Rak, J., Walkowiak, K.: Reliable anycast and unicast routing: protection against attacks. Telecommun. Syst. **52**(2), 889–906 (2013)
60. Sallai, G.: Chapters of Future Internet research. In: Proc. 4th International Conference on Cognitive Infocommunications (CogInfoCom'13), pp. 161–166 (2013)
61. Schoenwaelder, J., Fouquet, M., Rodosek, G.D., Hochstatter, I.C.: Future Internet = content + services + management. IEEE Commun. Mag. **47**(7), 27–33 (2009)
62. Software-defined networking: the new norm for networks. White paper, Open Networking Foundation (ONF), April 2012: https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf. Accessed on 8 Mar. 2015
63. The FP7 4WARD Project: http://www.4ward-project.eu/. Accessed on 25 Nov. 2014
64. Touch, J.: Dynamic internet overlay deployment and management using the X-bone. Comput. Netw. **36**(2–3), 117–135 (2001)
65. Triukose, S., Wen, Z., Rabinovich, M.: Content delivery networks: how big is big enough? ACM SIGMETRICS Perform. Eval. Rev. **37**(2), 59–60 (2009)
66. Trossen, D., Parisis, G.: Designing and realizing an information-centric Internet. IEEE Commun. Mag. **50**(7), 60–67 (2012)
67. Tselentis, G., et al. (eds.): Towards the Future Internet – Emerging Trends from European Research. Future Internet Assembly (FIA 2010), IOS Press, Amsterdam (2010)
68. Turner, J., Taylor, D.: Diversifying the Internet. In Proc. IEEE Global Communications Conference (IEEE GLOBECOM'05), vol. 2, pp. 765–760 (2005)
69. Walkowiak, K.: Anycast communications, a new approach to survivability of connection-oriented networks. Commun. Comput. Inf. Sci., Springer. **1**, 378–389 (2007)
70. Walkowiak, K.: Anycasting in connection-oriented computer networks: models, algorithms and results. Int. J. Appl. Math. Comput. Sci. **20**(1), 207–220 (2010)

71. Walkowiak, K., Rak, J.: Shared backup path protection for anycast and unicast flows using the node-link notation. In: Proc. IEEE International Conference on Communications (IEEE ICC'11), pp. 1–6 (2011)
72. Walkowiak, K., Rak, J.: Simultaneous optimization of unicast and anycast flows and replica location in survivable optical networks. Telecommun. Syst. **52**(2), 1043–1055 (2013)
73. Xia, W., Wen, Y., Foh, C.H., Niyato, D., Xie, H.: A survey on software-defined networking. IEEE Commun. Surv. Tutorials **17**(1), 27–51 (2015)
74. Xylomenos, G., Ververidis, C.N., Siris, V.A., Fotiou, N., Tsilopoulos, C., Vasilakos, X., Katsaros, K.V., Polyzos, G.C.: A survey of information-centric networking research. IEEE Commun. Surv. Tutorials **16**(2), 1024–1049 (2014)
75. Yin, H., Liu, X., Min, G., Lin, C.: Content delivery networks: a bridge between emerging applications and future IP networks. IEEE Netw. **24**(4), 52–56 (2010)
76. Zhou, S., Mondragon, R.J.: The rich-club phenomenon in the Internet topology. IEEE Commun. Lett. **8**(3), 180–182 (2004)

# Chapter 4
# Resilience of Wireless Mesh Networks

The second research area considered in this book refers to *Wireless Mesh Networks* (*WMNs*) formed by stationary mesh routers organized in a mesh topology [3, 22], providing transportation of flows originating from mesh clients (with little or no mobility). As presented in Fig. 4.1, WMN nodes have the *mesh* capability meaning that their functioning is not restricted only to transmission of local data. Instead, they are also able to relay in a multi-hop fashion information belonging to flows from other WMN nodes [18, 25]. If equipped with necessary functionality at certain nodes (i.e., gateways), WMNs may be also utilized to provide connectivity with external networks, e.g., Internet [5, 8, 68].

Most of WMN architectures are based on IEEE 802.11 standard defining how wireless devices can be mutually interconnected to create a mesh network [26]. In general, compared to Wi-Fi solutions, mesh structure of these networks implies a substantial enhancement in terms of the coverage area, connectivity, and scalability improvement, as well as brings about the simplification of deployment and maintenance activities [18, 68]. Additionally, WMN end users are provided with single-domain connectivity, as opposed to switching between Wi-Fi hot-spots. It has been proved that grid organization of WMN nodes provides up to 50 % higher throughput, compared to random node placement [68].

Due to utilization of the 71–86 GHz band [29, 39, 66], as well as highly directional antennas, effective transmission rate can be as high as 1–10 Gb/s per a millimeter-wave link with transmission range of at least several kilometres [64, 72]. Therefore, WMNs can be seen as a promising alternative to wired local or even metropolitan area networks providing last few miles connectivity especially in sparsely populated rural areas [22, 42].

It is also possible to equip each WMN router with MIMO technology (i.e., multiple-input multiple-output) utilizing multiple orthogonal channels [8]. This in turn leads to a further substantial increase of the network capacity [31, 71]. MIMO transmission is especially important in urban areas encountering signal distortions, where such systems help amplify and rebuild signal levels, while directional antenna settings visibly reduce interference between neighboring channels [68].

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications
and Networks, DOI 10.1007/978-3-319-22333-9_4

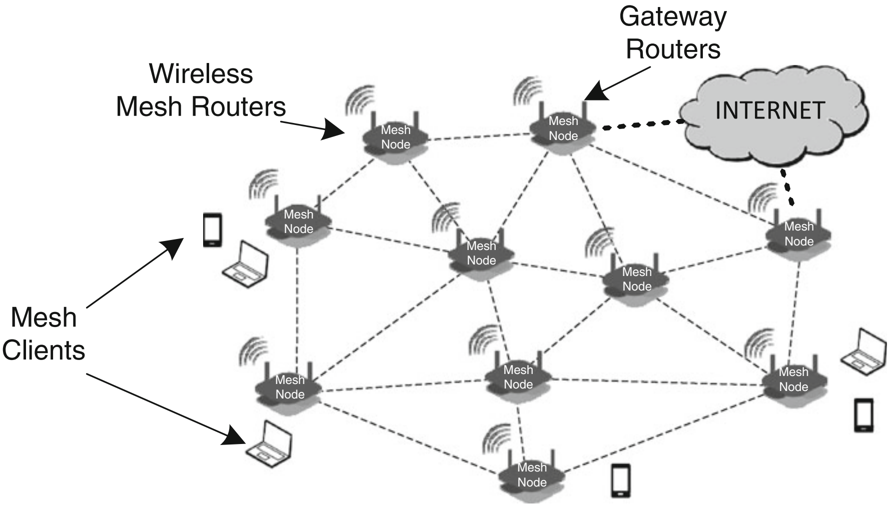


**Fig. 4.1** Example architecture of a Wireless Mesh Network including wireless mesh routers, mesh clients, and gateway routers

What is similarly important, WMNs can provide connectivity among users without direct Line of Sight (LOS) links.

WMNs have been also shown to be able to offer low costs of connections in the backhaul area [8]. That is why, utilization of WMN solutions (e.g., instead of applying the fiber optic technology) is well justified for economical, as well as practical reasons. It especially refers to 3G (4G) operators not having their own fiber infrastructure, who otherwise would have to either deploy their own fiber network (which is very expensive in rural areas [20]), or try to lease capacity from other network providers. Deployment of WMNs has been also proposed to obtain affordable access networks for underdeveloped regions [42].

In the last decade, many research teams have been addressing the problems of capacity planning, placement of WMN nodes, as well as routing, channel assignment, power control, topology control, etc. These problems are indeed very closely linked due to the nature of wireless interference. Therefore, when designing a WMN network, a joint consideration of these problems provides much better results in practice than in case of a separate analysis. A comprehensive overview of joint design problems is presented in [42].

A number of WMN installations are already in use in Europe, Australia, and US [17], deployed using equipment provided by, e.g., TerraNet, ArubaNetworks, or Motorola [4, 37, 62]. Example WMN architectures include city-wide (or campus-wide) networks in Las Palmas-Spain and Corpus Cristi [65], Cambridge-Massachusetts US [68], Houston-US [49], Oulu-Finland [59], Madison-US [69], or Dartmouth-US [24] with the number of nodes ranging from tens to hundreds, and the area of coverage measured in tens of square kilometres.

Apart from inheriting the common characteristics of the general ad-hoc networking concept (i.e., decentralized design, distributed communications), WMNs are known to exhibit characteristics that are novel in the wireless context, but rather typical to wired networks, i.e., stationary nodes, no LOS connectivity, high capacity, no limitations referring to node energy consumption [42].

Considering transmission of information itself, we can even say that WMNs possess most of wired networks characteristics with the only clear exception being the time-varying link stability. Therefore, applying the hop-count metric for routing purposes in WMNs is inefficient (as shown in [13]). To respond to dynamic characteristics of WMN links, several routing metrics have been proposed, the most important ones including: expected transmission count (ETX) [12], expected transmission time (ETT) [16], metric of interference and channel switching (MIC) [70], or multi-channel routing (MCR) [32]. They were designed to support WMN routing algorithms, e.g., AODV-ST [46], opportunistic Ex-OR [9], multipath routing [19], geographic routing [33], hierarchical routing [48], or multi-radio routing [32].

However, by incorporating the mentioned metrics into either a single-path or multipath routing [18], the impact of time-varying disruptions leading to partial/full degradation of the effective capacity of WMN links can be reduced only in a reactive way. Proactive protection against failures (commonly known to achieve better performance, e.g., in terms of reduction of the lost traffic after failures) is a rather new research direction for WMNs. The problem is indeed important, since independent of the failure cause (whether the result of an accident, forces of nature, or an intentional attack [63]), data and revenue losses encountered at high transmission rates of several Gb/s may be certainly severe.

In this chapter, we focus on failures of both WMN nodes and links. In particular, failures of WMN links can be covered by failure scenarios of the respective incident nodes (the topic addressed in Sect. 4.1). If referred to WMN links only (as in Sect. 4.2), they are commonly temporal (i.e., not observed after the interval of a negative factor duration).

Although a significant part of research efforts is related to scenarios of isolated random failures of single nodes being result of software errors, or physical faults [1], such an assumption is not proper for WMNs in many realistic scenarios. Example cases comprise natural disasters like earthquakes, volcano eruptions, tornadoes, or malicious human activities, including, e.g., bomb explosions [35] resulting in spatial correlation of failures of WMN nodes. WMN links are in turn very vulnerable to heavy precipitation responsible for remarkable signal attenuation.

In such cases, it is commonly assumed that the extent of negative outcomes depends on characteristics of a particular event, with the major factor being the distance of a network element from the failure epicenter. This in turn gives rise to the region failure scenario [30, 38, 50, 51] addressing simultaneous failures of multiple nodes located close enough to suffer from the results of the event.

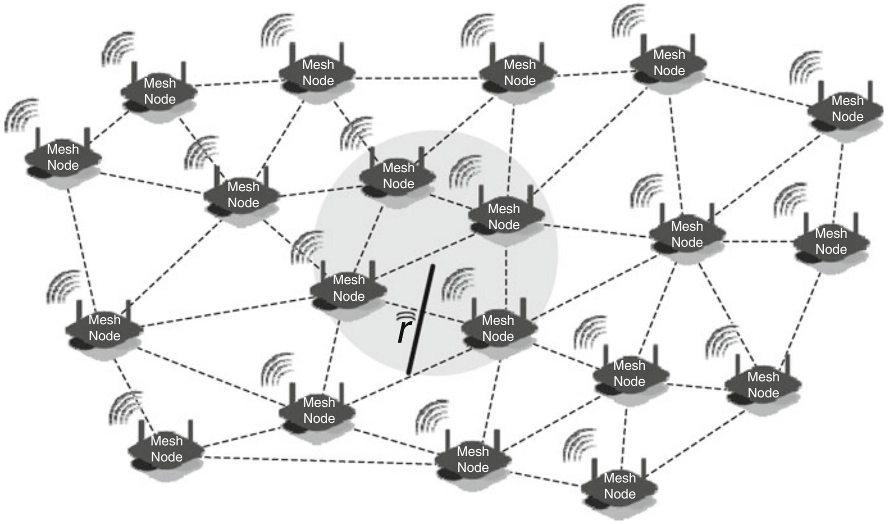


**Fig. 4.2** Example of a region failure: dark gray circle centered at the epicenter of disruptions and characterized by a given radius $\hat{\hat{r}}$ represents the area of possible failures of WMN nodes

Following [51], regions of failure can be defined with respect to either network topology or geometry. The latter approach, i.e., geometrical representation of a failure region determined by a circular area of radius $\hat{\hat{r}}$, shown in Fig. 4.2, is mostly used due to the predominant role of a node distance from the event epicenter [50, 51].

In particular, to the best of our knowledge, there are no survivability measures available designed to evaluate the performance of WMNs under region failures leading to simultaneous failures of multiple WMN nodes (as well as related links). Also, there are very few proposals referring to proactive protection of WMN flows against link failures. To provide the respective solutions, in Sect. 4.1, we introduce the appropriate survivability measures for WMNs, while in Sect. 4.2 – a new approach to proactive protection against weather-based region disruptions based on automatic antenna alignment features. Section 4.3 concludes this chapter.

## 4.1 Measures of Wireless Mesh Networks Survivability

Due to dependency of region-based failures on multiple characteristics, region failures need a detailed evaluation concerning their influence on the ratio of WMNs performance degradation (e.g., measured in terms of the fraction of flow surviving failures of WMN nodes located inside a given failure region).

In this section, we present our approach to WMN region failure assessment from [45] based on three introduced measures of WMNs survivability for a circular region failure scenario under random location of failure epicenters, i.e.:

- region failure survivability function (RFS) being the cumulative probability of all region failure scenarios $\delta$ occurrence, for which at least $\psi$ percent of flows are successfully served after failures,
- $p$-fractile region failure survivability function (PFRS), providing information on total flow reduction to at most $\psi$ percent after a failure at certain probability $p$,
- expected percentage of total flow delivered after a region failure as a function of region radius $\hat{\hat{r}}$ (EPFD).

Apart from providing the means of assessment of a given WMN to region disruptions, these measures are also proposed to enable comparisons of characteristics between different WMNs. To the best of our knowledge, besides our methodology from [45], there are currently no other relevant techniques available in the literature appropriate for measuring the vulnerability of WMNs to region failures of differentiated radiuses $\hat{\hat{r}}$ of failure regions.

Methodology of network survivability evaluation is well established with respect to wired networks (see e.g., [21, 47, 53, 55, 61, 67]). Concerning wireless networks, only a few proposals are available focusing, e.g., on connectivity of a network topology as a measure of fault-tolerance [52]. Connectivity can be generally used to provide a binary answer to the question whether the network is $k$-connected, i.e., able to provide transmission continuity after a simultaneous failure of $k$-1 nodes. This idea has been extended to cover, e.g., average connectivity [7], distance connectivity [6], or path connectivity [23].

However, majority of existing proposals of WMN evaluation are not suitable in the case of a region failure scenario with faults assumed to occur only in bounded areas. To address this problem, the respective region-based connectivity was proposed (see e.g., [35, 50, 51, 52]). Concerning the scenario of circular failure regions, we can distinguish the models of:

- deterministic failures (e.g., the single circular model from [51]), where, any node located within the failure region is assumed to always fail with probability 1,
- probabilistic failures with probability of a node failure due to a disruptive event depending on the node distance from the failure epicenter [35]. This failure probability is assumed to decrease when increasing the node distance from the failure epicenter.

Probabilistic models seem to provide more accurate results due to the common non-deterministic characteristics of natural disasters or attacks, resulting in failures of nodes located within failure regions with a certain probability. It is worth noting that available probabilistic approaches are not limitation-free. For instance in [35], the size of a failure region (given by radius $\hat{\hat{r}}$) is assumed to be constant. Another constraint in [35] is that probability of a node failure (even though decreasing with the increase of a node distance from the failure epicenter) is constant in each $i$-th area between two consecutive concentric annuluses (see Fig. 4.3a), which results in over- or underestimating the node failure probability values in some areas.

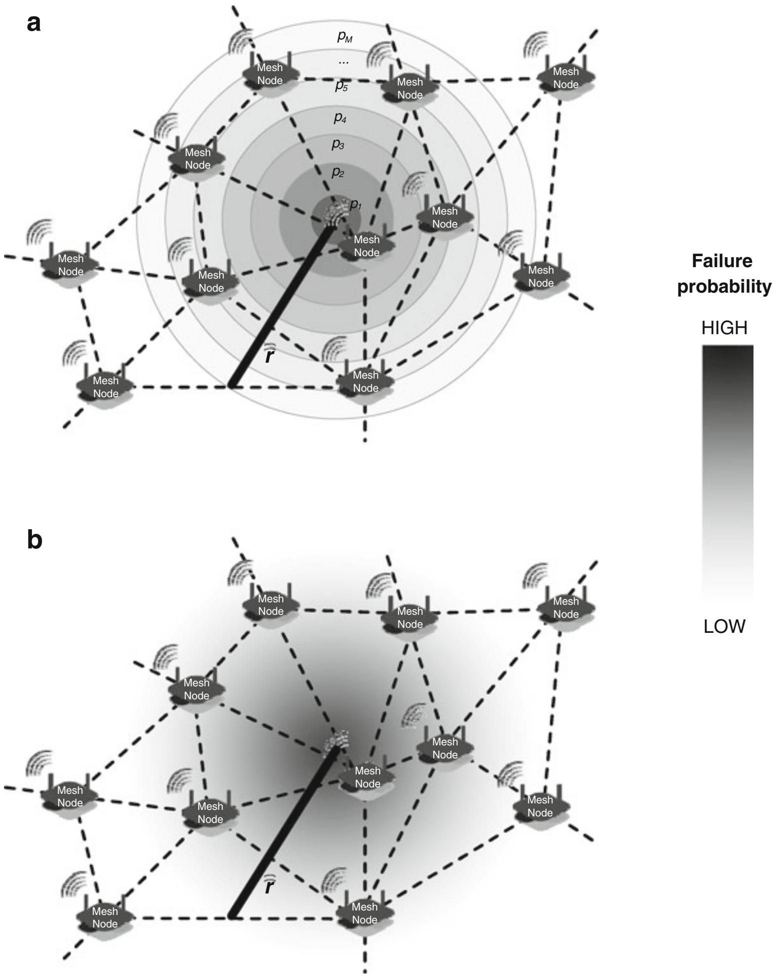


**Fig. 4.3** Visualization of region failure probabilities: (**a**) from [35], and (**b**) the proposed one

Considering proposals of WMNs characteristics evaluation under region failures, several approaches have been introduced (e.g., [50, 51, 52]) to determine whether transmission in WMNs is possible between pairs of non-faulty nodes. To the best of our knowledge, our proposal described in this section is the first one to introduce the WMN survivability measures for the case of varying region radiuses $\widehat{r}$, and using the continuous function of node failure probability (see Fig. 4.3b and Eq. 4.3) that covers the models from [35, 51] as special cases.

It is worth noting that similar survivability measures have been proposed in the literature so far only for random failure scenarios in wired networks (see e.g., [36]). However, they were designed for failures of network elements assumed to be statistically independent and equally probable, which is completely in contrast to characteristics of WMN region failures.

In the remaining part of this section, we first present details of the assumed network model (Sect. 4.1.1) followed by introduction of the proposed measures to evaluate the vulnerability of WMNs to region failures (Sect. 4.1.2). Next, we describe the methodology of WMN survivability evaluation (Sect. 4.1.3) and comment on results of simulations performed for example network topologies (Sect. 4.1.4).

### *4.1.1 Network Model*

In this chapter, we model the WMN topology by graph $\Gamma = (N, A)$, where $N$ represents the set of WMN stationary nodes (following [42]), while $A$ denotes the set of directed arcs $a_h = (i, j)$. Each WMN link between neighboring nodes $i$ and $j$ is represented by two arcs in opposite directions. Additional information refers to location of each node $n$ defined by coordinates $(\overline{x}_n, \overline{y}_n)$. Despite the assumed stationary characteristics of network nodes, methodology of network assessment presented in this section can be also easily adapted to the case of mobile nodes (if performed with respect to the instant topology of a network at time $t$).

Available capacity of any WMN link is a result of multiple factors the most important ones being: medium access protocol implementation, inter-channel interference implied by the respective link scheduling algorithm [11, 18], or time-varying factors including, e.g., weather-based disruptions caused by heavy rain falls (general propagation conditions) [27]. Since the effective capacity of any WMN link changes over time, it is reasonable to perform evaluations at a given time $t$, i.e., assuming that capacity of arc $a_h$ is equal to $c_h(t)$.

The set of demands $D$ consists of demands indexed by $r$ defined by ordered triples $(s_r, t_r, d_r)$, i.e., described by source and destination nodes $s_r$ and $t_r$, and the demanded capacity $d_r$.

Two matrices are used in our model description: $A_{nn}$ and $D_{nn}$. Node-to-node incidence matrix $A_{nn}$ provides information on connectivity with elements $a_{ij}$ defined by formula (4.1).

$$a_{ij} = \begin{cases} 1, & \mathit{if} \ \text{arc} \ a_h = (i, j) \in A_{nn} \\ 0, & \text{otherwise} \end{cases} \tag{4.1}$$

Information about aggregate capacities required for flows (commodities) between given pairs of end nodes is stored in elements $d_{st}$ of matrix $D_{nn}$.

$$d_{st} \equiv (s_r, t_r, d_r) \tag{4.2}$$

During evaluations, location of a failure epicenter is chosen at random (i.e., following the uniform distribution function of failure epicenter coordinates) within the smallest rectangular area containing the network. We assume a probabilistic failure scenario with a disruptive event affecting nodes localized within a given radius $\widehat{\widehat{r}}$ from the failure epicenter. In particular, in our model:

- radius $\widehat{\widehat{r}}$ of a failure circular region is uniformly distributed over $(0, \widehat{\widehat{r}}_{\max})$, where $\widehat{\widehat{r}}_{\max}$ is equal to half of the largest Euclidean distance between any two nodes in the network,
- probability $P(\widehat{\widehat{r}}_n)$ of node $n$ failure is given by a decreasing continuous function of distance $\widehat{\widehat{r}}_n$ between node $n$ and the failure epicenter (see Fig. 4.3b and Eq. 4.3). $P(\widehat{\widehat{r}}_n)$ is thus the generalization of the respective formula from [35].

$$P\left(\widehat{\widehat{r}}_n\right) = \begin{cases} -\dfrac{\widehat{\widehat{r}}_n}{\widehat{\widehat{r}}} + 1 = -\dfrac{\sqrt{\left(\bar{x}_n - \widehat{\widehat{x}}\right)^2 + \left(\bar{y}_n - \widehat{\widehat{y}}\right)^2}}{\widehat{\widehat{r}}} + 1, & \mathit{if}\ \widehat{\widehat{r}}_n \le \widehat{\widehat{r}} \\ 0, & \text{otherwise} \end{cases} \tag{4.3}$$

where

$(\bar{x}_n, \bar{y}_n)$ are coordinates (location) of node $n$

$\left(\widehat{\widehat{x}}, \widehat{\widehat{y}}\right)$ are coordinates (location) of the failure epicenter

$\widehat{\widehat{r}}$ is the radius of a failure region

$\widehat{\widehat{r}}_n$ is the distance of node $n$ from the failure epicenter

It is reasonable to introduce the WMN node failure probability function as given in Eq. 4.3, since, following [35], the negative impact of real physical attacks (e.g., bomb explosions, or electromagnetic pulse (EMP) attacks), as well as natural disasters (earthquakes, floods, etc.) attenuates gradually with the increase of the distance of WMN nodes from the failure epicenter. As given in [35], the maximum value of node failure probability can be assumed to be equal to 1 for locations of nodes matching exactly the failure epicenter. Its lowest value of 0 is in turn attributed to nodes located at distance $\widehat{\widehat{r}}_n$ not smaller than $\widehat{\widehat{r}}$ from the failure epicenter.

It is worth noting that this gradual attenuation of $P\left(\widehat{\widehat{r}}_n\right)$ values with the increase of the distance $\widehat{\widehat{r}}_n$ can be disturbed by several environmental factors including, e.g., topography or node protection characteristics. However, if we neglect them to simplify the analysis (following [35]), the decrease of probability $P\left(\widehat{\widehat{r}}_n\right)$ of node $n$ failure becomes linear with the increase of node $n$ distance from the epicenter of disruptions, as introduced in Eq. 4.3.

### *4.1.2 Proposed Measures to Evaluate the Survivability of WMNs*

The following notation is used in the remaining part of Sect. 4.1:

$\delta$ a region failure scenario given by the set of non-operational nodes (after the outage)
$P(\delta)$ probability of occurrence of a failure scenario $\delta$
$\Psi(\delta)$ random variable referring to the percentage $\psi$ of flows delivered in scenario $\delta$
$p_{\Psi}(\psi)$ probability density function of percentage $\psi$ of flows surviving the region failure, defined by Eq. 4.4

$$p_{\Psi}(\psi) = \sum_{\delta : \Psi(\delta) = \psi} P(\delta) \tag{4.4}$$

We introduce three measures of WMN survivability for a region failure scenario, i.e.:

(a) Region failure survivability function (RFS) of the percentage $\psi$ of flows successfully transmitted after region failures:

$$RFS(\psi) = \sum_{\delta : \Psi(\delta) \geq \psi} P(\delta) = 1 - \sum_{\delta : \Psi(\delta) < \psi} P(\delta) = 1 - cdf(\Psi) \tag{4.5}$$

As given in Eq. 4.5, RFS($\psi$) is defined for any value of $\psi$ as the cumulative probability of all region failure scenarios $\delta$ (i.e., for differentiated radiuses $\hat{\hat{r}}$ of failure regions), for which at least $\psi$ percent of flows survived the failure. It can be thus expressed as the reverse cumulative distribution function of $\Psi$. Although Eq. 4.5 shows some similarities with the respective one from [36] for wired networks, calculation of $P(\delta)$ values is completely different.

(b) $p$-fractile region survivability (PFRS):

$$PFRS(p) = \inf \left\{ \psi : \sum_{\delta : \Psi(\delta) < \psi} P(\delta) = p \right\} \tag{4.6}$$

Following formula (4.6), the value of $p$-fractile region survivability refers to the minimum percentage $\psi$ of flows delivered after a region failure, for which the probability of not exceeding this value is equal to $p$. PFRS thus returns useful information about probability $p$ that the total flow is reduced to at most $\psi$ percent after the failure.

Since RFS and PFRS measures do not depend directly on radius $\hat{\hat{r}}$ (i.e., they allow radius $\hat{\hat{r}}$ to take any value from (0, $\hat{\hat{r}}_{\max}$) interval), they are designed to give a general information on network vulnerability to region failures. These measures are thus appropriate, if the objective is to analyze the performance of WMNs independent of the failure region size $\widehat{\widehat{r}}$. However, information they provide is of different types.

For instance, if for a given WMN at least $\psi$ percent of traffic should be delivered (e.g., because such a portion of traffic is considered to be critical based on the Service Level Agreement), then RFS is the appropriate one to provide information about probability $p$ of fulfilling this requirement under region failures independent of size $\widehat{\widehat{r}}$ of the failure region. Naturally, the greater is the value of $p$, the better performance of a network can be achieved.

PFRS is in turn a suitable measure for a network operator to determine, given the respective probability $p$, what is the upper bound on the fraction $\psi$ of flow surviving a region failure. It is therefore useful to give information on probability that not all of $\psi$ percent of flows (e.g., referred to as the critical flow) will survive the region failure, i.e., in statements like: "with probability 0.7 the total flow will be reduced to at most 80 % of the traffic served before the region failure".

The following EPFD function is introduced to obtain a detailed characteristics of a WMN performance related to particular radiuses $\widehat{\widehat{r}}$ of failure regions.

(c) Expected percentage of total flow delivered after a failure (EPFD) as a function of region radius $\widehat{\widehat{r}}$:

$$EPFD\left(\widehat{\widehat{r}}\right) = \sum_{\psi} \psi \cdot p_{\Psi}\left(\psi, \widehat{\widehat{r}}\right) \tag{4.7}$$

where

$\widehat{\widehat{r}}$ is the radius of a failure region

$p_{\Psi}\left(\psi, \widehat{\widehat{r}}\right)$ is the probability density function of $\Psi$ defined for region failures of radius $\widehat{\widehat{r}}$

$$p_{\Psi}\left(\psi, \widehat{\widehat{r}}\right) = \sum_{\delta:\Psi(\delta)=\psi;\widehat{\widehat{r}}} P(\delta) \tag{4.8}$$

EPFD($\widehat{\widehat{r}}$) is defined in Eq. 4.7 as the expected value of percentage of flows to survive failures of nodes bounded in circular regions, i.e., derived using the probability density function $p_{\Psi}\left(\psi, \widehat{\widehat{r}}\right)$ obtained for failure regions of a given radius $\widehat{\widehat{r}}$ (see formula (4.8)).

Concerning scenarios of EPFD measure utilization, it can be useful in any performance analysis/comparison of WMNs under region failures being result of, e.g., natural disasters (like floods, or volcano eruptions), for which the failure region is commonly expected to have a circular shape defined by a given radius $\widehat{\widehat{r}}$. Another application of EPFD measure would be, e.g., when expecting failures confined to a given region characterized by radius $\widehat{\widehat{r}}$ (e.g., incoming flood), to predict their impact on WMN performance being helpful to take preventive actions.

The later part of this section provides information on how to utilize the three introduced measures to evaluate vulnerability of WMNs to region failures, as well as how to use them to provide comparisons of performance characteristics of different topologies.

### 4.1.3 Method of a WMN Survivability Evaluation

In this section, we explain our methodology of WMN survivability characteristics evaluation under region failures. In particular, we focus on how to determine the introduced RFS, PFRS, and EPFD characteristics for example WMNs.

Proposed measures are derived from the auxiliary function $F[\psi]$ providing information on the frequency of a given percentage $\psi$ of flows ($\psi \in \{0,1,\ldots, 100\}$) is successfully delivered after region failures. $F[\psi]$ values can be collected for a given WMN based on network performance observations after consecutive occurrences of disruptive events implying failures of WMN nodes confined to given regions. However, due to rather long inter-failure time intervals (typically measured in terms of months/years), deriving any characteristics based on real-life experiments is rather time-consuming and practically impossible.

In this section, an iterative procedure is presented to simulate consecutive region failures in a way to eliminate the inter-failure time. In this way, it is possible to analyze not only the performance of existing networks, but also to predict the survivability characteristics of planned (i.e., non-deployed) WMNs using information related to the abstract WMN topology and estimated demand volumes.

The 13-steps procedure to determine $F[\psi]$ values for a single set of demands is given in Fig. 4.4. The most important input information is related to:

- topology of existing/planned WMN defined by graph $\Gamma$ with sets $N$ and $A$ of nodes and directed arcs, representing network nodes and links, accordingly,
- location of network nodes defined by coordinates $(\overline{x}_n, \overline{y}_n)$,
- demands $r$, given by the requested throughput $d_r$, as well as source and destination nodes $s_r$ / $t_r$.

After initialization Steps 1–2, the purpose of each iteration given by Steps 3–13 is to obtain the percentage $\psi$ of flows delivered after failures of WMN nodes occurring in a given failure region. Coordinates of each failure epicenter and radius $\widehat{\widehat{r}}$ of a failure region are defined as random values by the continuous uniform distribution function (following [35]).

In particular, it implies that in each iteration of the analyzed procedure:

**INPUT**

- WMN topology given by graph $\Gamma = (N, A)$, where $N$ and $A$ are the sets of nodes and directed arcs, accordingly,
- location of network nodes determined by coordinates $(\overline{x}_n, \overline{y}_n)$,
- node-to-node incidence matrix $A_{nn}$,
- capacities $c_h$ of arcs $a_h = (i, j) \in A$,
- matrix $D_{nn}$ of aggregate capacities $d_r$ required for demands $r$ between end nodes $s_r$ and $t_r$,
- total load $c$ (the aggregate value of all transported flows before occurrence of a region failure),
- total number $FR$ of analyzed failure regions

**OUTPUT** $\boldsymbol{F}[\psi]$ function

**VARIABLES**

$\hat{f}$ the aggregate flow restored after a region failure,

$\overline{c_h}$ free (residual) capacity at arc $a_h$,

$ic$ iteration counter,

$\overline{c_r}$ capacity to be reserved for demand $r$ along links traversed by the respective paths in $\Gamma$

```
Step 1  For each $\psi \in \{0,1,...,100\}$, set $\boldsymbol{F}[\psi] = 0$.
Step 2  Set $ic := 0$.
Step 3  Create the temporal incidence matrix $\overline{A_{nn}}$ by assigning $\overline{A_{nn}} := A_{nn}$.
Step 4  Set $\hat{f} := 0$.
Step 5  Use the uniform distribution function to determine coordinates $(\hat{x}, \hat{y})$ of the next failure
        epicentre, as well as radius $\hat{r}$ of a failure region taken from range $(0; \hat{r}_{\max})$.
Step 6  Use the node failure probability function (Eq. 4.3) to determine the set of failed nodes.
Step 7  In $\overline{A_{nn}}$, set 0 to all elements representing failed links after failures in a given region.
Step 8  For each arc $a_h$, set the initial residual capacity $\overline{c_h} = c_h$ (i.e., to the value of the total link ca-
        pacity available at $a_h$).
Step 9  For each demand $r$ with both end nodes $s_r$ and $t_r$ not affected by the failure:
    9.1 Set the value $\overline{c_r}$ denoting capacity not assigned to demand $r$ to the initial value: $\overline{c_r} := d_r$.
    9.2 Find the shortest path $\pi$ using the distance metric and the incidence matrix $\overline{A_{nn}}$,
    9.3 Determine the capacity $c_r := \min_{a_h \in \pi} c_h$ of $\pi$, where $\overline{c_h}$ is the current residual capacity at
        arc $a_h$. If $\overline{c_r} \le c_r$, then increase $\hat{f}$ by $\mu := \overline{c_r}$, else increase $\hat{f}$ by $\mu := c_r$.
    9.4 Decrease $\overline{c_r}$ by $\mu$.
    9.5 For each arc $a_h$ traversed by path $\pi$, calculate new residual capacity $\overline{c_h} := \overline{c_h} - \mu$.
Step 10 For all affected flows being already not fully served (i.e., for which $\overline{c_r} > 0$), try to find the
        next shortest path. If such a path exists, then assign a new portion $\mu$ of capacity to it along
        the respective links, increase $\hat{f}$ by $\mu$, decrease $\overline{c_r}$ by $\mu$ and calculate the respective new
        residual capacities $\overline{c_h}$ of arcs $a_h$ traversed by this path. Repeat these actions for each de-
        mand $r$ until $\overline{c_r} = 0$, or no new path can be found.
Step 11 Calculate the percentage of flows $\hat{f}/f$ restored after failures occurring in a given region
        (where $f$ is the total traffic served before the failure), and increment the value of the element
        in $\boldsymbol{F}$ determined by index $\lfloor 100 \cdot \hat{f} / f \rfloor$.
Step 12 Increment the value of $ic$.
Step 13 If $ic < FR$, then go to Step 3.
```

**Fig. 4.4** Method of determining $F[\psi]$ values

- location of a failure epicenter is chosen at random within the smallest rectangular area containing the WMN topology, using the continuous uniform distribution function,
- radius $\hat{\hat{r}}$ of a failure circular region is uniformly distributed over $\left(0, \hat{\hat{r}}_{\max}\right)$, with $\hat{\hat{r}}_{\max}$ equal to half of the largest Euclidean distance between any two nodes in the network.

After the iteration initialization Steps 3–5, Step 6 is to identify the set of failed nodes (based on formula (4.3)). To evaluate the percentage $\psi$ of flows delivered in a given region failure scenario, for each flow with both end nodes being non-faulty, our method tries to find an alternate path of capacity $d_r$ (Steps 7–9). If the new path is found, but, due to link capacity limitations, it cannot be assigned the demanded capacity $d_r$, multipath routing is then applied to increase as much as possible the capacity assigned to demand $r$ after a region failure (Step 10).

The percentage $\psi$ of flows successfully delivered after a failure is calculated in Step 11 based on the ratio of the aggregate flow $\overset{\frown}{f}$ restored after the failure to the total flow $f$ being transported before the failure (i.e., after finding the alternate paths for all demands in a given region failure scenario). Following Steps 12–13, analysis is repeated until the number $FR$ of failure regions are evaluated.

All three introduced functions (RFS, PFRS, and EPFD) are next derived based on $\boldsymbol{F}[\psi]$ values. In particular:

- RFS($\psi$) is calculated based on empirical probabilities of restoring $\psi$ percent of flows after failures (each such probability is obtained by dividing the respective value of $\boldsymbol{F}[\psi]$ by $FR$, i.e., by the total number of analyzed region failures). According to formula (4.5), RFS($\psi$) is determined as the reverse cumulative distribution function of $\Psi$,
- PFRS($p$) is obtained based on the cumulative distribution function of $\Psi$ (formula (4.6)),
- EPFD($\hat{\hat{r}}$) is calculated based on probability density functions $p_{\Psi}\left(\psi, \hat{\hat{r}}\right)$ found separately for each radius $\hat{\hat{r}}$ of a failure region using Eq. 4.7.

In order to find the optimal solution to the problem of determining a new set of paths in a capacity-constrained network after failures with the objective to maximize the amount of restored flows, the respective linear programming formulation of the problem (LP) is necessary [40]. However, due to its $NP$-completeness (see e.g., [43]), the optimal solution can be found in reasonable time using offline approaches only for small problem instances (e.g., for networks up to 12–15 nodes). Therefore, in the proposed method, calculating the alternate paths (Steps 9.2 and 10 in Fig. 4.4) is done using the heuristic approach based on Dijkstra's algorithm [15] that is proved to have the polynomial computational complexity bounded in above by $O(|N|^2)$, where $|N|$ is the number of WMN nodes.

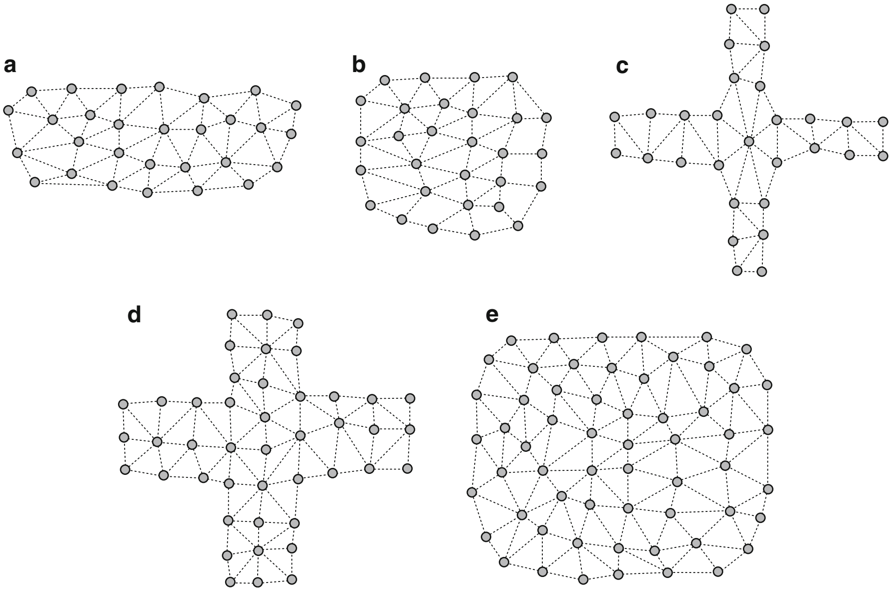


**Fig. 4.5** Evaluated topologies of: (**a**) N29, (**b**) N29_2, (**c**) N_29_3, (**d**) N44, and (**e**) N59 networks

### 4.1.4 Analysis of Modeling Results and Conclusions

In this section, we present evaluation of vulnerability of five example WMNs to region failures (i.e., N29, N29_2, N29_3, N44, and N59 networks from Fig. 4.5), utilizing the proposed survivability measures. First three networks (presented in Figs. 4.5a–c) are formed by 29 nodes located in $4000 \times 10{,}000$ m$^2$, $6000 \times 6000$ m$^2$, and $8000 \times 8000$ m$^2$ fields, accordingly, connected by 68, 68, and 57 wireless links, respectively. The other two networks shown in Figs. 4.5d, e consist of 44 and 59 nodes (located in fields of $10{,}000 \times 10{,}000$ m$^2$), respectively, connected by 97 and 150 wireless links, accordingly.

It is worth noting that for N29 network, due to visible differences between horizontal and vertical sizes of the rectangular area (4000 m and 10,000 m, accordingly), this network is likely to obtain the worst results concerning the portion of flows surviving the region failures (since for each network, the analyzed radiuses $\widehat{\hat{r}}$ of failure regions were up to half of the largest Euclidean distance between any two nodes in the network).

When assessing the vulnerability of network flows to region disruptions, all transmission paths (both before and after failures) were calculated as the cheapest ones using the standard metric of distance [34, 41]. After failures, reactive approach was utilized to redirect flows with survived end nodes. To provide the appropriate statistical analysis related to RFS, PFRS, and EPFD functions, the original values of $F[\psi]$ were obtained as the aggregate ones including all 100 investigated demand sets of a certain size. For each set of demands, failures related to $FR = 9000$ random regions were simulated.

Three simulation scenarios were considered. The first two, referred to as Scenarios A and B, were prepared to use the proposed measures to evaluate characteristics of different WMNs under a similar network load. To achieve this, the sets of unicast transmission demands included 25 % of randomly chosen node pairs. Scenario A was to verify characteristics of WMNs of the same size in terms of the number of nodes (i.e., N29, N29_2, and N29_3 networks consisting of 29 nodes), while Scenario B was aimed at evaluating networks of a similar area they covered (i.e., not necessarily comparable in terms of the number of nodes). Therefore, topologies analyzed in Scenario B included: N29, N44, and N59.

Additional Scenario C was to verify the properties of our measures under differentiated loads of N59 network. In particular, four sizes of demand sets (i.e., consisting of randomly chosen 25, 50, 75, and 100 % node pairs) were examined. Capacity $d_r$ of each unicast demand $r$ was assumed to be unitary.

Each network link offered 160 units of unitary capacity in each direction. Considering failure scenarios, radiuses $\widehat{\widehat{r}}$ of failure regions were uniformly distributed in range $\left(0, \widehat{\widehat{r}}_{\max}\right)$, where $\widehat{\widehat{r}}_{\max}$ was equal to half of the largest Euclidean distance between any two network nodes. Statistical analysis of results was based on 95 % confidence intervals. However, since sizes of obtained intervals did not exceed 1 % of the original values, due to low visibility they are not shown in Figs. 4.6–4.12.

### Region Failure Survivability (RFS)

Evaluation of vulnerability of WMN topologies to region failures using the RFS measure under the assumptions of Scenario A is presented in Figs. 4.6 and 4.7. Recall that RFS measure, defined in Eq. 4.5, was introduced to evaluate the probability that at least $\psi$ percent of flows survives after a region failure.

As presented in Figs. 4.6 and 4.7, with the increase of $\psi$, RFS starts decaying from the value of 1 (since independent of the network topology, probability of reducing the total flow to at least 0 % is equal to 1). When comparing RFS characteristics for any two network topologies, greater values of RFS for any value of $\psi$ imply a better performance of a network after a failure (since they reflect a greater chance of total flow reduction to at least $\psi$ percent after a failure).

The general conclusion following from Figs. 4.6 and 4.7 is that better results concerning network survivability characteristics under region failures are attributed

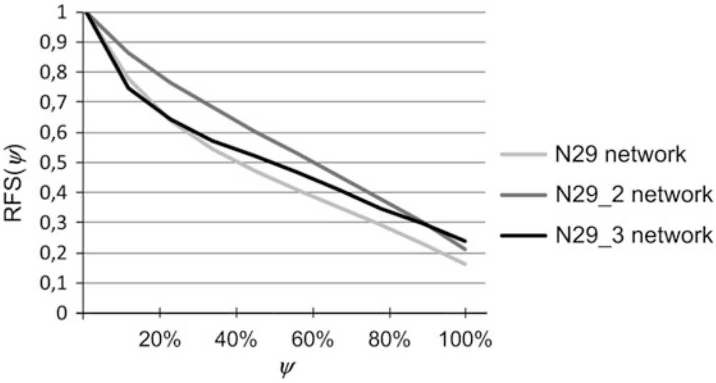


**Fig. 4.6** RFS($\psi$) function (Scenario A)

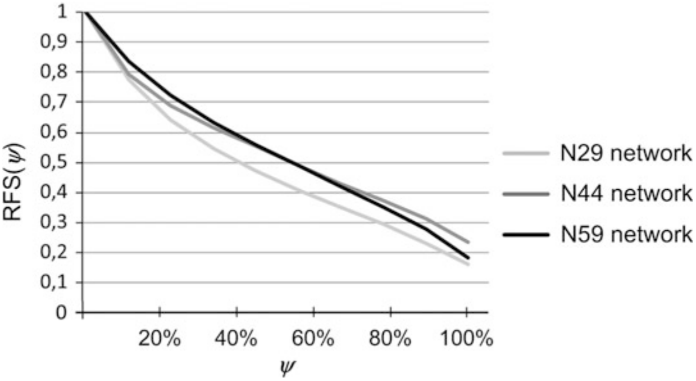


**Fig. 4.7** RFS($\psi$) function (Scenario B)

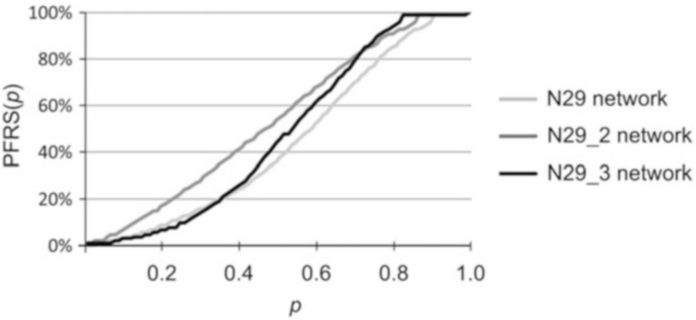


**Fig. 4.8** PFRS( $p$) function (Scenario A)

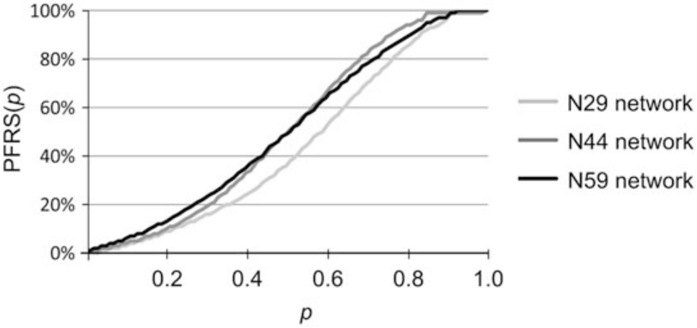


**Fig. 4.9** PFRS($p$) function (Scenario B)

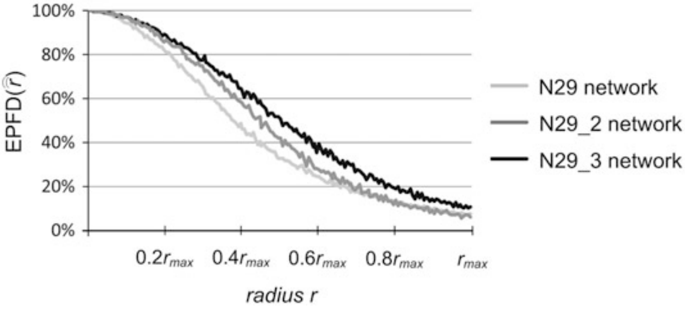


**Fig. 4.10** EPFD($\widehat{r}$) function (Scenario A)

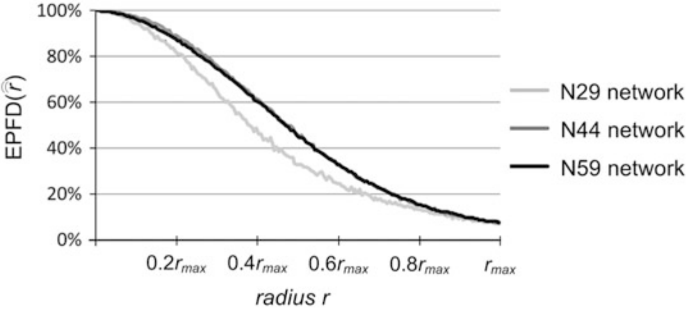


**Fig. 4.11** EPFD($\widehat{r}$) function (Scenario B)

to WMN networks with RFS functions driven by a slower decay with the increase of $\psi$ (i.e., for which independent of $\psi$ parameter, RFS values are higher). For instance, as shown in Fig. 4.6, N29 network (for which its horizontal and vertical sizes are remarkably different) is outperformed by N29_2 and N29_3 networks (located inside a square area) in Scenario A. In the same way, N44 and N59 networks turned out to outperform the N29 network in Scenario B (Fig. 4.7).

### *p*-Fractile Region Survivability (PFRS)

Figures 4.8 and 4.9 show the evaluation of WMN survivability characteristics using the $p$-fractile region survivability (PFRS) measure for Scenarios A and B. Recall that PFRS (Eq. 4.6) is to provide information on probability $p$ that the fraction of total flow delivered after region failures will not exceed $\psi$ (Y axis on Figs. 4.8 and 4.9).

For any WMN, it is thus better if, for any value of $p$, the upper bound on the portion $\psi$ of flow surviving the failure is higher. As shown in Figs. 4.8 and 4.9, independent of the network topology, PFRS values are always positively correlated with $p$. In general, the lower the values of PFRS, the network is more vulnerable to region failures. Similar to results for RFS measure, PFRS also showed that N29 network has the worst properties among all analyzed WMNs in Scenarios A–B.

### EPFD Function

Figures 4.10 and 4.11 show values of EPFD function obtained in Scenarios A and B. Recall that EPFD function is defined by formula (4.7) as the expected percentage of the total flow delivered after failures occurring in circular areas of a certain radius $\widehat{\widehat{r}}$. For any radius $\widehat{\widehat{r}}$, greater values of EPFD function imply more network flows surviving the failures. As shown in Figs. 4.10 and 4.11, N29 network obtained the worst characteristics also with respect to EPFD measure (which is compliant with the respective RFS and PFRS characteristics from Figs. 4.6–4.9, accordingly).

It is worth mentioning that all three measures do not depend on the network load (as shown in Fig. 4.12 for Scenario C). Therefore, they can be used to compare characteristics of different WMN topologies.

In this section, we focused on the evaluation of vulnerability of WMNs to region failures occurring in circular areas and introduced three measures for evaluation of WMN survivability. The first two measures, i.e., region failure survivability function – RFS, and $p$-fractile region survivability function – PFRS, were proposed to provide assessment of WMN vulnerability to region failures independent of the radius $\widehat{\widehat{r}}$ of the failure region. The third measure – the expected percentage of total flow delivered after a region failure as a function of region radius $\widehat{\widehat{r}}$ (EPFD) – was in turn designed for the evaluation of WMN performance depending on radius $\widehat{\widehat{r}}$ of a circular failure region.

Proposed measures were later utilized to evaluate the properties of three example topologies of WMNs. Simulation analysis confirmed that these measures give adequate and consistent information on WMN networks vulnerability to region failures. Since for all introduced measures, achieved characteristics did not depend on the network load, they can be thus utilized in comparisons of different WMNs.

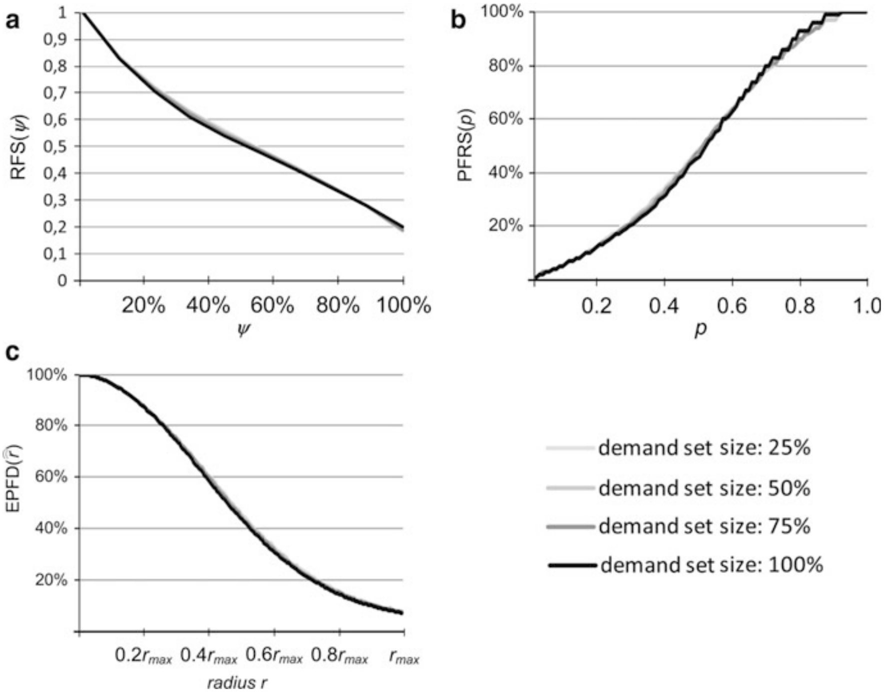


**Fig. 4.12** Characteristics of: (a) RFS($\psi$), (b) PFRS($p$), and (c) EPFD($r$) functions for Scenario C (N59 network)

## 4.2 A New Approach to Design of Weather Disruption-Tolerant Wireless Mesh Networks

As discussed in the former part of this chapter, failures of WMN nodes/links may imply severe data losses. In this section, we focus on link failures and present the respective approach to survivable routing to improve the WMN performance under link failures. As stated in [57], WMN links are very susceptible to weather disruptions in particular related to precipitation. Heavy rain storms may cause high signal attenuation remarkably reducing the available link capacity or implying a link failure leading to instability problems of routing (i.e., route flapping).

Issue of survivable routing is well researched with respect to wired networks (see e.g., [47, 55, 58, 61, 67]), in particular concerning protection of WDM network flows ([47, 55, 56, 60]). Among few proposals related to resilience of routing in wireless networks, we can mention reference [10] addressing shared medium problems and node mobility issues. However, these solutions cannot be directly applied to WMNs due to remarkably different characteristics. In particular, WMNs are commonly non-mobile and do not encounter contention problems (if equipped with directional antennas). Therefore, except for link stability issues, WMNs seem to share the most important characteristics with wired networks [27].

In order to provide protection of flows against weather-based disruptions of WMN links, it seems reasonable to use information related to expected incoming rain storms (e.g., achieved from radar echo measurements) to predict the real shapes of signal attenuation regions. Based on this idea, two approaches were introduced in [27], called XL-OSPF and P-WARP, to modify the link-state OSPF routing based on weather predictions. Both techniques utilize formulas (4.9–4.10) from [14] defining the dependency of signal attenuation on the rain rate.

$$\Omega\left(R_p, \varTheta\right) = \alpha R_p^{\beta}\left[\frac{e^{u\beta\vartheta}-1}{u\beta} - \frac{b^{\beta}e^{\iota\beta\vartheta}}{\iota\beta} + \frac{b^{\beta}e^{\iota\beta\varTheta}}{\iota\beta}\right], \quad \vartheta \le \varTheta \le 22.5\ \text{km} \tag{4.9}$$

$$\Omega\left(R_p, \varTheta\right) = \alpha R_p^{\beta}\left[\frac{e^{u\beta\varTheta}-1}{u\beta}\right], \quad 0 \le \varTheta \le \vartheta \tag{4.10}$$

where

$\Omega$ is the signal attenuation in dB
$\Theta$ is the length of the path over which the rain is observed
$R_p$ is the rain rate in mm/h
$\alpha$, $\beta$ are the numerical constants from [14]

$$u = \frac{\ln\left(be^{\iota\vartheta}\right)}{\vartheta}, \qquad b = 2.3{R_p}^{-0.17},$$
$$\iota = 0.026 - 0.03\ln R_p, \quad \vartheta = 3.8 - 0.6\ \ln R_p.$$

In particular, XL-OSPF utilizes a special metric of link cost being proportional to the observed bit error rate (BER) of the link (which is justifiable due to the clear impact of signal attenuation on the effective BER, as well as on packet error rate – PER). This metric is utilized in a reactive manner to update the OSPF routing characteristics. However, such an approach is not easy to deploy, since in the Media Access Control (MAC) layer there is no information on the actual BER between network nodes (it can be estimated using signal-to-noise ratio – SNR).

P-WARP in turn estimates the costs of WMN links using weather-based predictions of future conditions of links. This can be done either at one dedicated node or at a subset of nodes capable of collecting the weather-related radar data.

In this section, we focus on the issue of reducing the level of signal attenuation along millimeter-wave links in the presence of rain storms. In particular, in Sect. 4.2.1, we present in detail our method from [44] to perform in advance the periodic updates of a WMN topology following forecasts of heavy rain storms, using the functionality of a dynamic antenna alignment offered by a number of equipment vendors (see e.g., [54]). Next, in Sect. 4.2.2, we describe the ILP model proposed by us to obtain the optimal routing solution in accordance with the forecasted levels of signal attenuation at WMN links (that also returns the proper assignment of non-interfering channels to intersecting links). After that, in Sect. 4.2.3, we present the analysis of computational complexity of the problem followed by evaluation of our approach characteristics (Sect. 4.2.4).

To the best of our knowledge, protection of WMN links against weather-based region failures has not been sufficiently researched so far. In particular, there is no other proactive approach that is based on periodic updates of a WMN topology.

### *4.2.1 Proposed Approach*

The technique to provide protection of WMN links against weather-based disruptions described here does not impose any modifications of the routing algorithm. Therefore, it can be used in conjunction with practically any routing scheme, which makes our solution easily deployable. In particular, transmission paths are established based on conventional metric of link costs (e.g., the number of hops).

The main idea of our approach is to prepare the network to changing weather conditions by applying the periodic updates of WMN topology to improve the throughput during rain storms. We propose to perform the consecutive updates of a WMN topology by means of dynamic antenna alignment features (offered by a number of equipment vendors) utilizing predictions related to future conditions of WMN links based on rain storm forecasts obtained from real echo rain maps. This in turn implies periodic creation (or deletion) of WMN links, if low (or high) values of signal attenuation are expected for them, accordingly.

The network is modeled in this section by graph $\Gamma = (N, A)$ in a similar way as in Sect. 4.1.1. In particular, any link between two neighboring nodes $i$ and $j$ is represented by two directed arcs $a_h = (i, j)$ and $a_{h'} = (j, i)$, accordingly, and is assigned a given transmission channel from the set of available transmission channels. In order to focus on time-varying characteristics of WMN links, definition of graph $\Gamma$ is extended by:

– $\breve{T}$ denoting the lifetime of a network
– $\vartheta\left(\breve{T}\right): A \times \breve{T} \to \{0,\ 1\}$ function determining existence of links at time $t \in \breve{T}$
– $\gamma\left(\breve{T}\right): A \times \breve{T} \to \boldsymbol{R}$ link cost function based on signal attenuation ratio at time $t \in \breve{T}$ (formulas (4.9–4.10))

We assume the existence of a dedicated core node responsible for the alignment of antennas of all network nodes that has access to:

– the set of active network nodes and their locations,
– radar echo rain measurements (received periodically),
– demands to provide transmission between WMN end nodes.

The role of this core node is also to execute the procedure shown in Fig. 4.13. In particular, in Step 1 of this scheme, the estimated signal attenuation $\omega_h$ at each potential arc $a_h = (i,\ j)$ is determined using formulas (4.9–4.10). Actions of Step 2 are to return a new configuration of WMN links. In particular, in the proposed scheme $\omega_h$ values are used as link costs to obtain the set of the cheapest (in terms of signal attenuation) potential paths. If in Step 2, a given link is not used by any path, it will not be present in the updated WMN topology.

In the method from Fig. 4.13, we propose to utilize the heuristic approach to proceed with Step 2, since the problem to determine the optimal alignment of WMN antennas with the objective to minimize the aggregate signal attenuation over all transmission paths, defined in Sect. 4.2.2, is *NP*-complete (as proved in Sect. 4.2.3). New alignment of antennas (Step 3) is expected every $\tau$ time units (as defined in Step 4).

It is worth to recall that metric $\omega_h$ is used in our approach only to update the alignment of antennas at WMN nodes. Routing is in turn performed by means of a conventional protocol with all its characteristics unchanged. This implies that the original metric of link costs (i.e., the one normally used by the routing algorithm) is utilized instead of $\omega_h$ values to obtain the real transmission paths.

**Input**

- set of network nodes $N$, each node $i$ characterized by its coordinates $(\bar{x}_i, \bar{y}_i)$,
- initial set of WMN links extended by possible links between each pair of neighboring nodes,
- frequency of antenna alignment updates defined by interval $\tau$,
- current radar echo rain measurements,
- aggregate demand volumes for each pair of nodes $s_r$ and $t_r$ of $r$-th demand

**Output** Updated alignment of antennas corresponding to the forecasted level of signal attenuation based on rain storm predictions

Step 1 For each pair of neighboring nodes $i$ and $j$, determine signal attenuation $\omega_h$ of arc $a_h$=$(i, j)$ to be potentially installed between nodes $i$ and $j$ based on the forecasted radar rain information.

Step 2 Determine a new configuration of links based on estimated values of signal attenuation from Step 1. For this purpose, for each demand $r$ to provide transmission between nodes $s_r$ and $t_r$, find the cheapest transmission path in terms of costs $\omega_h$ calculated in Step 1.

Step 3 Distribute the results of Step 2 to all network nodes to set the alignment of WMN antennas.

Step 4 Wait $\tau$ units of time and go to Step 1.

**Fig. 4.13** Proposed methodology of periodic updates of alignment of WMN antennas

### 4.2.2 ILP Formulation of Weather-Resistant Links Formation Problem (WRLFP)

The problem to determine the optimal alignment of WMN antennas (Step 2 from Fig. 4.13) to minimize the aggregate signal attenuation over all transmission paths at time $t$ can be solved by determining the solution to the following ILP model.

**Indices**

| | |
|---|---|
| $\Gamma(N, A)$ | directed network |
| $N$ | set of network nodes; $\lvert N \rvert$ is the number of network nodes |
| $A$ | set of directed arcs; $\lvert A \rvert$ is the number of arcs |
| $h$ | arc index; $h = 1, 2, \ldots, \lvert A \rvert$ |
| $D$ | set of demands; $\lvert D \rvert$ is the number of demands |
| $r$ | demand index; $r = 1, 2, \ldots, \lvert D \rvert$ |
| $L_h$ | set of transmission channels available at arc $a_h = (i, j)$ |
| $1 \ldots \Lambda_h$ | indices of transmission channels at arc $a_h = (i, j)$; $\forall_h \Lambda_h = \Lambda$ |

**Constants**

| | |
|---|---|
| $s_r(t_r)$ | source (destination) node of $r$-th demand |
| $d_r$ | capacity of $r$-th demand |
| $c_h(t)$ | estimated total capacity of arc $a_h = (i, j)$ at time $t$ |
| $\omega_h(t)$ | estimated signal attenuation due to rain falls for arc $a_h = (i, j)$ at time $t$ |

**Variables**

| | |
|---|---|
| $x^{l}_{r;h}$ | equals 1, if $l$-th channel is assigned for $r$-th demand path at arc $a_h = (i, j)$; 0 otherwise |

**Objective**

It is to find the end-to-end transmission paths for all demands minimizing the cost defined by formula (4.11):

$$\varphi(x, t) = \sum_{r \in D} \sum_{l \in L_h} \sum_{h \in A} \omega_h(t) \cdot x^{l}_{r,h} \tag{4.11}$$

where $\omega_h(t)$ is the cost of arc $a_h = (i, j)$ based on signal attenuation ratio at time $t$.

**Constraints**

1. Flow conservation rules (based on Kirchhoff's law) for end-to-end paths:

$$\sum_{l \in L_h} \sum_{\substack{h \in \{h : a_h \equiv (n,j) \in A; \\ j \in N; j \neq n\}}} x^l_{r,h} - \sum_{l \in L_h} \sum_{\substack{h \in \{h : a_h \equiv (i,n) \in A; \\ i \in N; i \neq n\}}} x^l_{r,h} = \begin{cases} 1, & \textit{if } n = s_r \\ -1, & \textit{if } n = t_r \\ 0, & \text{otherwise} \end{cases} \tag{4.12}$$

   where $a_h = (n, j)$ arc incident out of node $n$; $a_h = (i, n)$ arc incident into node $n;$ $r \in D$; $n \in N$

2. On finite capacity of arcs $a_h$ (i.e., to assure that the total flow assigned to arc $a_h$ will not exceed the maximum available capacity):

$$\sum_{l \in L_h} \sum_{r \in D} x^l_{r,h} \cdot d_r \leq c_h(t); \qquad h \in A \tag{4.13}$$

3. On selection of different channels to interfering links (at most one link from the set of interfering links can be assigned a given channel $l$):

$$\sum_{r \in D} x^l_{r,h} + \sum_{r \in D} x^l_{r,h'} \leq 1 \tag{4.14}$$

   for each pair of intersecting arcs $a_h$ and $a_{h'}$; $l \in L_h$

### *4.2.3 Computational Complexity of WRLFP Problem*

In this section, we discuss the complexity of the considered optimization problem (4.11–4.14). In particular, by proving that it belongs to the class of *NP*-complete problems (by showing that one of its subproblems being the channel assignment problem, referred to as WR_CAP, is *NP*-complete), we explain that there is no efficient algorithm proposed so far to find the optimal solution in polynomial time.

Since assignment of channels to links is confined to the set of $\Lambda$ available channels (where $\Lambda$ can be any arbitrarily chosen small integer value), optimization version of WR_CAP channel allocation subproblem can be defined as follows.

**WR_CAPopt($A'$)**

*Given the set of network arcs $A'$ utilized by paths in Step 2 from Fig.* 4.13*, find the optimal assignment of transmission channels to arcs $a_h$ minimizing the number of used channels, providing that none of intersecting arcs receives the same channel.*

To show the *NP*-completeness of WR_CAP, it is sufficient to analyze its recognition version (i.e., a problem with "yes/no" answer) [28] shown below.

**WR_CAPrec($A'$, $k$)**

*Given a set of arcs $A'$ utilized by paths in Step 2 from Fig. 4.13, is it possible to find the optimal assignment of channels to arcs $a_h$ in the network that requires k different channels, providing that none of intersecting arcs receives the same channel?*

If recognition version of the problem is *NP*-complete, so is its optimization version [2].

**Theorem** WR_CAP problem is *NP*-complete.

*Proof* Following [2], when proving the *NP*-completeness of WR_CAP problem, it is sufficient to show that:

(a) WR_CAPrec($A'$, $k$) belongs to the class of *NP* problems

(b) A known *NP*-complete problem polynomially reduces to WR_CAPrec($A'$, $k$)

Regarding (a): WR_CAP problem belongs to complexity class *NP*, since it can be determined in polynomial time whether a given assignment of transmission channels to arcs $a_h$ is valid (i.e., whether it requires exactly $k$ channels from the set $\{1,\ldots, |\Lambda|\}$). In particular, checking the assignment of channels can be done in at most $O(|A'|) \leq O(|n^2|)$ operations, while verifying whether different channels are assigned to intersecting links requires at most $O(|n^2|)$ steps.

Regarding (b): To provide the second part of the proof, we will show that the known *NP*-complete problem of determining the optimal vertex-coloring of a graph of conflicts $G$ [28], here referred to as VCGC, can be transformed in polynomial time to WR_CAP problem. As shown in [28], recognition version of VCGC problem can be defined in the following way.

**VCGCrec($G$, $k$)**

*Given a graph of conflicts $G = (V, E)$, where V is the set of vertices, and E is the set of edges $e_h = (i, j)$ representing conflicts between the respective vertices i and j, is it possible to find the optimal assignment of colors to vertices from V requiring exactly k colors in a way that any two conflicting vertices i and j (i.e., connected by an edge in G) receive different colors?*

Assume that:

- $\{G = (V, E), k\}$ is the input to the VCGC recognition instance of the problem
- $G$ also represents the graph of conflicts for links to be installed in the network after executing Step 2 of the method from Fig. 4.13. In this graph:
  - ➢ vertices from $V$ represent links to be installed in the network,
  - ➢ there exists edge $e_h = (j, k)$ in $G$, if the respective network arcs $a_j$ and $a_k$ in $\Gamma$ intersect with each other, i.e., if they have to be assigned different channels

(⇒) Let us assume that it is feasible to color vertices from $G$ using $k$ different colors. In this case, any valid coloring of $G$ by $k$ different colors in

VCGCrec($G$, $k$) automatically returns a proper assignment of $k$ different channels to interfering links in WR_CAPrec($A'$, $k$).

(⇐) Assume that $k$ channels are sufficient to determine the solution to WR_CAPrec($A'$, $k$) problem. Then, after creating the respective graph of conflicts $G$ for interfering WMN links, we automatically have a valid coloring of $G$ vertices that requires $k$ different colors.

■

If we relax the problem by disregarding the requirement on allocation of different channels to intersecting links, the simplified problem remains *NP*-complete as a basic task to determine transmission paths between |$D$| pairs of nodes in capacity-constrained networks (classified as *NP*-complete in [43]). Therefore, to perform Step 2 from Fig. 4.13, heuristic Dijkstra's algorithm from [15] is used.

### Example Execution Steps of the Proposed Method

Results of a single iteration of the proposed method execution are presented in Fig. 4.14. Initial alignment of antennas is shown in Fig. 4.14a. Based on actual information related to the predicted rain intensity from Fig. 4.14b, a single iteration of our procedure is to provide the update of the network topology necessary to prepare the network for the forthcoming rain.

For this purpose, the WMN topology is first extended by the respective core node (responsible for determining the updates of a network topology) in a way to include all possible links between neighboring nodes (see Fig 4.14b). Based on the forecasted attenuation of a signal along each potential link, a new alignment of antennas is next determined (see Fig. 4.14c). As a result, the updated topology from

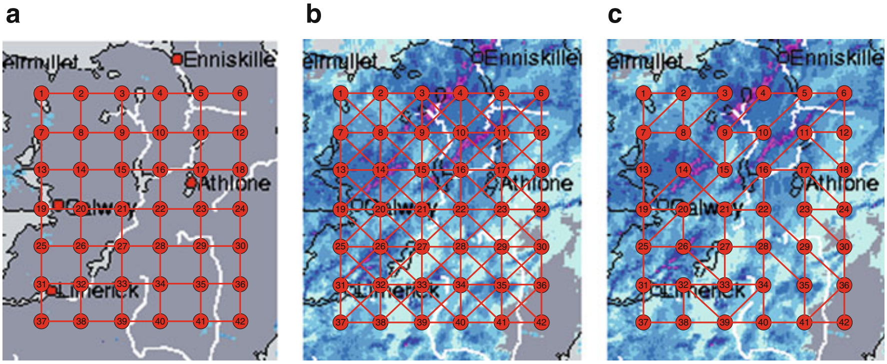


**Fig. 4.14** Example execution steps of the proposed procedure to modify the network topology (here the artificial Irish Network) according to the current rain storm forecasts including: (**a**) initial topology of the network, (**b**) extended topology including all possible links, and (**c**) results of the algorithm execution

Fig. 4.14c does not include links located within heavy rain storm areas (e.g., links (3, 4), (10, 11), (14, 15), and (15, 16)).

### 4.2.4 Analysis of Modeling Results and Conclusions

Simulations were performed to verify characteristics of our approach for two example artificial WMN topologies from Fig. 4.15, located in the area of Southern England and Ireland, respectively. Topology of each network included 42 nodes and formed a grid structure, with link lengths equal to 15 km. Characteristics of our technique (here referred to as "with protection") were compared with the common one implying no changes in the alignment of antennas (further referred to as the "no protection" case).

In the proposed technique, the initial set of WMN links included the ones marked with solid red lines in Fig. 4.15. Dashed blue lines are in turn used in Fig. 4.15 to indicate the extension of the set of links for possible utilization by the proposed technique. In the reference "no protection" approach, the set of links did not change over time (i.e., it was determined only by red lines from Fig. 4.15). In each network, nodes 1 and 42 were configured as gateways connecting the other ones to the Internet. Traffic outgoing the network via one of these gateways was assumed to be generated by each WMN node at a rate of 3 Mb/s.

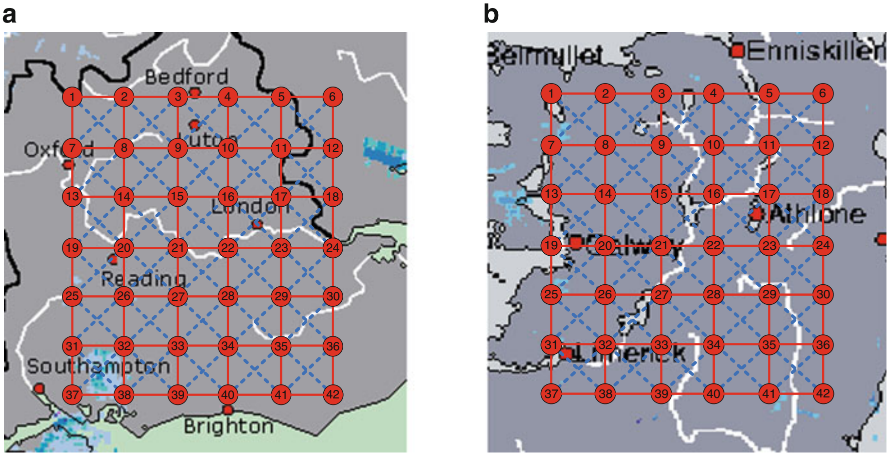


**Fig. 4.15** Example topologies of WMNs used in simulations. (**a**) Southern English Network (**b**) Irish Network

Simulations were focused on measuring the average signal attenuation ratio due to rain storms along transmission paths, as well as the average path hop count for three real scenarios of rain storms that occurred in November 2011:

- Scenario A: Southern England, Nov. 25, 2011, from 3:00 AM till 10:00 AM
- Scenario B: Ireland, November 26–27, 2011, from 8:00 PM till PM 7:00 AM
- Scenario C: Ireland, November 24, 2011, from 10:00 AM till 12:00 PM

Radar rain maps utilized in simulations were recorded every 15 min. Duration of the analyzed rain storms varied from 7 to 14 h. A limited set of investigated rain maps (one map per hour) is shown in the Appendix (Sect. 4.2.5).

### Signal Attenuation

As shown in Fig. 4.16, during heavy rain intervals, the level of signal attenuation increased remarkably. However, due to periodic updates of antenna alignment according to the forecasted signal attenuation ratio, our approach was able to prepare the WMN topology in advance for the forthcoming rain, and, as a result, to significantly decrease the signal attenuation ratio (up to 90 %, as shown in Fig. 4.16). A general conclusion is that the greatest improvement was observed for periods of heavy rain (which is a very desired feature). On the contrary, in the case of light rains, updating the alignment of antennas implied only a slight reduction of the analyzed signal attenuation ratio.

### Number of Path Links

Considering the average hop count of end-to-end transmission paths, for the common "no protection" method (for which the costs of links were independent of signal attenuation ratio), the average number of path links was equal to 5.6.

Our technique, due to operations of WMN links creation/deletion being implication of changing attenuation conditions, resulted in establishing WMN links in a more elastic way. In particular, this often implied forming diagonal links (e.g., between nodes 1 and 8), which in general resulted in shorter paths. As presented in Fig. 4.17, the average end-to-end hop count for our technique was often visibly lower than for the reference approach. However, during heavy rain periods (Scenario B, 10:00 PM–1:00 AM; Scenario C, 4:00 PM–10:00 PM), the average hop count for our approach was higher due to the need to provide detours over heavy rain areas.

In this section, we addressed the problem of signal attenuation in WMNs due to heavy rain storms. In order to improve the performance of the network during rainy intervals, we presented a method to apply in advance the periodic updates of a WMN topology that utilizes information from radar echo rain measurements. Our approach can be easily implemented in practice, as functionality of dynamic

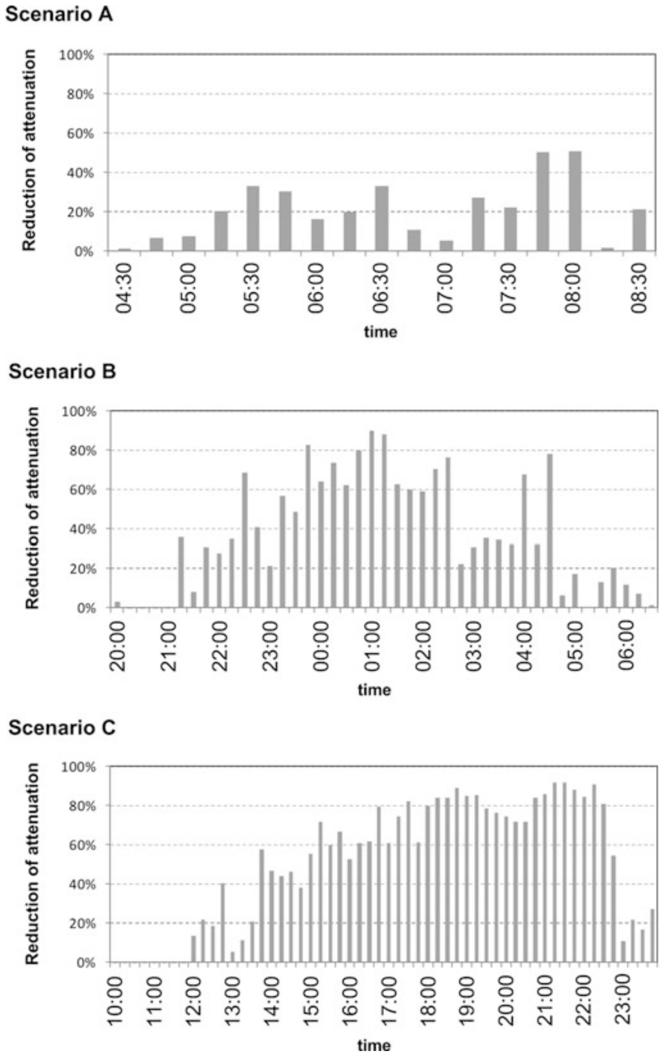


**Fig. 4.16** Obtained results concerning reduction of signal attenuation

antenna alignment is available in a number of commercial products. Another advantage is that our approach does not imply any changes of a routing algorithm.

It was verified by simulations performed for real radar rain maps that the proposed technique can bring about a significant decrease (up to 90 %) of signal attenuation, compared to the results of the reference "no protection" approach of not applying any changes to WMN topology. This improvement was observed for heavy rain periods (which is indeed a very desired feature).

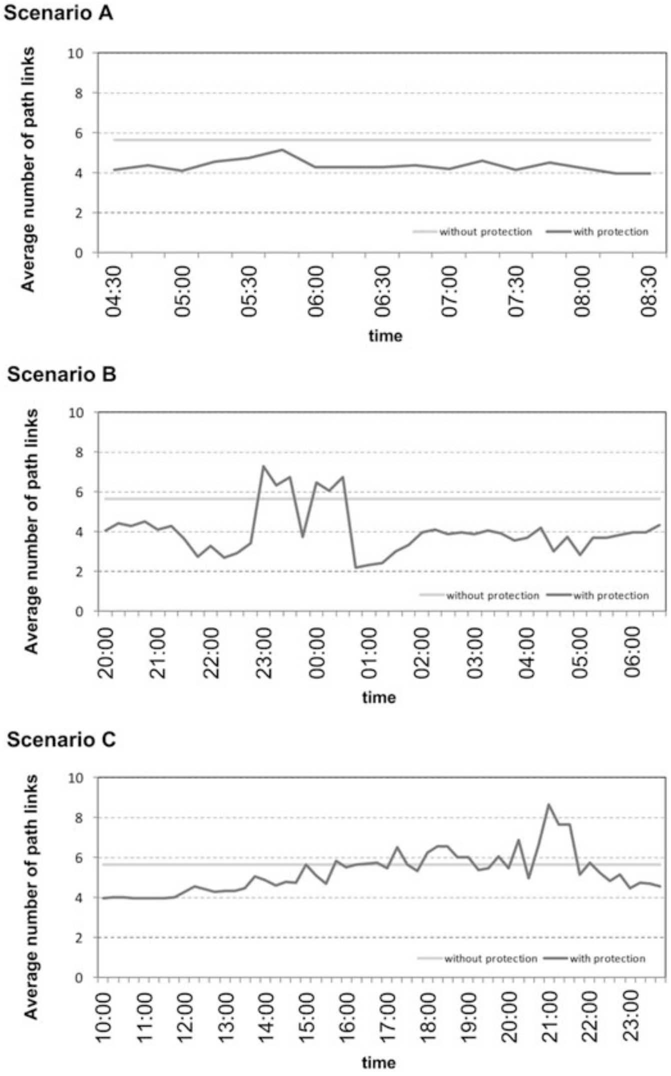
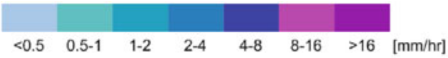


**Fig. 4.17** Obtained results concerning the average hop count

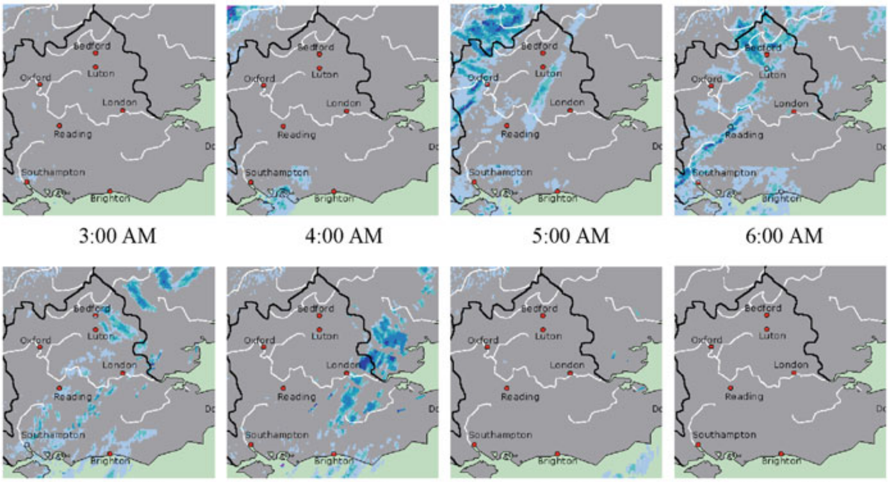
### *4.2.5 Appendix – Rain Radar Maps Used in Simulations*

Radar rain maps used in Sect. 4.2 are presented in this Appendix in 1 h interval (during simulations, rain maps were, however, collected every 15 min).

Each map presented here was created based on the following rain intensity scale provided by www.weatheronline.com service:



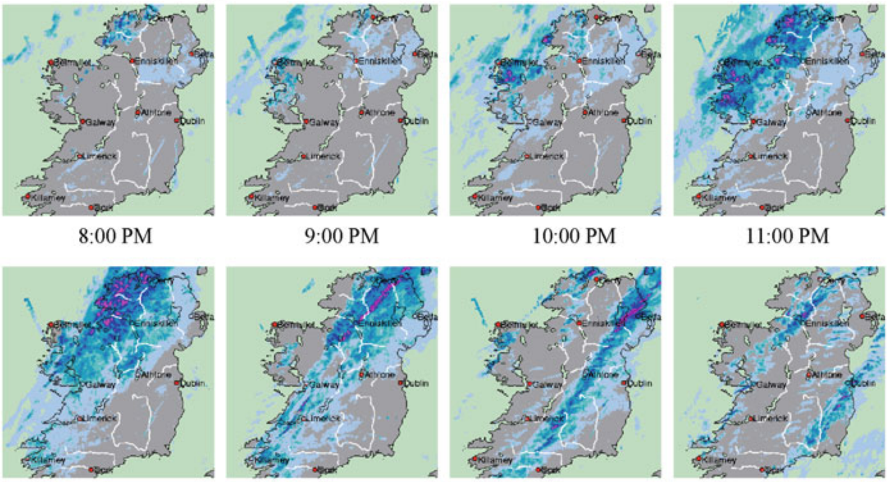
*Scenario A: Southern England, November 25, 2011*



3:00 AM 4:00 AM 5:00 AM 6:00 AM

7:00 AM 8:00 AM 9:00 AM 10:00 AM

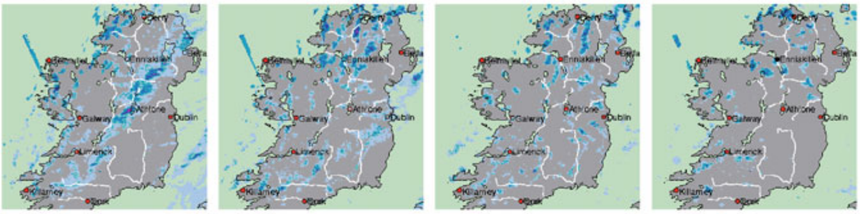
*Scenario B: Ireland, November 26-27, 2011*



8:00 PM 9:00 PM 10:00 PM 11:00 PM

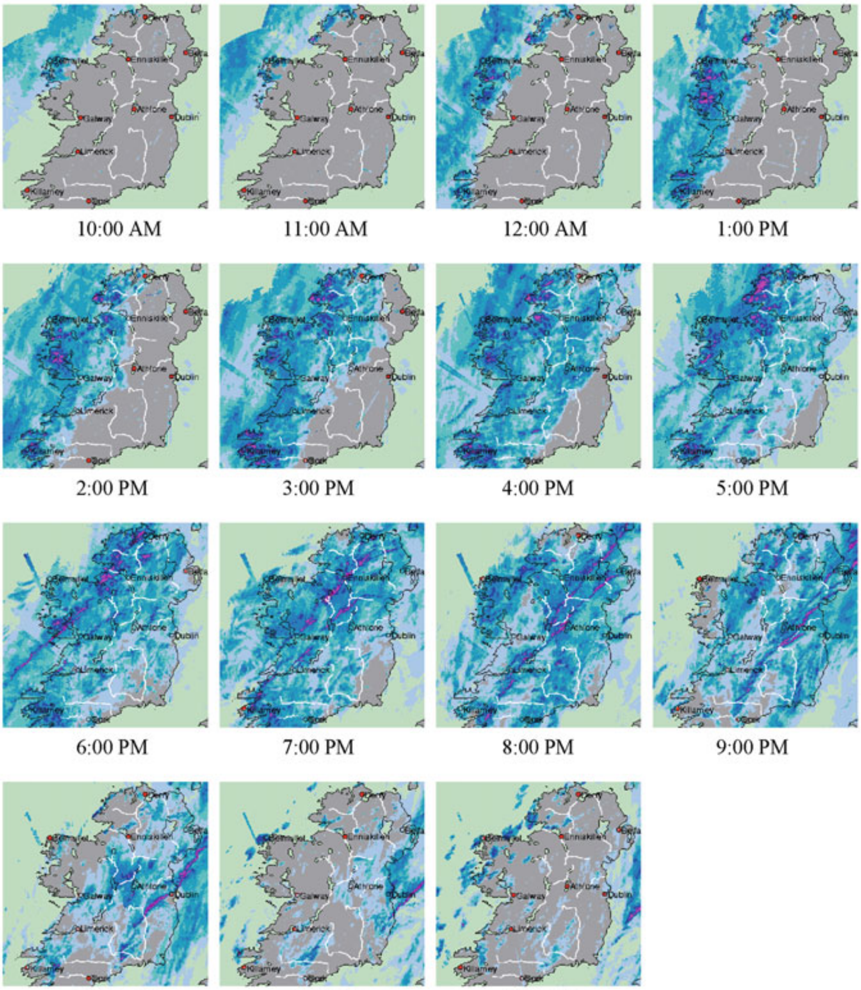
0:00 AM 1:00 AM 2:00 AM 3:00 AM

*Scenario B: Ireland, November 26-27, 2011 (continued from the previous page)*



4:00 AM 5:00 AM 6:00 AM 7:00 AM

*Scenario C: Ireland, November 24, 2011*



10:00 AM 11:00 AM 12:00 AM 1:00 PM

2:00 PM 3:00 PM 4:00 PM 5:00 PM

6:00 PM 7:00 PM 8:00 PM 9:00 PM

10:00 PM 11:00 PM 12:00 PM

## 4.3 Summary

As shown in this chapter, resilience of WMNs is an emerging issue. In terms of resilient routing, WMNs seem to exhibit most of characteristics commonly attributed to wired networks (e.g., stationary nodes, high capacity, or no limits on energy consumption), however, with a clear exception referring to the time-varying link stability. Due to high frequency communications, vulnerability of WMN links to weather-based disruptions is even more challenging than in conventional 802.11 architectures. That is why, direct application of resilience mechanisms originally designed for pure wired or ad hoc (wireless) networks is not proper.

As shown in this chapter, the number of proposals addressing the resilient routing issue in WMNs is limited. They include, e.g., updates of routing metrics to keep changing in a reactive way the communication paths as a response to time-varying characteristics of WMN links. However, a general observation (following from research results on wired networks resilience) is that considering the extent of losses after failures, better results would be achieved when applying the proactive approach (implying preparation of an alternate transmission solution in advance – before occurrence of a failure). Additionally, there have been no survivability measures proposed so far to evaluate the WMN performance for a common scenario of region failures (implied e.g., by weather-based region disruptions).

To address these issues, the respective survivability measures have been proposed in this chapter to allow for evaluation of a WMN performance under region failures leading to massive failures of WMN nodes/links. Unique characteristics of WMN links also made us propose the transmission scheme able to prepare the network in advance for the forthcoming heavy rain by means of automatic antenna alignment features. As a result, due to information from radar echo rain maps, settings of WMN antennas could be proactively updated to create links omitting areas of predicted heavy rain (which reduced the signal attenuation ratio up to 90 %).

It seems that other resilience approaches proposed for wired networks, e.g., based on multiple alternate paths could be also applied to WMNs after adapting them to characteristics of WMN links. This is a wide area for future research.

## References

1. Agarwal, P.K., Efrat, A., Ganjugunte, S.K., Hay, D., Sankararaman, S., Zussman, G.: Network vulnerability to single, multiple and probabilistic physical attacks. In: Proc. Military Communications Conference (MILCOM'10), pp. 1824–1829 (2010)
2. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: Network Flows: Theory, Algorithms, and Applications. Prentice Hall, Englewood Cliffs (1993)
3. Akyildiz, I.F., Wang, X., Wang, W.: Wireless Mesh Networks: a survey. Comput. Netw. **47**(7), 445–487 (2005)
4. Aruba Networks: http://www.arubanetworks.com/. Accessed on 24 Nov. 2014
5. Avallone, S., Akyildiz, I.F., Giorgio, V.: A channel and rate assignment algorithm and a layer-2.5 forwarding paradigm for multi radio wireless mesh networks. IEEE/ACM Trans. Networking **17**(1), 267–280 (2009)

6. Balbuena, M.C., Carmona, A., Fiol, M.A.: Distance connectivity in graphs and digraphs. J. Graph. Theory **22**(4), 281–292 (1998)
7. Beineke, L.W., Oellermann, O.R., Pipperta, R.E.: The average connectivity of a graph. Discret. Math. **252**(1–3), 31–45 (2002)
8. Benyamina, D., Hafid, A., Gendreau, M.: Wireless Mesh Networks design – a survey. IEEE Commun. Surv. Tutorials **14**(2), 299–310 (2012)
9. Biswas, S., Morris, R.: ExOR: opportunistic multi-hop routing for wireless networks. SIGCOMM Comput. Commun. Rev. **35**(4), 133–144 (2005)
10. Campista, M.E.M., Esposito, P.M., Moraes, I.M., Costa, L.H.M.K., Duarte, O.C.M.B., Passos, D.G., de Albuquerque, C.V.N., Saade, D.C.M., Rubinstein, M.G.: Routing metrics and protocols for wireless mesh networks. IEEE Netw. **22**(1), 6–12 (2008)
11. Capone, A., Carello, G., Filippini, I., Gualandi, S., Malucelli, F.: Routing, scheduling and channel assignment in Wireless Mesh Networks: optimization models and algorithms. Ad Hoc Netw. **8**(6), 545–563 (2010)
12. Couto, D.S.J.D., Aguayo, D., Bicket, J., Morris, R.: A high throughput path metric for multi-hop wireless routing. In: Proc. 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 134–146 (2003)
13. Couto, D.S.J.D., Aguayo, D., Chambers, A., Morris, R.: Performance of multihop wireless networks: shortest path is not enough. SIGCOMM Comput. Commun. Rev. **33**(1), 83–88 (2003)
14. Crane, R.: Prediction of attenuation by rain. IEEE Trans. Commun. **28**(9), 1717–1733 (1980)
15. Dijkstra, E.: A note on two problems in connexion with graphs. Numer. Math. **1**, 269–271 (1959)
16. Draves, R., Padhye, J., Zill, B.: Routing in multi-radio, multi-hop wireless mesh network. In: Proc. 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04), pp. 114–128 (2004)
17. Efstathiou, E.C., Frangoudis, P.A., Polyzos, G.C.: Stimulating participation in wireless community networks. In: Proc. 25th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'06), pp. 1–13 (2006)
18. Gabale, V., Raman, B., Dutta, P., Kalyanraman, S.: A classification framework for scheduling algorithms in Wireless Mesh Networks. IEEE Commun. Surv. Tutorials **15**(1), 199–222 (2013)
19. Ganjali, Y., Keshavarzian, A.: Load balancing in ad hoc networks: single-path routing vs. multi-path routing. In: Proc. 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'04), vol. 2, pp. 1120–1125 (2004)
20. Gass, R., Diot, C.: Measurements of in-motion 802.11 networking. In: Proc. 7th IEEE Workshop on Mobile Computing Systems and Applications (HotMobile'06), pp. 69–74 (2006)
21. Ghazisaidi, N., Scheutzow, M., Maier, M.: Survivability analysis of next-generation passive optical networks and fiber-wireless access networks. IEEE Trans. Reliab. **60**(2), 479–492 (2011)
22. Gore, D.A., Karandikar, A.: Link scheduling algorithms for Wireless Mesh Networks. IEEE Commun. Surv. Tutorials **13**(2), 258–273 (2011)
23. Guo, Y.: Path connectivity in local tournaments. Discret. Math. **167**(168), 353–372 (1997)
24. Henderson, T., Kotz, D., Abyzov, I.: The changing usage of a mature campus-wide wireless network. In: Proc. 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04), pp. 187–201 (2004)
25. Huang, S., Dutta, R.: Design of Wireless Mesh Networks under the additive interference model. In: Proc. IEEE International Conference on Computer Communications and Networks (ICCCN'06), pp. 253–260 (2006)
26. IEEE standards: http://standards.ieee.org/findstds/standard/802.11s-2011.html. Accessed on 11 Jan. 2015
27. 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)

28. Karp, R.M.: Reducibility among combinatorial problems. In: Complexity of Computer Computations, pp. 85–103. Plenum, New York (1972)
29. Khan, J.A., Alnuweiri, H.M.: Traffic engineering with distributed dynamic channel allocation in BFWA mesh networks at millimeter wave band. In: Proc. 14th IEEE Workshop on Local and Metropolitan Area Networks (IEEE LANMAN'05), pp. 1–6 (2005)
30. Kim, K., Venkatasabramanian, N.: Assessing the impact of geographically correlated failures on overlay-based data dissemination. In: Proc. IEEE Global Communications Conference (IEEE Globecom'10), pp. 1–5 (2010)
31. Kodialam, M., Nandagopal, T.: Characterizing the capacity region in multi-radio multi-channel Wireless Mesh Network. In: Proc. 11th Annual International Conference on Mobile Computing and Networking (MIBICOM'05), pp. 73–87 (2005)
32. Kyasanur, P., Vaidya, N.H.: Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. SIGMOBILE Mob. Comput. Commun. Rev. **10**(1), 31–43 (2006)
33. Lee, S., Bhattacharjee, B., Banerjee, S.: Efficient geographic routing in multihop wireless networks. In: Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05), pp. 230–241 (2005)
34. Li, H., Cheng, Y., Zhou, C., Zhuang, W.: Routing metrics for minimizing end-to-end delay in multiradio multichannel wireless networks. IEEE Trans. Parallel Distrib. Syst. **24**(11), 2293–2303 (2013)
35. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: Reliability assessment for wireless mesh networks under probabilistic region failure model. IEEE Trans. Veh. Technol. **60**(5), 2253–2264 (2011)
36. Molisz, W.: Survivability function – a measure of disaster-based routing performance. IEEE J. Sel. Areas Commun. **22**(9), 1876–1883 (2004)
37. Motorola: http://wirelessnetworks-asia.motorola.com/. Accessed on 11 Jan. 2015
38. Neumayer, S., Modiano, E.: Network reliability with geographically correlated failures. In: Proc. 29th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'10), pp. 1–9 (2010)
39. Ohata, K., Maruhashi, K., Ito, M., Nishiumi, T.: Millimeter-wave broadband transceivers. NEC J. Adv. Technol. **2**(3), 211–216 (2005)
40. Papadimitriou, C.: Computational Complexity. Addison-Wesley, Boston (1994)
41. Paris, S., Nita-Rotaru, C., Martignon, F., Capone, A.: Cross-layer metrics for reliable routing in wireless mesh networks. IEEE/ACM Trans. Networking **21**(3), 1003–1016 (2013)
42. Pathak, P.H., Dutta, R.: A survey of network design problems and joint design approaches in Wireless Mesh Networks. IEEE Commun Surv. Tutorials **13**(3), 396–428 (2011)
43. Pioro, M., Medhi, D.: Routing, Flow and Capacity Design in Communication and Computer Networks. Morgan Kaufmann Publishers, San Francisco (2004)
44. Rak, J.: A new approach to design of weather disruption-tolerant Wireless Mesh Networks. Telecommun. Syst., 1–12 (2015). doi:10.1007/s11235-015-0003-z
45. Rak, J.: Measures of region failure survivability for wireless mesh networks. Wirel. Netw. **21**(2), 673–684 (2015)
46. Ramachandran, K., Buddhikot, M., Chandranmenon, G., Miller, S., Belding-Royer, E., Almeroth, K.: On the design and implementation of infrastructure mesh networks. In: Proc. IEEE Workshop on Wireless Mesh Networks (WiMesh'05), pp. 1–12 (2005)
47. Ramamurthy, S., Sahasrabuddhe, L., Mukherjee, B.: Survivable WDM mesh networks. IEEE/OSA J. Lightwave Technol. **21**(4), 870–883 (2003)
48. Ramanathan, R., Steenstrup, M.: Hierarchically-organized multihop mobile wireless networks for quality-of-service support. Mob. Netw. Appl. **3**(1), 101–119 (1998)
49. Robinson, J., Swaminathan, R., Knightly, E.W.: Assessment of urban-scale wireless network with a small number of measurements. In: Proc. 12th Annual International Conference on Mobile Computing and Networking (MobiCom'08), pp. 187–198 (2008)
50. Sen, A., Banerjee, S., Ghosh, P., Shirazipourazad, S.: Impact of region based faults on the connectivity of wireless networks: In: Proc. 47th Allerton Conference on Communication, Control and Computing, pp. 1430-1437 (2009)

51. Sen, A., Murthy, S., Banerjee, S.: Region-based connectivity – a new paradigm for design of fault-tolerant networks. In: Proc. 15th International Conference on High Performance Switching and Routing (HPSR'09), pp. 1–7 (2009)
52. Sen, A., Shen, B.H., Zhou, L., Hao, B.: Fault-tolerance in sensor networks: a new evaluation metric. In: Proc. 25th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'06), pp. 1–12 (2006)
53. Shengli, Y., Wang, B.: Highly available path routing in mesh networks under multiple link failures. IEEE Trans. Reliab. **60**(4), 823–832 (2011)
54. SkyPilot: http://skypilot.trilliantinc.com/pdf/broch_sp_products.pdf. Accessed on 9 Jan. 2015
55. Somani, A.: Survivability and Traffic Grooming in WDM Optical Networks. Cambridge University Press, Cambridge (2006)
56. Soproni, P., Cinkler, T., Rak, J.: Methods for physical impairment constrained routing with selected protection in all-optical networks. Telecommun. Syst. **56**(1), 177–188 (2014)
57. Sterbenz, J.P.G., Cetinkaya, E.K., Hameed, M.A., Jabbar, A., Shi, Q., Rohrer, J.P.: Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation and experimentation. Telecommun. Syst. **52**(2), 705–736 (2013)
58. Sterbenz, J.P.G., Hutchison, D., Cetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schoeller, M., Smith, P.: Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance. Telecommun. Syst. **56**(1), 17–31 (2014)
59. Strix Systems: http://www.strixsystems.com/Service_Providers.aspx. Accessed on 11 Jan. 2015
60. Tapolcai, J.: Survey on out-of-band failure localization in all-optical mesh networks. Telecommun. Syst. **56**(1), 169–176 (2014)
61. 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)
62. TerraNet AB: http://www.terranet.se. Accessed on 12 Jan. 2015
63. Todd, B., Doucette, J.: Multi-flow optimization model for design of a shared backup path protected network. In: Proc. IEEE International Conference on Communications (IEEE ICC'08), pp. 131–138 (2008)
64. Torkildson, E., Ananthasubramaniam, B., Madhow, U., Rodwell, M.: Millimeter-wave MIMO: wireless links at optical speeds. In: Proc. 44th Allerton Conference on Communication, Control and Computing, pp. 1–9 (2006)
65. Tropos: http://www.tropos.com/index1.php. Accessed on 11 Jan. 2015
66. TU-R F.1704. Characteristics of multipoint-to-multipoint fixed wireless systems with mesh network topology operating in frequency bands above about 17 GHz, ITU-R Recommendation F.1704 (2005)
67. Vasseur, J.-P., Pickavet, M., Demeester, P.: Network Recovery. Morgan Kaufmann, San Francisco (2004)
68. Vural, S., Wei, D., Moessner, K.: Survey of experimental evaluation studies for wireless mesh network deployments in urban areas towards ubiquitous Internet. IEEE Commun. Surv. Tutorials **15**(1), 223–239 (2013)
69. XIOCOM: http://www.xiocom.com/serv_ind.html. Accessed on 9 Mar. 2015
70. Yang, Y., Wang, J., Kravets, R.: Interference-Aware Load Balancing for Multihop Wireless Networks. Technical Report, University of Illinois at Urbana-Champaign (2005)
71. Zhang, J., Wu, H., Zhang, Q., Li, B.: Joint routing and scheduling in multi-radio multi-channel multi-hop wireless networks. In: Proc. IEEE International Conference on Broadband Networks (BroadNETS'05), pp. 631–640 (2005)
72. Zhao, L., Gao, L., Zhao, X., Ou, S.: Power and bandwidth efficiency of wireless mesh networks. IET Netw. **2**(3), 131–140 (2013)

# Chapter 5
# Disruption-Tolerant Routing in Vehicular Ad-hoc Networks

Owing to a significant increase of a number of vehicles on roads raising the possibility of accidents, we have been recently observing a growing interest in *inter-vehicular communications* (*IVC*) [55] enabled by deployment of vehicular wireless communication systems. Following [24, 31, 55], *Vehicular Ad-hoc NETworks* (*VANETs*) are now considered by car manufacturers as an emerging solution to provide communications for a wide range of applications designed to solve a number of mutually non-independent problems, in particular related to:

- *public safety* aspects. Road safety can be improved by messages exchanged by vehicles, e.g., in the case of accidents/collisions, bad weather conditions (ice/water on road) [67], unexpected events (e.g., low bridges, oil on road), or to assist the drivers in lane change/overtaking operations [5, 6, 60],
- *traffic coordination* issues. VANETs can be utilized to provide traffic monitoring/shaping (including traffic light management), i.e., aimed at adjusting the scheduling of traffic lights to help the drivers move in the green phase, thus also contributing to *reduction of the environmental pollution* [1],
- *infotainment* providing the travelers with on-board information and entertainment services such as Internet access or music download [27, 36, 64].

Based on ability of forwarding information at transit nodes, IVC networks can be next classified as either: (1) single-, or (2) multi-hop IVCs (shortly SIVCs and MIVCs, accordingly) [55], as shown in Fig. 5.1. Single-hop systems are often used by applications requiring short-range communications (e.g., automatic cruise control, lane merging). The latter group (i.e., multi-hop vehicular ad-hoc networks used, e.g., by traffic monitoring applications) is investigated in detail later in this chapter. A detailed overview on vehicular networking issues is presented in [31].

It is worth noting that many VANET applications (e.g., related to collision warning or traffic coordination issues) require reliable real-time communications to work efficiently, since information arriving too late is often no longer useful.

Another important fact is that usability of a VANET system frequently strongly depends on the *penetration rate* defined as the ratio of vehicles equipped with

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications and Networks, DOI 10.1007/978-3-319-22333-9_5

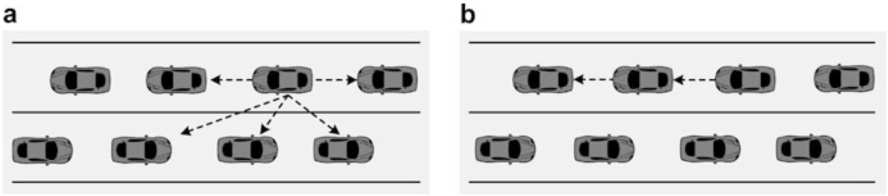


**Fig. 5.1** Examples of (**a**) single-, and (**b**) multi-hop inter-vehicular communications

**Table 5.1** Utilization of VANET channels based on [2]

| Channel number | CH 170 | CH 172 | CH 174 | CH 176 | CH 178 | CH 180 | CH 182 | CH 184 |
|---|---|---|---|---|---|---|---|---|
| | | | CH 175 | | | CH 181 | | |
| Channel use | For future use | SCH | SCH | SCH | CCH | SCH | SCH | SCH |
| Bandwidth [MHz] | 5 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| | | | 20 | | | 20 | | |
| Bit rate [Mbps] | – | 3–27 | 3–27 | 3–27 | 3–27 | 3–27 | 3–27 | 3–27 |
| | | | 6–54 | | | 6–54 | | |

VANET solutions. Any vehicle equipped with a system with *p* percent penetration rate will benefit in only *p* percent of all situations [55].

As proposed by the U.S. Federal Communications Commission (FCC) and defined in the IEEE 802.11-2012 specification (formerly the 802.11p standard [27]), vehicles equipped with wireless devices can form in ad-hoc manner a VANET network utilizing seven 10 MHz channels in the 5.880–5.925 GHz band (often referred to as *Dedicated Short Range Communications* (*DSRC*) [64, 67]). According to this specification, effective channel capacity is in range of 3–54 Mbps, while the typical link length is limited to about 300 m [2, 55, 64].

As shown in Table 5.1, the set of channels consists of one *control channel – CCH* (also denoted as CH 178), and six 10 MHz *service channels* (*SCH*), namely: CH 172, 174, 176, 180, 182, and 184. Additional channel CH 170 (with 5 MHz bandwidth) is reserved for future use. High-power channel CH 184 is used for safety messages distribution only. Except for CH 184, all other service channels can be utilized by non-safety applications. To obtain higher data rates, channels CH 174 and 176 can be combined into a single 20 MHz channel CH 175. The same can be done for channels CH 180 and CH 182 to form channel CH 181.

In DSRC, each device when tuned to the control channel (CCH) for half of the frame time (i.e., 50 ms) can distribute beacon messages containing information related to vehicle speed, location (coordinates), etc. [1]. Such beacons can be exchanged periodically with frequency in range (1, 10) Hz, i.e., every 100 ms – 1 s. In the same interval, emergency messages can be also generated. As shown in Fig. 5.2, at the end of the CCH interval, devices can switch to one of six service channels for next 50 ms (SCH interval) to perform tasks related to distribution of applications data (preceded by a negotiation phase at the end of CCH interval).

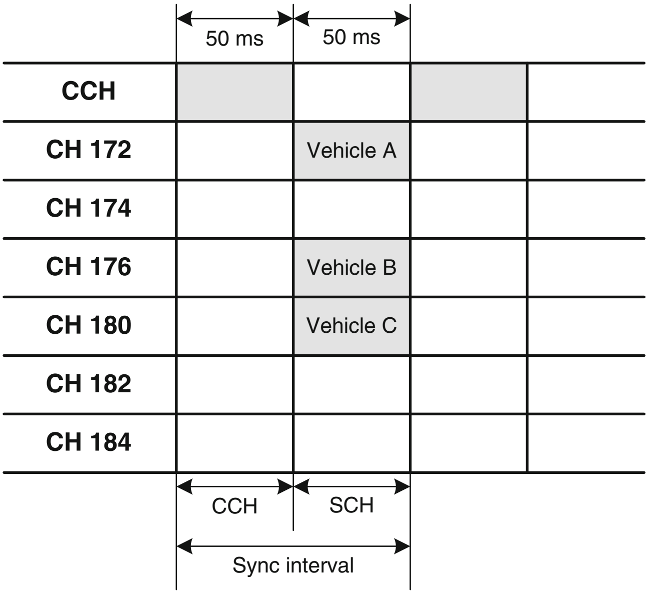


**Fig. 5.2** Example of multichannel operation of DSRC

IVC networks implement the major assumptions of 802.11 standards family, since IEEE 802.11a is used by both ETSI in Europe and IEEE in the US as a basis for vehicular communications. In particular, in the US, the respective IEEE 802.11p and 1609 standards for the IVC have been already ratified. However, the respective European (ETSI) standards (commonly deviating from the analogous US specifications) are still under preparation.

Vehicular communications can be provided either without or with the support of a roadside infrastructure, also referred to as *vehicle-to-vehicle* (*V2V*) and *vehicle-to-infrastructure* (*V2I*) wireless networking, accordingly [31, 65]. V2V communications is infrastructure-free and provided only by *On-Board Units* (*OBUs*) – the appropriate in-vehicle equipment. In the case of V2I class, message forwarding always takes place between OBUs installed inside vehicles and the respective roadside infrastructure (including *Road-Side Units – RSUs*) [55].

Following [55], V2I systems can be further decomposed into *sparse* and *ubiquitous* systems offering services at selected points (e.g., hotspots, road intersections, or in the entire network area, accordingly). Examples of sparse V2I systems applications include parking availability, parking payment, collection of tolls for roads/bridges/tunnels, busy intersection scheduling, or gas station advertisement.

An example ubiquitous V2I system would be related, e.g., to vehicle-to-land-based communications offering high-speed Internet access providing onboard entertainment by means of an entire range of applications, from e-mail and media streaming to Web browsing and voice over IP, independent of vehicle location, but, therefore, prohibitively expensive.

Following [55], each OBU to work properly should be equipped with:

- Central Processing Unit (CPU) implementing applications and communication protocols,
- wireless transceiver (to transmit/receive data to/from the neighboring vehicles, or a roadside infrastructure),
- Global Positioning System (GPS) receiver providing positioning and time synchronization information,
- sensors measuring differentiated parameters,
- interface allowing for human-system interaction.

VANETs can be considered as a special case of Mobile Ad-hoc NETworks (MANETs) due to their self organization, self management, short transmission range, as well as relatively low bandwidth. Following [28, 38, 63], individual characteristics of VANETs include:

- highly dynamic topology with frequent topology changes resulting in common *path unavailability*, or even causing network disconnections/partitioning (lifetime of a VANET link is typically measured in terms of seconds),
- sufficient level of energy and storage (since vehicles, contrary to sensors, are not small devices). The only clear exception to this rule refers to nodes formed by *Vulnerable Road Users* (*VRUs*), e.g., pedestrians [3],
- utilization of geographic-based message distribution providing fast dissemination of time-critical information to other vehicles,
- stringent requirements on message propagation delay (e.g., for safety applications).

Due to these characteristics, providing reliable transmission is a challenging issue. Definition of communications reliability for VANETs is also significantly different from the generic one, originally proposed for communication systems.

Following [40], *reliability of inter-vehicular communications* can be defined as the ability to deliver messages to destination vehicles within the specified operation duration.

Although in the last decade, several tutorials have been published in the literature (covering, e.g., vehicular networking issues [24, 31], mobility models [22], information distribution [38, 49], characteristics of VANET applications [58], or green communications [1]), reliability of end-to-end vehicular communications is a rather new issue with few proposals/results available.

In VANETs, data distribution (commonly referred to as *data dissemination*) is defined as the transportation of data to the intended recipients while satisfying certain requirements such as, e.g., delay [58]. These requirements are obviously differentiated depending on the characteristics of applications and disseminated data.

In order to focus on reliability of inter-vehicular communications, it is necessary to identify first the respective QoS requirements of VANET applications in terms of reliability attributes, in particular including message delivery latency, as presented in Sect. 5.1. Such differentiation of application types implies differentiated QoS requirements. In particular, apart from services requiring real-time message delivery (e.g., safety applications), there also exist delay-tolerant applications (e.g., providing infotainment services).

Since one-hop broadcasting, also referred to as a *single-hop message dissemination* [57], is the basic networking technique for many VANET applications (especially for safety-related services), there is a group of recent papers focusing on reliability issues of inter-vehicle links. For instance, authors of [4, 8, 64] investigate the inter-vehicle distance distribution characteristics and vehicle movement patterns as the main factors of limited lifetime of links. Indeed, for any two neighboring vehicles moving in opposite directions at speed of 96 km/h, the average link lifetime is at most 10 s [38]. A detailed overview of single- and multi-hop message dissemination protocols can be found in [49].

Many VANET applications require multi-hop communications to deliver information to distant end nodes. Examples include V2V communications providing dissemination of safety-related messages to vehicles separated by several transit nodes. For them, communications reliability should be analyzed on the path level [17, 69], or in terms of end-to-end communications, e.g., in the case of multi-hop multipath routing/broadcasting [25, 54].

Issues of multi-hop data delivery are investigated in detail in Sect. 5.2. Sections 5.3 and 5.4 in turn include our two original proposals to improve reliability of end-to-end V2V communications. Section 5.5 presents the concluding remarks.

## 5.1 Reliability Requirements of VANET Applications

Following [24], VANET applications can be classified into three groups, namely: safety, transport efficiency, and infotainment. In each case, transmission reliability, due to its obvious relation with message delivery latency, is an important part of QoS requirements. In general, due to short-range communications, reliability of inter-vehicular communications depends on the number of vehicles equipped with VANET solutions. However, differentiated characteristics of applications imply differentiated ways to achieve this goal. Categories of safety applications, as identified by the Vehicle Safety Communications Consortium (VSCC) in [59], are presented in Table 5.2 with information from [31] related to the upper bound on message delivery latency (i.e., the *critical latency*).

Safety applications require real-time communications, since validity of exchanged information (e.g., post-crash warnings) expires very fast, and any such delayed information shortly becomes useless for neighboring vehicles. Therefore, following [1, 31], 100 ms is considered to be the maximum latency of safety messages delivery, while 10 Hz is the minimum frequency of such messages exchange.

Safety-related notifications can be either *event-driven* or *periodic* [24]. Event-driven messages are disseminated after identification of an event. Periodic

**Table 5.2** Classification of safety applications based on [31, 59]

| Category | Application scenario | Minimum frequency (Hz) | Critical latency (ms) |
|---|---|---|---|
| Intersection collision avoidance | Blind merge warning | 10 | <100 |
| | Intersection collision warning | | |
| | Left turn assistant | | |
| | Pedestrian crossing information warning | | |
| | Stop sign movement assistant | | |
| | Stop sign violation warning | | |
| | Traffic signal violation warning | | |
| Public safety | Approaching emergency vehicle warning | 10 | <100 |
| | Emergency vehicle signal preemption | | |
| | Post-crash warning | | |
| | SOS services | | |
| Sign extension | Curve speed warning | 10 | <100 |
| | In-vehicle amber alert warning | | |
| | Low bridge warning | | |
| | Low parking structure warning | | |
| | Work zone warning | | |
| | Wrong way driver warning | | |
| Vehicle diagnostics and maintenance | Just-in-time repair notification | 10 | <100 |
| | Safety recall notice | | |
| Information from other vehicles | Adaptive headlamp aiming | 10 | <100 |
| | Automation system (Platoon) | | |
| | Blind spot warning | | |
| | Cooperative adaptive cruise control | | |
| | Cooperative collision warning | | |
| | Cooperative forward collision warning | | |
| | Cooperative glare reduction | | |
| | Cooperative vehicle-highway | | |
| | Emergency electronic brake lights | | |
| | Highway merge assistant | | |
| | Highway/railroad collision warning | | |
| | Lane change warning | | |
| | Pre-crash sensing | | |
| | Road condition warning | | |
| | Vehicle-to-vehicle road feature notification | | |
| | Visibility enhancer | | |

notifications are in turn utilized to provide proactive distribution of messages related to vehicle status/location (e.g., in the case of forward collision warnings).

Safety applications, commonly using one-hop broadcasting, have stringent requirements on the minimum scope of message dissemination. According to [24], it should be feasible to send safety-related messages over a distance of at least 150 m by one-hop broadcast communications. In the case of multi-hop distribution of safety messages (each hop realized by one-hop broadcasting), the total coverage distance of safety applications is in the range between 300 m and 20 km [19, 42].

Table 5.3 presents classification of non-safety applications, as identified by the Car-to-Car Communications Consortium (C2C-CC) consisting of Audi, BMW, DaimlerChrysler, Fiat, Renault, and Volkswagen from [42], including information related to traffic efficiency and infotainment applications.

The former class (traffic efficiency) comprises applications utilizing either vehicle-to-infrastructure communications (e.g., traffic light scheduling to help the driver move in the green phase by keeping the green-light optimal speed), or vehicle-to-vehicle communications (e.g., V2V merging assistance). Analogously, for the latter class of infotainment applications, either V2I communications (e.g., for point of interest (POI) notifications) or V2V communications (e.g., multi-hop Internet wireless access) can be utilized. However, in general, there is no standardized consensus about the requirements concerning reliable communications characteristics and metrics to measure them.

A significant part of non-safety applications (especially related to infotainment issues) belongs to the class of delay-tolerant services, for which real-time data delivery is not required. For them, the respective maximum end-to-end latency can be thus higher (e.g., 500 ms, as given in Table 5.3). Another characteristics is that, contrary to safety applications, non-safety services, e.g., Internet access apart from operating in V2I environment, often use multi-hop V2V communications.

For non-safety applications without stringent requirements on real-time data delivery, it is frequently sufficient to use the best-effort scheme, e.g., by incorporating the store-carry-forward technique [47, 63]. This solution allows for storing the messages at a given transit node until the next forwarding node becomes available (i.e., if it appears available in the communications range of the transit node).

**Table 5.3** Classification of non-safety applications based on [42]

| Category | Application scenario | Minimum frequency (Hz) | Critical latency (ms) |
|---|---|---|---|
| Traffic efficiency | Enhanced route guidance and navigation | 10 | <100 |
| | Green light optimal speed advisory | 10 | <100 |
| | V2V merging assistance | 10 | <100 |
| Infotainment and others | Internet access in vehicle | 1 | <500 |
| | Point of interest notification | 1 | <500 |
| | Remote diagnostics | 1 | <500 |

Table 5.4 presents the summary of functionalities related to communications type, addressing, efficiency, and real-time requirements of selected applications.

## 5.2 Network Layer Addressing and Routing Issues

Concerning addressing issues, two schemes can be distinguished, namely fixed and geographical addressing [55]. In *fixed addressing*, a node is assigned a specified address once it joins the network, which remains unchanged until the node leaves the network.

In *geographical addressing*, where each node is characterized based on its geographical coordinates, address assigned to a given node based on its location changes as the vehicle moves (i.e., not necessarily leaving the network). Apart from geographical information, packet forwarding often depends on additional attributes, e.g., direction of vehicle movement, road ID, vehicle type, height, weight, maximum speed, or even driver characteristics (i.e., beginner, professional) [55].

In the later part of this chapter, we focus on multi-hop V2V communications where data is forwarded via multiple hops from a sender to one/multiple receivers. At this point, it is necessary to emphasize that in some papers, e.g., in [38], multi-hop broadcasting is improperly considered as one of VANET routing schemes, since in practice it does not involve any Layer 3 processing (apart from Layer 2 broadcasting). Therefore, multi-hop routing and multi-hop broadcasting should be analyzed separately, as considered in Sects. 5.3 and 5.4, accordingly.

Multi-hop V2V networking practically has no physical boundaries. As a result, capacity of such an unbounded system does not scale. To find a scalable solution, it is usually assumed that data can be forwarded to vehicles located within a specific area [55]. Depending on application requirements, the following routing approaches can be distinguished [55]:

- unicast routing with fixed addressing (e.g., for entertainment applications like file transfer),
- unicast routing with geographical addressing utilized to improve routing efficiency (compared to fixed addressing),
- multicast routing with fixed addressing – possible in theory, but practically not used due to a huge overhead related to multicast groups maintenance,
- multicast routing with geographical addressing – used by most applications (including, e.g., emergency warning or traffic monitoring applications).

However, multicast routing with geographical addressing is often replaced by broadcast multi-hop transmission addressed in Sect. 5.4.

**Table 5.4** Summary of representative applications requirements based on [55]

| | Communications type | | | | | | |
|---|---|---|---|---|---|---|---|
| Application | Single-hop V2V | Multi-hop V2V | Sparse V2I | Ubiquitous V2I | Addressing scheme | Efficiency dependent on OBU density | Real-time requirements |
| Car-to-land communications | | | | + | *Fixed* | | |
| Collision warning (highway) | | + | | + | *Geo* | + | + |
| Collision warning (intersection) | + | + | + | + | *Geo* | + | + |
| Targeted vehicular communications | + | + | | + | *Fixed* | + | |
| Traffic coordination | + | + | | + | *Geo* | + | + |
| Traffic light scheduling | | | + | + | *Geo* | + | |
| Traffic monitoring | | + | | + | *Geo* | + | |
| Traveller information support | | | + | + | *Geo* | | |

### 5.2.1 Unicast Routing with Fixed Addressing

Targeted (i.e., unicast) multi-hop forwarding allows for *localized* communications between two vehicles. Example applications include voice/video transmission or instant messaging between vehicles traveling together for long distances [55]. For this combination of routing and addressing, two sorts of routing protocols can be distinguished, namely AODV-based and cluster-based protocols.

*Ad-hoc On Demand Distance Vector routing* (shortly *AODV*), being an example of a standard reactive routing protocol for ad-hoc networks [50], has been also investigated as a base routing protocol for vehicular networking [46]. AODV does not maintain any route that is not needed [51, 58]. Before a packet is sent, route discovery is initiated by the source node by broadcasting the `Route Request (RReq)` message towards the destination node. Upon receiving the `RReq` message by any transit node, its routing table is updated, and the `RReq` is rebroadcast. After `RReq` is received by the destination node, the `Route Response (RRep)` unicast message is sent back towards the source node along the reverse path. The path is finally set up after `RRep` is received by the source node. The route is used as long as it is active.

The respective changes to conventional AODV protocol are needed to adapt it to VANET networks due to lack of obvious boundaries of VANET systems topologies, e.g., as in [48] where `RReqs` are forwarded only in certain zones, or as in [62], where `RReqs` are broadcast up to the maximum number of hops.

End-to-end unicast communications can be also performed in a hierarchical way, e.g., using one of cluster-based routing protocols, where vehicles are organized into virtual clusters coordinated by cluster heads (see Fig. 5.3) [12]. Inter-cluster communications is done via cluster heads, while intra-cluster message dissemination is feasible via direct links.

### 5.2.2 Unicast Routing with Geographical Addressing

Concerning geographical addressing, a large number of proposals are based on Greedy Perimeter Stateless Routing (GPSR) protocol from [32], i.e., the location-based unicast routing protocol, assuming that VANET nodes maintain only information about neighboring vehicles related, e.g., to their location.

Under geographical addressing, two major methods of packet forwarding can be distinguished: *greedy forwarding* and *perimeter forwarding* [28]. The former one assumes that the packet is forwarded to the neighboring node located geographically closest to the destination node. If such a neighbor does not exist (e.g., due to the respective gap region with no nodes between the current node and the destination node), the latter (i.e., perimeter) forwarding can be used to forward the packet

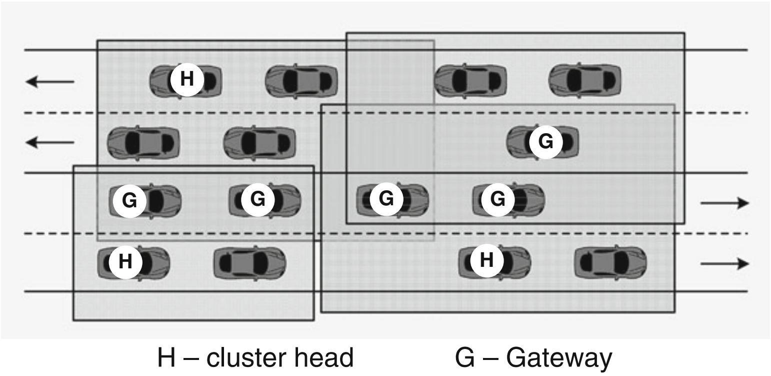


**Fig. 5.3** Example scenario of cluster-based routing

around the perimeter of this gap region to the counterclockwise neighbor with respect to the current node.

### 5.2.3 Multicast Routing with Geographical Addressing

Since geographical addressing is better suited for multicasting, such a combination (often referred to as *geocasting* [41]), is frequently in use for VANET communications with the objective to forward the message to vehicles located in a specified geographical region (commonly of a rectangular/circular shape). This forwarding is typically provided by means of flooding the packets [21] within a forwarding zone. For instance, information referring to road accidents or traffic lights (see Fig. 5.4) would typically affect only vehicles coming from behind [1, 9].

Summary of fundamental characteristics of VANET routing protocols is presented in Table 5.5.

### 5.2.4 Broadcast Multi-hop Message Dissemination

Multi-hop broadcasting [38] is a frequently used method of multi-hop dissemination of messages such as e.g., weather-, road condition-, or accident-related announcements, including, e.g., a detour route, an accident alert, or a construction warning [31]. It is also often used in the initial phase of unicast route discovery (for instance as in AODV routing). Finally, broadcasting is a good scheme if a message needs to be disseminated in a broadcast way to multiple nodes, but the transmission range exceeds a single-hop distance.

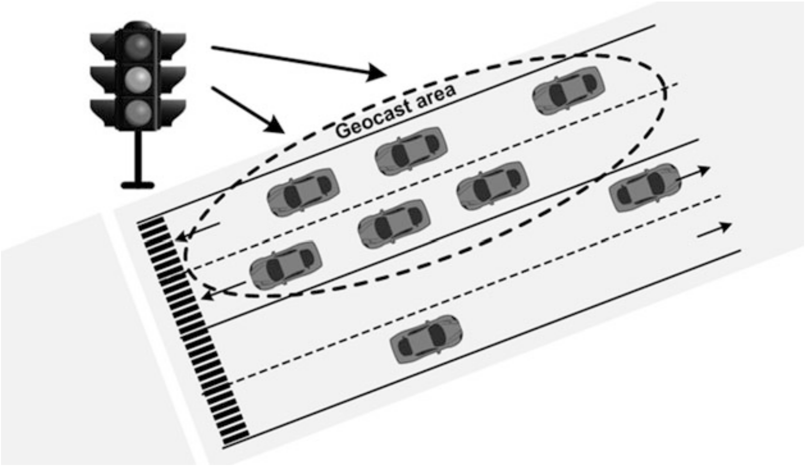


**Fig. 5.4** Example geocast area used in geographical routing (comprising vehicles based on their geographical location)

**Table 5.5** Characteristics of example VANET routing protocols

| Protocol | Addressing | Uni/multicast | Path state | Neighbor state | Hierarchical |
|---|---|---|---|---|---|
| AODV | Fixed | Unicast | Yes | Yes | No |
| Cluster | Fixed | Unicast | Yes | Yes | Yes |
| GPSR | Geographical | Unicast | No | Yes | No |
| Geocasting | Geographical | Multicast | No | No | No |

Since the main focus of this book is on reliability of routing schemes, in the later part of this chapter, we will focus on the reliability of multi-hop end-to-end V2V communications. In particular, we will address an important problem of VANET communications availability for end-to-end unicast routing, which to our knowledge has been only marginally considered in the literature. The problem is important due to existence of numerous applications making use of end-to-end unicast communications, including e.g., voice/video, instant messaging between vehicles traveling together, or multi-hop Internet access, just to mention a few.

In VANETs, end-to-end path availability is a challenging task due to frequent faults of VANET links [65]. Therefore, we will focus on providing high level of disruption tolerance by searching for "stable links" able to increase the lifetime of communication paths, and present two original algorithms of multipath and anypath communications in Sects. 5.3 and 5.4, accordingly.

## 5.3 Improving Resilience of End-to-End V2V Communications by Multipath Routing Focused on Establishing Stable Paths

In this section, we focus on resilience of multi-hop unicast V2V communications. In particular, we present our technique of multi-hop multipath end-to-end V2V routing enhanced with functionalities to select stable VANET links in path computations, and being able to provide differentiated levels of service availability to respond to differentiated requirements of applications, published in [53]. To the best of our knowledge, such a solution jointly taking into consideration the issues of: (1) communications paths stability, (2) multipath routing, and (3) provisioning of multiple levels of service availability for differentiated application classes has not been proposed before.

In the literature, there is currently no consensus concerning the inter-vehicle distance distribution having a direct influence on lifetime of VANET links, as well as on end-to-end communication paths. For instance, in [56], the respective analysis of link lifetime was presented for a co-directional vehicles scenario (i.e., for vehicles moving in the same direction) under the assumption of equal spaces between vehicles, as well as normally distributed velocities. For such a scenario, the log-normal distribution was shown in [13] to be proper for modeling the headway distance, and next utilized in [64] to present an improved analysis of link lifetime including differentiated velocities and accelerations of co-directional vehicles.

However, such a simplified case of co-directional vehicles, even though quite realistic for a highway scenario, seems to be of less importance, e.g., in urban environment for which differentiated directions of vehicle movements play the major role. Besides, as shown in other papers, inter-vehicle distances can be modeled by gamma [64], exponential [23, 67], or Poisson distribution [30] as well.

In order to mitigate the problem of short lifetime of V2V multi-hop paths, several approaches to multi-hop routing have been proposed in the literature aimed at improving path characteristics related to the stability of traversed links. Among them, we can distinguish single-path algorithms (e.g., [45]) utilizing mobility-related information (direction and velocity of vehicles) to find transmission paths traversing links with low probability of being broken in the nearest future. However, following [7], even if link stability criterion is incorporated into the path computation scheme, owing to a high level of nodes mobility, the lifetime of a multi-hop path is commonly shorter than the time needed to install the path.

Another solution to improve reliability of end-to-end transmission is to utilize the multipath routing able to transmit information via multiple (frequently disjoint) paths. Additionally, multipath routing is also characterized by improved network throughput, load balancing, and packet delivery ratio [25].

Among end-to-end multipath routing algorithms available in the literature, two extensions of AODV routing scheme are worth distinguishing, namely Ad hoc On-demand Multipath Distance Vector – AOMDV introduced in [43], and Ad hoc

On-demand Distance Vector Multipath – AODVM from [66] establishing multiple link-(node-) disjoint paths, accordingly. However, multipath concept itself may be not sufficient since high mobility of vehicles is often responsible for failures of all alternate paths between a certain pair of end nodes in a short time [63].

Despite clear advantages of both approaches, i.e., link stability-oriented path selection and multipath routing, there is practically no approach available combining both features, apart from our one from [53] presented in this section as follows. Section 5.3.1 includes: (1) analysis of probability of end-to-end transmission availability for multi-hop multipath V2V communications in the presence of link failures under the assumption on exponential distribution of inter-vehicle distances, and (2) numerical results necessary to determine the number of end-to-end disjoint paths sufficient to visibly improve the multipath transmission availability.

These results are next utilized in Sect. 5.3.2 to propose the concept of multipath link-disjoint end-to-end routing aimed at establishing paths characterized by increased lifetime. This approach is also designed to provide differentiated service availability levels to respond to differentiated requirements of applications.

Simulation results and final conclusions are presented in Sect. 5.3.3.

### *5.3.1 Probability of V2V Transmission Availability*

A V2V network model considered in this section is focused on analyzing the inter-vehicle connectivity. Therefore, it disregards other issue like transmission errors, delay, or contention. Since link faults are responsible for the majority of VANET failures, here we focus on protection against link faults. Any two vehicles $i$ and $j$ are said to be connected by a direct link $a_h = (i, j)$, if distance $r_{i,j}$ between them is not greater than the maximum range $r_{\max}$ [20]. Therefore, probability $\rho_h$ that two vehicles are connected by link $a_h$ at any time $t$ can be calculated based on a probability density function of inter-vehicle distance $p(r_{i,j})$, as given in Eq. 5.1.

$$\rho_h = P\left(r_{i,j} < r_{\max}\right) = \int\limits_0^{r_{\max}} p(s)ds \tag{5.1}$$

In the case of a single path routing (Fig. 5.5a), if path $\eta$ consists of $k_n$ links, then assuming mutual independence of link lengths (as being commonly investigated [44, 67]), probability $\widetilde{\pi}_n$ of path existence can be expressed by Eq. 5.2.

$$\widetilde{\pi}_n = \prod_{h:\ a_h \in \eta} \rho_h = \left( \int\limits_0^{r_{\max}} p(s)ds \right)^{k_n} \tag{5.2}$$

In a multipath transmission scenario including $m$ end-to-end link-disjoint paths (see Fig. 5.5b), destination node can be reached, if at least one of all $m$ end-to-end

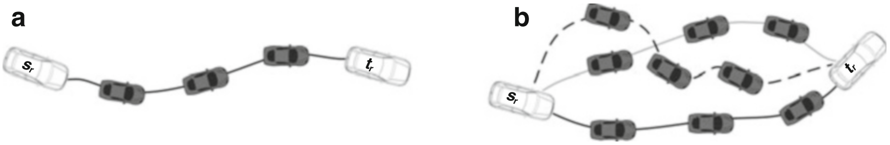


**Fig. 5.5** Examples of (**a**) single-path, and (**b**) multipath link-disjoint routing

link-disjoint paths is operational. In such a scheme, probability of multipath transmission availability $\widetilde{\Psi}_m$ can be determined for any time $t$, as given in Eq. 5.3.

$$\widetilde{\Psi}_m = 1 - \prod_{n=1}^{m} (1 - \widetilde{\pi}_n) = 1 - \prod_{n=1}^{m} \left(1 - \left(\int_0^{r_{\max}} p(s)ds\right)^{k_n}\right) \tag{5.3}$$

Assuming the exponential distribution of inter-vehicle distances (following e.g., [23, 67]), probabilities of link existence ($\rho_h$), and multipath transmission availability ($\widetilde{\Psi}_m$) at any time $t$ are given by Eqs. 5.4 and 5.5, accordingly.

$$\rho_h = \int_0^{r_{\max}} \lambda e^{-\lambda s} ds = 1 - e^{-\lambda \cdot r_{\max}} \tag{5.4}$$

$$\widetilde{\Psi}_m = 1 - \prod_{n=1}^{m} \left(1 - \left(1 - e^{-\lambda \cdot r_{\max}}\right)^{k_n}\right) \tag{5.5}$$

Example values of $\widetilde{\Psi}_m$ as a function of end-to-end path count $m$, assuming that $r_{\max} = 300$ m and $\lambda = 0.01$, are presented in Table 5.6. These results show that multipath routing can provide a suitable means to improve the probability of transmission availability. However, increasing $m$ above 2–3 does not provide any significant improvement. In path computations, it is thus reasonable to limit the number of end-to-end disjoint paths to the value sufficient to meet the requirements of particular applications.

To analyze the time-dependent probability of multi-hop path availability, for any time $t_0$, we need to derive first the formula determining existence of a single link $a_h$ after $\Delta t$ time. We assume that for each vehicle $i$, $\boldsymbol{\Phi_i}(t_0) = [x_i(t_0),\ y_i(t_0)]^{\mathrm{T}}$ is its position vector at initial time $t_0$. The initial distance between vehicles $i$ and $j$ (see Fig. 5.6) can be defined by Eq. 5.6.

$$r_{i,j}(t_0) = \left|\boldsymbol{\Phi}_i(t_0) - \boldsymbol{\Phi}_j(t_0)\right| = \sqrt{\left(x_i(t_0) - x_j(t_0)\right)^2 + \left(y_i(t_0) - y_j(t_0)\right)^2} \tag{5.6}$$

**Table 5.6** Example values of $\widetilde{\Psi}_m$ as a function of end-to-end link-disjoint path count $m$ for exponential inter-vehicle distance distribution

| | $m=1$ path | $m=2$ paths | $m=3$ paths | $m=4$ paths | $m=5$ paths |
|---|---|---|---|---|---|
| $\widetilde{\Psi}_m{}^*$ | 0.8257 | 0.9622 | 0.9905 | 0.9973 | 0.9991 |

* for average hop counts of 1st–5th path equal to 3.75, 4.79, 5.69, 6.63, and 7.61, accordingly

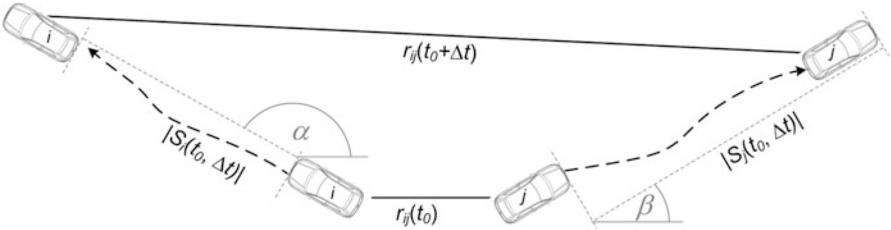


**Fig. 5.6** Example scenario of vehicle movements

After $\Delta t$ time units, information on vehicle $i$ displacement can be represented by the movement vector $\boldsymbol{S_i}(t_0, \Delta t) = [s_i^x(t_0,\Delta t), s_i^y(t_0,\Delta t)]^T$ with consecutive elements referring to movement information along X and Y axis, accordingly, depending on vehicle $i$ velocity function $\boldsymbol{v_i}(t) = [v_i^x(t), v_i^y(t)]^T$ in $(t_0, t_0 + \Delta t)$ interval. For each vehicle $i$, $S_i$ thus also includes information on direction. At time $t_0 + \Delta t$, a new position vector $\boldsymbol{\Phi_i}(t_0 + \Delta t)$ of vehicle $i$ is given by Eq. 5.7.

$$\Phi_i(t_0+\Delta t) = \Phi_i(t_0) + S_i(t_0,\Delta t) = \begin{bmatrix} x_i(t_0) \\ y_i(t_0) \end{bmatrix} + \begin{bmatrix} s_i^x(t_0,\Delta t) \\ s_i^y(t_0,\Delta t) \end{bmatrix}$$

$$= \begin{bmatrix} x_i(t_0) \\ y_i(t_0) \end{bmatrix} + \begin{bmatrix} \int\limits_{t_0}^{t_0+\Delta t} v_i^x(s)ds \\ \int\limits_{t_0}^{t_0+\Delta t} v_i^y(s)ds \end{bmatrix} \tag{5.7}$$

Vehicles $i$ and $j$ thus remain connected at $t_0 + \Delta t$, if:

$$r_{i,j}(t_0+\Delta t) = \left|\Phi_i(t_0+\Delta t) - \Phi_j(t_0+\Delta t)\right| \le r_{\max} \tag{5.8}$$

Left part of formula (5.8) can be extended based on Eqs. 5.6 and 5.7, as in Eq. 5.9.

$$r_{i,j}(t_0+\Delta t)=\sqrt{\left(x_i(t_0+\Delta t)-x_j(t_0+\Delta t)\right)^2+\left(y_i(t_0+\Delta t)-y_j(t_0+\Delta t)\right)^2}$$
$$=\sqrt{\begin{array}{l}\left(x_i(t_0)+\int\limits_{t_0}^{t_0+\Delta t}v_i^x(s)ds-\left(x_j(t_0)+\int\limits_{t_0}^{t_0+\Delta t}v_j^x(s)ds\right)\right)^2\\+\left(y_i(t_0)+\int\limits_{t_0}^{t_0+\Delta t}v_i^y(s)ds-\left(y_j(t_0)+\int\limits_{t_0}^{t_0+\Delta t}v_j^y(s)ds\right)\right)^2\end{array}} \tag{5.9}$$

The respective probabilities of single link existence ($\rho_h$), single-path ($\widetilde{\pi}_n$), and multipath ($\widetilde{\Psi}_m$) transmission availability can be defined by Eqs. 5.10–5.12.

$$\rho_h(t_0+\Delta t)=P\left(r_{i,j}(t_0+\Delta t)<r_{\max}\right) \tag{5.10}$$

$$\widetilde{\pi}_n(t_0+\Delta t)=\prod_{h:\,a_h\in\eta}\rho_h(t_0+\Delta t)=\left(P\left(r_{i,j}(t_0+\Delta t)<r_{\max}\right)\right)^{k_n} \tag{5.11}$$

$$\begin{aligned}\widetilde{\Psi}_m(t_0+\Delta t)&=1-\prod_{n=1}^{m}\left(1-\widetilde{\pi}_n(t_0+\Delta t)\right)\\&=1-\prod_{n=1}^{m}\left(1-\left(P\left(r_{i,j}(t_0+\Delta t)<r_{\max}\right)\right)^{k_n}\right)\end{aligned} \tag{5.12}$$

Further analysis of $\widetilde{\Psi}_m(t_0+\Delta t)$ requires information related to specific traffic pattern, as well as its impact on $\rho_h(t_0+\Delta t)$ values. Since our main interest is to improve multi-hop transmission availability in the presence of link failures, the above formulas will be helpful to introduce a routing technique that establishes paths traversing "stable links", i.e., links with high probability of existence after $\Delta t$ time.

### *5.3.2 Provisioning of Multiple Availability Classes*

VANET applications, like any others designed for various network architectures, are characterized by differentiated requirements related with *service availability* (i.e., probability of being in an "up" state [14]). In order not to overprovision a remarkable set of low-priority applications by offering only a single class of service, there is a reasonable need to propose an elastic approach able to meet these differentiated characteristics. Otherwise, most applications would be offered better level of service than necessary at the price of the increased network load. Therefore, in this section, we introduce the respective class-based approach and define three availability classes shown in Table 5.7.

**Table 5.7** Proposed classes of path availability

| Class | Example applications |
|---|---|
| Bronze | Delay-tolerant services (e.g., Internet access; infotainment) |
| Silver | E.g., traffic coordination |
| Gold | Real-time services (e.g., emergency warnings) |

In the literature, there are also other approaches related to service differentiation. However, in the case of VANETs, they refer, e.g., to differentiation of transmission opportunity time (like EDCA approach from [10, 26]). However, unlike in EDCA, the objective of our approach is to provide differentiation in terms of levels of protection against link failures

Differentiated guarantees on path availability are achieved here by the routing scheme establishing multiple end-to-end link-disjoint paths as follows:

– *bronze class* a single multi-hop path,
– *silver class* $m = 2$ link-disjoint multi-hop paths,
– *gold class* $m = 3$ link-disjoint multi-hop paths.

Based on topological constraints of VANETs often limiting the number of disjoint end-to-end paths nearly equal to the average node's degree [15], the maximum number of link-disjoint paths is assumed here to be equal to 3 (which also complies with the results from Table 5.6 showing only marginal increase of probability of transmission availability for the number of disjoint paths $m$ over 3).

### Proposed Metric of Link Costs

In order to establish multi-hop paths with low probability of being broken in a short time, we need to introduce a metric of link costs aimed at selecting links with estimated long lifetime. This can be obtained, e.g., by selecting links between neighboring vehicles having similar velocity vectors. In the ideal case, if for any $t$ in the $(t_0, t_0 + \Delta t)$ interval, conditions: $|v_i(t)| = |v_j(t)|$, and $\alpha = \beta$ are satisfied (see Fig. 5.6), then inter-vehicle distance will be unchanged after $\Delta t$ units of time.

Figure 5.7 presents example changes of inter-vehicle distance $r_{i,j}$ as a function of $\Delta t$ analyzed for various relations of angles $\alpha$ and $\beta$ from Fig. 5.6, for two scenarios of constant linear velocities of vehicles $i$ and $j$ and the initial inter-vehicle distance at $t_0$ equal to 100 m.

Figure 5.7 thus shows that in order to increase the lifetime of any VANET multi-hop path, it is important to select links between neighboring vehicles characterized by similar movement vectors. However, at any time $t_0$, precise information related to movement vectors is for obvious reasons available only with respect to the past $(t_0 - \Delta t, t_0)$ interval. Therefore, in our approach we propose to estimate the future inter-vehicle distance at time $t_0 + \Delta t$ based on the respective information on vehicles movement from the past $(t_0 - \Delta t, t_0)$ interval.

In particular, we propose to use formula (5.13) to evaluate the cost $\xi_h$ of any link $a_h$ using information on neighboring vehicles movement in interval $(t_0 - \Delta t, t_0)$. According to (5.13), the minimum cost $(\xi_h = \varepsilon)$ is assigned to links between

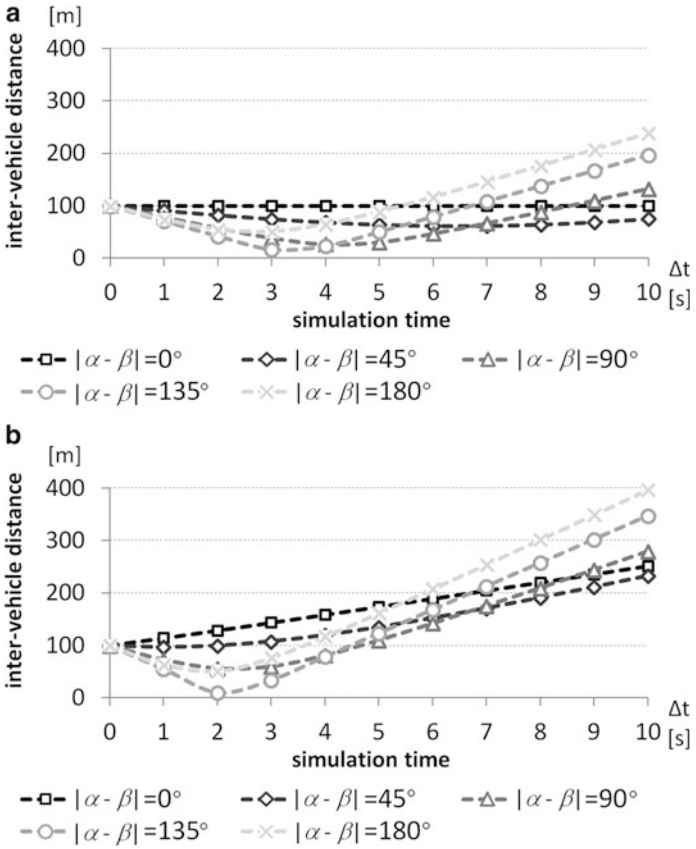


**Fig. 5.7** Examples of inter-vehicle distance $r_{i,j}$ as a function of $\Delta t$ for various values of $|\alpha$-$\beta|$ difference from Fig. 5.6, and constant linear velocity values (**a**): $|v_i| = |v_j| = 16$ m/s, and (**b**): $|v_i| = 16$ m/s, $|v_j| = 32$ m/s

neighboring vehicles $i$ and $j$ characterized by equal movement vectors in $(t_0 - \Delta t,\ t_0)$ interval. Contrary to existing approaches (e.g., [13, 56, 64]), links with estimated long lifetime are thus preferred in our scheme.

$$\xi_h = \sqrt{\left(s_i^x(t_0 - \Delta t, t_0) - s_j^x(t_0 - \Delta t, t_0)\right)^2 + \left(s_i^y(t_0 - \Delta t, t_0) - s_j^y(t_0 - \Delta t, t_0)\right)^2} \tag{5.13}$$

## Remarks on Routing Algorithm Extensions

Proposed approach can be applied to any V2V routing algorithm. Due to popularity of AODV routing, as well as availability of its multipath link-disjoint AOMDV version in the literature, here we evaluate our method by introducing the Class-Based Multipath link-disjoint V2V routing scheme based on AODV algorithm (CBM-AODV), as given in Fig. 5.8. AOMDV is also used in Sect. 5.3 as a reference approach in all performance comparisons.

To implement our solution, several updates to conventional AODV routing algorithm are necessary. In order to obtain *m* end-to-end link-disjoint paths, source node $s_r$ has to send towards destination node $t_r$ multiple (i.e., *m*) `Route Request` messages – `RReqs` (see Steps 1–2 from Fig. 5.8). `RReqs` are followed by receiving *m* `Route Reply` messages (`RReps`), characterized by *m* lowest total path costs (compared to sending one `RRep` message only in the original AODV scheme)[1] – Step 3 from Fig. 5.8. To make it feasible, information on the number of required `RReps` should be included in the `RReq` message.

Another important modification refers to the desired link disjointedness of multiple end-to-end paths, which can be provided by structures shown in Fig. 5.9 to be stored at each transit node *i*. This is to assure that the next copy of the `RReq`

```
INPUT
  – set $V$ of vehicles; $A$ – set of links $a_h$=$(i, j)$ between neighboring vehicles $i$ and $j$
  – set $D$ of transmission demands, each demand $r$ represented by the end nodes $s_r$ and $t_r$, and class
    of a demand
OUTPUT  a set of $m$ end-to-end link-disjoint paths
For each demand:
Step 1  Determine the number $m$ of necessary end-to-end link-disjoint paths.
Step 2  Send $m$ copies of RREQ broadcast message from source node $s_r$ towards destination node $t_r$.
   In order to provide link disjointedness of established end-to-end paths, when forwarding the
   RREQ messages by each transit node $i$ received from a given preceeding node $j$:
    2.1  Update the current cost of a path from $s_r$ to $i$ based on the cost of link $(j, i)$ using Eq. 5.13.
    2.2  Forward the RREQ message towards $t_r$, if the incoming RREQ message has not been sent
         by preceeding node $j$ to node $i$ before (to be determined based on structures from Fig. 5.9).
Step 3  Upon receiving RREQ messages by the destination node $t_r$, send the respective RREP
        messages towards the source node $s_r$ with respect to $m$ RREQ messages having the lowest
        total path cost according to formula (5.13).
```

**Fig. 5.8** CBM-AODV procedure to establish end-to-end link-disjoint paths

| application ID | source node $s_r$ | destination node $t_r$ | preceding node $j$ |
|---|---|---|---|

**Fig. 5.9** Structures used in CBM-AODV to establish link-disjoint paths

[1] In our multipath algorithm, the number of exchanged control messages is the same as for the reference AOMDV technique.

message originally sent from source node $s_r$ towards destination node $t_r$ via a given preceding node $j$ is not sent by node $i$ towards $t_r$ again, as long as the respective paths remain operational (Steps 2.1–2.2).

In a typical scenario of broadcasting the `RReq` messages followed by sending back the `RRep` messages, established paths are commonly the cheapest ones in terms of the message propagation delay (which does not guarantee establishing paths that traverse links with estimated long duration time, referred to as "stable links" in this section). This problem is overcome in our scheme by implementing the cost metric from formula (5.13) by extending the `RReq` message broadcasted by vehicle $j$ to include additional fields for storing the values $s^x{}_j(t_0 - \Delta t,\ t_0)$ and $s^y{}_j(t_0 - \Delta t,\ t_0)$, and the total path cost.

In order to increase the level of service availability, the procedure of finding a new path is launched immediately after detecting the failure of any path (i.e., not waiting for detection of failures of all $m$ alternate paths).

For each demand, the proposed scheme is characterized by the polynomial complexity bounded in above by O(|$N$|), where |$N$| is the number of network nodes, since its main determinant is related with the task to establish a single end-to-end path by broadcasting the `RRep` messages (of O(|$N$|) complexity).

### 5.3.3 Analysis of Modeling Results and Conclusions

Evaluation of characteristics of our approach was performed by means of simulations for the realistic scenario of a 53-node VANET network from Fig. 5.10. The

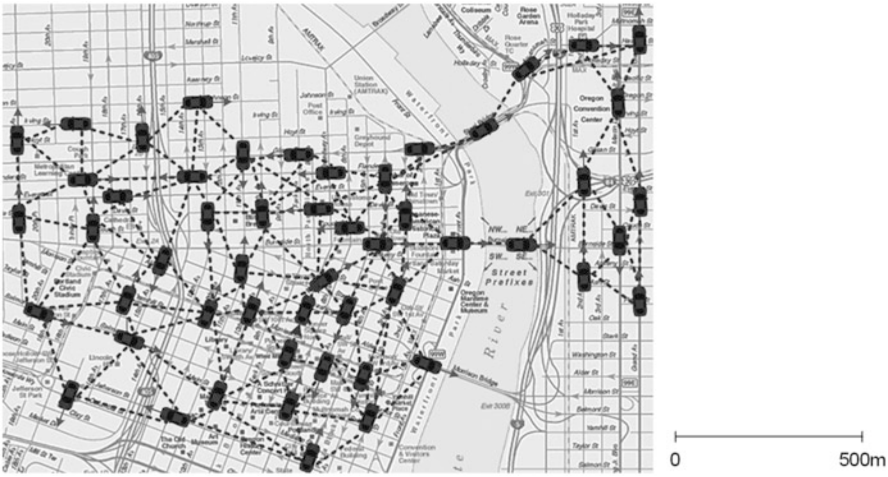


**Fig. 5.10** Example VANET network (Portland area, US) used in simulations

aim of simulations was to evaluate the average values of path length, hop count, and the forecasted path lifetime. As proposed in the former subsection, movement vector $S_i$ of any vehicle $i$ in interval $(t_0, t_0 + \Delta t)$ was estimated based on the respective information from the past interval $(t_0 - \Delta t, t_0)$, with $\Delta t = 1$ s. Following [30], since message transmission delay can be considered negligible, network topology (i.e., locations of vehicles, and their velocities) was assumed to be "frozen" in all path computations (i.e., it did not change).

Experiments included two scenarios. In Scenario A, all vehicles were assumed to have equal average linear velocity (i.e., 10 m/s) in time interval $(t_0 - \Delta t, t_0)$. Scenario B was in turn designed to simulate uniform distribution of the average linear velocity in range 0–16 m/s (complying with common speed limitations in urban areas). In each scenario, the set of transmission demands comprised all pairs of vehicles equally divided into three proposed classes (i.e., bronze, silver and gold) (Table 5.7).

Characteristics of the proposed approach were compared with the respective reference ones of AOMDV link-disjoint multipath routing algorithm from [43] using common transmission delay metric. Evaluation results are presented in Tables 5.8 and 5.9 for 1st, 2nd, and 3rd link-disjoint path (denoted as P1, P2, and P3, accordingly). The respective lengths of 95 % confidence intervals of the average values of analyzed parameters are not presented due to negligibly small sizes.

In general, the average length of paths calculated by the proposed CBM-AODV algorithm was about 17 % greater in relation with characteristics of the reference approach. However, this implied an increase of the end-to-end transmission delay only by about 1 ms for the analyzed network from Fig. 5.10, which was almost negligible.

The average cost of established paths calculated based on Eq. 5.13 for our CBM-AODV approach was up to 33 % lower (Scenario A). For Scenario B with differentiated linear velocities of vehicles, this difference was insignificantly lower. These results show that our approach is able to establish end-to-end paths with remarkably improved lifetime. A detailed analysis of path lifetime presented in the right part of Tables 5.8 and 5.9 also indicated up to 45 % (22.64 % on average) better results for CBM-AODV approach, compared to the reference scheme.

For each analyzed algorithm, path lifetime decreased with the increase of the number of path links, since it was determined by the minimum value of individual lifetime of path links. It is worth noting that in each scenario the maximum time needed to establish the alternate path after a link failure was at most 15 ms, which in turn allowed any vehicle to change its location by at most 0.48 m (if we consider the maximum velocity of 32 m/s, e.g., as commonly assumed for highways).

Therefore, especially for the introduced silver and gold availability classes, it is hardly probable that the remaining working paths will fail while re-establishing one of the failed paths. This in turn confirms efficiency of our solution in assuring the transmission continuity in the presence of VANET link failures.

**Table 5.8** Path characteristics for Scenario A

| Service class | Algorithm | Hop count | | | Path cost | | | Path lifetime [s] | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | P1 | P2 | P3 | P1 | P2 | P3 | P1 | P2 | P3 |
| Bronze | CBM-AODV | **4.97** | – | – | **12.73** | – | – | **84.78** | – | – |
| | Reference approach | 4.20 | – | – | 18.85 | – | – | 70.12 | – | – |
| Silver | CBM-AODV | **4.87** | **6.50** | – | **12.29** | **21.25** | – | **86.40** | **57.52** | – |
| | Reference approach | 4.29 | 5.54 | – | 16.62 | 28.01 | – | 77.77 | 39.44 | – |
| Gold | CBM-AODV | **3.82** | **4.40** | **5.54** | **10.00** | **15.55** | **23.06** | **107.36** | **76.40** | **38.93** |
| | Reference approach | 3.40 | 3.86 | 4.74 | 13.08 | 19.08 | 28.32 | 99.88 | 66.24 | 31.92 |

**Table 5.9** Path characteristics for Scenario B

| Service class | Algorithm | Hop count | | | Path cost | | | Path lifetime [s] | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | P1 | P2 | P3 | P1 | P2 | P3 | P1 | P2 | P3 |
| Bronze | CBM-AODV | **5.04** | – | – | **26.77** | – | – | **28.58** | – | – |
| | Reference approach | 4.20 | – | – | 35.65 | – | – | 22.21 | – | – |
| Silver | CBM-AODV | **5.04** | **6.59** | – | **26.76** | **45.10** | – | **28.58** | **21.20** | – |
| | Reference approach | 4.37 | 5.46 | – | 31.47 | 55.15 | – | 24.79 | 15.20 | – |
| Gold | CBM-AODV | **3.73** | **4.79** | **5.75** | **19.82** | **28.82** | **42.88** | **35.06** | **26.59** | **18.34** |
| | Reference approach | 3.29 | 4.01 | 4.71 | 23.35 | 35.92 | 51.55 | 31.10 | 21.02 | 14.51 |

## 5.4 A New Approach to Anypath Forwarding Providing Long Path Lifetime

In this section, we focus on anypath forwarding being another means to improve reliability of multi-hop communications. The general difference between end-to-end multipath and anypath forwarding is that in the former scheme (considered in Sect. 5.3) a packet is sent in parallel along multiple paths (see Fig. 5.11a), while in the latter (i.e., anypath) forwarding, at each stage it is received as a broadcast message by several neighboring nodes, but is later forwarded by only one of them (Fig. 5.11b).

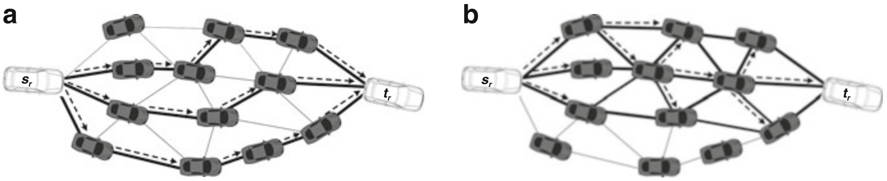


**Fig. 5.11** Difference between (**a**) multipath and (**b**) anypath forwarding

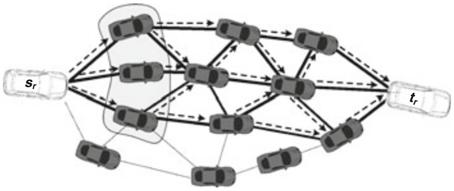


**Fig. 5.12** Example anypath between vehicles $s_r$ and $t_r$ marked with bold arrows. The respective forwarding set (shown for source node $s_r$ towards node $t_r$) is marked with a gray area

In anypath scheme, also called (*opportunistic*) *routing* [16], the set of neighboring nodes, a packet is sent to, is called the *forwarding set* – Fig. 5.12. This set is selected in advance in the route planning phase for each transit node forwarding the packets towards a given destination node [35].

Under anypath forwarding, nodes from the forwarding set act in a cooperative manner to forward the packet towards the destination node.[2] However, based on relay priorities assigned to neighboring nodes by a reliable anycast scheme [35], only one of these neighboring nodes will next forward the packet towards the destination. This feature is to avoid unnecessary duplicate forwarding at each transit node.

A general rule is to assign higher priorities to relaying nodes characterized by lower costs of paths towards the destination node. A packet will be forwarded by a certain lower-priority node, only if it is not forwarded by all the respective higher-priority neighboring nodes (e.g., because they fail to receive the packet), determined by lack of MAC acknowledgement (i.e., ACK message) sent in a given timeslot by a higher-priority node upon receiving the packet [68]. The packet is lost, only in case none of nodes belonging to the forwarding set receive it [35].

In general, following [16], the cost of an anypath towards the destination node decreases with the increase of a number of forwarding relays. However, this may

[2] It is important to note that different forwarding sets are generally used for different destination nodes.

also imply increased transmission delay (too many nodes in the forwarding set may result in longer paths, or even create loops). Therefore, the size of any forwarding set should be a trade-off between these two characteristics. Since under anypath communications, for each transit node, probability of forwarding a packet successfully to at least one neighboring node is greater than the probability of delivering it to a specified forwarding node only [16, 68],[3] reliability of anypath communications is obviously greater than of the unicast scheme.

However, each packet may traverse a multitude of possible paths (forming the anypath) to reach the destination, since the rule for selecting the next hop is non-deterministic (Fig. 5.12). Therefore, possible disadvantage of this opportunistic forwarding scheme can be route flapping due to choosing a particular route on a per packet basis by the respective link- and network-layer protocol mechanisms.

In VANETs, anypath flapping can be additionally increased by frequent failures of inter-vehicle links. Therefore, in this section, we focus on link stability issue as an important factor to prevent from route flapping in anypath communications. This problem is of a significant importance especially for a number of real-time safety services having stringent QoS requirements (e.g., safe-driving assistance including real-time video transmission, or emergency warnings [60]).

The concept of anypath communications in VANETs is rather new, and the number of relevant proposals (e.g., [11, 29, 34, 37]) is limited. In particular, apart from our proposal from [52] presented in detail in the latter part of this section, there is practically no other approach available focusing on reliability of anypath communications, and, in particular, aimed at improving stability of established anypaths.

In particular, Sect. 5.4.1 is to present: (1) definition of a scheme of long-lifetime anypath (LLA) routing that utilizes a new metric of link costs based on the introduced link stability index, and (2) details of LLA solution deployment. Evaluation of algorithm characteristics is in turn presented in Sect. 5.4.2.

### *5.4.1 Long-Lifetime Anypath (LLA) Concept*

When modeling point-to-multipoint links characteristic to anypath forwarding (see Fig. 5.13), the network is commonly represented by a hypergraph $\Gamma = (V, A)$, where $V$ denotes the set of network vehicles, and $A$ represents the set of hyperlinks, each hyperlink defined by an ordered pair $(i, J)$ used to describe a given vehicle $i$ connected with the forwarding set $J$ of neighboring vehicles.[4]

[3] Other benefits of anypath scheme utilization include: reduced cost of retransmissions, improved throughput, and better energy efficiency.

[4] Under anypath routing, for each forwarding set $J$, indices $\{1, 2, \ldots, n\}$ are assigned to nodes ascending the remaining path costs $\sigma_j$ to destination node $t_r$ (i.e., $\sigma_1 \leq \sigma_2 \leq \ldots \leq \sigma_\mathrm{n}$).

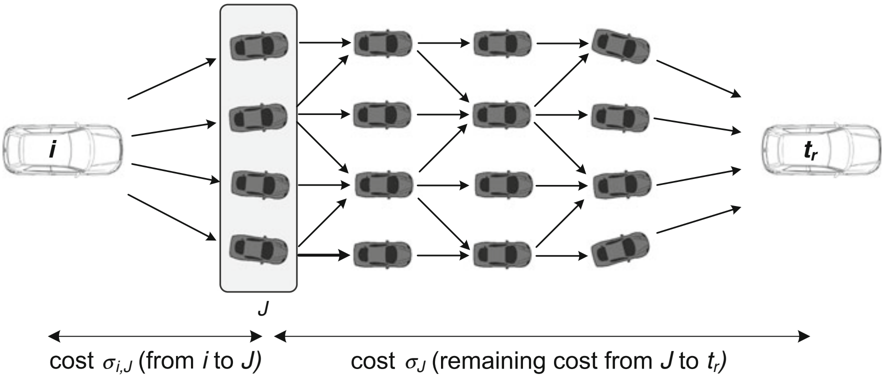

i
J
$t_r$
cost $\sigma_{i,J}$ (from i to J)
cost $\sigma_J$ (remaining cost from J to $t_r$)

**Fig. 5.13** Calculation of anypath total cost based on division into two costs

The anypath cost between vehicles $i$ and $t_r$ can be defined by the Bellman equation given by formula (5.14), i.e., formed by the cost $\sigma_{i,J}$ of a hyperlink $(i, J)$ from vehicle $i$ to $J$ and the remaining anypath cost $\sigma_J$ from $J$ to vehicle $t_r$ [34].

$$\sigma_{i,t} = \sigma_{i,J} + \sigma_J \tag{5.14}$$

Following [16, 35], the hyperlink cost $\sigma_{i,J}$ can be in turn defined as:

$$\sigma_{i,J} = \frac{1}{p_{i,J}} \underset{\left(\substack{\text{in case of}\\ \text{independent}\\ \text{packet losses}}\right)}{\equiv} \frac{1}{1 - \prod_{j \in J} \left(1 - p_{i,j}\right)} \tag{5.15}$$

where $p_{i,J}$ denotes probability of delivering the packet from node $i$ to at least one node from $J$ calculated based on individual probabilities of packet delivery $p_{i,j}$ obtained from Layer 2.

Another important meaning of $\sigma_{i,J}$ is that it represents the expected number of anypath transmissions required to successfully deliver the packet sent by node $i$ to any node from $J$ (see e.g., definition of EATX metric from [16]).

The remaining cost $\sigma_J$ of an anypath from $J$ to $t_r$ can be defined as the weighted average of costs of all paths from $J$ to $t_r$ as given in Eq. 5.16.

$$\sigma_J = \sum_{j \in J} w_{i,j} \sigma_j \tag{5.16}$$

where weight $w_{i,j}$ reflects the probability of node $j$ being the forwarding node of a packet received from vehicle $i$, while $\sigma_j$ represents the cost of a path between vehicle $j$ from $J$ and destination vehicle $t_r$ [16]. Under the common simplified assumption of independent packet losses, $w_{i,j}$ values can be defined based on probabilities $p_{i,j}$ as given in Eq. 5.17.

$$w_{i,j} = \frac{p_{i,j}\prod\limits_{k=1}^{j-1}\left(1 - p_{i,k}\right)}{1 - \prod\limits_{j\in J}\left(1 - p_{i,j}\right)}; \qquad \sum_{i} w_{i,j} = 1 \tag{5.17}$$

Mobility characteristics of vehicles play a crucial role for determining $p_{i,j}$ values. Therefore, for any time $t_0$, future values of $p_{i,j}$ depend on time-varying movement information of vehicles. For any time $t_0$, any two connected vehicles $i$ and $j$ remain connected after $\Delta t$ time units, if distance $r_{i,j}$ between them at $t_0 + \Delta t$ remains in communications range $<0, r_{\max}>$, i.e.,

$$r_{i,j}(t_0 + \Delta t) = \left|\Phi_i(t_0 + \Delta t) - \Phi_j(t_0 + \Delta t)\right| \le r_{\max} \tag{5.18}$$

where $\Phi_i(t_0 + \Delta t)$ is a position vector of vehicle $i$ at $t_0 + \Delta t$ defined by Eq. 5.19.

$$\Phi_i(t_0 + \Delta t) = \Phi_i(t_0) + S_i(t_0, \Delta t) = \begin{bmatrix} x_i(t_0) \\ y_i(t_0) \end{bmatrix} + \begin{bmatrix} s_i^x(t_0, \Delta t) \\ s_i^y(t_0, \Delta t) \end{bmatrix} \tag{5.19}$$

$S_i(t_0, \Delta t) = [s_i^x(t_0,\Delta t), s_i^y(t_0,\Delta t)]^{\mathrm{T}}$ – movement vector of vehicle $i$.

Therefore, in order to reduce the effect of route-flapping in anypath communications for consecutive packets, similar to Sect. 5.3, "stable links" (i.e., links between vehicles moving in similar directions with similar speeds) need to be identified and selected by the anypath calculation algorithm. We define the *stability index* $s_{i,j}$ of link $(i, j)$ at any time $t_0$ as a value in range $<0; 1>$, as given in Eq. 5.20, i.e., as the normalized increase of distance between vehicles $i$ and $j$ in the past $(t_0 - \Delta t, t_0)$ interval.

$$s_{i,j} = 1 - \frac{\min\left(\sqrt{\begin{array}{l}\left(s_i^x(t_0 - \Delta t, t_0) - s_j^x(t_0 - \Delta t, t_0)\right)^2 \\ +\left(s_i^y(t_0 - \Delta t, t_0) - s_j^y(t_0 - \Delta t, t_0)\right)^2\end{array}}; r_{\text{upper}}\right)}{r_{\text{upper}}} \tag{5.20}$$

According to Eq. 5.20, the best value of stability index $(s_{i,j} = 1)$ is assigned to links between nodes $i$ and $j$ characterized by equal movement vectors in the past $(t_0 - \Delta t,\ t_0)$ interval (i.e., implying no change in inter-vehicle distance). The worst value of $s_{i,j} = 0$ is assigned to links that changed their length by more than the maximum assumed value $r_{\text{upper}}$ in $\Delta t$ time (based on maximum allowed speed).

Probability of packet delivery at link destination nodes $j$ in the near future (i.e., in $(t_0,\ t_0 + \Delta t)$ interval) is much influenced by link stability indices, since probability $p_{i,j}$ of packet delivery between a pair of neighboring vehicles $i$ and $j$ is negatively correlated with link lengths [60]. Therefore, to limit the possibility of anypath route flapping, in this section we propose to determine the cost of a link between any pair of neighboring vehicles $i$ and $j$ as given in Eq. 5.21, i.e., to include the value of stability index $s_{i,j}$.[5]

$$\xi_{i,j} = \frac{1}{p_{i,j} \cdot s_{i,j}} \tag{5.21}$$

Based on Eq. 5.21, the lowest cost $\xi_{i,j}$ (with a lower bound equal to 1.0) is assigned to links characterized by high values of stability index $s_{i,j}$ (i.e., links with estimated long lifetime), as well as high values of packet delivery ratio $p_{i,j}$ (specific for short links). Analogously, the respective costs $\sigma_{i,J}$ and weights $w_{i,j}$ are defined in our scheme as given in Eqs. 5.22 and 5.23.

$$\sigma_{i,J} = \frac{1}{1 - \prod_{j \in J} \left(1 - p_{i,j} s_{i,j}\right)} \tag{5.22}$$

$$w_{i,j} = \frac{p_{i,j} s_{i,j} \prod_{k=1}^{j-1} \left(1 - p_{i,k} s_{i,k}\right)}{1 - \prod_{j \in J} \left(1 - p_{i,j} s_{i,j}\right)} \tag{5.23}$$

## Details of LLA Approach Deployment

In order to enhance the anypath forwarding scheme with the proposed LLA functionality, it is necessary to implement a procedure to evaluate link stability indices ($s_{i,j}$). Necessary extensions are related to periodic calculation of these values at each transit node $i$ utilizing the `MOVEMENT` structures from Fig. 5.14 that should be stored at nodes $i$ for each neighboring vehicle $j$. The respective X and Y axis movement values of neighboring vehicle $j$, stored in these structures, should be calculated at node $i$ every $\Delta t$ time units based on the default content of `Cooperative Awareness Messages (CAMs)` [18].

CAMs are commonly broadcast every 0.1–1 s by vehicles $j$ via the Control Channel [34, 61]. In particular, CAMs include by default information on vehicle current location (X and Y coordinates) obtained from the Global Positioning System. In order to derive the individual link delivery ratios $p_{i,j}$ for ($t_0 - \Delta t$, $\Delta t$) interval, a standard procedure of broadcasting the common `Hello` messages from

| Vehicle ID | X axis movement | Y axis movement |
|---|---|---|

**Fig. 5.14** MOVEMENT messages of neighboring vehicles $j$ stored at vehicles $i$

[5] similar to *end-to-end path reliability* being a product of delivery ratios $p_{i,j}$ of path links [33, 53], end-to-end transmission stability $S_{s,t}^{r}$ for demand $r$ between source and destination vehicles $s_r$ and $t_r$ can be defined as a product of stability indices of all links of path $\eta$: $S_{s,t}^{r} := \Pi_{(i,j) \in \eta} (s_{i,j})$.

**Input**

- set $V$ of vehicles
- a demand to establish the anypath between vehicles $s_r$ and $t_r$

**Output** Anypath between vehicles $s_r$ and $t_r$

**Indices**

$D$ the set of nodes having the anypath to node $t_r$ already defined

$J$ forwarding set

$J_i$ forwarding set for vehicle $i$ to reach $t_r$

$N$ the queue of nodes that do not have the shortest anypath to $t_r$ yet calculated (ordered ascending the $\sigma_i$ values)

$\sigma_j$ the upper bound on the cost of the shortest anypath from $j$ to $t_r$

```
Step 1  for each node $i$ from $V$, set:
            $\sigma_i := \infty$;  $J_i := 0$
Step 2  Set $\sigma_d := 0$;  $D := \emptyset$; $N := V$
Step 3  while $N \neq \emptyset$:
            $j := \min_{k:\, node\ k \in N} \sigma_k$
            $D := D \cup \{j\}$
            for each incoming arc $(i, j)$
                $J := J_i \cup \{j\}$
                if $\sigma_i > \sigma_j$
                    $\sigma_i := \sigma_{i,J} + \sigma_J$ (using Eqs. 5.21-5.23)
                    $J_i := J$
```

**Fig. 5.15** LLA procedure

each vehicle $i$ via CCH followed by receiving the ACK messages from vehicles $j$ [39] can be utilized.

Our algorithm of Long-Lifetime Anypath establishment (LLA), presented in Fig. 5.15, is based on the Shortest Anypath First (SAF) approach from [35]. In particular, in order to implement the LLA characteristics into the SAF approach, we need to replace the costs and weights from Eqs. 5.15 and 5.17 by the respective Eqs. 5.22 and 5.23. Due to lack of other approaches similar to LLA in the literature, SAF is used as a reference technique in all comparisons presented in this section.

After performing the initialization Steps 1–2, each $i$-th iteration (Step 3 of LLA procedure) is to determine the final cost of anypath with respect to one transit vehicle $j$ from $N$ having the minimum value of $\sigma_j$.

## Numerical Example

We are interested in finding the anypath between vehicles 1 and 7, as shown in Fig. 5.16a including example values of packet delivery probability $p_{i,j}$ and instant stability indices $s_{i,j}$ for the past $(t_0 - \Delta t, t_0)$ interval in the form of the ordered pairs $(p_{i,j}, s_{i,j})$. When executing the LLA algorithm, all costs $\sigma_j$ are initially set to infinity. The only exception is for the cost $\sigma_7$ (referring to a destination vehicle 7), which is set to 0.

As shown in Figs. 5.16 and 5.17, the set of candidate next hops (relays) is formed in a way to minimize the cost $\sigma_j$. After establishing the anypath, general rules of

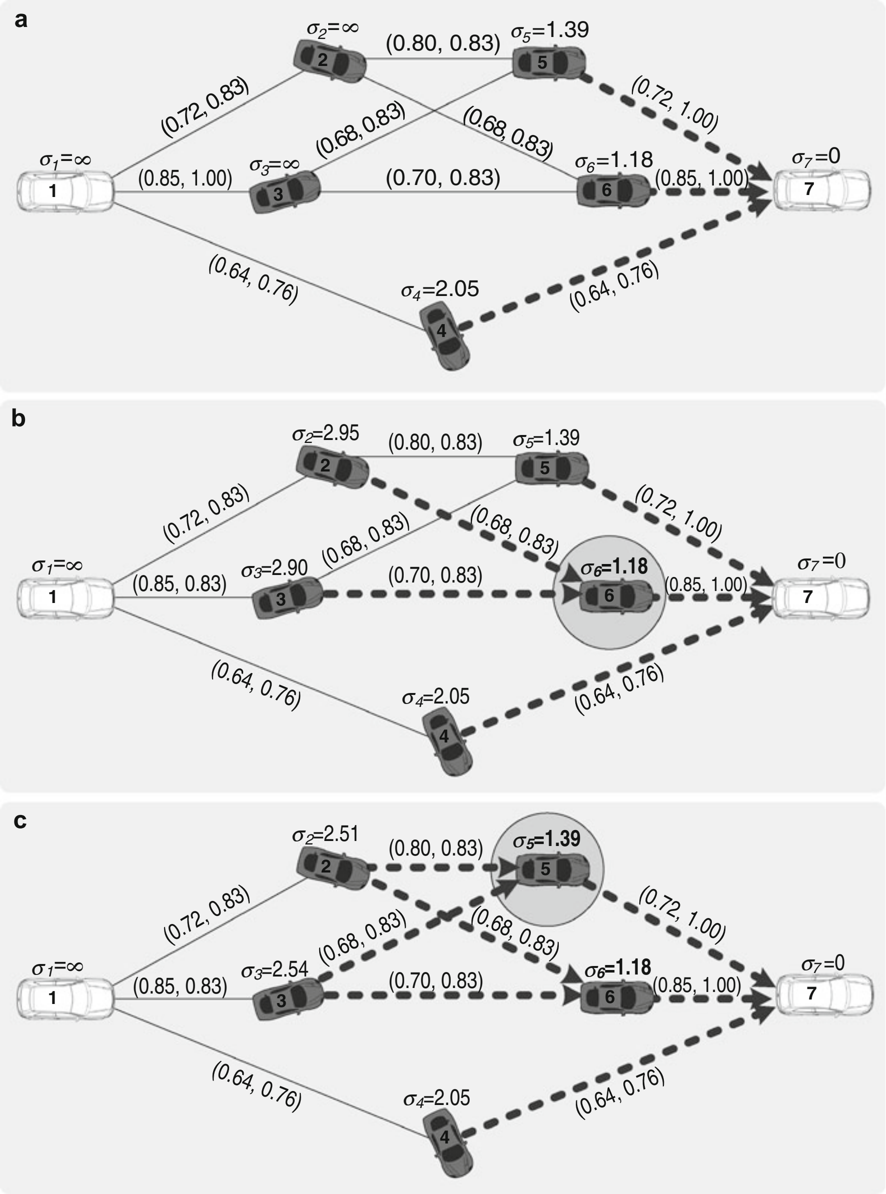


**Fig. 5.16** Example execution steps of the LLA algorithm to determine the anypath between vehicles 1 and 7, including: (**a**) initial graph with link stability indices $s_{i,j}$ and one-hop anypaths; (**b**)–(**c**) results of the first two successive iterations of LLA algorithm execution

anypath forwarding are utilized to deliver the packets towards the destination node. In particular, relay priorities of vehicles $j$ are determined for each forwarding set $J$, based on costs $\sigma_j$ evaluated using our formulas (5.22) and (5.23).

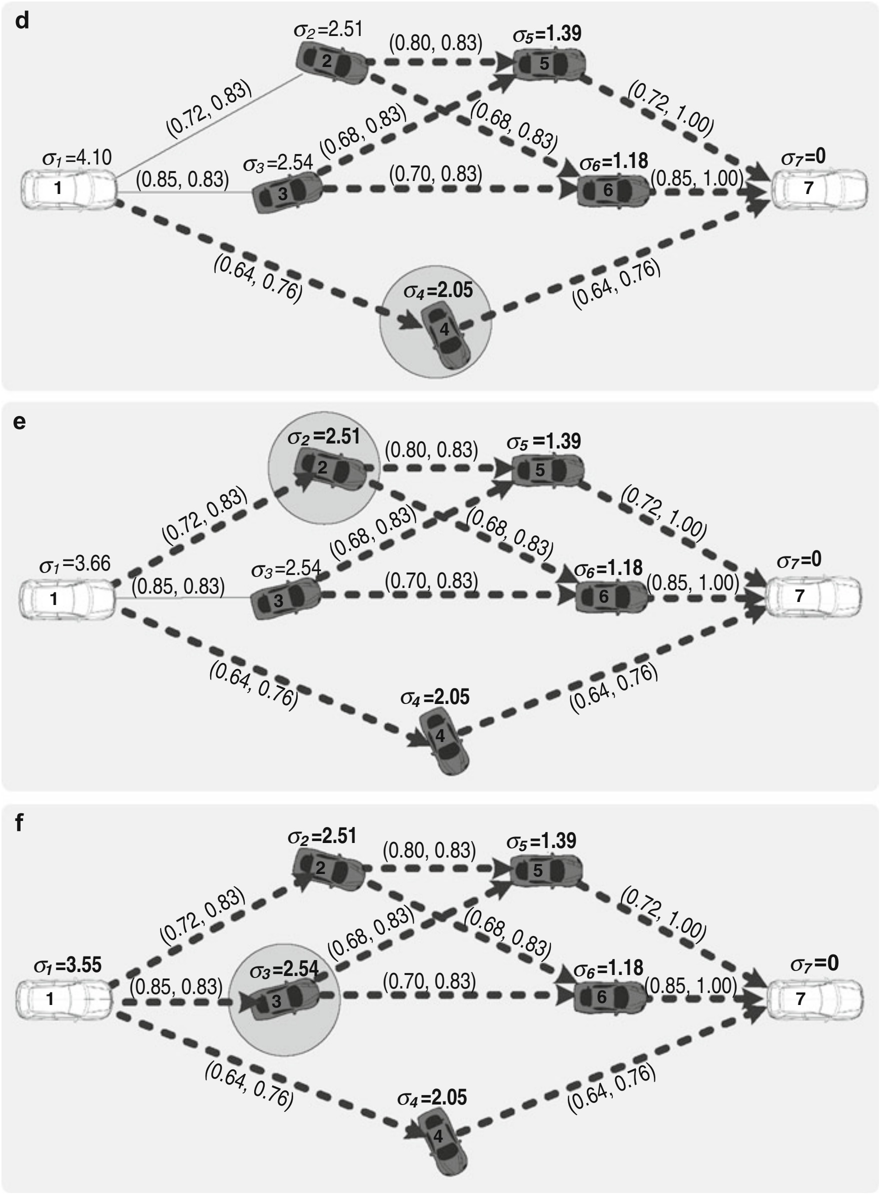


**Fig. 5.17** Example execution steps of the LLA algorithm to determine the anypath between vehicles 1 and 7, including next three successive iterations of LLA algorithm execution

Execution of LLA algorithm is terminated after $|V|$ iterations, i.e., after setting the final anypath cost $\sigma_j$ to all nodes in the network. Assuming that selection of a vehicle with the current minimum cost $\sigma_j$ can be done in O(log$|V|$) steps (e.g., using the binary search), our LLA approach is characterized by the overall complexity bounded in above by O($|V|$·log$|V|$).

### 5.4.2 Analysis of Modeling Results and Conclusions

This section presents results of LLA approach evaluation, in particular including the average values of path cost, hop count, message transmission delay, minimum and average path link stability, as well as end-to-end transmission stability. For each anypath, these characteristics are shown with respect to its primary path (i.e., path of the lowest cost). Evaluation was performed for a realistic case of a 53-node network from Fig. 5.10 (i.e., the same one as in Sect. 5.3). In each of 50 conducted experiments, the following assumptions were considered:

- the set of transmission demands comprised all pairs of vehicles,
- at time $t_0$, cars were moving in directions compliant with the roadmap from Fig. 5.10,
- linear velocities at time $t_0$ were uniformly distributed in range 0–16 m/s (based on common speed limitations in urban areas), with the maximum change $r_{\text{upper}}$ of inter-vehicle distance in $\Delta t = 1$ s interval set to $r_{\text{upper}} = 16$ m.

Similar to Sect. 5.3, estimated movement vectors $S_i$ of vehicles in the future ($t_0$, $t_0 + \Delta t$) interval were calculated based on the respective ones referring to the past ($t_0 - \Delta t$, $t_0$) interval, where $\Delta t = 1$ s. Due to negligibly small values of transmission delay times [30], network topology (including location of vehicles and their speeds) was assumed to be "frozen", i.e., it did not change during path computations. Results obtained for LLA algorithm were next compared to ones of the reference SAF algorithm from [35]. Following [60], formula (5.24) was used to estimate link delivery ratios $p_{i,j}$, while calculation of path costs was realized according to introduced formulas (5.21–5.23) and based on metric from Eq. 5.14.

$$p_{i,j} = \begin{cases} 0.999, & \textit{if} \;\; r_{i,j} \le 400 \\ (-0.4x + 210)/100, & \textit{if} \;\; 400 < r_{i,j} \le 500 \\ 0.1, & \textit{if} \;\; 500 < r_{i,j} \le 600 \\ 0, & \textit{if} \;\; r_{i,j} > 600 \end{cases} \tag{5.24}$$

Obtained average values of analyzed characteristics together with the lengths of the respective 95 % confidence intervals are presented in Table 5.10. Results achieved by our LLA scheme concerning the total path cost were about 76 % better than the reference ones characteristic for the SAF algorithm (36.60 against 150.20). Additionally, our LLA approach also achieved better ratios of minimum link stability (0.25 against 0.11), average link stability (0.55 against 0.33), as well as end-to-end stability (50 % of improvement) of established anypaths. All these results confirmed ability of LLA approach to establish paths characterized by improved stability, as opposed to the common SAF technique. This is additionally shown in Fig. 5.18 presenting histograms of minimum and average values of link stability indices extended by the respective 95 % confidence intervals.

LLA advantages came at a price of increased length of transmission paths (they were about 28 % longer, on average, compared to the SAF reference scheme),

**Table 5.10** Average values of obtained characteristics enhanced with 95 % confidence intervals analysis

| Algorithm | | Path cost | Minimum link stability | Average link stability | End-to-end stability ($S_{s,t}$) | Hop count | Transmission delay [ms] |
|---|---|---|---|---|---|---|---|
| LLA | Average value | **36.60** | **0.25** | **0.55** | **0.09** | **5.61** | **15.36** |
| | Length of 95 % confidence intervals | 6.56 | 0.02 | 0.03 | 0.01 | 0.28 | 0.08 |
| SAF | Average value | **150.20** | **0.11** | **0.33** | **0.06** | **4.38** | **12.01** |
| | Length of 95 % confidence intervals | 23.55 | 0.02 | 0.03 | 0.01 | 0.26 | 0.06 |

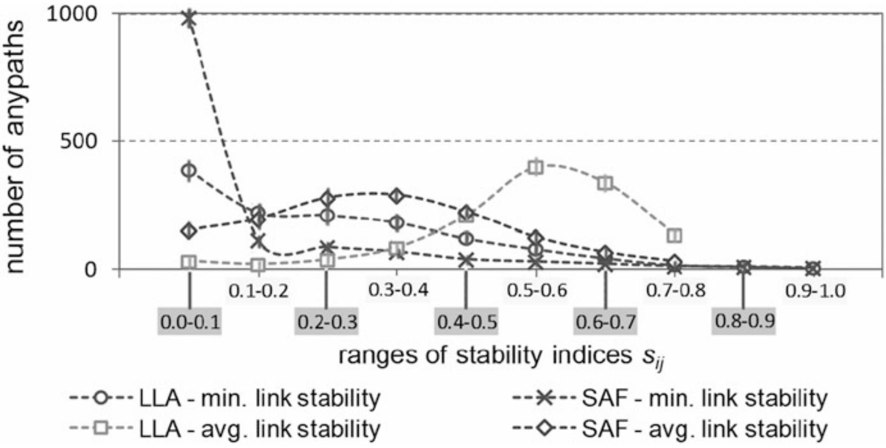


**Fig. 5.18** Histogram of link stabilities

which implied only a small increase of message transmission delay of about 3.3 ms, on average.

## 5.5 Summary

As discussed in this section, resilience of end-to-end multi-hop communications in vehicular ad-hoc networks is a challenging issue due to mobility of vehicles, as well as characteristics of DSRC links. In such a time-dependent environment, broadcasting commonly turns out to be the most efficient way to deliver messages to destination nodes. However, it frequently brings about extensive load of VANET links, which, due to their rather low capacity, is frequently unacceptable. Therefore, to limit the negative effect of broadcasting on network performance, and at the same time improve stability of end-to-end paths, in this chapter we proposed two mechanisms of multipath and anypath forwarding enhanced with selection of links based on current information related to links stability. Evaluation of the proposed methods characteristics showed that they can significantly improve stability of end-to-end paths at a price of practically negligible increase of path length.

## References

1. Alsabaan, M., Alasmary, W., Albasir, A., Naik, K.: Vehicular networks for a greener environment: a survey. IEEE Commun. Surv. Tutorials **15**(3), 1372–1388 (2013)
2. Amendment of the commission's rules regarding dedicated short-range communication services in the 5.850-5.925 GHz band (5.9 GHz band), Federal Communications Commission FCC 03–324 (2004)
3. Anaya, J.J., Merdrignac, P., Shagdar, O., Nashashibi, F., Naranjo, J.E.: Vehicle to pedestrian communications for protection of vulnerable road users. In: Proc. IEEE Intelligent Vehicles Symposium (IVS'14), pp. 1037–1042 (2014)
4. Bauza, R., Gozalvez, J., Sepulcre, M.: Power-aware link quality estimation for vehicular communication networks. IEEE Commun. Lett. **17**(4), 649–652 (2013)
5. Belyaev, E., Molchanov, P., Vinel, A., Koucheryavy, Y.: The use of automotive radars in video-based overtaking assistance applications. IEEE Trans. Intell. Transp. Syst. **14**(3), 1035–1042 (2013)
6. Belyaev, E., Vinel, A., Egiazarian, K., Koucheryavy, Y.: Power control in see-through overtaking assistance system. IEEE Commun. Lett. **17**(3), 612–615 (2013)
7. Blum, J.J., Eskandarian, A., Hoffman, L.: Challenges of intervehicle ad-hoc networks. IEEE Trans. Intell. Transp. Syst. **5**(4), 347–351 (2004)
8. Boukerche, A., Rezende, C., Pazzi, R.W.: A link-reliability-based approach to providing QoS support for VANETs. In: Proc. IEEE International Conference on Communications (IEEE ICC'09), pp. 1–5 (2009)
9. Briesemeister, L., Schäfers, L., Hommel, G.: Disseminating messages among highly mobile hosts based on inter-vehicle communication. In: Proc. IEEE Intelligent Vehicle Symposium (IVS'00), pp. 522–527 (2000)
10. Campolo, C., Molinaro, A., Vinel, A., Zhang, Y.: Modeling prioritized broadcasting in multichannel vehicular networks. IEEE Trans. Veh. Technol. **61**(2), 687–701 (2012)
11. Chachulski, Sz., Jennings, M., Katti, S., Katabi, D.: Trading structure for randomness in wireless opportunistic routing. In: Proc. ACM Annual Conference of the Special Interest Group on Data Communication (ACM SIGCOMM'07), pp. 169–180 (2007)
12. Chen, W., Cai, S.: Ad hoc peer-to-peer network architecture for vehicle safety communications. IEEE Commun. Mag. **43**(4), 100–107 (2005)
13. Chen, X., Li, L., Zhang, Y.: A Markov model for headway/spacing distribution of road traffic. IEEE Trans. Intell. Transp. Syst. **11**(4), 773–785 (2010)
14. Chołda, P., Mykkeltveit, A., Helvik, B.E., Wittner, O.J., Jajszczyk, A.: A survey of service resilience differentiation frameworks in communication networks. IEEE Commun. Surv. Tutorials **9**(2), 32–55 (2007)

15. Deb, B., Bhatnagar, S., Nath, B.: ReInForM: reliable forwarding using multiple paths in sensor networks. In: Proc. 28th IEEE Conference on Local Computer Networks (IEEE LCN'03), pp. 406–415 (2003)
16. Dubios-Ferriere, H., Grossglauser, M., Vetterli, M.: Valuable detours: least cost anypath routing. IEEE/ACM Trans. Networking **19**(2), 333–346 (2011)
17. El-atty, S.M.A., Stamatiou, G.K.: Performance analysis of multihop connectivity in VANET. In: Proc. 7th International Symposium on Wireless Communication Systems (ISWCS'10), pp. 335–339 (2010)
18. ETSI: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service: http://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf. Accessed on 25 Nov. 2014
19. ETSITR102638, Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Definition, ETSI Std. ETSI ITS, Specification TR 102 638 version 1.1.1 (June 2009)
20. Federal Communications Commission: Standard specification for telecommunications and information exchange between roadside and vehicle systems – 5GHz band dedicated short range communications (DSRC) medium access control (MAC) and physical layer (PHY) specifications, ASTM E2213-01 (Sept. 2003)
21. Fukuhara, T., Warabino, T., Ohseki, T., Saito, K., Sugiyama, K., Nishida, T., Eguchi, K.: Broadcast methods for Inter-Vehicle Communication system. In: Proc. IEEE Wireless Communications and Networking Conference (IEEE WCNC'05), vol. 4, pp. 2252–2257 (2005)
22. Harri, J., Filali, F., Bonnet, C.: Mobility models for vehicular ad hoc networks: a survey and taxonomy. IEEE Commun. Surv. Tutorials **11**(4), 19–41 (2009)
23. Hartenstein, H., Bochow, B., Ebner, E., Lott, M., Radimirsch M., Vollmer, D.: Position-aware ad hoc wireless networks for inter-vehicle communications: the Fleetnet project. In: Proc. 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MobiHoc'01), pp. 259–261 (2001)
24. Hartenstein, H., Laberteaux, K.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
25. Huang, X., Fang, Y.: Performance study of node-disjoint multipath routing in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **58**(4), 1942–1950 (2009)
26. Hui, J., Devetsikiotis, M.: A unified model for the performance analysis of IEEE 802.11e EDCA. IEEE Trans. Commun. **53**(9), 1498–1510 (2005)
27. IEEE Standards: http://standards.ieee.org/findstds/standard/802.11p-2010.html. Accessed 21 July 2014 (2010)
28. Jerbi, M., Senouci, S.-M., Rasheed, T., Ghamri-Doudane, Y.: Towards efficient geographic routing in urban vehicular networks. IEEE Trans. Veh. Technol. **58**(9), 5048–5059 (2009)
29. Jie, Z., Huang, Ch., Xu, L., Wang, B., Chen, X., Fan, X.: A trusted opportunistic routing algorithm for VANET. In: Proc. 3rd International Conference on Networking and Distributed Computing Conference (ICNDC'12), pp. 86–90 (2012)
30. Jin, W.-L., Recker, W.W.: An analytical model of multihop connectivity of inter-vehicle communication systems. IEEE Trans. Wirel. Commun. **9**(1), 106–112 (2010)
31. 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)
32. Karp, B., Kung, H.: GPSR: Greedy Perimeter Stateless Routing for wireless networks. In: Proc. ACM Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 243–254 (2000)
33. Khandani, A.E., Abounadi, J., Modiano, E., Zheng, L.: Reliability and route diversity in wireless networks. IEEE Trans. Wirel. Commun. **7**(12), 4772–4776 (2008)

34. Kim, W., Oh, S.Y., Gerla, M., Lee, K.C.: CoRoute: a new cognitive anypath routing protocol. In: Proc. 7th International Conference on Wireless Communications and Mobile Computing Conference (IWCMC'11), pp. 766–771 (2011)
35. Laufer, R., Dubois-Ferriere, H., Kleinrock, L.: Polynomial-time algorithms for multirate anypath routing in wireless multihop networks. IEEE/ACM Trans. Networking **20**(3), 742–755 (2012)
36. Lee, K.C., Gerla, M.: Opportunistic vehicular routing. In: Proc. 16th European Wireless Conference (EW'10), pp. 873–880 (2010)
37. Leontiadis, I., Marfia, G., Mack, D., Pau, G., Mascolo, C., Gerla, M.: On the effectiveness of an opportunistic traffic management system for vehicular networks. IEEE Trans. Intell. Transp. Syst. **12**(4), 1537–1548 (2011)
38. Li, F., Wang, Y.: Routing in vehicular ad hoc networks: a survey. IEEE Veh. Technol. Mag. **2**(2), 12–22 (2007)
39. Li, T., Leith, D., Qiu, L.: Opportunistic routing for interactive traffic in wireless networks. In: Proc. 30th International Conference on Distributed Computing Systems (ICDCS'10), pp. 458–467 (2010)
40. Ma, X., Yin, X., Trivedi, K.: On the reliability of safety applications in VANETs. Int. J. Perform. Eng. **8**(2), 115–130 (2012)
41. Maihöfer, C.: A survey of geocast routing protocols. IEEE Commun. Surv. Tutorials **6**(2), 32–42 (2004)
42. Manifesto of the Car-to-Car Communication Consortium; http://www.car-to-car.org. Accessed 22 July 2014 (Sept. 2007)
43. Marina, M.K., Das, S.R.: On-demand multipath distance vector routing in ad hoc networks. In: Proc. 9th International Conference on Network Protocols (IEEE ICNP'01), pp. 14–23 (2001)
44. Nagel, R.: The effect of vehicular distance distributions and mobility on VANET communications. In: Proc. IEEE Intelligent Vehicles Symposium (IEEE IVS'10), pp. 1190–1194 (2010)
45. Naumov, V., Gross, T.: Connectivity-aware routing (CAR) in vehicular ad-hoc networks. In: Proc. 26th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'07), pp. 1919–1927 (2007)
46. Nishida, T., Eguchi, K., Okamoto, Y., Warabino, T., Ohseki, T., Fukuhara, T., Saito, K.: Inter-vehicle P2P communication experimental on-board terminal. In: Proc. 2nd IEEE Consumer Communications and Networking Conference (IEEE CCNC'05), pp. 434–438 (2005)
47. Oka, H., Higaki, H.: Multihop data message transmission with inter-vehicle communication and Store-Carry-Forward in sparse vehicle ad-hoc networks (VANET). In: Proc. New Technologies, Mobility and Security Conference (NTMS'08), pp. 1–5 (2008)
48. Ooi, Ch.-Ch., Fisal, N.: Implementation of geocast-enhanced AODV-Bis routing protocol in MANET. In: Proc. IEEE TENCON'04, pp. 660–663 (2004)
49. Panichpapiboon, S., Pattara-Atikom, W.: A review of information dissemination protocols for vehicular ad hoc networks. IEEE Commun. Surv. Tutorials **14**(3), 784–798 (2012)
50. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc on-demand distance vector (AODV) routing. IEFT RFC 3561 (2003)
51. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pp. 90-100 (1999)
52. Rak, J.: LLA: a new anypath routing scheme providing long path lifetime in VANETs. IEEE Commun. Lett. **18**(2), 281–284 (2014)
53. Rak, J.: Providing differentiated levels of service availability in VANET communications. IEEE Commun. Lett. **17**(7), 1380–1383 (2013)
54. Sermpezis, P., Koltsidas, G., Pavlidou, F.-N.: Investigating a junction-based multipath source routing algorithm for VANETs. IEEE Commun. Lett. **17**(3), 600–603 (2013)
55. Sichitiu, M.L., Kihl, M.: Inter-vehicle communication systems: a survey. IEEE Commun. Surv. Tutorials **10**(2), 88–105 (2008)

56. Sun, W., Yamaguchi, H., Yukimasa, K., Kusumoto, S.: GVGrid: A QoS routing protocol for vehicular ad hoc networks. In: Proc. 14th IEEE International Workshop on Quality of Service (IEEE IWQoS'06), pp. 130–139 (2006)
57. Suthaputchakun, C., Dianati, M., Sun, Z.: Trinary partitioned black-burst-based broadcast protocol for time-critical emergency message dissemination in VANETs. IEEE Trans. Veh. Technol. **63**(6), 2926–2940 (2014)
58. Toor, Y., Muhlethaler, P., Laouiti, A.: Vehicle ad hoc networks: applications and related technical issues. IEEE Communications Surveys & Tutorials. **10**(3), 74–88 (2008)
59. Vehicle Safety Communications Project, Final Report, DOT HS 810 591, http://www-nrd.nhtsa.dot.gov/pdf/surplus/nrd-12/060419-0843/. Accessed 21 July 2014 (April 2006)
60. Vinel, A., Belyaev, E., Egiazarian, K., Koucheryavy, Y.: An overtaking assistance system based on joint beaconing and real-time video transmission. IEEE Trans. Veh. Technol. **61**(5), 2319–2329 (2012)
61. Vinel, A., Campolo, C., Petit, J., Koucheryavy, Y.: Trustworthy broadcasting in IEEE 802.11p/WAVE vehicular networks: delay analysis. IEEE Commun. Lett. **15**(9), 1010–1012 (2011)
62. Wakikawa, R., Sahasrabudhe, M.: Gateway management for vehicle to vehicle communication. In: Proc. 1st International Workshop on Vehicle-to-Vehicle Communications, UCSD, San Diego (2005)
63. Wu, Ch.-Sh., Pang, A.-Ch., Hsu, Ch.-Sh.: Design of fast restoration multipath routing in VANETs. In: Proc. International Computer Symposium (ICS'10), pp. 73–78 (2010)
64. Yan, G., Olariu, S.: A probabilistic analysis of link duration in vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **12**(4), 1227–1236 (2011)
65. Yang, Q., Lim, A., Li, Sh., Fang, J.: ACAR: adaptive connectivity aware routing protocol for vehicular ad-hoc networks. In: Proc. International Conference on Computer Communications and Networks (ICCCN'08), pp. 1–6 (2008)
66. Ye, Z., Krishnamurthy, S.V., Tripathi, S.K.: A framework for reliable routing in mobile ad-hoc networks. In: Proc. 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'03), pp. 270–280 (2003)
67. Yousefi, S., Altman, E., El-Azouzi, R., Fathy, M.: Analytical model for connectivity in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **57**(6), 3341–3356 (2008)
68. Zeng, K., Lou, W., Zhai, H.: On end-to-end throughput of opportunistic routing in multirate and multihop wireless networks. In: Proc. 27nd Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM'08), pp. 1490–1498 (2012)
69. Zhang, W., Chen, Y., Yang, Y., Wang, X., Zhang, Y., Hong, X., Mao, G.: Multi-hop connectivity probability in infrastructure-based vehicular networks. IEEE Selected Areas in Communications. **30**(4), 740–747 (2012)

# Conclusions

In this book, we focused on resilient routing issues in communication networks. The general conclusion is that it is not possible to eliminate majority of failures of network elements. Driven by forces of nature, unintentional activities of third parties, or malicious attacks, failures will continue to interrupt the normal functioning of any network. However, by appropriate application of preventive techniques, their negative impact on networks performance can be remarkably limited.

Discussions from Chap. 2 conclude that in order to provide efficient means of prevention against disruptions, one must first properly identify the challenges leading to network failures, based on characteristics of the network itself, as well as environmental factors favoring the occurrences of faults. After that, it is crucial to apply the appropriate resilience mechanisms of fast identification of failures, as well as to maintain the continuity of service after a failure, e.g., by using the spare network resources to reduce (or eliminate) possible losses.

If resilient routing is concerned, the choice of an effective scheme basically depends on individual characteristics of the network architecture often making it vulnerable to certain types of disruptions only. For instance, heavy rain falls, despite bringing about a remarkable degradation of link capacities, e.g., in WMNs, in turn have no impact on the respective links in wired (e.g. optical) networks.

Another important issue refers to the availability of resilient routing schemes in the literature, as well as their applicability in practice. In the case of wired networks (and especially for optical WDM networks, IP networks, as well as multilayer schemes), the issue of resilient routing has been already extensively investigated, and the number of proposed solutions is significant. However, each time a new communications concept is announced, in the initial phase it commonly lacks solutions related to resilience, as well as often faces unexpected challenges.

In this book, we focused on three research areas of network resilience referring to selected emerging network architectures that are expected to gain a significant importance in the nearest future. First of them is the concept of the Internet of the Future. Due to a visible orientation of routing around content, common schemes to

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

provide resilient routing based on utilization of backup paths were shown to require adaptation to provide the alternate paths to access information often replicated at several network nodes. In Chap. 3, we introduced three routing schemes providing access to content after failures of network nodes. By applying the anycast routing, our methods based on the utilization of backup paths leading to different replica servers also provided protection in the case of a failure of a node hosting the content (which is commonly not possible for the classical unicast communications). Proposed variants included scenarios of dedicated and shared protection against random failures, as well as dedicated protection under attacks.

In Chap. 4, we focused on continuity of end-to-end transmission under failures affecting high frequency links in Wireless Mesh Networks. Indeed, due to high frequency communications, WMN links are very susceptible to rain falls. As a result, effective capacity of WMN links can be seriously degraded. To provide the appropriate solutions to improve the WMN resilience, we first introduced the measures of WMN survivability necessary to evaluate the vulnerability of WMN topologies to disruptions (e.g., weather-based) occurring in bounded areas leading to multiple correlated failures. These measures were also designed with the aim to be helpful in designing the WMNs with improved resistance to region failures.

Second important contribution of Chap. 4 was a new networking concept to adapt the structure of a WMN to changing weather conditions by periodic updates of antenna alignment based on the forecasted heavy rain falls following from radar echo rain maps. The objective was to avoid creating direct links between WMN nodes over areas with predicted heavy signal attenuation. As verified by means of simulations for real rain scenarios, average signal attenuation could be significantly reduced, compared to the reference scheme not applying any changes to WMN antenna alignment.

Chapter 5 focused on resilience issues in wireless mobile networks organized in ad-hoc manner around vehicles (i.e., Vehicular Ad-hoc Networks – VANETs). In this case, wireless links often encounter availability problems related to high mobility of vehicles, visibly reducing the link lifetime, as well as the lifetime of end-to-end communication paths. VANETs are expected to improve road safety (e.g., by messages exchanged in the case of accidents, or bad weather conditions), traffic coordination (e.g., to help the drivers to move in the green phase), as well as provide the travelers with infotainment services. To work effectively, VANETs need reliable schemes of message dissemination, in particular resistant to mobility-based link disconnections.

To address this issue, in Chap. 5 we proposed two schemes of end-to-end routing that focus on establishing end-to-end communication paths with increased lifetime. This was achieved by a dedicated metric of link costs that utilizes information on predicted stability of VANET links (based on actual movement information). Two proposed routing schemes based on multipath and anypath forwarding resulted in a notable increase of stability of each primary transmission path.

Analyzing the past activities related to existing communications standards, it seems that in most cases, deployed architectures have not offered resilient routing solutions from the beginning. Instead, researchers have focused much more on other aspects. However, the observed increasing importance of Quality of Resilience attributes should change the way of designing new networking solutions, and resilience may soon become one of the leading aspects. How to involve resilience issues into design of a new architecture from the very beginning is indeed one of the main directions of future works.

# Glossary

**1+1 protection** a transmission scheme in which traffic is transmitted in a normal operational network state in parallel over two link-(node-)disjoint paths, one of which takes the role of the only valid path, if the other one fails

**1:1 protection** a path protection scheme assuming usage of a backup path only after a failure of a node/link affecting the primary path

**3G** abbreviation for "third generation" mobile telecommunications conforming to a set of International Mobile Telecommunications-2000 (IMT-2000) specifications defined by ITU-T offering wireless voice telephony, video calls, mobile TV, mobile Internet access, as well as fixed wireless Internet access

**4G** a short form of the "fourth generation" mobile telecommunications (the successor of 3G and the predecessor of 5G) introducing, e.g., mobile broadband Internet access, IP telephony, gaming services, 3D TV, high-definition TV, video conferencing, as well as cloud computing

**Active Path First (APF)** a scheme of establishing the pair (or the set) of end-to-end disjoint paths of a demand assuming that calculation of the primary path is done first and is followed by determination of backup path (or backup paths) over the topology of a residual network – i.e., after excluding the arcs traversed by the primary path (for link disjointedness), or arcs incident to transit nodes of the primary path (for nodal disjointedness)

**Ad hoc On demand Distance Vector (AODV)** a reactive routing protocol developed for wireless ad hoc networks to establish transmission paths on-demand (using Route Request and Route Response messages) and maintaining them as long as they are necessary

**Ad hoc network** a wireless network of a decentralized type not relying on fixed infrastructure, with data forwarding provided by each network node in a dynamic way subject to instantaneous network connectivity

**Add-Drop Multiplexer (ADM)** a wavelength-division multiplexing device used for routing as well as multiplexing/demultiplexing (i.e., adding/dropping) of different channels of light into or out of a single-mode fiber

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

**Alternate path** a backup transmission path used as the only path after a failure of a network element (node/link) affecting the primary transmission path

**Anycast routing** a one-to-one-of-many transmission scheme allowing for accessing the content at one of many potential servers, each one storing a copy (also called a replica) of the original content

**Anypath routing** a transmission scheme utilized, e.g., in VANETs where the set of neighboring nodes (called the forwarding set) act in a cooperative manner to forward each packet toward the destination node

**Asynchronous Transfer Mode (ATM)** a telecommunications concept defined by ITU-T in late 1980s for carriage of a diverse set of voice, data, and video signals (i.e., designed to unify telecommunication and computer networks), providing functionality similar to both circuit switching and packet switching network architectures

**Auditability** assessment whether the communication system is safeguarding information, maintaining data integrity, as well as operating in a way to achieve the goals/objectives of the organization

**Augmented model** a multilayer network scheme being an extension to the overlay model of cooperation between network layers that makes information about nodes reachability available at the UNIs

**Authencity** assurance that the considered principals are exactly who they claim to be

**Authorisability** assurance that the considered elements of a system are accessed according to granted permissions

**Automatic Protection Switching (APS)** a transmission scheme involving establishing of a dedicated/shared protection path of the same capacity as the primary path to be protected

**Availability (of a networking system) at time *t*** readiness for usage of a system at time *t*

**Backbone network** the core part of a communication network infrastructure interconnecting other parts of network, as well as different networks

**Backup path** see “alternate path”

**Best-effort delivery** a network service that does not offer any guarantee on data delivery or that a user is provided with a pre-defined level of QoS/priority

**Betweenness Centrality (BC)** a measure of a network node centrality defined in terms of a number of the shortest paths that traverse the considered node, and, therefore, an important indicator of a node vulnerability to attacks

**Bi-directional Line Switched Ring (BLSR)** a ring network providing protection against failures by offering two transmission rings (for working and backup paths, accordingly)

**Bit Error Rate (BER)** a number of bit errors per total number of bits transferred

**Bottom-up recovery** a recovery scheme in a multilayer network where recovery actions with respect to the affected flows are initiated in the lowermost layer and are then continued in the upper layers

**Broadcasting** transmission of information to every node located within a direct reach of a sender

**Car-to-Car Communications Consortium (C2C-CC)** a non-profit industrial organisation driven by European vehicle manufacturers and supported by equipment suppliers and research organizations with the objective to increase the safety and efficiency of road traffic by means of inter-vehicular wireless communications

**Cascading failures** failures of multiple network elements triggered by the initial failure (e.g., failures of network nodes as a result of power outage implied by an earthquake)

**Central node** a network node switching large amount of data characterized by one of the highest degrees in the network

**Central Processing Unit (CPU)** an electronic circuitry caring out arithmetic, logical, control, and input/output (I/O) operations specified by the instructions

**Challenge** a characteristics/condition that may occur as an event affecting the normal operation of a network

**Challenge probability** probability of a challenge occurrence

**Challenge tolerance** a network resilience category focusing on network design approaches to provide service continuity in the presence of challenges

**Class of Service (CoS)** a parameter utilized to identify the type of a packet payload to provide differentiated transmission services to packets based on assigned priorities

**Clean-slate** a concept of deploying new solutions under the assumption that other parts of the network architecture remain unchanged

**Cloud computing/communications** a computing/communications paradigm based on the utilization of computer resources combining the global-scale resource centres and computation possibilities into the cloud to form a "computing utility" available over the Internet

**Coexistence (of virtual networks)** parallel existence of multiple virtual networks over the same resources of one or several infrastructure providers

**Common pool** technique of sharing the backup resources in a multilayer network in a way that the respective protection (backup) paths from different layers do not share the risk of being activated at the same time

**Confidentiality** assurance of not disclosing information without a proper authorization

**Content-Aware Networking (CAN)** a paradigm of network intelligence to identify, based on incoming request to access the content, where to find it, and how to deliver it

**Content-Centric Networking (CCN)** see *Content-Aware Networking*

**Content Delivery Network (CDN)** a distributed system of interconnected data centers to provide the end users with content at high availability and performance guarantees

**Content-Oriented Networking (CON)** an opposite solution to the conventional host-to-host information delivery shifting the issues of item identification from hosts to information (i.e., making information rather than conventional IP addresses the primary search goal); see *Content-Aware Networking*

**Control Channel (CCH)** a communication channel in VANETs used to transmit the control messages

**Cooperative Awareness Message (CAM)** information broadcasted periodically once every 0.1–1 s by a vehicle in VANETs to inform other vehicles, e.g., about its current location

**Correlated failures** concurrent failures of multiple network elements being interdependent (as e.g., in the region failure scenario)

**Critical information infrastructure** an information system that is essential for the functioning of a society and economy

**Critical latency** the upper bound on message delivery latency

**Cyber attack** any type of malicious activity (usually originating from an anonymous source) driven by individuals/organizations aimed at causing significant losses with respect to target information systems, infrastructures, computer networks, and/or personal computer devices

**Dedicated protection** a resilient communications scheme based on the assignment of backup paths exclusively for a given working path

**Dedicated Short Range Communications (DSRC)** specification of short-range to medium-range wireless communication channels for use in inter-vehicular communications

**Delay** a QoS attribute defined with respect to transmission of information as an interval between given two time limits determined in various ways (e.g., concerning the time needed for a message to be transmitted end-to-end over the network)

**Delay-tolerant transmission** a transmission scheme not requiring real-time data delivery

**Dense Wavelength Division Multiplexing (DWDM)** an optical transmission scheme originally related with optical signals multiplexed within the 1550 nm band allowing for co-existence of many independent transmission channels per link

**Dependability** a discipline used to quantify the level of service reliance

**Disaster-based failure** a failure of network element(s) implied by occurrence of a disaster of any kind, including natural disasters, technology-related disasters, and malicious attacks

**Disjoint paths** a set of end-to-end paths having no common links (for link disjointedness) or no common transit nodes (for nodal disjointedness)

**Disruption tolerance** the ability of communication paths to survive from disruptions affecting the network nodes/links

**Dissemination of data/messages** a Layer 2 transmission scheme utilized, e.g., in VANETs to deliver messages frequently via multiple hops based on single-hop broadcasting

**Distributed Denial of Service (DDoS)** an attempt performed in a distributed way (e.g., by multiple parties) to make the network node resources unavailable to end users mostly by temporarily/indefinitely interrupting the services of a host

**Diversity** a networking paradigm aimed to assure that the same flaw does not affect multiple elements of a communication system

**Domain Name System (DNS)** a hierarchical distributed naming system to associate information such as IP addresses with domain names assigned to the considered network nodes

**E.800** ITU-T recommendation "Definitions of terms related to Quality of Service"

**E.802** ITU-T recommendation "Framework and methodologies for the determination and application of QoS parameters"

**E.820** ITU-T recommendation "Call models for serveability and service integrity performance"

**E.850** ITU-T recommendation "Connection retainability objective for the international telephone service"

**E.855** ITU-T recommendation "Connection integrity objective for the international telephone service"

**E.860** ITU-T recommendation "Framework of a service level agreement"

**E.862** ITU-T recommendation "Dependability planning of telecommunication networks"

**E.880** ITU-T recommendation "Field data collection and evaluation on the performance of equipment, networks and services"

**Electromagnetic Pulse attack (EMP)** a malicious activity based on a transient electromagnetic disturbance via a short burst of electromagnetic energy

**End-to-end routing** transmission of information from the source node towards the destination node frequently over multiple transit nodes

**Error** a deviation between the observed value/state and its specified (correct) value/state

**European Telecommunications Standards Institute (ETSI)** a non-profit telecommunications standardization organization issuing standards for Information and Communications Technologies (fixed, mobile, radio, converged, broadcast, and Internet technologies).

**Event-driven notifications/messages** information sent after identification of an event

**Failure (of network services)** a negative result of error propagation affecting the normal functioning of network services

**Failure probability** probability that a particular challenge will result in a fault

**Failures in time (FIT)** the number of failures per billion device hours

**Fault** a flaw being either an accidental design flaw (for instance a software bug), or an intentional flaw not eliminated for instance due to the cost constraints of the system

**Fault detection** network activity leading to determination of fault in real-time either in the physical layer (e.g., due to loss of signal, loss of modulation, or loss of clock) by means of signal degradation recognition (e.g., increased bit error rate – BER), or Quality of Service degradation (indicated by decreased throughput, or increased transmission delay)

**Fault localization** network activity aimed at determination of the point of fault occurrence

**Fault notification** network activity necessary to start redirection of the affected traffic onto the alternate paths

**Fault tolerance** ability of a communication system to cope with faults being result of events other than service failures

**Federal Communications Commission (FCC)** an agency of the United States government aimed to regulate the US interstate communications by radio, television, wire, satellite, and cable focusing on broadband, competition, spectrum, media, public safety, as well as homeland security issues

**Five nines property** guarantee on a communication system availability of at least 99.999%

**Fixed addressing** a scheme of assigning the address to a VANET node once it joins the network, which remains unchanged until the node leaves the network

**Forwarding set** a set of VANET neighboring nodes used in anypath communications to forward the packet towards the destination node

**Free capacity** capacity of a link not assigned to any communication path

**Full restoration time** time required for traffic to be routed onto links, which are capable of or have been engineered sufficiently to handle traffic in recovery scenarios

**Future Internet (FI)** a set of relevant capabilities of the global communications infrastructure not existing in the current Internet architecture

**Future Internet Assembly (FIA)** an European forum organized once/twice a year for a collaboration between members of FI projects to maintain European competitiveness in the global marketplace

**G.911** ITU-T recommendation "Parameters and calculation methodologies for reliability and availability of fibre optic systems"

**Generalized Multiprotocol Label Switching (GMPLS)** an extension to MPLS to manage additional classes of interfaces and switching technologies such as TDM, layer-2 switching, wavelength switching, or fiber-switching

**Geocasting** see "geographical addressing"

**Geographical addressing** a scheme of address assignment based on location of a mobile node (frequently used, e.g., in VANETs, where an address of a VANET node changes as the vehicle moves – not necessarily leaving the network)

**Global Positioning System (GPS)** a space-based satellite navigation system to offer location and time information anywhere on the earth (or near the earth) provided that there is an unobstructed line of sight to at least four GPS satellites

**Global recovery (protection) scheme** resilience scheme assuming utilization of a single backup path providing the end-to-end protection with respect to a given primary path

**Goodput** the application-level throughput defined as the number of bits referring to useful information delivered to the application per unit of time

**Graph of conflicts** a graph with vertices modeling objects of a given kind interconnected by edges representing the conflict states with respect to the vertices

**High-degree node** a network node connected to many other nodes via direct links

**Hold-off timer** a recovery mechanism designed for multilayer networks to postpone the recovery actions in the higher layer to give the lower layer time for recovery of the affected traffic

**Host-centric communications** conventional communications scheme assuming that named hosts are the main network entities to be addressed

**Hypertext Transfer Protocol (HTTP)** a common application protocol for hypermedia information systems – the major protocol for data communications for the World Wide Web

**IEEE 802.11** a set of specifications referring to MAC and PHY layers addressing implementation issues of wireless local area network communications developed and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802)

**Information-Centric Networking (ICN)** see "Content-Oriented Networking"

**Infotainment** a group of VANET applications providing travellers with on-board information and entertainment services such as Internet access, or music download

**Infrastructure Provider (InP)** an entity managing the physical infrastructure of networks

**Inheritance** characteristics of a virtual network allowing the child virtual networks inherit the architectural attributes of their parent virtual networks

**Integer Linear Programming (ILP)** a paradigm of solving the optimization problems or feasibility tests, in which the objective function and constrains are linear and some (or all) of the variables are restricted to be integers

**Integrated (peer) recovery model** a multilayer network resilience scheme allowing for sharing of routing information between network layers

**Integrity** the absence of improper (unauthorized) system alterations

**Inter-domain recovery** a recovery scheme (e.g., based on utilization of alternate paths) that involves resources from multiple network domains

**International Federation for Information Processing (IFIP)** a non-profit organization working in the field of information technology, focusing on sponsoring and organizing conferences and workshops in the area of Information and Communications Technology

**International Telecommunication Union - Telecommunication Standardization Sector (ITU-T)** one of the three units of ITU responsible for coordination of telecommunication standards

**Internet Engineering Task Force (IETF)** the open standards organization without formal membership requirements established to develop Internet standards on voluntary basis in particular referring to the TCP/IP protocols family

**Internet of Things (IoT)** a network of physical objects ("things") commonly embedded with electronics, sensors, and software, and therefore provided with ability to exchange information with other connected devices (or the manufacturer/operator)

**Internet Protocol (IP)** the major communications protocol in the set of Internet protocols responsible for relaying datagrams across communication networks (i.e., routing)

**Internet Protocol version 6 (IPv6)** the latest version of the Internet Protocol (intended to replace IPv4) developed by IETF, e.g., to solve the problem of IPv4 address exhaustion

**Internet Service Provider (ISP)** commercial, community-owned, non-profit, or privately-owned entity offering services related with participating in the Internet

**Inter-Vehicular Communications (IVC)** a type of wireless communications between vehicles and roadside units to exchange information (e.g., safety- and traffic-related)

**IP packet Delay Variation (IPDV)** the end-to-end one-way delay difference between consecutive packets in a flow in an IP network (with any lost packets being disregarded)

**IP packet Error Ratio (IPER)** the number of packets being incorrectly received in an IP network divided by the total number of received packets

**IP packet Loss Ratio (IPLR)** the number of lost packets divided by the total number of sent packets

**IP packet Transfer Delay (IPTD)** the aggregate value of end-to-end store-and-forward delays a packet encounters in each transit node before being received by the destination node (i.e., depending on network congestion and the number of transit routers along a transmission path)

**Jitter** a deviation from the assumed periodicity of packets delivery

**Jitter-sensitive transmission** a transmission scheme that does not tolerate jitter with respect to consecutive packets delivery

**Label Switched Path (LSP)** a communication path set up by a signalling protocol in an MPLS network

**Large-scale testbed** a communication infrastructure of a large (e.g., national/continental) scale deployed to validate the proposed global communications solutions

**Lightpath** a multihop optical path providing end-to-end connectivity in the optical network

**Line of Sight (LOS) propagation** a characteristic of electromagnetic radiation with emissions of light travelling along a straight line

**Linear Programming (LP)** a paradigm of solving the optimization problems or feasibility tests in which the objective function and constrains are linear and variables are continuous

**Link downtime** a period of link unavailability

**Link-Path formulation** formulation of an optimization problem with variables referring to a set of pre-computed paths traversing the network links

**Link State Advertisement (LSA)** a basic communication methodology of the OSPF routing protocol in which network nodes periodically distribute information related to the current characteristics of incident links

**Local recovery (protection) scheme** a recovery scheme assuming utilization of a backup path designed to redirect the affected traffic over the failed link/node (i.e., short detours)

**M.3342** ITU-T recommendation “Guidelines for the definition of SLA representation templates”

**M.60** ITU-T recommendation “Maintenance terminology and definitions”

**Maintainability** predisposition of a system to updates/evolution

**Mean Downtime (MDT)** an interval during which an item is in a “down” state

**Mean Time Between Failures (MTBF)** the mean time between consecutive failures

**Mean Time Between Interruptions (MTBI)** the mean time between the end of one interruption and the beginning of the next one

**Mean Time to Failure (MTTF)** time duration of an item from the instant of time it goes from a “down” state to an “up” state until the occurrence of the next failure

**Mean Time to First Failure (MTFF)** the mean time duration before occurrence of the first failure

**Mean Time to Repair/Recovery (MTTR)** a mean time interval during which an item is in a “down” state due to a failure

**Mean Time to Restore Service (MTRS)** a mean time interval during which a service is not available due to a failure

**Mean Uptime (MUT)** interval during which an item is in an “up” state

**Media Access Control (MAC)** a sublayer of the Layer 2 (data link layer) responsible for proper addressing and efficient channel access control mechanisms to enable multiple network nodes to communicate over a shared medium (e.g., in Ethernet network)

**Millimeter-wave communications** communications over extremely high-frequency radio communication channels in the electromagnetic spectrum from 30 to 300 GHz (ITU definition)

**Multicast routing** a one-to-many routing scheme suitable for group communications where a message needs to be sent to a group of destination nodes

**Multi-cost network** a scheme with differentiated costs assigned to network links in computations of multiple disjoint paths of the same demand

**Multi-domain routing** routing of information over multiple network domains

**Multi-hop Inter-Vehicular Communications (MIVC)** inter-vehicular communications utilizing multi-hop transmission scheme

**Multi-hop routing** routing of information via multiple transit nodes

**Multi-layer network** a general scheme for contemporary wide-area networks composed of multiple layers, each layer acting as a network of a certain type (e.g., WDM, SONET, IP), allowing for existence of the upper-layer virtual links provided by the physical lower-layer paths

**Multipath routing** a routing scheme enabling simultaneous transmission of information over multiple end-to-end (frequently disjoint) paths

**Multiple-input multiple-output (MIMO)** a technique to multiply the capacity of a radio link by means of multiple transmit and receive antennas to benefit from multipath propagation

**Multiprotocol Label Switching (MPLS)** a forwarding mechanism that relays information between network nodes based on path labels rather than network addresses, which prevents from time-consuming searches in a routing table

**Named Data Object (NDO)** the main abstraction in information-centric networking representing the addressable content

**Nesting** see “recursion”

**Network-Network Interface (NNI)** an interface to signalling and management functions between neighboring networks enabling interconnection of signalling, IP-MPLS, or ATM networks

**Network Virtualization Environment (NVE)** a set of multiple heterogeneous network architectures (often from different service providers) that can be utilized to form a virtual network by the InP

**Node-Link formulation** formulation of an optimization problem including variables referring to utilization of a link connecting the source node *i* and leading to a destination node *j* by communication paths for the purpose of serving given demands *r*

**Non-repudiability** assurance provided by a neutral third party that a given transaction/event did (or did not) occur

**Non-shareable spare capacity** capacity already reserved at a link for backup path purposes that cannot be shared by the backup path of the considered demand

**Normalization** (in relation with the recovery process) recognition of the repaired element and return to the normal operational state of a network

**NP-complete problem** a problem that belongs to the class of NP problems, as well as can be obtained by a polynomial reduction from another NP-complete problem

**NP problem** a problem for which it can be verified in polynomial time whether the answer “yes” to its recognition version is indeed “yes”

**Number of concurrent faults** number/ratio of faults a selected recovery scheme can cover

**OC-48** a network link with transmission rate of up to 2488.32 Mbit/s

**On-Board Unit (OBU)** the appropriate in-vehicle wireless communications device enabling VANET communications

**Open Shortest Path First (OSPF)** a routing protocol belonging to the class of link-state routing algorithms widely used in IP networks to establish and maintain the communication paths

**Opportunistic routing** see “anypath routing”

**Optical Cross Connect (OXC)** a network device designed to switch optical signals in a fiber optic network at high-speed rates

**Overlay networking** a multilayer network scheme assuming that routing is performed in each layer separately (i.e., no routing information is shared between the network layers)

***p*-cycles** see “protection cycles”

**Packet Delivery Ratio (PDR)** the ratio of the number of delivered data packets to the destination node

**Packet Error Rate (PER)** the number of incorrectly received data packets (i.e., including at least one erroneous bit) divided by the total number of received packets

**Packet Loss Ratio (PLR)** the ratio of the number of lost data packets transmitted by a given node

**Peer model** a multilayer network model allowing for sharing of routing information between network layers

**Peer-to-peer (P2P) networking** a scheme of partitioning tasks or workloads among peers (equally privileged entities)

**Percent of IP service availability (PIA)** percentage of total scheduled IP service time categorized as available using the IP service availability function

**Percent of IP service unavailability (PIU)** percentage of total scheduled IP service time categorized as unavailable using the IP service availability function

**Performability** discipline that is used to provide measures on performance of a system compared with the respective Quality of Service requirements following from service specifications in terms of delay, jitter, bandwidth, and packet losses

**Physical layer (PHY)** the lowest layer in the seven-layer network model, responsible for sending/receiving signals, and, therefore, comprising the respective hardware transmission technologies

**Point of Interest (POI)** a specific location point that may be found useful/interesting (in VANET communications)

**Preferential attachment rule** a principle of adding a new node to the network by linking it with existing nodes with probability proportional to the degree of existing nodes

**Preplanned protection** a resilient communication scheme based on backup paths installed in advance (when establishing the respective primary path)

**Primary path** the main transmission path of a demand

**Problem reduction** an algorithm for transforming one problem into another problem

**Protection cycles** a scheme to provide protection of a mesh network from a link failure based on ring structures characterized by ring-like high recovery speed and mesh-like high capacity efficiency

**Protection-switching time** a time interval from the occurrence of a network fault until the completion of protection-switching operations

**Quality of Resilience (QoR)** a separate aspect of quality provisioning focusing on QoS measures related to network resilience

**Quality of Service (QoS)** the overall performance of a communication network seen by the end users in terms of delay, jitter, bandwidth, and packet losses

**Random failure** a failure of a network element (node/link) being independent of the element characteristics

**Reactive restoration** a methodology of redirecting the affected flows onto backup paths found reactively upon occurrence of a failure

**Recognition problem** a problem with “yes/no” answer

**Recovery ratio** a quotient of the actual recovery bandwidth divided by the traffic bandwidth that is intended to be protected

**Recovery switching** redirection of the affected traffic onto the alternate path

**Recovery time** see “restoration time”

**Recovery token** a signal used in a multilayer recovery scheme allowing to synchronize the recovery actions at consecutive layers

**Recursion** a parent-child relationship for virtual networks creating the VN hierarchy (i.e., VNs built on top of other VNs), often referred to as nesting

**Redundancy** the ratio of protection capacity to working capacity

**Region-based failure** a scenario of simultaneous failures of multiple network elements located close enough to the failure epicentre to suffer from the results of the event

**Reliability** a measure of service continuity referring to the probability that a system/service remains operable in a given time frame $(0, t)$

**Replica server** a node hosting the copy of the content in anycast communications

**Request for Comments (RFC)** a publication of the Internet Engineering Task Force (IETF) and the Internet Society – the major standards-setting and technical development Internet bodies

**Resilience** 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

**Resilience differentiation** distinction of differentiated Quality of Resilience features tailored to differentiated demands of end-users

**Resilient routing** a routing scheme that is able to provide the continuity of service in the presence of disruptions

**Restoration time** a time interval from the occurrence of a network fault to the instant of time when the affected traffic is either completely restored, or until spare resources are exhausted, or no more extra traffic exists

**Retainability** probability that a service will continue to be provided

**Revisitation** characteristics of a virtualization scheme enabling hosting multiple virtual nodes from a given virtual network by a single physical node

**RFC 2330** IETF specification "Framework for IP performance metrics"

**RFC 3386** IETF specification "Network hierarchy and multilayer survivability"

**RFC 3469** IETF specification "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery"

**RFC 3945** IETF specification "Generalized Multi-Protocol Label Switching (GMPLS) Architecture"

**RFC 4378** IETF specification "A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)"

**RFC 4427** IETF specification "Recovery (protection and restoration) terminology for Generalized Multi-Protocol Label Switching (GMPLS)"

**RFC 4428** IETF specification "Analysis of Generalized Multi-Protocol Label Switching (GMPLS)-based recovery mechanisms (including protection and restoration)"

**Road-Side Unit (RSU)** a roadside communications infrastructure deployed to enable vehicle-to-infrastructure communications in VANETs

**Robustness** indicator of performance of a network under perturbative conditions

**Route Request (RREQ)** a message sent by a source node towards the destination node in AODV routing protocol to initiate establishing of a communication path

**Route Response (RREP)** a message sent back by a destination node towards the source node in AODV routing protocol to confirm establishing of a communication path

**Safety** a measure of a system dependability under catastrophic failures, in particular referring to the effect rather than the cause of a failure

**Scope of a recovery procedure** the size of the primary path segment protected by a single backup path

**Security** ability of a system to protect itself from various unauthorized activities

**Segment recovery (protection) scheme** a recovery scheme assuming utilization of a backup path to redirect the affected traffic over a given segment of a primary path

**Service Channel (SCH)** a communication channel in VANETs used to transmit the applications data

**Service continuity** the length of a time period during which the service is not interrupted

**Service interruption time** the length of a time period the service is interrupted

**Service Level Agreement (SLA)** a service contract in use between the service provider and the customer

**Service Loss Block (SLB)** an event occurring for a block of packets at an ingress node when the ratio of lost packets at an egress node exceeds some threshold

**Service Provider (SP)** an entity providing clients with communications, storage, and/or processing services

**Service recovery** actions a service provider performs as a response to the service failure

**Setup vulnerability** amount of time that a working path is left unprotected during such tasks as recovery path computation and recovery path setup

**Shareable spare capacity** capacity already reserved at a link for backup path purposes that can be shared by the backup path of the considered demand

**Shared protection** a scheme and conditions of backup path installation allowing for sharing the link capacities among multiple backup paths

**Shared Risk Link Group (SRLG)** a set of network elements, being either links, nodes, physical devices, or a mix of these, subject to a common risk of failure

**Signal-to-Noise Ratio (SNR)** a measure used to compare the level of a signal against the level of a background noise

**Single-cost network** a scheme with the same link cost assigned to a given link in computations of all paths for each demand

**Single-hop Inter-Vehicular Communications (SIVC)** inter-vehicle communications strategy using one-hop message dissemination

**Software-Defined Networking (SDN)** an approach to communication networks allowing for management of network services by abstraction of lower-level functionality

**Spare capacity** capacity reserved at network links for backup path purposes

**Sparse V2I system** a VANET system designed to provide vehicle-to-land communication services at hot-spots (e.g., parking availability, parking payment, or collection of tolls for roads/bridges/tunnels)

**Store-carry-forward transmission** a transmission scheme assuming that information is sent to an intermediate node where it is stored for some time (e.g., due to lack of connectivity) and next sent to another intermediate node to approach the destination node

**Survivability** capability of a system to fulfil its mission in a timely manner in the presence of threats including attacks or natural disasters

**Synchronous Digital Hierarchy (SDH)** a common technology for transmission of synchronous data over optical links being the word-wide equivalent of SONET (from the US)

**Synchronous Optical Network (SONET)** North American equivalent of Synchronous Digital Hierarchy (SDH) network architecture

**Throughput** a measure of a successful message delivery rate for the analyzed communication channel

**Time Division Multiplexing (TDM)** a method of transmitting and receiving independent signals over a common communication path by means of a synchronized time-dependent exclusive access to medium

**Top-down recovery** a recovery scheme in a multilayer network where recovery actions with respect to affected flows are initiated in the uppermost layer and are then continued at the lower layers

**Traffic grooming** consolidation of lower-rate flows into larger units using TDM scheme

**Traffic tolerance** ability of a network to tolerate additional (unusual) volume of traffic that is injected into the network (e.g., as a result of excessive activity of end users)

**Transient failure** a failure lasting relatively shortly (e.g., less than a minute)

**Transmission Control Protocol (TCP)** a connection-based, reliable, streaming communication protocol (being part of the widely used TCP/IP protocols family) used to send data between processes

**Trap problem** a scenario when the algorithm fails to establish the next disjoint path of a demand, even though it would be feasible for a given topology

**Trustworthiness** a resilience category comprising measurable characteristics of analyzed communication systems

**Ubiquitous V2I system** a VANET communication system offering vehicle-to-land-based communication services to end-users not restricted to selected locations

**Unicast routing** a one-to-one routing transmission scheme

**Unidirectional Path-Switched Ring (UPSR)** a ring network in which two copies of information are sent in either direction around a ring

**User-Network Interface (UNI)** an interface between a user and a network provider defining responsibilities of the service provider and of the user

**Vehicle Safety Communications Consortium (VSCC)** a consortium consisting of BMW, DaimlerChrysler, Ford, GM, Nissan, Toyota, and VW with the aim to contribute to standards/specifications focusing on vehicular safety issues

**Vehicle-to-infrastructure (V2I)** a VANET communication scheme between vehicles and a roadside infrastructure

**Vehicle-to-vehicle (V2V) communications** short-range wireless communications between vehicles in VANETs without support of a roadside infrastructure

**Vehicular Ad-hoc NETwork (VANET)** an ad-hoc self-organized network using vehicles as mobile nodes

**Virtual link** a logical link in the overlay structure created over a physical communication infrastructure as an end-to-end (commonly multihop) physical path

**Virtual Local Area Network (VLAN)** a local-area virtual network

**Virtual Network (VN)** a network created based on resources of a physical network including virtual links and communication nodes (that can also be virtual) having its broadcast domain separated from other co-existing virtual networks

**Virtual node** functionality of a communication node hosted on one/several physical nodes

**Virtual Private Network (VPN)** an extension of a private network across the public network (e.g., Internet) enabling communication devices exchange data across a shared or a public network, as if they were in a direct scope in a private network

**Virtualization** creation of a virtual instance of a communication network

**Voice over IP (VoIP)** a methodology of delivery of voice communications as well as multimedia sessions over IP networks (e.g., Internet)

**Vulnerable Road User (VRU)** a pedestrian in a VANET communications scheme

**Wavelength** distance over which the shape of the wave is repeated

**Wavelength Division Multiplexing (WDM)** a communications technology enabling frequency division multiplexing of multiple optical carrier signals onto a single optical fiber with multiple wavelengths of laser light, providing bidirectional communications per each wavelength over a fiber link

**Weapon of Mass Destruction (WMD)** a nuclear, radiological, or other type of weapon able to cause significant damage to human-made structures (e.g., buildings, communication networks) resulting in multiple failures bounded in certain regions of occurrence

**Wi-Fi** specification of a local area wireless communication network allowing for communications of devices via 2.4 Ghz and 5 GHz radio bands

**Wireless Mesh Network (WMN)** a wireless network organized in a mesh topology, consisting of mesh clients and mesh routers interconnected by wireless links (frequently of high-speed – as e.g., in the case of links between mesh routers)

**Wireless Sensor Network (WSN)** a set of autonomous sensors interconnected via wireless links set up to monitor physical/environmental conditions, e.g., pressure, temperature, or sound, etc., and to forward such information in a cooperative manner to the main location in the network

**Wireless transceiver** a networking device capable of sending and receiving information via a wireless communication channel

**Working capacity** capacity reserved at network links for working paths purposes

**Working path** see “primary path”

**Y.1540** ITU-T recommendation “Internet protocol data communication service – IP packet transfer and availability performance parameters”

**Y.1541** ITU-T recommendation “Network performance objectives for IP-based services”

**Y.1542** ITU-T recommendation “Framework for achieving end-to-end IP performance objectives”

**Y.1561** ITU-T recommendation “Performance and availability parameters for MPLS networks”

**Y.1562** ITU-T recommendation “Framework for higher layer protocol performance parameters and their measurement”

# Index

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