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