Chapter 8
Resilience of Future Internet Communications

Over the last 40 years, we have been observing a gradual evolution of the Internet from an academic network toward a widespread commercial architecture. Indeed, the classic 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 USA [43].

The 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 concerning services and daily use applications to enhance the quality of life [9]. In particular, owing to the observed convergence of telecommunications, media, and information technology, the 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, the conventional Internet has already reached its limits where even minor improvements do not have much chance to succeed. Therefore, a comprehensive Internet transformation from a simple "host-to-host" packet exchange environment toward 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
- Resilience
- Energy efficiency

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications and Networks, https://doi.org/10.1007/978-3-031-64657-7_8

Since, without doubt, future knowledge society will be built on the Internet communications base, any limitations referring to the efficiency of the Internet must be defeated. Otherwise, end users may not be able to fully benefit from several 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 (NSF) in the USA [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, [6, 23, 67]).

Apart from the European activities in this area, including, e.g., 4WARD [63], FIRE [27], GEANT2 [30], or IIP [29], there have also been other important initiatives from the USA (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 mainly described by a set of relevant capabilities not existing in the classic Internet architecture. As discussed in [6, 23, 24, 55, 56, 61], the list of desired functionalities of the Future Internet architecture includes the following:

- *Content-oriented networking* (*CON*) being an opposite solution to the conventional host-to-host information delivery, as the primary utilization of the Internet visibly 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 centers 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* (*HCI*) 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. 10 of this book), where a system installed in a vehicle may automatically inform other vehicles about accidents, ice on the road, etc.

- *Personalized services* including individualized (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 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 classic Internet), which is justified from both technical and economic reasons.
- *Energy efficiency*. The gradual growth of Internet traffic volume increases energy consumption by networking equipment to accommodate the demands. One of the solutions to save energy may be switching off the devices or putting them into sleep mode in inactive periods.
- *Availability and disruption tolerance*. The Internet is currently viewed as an important element of critical infrastructure (similar to, e.g., fresh water supplies or power grids). Therefore, the architecture of the Future Internet should also be resistant to disruptions of any kind, providing an alternate means for content distribution/processing in the face of failures and guaranteeing fast recovery of affected network elements.

Another classification of FI main research areas from [60] is presented in Fig. 8.1. In particular, issues of Future Internet resilience are included in areas #2 (Future Internet modeling, analysis, and design) and #3 (Future Internet network architectures), respectively.

To support these functionalities, one of the 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 and be evolvable and flexible to accommodate 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 connects billions of nodes and supports 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 must be designed dynamically and modularly, allowing for further adaptive changes [9].

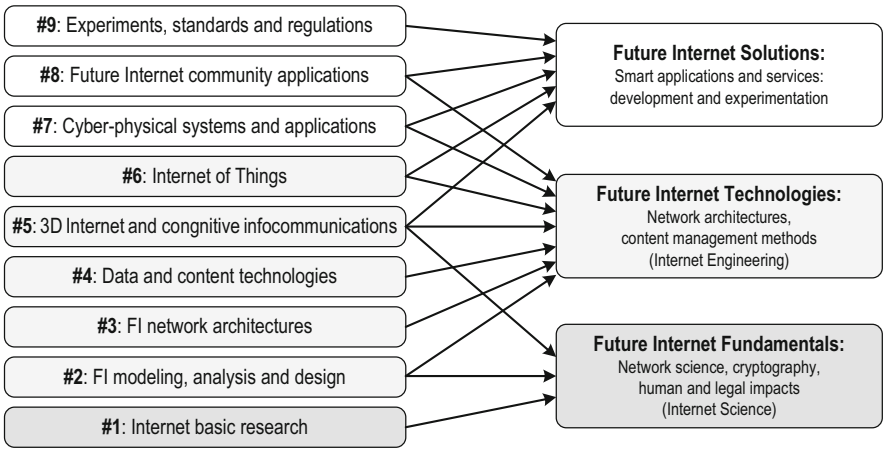

Fig. 8.1 Future Internet research areas in relation to their goals from [60]

In the remaining part of this chapter, we will discuss in detail the key research topics and requirements for the FI architecture (Sect. 8.1), present our solutions to network resource provisioning necessary to provide network resilience (Sect. 8.2), and describe in Sect. 8.3 three proposals to improve the resilience of content-oriented FI networking. The chapter is summarized in Sect. 8.4.

8.1 Key Research Topics and Requirements for the Future Internet Architecture

Considering the architectural requirements of the Future Internet, a distinction between providers of a network infrastructure (i.e., physical resources) and providers of network services becomes apparent. It justifies the need for *virtual networks* (*VNs*) implementation. Such a scheme allowing for leasing 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 concerning 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

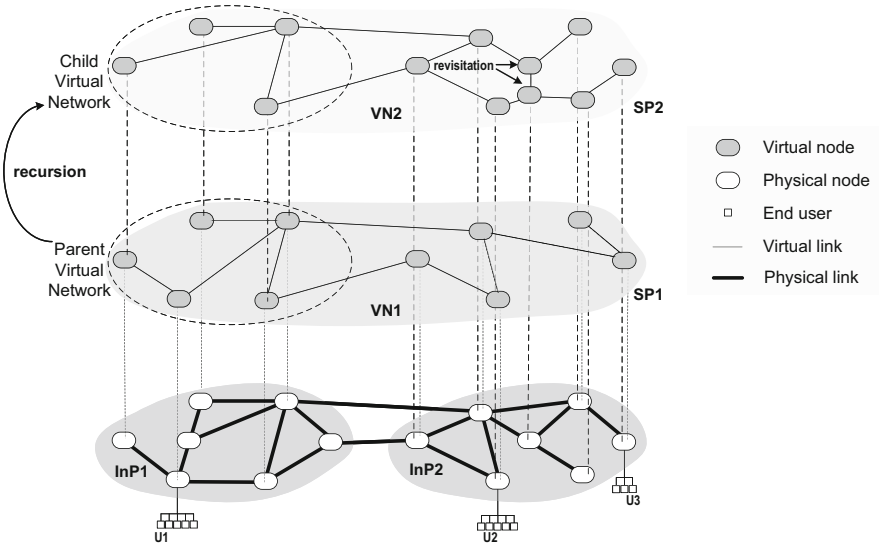

Fig. 8.2 Example network virtualization environment (NVE) with virtual network VN1 created on top of InP1 and InP2 resources and VN2 additionally implementing partial parent-child relationship with VN1

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 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. 8.2.

A 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 [7]
– *Inheritance* allowing child VNs to inherit the architectural attributes of their parent VNs [43]

[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).

– *Recursion* being a parent-child relationship for virtual networks (see Fig. 8.2) 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. Like the original idea of overlays, deploying new network virtualization environments does not require changes to the underlying physical network once it is set up to support network virtualization [18]. Therefore, virtualization is expected to be a scalable scheme that offers 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, several 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 classic 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 end-to-end services by service providers to meet the stringent Quality of Service requirements. As such, it is also essential to support resilient routing (for instance, by efficient reservation of network resources for alternate paths establishment) in the face of differentiated challenges and should be considered an essential part of any Future Internet architecture.

Therefore, in Sect. 8.2, we will highlight the concept of network resource provisioning for virtualization environments proposed in the example framework of one of the major European research projects on Future Internet architecture by researchers from Polish technical universities and research centers 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 coexisting virtual networks of differentiated transmission types.

The respective network resource provisioning module we implemented 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 in end-to-end demands over time.

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

Among several 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 the coexistence of 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. 8.3.

In this section, we focus on the Future Internet resource provisioning issues, particularly concerning architectural aspects of the L1/L2 resource provisioning module we implemented 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 (e.g., on link propagation delay concerning given PIs) may also be 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].

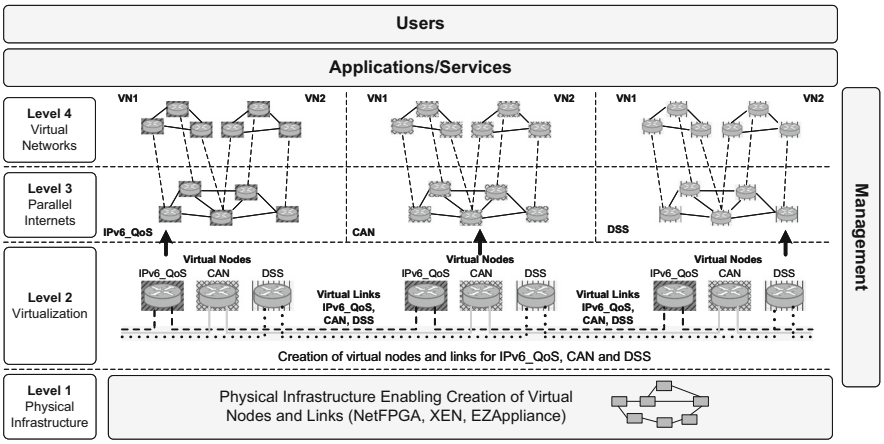

Fig. 8.3 Architecture of System IIP from [12]

Model 8.1 Formulation of Link Bandwidth Utilization Optimization Problem Respecting Basic Requirements on Routing (LBUO)

Symbols

$G(N,A)$	Directed network, where N and A are the sets of network nodes and directed arcs, respectively; each network link is represented by two opposite arcs $a_h = (i, j)$ and $a'_h = (j, i)$; and $\|N\|$ and $\|A\|$ are the numbers of network nodes and arcs, respectively.
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, respectively; $\|M\| = 3$),
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
$\hat{c}_{m,h}$	The lower bound on capacity (i.e., fraction of link capacity) required at arc a_h for m-th instance of PI
$c_{r,m}$	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 (8.1).

$$\min \ \varphi(x) = \sum_{m \in M} \sum_{h \in A} x_{m,h} \tag{8.1}$$

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 $a_h = (i, j)$:

$$\sum_{n:a_h=(i,n)\in A} x_{m,h} = \sum_{n:a_h=(n,j)\in A} x_{m,h}; \quad m \in M; \quad h \in A \tag{8.2}$$

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

$$\sum_{\substack{h\in\{h:a_h=(t,j)\in A;\\ j=1,2,\ldots,|N|;j\neq n\}}} x_{m,h} = \sum_{\substack{h\in\{h:a_h=(i,t)\in A;\\ i=1,2,\ldots,|N|;i\neq n\}}} x_{m,h}; \quad m \in M; \quad t \in T \tag{8.3}$$

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

$$x_{m,h} \geq \hat{c}_{m,h} c_h \quad m \in M; \quad h \in A \tag{8.4}$$

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

$$\sum_{m\in M} x_{m,h} \leq c_h; \quad h \in A \tag{8.5}$$

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

$$\sum_{\substack{h\in\{h:a_h=(n,j)\in A;\\ j=1,2,\ldots,|N|;j\neq n\}}} z_{r,m,h} - \sum_{\substack{h\in\{h:a_h=(i,n)\in A;\\ i=1,2,\ldots,|N|;i\neq n\}}} z_{r,m,h} = \begin{cases} c_{r,m}, & \text{if } n = s_{r,m} \\ -c_{r,m}, & \text{if } n = t_{r,m} \\ 0, & \text{otherwise} \end{cases} \tag{8.6}$$

where $r \in D_m$, $m \in M$, and $n \in N$.

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:

$$\sum_{r\in D_m} z_{r,m,h} \leq x_{m,h}; \quad m \in M; \quad h \in A \tag{8.7}$$

We also implemented another objective function aimed at maximizing the total residual (free) capacity at all arcs, as given in Eq. 8.8. 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).

$$\max \ \varphi(x) = \sum_{h\in A} \left(c_h - \sum_{m\in M} x_{m,h} \right) \tag{8.8}$$

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 8.2 Extension of the LBUO Model Including Basic Requirements on Node Resource Utilization Optimization Issue (LBNR)

Symbols
The set of symbols is the same as in the 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

ϕ_n Aggregate processing power at node n

Variables
The list of variables is the same as in the LBUO model and extended by 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 (8.9).

$$\min \ \varphi(x) = \sum_{m \in M} \sum_{n \in N} \wp_{m,n} \tag{8.9}$$

Constraints
The set of constraints includes formulas (8.2)–(8.7) and is additionally extended by constraint (8.10) referring to calculation of node n processing power utilization related to the portion of capacity reserved for each m-th PI and formula (8.11) providing the upper bound on the total processing power available at node n to serve all demands.

$$\wp_{m,n} = \sum_{\substack{h \in \{h: a_h = (n,j) \in A; \\ j=1,2,\ldots,|N|; j \neq n\}}} \theta_{m,h} x_{m,h} + \sum_{\substack{h \in \{h: a_h = (i,n) \in A; \\ i=1,2,\ldots,|N|; i \neq n\}}} \rho_{m,h} x_{m,h}; \quad m \in M; \quad n \in N \tag{8.10}$$

$$\sum_{m \in M} \wp_{m,n} \leq \phi_n; \quad n \in N \tag{8.11}$$

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

concerning 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 8.3 Extension of LBNR Model Including Additional Constraints on End-to-end Delay (LBDC)

Symbols
The set of symbols is the same as in the 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 the 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 and 0 otherwise

Objective
The same as in the LBUO model (i.e., Eq. 8.1).

Constraints
The set of constraints includes formulas (8.2)–(8.7) and (8.10)–(8.11) and is extended by formula (8.12) 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 (8.13) combined with constant G necessary to bind the respective binary variable $v_{r,m,h}$ with the continuous variable $z_{r,m,h}$.

$$\sum_{h \in A} v_{r,m,h} p_h \leq p_{m,r}; \quad r \in D_m; \quad m \in M \tag{8.12}$$

$$z_{r,m,h} \leq v_{r,m,h} G; \quad r \in D_m; \quad m \in M; \quad h \in A \tag{8.13}$$

All three problems were generally proved to be $\mathcal{NP}$-complete in [37]. Therefore, for larger problem instances, it is necessary to use one of the suboptimal heuristic approaches, e.g., the one we proposed in [37].

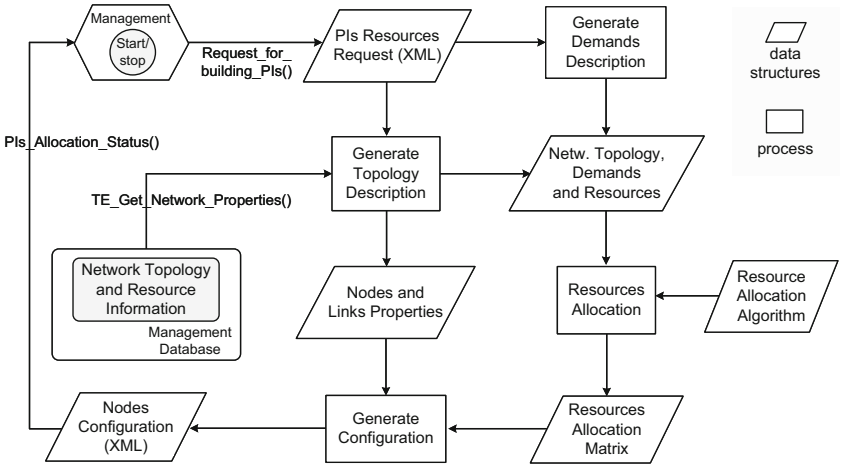

Fig. 8.4 The functional diagram of network resource provisioning module in System IIP architecture from [37]

Owing to the utilization of the implemented network resource provisioning module concerning 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 8.4 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 the 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 to decide on not only resource provisioning concerning the primary communication paths but also concerning backup routes, as discussed in detail in Sect. 8.3 for the information-centric networking concept (the paradigm of one of PIs addressed in this chapter).

8.3 Fault Tolerance of Content-Oriented Networking

Owing to the remarkable increase in Internet traffic in recent years [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, the *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 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 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 unavailable (for instance, due to node failure or a failure of a transit link/node of a communication path). It is essential to ensure a reliable content distribution in a failure-prone environment, especially with sparse connectivity or high-speed mobility [19].

Considering routing issues, there are several approaches to retrieving information from the source nodes of the content. Among them, it is essential to mention the strategy implemented in the 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 the 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 the 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 protect against failures of network elements using alternate paths to such a replicated content.

8.3.1 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

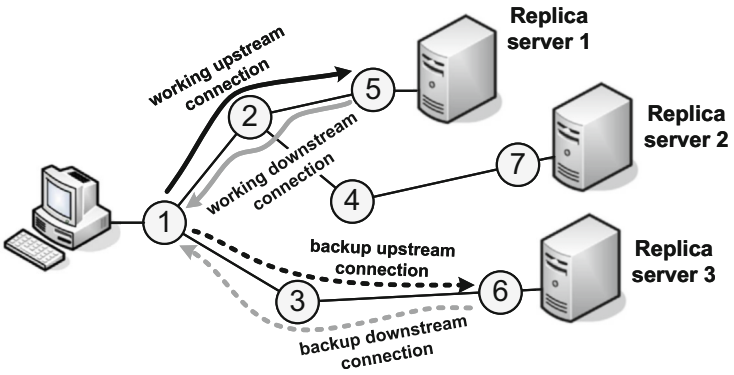

Fig. 8.5 An example of survivable anycast routing with a backup path leading to another replica server

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 and 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. 8.5) [70].

Our proposal from [72] presented here aims at optimizing the routing of anycast and unicast flows with a particular focus on assuring the survivability of the affected traffic. Such a joint optimization scheme is reasonable due to the coexistence 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 the case of anycast traffic, to provide survivability against single failures of end nodes, the content has to be stored in parallel at two different replica servers accessible using node-disjoint paths [69]. For unicast traffic, a conventional end-to-end path protection scheme can be employed. The novelty of our approach, compared to other results available in the literature (e.g., [8, 22, 46, 49, 69]), is in the 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 protect against single link failures (i.e., establishing link-disjoint paths), as well as failures 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 $G(N, A)$, where N is a set of nodes, and A is a set

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

of directed arcs. Each arc $a_h \in A$ is characterized by cost ξ_h (referring to the length of arc a_h) and offers Λ 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 equals the capacity of a single WDM channel (i.e., $c_r = 1$). In anycast communications, we have upstream and downstream demands (referring to sets D^{US} and D^{DS}, respectively). 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. 8.5, both associated anycast demands r and $\tau(r)$ must be related to 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:

Symbols

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 downstream 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 Λ of unidirectional optical channels
ξ_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 using working and backup paths given by formula (8.14).

$$\min \ \varphi(x) = \sum_{r \in D} \sum_{h \in A} \xi_h (x_{r,h} + y_{r,h}) \tag{8.14}$$

Constraints

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

$$\sum_{\substack{h \in \{h: a_h = (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} x_{r,h} - \sum_{\substack{h \in \{h: a_h = (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} x_{r,h} = \begin{cases} 1, & \text{if } n = s_r \\ -1, & \text{if } n = t_r; \quad r \in D^{UN}; \quad n \in N \\ 0, & \text{otherwise} \end{cases} \tag{8.15}$$

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

$$\sum_{\substack{h \in \{h: a_h = (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} y_{r,h} - \sum_{\substack{h \in \{h: a_h = (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} y_{r,h} = \begin{cases} 1, & \text{if } n = s_r \\ -1, & \text{if } n = t_r; \quad r \in D^{UN}; \quad n \in N \\ 0, & \text{otherwise} \end{cases} \tag{8.16}$$

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

$$\sum_{\substack{h \in \{h: a_h = (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} x_{r,h} - \sum_{\substack{h \in \{h: a_h = (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} x_{r,h} = \begin{cases} -1, & \text{if } n = t_r \\ \kappa_{r,n}, & \text{if } n \neq t_r; \quad r \in D^{DS}; \quad n \in N \end{cases} \tag{8.17}$$

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

$$\sum_{\substack{h \in \{h: a_h = (n,j) \in A; \\ j = 1,2,\ldots,|N|; j \neq n\}}} y_{r,h} - \sum_{\substack{h \in \{h: a_h = (i,n) \in A; \\ i = 1,2,\ldots,|N|; i \neq n\}}} y_{r,h} = \begin{cases} -1, & \text{if } n = t_r \\ v_{r,n}, & \text{if } n \neq t_r; \quad r \in D^{DS}; \quad n \in N \end{cases} \tag{8.18}$$

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

$$\sum_{\substack{h\in\{h:a_h=(n,j)\in A;\\ j=1,2,...,|N|;j\neq n\}}} x_{r,h} - \sum_{\substack{h\in\{h:a_h=(i,n)\in A;\\ i=1,2,...,|N|;i\neq n\}}} x_{r,h} = \begin{cases} 1, & \text{if } n = s_r \\ -\kappa_{r,n}, & \text{if } n \neq s_r; \end{cases} \quad r \in D^{US}; \quad n \in N \tag{8.19}$$

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

$$\sum_{\substack{h\in\{h:a_h=(n,j)\in A;\\ j=1,2,...,|N|;j\neq n\}}} y_{r,h} - \sum_{\substack{h\in\{h:a_h=(i,n)\in A;\\ i=1,2,...,|N|;i\neq n\}}} y_{r,h} = \begin{cases} 1, & \text{if } n = s_r \\ -v_{r,n}, & \text{if } n \neq s_r; \end{cases} \quad r \in D^{US}; \quad n \in N \tag{8.20}$$

7. To provide a proper selection of replica nodes:

$$\kappa_{r,n} \leq u_n; \quad r \in D^{AN}; \quad n \in N \tag{8.21}$$

$$v_{r,n} \leq u_n; \quad r \in D^{AN}; \quad n \in N \tag{8.22}$$

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

$$\kappa_{r,n} = \kappa_{\tau(r),n}; \quad r \in D^{DS}; \quad n \in N \tag{8.23}$$

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

$$v_{r,n} = v_{\tau(r),n}; \quad r \in D^{DS}; \quad n \in N \tag{8.24}$$

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

$$\sum_{n\in N} \kappa_{r,n} = 1; \quad r \in D^{AN} \tag{8.25}$$

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

$$\sum_{n\in N} v_{r,n} = 1; \quad r \in D^{AN} \tag{8.26}$$

12. On finite arc capacity:

$$\sum_{r \in D} (x_{r,h} + y_{r,h}) \leq c_h; \quad h \in A \tag{8.27}$$

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

$$(x_{r,h} + y_{r,h}) \leq 1; \quad r \in D; \quad h \in A \tag{8.28}$$

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

$$(x_{\tau(r),h} + y_{\tau(r),h}) \leq 1; \quad r \in D^{AN}; \quad h \in A \tag{8.29}$$

The objective is to minimize the overall cost of the flow (formula (8.14)) subject to constraints (8.15)–(8.29). In the model given by formulas (8.14)–(8.29), 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 (8.14)–(8.29) is called Any Replica (AR) here.

Our investigations are also extended by:

- An additional constraint (8.30) to provide disjointness of working and backup replica servers (forming the Disjoint Replica (DR) model defined by formulas (8.14)–(8.30))
- Constraint (8.31) 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 (8.14)–(8.29) and (8.31))
- Constraint (8.32) 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 (8.14)–(8.29) and (8.32)

$$\sum_{n \in N} (\kappa_{r,n} + v_{r,n}) \leq 1; \quad r \in D^{AN} \tag{8.30}$$

$$\kappa_{r,n} = v_{r,n}; \quad r \in D^{AN}; \; n \in N \tag{8.31}$$

$$\kappa_{r,n} = v_{r,n} = \chi_{r,n}; \quad r \in D^{AN}; \; n \in N \tag{8.32}$$

Simulation Results and Conclusions

Verification of characteristics of four introduced models focusing on evaluation of the total network cost (defined as given in formula (8.14)), 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. 8.6. All links were assumed to have $\Lambda = 160$ channels of equal capacity.

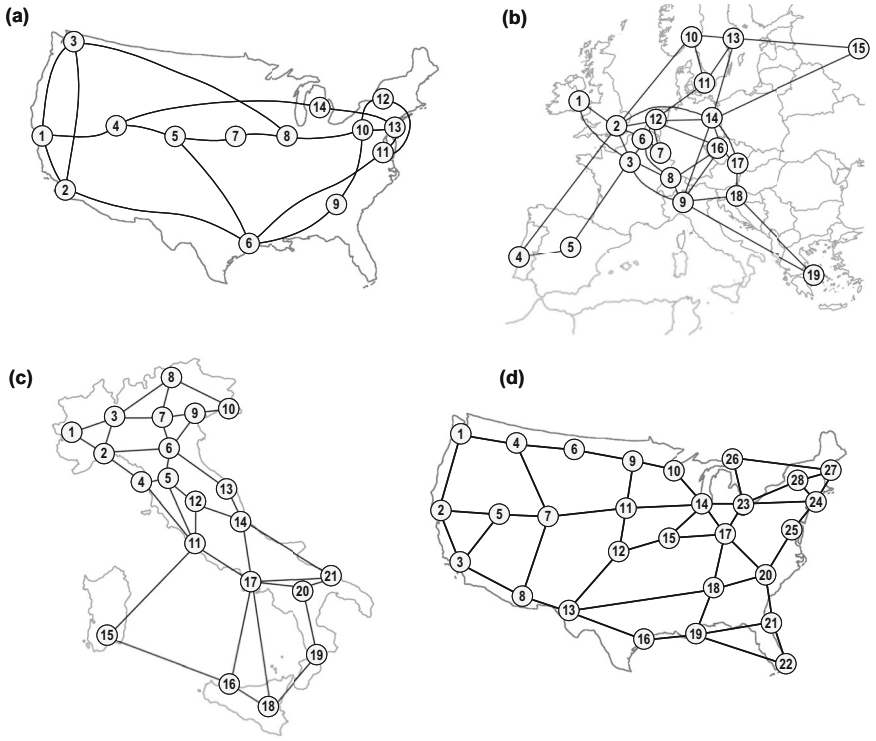

Fig. 8.6 Network topologies used in the analysis: NSF Network **(a)**, COST 239 Network **(b)**, Italian Network **(c)**, and US Long-Distance Network **(d)**

Table 8.1 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

Nodes had a full wavelength conversion capability (i.e., at each transit node, flows arriving at any wavelength λ_i of the incoming link could be switched onto any wavelength λ_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 8.1, 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. 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 a 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). An analysis of multiple scenarios of network load, replica servers count, and other extensions of our ILP model is given in [72].

Table 8.2 presents the average execution time for each analyzed topology and replica model. As shown in Table 8.2, all four models are characterized by comparable values of the average execution time. The only exception is the CR model, for which the average execution time is about two times greater than for the other models. This is due to additional constraints (8.31), including working and backup replica variables.

Figures 8.7 and 8.8 present the average network costs calculated based on formula (8.14), as well as their relation with the number of available 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 in 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 the characteristics of analyzed models, the AR approach outperforms the other ones. This is due to its flexibility (i.e., it does not impose additional constraints on replica servers selection). The performance of the other models depends on network characteristics and the number of available replica servers.

Table 8.2 Average execution time

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

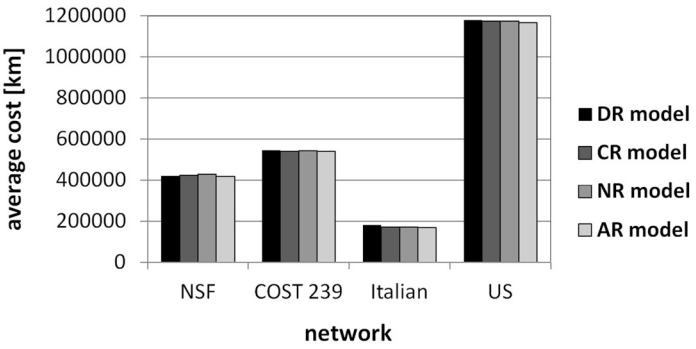

Fig. 8.7 Average network cost for two replica servers

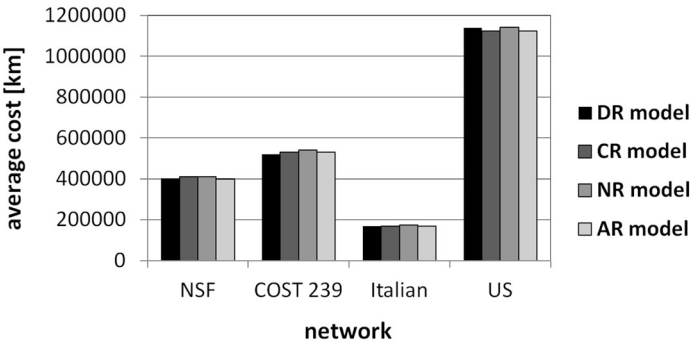

Fig. 8.8 Average network cost for four replica servers

As discussed in Chap. 4 of this book, providing preplanned protection against failures by 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, 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.

8.3.2 Shared Protection for Survivable Anycasting

As discussed in Chap. 2, 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 the condition that the respective working paths being protected are mutually node-/link-disjoint [4, 41]. This section presents our proposal from [71] of sharing the backup path resources for routing 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 [39–41, 58]. Considering backup path resource sharing for survivable anycast routing (as illustrated in Fig. 8.9), 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 predefined 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 the investigation of all possible backup paths and, consequently, allowing us to reach optimal results. This model, being an extension of the respective one from Sect. 8.3.1, is defined as follows.

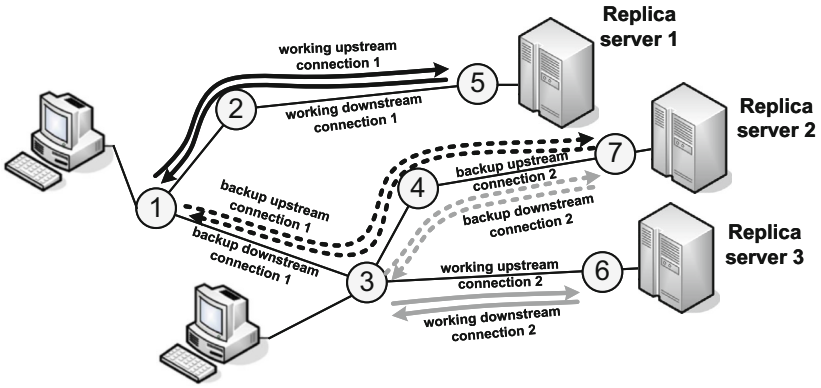

Fig. 8.9 Example of survivable anycast routing with different backup replica servers. Sharing the backup path capacities may be performed at links (3, 4) and (4, 7)

Symbols

The set of symbols is the same as in Sect. 8.3.1 and is extended by the following:

c_r Volume (capacity) of demand r

Variables

The set of variables is the same as in Sect. 8.3.1 and is 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, and 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 protect against a failure of each single link

Objective

It is to minimize the total cost of delivery of flows using working and backup paths given by formula (8.33).

$$\min \ \varphi(x) = \sum_{r \in D} \sum_{h \in A} \xi_h c_r x_{r,h} + \sum_{h \in A} \xi_h b_h \tag{8.33}$$

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 (8.15)–(8.20)
2. To provide a proper selection of replica nodes: formulas (8.21)–(8.22)

3. To assure that the associated upstream and downstream demands use the same corresponding replica node for working and backup paths: formulas (8.23)–(8.24)
4. To guarantee that exactly one node is selected as a working and backup replica node for each anycast demand: formulas (8.25)–(8.26)
5. On finite arc capacity:

$$\sum_{r \in D} c_r x_{r,h} + b_h \leq \Lambda; \quad h \in A \tag{8.34}$$

6. To provide link disjointness of working and backup paths: formulas (8.27)–(8.28)
7. To obtain shared protection concerning the considered backup paths:

$$x_{r,g} + y_{r,h} \leq 1 + b_{r,h,g}; \quad r \in D; h \in A; g \in A; g \neq h \tag{8.35}$$

$$2b_{r,h,g} \leq x_{r,g} + y_{r,h} \quad r \in D; h \in A; g \in A; g \neq h \tag{8.36}$$

8. To provide bounds on arc spare capacity:

$$b_{h,g} = \sum_{r \in D} c_r b_{r,h,g}; \quad h \in A; g \in A; g \neq h \tag{8.37}$$

$$b_{h,g} \leq b_h; \quad h \in A; g \in A; g \neq h \tag{8.38}$$

9. To assure location of working and backup replica servers at the nearest nodes: formula (8.32)

If we replace formula (8.38) with the following formula (8.39), we obtain the model without shared protection, since b_h is then defined simply as the sum of backup capacities over all link failures.

$$b_h = \sum_{g \in A} b_{h,g} \tag{8.39}$$

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

– SBPP-AR: Any Replica model; shared protection: formulas (8.33), (8.15)–(8.20), (8.23)–(8.28), (8.34)–(8.38)
– SBPP-NR: Nearest Replica model; shared protection: formulas (8.33), (8.15)–(8.20), (8.23)–(8.28), (8.32), (8.34)–(8.38)
– noSBPP-AR: Any Replica model; dedicated protection: formulas (8.33), (8.15)–(8.20), (8.23)–(8.28), (8.34)–(8.37), (8.39)
– noSBPP-NR: Nearest Replica model; dedicated protection: formulas (8.33), (8.15)–(8.20), (8.23)–(8.28), (8.32), (8.34)–(8.37), (8.39)

Simulation Results and Conclusions

Numerical experiments aimed to evaluate the efficiency of the introduced shared protection schemes in terms of (1) the total cost of a solution, (2) the 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 8.3, 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 of 8–28 and 7–44, respectively. To obtain a given value of anycast ratio, demand volumes c_r were selected from the range 1–9. Two cases of replica servers count (2 and 3, respectively) and four analyzed variants of our ILP model in total gave 192 different experiments, all performed for the analyzed NSF network from Fig. 8.6a.

Experiments were also prepared to evaluate the performance of shared backup capacity models compared to schemes without backup capacity sharing. Therefore, the first set of results, presented in Fig. 8.10, refers to the average overall cost of solutions (based on formula (8.33)) in terms of ratios $cost^{\text{SBPP}}/cost^{\text{noSBPP}}$ as a function of the anycast ratio parameter. The average value of this coefficient (obtained for all experiments) was 0.64, meaning that shared backup path approaches outperformed the respective "no sharing" ones by 36%. As shown in Fig. 8.10, the difference between the analyzed approaches decreases with the increase of the anycast ratio parameter since, under anycasting, one of the end nodes of demand is also related to one of the replica servers located at a limited number of

Table 8.3 Locations of replica servers (node indices)

2 replica servers	4 replica servers
6, 10	4, 6, 10

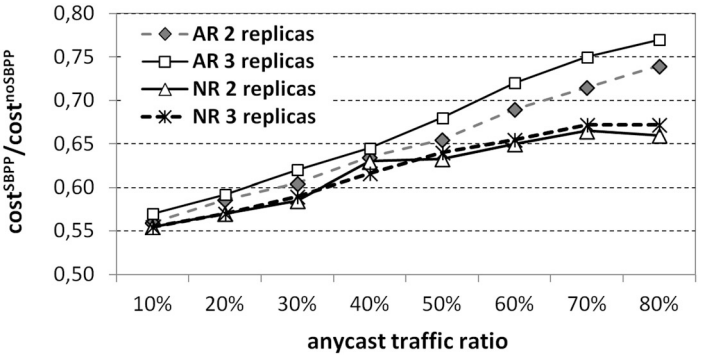

Fig. 8.10 Average cost ratios between SBPP and noSBPP solutions

Table 8.4 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

network nodes. This, in turn, limits the possibility of backup path sharing (following the general backup capacity sharing rule).

As shown in Fig. 8.10, 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 in the number of replica servers, the average path hop count decreases, which implies fewer possibilities of backup capacity sharing.

Table 8.4 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, can 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 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, and the number of replicas, the difference between SBPP and noSBPP scenarios (42%, on average), becomes less visible.

The most crucial 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. 8.33) reflecting only the extra capacity that has to be reserved for backup paths (i.e., the fraction of backup capacity without the 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. 8.11, with the increase of the anycast traffic ratio, the 3 replica/2 replica ratio considering cost and capacity parameters decreases, implying

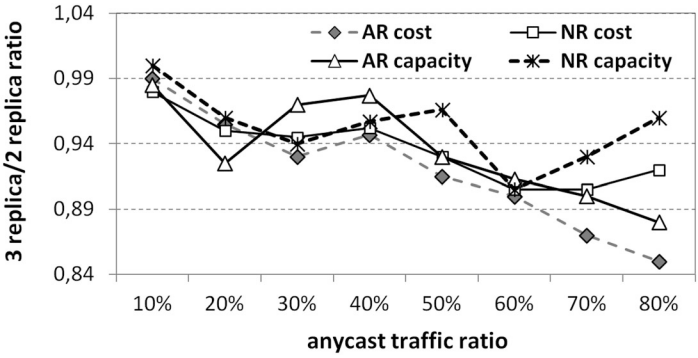

Fig. 8.11 Average ratios of results between 3 and 2 replica servers

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 reducing the average path length (observed with the increase of the anycast traffic ratio). The obtained results confirm the remarkable capacity efficiency of our shared protection scheme at the price of the increased length of backup paths.

8.3.3 Protection of Information-Centric Communications Against Intentional Failures

The majority of proposals available in the literature are related to protection against random failures, being the 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 amounts 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 mainly for networks of irregular topology (obtained due to 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 (8.40). In case of such an uncontrolled growth, network topologies commonly gradually evolve toward irregular ones (as illustrated in Fig. 8.12) with asymptotic power law degree distribution of node degrees k given by formula (8.41) [10]. Examples include, e.g., topology of the Internet with $\gamma = 2.22$ [76].

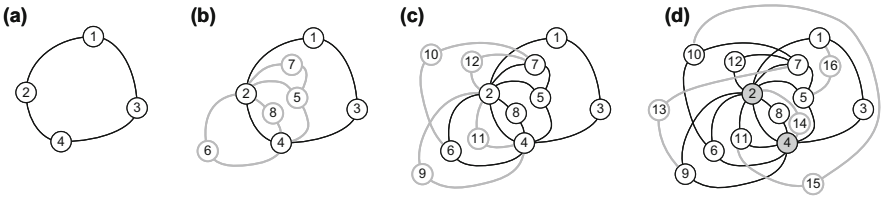

Fig. 8.12 Example evolution of the network topology from (**a**) illustrated in steps (**b**)–(**d**) following the preferential attachment rule

$$\Pi(n) = \frac{\deg(n)}{\sum_j \deg(j)} \tag{8.40}$$

$$P(k) \sim k^{-\lambda} \tag{8.41}$$

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 high risk of being affected by an attacker. Therefore, shortest path routing is not a proper solution for networks of dynamically evolving topologies. This is especially true for the current Internet, which is 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.

This section describes 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 a path protection scheme to ensure the 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.

The 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 network topology changes. 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 (8.42), providing a proper estimation of a node centrality ratio, and thus being an essential indicator of node vulnerability to attacks.

$$BC(n) = \sum_{p \neq q} \frac{sp_n(p,q)}{sp(p,q)} \tag{8.42}$$

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 ξ_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 (8.43). Since the cost of any link incident to a high degree node should be high as well, working paths calculated based on costs (8.43) are thus expected not to traverse such central nodes (as, e.g., nodes 6, 11, and 17 in Fig. 8.13) and, as a result, be less vulnerable to attack-based disruptions.

$$\xi_h = \xi_{i,j} = \frac{BC^*(i) + BC^*(j)}{2} \tag{8.43}$$

where

$$BC^*(n) = \frac{BC(n)}{\max_i BC(i)} \tag{8.44}$$

For the purpose of backup path computations, the cost ζ_h of any network arc a_h is defined here by formula (8.45) as the normalized length of this arc.

$$\zeta_h = \frac{s_h}{\max_i s_i} \tag{8.45}$$

Backup paths are thus established as the shortest ones. Although they are allowed to transit high-degree nodes (as shown in Fig. 8.13), they are used in relatively short periods (for a temporary recovery until the time of manual repair of failed elements).

Similar to Sects. 8.3.1–8.3.2, under anycast routing, working and backup paths may lead to different replica servers to protect against a failure of a replica node (Fig. 8.13).

The ILP model necessary to find the solution to our optimization problem is the same as the Disjoint Replica model from Sect. 8.3.1 defined by formulas (8.14)–(8.30) with the only one exception for the objective function (8.14) here replaced with formula (8.46).

$$\min \ \varphi(x) = \sum_{r \in D} \sum_{h \in A} \xi_h x_{r,h} + \sum_{r \in D} \sum_{h \in A} \zeta_h y_{r,h} \tag{8.46}$$

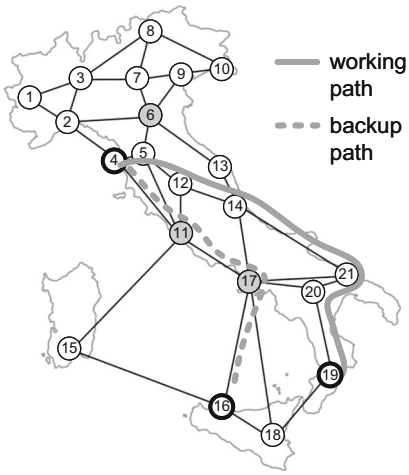

Fig. 8.13 Example anycast routing following the proposed approach; Italian network from Fig. 8.6c

However, the considered problem defined by formulas (8.15)–(8.30) and (8.46) is $\mathcal{NP}$-complete due to $\mathcal{NP}$-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 [57], 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 $\mathcal{NP}$-complete even for a single demand.

The heuristic scheme from Fig. 8.14, 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 [57]. After initialization of Steps 1–3 for each demand, 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 path computations, contrary to the APF scheme, in our approach, to provide nodal disjointness 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 η_i, the cost of any forbidden arc is first increased by the total cost of path η_i calculated based on the matrix of backup link costs $\boldsymbol{c}^j$ (Step 4). However, after finding the next path (η_j) of a demand in Step 5 and detecting that more than one of the 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 η_j in all matrices $\boldsymbol{c}^i$ (calculated based on arc costs from $\boldsymbol{c}^i$), and the execution starts from the beginning (Step 6).

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 $\boldsymbol{c}^1$, $\boldsymbol{c}^2$, ..., $\boldsymbol{c}^k$ of arc costs ξ_h^1, ξ_h^2,..., ξ_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	$\boldsymbol{c}^{tmp}$	auxiliary matrix of arc costs ξ_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 η_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 η_i, then increase the arc cost ξ_h^{tmp} by the total cost ξ^i of η_i in $\boldsymbol{c}^j$.

Step 5 Find path η_j using the Dijkstra's algorithm and the costs matrix $\boldsymbol{c}^{tmp}$.

Step 6 If η_j is not disjoint with the previously found $j-1$ paths of r-th demand then:

- Step 6.1 Increase the costs ξ_h^i of each *conflicting arc*** a_h of η_j by the total cost ξ^j of η_j in all matrices $\boldsymbol{c}^i$. 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 disjointness of the set of k end-to-end paths of a demand, a forbidden arc of η_i is an arc that is incident to any transit node of η_i

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

Fig. 8.14 Heuristic approach to find the set of k end-to-end node-disjoint paths

After several possible conflicts, the method is expected to terminate successfully (as shown later in this section). Our scheme's time complexity depends on the base approach of path computations. If Dijkstra's algorithm from [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, and the time of connection restoration were evaluated using 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).

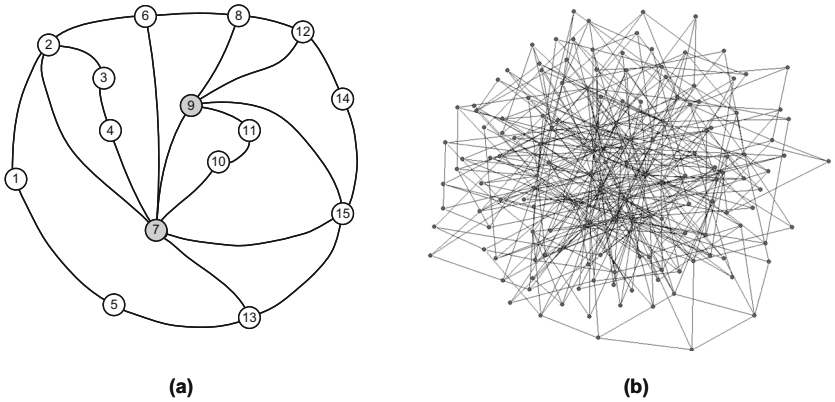

Fig. 8.15 Network topologies used in simulations: ASF Network (**a**) and BA-150 Network (**b**)

The 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. 8.14 for topologies of two irregular networks shown in Fig. 8.15 (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., without sharing 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, respectively.

A single simulation comprised 50 different sets of demands for a given network topology and the number of available replica servers. The probability of node failures was proportional to the values of the normalized betweenness centrality coefficient defined for network nodes by Eq. 8.44.

One of the objectives of the simulations was to evaluate the efficiency of our heuristic method in comparison with the results of ILP modeling. This analysis is presented in Fig. 8.16 for ASF network from Fig. 8.15a (with assumed $\Lambda = 40$ channels available at each network link) in terms of the total link capacity per

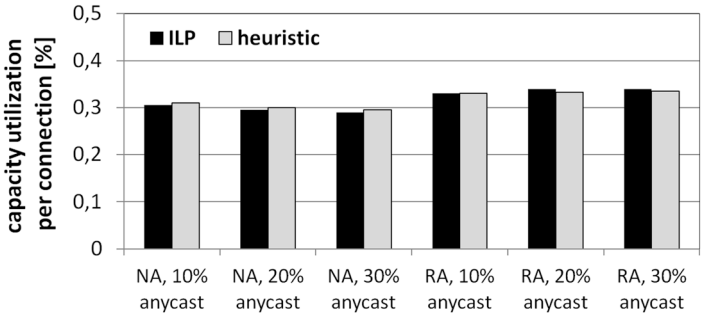

Fig. 8.16 Ratios of total link capacity utilization per connection for ASF network from Fig. 8.15a achieved for different network loads (number of replica servers: 2)

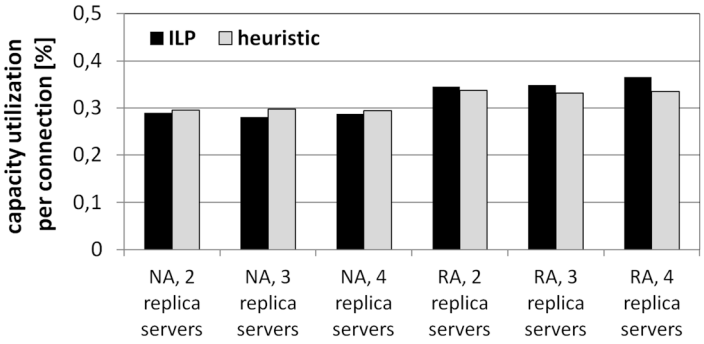

Fig. 8.17 Ratios of total link capacity utilization per connection for ASF network from Fig. 8.15a achieved for different numbers of replica servers (anycast ratio: 30%)

connection necessary to serve the demands as a function of the network load (Fig. 8.16) and the number of replica servers (Fig. 8.17).

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. Our technique sometimes required even less capacity (up to 2.49% less). However, this was an implication of the 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. 8.15b with three replica servers and $\Lambda = 160$ channels available at each link), evaluation was feasible for the heuristic approach only.

For our RA approach, the average length of working paths was up to 2.26 times greater than the common NA scheme (because in the RA scheme, working paths

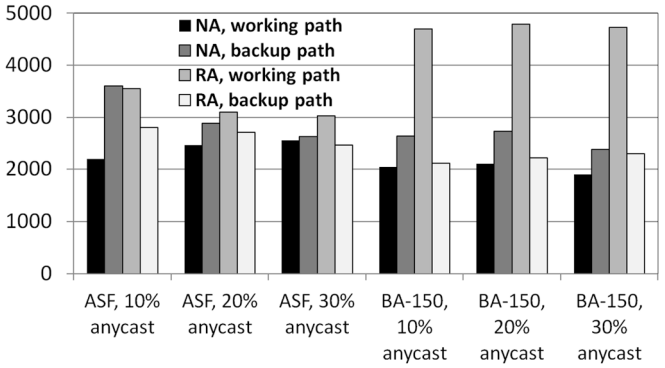

Fig. 8.18 Average length of paths

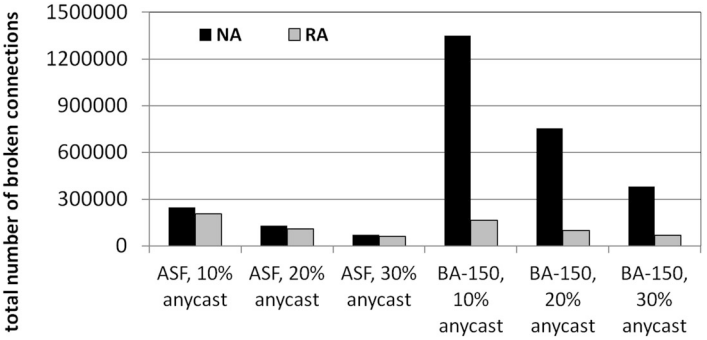

Fig. 8.19 Total number of broken connections

tried to omit high-degree nodes). On the contrary, RA backup paths were about 25% shorter than the respective NA ones (Fig. 8.18).

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. 8.19 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. 8.20).

To conclude, the proposed approach to establishing working paths in a way to omit nodes of a high degree results in a remarkable decrease in the number of connections affected after attacks at a price of only an insignificant increase in the length of working paths. The dynamic properties of our scheme make it a suitable solution at any stage of 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].

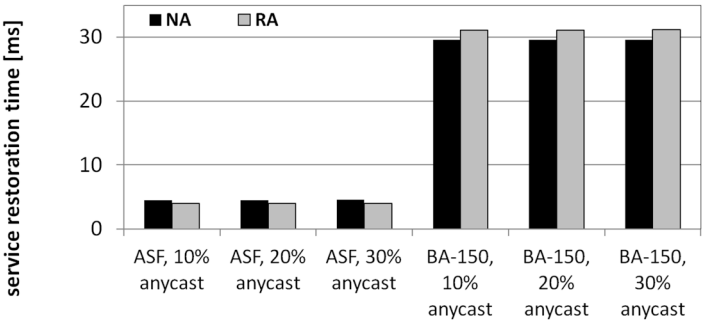

Fig. 8.20 Average service restoration time

8.4 Summary

The diversity of Future Internet desired functionalities, routing paradigms, and challenges threatening the normal operation of any global network altogether make the resilience of FI communications a complex issue. Considered by many to be an important part of a critical infrastructure expected to offer 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 the routing and network resource provisioning problem deployed by us in one of European research projects on Future Internet architecture, called Future Internet Engineering. Next, we focused on the 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 and (3) dedicated protection of flows under attack-based disruptions.

Obtained results confirmed the efficiency of our techniques in assuring the uninterrupted routing of FI demands in differentiated scenarios, including dedicated protection (Sect. 8.3.1), shared protection (Sect. 8.3.2 with the achieved 36% reduction of redundancy ratio, compared to the case of dedicated protection) in random failure scenarios, and a significant improvement in terms of reduction 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. 8.3.3).

References

1. Ahlgren, B., Dannewitz, Ch., 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 08 Mar 2015

3. Akari architecture design project: http://www.nict.go.jp/en/photonic_nw/archi/akari/akari-top_e.html. Accessed on 08 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 Network **28**(3), 36–42 (2014)
6. Álvarez, F., Cleary, F., Daras, P., Domingue, J., Galis, A., Garcia, A., Gavras, A., Karnourskos, S., Krco, S., Li, M.-S., Lotz, V., Mueller, 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. Lecture Notes in Computer Science, vol. 7281. Springer, Berlin (2012)
7. Anderson, T., Peterson, L., Shenker, S., Turner, J.: Overcoming the Internet impasse through virtualization. IEEE Comput. **38**(4), 34–41 (2005)
8. Awerbuch, B., Brinkmann, A., Scheideler, C.: Anycasting in adversarial systems: routing and admission control. Lect. Notes Comput. Sci. **2719**, 1153–1168 (2003)
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: Proceedings of the 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. Cholda, P., Gozdecki, J., Kantor, M., Wielgosz, M., Pach, A.R., Wajda, K., Rak, J.: Provisioning concepts of the IIP Initiative. In: Proceedings of the 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: Proceedings of the 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., Mueller, 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. Lecture Notes in Computer Science, vol. 6656. Springer, Berlin (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: Proceedings of the ACM SIGCOMM'11 Workshop on Information-Centric Networking, pp. 1–6 (2011)
33. Gladysz, J., Walkowiak, K.: Optimization of survivable networks with simultaneous unicast and anycast flows. In: Proceedings of the 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: Proceedings of the 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. Telecommun. Syst. **61**, 235–246 (2016)
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., Mouftah, H.T.: Diverse routing for shared protection in survivable optical networks. In: Proceedings of the IEEE Global Communications Conference (IEEE GLOBECOM'03), vol. 5, pp. 2519–2523 (2003)
41. 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)
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 edn. 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: Proceedings of the 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 Int. 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. **3685**, 442–447 (2005)
50. Mukherjee, B.: Optical WDM Networks. Springer, Berlin (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.: *k*-Penalty: a novel approach to find *k*-disjoint paths with differentiated path costs. IEEE Commun. Lett. **14**(4), 354–356 (2010)
58. Rak, J.: Fast service recovery under shared protection in WDM networks. IEEE/OSA J. Lightwave Technol. **30**(1), 84–95 (2012)
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: Proceedings of the 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 08 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. Networks **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: Proceedings of the 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. Inform. Sci. **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: Proceedings of the 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, Ch.: Content delivery networks: a bridge between emerging applications and future IP networks. IEEE Network **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)