Chapter 5
Comparing Destructive Strategies for Attacking Networks

Hale Cetinay, Carmen Mas-Machuca, Jose L. Marzo, Robert Kooij, and Piet Van Mieghem

Abstract The failures of multiple elements in a network can have disastrous consequences on its operation. Therefore, understanding the robustness of networks that experience multiple failures is utterly important. In this chapter, we review well-defined metrics related to the topology and resilience of the network, and use them to analyze the robustness of real-world networks under multiple failures. We consider 52 real-world networks from three different infrastructure domains, namely metro networks, power grids and telecommunication networks. We quantify the impact of targeted node removals from a network on the relative size of the largest connected component of the network. Nodes are attacked according to traditional centrality metrics, such as degree, betweenness, closeness and the principal adjacency matrix eigenvector. In addition, we consider attacks based upon the recently proposed "zeta-vector", that is the diagonal elements of the pseudo-inverse of the Laplacian matrix. Finally, we compare and rank these node-removal strategies, applied to the selected set of real-world infrastructures.

Hale Cetinay
Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, The Netherlands,
Institute of Environmental Sciences, Leiden University, The Netherlands,
e-mail: H.Cetinay.iyicil@cml.leidenuniv.nl

Carmen Mas-Machuca
Technical University of Munich, Department of Electrical and Computer Engineering, Germany,
e-mail: cmas@tum.de

Jose L. Marzo
University of Girona, Department of Electrical and Computer Engineering, Spain,
e-mail: joseluis.marzo@udg.edu

Robert Kooij
Singapore University of Technology and Design, Centre for Research in Cyber Security,
Singapore, e-mail: robert_kooij@sutd.edu.sg

Piet Van Mieghem
Delft University of Technology, Faculty of Electrical Engineering, Mathematics and Computer Science, The Netherlands, e-mail: P.F.A.VanMieghem@tudelft.nl

5.1 Introduction

Networks support most areas of daily life including fundamental systems and services that are indispensable to the security, economy, and social well-being of our countries and communities [27, 29]. Customers, business, governments and military depend on various networks for accessing information, obtaining products and services, managing finances, commencing transactions, responding to disasters and executing network central operations etc. [29].

Telecommunication networks are described as one of the critical infrastructures, along with the water supply systems, power grids, transportation systems, and oil and gas distribution networks. Therefore, these infrastructures must have the ability to provide and maintain an acceptable level of service when facing multiple failures and challenges to normal operation [29]. *Network robustness* that is the ability of a network to continue to operate [8] can be evaluated by measuring the impact of large-scale failures under different scenarios.

Large-scale failures in critical infrastructures rarely occur, but when they do, their consequences are catastrophic and expensive. Failures in critical infrastructures imply service disruptions that can affect thousands of people, multiple communities in certain geographical areas or in the entire country [23]. For instance, in 2014, a configuration error in Time-Warners Internet routers in the United States resulted in a failure that prevented more than 10 million clients from accessing the services for three hours [31].

Research into the robustness analysis of telecommunication networks has been carried out and different metrics to measure the network robustness have been proposed. In [29], some of the traditional robustness metrics are studied for a set of real telecommunication networks, and the most robust networks are identified by comparing the metrics obtained by the simulations for various failure scenarios. In [8], the robustness of real networks and generic topologies (with node degrees following random, scale-free and exponential distribution) in non-failure scenarios are compared. Both works [8, 29] rank the topologies based on their robustness metrics. In [23], an analytic comparison of well-known robustness metrics in some real and empirical networks under random and targeted attacks is performed.

The aim of this chapter is to introduce the fundamental graph theory on network robustness and to investigate the impact of different attack strategies on metro networks, power grids and telecommunication networks.

5.1.1 Representing the Network Topology by a Graph

A graph G is a mathematical structure used to describe pairwise relations between objects. In this context, a graph is made up of N nodes, which are connected by L links. An example of a graph is given in Fig. 5.1. This graph has $N = 4$ nodes and $L = 5$ links.

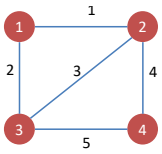


Fig. 5.1 An example of a graph consisting of four nodes connected by five links

The structure or interconnection pattern of a network can be represented by a graph. In Table 5.1, we give the examples of the graph representations of telecommunication, power and metro networks.

Table 5.1 The graph representations of telecommunication, power and metro networks

Type	Nodes	Links
Telecommunication networks	routers, switches, hosts	fibre cables, wired or wireless links
Power grids	substations, generators, loads	cables, transmission lines, transformers
Metro networks	transfer stations, terminals	rail tracks

5.1.2 Adjacency and Weighted Adjacency Matrices

The $N \times N$ adjacency matrix $\mathbf{A}$ specifies the interconnection pattern of the graph. The element of the adjacency matrix $a_{ik} = 1$ only if the pair of nodes i and k are connected by a direct link; otherwise $a_{ik} = 0$. In Fig. 5.2, we show the adjacency matrix of an example graph with four nodes and four links. For example, the element in the first row and second column of the adjacency matrix is $a_{12} = 1$, as there is a direct link between nodes `1` and `2`, whereas the element in the first row and fourth column is $a_{14} = 0$ as there is no direct link between nodes `1` and `4`.

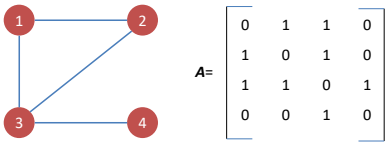


Fig. 5.2 The adjacency matrix $\mathbf{A}$ of an example graph consisting of 4 nodes connected by 4 links

Furthermore, an $N \times N$ weighted adjacency matrix $\mathbf{C}$ extends the information in $\mathbf{A}$ by associating each link between two connected nodes with a weight: $c_{ik} = 0$

if the pair of nodes i and k are not connected by a direct link; otherwise $c_{ik} \neq 0$ where $c_{ik} \in \mathbb{R}$ is the weight of the direct link between i and k. This weight can represent length, resistance, cost, delay, available capacity, etc. depending on the study. Figure 5.3 depicts both the weighted network and the associated symmetric weighted adjacency matrix.

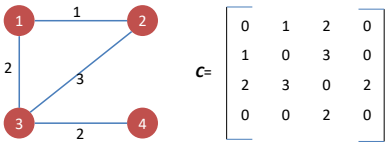


Fig. 5.3 The weighted adjacency matrix **C** of an example graph whose links have costs associated with the links

5.1.3 Laplacian Matrix

The $N \times N$ Laplacian matrix $\mathbf{Q}$ is defined as

$$\mathbf{Q} = \Delta - \mathbf{A}, \tag{5.1}$$

where $\Delta = \mathrm{diag}(d_i)$ is the $N \times N$ diagonal degree matrix and the degree of node i is $d_i = \sum_{k=1}^{N} a_{ik}$. Therefore, the elements of $\mathbf{Q}$ satisfy $q_{ij} = -a_{ij}$ if $i \neq j$, and $q_{ii} = \sum_{k=1}^{N} a_{ik}$. The Laplacian matrix has zero row and column sum, i.e., $\mathbf{Qu} = \mathbf{0}$ and $\mathbf{u}^T\mathbf{Q} = \mathbf{0}^T$, where $\mathbf{u} = (1, 1, \ldots, 1)^T$ is the all-one vector. In Fig. 5.4, we show the Laplacian of an example graph with four nodes and four links.

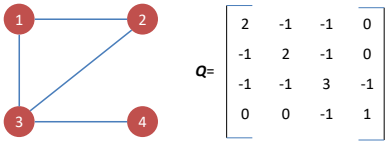


Fig. 5.4 The Laplacian matrix **Q** of an example graph consisting of 4 nodes connected by 4 links

Some graph metrics, such as the algebraic connectivity, are based on the eigenvalues of the Laplacian matrix $\mathbf{Q}$, which are also referred as the Laplacian eigenvalues. These eigenvalues are denoted as μ_i where $\mu_N = 0 \leq \mu_{N-1} \leq \cdots \leq \mu_1$. For the Laplacian matrix of the graph in Fig. 5.4, the eigenvalues are $\mu_4 = 0 \leq \mu_3 = 1 \leq \mu_2 = 3 \leq \mu_1 = 4$.

5.1.4 Walks, Paths, and Shortest Paths

A *walk* is an alternating sequence of nodes and connecting links in a graph. A walk can travel over any link and any node any number of times. A *path* is a walk which does not include any node twice. The length of a path is the number of links between a source and a target node in a graph, and the *shortest path* is the path between two nodes in a graph such that its length is minimal. For instance, in Fig. 5.5, two different paths (in bold) between nodes 2 and 3 are shown. The first path consist of two links, whereas the second path has one link, which is indeed the shortest path between nodes 2 and 3.

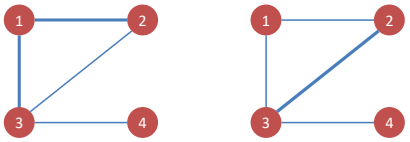


Fig. 5.5 Two different paths (in bold) between nodes 2 and 3 in the example graph. The first path (left) has two hops, whereas the second path (right) has one hop, which is the shortest path between nodes 2 and 3

5.2 Robustness of Networks

The robustness of a network shows the extent to which a network is capable to withstand failures during a given time interval. In other words, robustness quantifies how the network behaves after the occurrence of one or more failures. The robustness assessments can consider any failure, and any number of failures at any order, as well as it can consider intentional failures (so-called attacks [3]).

For the network over which a specific service is being delivered, when we want to assess its robustness, we have to consider two features: the network topology and the service (or the function) for which the network is designed for [22, 36]. The network topology specifies how nodes are interconnected to other nodes by links. The network service is less clearly defined and more abstract. The service mainly uses the network topology to transport items between a group of nodes. For example, in power grids, a service transports the item (electrical power) from a source node (such as a power plant) to a destination node (such as houses) over the network topology.

Currently, there is not a commonly agreed answer to the basic question "What is the robustness of the network?" [36]. A first and natural way to define the robustness of a network is to resort to graph theory [16, 33].

Let us consider the case of an operator studying the network operation after multiple node failures. We assume that when a node fails in the network, all adjacent

links of that node also fail. Thus, the node and all its links are removed from the underlying graph. For instance, Fig. 5.6 shows the failure of node 2 in the example graph in Fig. 5.2. When node 2 fails, node 2 and all its links (link between nodes 2 and 1, and link between node 2 and 3) are removed from the graph. The remaining graph after the removal of node 2 is still connected (there is a path between each node).

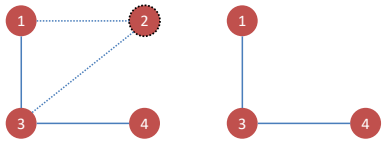


Fig. 5.6 Removal of node 2 and all its links from the initial graph (left). After the removal of node 2 the remaining graph (right) is connected

In some cases, a removal of a node can disconnect the graph, leading to a partitioning of the original graph into several components, which are disconnected from each other. Each component is a connected subgraph of the original graph. For instance, Fig. 5.7 shows the failure of node 3 in the example graph in Fig. 5.2. When node 3 fails, node 3 and all its links (link between nodes 1 and 3, link between nodes 2 and 3, and link between node 3 and 4) are removed from the graph. The remaining graph after the removal of node 3 is partitioned into two components: the first component contains nodes 1 and 2, and the second component consists only of node 4.

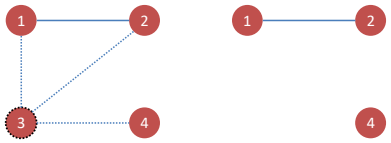


Fig. 5.7 Removal of node 3 and its links from the initial graph (left). After the removal of node 3 the remaining graph (right) has two components

Ideally, a robustness metric should capture both the structural and functional aspects of a network [30, 36]. The examples in Figs. 5.6-5.7 illustrate that the removal of a node can partition the network into multiple components. This is usually undesirable for the network: (i) the structure is distorted, as the size (i.e., the number of nodes) of the connected component of the network is decreased, and (ii) the service (function) is adversely affected since parts of network become disconnected from each other. In this work, we consider the size of the largest connected component (giant component) in the graph as the robustness metric to assess the effect of multiple node failures.

We start with a connected initial network, therefore, the initial size of the largest connected component of its underlying graph is N. Then, we remove the nodes of the network one by one and after each node removal, we calculate the relative size of the largest connected component as the ratio between the size of the current largest

connected component and the initial network size N. In the example in Fig. 5.6, the relative size of the largest connected component after the removal of node 2 is $(3/4) = 0.75$, whereas in Fig. 5.7, the relative size of the largest connected component after removal of node 3 is $(2/4) = 0.5$, which shows that the removal of node 3 can put the network in a worse condition than the removal of node 2.

It is important to identify the node removals that put the network in an undesirable or critical condition. However, in the case of sequential multiple node removals, the computational complexity of the analyzes is high. For instance, for the example network with four nodes in Fig. 5.2, there are $4 \times 3 \times 2 \times 1 = 24$ different ways to sequentially remove all nodes. In Table 5.2, we show all possible sequential attacks and their effect on the size of the giant component of the example graph in Fig. 5.2. Table 5.2 allows to identify the critical node removals (attacks) by comparing the effects on the relative size of the largest component. For instance, in Attack 1, after the removal of three nodes, the relative size of the largest component becomes 0.25; whereas in Attack 13, it requires the removal of two nodes to decrease the relative size of the largest component to 0.25.

Table 5.2 The effect of different sequential attacks on the relative size of the largest connected component (rLCC) of the graph in Fig. 5.2

	Removed nodes from the graph				rLCC after the removal of				
Attack number	First	Second	Third	Fourth	one node	two nodes	three nodes	four nodes	Average rLCC
1	1	2	3	4	0.75	0.50	0.25	0	0.3750
2	1	2	4	3	0.75	0.50	0.25	0	0.3750
3	1	3	2	4	0.75	0.25	0.25	0	0.3125
4	1	3	4	2	0.75	0.25	0.25	0	0.3125
5	1	4	2	3	0.75	0.50	0.25	0	0.3750
6	1	4	3	2	0.75	0.50	0.25	0	0.3750
7	2	1	3	4	0.75	0.50	0.25	0	0.3750
8	2	1	4	3	0.75	0.50	0.25	0	0.3750
9	2	3	1	4	0.75	0.25	0.25	0	0.3125
10	2	3	4	1	0.75	0.25	0.25	0	0.3125
11	2	4	1	3	0.75	0.50	0.25	0	0.3750
12	2	4	3	1	0.75	0.50	0.25	0	0.3750
13	3	1	2	4	0.50	0.25	0.25	0	0.2500
14	3	1	4	2	0.50	0.25	0.25	0	0.2500
15	3	2	1	4	0.50	0.25	0.25	0	0.2500
16	3	2	4	1	0.50	0.25	0.25	0	0.2500
17	3	4	1	2	0.50	0.50	0.25	0	0.3125
18	3	4	2	1	0.50	0.50	0.25	0	0.3125
19	4	1	2	3	0.75	0.50	0.25	0	0.3750
20	4	1	3	2	0.75	0.50	0.25	0	0.3750
21	4	2	1	3	0.75	0.50	0.25	0	0.3750
22	4	2	3	1	0.75	0.50	0.25	0	0.3750
23	4	3	1	2	0.75	0.50	0.25	0	0.3750
24	4	3	2	1	0.75	0.50	0.25	0	0.3750

Table 5.2 shows that the attacks starting with the removal of node 3 decrease the size of the giant component of the graph faster than the other attacks. If we investigate the centrality scores of nodes (refer to Sect. 5.3) in Figs. 5.8-5.12, they all identify node 3 as the most important node. In Table 5.2, we observe that after removing node 3, the removal of nodes 1 or 2 decrease the size of the giant component in the remaining graph faster than the removal of node 4. This observation also agrees with the centralities in Figs. 5.8-5.12, since nodes 1 and 2 are identified as the second important after node 3. Thus, if the aim of the attacks is to destroy the network as soon as possible, then, Attacks 13-16 in Table 5.2 are the most effective as they lead to the lowest value of the normalized size of the giant component of 0.250 faster than the others.

Table 5.2 helps to identify the most important nodes in the network. In larger networks, it is not possible to simulate the effects of all combinations of node removals. Instead, the centrality scores of the nodes can give insight in the severity of attacks and can identify the "worst case" attack scenarios. In the next section, we introduce both centrality metrics and structural metrics which can be used for robustness evaluation. In the subsequent section, we use network data from three types of real-world infrastructures and investigate the effect of sequential node removals on a number of robustness metrics.

5.3 Metrics Used for Robustness Analysis

Metrics used for robustness evaluations include *structural*, and *functional metrics*. Several works on these metrics are available, including [1, 5, 7, 10, 11, 15, 17, 19, 21, 24]. In this chapter, we use centrality metrics to measure the node importance in a network and then we evaluate the performance of the network to (targeted) attacks using structural metrics.

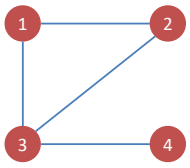
5.3.1 Centrality Metrics

– **Degree centrality**: The degree centrality of a node is the number of neighbouring nodes connected to that node [13, 34]. The degree d_i can be calculated using the adjacency matrix $\mathbf{A}$:

$$d_i = \sum_{j=1}^{N} a_{ij}. \tag{5.2}$$

A large degree centrality can indicate a node with high importance for network operation, since if that node fails, a high number of neighbouring nodes can be affected. In Fig. 5.8, we present the degree centralities of an example graph with four nodes and four links. For instance, nodes 1 and 2 have degree centrality of

2 (they have two direct neighbours), whereas node 3 has degree centrality of 3 (it has three direct neighbours).



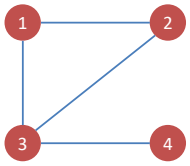
Node	Degree
1	2
2	2
3	3
4	1

Fig. 5.8 Degree centralities in an example graph

– **Closeness Centrality**: The closeness centrality assesses how close a node is to the other nodes in a graph [12]. The closeness centrality c_i of a node i is defined as

$$c_i = \frac{1}{\sum_{j \neq i} H(\mathcal{P}_{i \to j})}, \tag{5.3}$$

where the hop count $H(\mathcal{P}_{i \to j})$ is the number of links in the shortest path $\mathcal{P}_{i \to j}$ between a pair of nodes i and j.
The higher the closeness centrality of a node, the more central the node is. In Fig. 5.9, the length of the shortest path from node 1 to node 2 is 1, to node 3 is 1, to node 4 is 2, making the sum of the lengths of the shortest paths from node 1 to all other nodes 4. Then, the closeness centrality of node 1 is $(1/4) = 0.25$. For node 3, the lengths of the shortest paths to all other nodes are 1, making its closeness centrality $(1/3) = 0.33$.



Node	Closeness
1	0.25
2	0.25
3	0.33
4	0.20

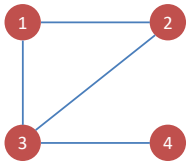
Fig. 5.9 Closeness centralities in an example graph

– **Betweenness centrality**: The betweenness centrality of a node is related to the number of all shortest paths that pass through that node. The betweenness b_i of node i is calculated as

$$b_i = \sum_{s,t \in \mathcal{N} \setminus \{i\}} \frac{|\mathcal{P}_{s \to t}(i)|}{|\mathcal{P}_{s \to t}|}, \tag{5.4}$$

where $|\mathcal{P}_{s \to t}|$ is the number of all possible shortest paths from node s to node t, and $|\mathcal{P}_{s \to t}(i)|$ is the number of those paths that pass through node i.
A node with a high betweenness centrality score can play an important role in the network such as in transportation or information diffusion [20, 37]. In Fig. 5.10, none of the shortest paths between nodes 1, 2 and 3 pass through

node 4, making its betweenness centrality 0. On the other hand, the betweenness centrality of node 3 is 2 as the shortest paths between nodes 1 and 4, and nodes 2 and 4 have to pass through node 3.



Node	Betweenness
1	0
2	0
3	2
4	0

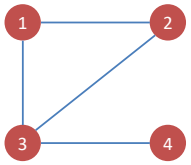
Fig. 5.10 Betweenness centralities in an example graph

The betweenness centrality metric can be extended to reflect the importance of a network region in which several nodes may reside [14]. In this case, the betweenness centrality of a network region is calculated by the number of shortest paths that pass through the region. The failure of a network region with higher betweenness centrality is often more crucial.

– **Eigenvector centrality**: The eigenvector centrality x_i of node i is equal to the i^{th} element of the eigenvector corresponding to the largest eigenvalue λ_1 of the adjacency matrix $\mathbf{A}$. The principal eigenvector centralities are

$$x_i = \frac{1}{\lambda_1} \sum_{k=1}^{N} a_{ik} x_k. \tag{5.5}$$

The eigenvector centrality score of a node depends on the number of its direct neighbouring nodes, 2-hop neighbouring nodes, 3-hop neighbouring nodes, and so on. Thus, a high eigenvector centrality can identify a node that is linked to other important nodes [18, 34]. In Fig. 5.11, the eigenvector corresponding to the largest eigenvalue of the adjacency matrix is given. Hence, the eigenvector centrality scores of nodes 1, 2, 3, and 4, are 0.53, 0.53, 0.61 and 0.28, respectively.

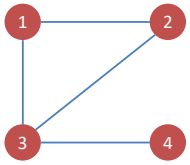


Node	Eigenvector
1	0.53
2	0.53
3	0.61
4	0.28

Fig. 5.11 Eigenvector centralities in an example graph

– **Zeta-vector score**: Inspired by electrical flows (effective resistance, [9]) in a resistor network, [35] proposes the zeta-vector, which contains the diagonal elements of the pseudo-inverse of the Laplacian matrix [4] of a graph, as a vector that quantifies nodal spread. For flow (e.g., water, gas, current) that is proportional to the potential difference of any pair of nodes i and j, the diagonal

element of the pseudo-inverse of the Laplacian matrix quantifies the average potential difference of a node i to all other nodes in the network. The node with the minimum value for the zeta score (the corresponding diagonal element of the pseudo-inverse of the Laplacian matrix), therefore, is regarded as the best spreader node. In Fig. 5.12, the diagonal elements in the pseudo-inverse of the Laplacian matrix of the graph are depicted. Hence the zeta-vector scores of nodes `1`, `2`, `3`, and `4`, are 0.35, 0.35, 0.18 and 0.69, respectively.



Node	Zetavector
1	0.35
2	0.35
3	0.18
4	0.69

Fig. 5.12 Zeta-vector scores in an example graph

5.3.2 Structural Metrics

Structural metrics are a well-know area in the conventional analysis of networks [28]. In this chapter, we use two structural metrics to assess the robustness of a network which experiences failures or targeted attacks.

- **Relative Size of the Largest Connected Component** (*rLCC*) is the ratio of the size of the largest cluster of connected nodes and the original number of nodes N.
- **Average Two-Terminal Reliability** ($ATTR$) [25, 26] is defined as the number of connected node pairs divided by the total amount of node pairs.

These metrics are widely used because of their straightforward interpretation: the *rLCC* is the expected relative size of the giant component, while the $ATTR$ is the probability that two randomly chosen nodes are connected.

Van Mieghem et al. [36] suggested the R-value, a normalized linear combination of structural metrics, as a robustness metric. For instance, the R-value could be defined as a weighted average of *rLCC* and $ATTR$, i.e., $R = \alpha\ rLCC + (1-\alpha)\ ATTR$, with $0 \leq \alpha \leq 1$. Typically, $R = 0$ (or R close to 0) represents a completely degraded network, whereas a value $R = 1$ corresponds to an optimally robust network.

The impact of multiple failures or attacks on a network are assessed by computing the impact of the failures (or attacks) on a structural metric. For instance, Fig. 5.13 depicts that the impact of removing up to 25% of all nodes in a real-life telecommunication network, the Geant2012 network [28], consisting of $N = 40$ nodes and $L = 61$ links.

Once a structural metric is evaluated for multiple failures (or attacks), it is desirable to quantify the robustness as a single scalar to compare different graphs.

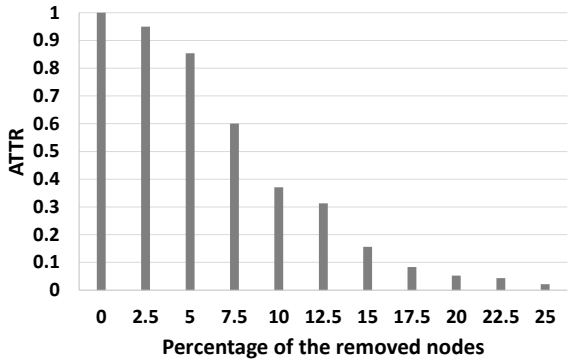


Fig. 5.13 The $ATTR$ metric as a function of node removals based on the degree centrality in the Geant2012 network

Trajanovski et al. [32] proposed the energy of the structural metric ε which is the average value of the structural metric over the range of considered perturbations, i.e., node and / or link removals. For example, from Fig. 5.13, we can obtain the energy $\varepsilon_{ATTR} = 0.404$.

Wang et al. [38] suggest another robustness indicator: the smallest percentage of elements that need to be removed so that the structural metric decreases to a given fraction $f < 1$. For example, from Fig. 5.13 we can deduce that in order to decrease $ATTR$ below $f = 0.9$, we need to remove at least 5% of the nodes in Geant2012.

Finally, the value of the structural metric for the maximum number of considered removals (i.e., at the end of the attacks) can be also used as a robustness indicator. For example, according to Fig. 5.13, this robustness indicator yields $ATTR_{25\%} = 0.022$.

In this chapter, we use the energy of the structural metric as the robustness indicator. The advantage of this indicator is that the energy assesses for the whole range of perturbations imposed upon the network. In the next section, we determine the energy for the Geant2012 network and 51 other real-life networks for a variety of attacks.

5.4 Case Studies

In this section, we analyze the effect of removals of nodes and links on the robustness metric of real-world networks. First, we introduce the set of real-world networks, from the domains of public transportation, energy and telecommunication. Then, we evaluate the energy of the relative size of the largest connected component (*rLCC*) of these real-world networks, for targeted node removals according to traditional centrality metrics (such as degree, betweenness, closeness, principal adjacency matrix eigenvector) and the recently proposed "zeta-vector", containing

the diagonal elements of the pseudo-inverse of the Laplacian matrix. Subsequently, we compare and rank these node-removal strategies, applied to the selected set of real-world infrastructures. Finally, we determine the *rLCC* and the $ATTR$ for the Geant2012 telecommunication network, both for random and targeted link removals.

5.4.1 Data of Three Types of Real-world Infrastructures

In this section, we focus on three subsets of real-world infrastructures that are vital for society: metro networks, power grids and telecommunication networks. The selected networks have different numbers of nodes and links. In Table 5.3, we present the details of the networks. Additionally, below, we give an example graph and the references used for each infrastructure.

– **Metro networks**: 33 metro networks from different countries and in different sizes varying from $N = 5$ to $N = 83$ are used in the analyzes. More details on the networks can be found in [38] and [6]. As an example, Fig. 5.14 shows the graph of the Mexico City_metro network.

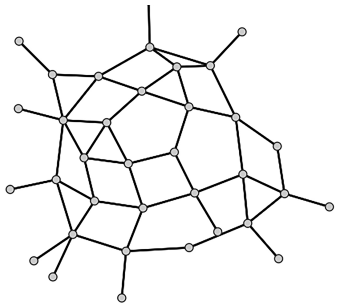


Fig. 5.14 The graph of the Mexico City_metro network

– **Power grids**: Both the real-world-like five test data topologies from IEEE[1] and the topologies of four European countries[2] are used. The sizes of the underlying graphs vary from $N = 24$ to $N = 3120$. In Fig. 5.15, we show the graph of the Netherlands High-Voltage (HV) network.

– **Telecommunication networks**: We use ten different networks, presented in [28]. These networks are also implemented in the Network Robustness Sim-

[1] IEEE Power Systems Test Case Archive, available at: https://www2.ee.washington.edu/research/pstca/.

[2] European power grids data set, available at: https://wiki.openmodinitiative.org/wiki/Transmission network datasets

Table 5.3 Details of the networks in the analyses

Network ID	Type	Name of the network	N	L
1	metro	Athens_metro	9	18
2	metro	Barcelona_metro	29	84
3	metro	Berlin_metro	32	86
4	metro	Boston_metro	21	44
5	metro	Brussels_metro	9	18
6	metro	Bucharest_metro	11	24
7	metro	Buenos.Aires_metro	12	26
8	metro	Cairo_metro	6	10
9	metro	Chicago_metro	25	58
10	metro	Delhi_metro	8	14
11	metro	Hong.Kong_metro	17	36
12	metro	Lisbon_metro	11	22
13	metro	London_metro	83	242
14	metro	Lyon_metro	10	20
15	metro	Madrid_metro	48	158
16	metro	Marseille_metro	6	10
17	metro	Mexico.City_metro	35	104
18	metro	Milan_metro	14	30
19	metro	Montreal_metro	10	20
20	metro	Moscow_metro	41	124
21	metro	New.York_metro	77	218
22	metro	Osaka_metro	36	102
23	metro	Paris_metro	78	250
24	metro	Prague_metro	9	18
25	metro	Rome_metro	5	8
26	metro	Seoul_metro	71	222
27	metro	Shanghai_metro	22	56
28	metro	Singapore_metro	12	26
29	metro	St.Peterburg_metro	14	32
30	metro	Stockholm_metro	20	38
31	metro	Tokyo_metro	62	214
32	metro	Toronto_metro	10	18
33	metro	Washington.DC_metro	17	36
34	power	Belgium HV	56	67
35	power	IEEE 24	24	34
36	power	Germany HV	231	302
37	power	IEEE 118	118	179
38	power	Poland HV	3120	3684
39	power	IEEE 300	300	409
40	power	IEEE 30	30	41
41	power	IEEE 57	57	78
42	power	Netherlands HV	35	43
43	telecommunication	Abilene	11	14
44	telecommunication	Cesnet201006	52	63
45	telecommunication	Cogentco	197	245
46	telecommunication	Deltacom	113	183
47	telecommunication	Garr201201	61	89
48	telecommunication	Geant2012	40	61
49	telecommunication	GpENI_L2	51	61
50	telecommunication	Kdl	754	899
51	telecommunication	Renater2010	43	56
52	telecommunication	UsCarrier	158	189

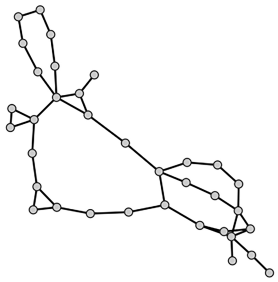


Fig. 5.15 The graph of the Netherlands HV network

ulator[3]. The sizes of the underlying graphs vary from $N = 11$ to $N = 754$. As an example, Fig. 5.16 shows the graph of the Renater2010 network.

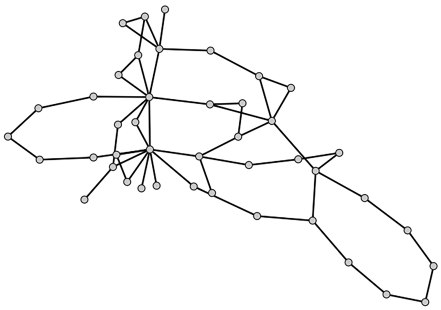


Fig. 5.16 The graph of the Renater2010 network

Although the networks in Figs. 5.14-5.16 have similar number of nodes, their graphs look different. Each infrastructure can have different characteristics which can affect both its underlying graph and its robustness with respect to node and / or link removals.

5.4.2 The Effect of Node Attacks on the Relative Size of the Largest Connected Component

In this section, we investigate the effect of multiple node removals on the relative size of the largest connected component (*rLCC*) and its energy. At the beginning of the attacks, each network attains a *rLCC* of value 1. Next, for each centrality metric, we start the attacks by removing the node (and all its links) with the highest ranking according to the chosen centrality metric (when two nodes have the same highest ranking at the step of the attack, the removed node is chosen randomly out of those two nodes). After each node removal, we recalculate the values of the centrality

[3] University of Girona, Network Robustness simulator, available at: http://nrs.udg.edu/

metric, and continue by removing the node with highest ranking of the centrality metric in the current giant component of the graph (sequential attacks). In addition to the targeted attacks based on the centrality metrics presented in Sect. 5.3.1, we also investigate the random attack strategy. In this random node-attack strategy, the node to be attacked is selected randomly out of the remaining network nodes.

In Fig. 5.17, we present the *rLCC* as a function of node removals in the underlying graph of the IEEE-118 network. We observe that when we sequentially remove 25% of the nodes according to their zeta-vector rankings, we can nearly destroy the underlying graph.

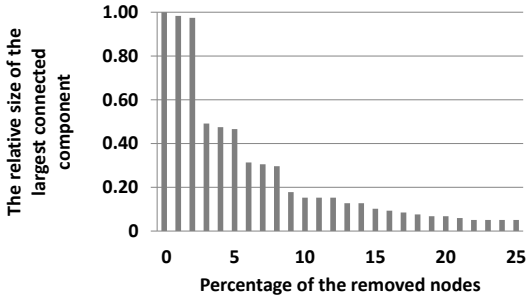


Fig. 5.17 Structural metric *rLCC* as a function of node removals based on the zeta-vector scores in the IEEE-118 network

Next, we investigate the effects of the attack strategies based on the centrality metrics presented in Sect. 5.3.1 and the random strategy. We sequentially remove up to 25% of the initial number of nodes in each real-world infrastructure, and observe the effect on the *rLCC*. When presenting our results in Tables 5.4, 5.5, and 5.6, we show the energy ε of the *rLCC*. This metric assesses the degree of a network's capability to withstand the perturbations during the node attacks. The energy ε_σ of a metric σ of the network over K successive targeted-node attacks is calculated as

$$\varepsilon_\sigma = \frac{\sum_{k=1}^{K} \sigma(k)}{K} \tag{5.6}$$

where $\sigma(k)$ is the value of the metric σ after k successive attacks. As an example, in Fig. 5.17, the energy for the IEEE-118 network against the node attacks is the sum of the *rLCC* after each attack divided by the total number of attacks.

Tables 5.4, 5.5, and 5.6 present the robustness value against the node attacks in the metro networks, power grids and telecommunication networks, respectively. The robustness value of 1 corresponds to a fully-robust network, while the lower the robustness values, the more vulnerable the network is against the targeted node attacks. For instance, among the metro networks in Table 5.4, we observe that the Rome_metro network is vulnerable to targeted attacks. The removal of 25% of the initial network nodes according to betweenness centrality or zeta-vector scores sig-

nificantly decreases the size of the giant component in the network. On the other hand, for the same networks, the random removal of nodes is slow in destroying the network.

Similar results are also valid for the attacks in power grids and telecommunication networks. As an example, according to Table 5.5, the removal of 25% of network nodes according to betweenness centrality, significantly decreases the size of the giant component in the network. In all networks, we observe that the targeted attacks based on centrality metrics are powerful ways to destroy real-world infrastructures.

Table 5.4 Robustness values for random and targeted attacks in metro networks: energy of the *rLCC*

Network name	Between-ness	Nodal degree	Close-ness	Eigen-vector	Zeta vector	Random
Athens_metro	0,447	0,508	0,616	0,528	0,459	0,656
Barcelona_metro	0,471	0,629	0,710	0,654	0,482	0,759
Berlin_metro	0,535	0,649	0,743	0,673	0,547	0,782
Boston_metro	0,369	0,432	0,551	0,450	0,347	0,682
Brussels_metro	0,428	0,540	0,592	0,511	0,409	0,699
Bucharest_metro	0,558	0,607	0,651	0,631	0,532	0,737
Buenos.Aires_metro	0,426	0,524	0,573	0,517	0,446	0,717
Cairo_metro	0,380	0,451	0,539	0,547	0,409	0,616
Chicago_metro	0,465	0,544	0,674	0,549	0,458	0,758
Delhi_metro	0,305	0,406	0,574	0,504	0,359	0,731
Hong.Kong_metro	0,359	0,458	0,528	0,488	0,374	0,620
Lisbon_metro	0,453	0,532	0,593	0,516	0,465	0,723
London_metro	0,445	0,621	0,712	0,608	0,469	0,780
Lyon_metro	0,483	0,515	0,625	0,557	0,469	0,724
Madrid_metro	0,568	0,713	0,774	0,759	0,619	0,823
Marseille_metro	0,380	0,451	0,539	0,547	0,409	0,616
Mexico.City_metro	0,628	0,704	0,775	0,755	0,666	0,801
Milan_metro	0,448	0,508	0,630	0,500	0,458	0,680
Montreal_metro	0,483	0,556	0,626	0,557	0,469	0,716
Moscow_metro	0,591	0,674	0,755	0,677	0,602	0,805
New.York_metro	0,462	0,618	0,710	0,635	0,495	0,781
Osaka_metro	0,562	0,688	0,731	0,693	0,608	0,779
Paris_metro	0,547	0,656	0,774	0,727	0,591	0,807
Prague_metro	0,453	0,535	0,596	0,554	0,471	0,713
Rome_metro	0,200	0,408	0,624	0,408	0,224	0,652
Seoul_metro	0,556	0,730	0,759	0,754	0,596	0,797
Shanghai_metro	0,552	0,613	0,708	0,590	0,527	0,761
Singapore_metro	0,514	0,577	0,649	0,596	0,491	0,710
St.Peterburg_metro	0,522	0,559	0,663	0,605	0,508	0.740
Stockholm_metro	0,312	0,416	0,444	0,379	0,315	0,670
Tokyo_metro	0,633	0,759	0,776	0,786	0,650	0,812
Toronto_metro	0,428	0,517	0,545	0,490	0,391	0,670
Washing.DC_metro	0,407	0,494	0,559	0.461	0,367	0,697

Table 5.5 Robustness values for random and targeted node attacks in power grids: energy of the *rLCC*

Network name	Betweenness	Nodal degree	Closeness	Eigenvector	Zeta vector	Random
Belgium_HV	0,251	0,337	0,552	0,382	0,249	0,703
IEEE 24	0,603	0,741	0,754	0,724	0,602	0,812
German_HV	0,280	0,437	0,629	0,492	0,309	0,732
IEEE 118	0,286	0,505	0,647	0,537	0,301	0,812
IEEE 300	0,225	0,399	0,549	0,379	0,262	0,720
IEEE 30	0,451	0,603	0,690	0,592	0,463	0,789
IEEE 57	0,490	0,643	0,692	0,677	0,498	0,772
Netherlands_HV	0,368	0,506	0,554	0,490	0,376	0,722
Poland_HV	0,222	0,364	0,568	0,563	0,258	0,726

Table 5.6 Robustness values for random and targeted node attacks in telecommunication networks: energy of the *rLCC*

Network name	Betweenness	Nodal degree	Closeness	Eigenvector	Zeta vector	Random
Abilene	0,659	0,723	0,701	0,741	0,670	0,752
Cesnet201006	0,208	0,242	0,590	0,310	0,232	0,769
Cogentco	0,239	0,409	0,520	0,378	0,242	0,686
Deltacom	0,347	0,526	0,693	0,519	0,305	0,738
Garr201201	0,206	0,301	0,614	0,333	0,221	0,745
Geant2012	0,491	0,605	0,741	0,643	0,503	0,812
GpENI_L2	0,196	0,271	0,525	0,296	0,166	0,689
Kdl	0,209	0,322	0,441	0,380	0,268	0,607
Renater2010	0,331	0,484	0,687	0,478	0,316	0,785
UsCarrier	0,228	0,355	0,426	0,340	0,223	0,606

5.4.3 Comparing the Attack Strategies in Real-world Networks

After observing the effect of the attacks on the robustness value of each network, the next step is to compare the attack strategies based on different centrality metrics. In this work, we focus on the attacks strategies according to the commonly used traditional centrality metrics (degree, betweenness, closeness, principal adjacency matrix eigenvector) and the recently proposed "zeta-vector", and random failures. To present our results, we group the networks according to their infrastructure and in Figs. 5.18-5.20, we present the comparison of the attack strategies for metro networks, power grids and telecommunication networks, respectively. In Figs. 5.18-5.20, the horizontal axis represents the ranking of the attack strategy to destroy the network, from left (1: best ranked) to right (6: worst ranked). The vertical axis represents the normalized total number of times that each attack strategy attained that rank number.

Among the different strategies, the attacks based on the betweenness centrality and zeta-vector score (in Sect. 5.3.1) are the most powerful ones to destroy the network. For instance, in the telecommunications networks in Fig. 5.20, the between-

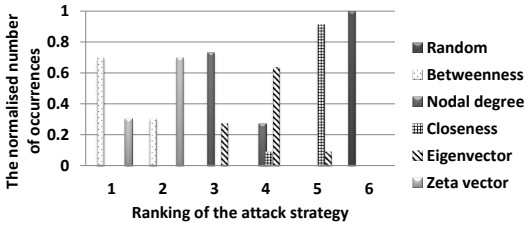


Fig. 5.18 Normalized histogram for different attack strategies in metro networks

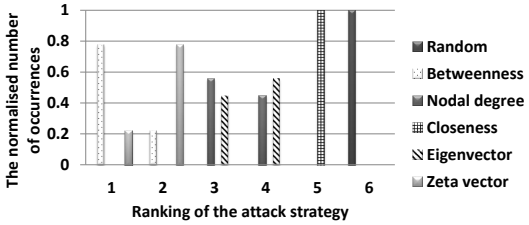


Fig. 5.19 Normalized histogram for different attack strategies in power grids

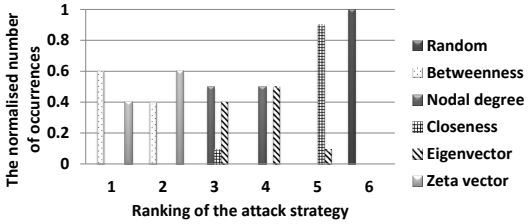


Fig. 5.20 Normalized histogram for different attack strategies in telecommunication networks

ness centrality strategy has been ranked as the *most* destructive strategy in six networks out of ten telecommunication networks, whereas the *second most* destructive strategy in the telecommunication networks is based on the zeta-vector. The worst attack strategy (i.e., the least powerful strategy to destroy the network) is a random attack strategy. This is also in-line with the common knowledge that real-world networks are usually robust against random attacks [2]. Among the attack strategies based on the tested 5 centrality metrics (i.e., among the attack strategies based on

degree, closeness, betweenness, eigenvector and zeta-vector score), the closeness centrality strategy was observed as the *worst* attack strategy.[4]

Similar results are also valid for metro networks and power grids in Figs. 5.18-5.19. In both networks, the attack strategy based on the betweenness centrality and the zeta-vector score are observed to be the most powerful strategies to destroy the network, followed by the attacks based on the degree centrality.

5.4.4 The Impact of Attacking Links: an Example

In the previous section, we have assessed the impact of multiple node removals on the *rLCC* for several real-world networks. Similarly, we can quantify the impact of multiple link removals. As an example, in this section, we study the impact of multiple link removals on the *rLCC* and the $ATTR$ metrics, for the Geant2012 telecommunication network, which consists of $N = 40$ nodes and $L = 61$ links. The link ranking and selection of links to be removed follow the same procedure as introduced in Sect. 5.4.2. However, for demonstration purposes, we perform the analysis using only the random selection of links and removal based upon betweenness centrality of the links. Link-betweenness is defined in a similar way as the nodal-betweenness, reflecting the relative importance of links.

Prior to the attack, the network attains both robustness metrics of value 1. As the links are removed, the metrics are expected to drop, and a lower value represents a less robust network.

Figure 5.21 presents the *rLCC* of the Geant2012 network when the links are removed at random or according to the ranking of their link-betweenness scores. The results confirm that random attacks (or failures) are less disruptive than targeted attacks. Moreover, after removing approximately 50% of the links, the network attains a very low *rLCC* value, which shows the attacks using link-betweenness centrality is effective in disconnecting the network.

For the link removal scenario presented in this subsection, we also investigate the $ATTR$ metric. Figure 5.22 shows the $ATTR$ metric as a function of the percentage of removed links. Regardless of the attack strategy, the network maintains an $ATTR$ equal to 1 until 10-15% of its links are removed. When the percentage of removed links is between 15% and 75%, the $ATTR$ under the random attack is much higher than the $ATTR$ the attack based upon the link-betweenness. Finally, for the attack based upon the link-betweenness, the network get severely disconnected when around 50% of its links are removed.

From Figs. 5.21-5.22, we observe that the *rLCC* and $ATTR$ seem to behave qualitatively the same under the same attack strategies. This is confirmed computing the Pearson correlation ρ between the two metrics. For the random link removals

[4] In fact, given a network destroyed by the targeted attacks, the following question arises: "What is the best strategy to reconnect the attacked nodes to return to the initial topology?", or, in other words: "In which order should the isolated nodes be reconnected?" In this *reconstruction* scenario, the robustness value of the network should increase as fast as possible.

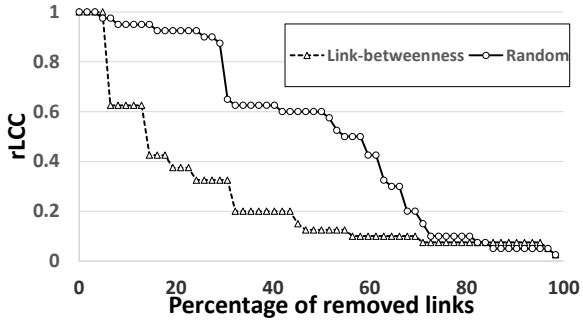


Fig. 5.21 *rLCC* metric as a function of percentage of removed links in Geant2012 network

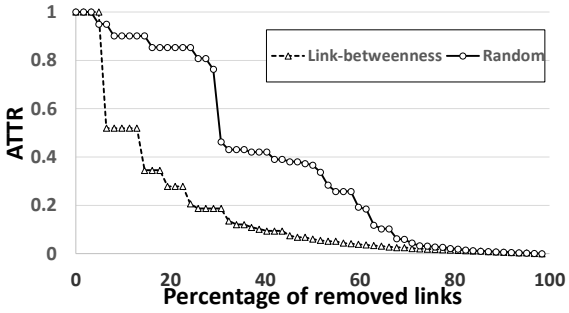


Fig. 5.22 *ATTR* metric as a function of percentage of removed links in Geant2012 network

we obtain $\rho(rLCC, ATTR) = 0.975$ while for the removals based upon the link-betweenness we find $\rho(rLCC, ATTR) = 0.993$.

5.5 Conclusions

In conclusion, in this chapter, we investigated the impact of node and links removals on real-world networks. We represented the topology of a network by a graph and identified the importance of the network nodes by using five different centrality metrics, commonly used in network science. Subsequently, we assessed the effect of targeted-node removals on the relative size of the largest connected component (*rLCC*) of the graphs and considered the energy of the *rLCC* as the robustness metric.

In most of the tested networks from three different infrastructure domains, a targeted node-attack strategy according to the betweenness centrality was the most effective in decreasing the robustness metric of the network. The strategy based upon the betweenness centrality is followed by the one based upon the zeta-vector, which is also a powerful way to decrease the overall robustness value of the network.

The worst method to destroy the tested networks is observed always as the random attack, which is expected in real-world network infrastructures. Finally, we also considered the impact of link removals on both the *rLCC* metric and the Average Two-Terminal Reliability ($ATTR$) for the Geant2012 telecommunication network. The presented methodology in this chapter can be used to evaluate the network robustness under targeted malicious attacks, natural disasters, misconfigurations, and other random events.

Acknowledgements This chapter is based on work from COST Action CA15127 ("Resilient communication services protecting end-user applications from disaster-based failures – RECODIS") supported by COST (European Cooperation in Science and Technology). The authors thank Dr. Carlos Natalino da Silva for his valuable comments and contributions.

References

1. Albert, R., Barabási, A.L.: Statistical mechanics of complex networks. Rev. Mod. Phys. **74**, 47–97 (2002). DOI 10.1103/RevModPhys.74.47. URL https://link.aps.org/doi/10.1103/RevModPhys.74.47
2. Barabasi, A.: Network Science. Cambridge University Press (2016)
3. Cetinay, H., Devriendt, K., Van Mieghem, P.: Nodal vulnerability to targeted attacks in power grids. Applied Network Science **3**(1), 34 (2018)
4. Cetinay, H., Kuipers, F.A., Van Mieghem, P.: A topological investigation of power flow. IEEE Systems Journal **12**(3), 2524–2532 (2018). DOI 10.1109/JSYST.2016.2573851
5. Cetinay, H., Soltan, S., Kuipers, F.A., Zussman, G., Van Mieghem, P.: Analyzing cascading failures in power grids under the AC and DC power flow models. In: SIGMETRICS Performance Evaluation Review, 45(3), 198-203, (2018)
6. Derrible, S., Kennedy, C.: The complexity and robustness of metro networks. Physica A: Statistical Mechanics and its Applications **389**(17), 3678–3691 (2010). DOI https://doi.org/10.1016/j.physa.2010.04.008. URL http://www.sciencedirect.com/science/article/pii/S0378437110003262
7. Dorogovtsev, S.N., Mendes, J.F.: Evolution of Networks: From Biological to the Internet and WWW. Oxford (2013)
8. Ellens, W.: Effective resistance and other graph measures for network robustness. Master thesis, Leiden University (2011)
9. Ellens, W., Spieksma, F., Van Mieghem, P., Jamakovic, A., Kooij, R.: Effective graph resistance. Linear Algebra and its Applications **435**(10), 2491–2506 (2011). DOI 10.1016/j.laa.2011.02.024
10. Estrada, E.: The Structure of Complex Networks: Theory and Applications. Oxford (2016)
11. da F. Costa, L., Rodrigues, F.A., Travieso, G., Boas, P.R.V.: Characterization of complex networks: A survey of measurements. Advances in Physics **56**(1), 167–242 (2007). DOI 10.1080/00018730601170527. URL https://doi.org/10.1080/00018730601170527
12. Freeman, L.C.: Centrality in social networks conceptual clarification. Social Networks **1**(3), 215–239 (1978). DOI https://doi.org/10.1016/0378-8733(78)90021-7. URL http://www.sciencedirect.com/science/article/pii/0378873378900217
13. Hernandez, J.M., Van Mieghem, P.: Classification of graph metrics. In: TU Delft Reports report20111111 (2011)
14. Iqbal, F., Kuipers, F.: On centrality-related disaster vulnerability of network regions. In: 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM), pp. 1–6 (2017). DOI 10.1109/RNDM.2017.8093023

15. Iyer, S., Killingback, T., Sundaram, B., Wang, Z.: Attack robustness and centrality of complex networks. PLoS ONE **8**(4), 1–17 (2013). DOI 10.1371/journal.pone.0059613. URL https://doi.org/10.1371/journal.pone.0059613
16. Jamakovic, A., Van Mieghem, P.: On the robustness of complex networks by using the algebraic connectivity. In: A. Das, H.K. Pung, F.B.S. Lee, L.W.C. Wong (eds.) NETWORKING 2008 Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet, pp. 183–194. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
17. Koschützki, D., Lehmann, K.A., Peeters, L., Richter, S., Tenfelde-Podehl, D., Zlotowski, O.: Centrality Indices, pp. 16–61. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). DOI 10.1007/978-3-540-31955-9_3. URL https://doi.org/10.1007/978-3-540-31955-9_3
18. Li, C., Wang, H., Van Mieghem, P.: Bounds for the spectral radius of a graph when nodes are removed. Linear Algebra and its Applications **437**(1), 319–323 (2012). DOI https://doi.org/10.1016/j.laa.2012.02.023. URL http://www.sciencedirect.com/science/article/pii/S0024379512001693
19. Lü, L., Chen, D., Ren, X.L., Zhang, Q.M., Zhang, Y.C., Zhou, T.: Vital nodes identification in complex networks. Physics Reports **650**, 1–63 (2016)
20. Martin Hernandez, J., Li, Z., Van Mieghem, P.: Weighted betweenness and algebraic connectivity. Journal of Complex Networks **2**(3), 272–287 (2014). DOI 10.1093/comnet/cnu007. URL http://dx.doi.org/10.1093/comnet/cnu007
21. McPhail, C., Maier, H., Kwakkel, J.H., Giuliani, M., Castelletti, A., Westra, S.: Robustness metrics: How are they calculated, when should they be used and why do they give different results? Earth's Future **6**(2), 169–191 (2018). DOI 10.1002/2017EF000649. URL https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1002/2017EF000649
22. Monsuur, H., Kooij, R., Van Mieghem, P.: Analysing and Modelling the Interconnected Cyberspace, chap. 8. P. Ducheine, F. Osinga and J. Soeters, Asser Press, The Hague, The Netherlands, Cyber warfare: critical perspectives (2012)
23. Neumayer, S., Modiano, E.: Network reliability under geographically correlated line and disk failure models. Computer Networks **94**, 14–28 (2016)
24. Newman, M.: The structure and function of complex networks. SIAM Review **45**(2), 167–256 (2003). DOI 10.1137/S003614450342480. URL https://doi.org/10.1137/S003614450342480
25. Oostenbrink, J., Kuipers, F.: Computing the impact of disasters on networks. SIGMETRICS Perform. Eval. Rev. **45**(2), 107–110 (2017). DOI 10.1145/3152042.3152075. URL http://doi.acm.org/10.1145/3152042.3152075
26. Oostenbrink, J., Kuipers, F., Heegaard, P., Helvik, B.: Evaluating local disaster recovery strategies. SIGMETRICS Perform. Eval. Rev. (2018). URL https://fernandokuipers.nl/papers/CINS2018.pdf
27. Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems **21**(6), 11–25 (2001)
28. Rueda, D.F., Calle, E., Marzo, J.L.: Robustness comparison of 15 real telecommunication networks: Structural and centrality measurements. Journal of Network and Systems Management **25**(2), 269–289 (2017). DOI 10.1007/s10922-016-9391-y. URL https://doi.org/10.1007/s10922-016-9391-y
29. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks **54**(8), 1245–1265 (2010). DOI https://doi.org/10.1016/j.comnet.2010.03.005. URL http://www.sciencedirect.com/science/article/pii/S1389128610000824. Resilient and Survivable networks
30. Sterbenz, J.P.G., Hutchison, D., Çetinkaya, E.K., Jabbar, A., Rohrer, J.P., Schöller, M., Smith, P.: Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks **54**(8), 1245–1265 (2010)
31. Talbot, D.: Massive Internet outage points to flaws in policy and technology. Available at: www.technologyreview.com/s/530431/massive-internet-outage-points-to-flaws-in-policy-and-technology/ (2014, retrieved on 2018-10-02)

32. Trajanovski, S., Marin-Hernandez, J., Winterbach, W., Van Mieghem, P.: Robustness envelopes of networks. Journal of Complex Networks **1**(1), 44–62 (2013). DOI 10.1093/comnet/cnt004. URL http://dx.doi.org/10.1093/comnet/cnt004
33. Van Mieghem, P.: Robustness of large networks. In: 2005 IEEE International Conference on Systems, Man and Cybernetics, vol. 3, pp. 2372–2377 (2005). DOI 10.1109/ICSMC.2005.1571503
34. Van Mieghem, P.: Performance Analysis of Communications Networks and Systems, 1st edn. Cambridge University Press, New York, NY, USA (2009)
35. Van Mieghem, P., Devriendt, K., Cetinay, H.: Pseudoinverse of the Laplacian and best spreader node in a network. Phys. Rev. E **96**, 032,311 (2017). DOI 10.1103/PhysRevE.96.032311. URL https://link.aps.org/doi/10.1103/PhysRevE.96.032311
36. Van Mieghem, P., Doerr, C.L., Wang, H., Hernandez, J.M., Hutchison, D., Karaliopoulos, M., Kooij, R.E.: A framework for computing topological network robustness. In: TU Delft Reports report20101218 (2010)
37. Wang, H., Hernandez, J.M., Van Mieghem, P.: Betweenness centrality in a weighted network. Phys. Rev. E **77**, 046,105 (2008). DOI 10.1103/PhysRevE.77.046105. URL https://link.aps.org/doi/10.1103/PhysRevE.77.046105
38. Wang, X., Koç, Y., Derrible, S., Ahmad, S.N., Pino, W.J., Kooij, R.E.: Multi-criteria robustness analysis of metro networks. Physica A: Statistical Mechanics and its Applications **474**, 19–31 (2017). DOI https://doi.org/10.1016/j.physa.2017.01.072. URL http://www.sciencedirect.com/science/article/pii/S0378437117300675