Inconsistencies Among Spectral Robustness Metrics

Xiangrong Wang[1(✉)], Ling Feng[2], Robert E. Kooij[1,3], and Jose L. Marzo[4]

[1] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, The Netherlands
x.wang-2@tudelft.nl

[2] Computing Science Department, Institute of High Performance Computing, A*STAR, Singapore, Singapore
fengl@ihpc.a-star.edu.sg

[3] iTrust, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, Singapore
robert_kooij@sutd.edu.sg

[4] Institute of Informatics and Applications, University of Girona, Girona, Spain
joseluis.marzo@udg.edu

Abstract. Network robustness plays a critical role in the proper functioning of modern society. It is common practice to use spectral metrics, to quantify the robustness of networks. In this paper we compare eight different spectral metrics that quantify network robustness. Four of the metrics are derived from the adjacency matrix, the others follow from the Laplacian spectrum. We found that the metrics can give inconsistent indications, when comparing the robustness of different synthetic networks. Then, we calculate and compare the spectral metrics for a number of real-world networks, where inconsistencies still occur, but to a lesser extent. Finally, we indicate how the concept of the R^*-value, a weighted sum of robustness metrics, can be used to resolve the found inconsistencies.

Keywords: Inconsistency · Graph theory · Network theory · Graph spectra · Robustness metrics

1 Introduction

Failures of real-world networks, such as blackouts in power grids, traffic congestion in transportation networks, and economic crisis in economic networks, can have an enormous impact on society, in terms of costs, safety and disruption [14]. Therefore, understanding the robustness of networks, which reflects the extent to which the networks can maintain their functionality under perturbations imposed upon them, is crucial for modern critical infrastructures. Quantifying the robustness of networks enables us to design, optimize and control the networks.

T. Q. Duong et al. (Eds.): Qshine 2018, LNICST 272, pp. 119–136, 2019.
https://doi.org/10.1007/978-3-030-14413-5_10

Recent advances in the field of network science present a number of robustness metrics, both from the topological domain and the spectral domain, characterizing the structural and dynamical properties of networks. Examples are degree distribution reflecting the connectivity of a network [1], modularity for the community structure [17], spectral radius [28] characterizing the virus spread in a network, and the algebraic connectivity [7,27] which relates to the synchronization of networks of coupled oscillators [25]. However, there is a lack of study on the relation between the robustness metrics and the interpretation of each metric in terms of the network robustness. In [19], it is shown that most metrics are not mutually independent, indicating redundancy in the characterization of robustness.

Spectral graph theory is applied in various aspects of complex networks, see for example surveys by Cvetković [5,6]. Particularly, eigenvalues and eigenvectors are used for the analysis of the robustness of complex networks [12,28,31,33]. In this paper we focus on the quantification of the robustness of complex networks, by means of spectral metrics [27]. Our main contribution is showing the occurrence of inconsistencies among the spectral metrics that quantify robustness. The inconsistencies mean that for a pair of graphs, say G and H, a pair of robustness metrics $\{M_1, M_2\}$ point in opposite direction, i.e. according to metric M_1 the graph G is more robust, but according to the metric M_2 the graph H is more robust. Because we consider eight different spectral metrics, we need to construct inconsistencies among 28 pairs of metrics. We will realize this number of inconsistencies with the help of 10 graphs, all having $N = 7$ nodes and $L = 10$ links. Next we show that inconsistencies also occur for arbitrary large pairs of graphs. Then, we calculate and compare the spectral metrics for a number of real-world networks, with numbers of nodes and links in the range 21–29 and 22–37, respectively. Finally, we indicate how the concept of the R^*-value, a weighted sum of robustness metrics, can be used to resolve the found inconsistencies.

2 Spectral Robustness Metrics

In this section, we present the definitions of the eight robustness metrics and their relation to the robustness of networks. Let $G(N, L)$ be an undirected graph with N nodes and L links. The adjacency matrix A of a graph G is an $N \times N$ symmetric matrix with elements a_{ij} that are either 1 or 0 depending on whether or not there is a link between nodes i and j. The eigenvalues of $A = A^T$ are real and can be ordered as $\lambda_N \leq \lambda_{N-1} \leq \ldots \leq \lambda_1$.

Another graph related matrix is the Laplacian matrix $Q = \Delta - A$, where $\Delta = \text{diag}(d_i)$ is the $N \times N$ diagonal degree matrix and the degree of node i is $d_i = \sum_{j=1}^{N} a_{ij}$. The eigenvalues of Q are non-negative and at least one of them is zero [27]. The eigenvalues of Q can be ordered as $0 = \mu_N \leq \mu_{N-1} \leq \ldots \leq \mu_1$.

We first present four robustness metrics which are based upon the adjacency spectrum.

2.1 Spectral Radius (SR)

The spectral radius [27] refers to *the largest eigenvalue* λ_1 of the adjacency matrix of a graph

$$SR = \lambda_1. \tag{1}$$

A larger spectral radius is associated with higher robustness of the networks with respect to link/node removals.

2.2 Spectral Gap (SG)

The spectral gap is expressed as

$$SG = \lambda_1 - \lambda_2. \tag{2}$$

According to the Perron-Frobenius theorem, λ_1 of a graph is always positive. The largest spectral gap $\lambda_1 - \lambda_2 = N$ occurs in the case of a complete graph. The spectral gap plays an important role in the dynamic processes on graphs [27]. The larger the spectral gap is, the higher the robustness of a network. A network with a large spectral gap is typically onion structured which is more robust against malicious attacks and random removals [34].

2.3 Natural Connectivity (NC)

Natural connectivity [10,16] is defined as

$$NC = \ln\left(\frac{1}{N}\sum_{k=1}^{N} e^{\lambda_k}\right). \tag{3}$$

where λ_k is the k^{th} eigenvalue of the adjacency matrix of a graph. The natural connectivity is proposed as a spectral measure for the robustness of complex networks in terms of the redundancy of alternative paths [16,33]. The higher the natural connectivity is, the higher the robustness of a network.

2.4 Minimum-Maximum Eigenvalue Ratio (MM)

The ratio of the maximum eigenvalue λ_1 to the minimum eigenvalue λ_N is defined as [36]

$$\text{MM} = \left|\frac{\lambda_1}{\lambda_N}\right|. \tag{4}$$

The ratio is used in signal detection and the stability of neural networks [22,36]. The higher the ratio of the maximum to the minimum is, the higher the robustness of a network.

Next, we introduce four spectral metrics based upon the Laplacian spectrum.

2.5 Algebraic Connectivity (AC)

The algebraic connectivity, coined by Fiedler [13], refers to the second smallest eigenvalue of the Laplacian matrix Q

$$AC = \mu_{N-1}. \tag{5}$$

It has been shown [15] that the larger the algebraic connectivity is, the more difficult it is to cut the network into components, and the higher the robustness of a network is [2,32].

2.6 Number of Spanning Trees (NST)

The total number of spanning trees [27] can be written in terms of the eigenvalues of the Laplacian matrix as

$$NST = \frac{1}{N} \prod_{j=1}^{N-1} \mu_j. \tag{6}$$

The total number of spanning trees is suggested as an indicator of network robustness [4,9]. The higher NST is, the higher the robustness of a network is.

2.7 Effective Graph Resistance (EGR)

The effective graph resistance is determined by

$$EGR = N \sum_{k=1}^{N-1} \frac{1}{\mu_k}, \tag{7}$$

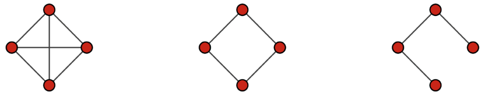
where μ_k is the k^{th} eigenvalue of the Laplacian matrix of a graph. The smaller the effective graph resistance is, the higher the robustness of a network is [8,30,31].

2.8 Eigenvalue Ratio (ER)

The eigenvalue ratio refers to the ratio of the second smallest eigenvalue μ_{N-1} to the largest eigenvalue μ_1 of the Laplacian matrix Q of a graph

$$ER = \frac{\mu_{N-1}}{\mu_1}. \tag{8}$$

The eigenvalue ratio is used to characterize the synchronizability of networks. If the eigenvalue ratio is larger, a network exhibits a better synchronizability [3,7,20].



(a) K_4 (b) C_4 (c) P_4

Fig. 1. Three types of graphs with 4 nodes.

Table 1. Spectral robustness metrics for three graphs with 4 nodes: complete graph K_4, cycle graph C_4 and path graph P_4. All of the metrics indicate that K_4 is the most robust graph.

Graphs	SR	SG	NC	MM	AC	NST	EGR	ER
K_4	3	4	1.667	3	4	16	3	1
C_4	2	2	0.868	1	2	4	5	0.5
P_4	1.618	1	0.647	1	0.586	1	10	0.172

3 Evaluation of the Spectral Metrics

First we illustrate the use of the robustness metrics, by applying them to three simple networks on 4 nodes: K_4: a complete graph, C_4: a cycle graph, P_4: a path graph, see Fig. 1. From Table 1, we see that the 8 different metrics, all rank the robustness of the three graphs, in the same way. For instance, all metrics indicate that K_4 is the most robust graph among the three graphs, as expected. This shows that, for the simple graphs here with only four nodes, the robustness metrics are consistent in their indications.

3.1 Ten Example Graphs

We use 10 different networks $G1 - G10$, to analyze the consistency of the 8 different metrics. For each of the networks, there are 7 nodes and 10 links, so that the differences are only in the way the links are constructed. Figure 2 presents the visual representations of the 10 networks. For the 10 networks, we determine the values of the 8 metrics described in the previous section. The results are listed in Table 2. It is clear that different metrics may give different indications as to which graph is the most robust, although each network has the same number of nodes and links. Such inconsistencies do not occur for the previous example of the simple graphs on four nodes.

To further illustrate this, we cross-compare each pair of metrics among the 8 metrics, and identify the pairs that give inconsistencies in Table 3. The pair of graphs in each cell are the graphs that lead to inconsistent indications of their relative robustness given by the two different metrics. For example, the cell that cross-compares the metrics Natural Connectivity (NC) and Algebraic Connectivity (AC), contains the graph pair $G1$ and $G3$. Indeed, according to Table 2, the NC indicates that $G1$ if more robust than $G3(1.51 > 1.44)$, while

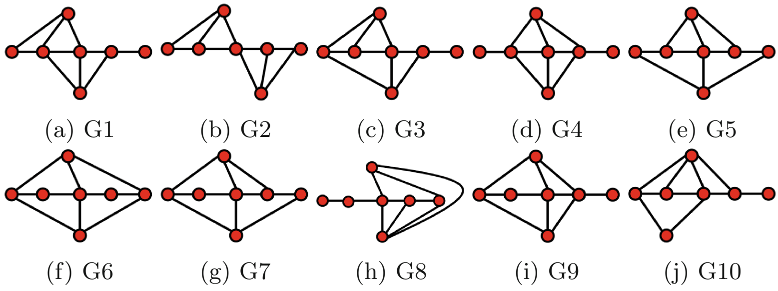


Fig. 2. The visualization of 10 artificial networks with 7 nodes and 10 links each.

AC indicates that $G3$ is more robust than $G1(0.67 > 0.63)$. For each pair of metrics, there is always at least one pair of graphs that are inconsistent, as seen in the Table 3. This means the inconsistencies are prevalent in the graphs studied, despite their similarities in terms of number of nodes and links.

3.2 All Connected Graphs with 7 Nodes and 10 Links

There are 132 possible non-isomorphic connected graphs with 7 nodes and 10 links. These graphs are generated from the programs called nauty and Traces [24]. We evaluate the inconsistency of the 8 spectral robust metrics for all the possible 132 graphs.

Figure 3 shows the rank of robustness for all the 132 graphs according to the 8 spectral robust metrics. The increase of ranking number means the decrease of robustness. The most robust graph has a ranking number 1.

The high variability in Fig. 3 suggests the inconsistency of the 8 spectral robust metrics when identifying the rank order for the 132 graphs. For example,

Table 2. Spectral robustness metrics, R* (P = 3). Every graph has $N = 7$ nodes and $L = 10$ links.

Gr	SR	SG	NC	MM	AC	NST	EGR	ER	R*
G1	3.21	1.74	1.51	**1.67**	0.63	55	21.67	0.12	0.697
G2	3	1	1.45	1.5	0.59	64	21.50	0.11	0.683
G3	3.12	1.68	1.44	1.43	0.67	64	20.56	0.12	0.681
G4	**3.35**	**2.35**	**1.58**	1.49	0.70	45	22.40	0.12	0.667
G5	3.01	1.92	1.37	1.23	**1.38**	95	16.32	**0.25**	0.649
G6	2.96	1.96	1.30	1	**1.38**	**105**	**15.62**	0.23	**0.715**
G7	2.98	1.98	1.33	1.16	1.33	101	15.88	0.23	0.698
G8	3.30	2.07	1.56	1.51	0.44	45	25.73	0.08	0.708
G9	3.16	2.16	1.44	1.25	0.83	69	18.99	0.14	0.662
G10	3.20	2.07	1.48	1.44	0.69	61	20.49	0.12	0.691

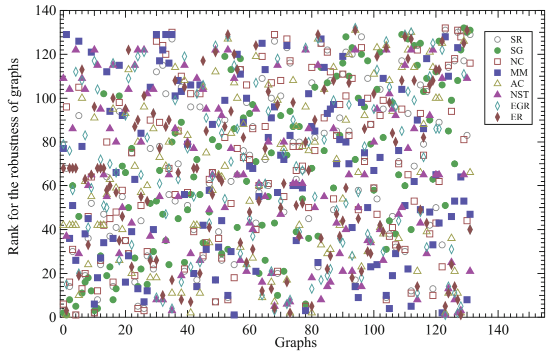


Fig. 3. Rank for the robustness of 132 graphs with 7 nodes and 10 links.

the most robust graph (rank 1, red line in Fig. 3) varies according to different spectral metrics. The spectra radius λ_1 and the natural connectivity NC identify graph 5 as the most robust network. The spectra gap SG and the algebraic connectivity AC rank graph 2 as the top robust network. According to the Minimum-Maximum eigenvalue detection MM, graph 56 is ranked the top. The number of spanning trees NST suggests that graph 124 is the most robust network. The effective graph resistance EGR identifies graph 95 and the eigenvalue ratio ER shows graph 129 as the most robust one.

Table 3. The comparison of spectral robustness metrics. For each pair of metrics, there is at least one pair of graphs that leads to inconsistent indication with respect to their relative robustness.

	SR	SG	NC	MM	AC	NST	EGR	ER
SR	X	G1:G5	G3:G9	G1:G4	G1:G3	G1:G2	G1:G2	G1:G3
SG	X	X	G1:G5	G1:G4	G3:G8	G1:G2	G1:G2	G3:G8
NC	X	X	X	G1:G4	G1:G3	G1:G2	G1:G2	G1:G3
MM	X	X	X	X	G1:G3	G1:G2	G1:G2	G1:G3
AC	X	X	X	X	X	G1:G2	G1:G2	G6:G7
NST	X	X	X	X	X	X	G3:G10	G1:G2
EGR	X	X	X	X	X	X	X	G1:G2
ER	X	X	X	X	X	X	X	X

For the pairs of graphs, the inconsistency of robust metrics is presented in Table 4 and Fig. 4. Table 4 shows the percentage of inconsistency among all possible pairs of graphs. For all the 132 graphs, there are $\binom{132}{2} = 8646$ possible graph pairs. For a pair of graphs, one robust metric concludes which graph is more robust than the other one. Two robust metrics provide either consistent conclusion or inconsistent conclusion for the same pair of graphs. After going through all the 8646 graph pairs, the percentage of inconsistency is computed for each pair of robust metrics and presented in each table cell. In Table 4, the minimum percentage is 0.06 resulted from the metric pair of the spectral radius and the natural connectivity. The non-zero minimum inconsistency percentage indicates that there is no complete consistency for all the possible pairs of graphs.

The maximum percentage of inconsistency is 91% between metrics of natural connectivity and number of spanning trees. The second and third top inconsistency percentages, 89% and 88% result from pairs of robust metrics (EGR, NST) and (EGR, ER). The top three percentages of inconsistency are further presented in Fig. 4. The high percentages (higher than 88%) highlight the challenges for graph designer to design a completely robust topology.

Table 4. The percentage of inconsistency between pairs of metrics.

	SR	SG	NC	MM	AC	NST	EGR	ER
SR	X	26%	6%	27%	68%	88%	19%	72%
SG	X	X	32%	46%	49%	64%	4%	53%
NC	X	X	X	23%	72%	91%	15%	75%
MM	X	X	X	X	67%	73%	26%	67%
AC	X	X	X	X	X	20%	86%	8%
NST	X	X	X	X	X	X	89%	16%
EGR	X	X	X	X	X	X	X	88%
ER	X	X	X	X	X	X	X	X

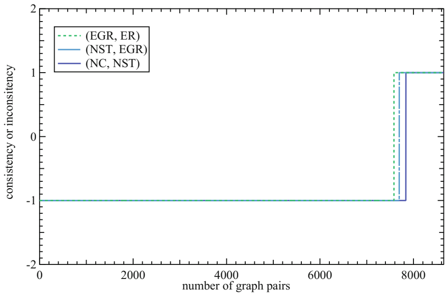


Fig. 4. The consistency (marked as 1) and inconsistency (marked as −1) results for metrics pairs of (NC, NST), (EGR, NST) and (EGR, ER).

3.3 Arbitrary Large Graphs

The examples given in the previous sections are for small graphs, with only 7 nodes. We will now give an example of an inconsistency occurring for a family of pairs of graphs that can be arbitrary large. We first consider a complete bi-partite graph K_{N_1,N_2}, consisting of two disjoint sets S_1 and S_2, containing, respectively, N_1 and N_2 nodes, such that all nodes in S_1 are connected to all nodes in S_2, while within each set no connections occur. According to [5], the spectral radius and algebraic connectivity for K_{N_1,N_2} satisfy $SR(K_{N_1,N_2}) = \sqrt{N_1 N_2}$ and $AC(K_{N_1,N_2}) = min\{N_1, N_2\}$, respectively. Note that K_{N_1,N_2} has $N_1 + N_2$ nodes.

The second graph we consider is the windmill graph $W(\eta, k)$, which consists of η copies of the complete graph K_k, with every node connected to a common node, see Fig. 5. Note that $W(\eta, k)$ has $\eta k + 1$ nodes.

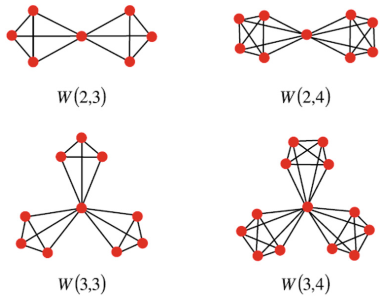


Fig. 5. Illustration of some windmill graphs $W(\eta, k)$

Estrada [11] has shown that the algebraic connectivity of $W(\eta, k)$ satisfies $AC(W(\eta, k)) = 1$, while the spectral radius $SR(W(\eta, k))$ is given by the largest zero of

$$f(\lambda) = \lambda^2 - (k-1)\lambda - \eta k = 0. \tag{9}$$

We now construct an inconsistency by choosing $N_1 = 2$ and $\eta = 2$. Assuming that the number of nodes for both graphs are equal, it follows that $N_2 = 2k - 1$. So we consider the family of pairs of graphs $H_1 = K_{2,2k-1}$ and $H_2 = W(2, k)$, with $k > 1$. It follows from the properties mentioned above that $AC(H_1) = 2 > 1 = AC(H_2)$. Substitution of $\lambda = k$ and $\eta = 2$ into Eq. (9) gives $f(k) = -k < 0$. Therefore the spectral radius of H_2 is larger than k. On the other hand, $SR(H_1) = \sqrt{2(2k-1)}$ which is smaller than k for $k \geq 4$. Hence, $SR(H_1) < SR(H_2)$, implying an inconsistency for the graphs $\{H_1, H_2\}$ for the pair of metrics $\{SR, AC\}$, for every $k \geq 4$.

For the inconsistency constructed above, the two graphs H_1 and H_2 have the same number of nodes, but not the same number of links. However, it is possible to construct inconsistencies for pairs of graphs with the same number of nodes and links. One could use a windmill graph $W(\eta, k)$ and an Erdös-Rényi graph $ER(N, L)$, choosing N and L such that the two graphs have the same number of nodes and links. For instance, consider $H_3 = W(10, 10)$ and $H_4 = ER(101, 550)$. Then both graphs have 101 nodes and 550 links. For one realization of $ER(101, 550)$ we obtain $AC(H_3) = 1 < 3.88 = AC(H_4)$ while $SR(H_3) = 15.47 > 11.66 = SR(H_4)$, which implies an inconsistency. It is possible to generalize this example to families of pairs of graphs of arbitrary size also.

3.4 Real-World Networks

In addition to artificial graphs, we now compare the different metrics on 6 real-world networks to analysis their consistencies. These networks are taken from the so-called Internet Topology Zoo (http://www.topology-zoo.org/), a collection of data network topologies from around the world, see also [18]. The networks include AboveNet, AGIS, Atmnet, Bbnplanet, Bizent and BtEurope networks. Their topologies are presented in Fig. 6. These networks have comparable number of nodes N and number of links L, but differ significantly in their topological structures, as shown. Table 5 shows the robustness metrics of the various networks, and Table 6 shows the relative rankings of them according to each metric. In both tables, the results depicted in columns R*5 (for P = 5) and R*10 (for P = 10) are analyzed in Sect. 5.

Table 5. The spectral robustness, R*5 (P=5) and R*10 (P=10) metrics for real-world networks.

Gr	N	L	SR	SG	NC	MM	AC	NST	EGR	ER	R*5	R*10
Abovenet	23	31	3.13	0.35	1.21	1.20	0.17	$262K$	425	0.027	0.776	0.638
AGIS	25	30	3.17	0.58	1.11	1.13	0.20	6376	579	0.027	0.768	0.668
Atmnet	21	22	2.29	0.28	0.87	1.00	0.09	107	592	0.019	0.742	0.572
Bbnplanet	27	28	2.89	0.42	0.95	1.05	0.12	34	931	0.018	0.762	0.654
Biznet	29	33	2.50	0.09	0.94	1.09	0.04	8856	1391	0.008	0.749	0.667
BtEurope	24	37	5.10	2.56	2.15	1.49	0.44	$612K$	372	0.031	0.799	0.665

Table 6. The relative rankings of real-world networks according to each spectral robustness metrics.

Graphs	SR	SG	NC	MM	AC	NST	EGR	ER	R*5	R*10
AboveNet	3	4	2	2	3	2	2	2	2	5
AGIS	2	2	3	3	2	4	3	3	3	1
Atmnet	6	5	6	6	5	5	4	4	6	6
Bbnplanet	4	3	4	5	4	6	5	5	4	4
Biznet	5	6	5	4	6	3	6	6	5	2
BtEurope	1	1	1	1	1	1	1	1	1	3

The same inconsistencies are found in these 6 networks, although the relative rankings do not differ much. In particular, the BtEurope network has the highest robustness ranking for every metric. In addition, we see that EGR and ER metrics give exactly the same rankings for all of the networks. Therefore, it is interesting to note that, although the various metrics could give different indications of relative robustness rankings, the most robust structure in real-world networks can be consistent across different metrics. It shows a certain level of consistency, with inconsistencies remaining in the less robust network structures.

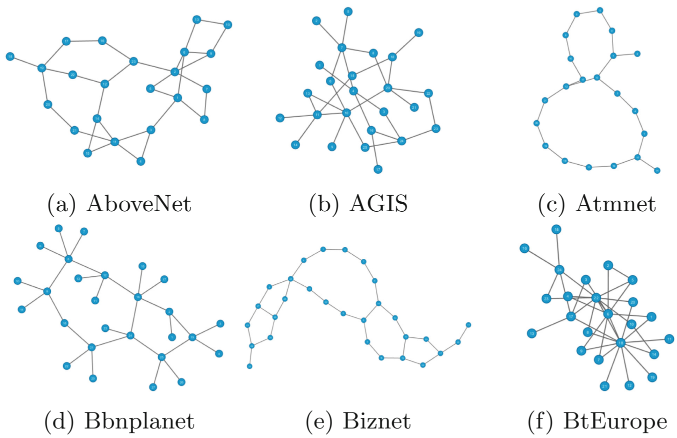


Fig. 6. The visualization of six real-world networks.

4 R^*-Value as Robustness Metric

One possible approach to deal with the observed inconsistencies, is to make explicit, for every specific case study, the definition of robustness. For instance, Wang et al. [29] studied the robustness of 33 metro networks in the world, and took as an experimental robustness definition, the fraction of nodes that have to be removed from the metro network, such that the remaining largest connected component is 90% of the original network size. It is shown in [29] that with this definition, the effective graph resistance captures very well the robustness of the metro networks.

Another way to deal with the inconsistencies is to use the information of all spectral metrics. As an example, based upon Table 2, we might conclude that graphs $G4$ and $G6$ are the most robust, because for both, 3 out of the 8 spectral metrics indicate them as the most robust. Of course one could construct much more complicated ways to combine the 8 spectral metrics.

4.1 R^*-Value: Definition

The idea of expressing the robustness value (or R-value) of a network as a weighted sum of a number of metrics, was first proposed by Trajanovski et al. [26]:

$$R = \sum_{k=1}^{K} s_k \, t_k, \tag{10}$$

where K is the number of considered metrics, t_k denote graph metrics and s_k their corresponding weights. However, this is a static analysis and the problem of determining the weights s_k is still present. To overcome this issue, the R-value concept was enhanced by Manzano et al. in [21], leading to the concept of the R^*-value, see Eq. (11):

$$R^* = \sum_{k=1}^{K} \widehat{v}_k \, t_k. \tag{11}$$

Here, the weights $\widehat{v}_k$ reflect the relative importance of the metrics t_k, when elements of the network are removed subsequently. The values of the weights are determined by applying Principal Component Analysis (PCA). In the next subsection we give more details about the calculation of the R^*-value.

4.2 R^*-Value: Calculation

The algorithm for calculating the R^*-value for a network, depends on two integers, denoted by P and M. Here P denotes the maximum number of network elements that are removed from the original network. For every number p of removed network elements, with $1 \leq p \leq P$, we conduct M independent experiments, in which each of the K metrics are determined.

The sequence of calculations is shown in Fig. 7 and detailed below. First, the metrics of the initial network with no attacks (i.e. $p = 0$) are calculated providing K metrics measurements. Note that this result is the same for all M experiments since the topology always remains the same (first row in the metrics matrix, see Fig. 7).

Once the list of elements to be removed is obtained, the K metrics are calculated for all $P \times M$ pairs. This provides a $(P \times M \times K)$ metrics matrix which contains all the computed metrics. Then, the correlation matrix $(K \times K)$ of all metric results is obtained. Then PCA is applied to the correlation matrix obtaining the v weights of each metric. PCA provides a K-dimensional eigenvector, the larger eigenvalue and its corresponding eigenvalue is selected. For comparison purposes, the initial value of R^* is normalized to 1 (maximum robustness) and the weights are modified accordingly.

Finally, by multiplying the $\widehat{v}_k$ weights for all rows in the $(P \times M \times K)$ metrics matrix as indicated in Eq. (11), the normalized robustness value R^* can be computed for all $P \times M$ cases. Then the robustness of a network is the average of all R^* values.

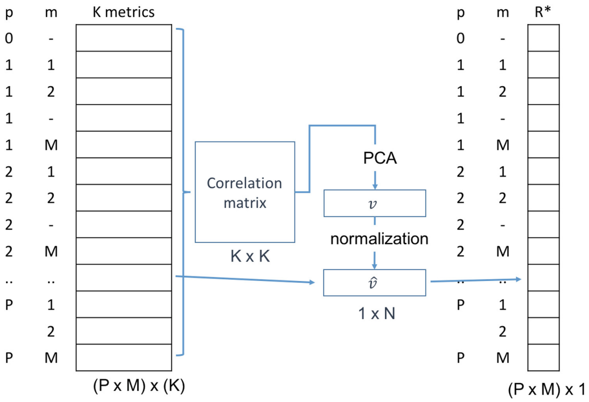


Fig. 7. $R*^{-}$value calculation overview

In the section we will use the concept of the R^*-value as the "ground truth" for the robustness of networks, in order to resolve the inconsistencies mentioned in Sect. 3.

Following the insights obtained in [23], we base the R^*-value on a combination of 10 relevant metrics. Average Nodal Degree (AND), Efficiency (EFF) and Spectral Radius (SR) are the representative structural metrics, while Largest Connected Component (LCC) and Average Two Terminal Reliability (ATTR) are the representative structural metrics for fragmentation. Algebraic Connectivity (AC) and Natural Connectivity (NC) for represent connectivity and, finally, Closeness Centrality (CLC) and Eigenvector Centrality (EC) represent centrality properties. The R^*-value is evaluated under a random node removal strategy.

5 R^*-Value Versus Spectral Metrics: Results

5.1 Comparison for the 10 Example Graphs $G1 - G10$

For this set of results, R^* has been computed by randomly removing up to 3 nodes (P = 3) in 20 independent samples (M = 20). The results are shown in column R^* of Table 2.

If we use the obtained R^*-values as ground truth, then we can resolve the inconsistencies reported in Table 3. For instance, the graph pair $G1 : G5$ leads to an inconsistency for the metric pair SR and SG. Because $R^*(G1) > R^*(G5)$ we resolve the inconsistency by stating that $G1$ is more robust than $G5$. In this way we can resolve Table 3 completely. Note that it is difficult to draw generic conclusions from this, because Table 3 only contains 8 graph pairs, namely, $\{(G1 : G5), (G3 : G9), (G1 : G4), (G1 : G3), (G3 : G8), (G1 : G2), (G3 : G10), (G6 : G7)\}$. To obtain generic conclusions one could study all resolved inconsistencies for the 8646 graph pairs mentioned in Sect. 3.2. This approach is left for further study.

Table 7. The relative rankings of artificial networks according to each spectral robustness metrics and R^* (P = 3).

Graphs	SR	SG	NC	MM	AC	NST	EGR	ER	R*
G1	3	8	3	1	8	8	8	5	4
G2	8	10	5	3	9	5	7	9	6
G3	6	9	6	4	7	5	6	5	7
G4	1	1	1	3	5	9	9	5	8
G5	7	7	8	6	1	3	3	1	10
G6	10	6	10	8	1	1	1	2	1
G7	9	5	9	7	3	2	2	2	3
G8	2	3	2	9	10	9	10	10	2
G9	5	2	6	5	4	4	4	4	9
G10	4	3	4	2	6	7	5	5	5

Table 7 presents the robustness ranking of the ten graphs G1–G10, according to the spectral metrics and the R^*-value. Here, rank 1 denotes the most robust network, while rank 10 denotes the least robust network. If we take the R^*-value as the ground truth for the robustness ranking, a few observations can be made from Table 7. Firstly, if we are only interested in the most robust network, then AC, NST and EGR lead to the same network as R^*, namely $G6$. However, the second most robust network according to R^*, i.e. $G8$, is ranked very low by these three spectral metrics, namely 10^{th}, 9^{th} and 10^{th}, respectively. Secondly, the least robust network according to R^*, i.e. $G5$, is never ranked as the least robust network by any of the 8 spectral metrics. The closest is metric NC, which gives $G5$ rank 8. Finally, out of the 10 considered graphs, the rankings of the spectral metrics re the most consistent with that of R^*, for $G10$. In contrast $G5$ is the least consistent with R^*.

5.2 Comparison for the 6 Real-World Networks

In this section we compare the robustness ranking of the six real-world networks introduced in Sect. 3.3, according to the spectral metrics and the R^*-value. We will consider two scenarios for the computation of the R^*-value, namely removal up til 5 nodes (P = 5) and up til 10 nodes (P = 10). The number of independent samples remains $M = 20$. We denote the resulting R^*-values by R^*5 and R^*10, respectively. The two right-most columns Table V give the values of R^*5 and R^*10. Table 7 gives the corresponding rankings for the real-world networks.

A few observations can be made from these tables. First of all, the two scenarios $P = 5$ and $P = 10$ lead to different rankings. This is not surprising because $P = 10$ corresponds to a more severe attack than $P = 5$. Secondly, R^*5 states that BtEurope is the most robust network. This is in line with the ranking of all spectral metrics. The least robust network according to R^*5, i.e.

Atmnet, is also recognized as a vulnerable network by the other metrics, with three metrics denoting it is the most vulnerable network.

Table 8. The distances of the rankings of real-world networks to R^*5 rankings.

Graphs	SR	SG	NC	MM	AC	NST	EGR	ER
AboveNet	1	2	0	0	1	0	0	0
AGIS	1	1	0	0	1	1	0	0
Atmnet	0	1	0	0	1	1	2	2
Bbnplanet	0	1	0	1	0	2	1	1
Biznet	0	1	0	1	1	2	1	1
BtEurope	0	0	0	0	0	0	0	0
Total distance	2	6	0	2	4	6	4	4

Table 9. The distances of the rankings of real-world networks to R^*10 rankings.

Graphs	SR	SG	NC	MM	AC	NST	EGR	ER
AboveNet	2	1	3	3	2	3	3	3
AGIS	1	1	2	2	1	3	2	2
Atmnet	0	1	0	0	1	1	2	2
Bbnplanet	0	1	0	1	0	2	1	1
Biznet	3	4	3	2	4	1	4	4
BtEurope	2	2	2	2	2	2	2	2
Total distance	8	10	10	10	10	12	14	14

Tables 8 and 9 present the distances between spectral metrics and R^* obtained by comparing the rankings of real-world networks presented in Table 6. The smaller the distance, the more similar the ranking is to the ranking of R^*5 and R^*10, respectively. The first conclusion is that, as expected, the rankings of the spectral metrics are the more similar, when the number of removed elements P is smaller. This makes sense as spectral metrics analyze the initial network (i.e. $P = 0$). For instance, Table 8 shows that NC gives exactly the same ranking as R^*5, i.e. the sum of distances equals 0. Similarly, SR and MM also present quite similar rankings (distances = 2). Instead, when comparing this with R^*10, accumulated distances are always larger (ranging from 8 (SR), best case, to 14 (EGR and ER), worst case).

Considering both tables, NC and RC complement each other, being quite similar to the R^* ranking both for small and large removal of nodes. On the other hand, NST, EGR and ER lead to less similarity in rankings, in most of the cases.

From the perspective of the network topologies, it is interesting to note that for BtEurope all spectral metrics provide very accurate results for small removal of nodes ($P = 5$), while Atmnet is the most consistent for $P = 10$.

6 Conclusion

We have shown that among 8 of frequently used spectral metrics, inconsistencies occur when using them to capture the robustness of networks. The non-zero and high percentages of inconsistency, for pair of graphs from the set of 132 graphs with 7 nodes and 10 links, suggest the challenge for the complete robust quantification of graphs. Such inconsistency is more pronounced in the artificial networks we generated than in the real-world networks tested.

One possible approach to deal with the inconsistencies, is to make explicit, for every specific case study, the definition of robustness, as was done by Wang et al. [29], who studied the robustness of 33 metro networks in the world. Another way to deal with the inconsistencies would be to use the information of all spectral metrics. With enough data at hand and with a baseline for explicit experimental values for the robustness, such as in [29], this line of reasoning, seems worth pursuing. This merging of network science and machine learning has recently also been suggested by Zanin et al. [35].

In this paper we resolved the inconsistencies by considering the so-called R^*-value, see [21], as the ground truth for robustness. In Sect. 5, Table 8 shows that robustness ranking according to spectral metrics is more similar to ranking according to R^*, when the number of removed elements (P) is small. This makes sense as spectral metrics analyze the initial network (i.e. $P = 0$). In particular, Natural Connectivity (NC) gives precisely the same ranking as R^* for $P = 5$, while Spectral Radius (SR) and Minimum-Maximum eigenvalue ratio (MM) are also good approximations. Comparisons for larger amounts of node removals ($P = 10$), show that spectral metrics generally give less similar rankings, see Table 9. When looking at the network topologies, all spectral metrics provide similar results for BtEuropa upon removal of small number of nodes and for Atmnet for larger numbers of removed nodes.

Acknowledgements. This research was supported in part by the Netherlands Organization for Scientific Research (NWO) with project number 439.16.107, the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R & D Programme (Award No. NRF 2014NCR-NCR001-40) and administered by the National Cybersecurity R & D Directorate, by the Spanish Ministry of Science and Innovation project GIROS TEC2015-66412-R and by the Generalitat de Catalunya research support program SGR-1469.

References

1. Albert, R., Jeong, H., Barabási, A.L.: Error and attack tolerance of complex networks. Nature **406**(6794), 378–382 (2000)
2. Almendral, J.A., Díaz-Guilera, A.: Dynamical and spectral properties of complex networks. New J. Phys. **9**(6), 187 (2007)
3. Barahona, M., Pecora, L.M.: Synchronization in small-world systems. Phys. Rev. Lett. **89**(5), 054101 (2002)
4. Baras, J.S., Hovareshti, P.: Efficient and robust communication topologies for distributed decision making in networked systems. In: Proceedings of the 48th IEEE Conference on Decision and Control, pp. 3751–3756 (2009)
5. Cvetković, D., Simić, S.: Graph spectra in computer science. Linear Algebra Appl. **434**(6), 1545–1562 (2011)
6. Cvetković, D.M.: Applications of graph spectra: an introduction to the literature. Appl. Graph Spectra **13**(21), 7–31 (2009)
7. Donetti, L., Hurtado, P.I., Munoz, M.A.: Entangled networks, synchronization, and optimal network topology. Phys. Rev. Lett. **95**(18), 188701 (2005)
8. Ellens, W., Spieksma, F., Van Mieghem, P., Jamakovic, A., Kooij, R.E.: Effective graph resistance. Linear Algebra. Appl. **435**(10), 2491–2506 (2011)
9. Ellens, W., Kooij, R.E.: Graph measures and network robustness. arXiv preprint arXiv:1311.5064 (2013)
10. Estrada, E.: Characterization of 3D molecular structure. Chem. Phys. Lett. **319**(5), 713–718 (2000)
11. Estrada, E.: When local and global clustering of networks diverge. Linear Algebra Appl. **488**, 249–263 (2016)
12. Estrada, E., Rodriguez-Velazquez, J.A.: Subgraph centrality in complex networks. Phys. Rev. E **71**(5), 056103 (2005)
13. Fiedler, M.: Algebraic connectivity of graphs. Czech. Math. J. **23**(2), 298–305 (1973)
14. Hines, P., Balasubramaniam, K., Sanchez, E.C.: Cascading failures in power grids. IEEE Potentials **28**(5), 24–30 (2009)
15. Jamakovic, A., Van Mieghem, P.: On the robustness of complex networks by using the algebraic connectivity. In: Das, A., Pung, H.K., Lee, F.B.S., Wong, L.W.C. (eds.) NETWORKING 2008. LNCS, vol. 4982, pp. 183–194. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79549-0_16
16. Jun, W., Barahona, M., Yue-Jin, T., Hong-Zhong, D.: Natural connectivity of complex networks. Chin. Phys. Lett. **27**(7), 078902 (2010)
17. Karrer, B., Levina, E., Newman, M.E.J.: Robustness of community structure in networks. Phys. Rev. E **77**(4), 046119 (2008)
18. Knight, S., Nguyen, H.X., Falkner, N., Bowden, R., Roughan, M.: The Internet topology zoo. IEEE J. Sel. Areas Commun. **29**(9), 1765–1775 (2011)
19. Li, C., Wang, H., De Haan, W., Stam, C.J., Van Mieghem, P.: The correlation of metrics in complex networks with applications in functional brain networks. J. Stat. Mech. Theory Exp. **25**(11), P11018 (2011)
20. Li, T., Fu, M., Xie, L., Zhang, J.F.: Distributed consensus with limited communication data rate. IEEE Trans. Autom. Control **56**(2), 279–292 (2011)
21. Manzano, M., Sahneh, F.D., Scoglio, C.M., Calle, E., Marzo, J.L.: Robustness surfaces of complex networks. Nature Sci. Rep. **4**(6133), 1–6 (2014)
22. Marcus, C.M., Westervelt, R.M.: Stability of analog neural networks with delay. Phys. Rev. A **39**(1), 347 (1989)

23. Marzo, J.L., Calle, E., Gomez-Cosgaya, S., Rueda, D., Manosa, A.: On selecting the relevant metrics of network robustness. In: 10th International Workshop on Reliable Networks Design and Modeling (RNDM) (2018)
24. McKay, B.D., Piperno, A.: Practical graph isomorphism, II. J. Symbolic Comput. **60**, 94–112 (2014)
25. Strogatz, S.H.: From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators. Phys. D Nonlinear Phenom. **143**(1), 1–20 (2000)
26. Trajanovski, S., Martín-Hernández, J., Winterbach, W., Van Mieghem, P.: Robustness envelopes of networks. J. Complex Netw. **1**(1), 44–62 (2013)
27. Van Mieghem, P.: Graph Spectra for Complex Networks. Cambridge University Press, Cambridge (2010)
28. Van Mieghem, P., Omic, J., Kooij, R.E.: Virus spread in networks. IEEE/ACM Trans. Netw. **17**(1), 1–14 (2009)
29. Wang, X., Koç, Y., Derrible, S., Ahmad, S.N., Pino, W.J., Kooij, R.E.: Multi-criteria robustness analysis of metro networks. Phys. A Stat. Mech. Appl. **474**, 19–31 (2017)
30. Wang, X., Koç, Y., Kooij, R.E., Van Mieghem, P.: A network approach for power grid robustness against cascading failures. In: 7th International Workshop on Reliable Networks Design and Modeling (RNDM), pp. 208–214. IEEE (2015)
31. Wang, X., Pournaras, E., Kooij, R.E., Van Mieghem, P.: Improving robustness of complex networks via the effective graph resistance. Eur. Phys. J. B **87**(9), 1–12 (2014)
32. Watanabe, T., Masuda, N.: Enhancing the spectral gap of networks by node removal. Phys. Rev. E **82**(4), 046102 (2010)
33. Wu, J., Barahona, M., Tan, Y.J., Deng, H.Z.: Spectral measure of structural robustness in complex networks. IEEE Trans. Syst. Man Cybern.-Part A Syst. Hum. **41**(6), 1244–1252 (2011)
34. Wu, Z.X., Holme, P.: Onion structure and network robustness. Phys. Rev. E **84**(2), 026106 (2011)
35. Zanin, M., et al.: Combining complex networks and data mining: why and how. Phys. Rep. **635**, 1–44 (2016)
36. Zeng, Y., Liang, Y.C.: Eigenvalue-based spectrum sensing algorithms for cognitive radio. IEEE Trans. Commun. **57**(6), 1784–1793 (2009)