Chapter 3
System- and Element-Related Metrics Useful in the Evaluation of Resilience

Failures of network elements will undoubtedly continue to occur since it is impossible to eliminate all the factors responsible for them. However, as we discuss in this chapter, the scale of the negative consequences of failure events is determined not only by the characteristics of the related challenges (such as their intensity, duration, and area, as, e.g., in the case of heavy rainfall, fire, hurricane) but also follows from the properties of the system architecture such as system topology, location of servers providing services to end users, transmission schemes, etc.

For instance, if transmission of information is configured via shortest paths (which is a common scenario), then due to the topological properties of networked systems, such as the location of a given node in the topology or the number of links attached to that node, certain network nodes tend to switch a greater amount of network traffic and, therefore, are of greater importance than the other nodes. This also means that their failure significantly impacts the provisioning of services to the end users, as many more transmission paths become affected. Similarly, a malicious attack leading to the failure of a server providing a multitude of services may be a direct consequence of the recognition by an attacker of the properties of that node.

Therefore, to assess the potential impact of a failure of a given network element on the functioning of the entire system, it is important to make use of a set of *metrics*, i.e., functions designed to measure either the individual properties of certain elements or of the entire system and its services. Apart from their essential role in assessing system properties during normal operation and failure scenarios, these metrics can also be helpful in all phases of design, deployment, and update/evolution of the networked system architecture.

Understanding the meaning of certain metrics quite often requires at least some level of knowledge on characteristics of individual elements (nodes/links) of the networked system, as well as the architectural properties of the entire system impacting its performance, being the ability of a unit to provide the function it has been designed for [30].

J. Rak, *Resilient Routing in Communication Networks*, Computer Communications
and Networks, https://doi.org/10.1007/978-3-031-64657-7_3

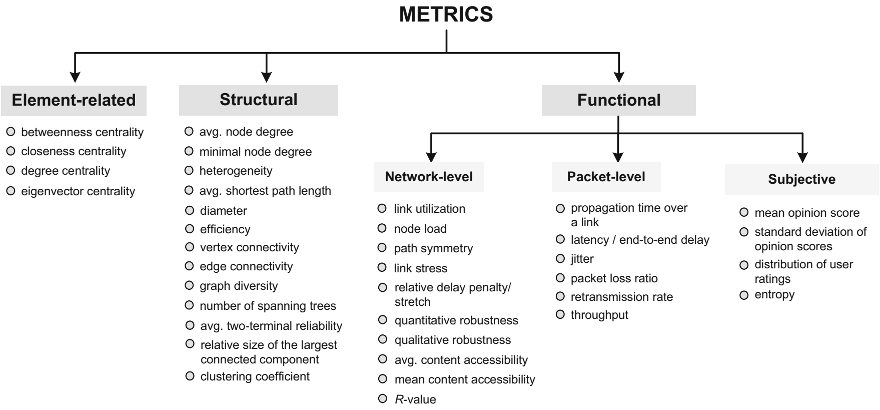


Fig. 3.1 A comprehensive classification for metrics of networked systems and their elements relevant in resilience evaluation

As the set of metrics for networked systems and their elements is relatively large, a particular focus in this chapter is on metrics useful from the perspective of the resilient functioning of a networked system in failure scenarios. In this context, as presented in Fig. 3.1, metrics relevant to evaluating the resilience of networked systems can be broadly divided into three categories: element-related, structural, and functional.

The first group of *element-related metrics* focuses on the properties of individual network elements (nodes/links) following from their existence in the system topology. The *structural metrics*, in turn, refer to the topological properties of the entire system. In contrast, *functional metrics* are used to analyze the system quality of service either at the network level (i.e., *network-level functional metrics*), at the packet level (referred to as *packet-level functional metrics*), or to assess user satisfaction with the service (often called quality of experience—QoE) referred to as the *subjective metrics*.

In the remaining part of this chapter, we first highlight in Sect. 3.1 the standard means of representing the topological properties of a system derived from the graph theory, which are useful in definitions of metrics analyzed later in this chapter. Next, in Sect. 3.2, we discuss the most important metrics dedicated to single elements of the system. Section 3.3 provides information about the most essential structural metrics. In Sect. 3.4, we explain the reasons for the diverse characteristics of system elements, the related irregular character of the system topology, and the resulting potential challenges. In Sect. 3.5, we analyze the major functional metrics, i.e., the ones for the evaluation of system performance at the network level and the packet level, as well as the subjective metrics referring to the satisfaction of users. In Sect. 3.6, we comment on examples of practical applications of the analyzed metrics in common use (e.g., in the configuration of routing protocols) as well as discuss proposals following from research papers for the use of these metrics at virtually every stage of the network system life cycle. Sect. 3.7 concludes the chapter.

3.1 The Formal Representation of Networked Systems Architecture

The architecture of networked systems consisting of a set N of nodes such as switches, routers, servers, etc., interconnected by communication links is commonly defined by graph $G(V, E)$, where V is a set of vertices representing the system nodes, $|V|$ is the number of vertices in G, while E stands for the set of edges of G representing the communication links. A given edge $e_{i,j}$ from E is assumed to interconnect the respective vertices v_i and v_j from V.

Set E of edges often represents *bidirectional network links* enabling transmission in both directions and often characterized by the same capacity $c_{i,j}$ in both directions, as illustrated by graph G_1 in Fig. 3.2a. However, as communication links are *directional* in certain configurations, they are then typically represented by directed arcs $a_h = (i, j)$ from set A (instead of set E). Therefore, in such cases, graph G takes the form of $G(V, A)$. An example representation of a networked system with directional communication links by graph G_2 with directed arcs is provided in Fig. 3.2b.

In general, the structure of any networked system can be defined by graph G at its various abstraction layers, such as the link layer (representing the system topology formed by physical links) or the Internet layer topology (formed by Internet links) [23].

Interconnection of network nodes (represented by a set V of vertices) by communication links represented by set E (or set A) for networks with bidirectional (or directional) links is often defined by the respective *adjacency matrix* $\mathcal{A}$ with elements $\hat{a}_{i,j}$ equal to 1 denoting the existence of communication link from network node i to network node j. Otherwise, $\hat{a}_{i,j}$ values are set to 0. Network nodes i and j are called neighbors if the respective vertices v_i and v_j are adjacent in G, i.e., connected by edge $e_{i,j}$ (or arc $a_h = (i, j)$, respectively).

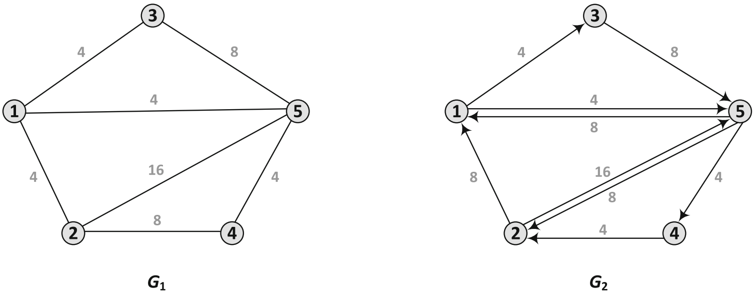


Fig. 3.2 Example graphs G_1 and G_2 representing networked systems with bidirectional and directional communication links, respectively (the numerical values located close to the respective edges/arcs denote the nominal capacity of network links)

Example adjacency matrices for graphs G_1 and G_2 from Fig. 3.2, denoted as $\mathscr{A}_1$ and $\mathscr{A}_2$, are then defined as follows:

$$\mathscr{A}_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad \mathscr{A}_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

It is clear that for networked systems with bidirectional (duplex) links, the respective matrices $\mathscr{A}$ are symmetrical, i.e., such that for every pair of nodes i and j connected by a duplex link, $\hat{a}_{i,j} = \hat{a}_{j,i} = 1$ (and 0, otherwise). This is also the case for matrix $\mathscr{A}_1$ provided for graph G_1 from Fig. 3.2a.

However, for networks with directional (simplex) links, for a given pair of network nodes i and j, transmission is often possible in one way only (e.g., from a given node i to a particular node j, but not vice versa). Therefore, the adjacency matrix for networks with simplex links need not necessarily be symmetrical, as in the case of matrix $\mathscr{A}_2$ above representing the interconnections of network nodes defined by graph G_2 in Fig. 3.2b.

Adjacency matrices can also provide additional information related to network links, such as link nominal capacity. For this purpose, values of $\hat{a}_{i,j}$ are replaced by the respective weights $c_{i,j}$, which leads to the concept of *weighted adjacency matrix* C. For graphs G_1 and G_2 from Fig. 3.2, the respective weighted adjacency matrices C_1 (symmetrical) and C_2 (nonsymmetrical), with weights $c_{i,j}$ denoting the nominal capacities of network links, are defined as follows:

$$C_1 = \begin{pmatrix} 0 & 4 & 4 & 0 & 4 \\ 4 & 0 & 0 & 8 & 16 \\ 4 & 0 & 0 & 0 & 8 \\ 0 & 8 & 0 & 0 & 4 \\ 4 & 16 & 8 & 4 & 0 \end{pmatrix} \qquad C_2 = \begin{pmatrix} 0 & 0 & 4 & 0 & 4 \\ 8 & 0 & 0 & 0 & 16 \\ 0 & 0 & 0 & 0 & 8 \\ 0 & 4 & 0 & 0 & 0 \\ 8 & 8 & 0 & 4 & 0 \end{pmatrix}$$

It is worth noting that the nonsymmetrical character of matrix C for directed graphs may follow not only from the directional nature of arcs representing unidirectional network links but can also refer to different nominal capacities of links in each direction for a given pair of neighboring network nodes. For example, as given in graph G_2 from Fig. 3.2b, the nominal capacity of a link between network nodes 2 and 5 depends on the source/destination of that link and is defined as $c_{2,5} = 16$ and $c_{5,2} = 8$, respectively.

Another way to represent the interconnection of network nodes is via the node–link *incidence matrix* $\mathcal{I}$ providing information on the neighborhood relation of network nodes and links. In this matrix, a given i-th row refers to network node i, while column m is associated with m-th network link. If a link with index m

incident to network node i exists, this is represented by the value of 1 assigned to an element in i-th row and m-th column of $\mathcal{I}$, 0 otherwise.

Example form of matrix $\mathcal{I}_1$ for graph G_1 from Fig. 3.2a based on the following assignment of indices m to graph G_1 edges:

$$\begin{array}{llll} e_{1,2} \rightarrow m = 1 & e_{1,3} \rightarrow m = 2 & e_{1,5} \rightarrow m = 3 & e_{2,4} \rightarrow m = 4 \\ e_{2,5} \rightarrow m = 5 & e_{3,5} \rightarrow m = 6 & e_{4,5} \rightarrow m = 7 & \end{array}$$

as well as the respective *weighted incidence matrix* $\hat{\mathcal{I}}$ is defined as follows:

$$\mathcal{I}_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \qquad \hat{\mathcal{I}}_1 = \begin{pmatrix} 4 & 4 & 4 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 8 & 16 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 4 \\ 0 & 0 & 4 & 0 & 16 & 8 & 4 \end{pmatrix}$$

For networks with directional links, values of elements in matrices $\mathcal{I}$ and $\hat{\mathcal{I}}$ are positive when representing indices m of links directed from given network nodes i and negative for links directed to given nodes i.

Another important structure useful in evaluating the topological properties of networked systems is the *Laplacian matrix* $\mathcal{L}$. Its elements $\mathcal{L}[i, j]$ are defined as given in formula (3.1).

$$\mathcal{L}[i, j] = \begin{cases} d_i, & \text{if } i = j \\ -1, & \text{if } i \neq j \wedge v_i \text{ is adjacent to } v_j \\ 0, & \text{otherwise} \end{cases} \tag{3.1}$$

where d_i is the degree of vertex v_i being the number of its incident edges (arcs).

The elements $\mathcal{L}[i, i]$ located along the main diagonal of $\mathcal{L}$ thus provide information on degrees of vertices v_i, while the other elements of $\mathcal{L}$ store information about the adjacency property of vertices v_i and v_j. For example, for graph G_1 from Fig. 3.2a, the related Laplacian matrix $\mathcal{L}$ is defined as follows:

$$\mathcal{L}_{G_1} = \begin{pmatrix} 3 & -1 & -1 & 0 & -1 \\ -1 & 3 & 0 & -1 & -1 \\ -1 & 0 & 2 & 0 & -1 \\ 0 & -1 & 0 & 2 & -1 \\ -1 & -1 & -1 & -1 & 4 \end{pmatrix}$$

An equivalent definition of $\mathcal{L}$ to the one from formula (3.1) is provided in Chapter 5 of [37] as given in formula (3.2).

$$\mathcal{L} = \Delta - \mathcal{A} \tag{3.2}$$

where Δ is a diagonal matrix with elements $\delta_{i,j}$ defined as given in formula (3.3).

$$\delta_{i,j} = \begin{cases} d_i, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases} \tag{3.3}$$

The Laplacian matrix is used to derive specific metrics for graphs representing the architecture of networked systems (see, e.g., [47]).

3.2 Centrality Metrics for Evaluation of Resilience of Single System Elements

In this subsection, we focus on centrality metrics aimed at quantifying the topological importance of single elements in networked systems. In the related literature, a particular interest is often in analyzing the centrality aspect of system nodes. This is indeed justifiable since communication paths, commonly established as the shortest ones between any pair of end nodes (to reduce the end-to-end transmission delay), typically traverse such "central" nodes. However, this feature also magnifies the negative consequences of failures of such elements. Also, since central nodes switch large amounts of data, they often become targets of malicious human activities. Therefore, correctly identifying the level of centrality of system nodes is crucial in implementing adequate resilience mechanisms.

The most common metrics for the centrality of networked system nodes are based on the degree, betweenness, closeness, and eigenvector topological properties of these elements. Their current form follows from results of the analysis done in the area of social networks (and the related mutual impact of people in graphs of social connections) starting from 50s of the 20th century (see, e.g., the related works of Bavelas [3], Freeman [11], or Albert and Barabási [1]).

Betweenness Centrality

The primary purpose of the *betweenness centrality* (BC) metric defined for a given network node i by formula (3.4) [6, 42] is to reflect the frequency of its involvement in switching the data transmitted along the shortest paths between all possible pairs of end nodes in the system (i.e., acting as a transit node along the shortest paths).

$$bc_i = \sum_{p \neq q} \frac{sp_i(p,q)}{sp(p,q)} \tag{3.4}$$

where:

$sp_i(p, q)$ is the number of the shortest paths between nodes p and q (of the same minimal cost) traversing node i;

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

Also, there exists a normalized version of betweenness centrality with the value of bc_i divided by the total number of pairs of vertices in G (except for vertex v_i), i.e., by $(|V|-1)(|V|-2)$. As discussed in [41], a formula similar to (3.4) can be provided for a given network link (i.e., *link betweenness centrality*) to reflect the importance of that link in making multi-hop connections possible.

Closeness Centrality

Closeness centrality (CC) has been formulated to reflect the distance of a given node i to all the other nodes in the system [6, 41]. Therefore, its evaluation is based on the analysis of the length of the shortest paths between a considered node i and all the other system nodes [41]. Its simplified definition provided, e.g., in [42] based on the analysis of the hop count (i.e., the number of path links of the shortest paths) is given by formula (3.5).

$$cc_i = \frac{1}{\sum_{j \in N \setminus \{i\}} h_{i,j}} \tag{3.5}$$

where $h_{i,j}$ is the number of hops for the shortest path between nodes i and j.

Based on formula (3.5), the higher the cc_i value for a given node i, the closer it is to all other nodes. This property can be useful, e.g., when choosing a location for system services, because services located in nodes characterized by high closeness centrality values are closer to end users and, therefore, easily accessible (due to low transmission delay values). An important observation is that nodes characterized by high closeness centrality values are also typically located close to other nodes of high closeness centrality [41].

A normalized version of formula (3.5) assumes multiplication of cc_i by $|V|-1$.

Degree Centrality

Degree centrality (DC) is considered as one of the simplest metrics for the importance of a network node. It is defined based on the degree of node i as the number of system nodes being direct neighbors of that node (i.e., connected by a direct link) [46]. Following [6], degree d_i of node i can be determined using the adjacency matrix $\mathcal{A}$ as given in formula (3.6).

$$d_i = \sum_{j=1}^{|V|} \hat{a}_{i,j} \tag{3.6}$$

Therefore, the importance of node i measured by its degree centrality d_i grows linearly with the increase of its degree [41]. This property remains well in line with the former observation that higher-degree system nodes (such as switches) commonly process larger data volumes. Also, in the case of failures of nodes characterized by high values of degree centrality, services provided to a large group of users are likely to become affected as well.

Concerning real architectures of networked systems, degree centrality values are often different for different nodes. Also, it is common that only a small subset of system nodes is characterized by high-degree centrality values.

It is worth mentioning that a normalized variant of node degree centrality also exists, where d_i is divided by the maximum possible degree of a node, i.e., by $|V|-1$.

Eigenvector Centrality

The purpose of the *eigenvector centrality* (EC) metric is to evaluate the influence of a given node in the network. Following [6], eigenvector centrality ec_i of node i is defined as the value of the ith element of the eigenvector referring to the largest eigenvalue λ_1 calculated for the adjacency matrix $\mathcal{A}$.

$$ec_i = \frac{1}{\lambda_1} \sum_{k=1}^{|V|} \hat{a}_{i,k} ec_k \tag{3.7}$$

Therefore, eigenvector centrality is another metric of the centrality of nodes, according to which a node should be considered an important one if it is a direct neighbor of another important node [41, 45]. Indeed, the value of ec_i reflects the number of direct, 2-hop, 3-hop (and so on) neighbors of node i [6].

For two example network topologies shown in Fig. 3.3, the respective normalized values of node centrality parameters are provided in Tables 3.1 and 3.2.

As can be seen in Tables 3.1 and 3.2, the values of node centrality metrics are generally consistent with each other, i.e., the highest value of one of them, say degree centrality (e.g., for node 7 for the NSF-14 network topology): $d_7 = 0.31$ in

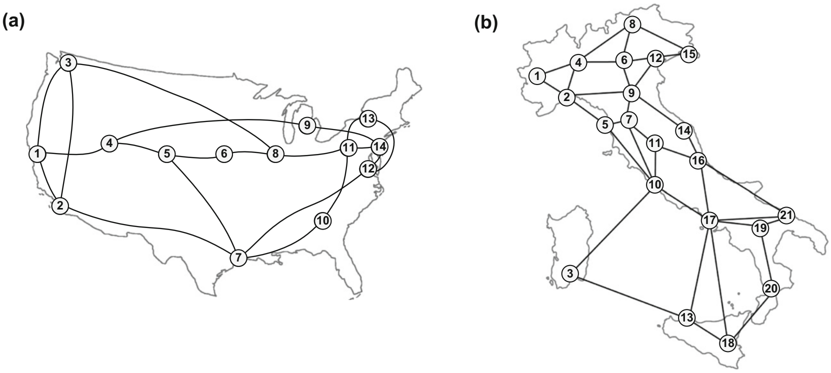


Fig. 3.3 Example topologies of (**a**) NSF-14 and (**b**) Italian-21 networks

Table 3.1 Values of normalized centrality parameters for the NSF-14 network nodes

Node index (i)	1	2	3	4	5	6	7	8	9	10	11	12	13	14
bc_i	0.06	0.08	0.07	0.11	0.12	0.03	0.24	0.15	0.06	0.03	0.19	0.10	0.01	0.11
cc_i	0.43	0.46	0.45	0.45	0.48	0.42	0.54	0.48	0.42	0.45	0.5	0.46	0.39	0.46
d_i	0.23	0.23	0.23	0.23	0.23	0.15	0.31	0.23	0.15	0.15	0.31	0.23	0.15	0.23
ec_i	0.29	0.32	0.29	0.24	0.26	0.18	0.37	0.27	0.17	0.23	0.32	0.28	0.20	0.26

Table 3.2 Values of normalized centrality parameters for the Italian-21 network nodes

Node index (i)	1	2	3	4	5	6	7	8	9	10	11	12	13	14
bc_i	0.00	0.17	0.03	0.05	0.15	0.08	0.16	0.02	0.33	0.31	0.02	0.08	0.02	0.14
cc_i	0.30	0.38	0.33	0.32	0.40	0.34	0.43	0.28	0.43	0.44	0.38	0.33	0.31	0.39
d_i	0.10	0.20	0.10	0.20	0.15	0.20	0.20	0.15	0.25	0.25	0.15	0.15	0.15	0.10
ec_i	0.10	0.20	0.15	0.16	0.23	0.18	0.30	0.11	0.26	0.36	0.25	0.14	0.20	0.15
Node index (i)	15	16	17	18	19	20	21							
bc_i	0.01	0.17	0.30	0.05	0.05	0.01	0.02							
cc_i	0.26	0.40	0.40	0.31	0.30	0.25	0.34							
d_i	0.10	0.20	0.30	0.15	0.15	0.10	0.15							
ec_i	0.07	0.28	0.39	0.19	0.20	0.10	0.23							

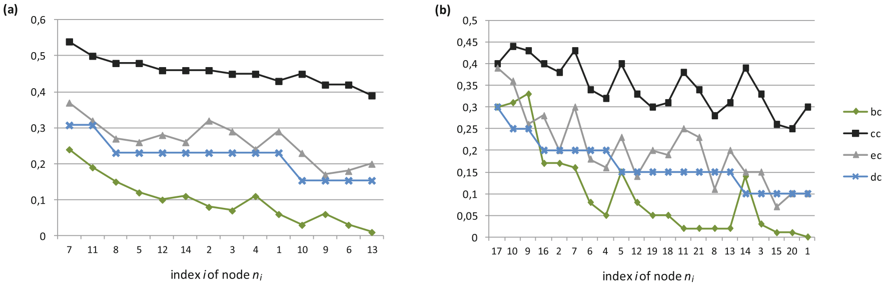


Fig. 3.4 Correlation of node centrality metrics for (**a**) NSF-14 and (**b**) Italian-21 network topologies

Table 3.1 also implies high values of the other three centrality metrics: $bc_7 = 0.24$, $cc_7 = 0.54$ and $ec_7 = 0.37$.

A detailed analysis of the correlation of node centrality coefficients is presented for both considered network topologies in Fig. 3.4, where nodes are sorted descending their degrees. A general observation from Fig. 3.4 is that, with the decrease of the network node degree, betweenness centrality values decrease the most rapidly among all considered centrality metrics. Therefore, to identify the central nodes that have the most remarkable contribution to end-to-end transmission, betweenness centrality, among all considered node centrality metrics, turns out to be the most proper one.

3.3 Structural Metrics for Evaluation of Resilience of Networked Systems Architectures

In this section, we highlight definitions and discuss the properties of the selected metrics applicable in the evaluation of the resilience of the entire structure of a networked system. Therefore, they are often referred to as structural metrics. Our analysis begins with metrics related to the degrees of network elements. Next, we consider metrics related to communication paths in the system. The last group of structural metrics analyzed in this section covers selected advanced aspects related to the topology of the networked system.

Average Node Degree

The *average node degree* (k) [41] is a simple measure of the density of the network topology. It provides information on the average number of links incident to a network node. Based on data stored in the adjacency matrix $\mathcal{A}$, this metric, here denoted by d_{avg}, can be calculated as given in formula (3.8).

$$d_{\text{avg}} = \frac{\sum_{i=1}^{|V|} \sum_{j=1}^{|V|} \hat{a}_{i,j}}{|V|} \tag{3.8}$$

Coefficient d_{avg} takes values from 0 (in the case of a system consisting only of isolated nodes) to $|V|-1$ (in the case of a system characterized by a topology of a full graph representing the architecture in which each network node has direct links to all the other nodes).

Since node degree values provide information on the maximum number of disjoint communication paths sourced from/destined to a given node, they are crucial in resilient routing, as they impact the ability of a system to set up multiple disjoint paths. The lower bound on this ability for the entire system is indeed constrained by the minimal node degree in the considered system.

Minimal Node Degree

The *minimal node degree* (d_{min}) is the minimal value of degrees of nodes in the networked system.

$$d_{\mathrm{min}} = \min_{i:v_i \in V} d_i \tag{3.9}$$

Indeed, to deploy a resilient routing scheme in the system involving k disjoint paths (for protection against a simultaneous failure of k-1 nodes), a necessary condition is that each network node i should be characterized by its degree of at least k, meaning that d_{min} of the entire networked system should be at least equal to k.

Heterogeneity

Heterogeneity has been introduced as a metric of inhomogeneity of node degrees. Following [41], it is defined as the standard deviation σ_{deg} of degrees of nodes in the system divided by the average node degree (d_{avg}), as given by formula (3.10).

$$h = \frac{\sigma_{\mathrm{deg}}}{d_{\mathrm{avg}}} \tag{3.10}$$

In general, the smaller the values of h (i.e., the closer they are to 0), the greater the homogeneity of the node degrees, and thus, the greater the robustness of the entire networked system architecture to failures of its elements.

Concerning the example topologies of NSF-14 and Italian-21 networks from Fig. 3.3, the related values of the average node degree, minimal node degree, and heterogeneity metrics are provided in Table 3.3.

In particular, the minimal value of node degree for both networks is equal to 2.00, which implies that for both networks, deploying resilient routing schemes for any pair of end nodes based on pairs of node-/link-disjoint paths may be possible.

Table 3.3 Values of structural metrics referring to degrees of network nodes for the example NSF-14 and Italian-21 network topologies from Fig. 3.3

Network	Average node degree	Minimal node degree	Heterogeneity
NSF-14	2.86	2.00	0.23
Italian-21	3.33	2.00	0.33

Topologies of systems with the minimal node degree of 2 are often called "two-connected." However, neither of the considered NSF-14 and Italian-21 network topologies can utilize schemes based on sets of three (or more) disjoint paths for a pair of nodes, as the degrees of some nodes in these networks are only equal to 2.

Concerning the value of the heterogeneity metric, it is lower for the NSF-14 network topology, implying that the topology of that network is more regular (relative differences of node degree values are lower than for the topology of the Italian-21 network).

Average Shortest Path Length

Average shortest path length (l) coefficient [40] provides information on the average distance (or the number of links) along the shortest paths calculated considering all pairs of source and destination vertices v_s and v_t in G, as given in formula (3.11).

$$l = \sum_{s,t:v_s,v_t \in V} \frac{hc_{s,t}}{|V| \cdot (|V| - 1)} \tag{3.11}$$

where $hc_{s,t}$ is the number of links (hop count) in the shortest path between vertices v_s and v_t.

It is worth noting that the calculation of the number of links in the shortest path instead of their length in the Cartesian sense is often applied due to a common assumption of the unitary length of all links in the system or follows simply from the assumption to focus on the number of hops in the shortest path. Another observation is that formula (3.11) remains valid also for directed graphs, where the number of links of the shortest path from v_s and v_t can be different from that for a reverse path from v_t and v_s.

As the number of nodes and links traversed by the shortest path is correlated with the risk of path failure due to failures of system elements (see the analysis from Chapter 2 of this book), the average shortest path length metric is useful in the resilience context, especially in terms of determining the average resistance of communication paths in the system to failures.

Diameter

Diameter of a network [46] is commonly defined as the minimum hop count between the two most distant nodes in the system. Therefore, to calculate the diameter of a networked system, the numbers of links of the shortest paths between every pair of system nodes s and t (i.e., $hc_{s,t}$) need to be first calculated, and next, the maximum of these values should be returned as provided by formula (3.12).

$$l = \max_{s,t:v_s,v_t \in V} hc_{s,t} \tag{3.12}$$

Similar to the average shortest path length, diameter (being, in fact, the "maximum shortest path length") can provide useful information about the related maximum risk of affection of a communication path in the system by failures of system elements.

Efficiency

Efficiency of a networked system focuses on the inverse values of the number of links of the shortest paths in the networked system. It can be, therefore, used to evaluate how quickly information can be transmitted between any pair of end nodes s and t in the system. Following [27, 41], it can be defined as the normalized sum of reciprocals of values of hop counts $hc_{s,t}$ for the shortest paths between all pairs of system nodes as given by formula (3.13).

$$\epsilon = \frac{\sum_{s,t:v_s,v_t \in V} \frac{1}{hc_{s,t}}}{|V| \cdot (|V| - 1)} \tag{3.13}$$

Therefore, the higher the value of ϵ, the shorter the communication paths are in the system, and, thus, the more efficient (i.e., faster) the delivery of information to the destination nodes, as well as the smaller the set of network elements traversed by a given path (i.e., the higher is the resilience of paths).

Vertex Connectivity

Following [41], *vertex connectivity*, $\kappa(G)$, is defined as the smallest number of vertices of graph G, the removal of which causes disconnection of system elements (i.e., partitioning of the system architecture into separated zones). As services are often provided by dedicated servers, such system partitioning (e.g., implied by failures due to many reasons discussed earlier in this book) might indeed bring severe consequences for many end users of not having access to these services.

Values of $\kappa(G)$ range from 1—as, e.g., in the case of network graphs being trees (see the example network topology in Fig. 3.5a) to $|V|-1$ for full graphs—see Fig. 3.5b. Therefore, $\kappa(G)$ can help assess the robustness of the system architecture to simultaneous failures of multiple network elements.

Concerning the topologies of two real networks analyzed earlier in this chapter, the related vertex connectivity $\kappa(G)$ is equal to 2 for both networks (see Fig. 3.6). A general observation following from the analysis of properties of different network graphs is that the more irregular the topology of a networked system, the lower the number of nodes, the removal of which partitions the system.

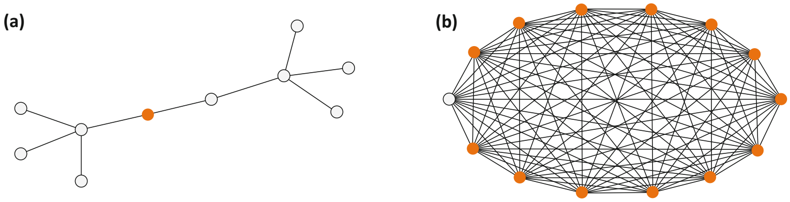


Fig. 3.5 Example network topologies characterized by vertex connectivity $\kappa(G)=1$ (graph (**a**)), and $\kappa(G)=|V|-1$ - graph (**b**) (the example subsets of vertices, the removal of which causes graph partitioning, are marked in orange)

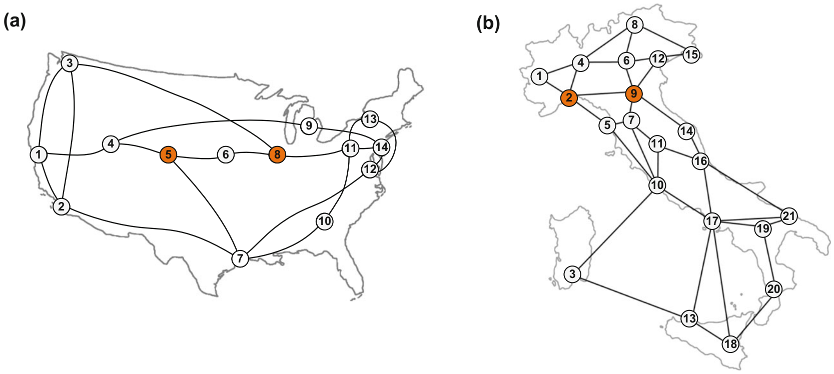


Fig. 3.6 Analysis of vertex connectivity $\kappa(G)$ for NSF-14 and Italian-21 network topologies (the example subsets of vertices, the removal of which causes graph partitioning, are marked in orange)

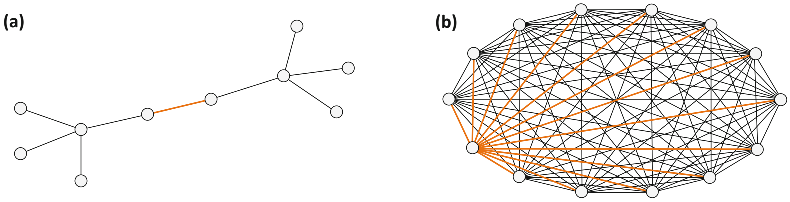


Fig. 3.7 Example network topologies characterized by edge connectivity $\lambda(G)$=1 (graph (**a**)), and $\lambda(G)$=$|V|$−1 - graph (**b**) (the example subsets of edges, removal of which causes graph partitioning, are marked in orange)

Edge Connectivity

Edge connectivity—$\lambda(G)$—is defined similarly to vertex connectivity as the smallest number of edges from G whose removal leads to system partitioning. Similar to vertex connectivity, edge connectivity values range between 1 (for tree graphs) and $|V|$-1 for full graphs, as illustrated in Fig. 3.7. As simultaneous failures of multiple links of the system can also take place (e.g., due to fires causing the burning of optical wired cables or cuts of links during dig-ups carried jointly in the same duct), $\lambda(G)$ provides valuable information on the resistance of the system architecture in such scenarios.

As illustrated in Fig. 3.8, for the NSF-14 topology and Italian-21 topology, $\lambda(G)$ equals 2. Similar to vertex connectivity, edge connectivity is generally higher for regular topologies and lower for topologies characterized by higher heterogeneity values.

Graph Diversity

According to [39, 41], *graph diversity* is a metric of the frequency of traversing the same communication links and transit nodes by communication paths between given pairs of end nodes s and t. This metric is defined concerning all possible pairs

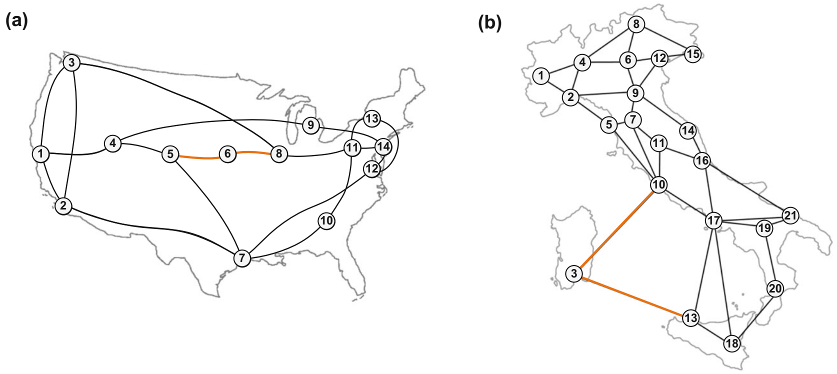


Fig. 3.8 Illustration of edge connectivity $\lambda(G)$ for NSF-14 and Italian-21 network topologies (the example subsets of edges, the removal of which causes graph partitioning, are marked in orange)

of end nodes s and t in the system and is based on values of the effective path diversity, each for a given pair of end nodes. In turn, the values of the effective path diversity follow from the values *path diversity* provided for paths P_i in the context of the respective shortest path P_0 (shortest in terms of the hop count).

For a given pair of end nodes, s and t, the related path diversity metric for a given arbitrary path P_i is defined in relation to the shortest path P_0 between these end nodes as given in formula (3.14).

$$D(P_i) = 1 - \frac{|P_i| \cap |P_0|}{|P_0|} \tag{3.14}$$

where $|P|$ denotes the number of links and transit nodes used by path P.

Therefore, $D(P_i)$ changes from 1 (if paths P_i and P_0 do not share any elements except for the end nodes) to 0 (if paths P_i and P_0 are identical, i.e., traverse the same set of links).

Following [39], the effective path diversity can be determined as an aggregation of path diversities for a selected set of paths between a given pair s and t of end nodes. Finally, the value of the graph diversity metric can be calculated as the average of all effective path diversity values determined for all pairs of end nodes.

Higher values of graph diversity indicate a greater level of system robustness.

Number of Spanning Trees

This metric calculates the total number of distinct spanning trees (i.e., trees that include all nodes of the networked system) that exist for a given network graph [25, 41].

In general, the analysis of the number of spanning trees can provide useful information on the ability of a system to switch to another configuration (i.e., based on another spanning tree) in scenarios of network element failures. This can help restore affected services quickly (see, e.g., the scheme proposed in [24]).

Average Two-Terminal Reliability

The *average two-terminal reliability* ($ATTR$) provides information on the probability that a randomly chosen pair of nodes s and t is connected, meaning a communication path exists between them in the network graph. Following [41], it is defined as the total number of pairs of nodes in all system components of the system divided by the total number of node pairs in the system. Therefore, for fully connected systems (see, e.g., Fig. 3.3), the value of ATTR is equal to 1. Otherwise, in the case of systems partitioned into several separate components, the value of ATTR belongs to the (0,1) range.

For example, for the topology shown in Fig. 3.9a, $ATTR_{Ga} = 111/231 \approx 0.48$. This follows from the fact that topology from Fig. 3.9a consists of two separate components: the upper one with ten nodes and the lower one with 12 nodes. Therefore, the number of connected node pairs is equal to 10·9/2 (the upper part) + 12·11/2 (the lower part) $= 45 + 66 = 111$, while the total number of node pairs is $22 \cdot 21/2 = 231$.

The topology from Fig. 3.9b also consists of two separate components. However, one of them is significantly smaller than the second one. They consist of 3 and 12 nodes, respectively. The number of connected node pairs is equal to 3·2/2 (the upper part) + $12 \cdot 11/2$ (the lower part)=3+66=69, while the total number of node pairs is $15 \cdot 14/2 = 105$. The value of $ATTR_{Gb}$ is, therefore, equal to $69/105 \approx 0.66$, which is higher than $ATTR_{Ga}$.

Relative Size of the Largest Connected Component

The *relative size of the largest connected component* ($rLCC$) metric is defined as the ratio of the number of nodes of the largest connected cluster of the system and the total number of system nodes [6].

Values of *rLCC* metric are generally positively correlated with ATTR values. For the example topologies from Fig. 3.9 with the related ATTR values: $ATTR_{Ga} \approx 0.48$ and $ATTR_{Gb} \approx 0.66$, the related values of $rLCC$ are: $rLCC_{Ga} = 12/22 \approx 0.55$ and $rLCC_{Gb} = 12/15 = 0.80$.

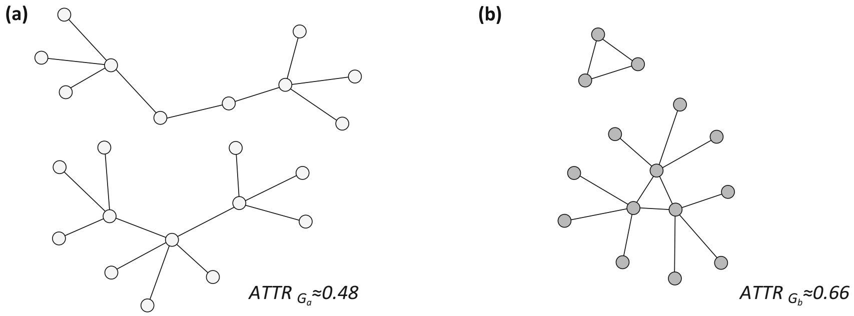


Fig. 3.9 Examples of topologies of two systems to illustrate ATTR properties

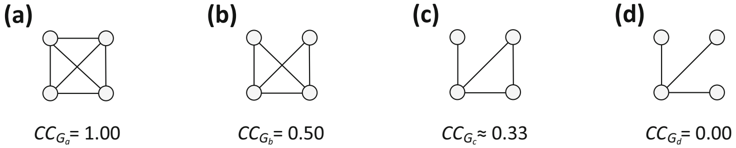


Fig. 3.10 Examples of four topologies for illustration of CC properties

Clustering Coefficient

The *clustering coefficient* (CC) has been proposed to evaluate the scale of cluster formation by nodes in the system topology [44]. This follows from a general observation that in the case of numerous real-world network topologies, system nodes frequently form tightly connected subsets (i.e., with either direct links or very short paths between node pairs in such groups).

The clustering coefficient for the system topology is evaluated based on the identification of triplets of nodes, i.e., groups of three nodes with direct links between them. Triplets can be either "open," i.e., formed by three vertices connected by two edges, or "closed," i.e., with three vertices connected by three edges. Three closed triplets, each centered at a different node, form a triangle.

The clustering coefficient is defined for a system topology as the ratio of the number of closed triplets over the total number of open and closed triplets [26]. Therefore, the cc parameter values range from 0 to 1. Fig. 3.10 presents example four topologies with the respective values of the clustering coefficient.

Concerning the topologies of real-world networked systems analyzed in this chapter, the clustering coefficients of the NSF-14 and Italian-21 topologies from Fig. 3.3 are equal to 0.071 and 0.278, respectively.

3.4 Reasons for Diverse Characteristics of System Elements

The structure of networked systems naturally evolves over time. This, in particular, means:

- Replacement of system nodes such as computing and storage nodes, communication links, and network nodes including, e.g., switches, routers, etc., by elements characterized by higher performance. Concerning network nodes, it is essential to mention that the new ones are commonly characterized by more communication ports than the ones being replaced.
- Addition of new elements to the system, increasing the size of the system and, therefore, raising its complexity.

It is also essential to notice that when adding a new element to the system (say, a network node), it is natural to link it to the existing ones characterized by many communication ports and, generally, by higher performance. By linking new elements to high-performance core nodes, one can thus fully benefit from the nominal capabilities of new elements not being bottlenecked by their neighbors' limitations.

When analyzing the related evolution of the system topology graph, we can equivalently say that when adding new vertices to the graph, it is more probable to link a new vertex with an existing one of high rather than low degree. This, in turn, forms the basis of the *preferential attachment rule* provided by Barabási and Albert in [2] defining the dependency between the probability $\Pi(v_i)$ that the existing node represented by vertex v_i in the topology graph will be linked to a new node as given in formula (3.15).

$$\Pi(v_i) = \frac{d_i}{\sum_j d_j} \tag{3.15}$$

As illustrated in Fig. 3.11, such an uncontrolled growth of the structure of a networked system can lead to system topologies being highly irregular, i.e., characterized by a high diversity of node degrees, often taking the power law asymptotic form characteristic to the so-called *scale-free networks* [2].

As can be seen in Fig. 3.11d, for nodes of high degree (the so-called *central nodes*—e.g., nodes 2 and 4), the distance to other high-degree nodes is often small, which follows from another property of scale-free structures, according to which vertices tend to cluster together in groups.

As discussed in Sect. 3.2 in this chapter, high-degree nodes often serve a significant share of network traffic. This is due to their high performance and their "central" location in the system topology. Therefore, their potential failure may lead to severe consequences for many end users, which, in turn, magnifies the risk of possible malicious activities aimed at such elements and raises the need for even more advanced protection mechanisms.

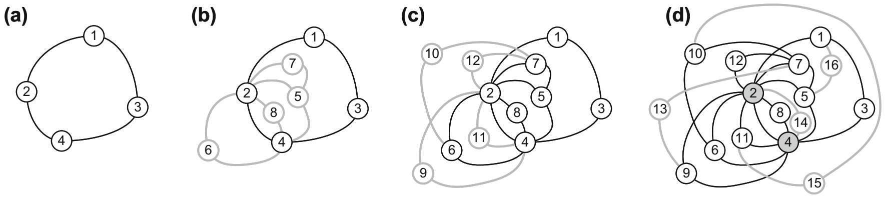


Fig. 3.11 Example illustration of the growth of a system topology following the preferential attachment rule

3.5 Functional Metrics for Networked Systems Resilience Evaluation

In this section, we highlight the selected metrics aimed at evaluating the performance of a networked system both in the case of the correct functioning of all system elements and in scenarios of failures. These metrics can be generally divided into network-level (i.e., focusing on the performance of system elements and multi-hop communication paths), packet-level (i.e., addressing the QoS features related to the transmission of packets), and subjective (i.e., designed to evaluate the performance of system services perceived by end users).

3.5.1 Network-Level Metrics

We start by highlighting the basic metrics for the operation of network elements referring to their involvement in multi-hop transmission. Next, we focus on the performance-related characteristics referring to communication paths, which are related mainly to the overall transmission delay and the probability of a successful setup of communication paths. Finally, we elaborate on network-level performance metrics for more advanced transmission configurations like anycast. We conclude this part by focusing on a selected complex metric aggregating the properties of a set of other metrics.

Link Utilization
Link utilization metric provides information on the percentage of the total (i.e., nominal) capacity used for data transmission [7]. It can refer to either the fraction of link capacity reserved in advance for serving all flows passing through that link (as in the case of allocation of channels of wired links in optical transport networks) or to the instant usage (at time t) of link resources in packet-switched systems.

Node Load
Following [32], *node load* metric has been proposed to measure node importance in overlay networks. It provides information on the number of overlay links passing through a given physical node. The higher the value of node load, the more overlay links get affected due to a failure of that physical node.

Path Symmetry
Following [23, 32], *path symmetry* (PSY) aims to measure the symmetry of paths between source and destination nodes s and t. It focuses on analyzing the end-to-end latency (expressed by the round trip time) and the hop count for the related forwarding and reverse paths, as given in formula (3.16).

$$PSY = \frac{hc}{hc'} \cdot \frac{RTT_{min}}{RTT'_{min}} \tag{3.16}$$

where hc and RTT_{min} denote the hop count and the lowest round trip time for packets concerning the forwarding path, while hc' and RTT'_{min} have the same meaning for the reverse path.

In the ideal case (i.e., when both paths are entirely symmetric), PSY=1. Otherwise, $PSY < 1$ denotes a longer reverse path, while $PSY > 1$ implies a longer forwarding path.

For the example configuration of two paths (i.e., forwarding and reverse), as illustrated in Fig. 3.12, we have hc=3 and hc'=5. Assuming that RTT_{min}= 75ms while RTT'_{min}= 100ms, the value of *PSY* is equal to (3/5)·(75/100)=0.45.

Link Stress

The *link stress* metric helps evaluate the efficiency of overlay networks, as it calculates the number of times packets traverse the same physical link [32].

Relative Delay Penalty/Stretch

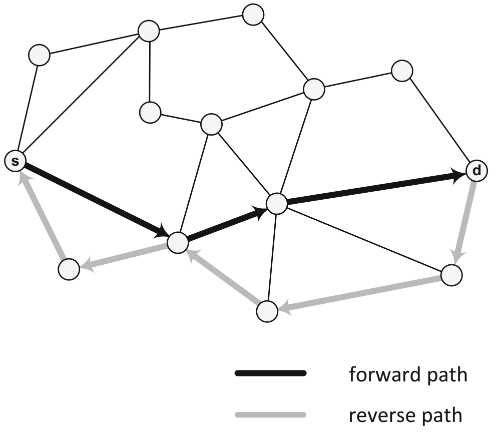
Relative delay penalty/stretch is another measure for evaluating the efficiency of overlay networks. It is defined as the time needed for a packet to be transmitted end-to-end (from node s to node t) via the overlay path consisting of overlay links divided by the time needed when transmitting this packet between the same pair of end nodes, however, measured directly in the underlying transport network [32].

For example, as illustrated in Fig. 3.13, a path in the overlay network between nodes B and H is provided by three virtual links: (B,C), (C,F) and (F,H). In particular:

- Virtual link (B,C) is established in the physical network via path (B,b,d,c,C) of the total delay equal to 79.
- Virtual link (C,F) is established in the physical network via path (C,c,d,e,f,F) of the total delay equal to 114.
- Virtual link (F,H) is established in the physical network via path (F,f,h,H) of the total delay equal to 49.

Therefore, the overall transmission delay between nodes B and H in such a configuration equals $79 + 114 + 49 = 242$. However, a path established between

Fig. 3.12 Example different forward and reverse paths implying the value of PSY different than 1



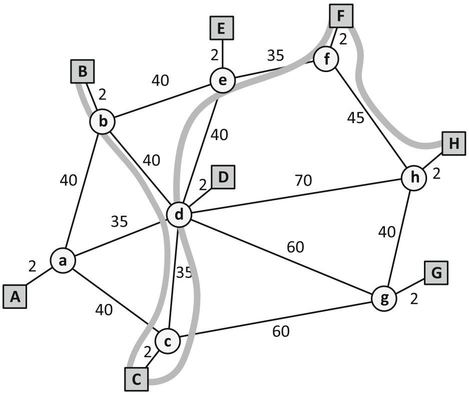


Fig. 3.13 Example of the overlay network (values next to links denote their nominal delay)

nodes B and H directly in the physical network without any intermediate forwarding in the overlay network would be (B,b,d,h,H), and its overall delay would be 114. Therefore, the relative delay penalty (stretch) of such a configuration equals 242/114≈2.12, meaning that the overlay configuration is at least twice as costly as the original one involving transit processing only at the physical network.

Quantitative Robustness

The *quantitative robustness* metric ($QNRM$) is proposed in [28] to evaluate the efficiency in establishing connections in a given time step t as the fraction of the number of established connections to the total number of connections that should have been established at time step t. For longer intervals of interest, the respective average value of QNRM over all consecutive time steps t_i should be determined.

Qualitative Robustness

The *qualitative robustness* metric ($QLRM$) is introduced in [28] to determine the variation of QoS parameters for a broad range of occurrences of impairments (including random attacks, targeted attacks, dynamic epidemical failures, and dynamic periodical failures). It is focused on the analysis of the average shortest path length (ASPL) and is defined as the quotient of the standard deviation of ASPL and ASPL itself divided by the analogous quotient obtained in the scenario of occurrence of a given impairment.

Average Content Accessibility

The metric of the *average content accessibility* (ACA) is proposed to evaluate the possibility of delivering the anycast traffic in scenarios of massive failures implied by disaster events [33]. Generally, this feature is associated with the design problem of locating replica servers in a way that allows the end users to receive information from at least one replica server in post-disaster periods.

Mean Content Accessibility

As discussed in [32, 33], the *mean content accessibility* (μ-ACA) is designed to evaluate the robustness of the networked system concerning the delivery of anycast traffic by taking into consideration a broad range of disasters. Therefore, it can be viewed as an extension of the average content accessibility metric.

R-value

Following [29], the *R-value* metric is defined as the weighted average of values of n other metrics of robustness, as given in formula (3.17).

$$R = \sum_{k=1}^{n} s_k \cdot t_k \tag{3.17}$$

where s_k and t_k denote the weight and the value of k-th metric, respectively ($\sum_{k=1}^{n} s_k = 1; t_k \in [0, 1]$).

3.5.2 Packet-Level Metrics

Packet-level metrics are useful in measuring the quality of transmission in packet-switched networks. This set of metrics focuses mainly on the aspects of *quality of service* (*QoS*) defined in [18] as the "totality of characteristics of a telecommunications service that bear on its ability to satisfy stated and implied needs of the user of the service." The set of major QoS characteristics comprises subjective parameters such as packet loss, bit rate, throughput, transmission delay, and jitter analyzed in scenarios of normal network operation and in post-failure periods when ensuring the assumed level of service evaluated by these metrics can be particularly difficult. In particular, concerning the failure scenarios, the following metrics are essential.

Propagation Time over a Link

Propagation time over a link is a metric of time for a packet necessary to travel via the considered link [32].

Latency/End-to-End Delay

The *latency* (*end-to-end delay*) metric [7] is used to determine the total propagation time for a message to travel via all consecutive links of the transmission path between the source and destination nodes s and t (i.e., the sum of the propagation time values over all consecutive links of a path).

Jitter

Jitter is a metric of the variation of latency likely to occur, e.g., due to changes in queueing/switching time at network nodes due to fluctuations in traffic intensity [32].

Packet Loss Ratio

Packet loss ratio metric is used to measure the fraction of packets that are not received correctly (i.e., received with errors or not received) at the destination node divided by the total number of transmitted packets in a given observation time window [32].

Retransmission Rate

The *retransmission rate* metric is used to evaluate the ratio of retransmitted packets over the total number of transmitted packets in a given observation time window for a certain pair of end nodes of transmission.

Throughput

The *throughput* metric provides information on the nominal message delivery rate via a given link. Depending on the environmental (propagation) properties (e.g., of wireless links) varying over time, throughput value is prone to fluctuations [35].

Generally, the values of almost all the above metrics will likely deteriorate in post-failure periods. This refers particularly to the increase of values of metrics such as latency, jitter, packet loss ratio, and retransmission rate, which, in fact, reflects difficulties of the networked system in failure scenarios (e.g., due to longer transmission paths and worse propagation characteristics). In the case of the last parameter (i.e., throughput), its deterioration denotes a decrease of its value, e.g., under adverse weather conditions such as dense fog in free-space optical networks—FSO [22].

3.5.3 Subjective Metrics

Subjective metrics are used to evaluate the performance of system services perceived by end users. Therefore, they help assess *quality of experience* (*QoE*), being largely subjective and integrating user perception, experience, and expectations [10]. In particular, the most comprehensive definition of QoE seems to be the one from the ITU-T P.10/G.100 recommendation, where QoE is described as “the degree of delight or annoyance of the user of an application or service” [19]. A detailed set of QoE-related definitions can be found, e.g., in [5].

While QoE ratings are certainly user-centric (i.e., referring to the needs and expectations of end users), they much depend on QoS characteristics (referring to the ability of a networked system to provide its services at a certain quality level defined by QoS parameters such as packet loss, bit rate, throughput, transmission delay, and jitter). In particular, the authors of [10] show that the dependency of QoE on QoS can be considered exponential.

QoS attributes are often regarded as network-centric and largely represent the interests of network operators/service providers. These two aspects, i.e., the viewpoint of users interested in as good service as possible and of network operators/service providers (often focusing on a minimal level of investments assuring the assumed level of QoS), can be seen as opposing.

A relatively rich set of research results on methods of ensuring and measuring the QoE is available in the literature. Among them, particularly noteworthy seem to be the ones by Hossfeld et al. (see, e.g. [15, 17, 21]). In this section, a selected set of subjective metrics is highlighted, and their usability in failure scenarios is discussed.

Mean Opinion Score

The *mean opinion score* (MOS) metric has been designed to evaluate the perceived quality of experience. It is based on subjective evaluations of users [10]. Following [20], users assign scores based on the following scale: 5-excellent, 4-good, 3-fair, 2-poor, 1-bad. In the final processing of results, the value of MOS is obtained as the arithmetic mean of user opinions. MOS is commonly considered as a standard metric for QoE [43].

Standard Deviation of Opinion Scores

Since assessing the level of QoE by end users might largely be sensitive (e.g., in the case of difficulties in making a clear assessment of QoE by particular users), relying only on the average values user experience of MOS may not be sufficient. Unfortunately, providing only the average values reflected by MOS hides the level of variation in ratings and thus provides, at most, partial information about user experience. It is, therefore, necessary to extend the analysis at least by the evaluation of the diversity of user opinions provided by the standard deviation of MOS focusing on the level of rating diversity, referred to as *standard deviation of opinion scores* (shortly SOS), as proposed in [16].

Other Statistical Metrics for the Evaluation of QoE

Since relying only on the mean values of user opinions in the evaluation of QoE is often not adequate, apart from the SOS metric of the distribution of user scores, one can also focus on distributions of user ratings (for comprehensive information about user ratings), entropy (referring to the level of unpredictability of user scores and the uncertainty of the measurement system), or on more detailed ratings coming from fractions of satisfied and dissatisfied users, as proposed in [13], as well as on estimating the confidence intervals for MOS values, as considered in [14].

In post-failure periods, it is naturally more challenging to fulfill obligations concerning the assumed level of QoS. Therefore, there is also a risk of deterioration of QoE perceived by the end users following the related degradation of QoS parameters. Investing in resilience mechanisms supporting communications in failure scenarios is thus an essential aspect of maintaining the QoE level in line with user expectations.

3.6 Selected Examples for Adaptation of Metrics in Networked Systems

Metrics discussed in this chapter are often used in practice. They are commonly applied in evaluating the performance of networked systems and their components. However, it is also worth emphasizing the vital role of some of them, e.g., in the operation of routing protocols (in particular, during the calculation of multi-hop paths characterized by the lowest cost according to a given metric). Another essential utilization of metrics refers to various optimization tasks concerning the design of resilient architectures networked systems, e.g., designing a system structure or determining the location of crucial components of such systems such as computing nodes or data servers. As the literature provides a large set of examples for the application of metrics, in this section, we will present selected ones that are particularly useful for routing mechanisms and methods of networked systems design.

Concerning the utilization of metrics in routing protocols, metrics relating to the characteristics of communication links are usually used. For instance, a classical *Routing Information Protocol* (*RIP*) [12] belonging to the distance-vector class of routing algorithms uses the hop count metric to determine the end-to-end paths characterized by the lowest cost expressed by the number of links traversed by these paths. As a result of these calculations, for each determined path, information about the related next-hop node is stored by each network node traversed by that path. Paths are recalculated periodically to respond to changes in network topology (for instance, as a result of a failure of a link or node). RIP is proper for medium-sized systems that are composed of relatively homogeneous equipment (e.g., identical nodes characterized by comparable node processing times and links of the same transmission rate). Then, assuming a comparable length of links in the system, the overall cost of a path can be, thus, well reflected by the number of path hops.

In the case of nonhomogeneous networks (i.e., consisting of nodes from different vendors characterized by differentiated times for packet processing and links of differentiated transmission rates), metrics other than the basic hop count are better suited to reflect the total path cost. For instance, in *Open Shortest Path First* (*OSPF*) [31], each link is associated with a cost metric which by default is assumed to be inversely proportional to the bandwidth of that link (i.e., network-level functional characteristics). In this protocol, belonging to the class of link-state protocols, each network node is aware of the state (up/down) of each link as well as the associated cost metric and calculates the cheapest communication paths based on the related transmission rates of network links, using Dijkstra's algorithm [8]. In path computations, high-speed links are thus preferred, which, in turn, reduces the overall transmission delay along multi-hop paths. However, as path computations in OSPF are CPU- and memory-intensive, practical utilization of OSPF is limited to medium-sized networks.

Another example of utilization of a network-level functional metric in routing is provided in [36], including a proposal of a routing algorithm using the node load metric to calculate the multi-hop paths. Since, for every demand to establish a multi-hop path, it selects the path associated with the least loaded nodes, an additional feature is that, in the long run, it also leads to balancing the load of nodes.

Metrics referring to node centrality characteristics are used in the literature both in the case of routing algorithms and in network design methods, e.g., to solve various service placement problems. For example, in [34], a routing algorithm is introduced for anycast communications using a metric based on a mix of node degree and hop count. In this algorithm, packets are forwarded by each transit node to the next hop, characterized by a greater number of alternate paths available.

As discussed earlier in this chapter, nodes characterized by high values of centrality metrics often switch large amounts of data (as the shortest paths often traverse them), as well as are good candidates for placement of certain services (due to low transmission delay from these nodes to other nodes in the system). Therefore, they are also common targets of malicious activities. As presented, e.g., in [38], the availability of communication paths, as well as of certain services, can be improved in scenarios of malicious attacks by using node centrality metrics to determine locations (placement) of services at low-degree nodes (i.e., characterized by a low risk of an attack), as well as by applying a routing scheme with link cost metric determined based on the average values of centrality metrics of its end nodes.

The properties of specific communication environments often call for a metric adjusted to a particular communication scenario. There are many proposals in this context in the related literature. For example, concerning wireless environments, reference [9] focuses on the use of packet-related characteristics: the *round trip time—RTT* (i.e., the round trip delay for unicast probes between neighboring nodes) and the *expected transmission count—EXT* (referring to the loss rate of packets between neighboring nodes) as a metric for wireless links used for routing purposes. Indeed, collisions of packets transmitted in parallel by different sources over the wireless medium (justifying the need to use certain transmission protocols such as CSMA/CA) [4], as well as other reasons for packet retransmissions (e.g., due to transmission errors) are reasonable justifications for focusing on the instant characteristics of wireless links performance.

3.7 Summary

The analysis of the properties of metrics provided in this chapter confirms their essential role in the correct functioning of networked systems in normal operating conditions and during periods of failures. In a normal operational state, these metrics can deliver valuable information about system functioning, potential disproportions concerning the network load, etc. Also, they can indicate areas of the system where the effects of possible failures would be particularly severe and thus provide valuable information useful for system design, configuration, and update.

? Questions

1. Characterize the ways of formal representation of the architecture of networked systems.
2. Describe and compare the metrics of node centrality.
3. Discuss the features and the purpose of structural metrics in evaluating networked systems resilience.
4. Describe and compare the structural metrics referring to node degrees.
5. Describe and compare the structural metrics referring to communication paths.
6. Describe and compare the structural metrics referring to the system connectivity.
7. Explain the reasons for the irregularities of the system topology.

8. Characterize the functional network-level metrics for evaluation of networked systems resilience.
9. Characterize the functional packet-level metrics for evaluation of networked systems resilience.
10. Explain the role and characteristics of subjective metrics of system performance evaluation.
11. Provide several examples of utilization of node- and link-related metrics in practice.

References

1. Albert, R., Barabási, A.-L.: Statistical mechanics of complex networks. Rev. Mod. Phys. **74**(1), 47–97 (2002)
2. Barabási, A.-L., Albert, R.: Emergence of scaling in random networks. Science **286**, 509–512 (1999)
3. Bavelas, A.: A mathematical model for group structure. Hum. Organ. Appl. Anthropol. **7**(3), 16–30 (1948)
4. Bianchi, G.: Performance analysis of the IEEE 802.11 distributed coordination function. IEEE J. Sel. Areas Commun. **18**(3), 535–547 (2000)
5. Brunnstrom, K., Beker, S.A., de Moor, K., Dooms, A., Egger, S. et al.: Qualinet white paper on definitions of Quality of Experience (2013). https://hal.science/hal-04638470v1. Accessed 11 Sep 2023
6. Cetinay, H., Mas-Machuca, C., Marzo, J.L., Kooij, R., Van Mieghem, P.: Comparing destructive strategies for attacking networks. In: Rak, J., Hutchison, D. (eds.) Guide to Disaster-Resilient Communication Networks, pp. 117–140. Springer, Berlin (2020)
7. Chu, Y., Rao, S.G., Seshan,. S., Zhang, H.: A case for end system multicast. IEEE J. Sel. Areas Commun. **20**(8), 1456–1471 (2002)
8. Dijkstra, E.: A note on two problems in connexion with graphs, Numerishe Mathematik **1**, 269–271 (1959)
9. Draves, R., Padhye, J., Zill, B.: Comparison of routing metrics for static multi-hop wireless networks, ACM SIGCOMM Comput. Commun. Rev. **34**(4), 133–144 (2004)
10. Fiedler, M., Hossfeld, T., Tran-Gia, P.: A generic quantitative relationship between quality of experience and quality of service. IEEE Netw. **24**(2), 36–41 (2010)
11. Freeman, Linton C. A set of measures of centrality based on betweenness. Sociometry **40**(1), 35–41 (1977)
12. Hedrick, C.: Routing Information Protocol, Request for Comments (RFC) 1058, IET. https://datatracker.ietf.org/doc/html/rfc1058. Accessed 30 Sept 2023
13. Hossfeld, T., Heegaard, P.E., Varela, M.: QoE beyond the MOS: Added value using quantiles and distributions. In: Proceedings of the 2015 Seventh International Workshop on Quality of Multimedia Experience (QoMEX'15), pp. 1–6 (2015)
14. Hossfeld, T., Heegaard, P.E., Varela, M., Skorin-Kapov, L.: Confidence interval estimators for MOS values ((2018)). arXiv:1806.01126 . https://arxiv.org/abs/1806.01126. Accessed 14 Sept 2023
15. Hossfeld, T., Keimel, Ch., Hirth, M., Gardlo, B., Habigt, J., Diepold, K., Tran-Gia, P.: Best practices for QoE crowdtesting: QoE assessment with crowdsourcing. IEEE Trans. Multimedia **16**(2), 541–558 (2014)

16. Hossfeld, T., Schatz, R., Egger, S.: SOS: The MOS is not enough! In: Proceedings of the 2011 Third International Workshop on Quality of Multimedia Experience, pp. 131–136 (2011)
17. Hossfeld, T., Schatz, R., Varela, M., Timmerer, C.: Challenges of QoE management for cloud applications. IEEE Commun. Mag. **50**(4), 28–36 (2012)
18. ITU-T: Recommendation E.800 – Definitions of terms related to quality of service (2008). https://www.itu.int/rec/T-REC-E.800. Accessed 11 Sept 2023
19. ITU-T Recommendation P.10/G.100: vocabulary for performance and quality of service. Amendment 5 (2016). https://www.itu.int/rec/T-REC-P.10-201607-S!Amd5/en. Accessed 11 Sept 2023
20. ITU-T: Recommendation P.800 – Methods for Subjective Determination of Transmission Quality. https://www.itu.int/rec/T-REC-P.800-199608-I. Accessed 11 Sept 2023
21. Jarschel, M., Schlosser, D., Scheuring, S., Hossfeld, T.: An evaluation of QoE in cloud gaming based on subjective tests. In: Proceedings of the 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 330–335 (2011)
22. Kalesnikau, I., Pioro, M., Rak, J., Ivanov, H., Fitzgerald, E., Leitgeb, E.: Enhancing resilience of FSO networks to adverse weather conditions. IEEE Access **9**, 123541–123565 (2021)
23. Lareida, A., Meier, D., Bocek, T., Stiller, B.: Towards path quality metrics for overlay networks. In: Proceedings of the 2016 IEEE 41st Conference on Local Computer Networks (LCN'16), pp. 156–159 (2016)
24. Lee, S.S.W., Li, K.-Y., Lin, Ch.-Ch.: Modeling and algorithm for multiple spanning tree provisioning in resilient and load balanced Ethernet networks. Math. Probl. Eng. **2015**, 676542 (2015)
25. Li, J., Chee Shiu, W., Chang, A.: The number of spanning trees of a graph. Appl. Math. Lett. **23**(3), 286–290 (2010)
26. Luce, R.D., Perry, A.D.: A method of matrix analysis of group structure. Psychometrika **14**(1), 95–116 (1949)
27. Maniadakis, D., Balmpakakis, A., Varoutas, D.: On the temporal evolution of backbone topological robustness. In: Proceedings of the 2013 18th European Conference on Network and Optical Communications & 2013 8th Conference on Optical Cabling and Infrastructure (NOC-OC&I'13), pp. 129–136 (2013)
28. Manzano, M., Calle, E., Harle, D.: Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In: Proceedings of the 2011 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT'11), Budapest, Hungary, pp. 1–7 (2011)
29. Manzano. M., Sahneh, F., Scoglio, C., Calle, E., Marzo, J.L.: Robustness surfaces of complex networks. Nat. Sci. Rep. **4**, 6133 (2014)
30. Moeller, S.: Quality of Telephone-Based Spoken Dialogue Systems. Springer, New York (2005)
31. Moy, J.: OSPF Version 2, Request for Comments (RFC) 2328, IETF. https://datatracker.ietf.org/doc/html/rfc2328. Accessed 30 Sept 2023
32. Natalino, C., Ristov, S., Wosinska, L., Furdek, M.: Functional metrics to evaluate network vulnerability to disasters. In: Rak, J., Hutchison, D. (eds.) Guide to Disaster-Resilient Communication Networks, pp. 47–62. Springer, Berlin (2020)
33. Natalino, C., Yayimli, A., Wosinska, L., Furdek, M.: Content accessibility in optical cloud networks under targeted link cuts. In: Proceedings of the 2017 International Conference on Optical Network Design and Modeling (ONDM'17), pp. 1–6 (2017)
34. Ohta, S., Makita, H.: Anycast routing based on the node degree for ad hoc and sensor networks. In: Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering, pp. 439–446 (2013)
35. Pyo, C.W., Harada, H.: Throughput analysis and improvement of hybrid multiple access in IEEE 802.15.3c mm-wave WPAN. IEEE J. Sel. Areas Commun. **27**(8), 1414–1424 (2009)
36. Qi, Z., Sun, J., Li, W.: A routing algorithm based loading ratio in nodes. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering 2004, pp. 595–598 (2004)

37. Rak, J., Hutchison, D. (eds.): Guide to Disaster-Resilient Communication Networks. Springer, Berlin (2020)
38. Rak, J., Walkowiak, K. Reliable anycast and unicast routing: Protection against attacks. Telecommun. Syst. **52**, 889–906 (2013)
39. Rohrer, J.P., Jabbar, A., Sterbenz, J.P.G.: Path diversification: A multipath resilience mechanism. In: Proceedings of the 2009 7th International Workshop on Design of Reliable Communication Networks (DRCN'09), pp. 343–351 (2009)
40. Routray, S.K., Sahin, G., da Rocha, J.R.F., Pinto, A.N.: Statistical analysis and modeling of shortest path lengths in optical transport networks. J. Lightwave Technol. **33**(13), 2791–2801 (2015)
41. Rueda, D.F., Calle, E. Marzo, J.L. Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. J. Netw. Syst. Manag. **25**, 269–289 (2017)
42. Santos, D., De Sousa, A., Mas-Machuca, C., Rak, J.: Assessment of connectivity-based resilience to attacks against multiple nodes in SDNs. IEEE Access **9**, 58266–58286 (2021)
43. Schatz, R., Hossfeld, T., Janowski, L., Egger, S.: From packets to people: Quality of experience as a new measurement challenge. In: Biersack, E., Callegari, C., Matijasevic, M. (eds.) Data Traffic Monitoring and Analysis. Lecture Notes in Computer Science, vol. 7754. Springer, Berlin, Heidelberg (2013)
44. Strogatz, S.H., Watts, D.J.: Collective dynamics of 'small-world' networks. Nature **393**, 440–442 (1998)
45. Tang, L., Liu, H.: Community Detection and Mining in Social Media. Morgan and Claypool Publishers (2010)
46. Van Mieghem, P.: Performance Analysis of Communications Networks and Systems. Cambridge University Press, Cambridge (2010)
47. Van Mieghem, P.: Pseudoinverse of the Laplacian and best spreader node in a network. Phys. Rev. E **96**(3), 032311 (2017)