J Netw Syst Manage (2017) 25:269–289
DOI 10.1007/s10922-016-9391-y

Robustness Comparison of 15 Real Telecommunication Networks: Structural and Centrality Measurements

Diego F. Rueda[1] · **Eusebi Calle**[1] · **Jose L. Marzo**[1]

Received: 1 August 2015 / Accepted: 2 August 2016 / Published online: 17 August 2016
© The Author(s) 2016. This article is published with open access at Springerlink.com

Abstract Multiple failures can have catastrophic consequences on the normal operation of telecommunication networks. In this sense, guaranteeing network robustness to avoid users and services being disconnected is essential. A wide range of metrics have been proposed for measuring network robustness. In this paper the taxonomy of robustness metrics in telecommunication networks has been extended and a classification of multiple failures scenarios has been made. Moreover, a structural and centrality robustness comparison of 15 real telecommunication networks experiencing multiple failures was carried out. Through this analysis the topological properties which are common for grouping networks with similar robustness are able to be identified.

Keywords Robustness analysis · Robustness metrics · Multiple failures · Targeted attacks · Random failures · Telecommunications networks

1 Introduction

Telecommunication networks are crucial infrastructures required to support a variety of human activities such as socialization, entertainment, information gathering, health and well-being, learning, transportation and emergency communications. The consequences of multiple failures in telecommunication networks are

✉ Diego F. Rueda
u1930599@campus.udg.edu

Eusebi Calle
eusebi.calle@udg.edu

Jose L. Marzo
joseluis.marzo@udg.edu

[1] Institute of Informatics and Applications, Universitat de Girona, P-IV Building, Campus Montilivi, 17071 Girona, Spain

dramatic as when they occur millions of users and services can be disconnected. In this work, and to enhance robustness, the vulnerability of networks under multiple failure scenarios has been addressed. Robustness can be defined as the ability of a network to continue performing well when it is subject to failures. Failures can be caused by fiber cuts, configuration errors, viruses and worms, cyber-attacks, terrorism or natural disasters [1].

Some research into the robustness analysis of telecommunication networks and data centers networks (DCN) has been carried out and different metrics to measure the network robustness have been proposed. In [2] some classical and contemporary robustness metrics are studied for a set of real telecommunication networks, and the most robust networks are identified by comparing the metrics obtained from simulations of failure scenarios. In [3] the robustness of real networks and generic topologies (random, scale-free and exponent) in non-failure scenarios are compared. Both, [2, 3] rank the better topologies based on their robustness metrics. In [4] an analytical comparison of well-known robustness metrics in some model and empirical networks, when random and targeted attacks occur, is performed. In [4] it is shown that the node degree centrality metric can be used as an effective strategy to remove nodes in simultaneous targeted attacks, whereas for sequential attacks it is betweenness centrality. The temporal evolution of the topological robustness of backbone telecommunication networks by identifying their trends is analyzed in [1]. In [1] it is found that modifying the structure of networks over time does not guarantee a better robustness. In [5] the robustness of random models and real networks under different scenarios is evaluated. The random and targeted attacks affect the network performance and although networks may have similar average-case performance under attack, they may differ significantly in their sensitivities to certain attack sequences [5]. In [6] the characteristics of network topologies that maintain a high level of throughput in spite of multiple attacks are studied.

As regards to DNC topologies, in [7] a multi-layered graph modeling of various DCNs topologies is presented and the structural robustness metrics analysis considering various failure scenarios is carried out. Moreover, in [7] a new procedure to quantify the DCN robustness is proposed based on the deterioration metric which evaluates the network robustness based on the percentage change in the graph structure. Classic connectivity measures are inadequate for evaluating DCN connectivity as shown in [8]. Therefore, a new connectivity metric called μ-A2TR (μ-*average two-terminal reliability*) is proposed in [8], which evaluates how difficult it is to break a network into components in the case of node or link failures. The benefits of different DCN topologies taking the reliability and survivability requirements into account are analyzed in [9]. The most robust DCN topology for both link and node failure scenarios is also identified in [9].

The aim of this work is to analyze the structural and centrality robustness of 15 real telecommunication networks under multiple failures (random and targeted). Through this analysis the topological properties for grouping networks with similar robustness are identified and compared with the results found in previous work. This paper is structured as follows. Section 2 extends the taxonomy to classify robustness metrics. Section 3 shows the type of failures that can affect telecommunication networks. In Sect. 4, the structural properties of the networks studied in this work are described while the simulation results of structural and centrality robustness metrics under multiple failure scenarios are presented and analyzed in Sect. 5. Finally, Sect. 6 provides conclusions and future work.

2 Taxonomy of Robustness Metrics

To classify robustness metrics we consider a taxonomy based on structural properties, centrality measures and services supported by networks. A preliminary version of this taxonomy can be found in [2]. Table 1 shows an extended taxonomy of robustness metrics. A description of the robustness metrics is presented in this section.

2.1 Structural Metrics

Structural metrics are a well-known area in the conventional analysis of graphs. They are also used to explain stability—or the lack of it—in a network, and

Table 1 Taxonomy of robustness metrics

Structural robustness	Centrality measures	Functional robustness
Average nodal degree ($\langle k \rangle$)	Degree centrality (d_c)	Elasticity (E)
Average shortest path length ($\langle l \rangle$)	Eigenvector centrality (e_c)	Quantitative robustness metric (QNRM)
Diameter (D)	Closeness centrality (c_c)	Qualitative robustness metric (QLRM)
Assortativity coefficient (r)	Betweenness centrality (b_c)	Endurance (ξ)
Heterogeneity (σ_k)	Cross-clique centrality	R-value
Efficiency (ε)	Spreaders	R*-value (robustness surfaces (Ω))
Vertex connectivity (κ)		
Edge connectivity (ρ)		
Cluster coefficient ($\langle C \rangle$)		
Symmetry ratio (SR)		
Largest eigenvalue (λ_1)		
Algebraic connectivity (λ_2)		
Natural connectivity ($\bar{\lambda}$)		
Effective graph resistance (EGR)		
Graph diversity (GD)		
Weighted spectrum (WS)		
Percolation limit (ρ_c)		
Number of spanning trees (NST)		
Average two-terminal reliability (ATTR)		
Viral conductance (VC)		

determine how viruses spread through a network under node/link removal [10]. Preliminary robustness analysis is carried out by considering the following basic network properties: *average nodal degree* ($\langle k \rangle$), *average shortest path length* ($\langle l \rangle$), *diameter* (D) and *assortative coefficient* (r) [2]. In this sense, networks with higher $\langle k \rangle$ are considered better-connected on average and, consequently, are likely to be more robust (i.e. there are more chances to establish new connections). In regards to $\langle l \rangle$, it is calculated as an average of all the shortest paths between all the possible origin–destination vertex pairs of the network. A network is more robust if $\langle l \rangle$ is at its lowest as it is likely to lose fewer connections. D is the longest of all the shortest paths between pairs of nodes, thus one would want the diameter of networks to be low. The r coefficient lies within the range [–1, 1] and it defines two types of networks. *Disassortative* networks with $r < 0$ have an excess of links connecting nodes of dissimilar degrees. The opposite properties apply to *assortative* networks with $r > 0$ that have an excess of links connecting nodes of similar degrees [11]. As can be found in [4], such networks exhibit greater vulnerability to certain types of targeted attacks.

Based on $\langle k \rangle$, the *heterogeneity* (σ_k) is a coefficient of variation of the connectivity. σ_k is defined as the standard deviation of the $\langle k \rangle$ divided by the $\langle k \rangle$. The lower σ_k value translates to higher network robustness. The *Efficiency* (ε) as the averaged sum of the reciprocal (multiplicative inverse) of the shortest paths is also defined. The greater the ε value, the greater its robustness is. *Vertex connectivity* (κ) represents the smallest number of nodes that must be removed to disconnect the network. The same definition can be applied to *edge connectivity* (ρ) when considering links instead of nodes. The *clustering coefficient* ($\langle C \rangle$) captures the presence of triangles formed by a set of three nodes, and compares the number of triangles to the number of connected triples.

In addition, structural metrics also use the adjacency and Laplacian matrices to abstract and calculate the robustness of the networks. The *symmetry ratio* (SR) is calculated as the quotient between the distinct eigenvalues of the network adjacency matrix and the diameter D. Networks with low SR are considered more robust to random failures or targeted attacks. The *largest eigenvalue or spectral radius* (λ_1) is the largest nonzero eigenvalue of the adjacency matrix of a network [10]. Generally, networks with high values of λ_1 have a small D and higher node distinct paths. The λ_1 metric also provides information on network robustness [11] and captures the virus propagation properties of networks defining an epidemic threshold of node infection [12].

Algebraic connectivity (λ_2) is defined as the second smallest Laplacian eigenvalue. λ_2 measures how difficult breaking the network into different components is. Higher λ_2 values indicate better robustness [13]. Networks with identical λ_2 can be compared using *natural connectivity* ($\overline{\lambda}$). The $\overline{\lambda}$ metric characterizes the redundancy of alternative paths by quantifying the weighted number of closed walks of all lengths. In addition, $\overline{\lambda}$ is expressed as the average of the eigenvalues of the adjacency matrix, where a higher value indicates a more robust network. [14]. *Effective graph resistance* (EGR), can be written as a function of nonzero Laplacian eigenvalues. The EGR metric measures the number of paths between two nodes and their length. The smaller the EGR value is, the more robust the network [15].

The *graph diversity* (GD) is related to the number of nodes shared with the shortest path considering all possible paths between two nodes. This metric is equal to one when paths do not share any common point of failure (node or link). The total graph diversity (TGD) is the average of all effective path diversity (EPD) over all paths. Consequently, calculating this metric requires significant computational resources. Larger TGD indicates greater robustness [16].

The *weighted spectrum* (WS) metric is based on the eigenvalues (λ_i) of the normalized Laplacian matrix and the N-cycle of a graph. Different values of N indicate different topology properties to be analyzed e.g. $N = 3$ is associated to the clustering coefficient, meanwhile $N = 4$ is related to the number of disjoint paths in a network. The network robustness is calculated as $W' - W$, where W denotes the default WS of the original graph and W' denotes the WS of the resulting graph after link or nodal failures [17].

The *percolation limit* or percolation threshold (ρ_c) returns the critical fraction of nodes that need to be removed before the network disintegrates. The *degree diversity* is taken into account to calculate the percolation limit, as can be seen in [3]. Hence, the higher degree diversity is, the higher the percolation limit is. Then, a higher ρ_c indicates the fraction of vertices that can be removed without disconnecting the network is higher, which means the network is more robust. The *number of spanning trees* (NST) counts all possible spanning trees that exist for a graph. It has been proven that the number of spanning trees can be written as a function of the unweighted Laplacian eigenvalues [3].

The *average two-terminal reliability* (ATTR) delivers the probability of connectivity between a randomly chosen node pair [18]. ATTR is one when the network is fully connected; otherwise ATTR is the number of node pairs in every connected component divided by the total number of node pairs in the network. ATTR also gives the fraction of node pairs that are connected to each other [19]. At failure scenarios, the higher the average two-terminal reliability is, the higher the robustness is.

The last structural metric is *viral conductance* (VC), where the robustness is measured with respect to virus spread [20]. This metric is measured by considering the area under the curve that provides the fraction of infected nodes in steady-state for a range of epidemic intensities. The lower the VC in a network, the more robust, with respect to virus spread, it is. However, as this work is focused on random failures and targeted attacks, the VC metric is not evaluated.

2.2 Centrality Metrics

This group of metrics attempts to identify which elements in a network are the most important or central [4]. Consequently, they could help disseminate information in the network faster, stopping epidemics, and protecting the network from breaking. These metrics also define the network centralization as a measure of how central the most central node is in relation to how central all the other nodes are [21]. Centralization, which is a key characteristic of a network, can be used to measure network robustness as the differences between the centrality of the most central node and that of all others [21]. In general, the most central network is the most robust i.e. if the network has more nodes with similar centrality values, there are then several spots to attack when centrality metrics are used to select the elements to be removed.

A wide number of centrality metrics has been proposed to identify the most central nodes in networks. However, the following are the most common: *degree centrality*, *eigenvector centrality*, *closeness centrality*, *betweenness centrality* and *spreaders*. In degree and eigenvector centralities the importance of a node is given in terms of its neighbors, whereas in closeness and betweenness centralities the importance is related to the path lengths.

Degree centrality (d_c) is the simplest measure of nodal centrality, and is determined by the number of neighbors connected to a node [22]. The larger the degree, the more important the node is. However, if a node with a high nodal degree fails, potentially higher numbers of connections are also prone to being affected. In many real networks only a small number of nodes have high degrees. Accordingly, *eigenvalue centrality* (e_c) is based on the notion that a node should be viewed as important if it is linked to other important nodes [22]. The e_c is proportional to the sum of the centrality scores of its neighbors, where the centrality corresponds to the largest eigenvector of the adjacency matrix. Thus, e_c can take a large value either by the node being connected to many other nodes or by it being connected to a small number of important nodes.

With *closeness centrality* (c_c) the nodal importance is measured by how close a node is to other nodes [22]. It is based on the length of the shortest path between a given node and all other nodes in the network. An important node is typically close to the other node if it can reach the whole network more quickly than non-close nodes. *Betweenness centrality* (b_c) is when the number of shortest paths that pass through a given node is counted [22]. A node may have a high betweenness centrality while being connected to only a small number of other vertices (not necessarily important/central). This is due to the fact that nodes that act as bridges between groups of other nodes typically have high b_c. Thus, nodes with high b_c play a broker role in the network and are important in communication and information diffusion [22]. Similar to b_c, the *link betweenness centrality* (l_c) can be also calculated as the degree to which a link makes other connections possible.

Centrality metrics also take into account measures in epidemic scenarios where the best spreaders of an epidemic do not correspond to the most central nodes. Instead, the most efficient spreaders are those located within the core of the network according to a *k*-shell decomposition analysis [23]. This metric is not evaluated in this work as it is focused on random and targeted attacks.

2.3 Functional Metrics

This set of metrics quantifies the variation of the performance of a network in response to multiple failures by focusing on the Quality of Service (QoS) parameters of the established connections. *Elasticity* (E), the *quantitative robustness metric* (QNRM) and the *qualitative robustness metric* (QLRM) measure the robustness based on a single QoS parameter such as the throughput, the number of blocked connections or the established connections as a function of $\langle l \rangle$, respectively, [6, 24]. The higher these metric values are, the more robust the network is. Using the *R-value*, the network robustness is given by an arbitrary topological vector and a weight vector. The topological vector components take into consideration one or more QoS parameters, network properties or any other structural robustness metric e.g. hop-count, average shortest path length ($\langle l \rangle$), maximum nodal degree (k_{max}) or algebraic connectivity (λ_2). The weight vector components reflect the importance of the topological vector for network service. The higher the *R-value*, the greater the robustness is [25].

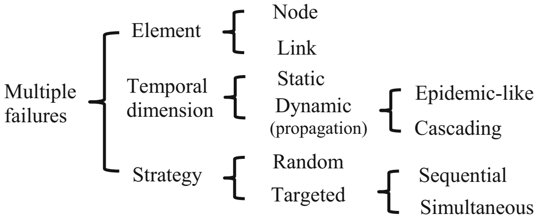
Endurance (ξ) is also calculated by one or more QoS parameters (e.g. delay) or topological metrics (e.g. size of the largest connected component). In contrast to the *R-value*, ξ places greater importance on perturbations affecting low percentages of elements in a network. ξ is normalized to the interval [0, 1], where $\xi = 1$ denotes the non-existence of robustness, whereas $\xi = 0$ is correlated to the maximum possible degree of robustness [26]. The last functional metric is *R*-value* which is the *R-value* computed via a normalized eigenvector or principal component (PC). The PC gives dimension and non-arbitrary weights to each of the robustness metrics. Without failures the *R*-value* is set to one and can take values in the interval $[0, +\infty)$ when failures are considered [27]. A graphical representation of the *R*-value* is called the robustness surface (Ω), and enables a visual assessment of network robustness variability [27] to be made.

3 Multiple Failure Scenarios

Failures can affect the normal operation of network elements (nodes or links). Therefore, services supported by a network and users connected to it may experience catastrophic consequences. Figure 1 shows how multiple failures can be classified. According to temporal dimension, failure types can be either static or dynamic. *Static multiple failures* are essentially one-off failures that affect one or more elements at any given moment. *Dynamic failures* have a temporal dimension and they can be determined as being epidemic or cascading failures [2].

Other failure scenarios are induced with the strategy used to remove nodes or links. Thus, when an object that causes an attack knows and uses precise information from the network's topological structure, it is called an attack with white-information (*targeted*). However, when the attacker has little or no

Fig. 1 Taxonomy of multiple failures



information, it is considered a black-information attack (*random*). The former would be more related to intentional failures, while the latter would be with unintentional failures [2].

In *random failures*, nodal or link failures occurs randomly e.g. a fiber cut by a natural disaster. While in *targeted failures,* network elements are attacked (removed) with the purpose of maximizing the impact of the attack over the network e.g. in backbone telecommunication networks the most vulnerable routers can be identified by the number of shortest paths passing through a given router or by the number of physical links from one router to others [4]. Moreover, other "real world" features, such as the number of potentially affected users and socio-political and economic considerations are also used to rank the nodes to be removed in telecommunication networks [2].

In *targeted failures* there are two distinct schemes for selecting the elements to be removed. In a *simultaneous targeted attack*, the centrality metric is calculated for all elements (node or link) in the network and then a specified fraction of the elements is removed in order of the centrality measure, from highest to lowest [4]. In a *sequential targeted attack* the centrality measure is calculated for all the elements in the initial network, and the element with the highest centrality value is then removed. Next, the centrality measures of all the elements in the resulting network are recalculated and once again the highest ranked element is removed. This process of recalculating the centrality measures and removing the highest ranked element is continued until the desired fraction of elements has been removed [4].

4 Network Topologies

In this section the topological properties of the 15 real telecommunication networks are described. This set of networks was selected through a careful search in specialized databases considering the number of times that they were used in relevant publications e.g. a preliminary robustness analysis of this set of topologies can be found in [1–3]. The topologies are part of important telecommunication networks repositories such as [28, 29]. Thus, the 15 real telecommunication networks serve as a standardized benchmark for testing, evaluating, and comparing several network robustness metrics.

Some of these networks are backbone transport networks (representing real physical links), whereas others are logical networks (representing the IP layer). Then, the selected networks offer a wide range of topological properties which allow structural and centrality robustness analysis to be carried out. By comparing their network robustness, the common topological properties that can be used to group networks with similar robustness under random failures and target attacks are identified.

Each network topology is modeled by a graph G (V, E), which is given by a vertex set $V = \{v_1, v_2, \ldots, v_n\}$ and an edge set $E = \{e_1, e_2, \ldots, e_m\}$. Vertex (i.e. nodes) can be routers, switches, hosts, or any telecommunication equipment, and edges (i.e. links) can be optical fiber cables, wired or wireless links (physical or virtual). The graph representation and topological map of this set of networks can be found in [28, 29]. Table 2 presents the main topological properties of the 15 real telecommunication networks: *number of nodes* (n), *number of links* (m), *average nodal degree* ($\langle k \rangle$) ± *standard deviation* (StDev), *maximum nodal degree* (k_{max}), *average shortest path length* ($\langle l \rangle$), *diameter* (D) and *assortativity coefficient* (r). The networks have different sizes ranging from 11 to 754 nodes and from 14 to 899 links. ABILENE is the smallest network with 11 nodes and 14 links, whereas the KDL network is the largest with 754 nodes and 899 links.

As can be seen in Table 2, the TISCALI_L3 and DELTACOM networks have higher $\langle k \rangle$ with 5.0588 and 3.2389, respectively. In contrast, SPRINT_L1 and KDL have the lowest $\langle k \rangle$ values, 2.3712 and 2.3846, respectively. According to k_{max}, TISCALI_L3 has the node with the highest number of connections (22), whereas ABILENE has the node with the lowest degree (3). In telecommunication networks, k_{max} is used to identify the most important node according to the number of links. Therefore, if the node with high nodal degree fails, a potentially higher number of connections are also prone to being affected.

In terms of $\langle l \rangle$ and D, ABILENE and TISCALI_L3 have the lowest values for these properties. The former has $\langle l \rangle = 2.4182$, while the latter has $\langle l \rangle = 2.4298$. Both networks have D = 5. Nonetheless, KDL and SPRINT_L1 with 22.727 and 14.705 have the higher values of $\langle l \rangle$, and KDL and US_MW have the higher D values, 58 and 42, respectively. Finally, Table 2 shows that most of the networks analyzed have a negative or near to zero value of r. DELTACOM (0.3158) is the most assortative network and CESNET (−0.3739) is the most disassortative. As explain above, when $r < 0$ the network is said to be *disassortative*, meaning that it has an excess of links connecting nodes of dissimilar degrees, whereas a*ssortative*

Table 2 Topological properties of the 15 real networks

Network	n	m	⟨k⟩ ± StDev	k_{max}	$\langle l \rangle$	D	r
ABILENE	11	14	2.55 ± 0.52	3	2.42	5	0.067
GEANT	40	61	3.05 ± 1.95	10	3.53	8	−0.204
RENATER	43	56	2.60 ± 1.70	10	3.93	9	−0.1544
GpENI_L2	51	61	2.39 ± 1.73	9	4.69	10	−0.232
TISCALI_L3	51	129	5.06 ± 5.42	22	2.43	5	−0.361
CESNET	52	63	2.42 ± 3.13	19	3.05	6	−0.374
GARR	61	89	2.92 ± 3.09	14	3.62	8	−0.258
CORONET_L1	100	136	2.72 ± 0.83	5	6.67	15	0.035
DELTACOM	113	183	3.24 ± 1.85	10	7.16	23	0.316
USCARRIER	158	189	2.39 ± 0.82	6	12.09	35	−0.095
COGENTCO	197	245	2.48 ± 1.06	9	10.51	28	0.02
SPRINT_L1	264	313	2.37 ± 0.81	6	14.70	37	−0.188
ATT_L1	383	488	2.55 ± 1.15	8	14.13	39	−0.062
US_MW	411	553	2.69 ± 1.13	7	13.65	42	0.112
KDL	754	899	2.38 ± 0.85	7	22.73	58	−0.096

networks are when $r > 0$ indicating an excess of links connecting nodes of similar degrees.

5 Results and Discussion

In this section, initially, the measurement of structural and centrality robustness metrics in a static scenario are presented and a preliminary robustness comparison is carried out. Then, some simulation scenarios are set up to allow the robustness under random and targeted attacks to be evaluated and analyzed. Most metrics presented in Fig. 2 were simulated under multiple failure scenarios. However, in this work only the more relevant results are presented as the metrics analyzed allow

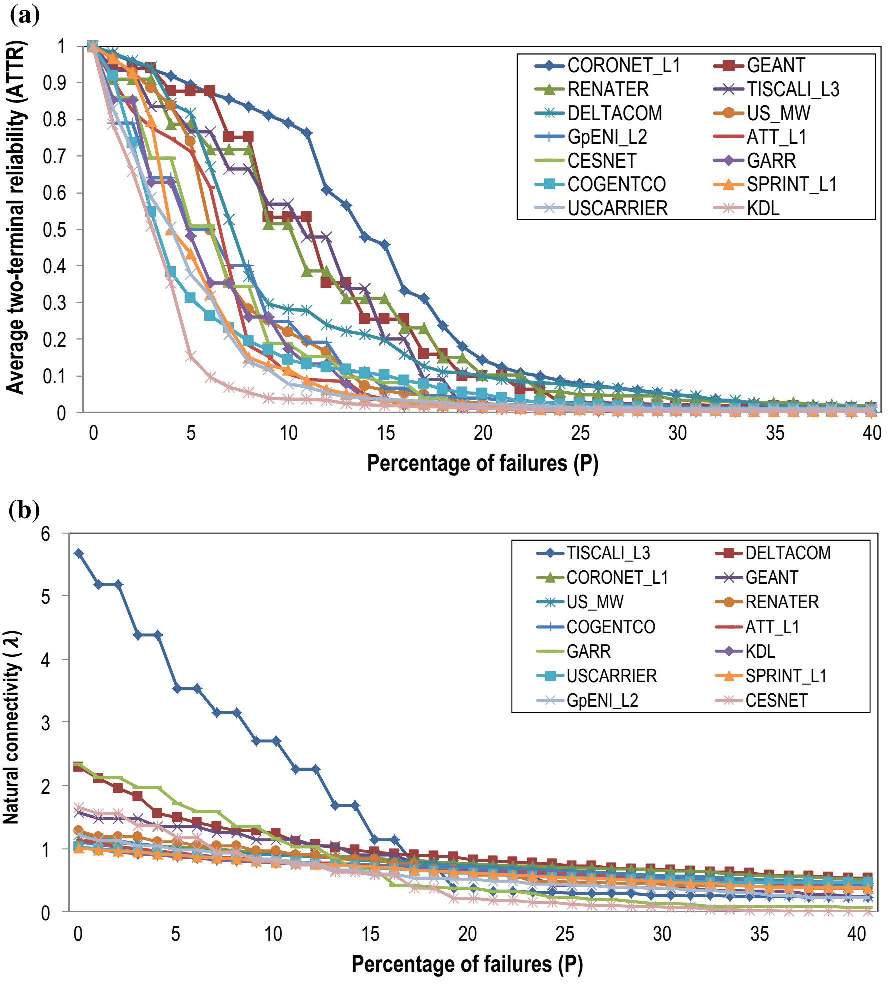


Fig. 2 Structural results for simultaneous targeted attack. **a** Average two-terminal reliability (ATTR) results and **b** natural connectivity ($\bar{\lambda}$) results

the robustness behavior of the set of the 15 real networks to be abstracted for grouping according to common topological properties.

Multiple failure scenarios were simulated for random and targeted attacks and in each one a subset of the structural and centrality robustness metrics is analyzed. The nodes to be removed in the simultaneous targeted attacks were selected by their *degree centrality*, whereas for the sequential targeted attacks they were selected by their *betweenness centrality*. In all scenarios, the percentage of nodes removed (P) ranged from 1 to 70 %. Twenty and ten runs were performed for random and targeted attacks, respectively. For each of the runs, different subsets of nodes were selected according to the failure scenario.

5.1 Robustness Comparison in a Static Scenario

Table 3 shows the measures of the structural and centrality robustness metrics for the defined set of real networks in a static scenario. The first and second columns in Table 3 show that ABILENE and CORONET_L1 have maximum *vertex connectivity* (κ) and *edge connectivity* (ρ), (two in each case), i.e. more than one element must be removed to break these networks. The *clustering coefficient* ($\langle C \rangle$) shows that the TISCALI_L3 (0.3776) and GPENI_L2 (0.1847) networks are the most robust. Their nodes are more interconnected with their neighbors as there are many triangles (i.e. many alternative paths) in case of nodal or link failures. However, for the CORONET_L1 network, $\langle C \rangle = 0$ as it does not have any triangles, as can be seen in its topological map available in [29]. As regards to the *symmetry ratio* (SR), the lowest value indicates high robustness. Thus, ABILENE and USCARRIER, with *SR* values equal to 2.2 and 4.5143, respectively, are the most robust networks. Thereby, SR suggests that the impact caused by removing a node does not depend on which node is removed [2].

With the *largest eigenvalue* (λ_1), TISCALI_L3 and DELTACOM are the more robust networks, with values of 9.5895 and 6.0015, respectively. On the other hand, TISCALI_L3 and ABILENE have the highest values of the second smallest Laplacian, each one with 0.5255 and 0.3238. Therefore, according to the *algebraic connectivity* (λ_2), they are the most robust networks. Also, for the TISCALI_L3 and ABILENE networks a similar robustness result can be concluded from their low values of D and $\langle l \rangle$. Nonetheless, DELTACOM is one the most robust networks according to λ_1, with a low λ_2 value (0.0233) and high values of $\langle l \rangle$ (3.2389) and D (10), the robustness results are opposite. In this case, a relevant conclusion about its robustness cannot be drawn as the λ_1 and λ_2 metrics rank DELTACOM network in a different way.

Based on *natural connectivity* ($\bar{\lambda}$), TISCALI_L3 and GARR are the most robust networks having the highest values at 5.6718 and 2.3343, respectively. With the *effective graph resistance* (EGR), the better robustness is for ABILENE and GEANT as they obtain the smallest values of EGR: 7.54E+01 and 1.31E+03, respectively, however, KDL and US_MW obtain the worst EGR (with values of 1.98E+06 and 3.48E+05, respectively). *Weighted spectrum* (WS) was calculated

Table 3 Structural and centrality robustness metrics in a static scenario

Network	κ	ρ	$\langle C \rangle$	SR	λ_1	λ_2	$\overline{\lambda}$	EGR	ρ_c	WS	NST	d_c	e_c	c_c	b_c	l_c
ABILENE	2	2	0.15	2.2	2.68	0.33	1.10	7.5E+01	0.39	0.33	2.5E+02	0.05	0.35	0.24	0.20	0.09
GEANT	1	1	0.15	5	4.39	0.14	1.57	1.3E+03	0.69	0.70	6.9E+10	0.18	0.79	0.30	0.45	0.09
RENATER	1	1	0.17	4.78	3.88	0.14	1.28	1.8E+03	0.63	0.71	4.3E+08	0.17	0.83	0.22	0.40	0.09
GpENI_L2	1	1	0.18	5.1	3.74	0.054	1.22	4.5E+03	0.62	1.25	5.5E+05	0.13	0.81	0.21	0.42	0.21
TISCALI_L3	1	1	0.38	10.2	9.59	0.53	5.67	1.3E+03	0.89	0.77	1.9E+22	0.34	0.76	0.38	0.29	0.01
CESNET	1	1	0.08	8.67	4.97	0.14	1.65	2.8E+03	0.81	0.41	8.7E+05	0.33	0.87	0.46	0.69	0.24
GARR	1	1	0.05	7.63	5.79	0.12	2.33	3.8E+03	0.80	0.19	5.6E+10	0.18	0.83	0.33	0.46	0.08
CORONET_L1	2	2	0	6.67	3.29	0.05	1.13	1.0E+04	0.49	0	1.5E+26	0.02	0.85	0.09	0.20	0.07
DELTACOM	1	1	0.09	4.91	6.00	0.02	2.29	1.8E+04	0.69	1.67	1.8E+33	0.06	0.94	0.15	0.40	0.05
USCARRIER	1	1	0.06	4.51	2.98	0.01	1.03	8.36E+04	0.40	1.78	4.6E+23	0.02	0.92	0.07	0.45	0.27
COGENTCO	1	1	0.01	7.04	3.79	0.01	1.09	9.4E+04	0.48	0.41	5.9E+34	0.03	0.94	0.09	0.34	0.15
SPRINT_L1	1	1	0.03	7.14	2.93	0.01	1.01	2.0E+05	0.39	1.42	7.6E+41	0.01	0.96	0.06	0.28	0.16
ATT_L1	1	1	0.04	9.82	3.71	0.01	1.14	3.3E+05	0.52	2.59	5.9E+74	0.01	0.97	0.05	0.19	0.10
US_MW	1	1	0.05	9.79	4.22	0.01	1.21	3.4E+05	0.54	3.44	2.0E+94	0.01	0.96	0.07	0.25	0.12
KDL	1	1	0.03	13	3.17	0.01	1.03	1.9E+06	0.41	3.91	3E+120	0.01	0.98	0.03	0.23	0.14

with $N = 3$ and the most robust networks are GARR and ABILENE with values of 0.1990 and 0.3333, respectively.

In the case of *percolation limit* (ρ_c), TISCALI_L3 (0.8974) and CESNET (0.8142) have the highest values which indicate these networks are more robust. With respect to *number of spanning trees* (NST), in general, the larger the network, the higher the NST is. Therefore, NST must be compared in networks of similar sizes. By comparing the NST of the whole set of networks, KDL and US_MW result in being the most robust networks. However, by comparing the NST of networks of a similar size, TISCALI_L3 is more robust than RENATER and CESNET because, as shown in Table 2, the first has more links than other. Therefore, the number of spanning trees in the TISCALI_L3 networks is higher. In the static scenario, the *average two-terminal reliability* (ATTR) for all networks is one.

As regards to centrality-based metrics, we consider *nodal degree centrality* (d_c), *nodal closeness centrality* (c_c), *nodal betweenness centrality* (b_c) and *link betweenness centrality* (b_c) to measure the network centralization. As explained above, in Sect. 2.2, the network centralization is used to analyze the network robustness based on these centrality metrics as the differences between the centrality of the most central node and that of all others [21]. This indicates that those networks close to uniform centrality distributions are more robust in the case of targeted attacks to the most central nodes. In Table 3 it can be seen that networks with the highest centralization values when considering d_c are TISCALI_L3 (0.3388) and CESNET (0.325); with e_c, the KDL (0.986) and ATT_L1 (0.9756) networks are the most centrals; based on c_c, CESNET (0.4605) and TISCALI_L3 (0.3837) networks have the highest centralization values; the most central networks based on b_c are CESNET (0.6939) and GARR (0.4591), and lastly USCARRIER (0.27) and CESNET (0.24) have the highest network centralization based on l_c.

This preliminary robustness analysis (summarized in Table 3) shows that some metrics differ when identifying the most robust networks. Hence, taking just one metric is not sufficient to measure the network robustness. Therefore, a set of significant metrics to calculate the robustness and compare their results should be considered. In order to identify the relationships between network properties and their robustness it is necessary to consider the behavior of this set of real telecommunication networks when multiple failures occur under targeted attacks and random failures.

5.2 Robustness Analysis Under Simultaneous Targeted Attacks

In this section, robustness analysis of the real telecommunication networks when nodes are removed under the simultaneous targeted attack is presented. According to [4], the *nodal degree centrality* (d_c), which is a purely local centrality measure, is the most effective technique for removing nodes in the case of simultaneous targeted attacks. In Fig. 2a the robustness results using the *average two-terminal reliability* (ATTR) metric are shown. When the network is fully connected, exactly one component exists and ATTR is one. Successive removal of nodes or links will bring it closer to zero [18]. If failures affect two topologies in the same percentage of nodes or links, the one that takes longer to reach a given critical ATTR can be considered the more robust [18]. ATTR provides an approximation to measure the network connections and to group networks with similar robustness. Then, for each subset of networks the common topological properties among them can be identified.

As can be observed in Fig. 2a, it is possible to identify different affectation levels i.e. the number of lost connections when a percentage of nodes are eliminated from the networks. The weak level is between 1 and 5 % of failures, where network connections can decrease dramatically to 60 %. When the percentage of nodes removed (P) is in the range of 5–20 %, networks have an intermediate affectation with a reduction of 70 % of connections. At 20 % or more of P, networks reduce their connection to <10 %, so networks are near to being completely disconnected with a severe affectation. Therefore, making robustness comparisons for $P > 20$ % is not relevant as these networks are close to being completely disconnected and robustness metrics do not reflect real behavior.

For each P, the number of nodes removed from the ABILENE network does not vary substantially due to its small number of nodes and links. Consequently, ABILENE was not considered in the present analysis. The robustness analysis using the ATTR metric (see Fig. 2a) shows that CORONET_L1 is the most robust network as its network connections are maintained at over 80 % when P is not more than 10 %. CORONET_L1 has high value of *average nodal degree* (k) (2.72), and low values of *maximum nodal degree* (k_{max}) (5) and *average shortest path length* ($\langle l \rangle$) (6.6741) which would explain this result. This network is also an assortative network with $r = 0.0357$. Nonetheless, the KDL network has the least robustness. For instance, in the range of 3 to 5 % of P, the connections of KDL are reduced to <15 %. This is because KDL has the lowest value of $\langle k \rangle$ (2.3846) and the highest value of $\langle l \rangle$ (22.727), and is also a disassortative network ($r = -0.096$).

In Fig. 2a it can be seen that the GEANT, RENATER and TISCALI_L3 networks have similar ATTR behavior and these networks remain in the top five of most robust networks. At 5 % of P their networks connections are reduced to 80 %. This first set of networks have high values of $\langle k \rangle$, and low values of $\langle l \rangle$ and *diameter* (D). In contrast, the COGENTCO, SPRINT_L1 and USCARRIER networks lose more than 50 % of their connections after 5 % of P. This second set of networks is characterized by low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D.

In Fig. 2b, the robustness results for *natural connectivity* ($\overline{\lambda}$) are presented. As can be seen, with <20 % of P it is possible to identify which networks are more robust than others and they can be grouped. Thus, the most robust networks are TISCALI_L3, DELTACOM and GARR, and the least robust are USCARRIER, SPRINT_L1 and KDL. Analogous robustness results for $\overline{\lambda}$ were obtained with the *largest eigenvalue* (λ_1) metric. Hence, structural metrics selected in this analysis agree in grouping the more and less robust networks. These sets of networks have similar topological properties, as can be seen in Table 2.

With respect to centrality-based metrics and comparing the structural robustness results, the networks with high centralization values are the most robust i.e. networks have more nodes with similar centrality values that can help to maintain network connections when the percentage of nodes removed increases according to targeted attacks. However, in simultaneous targeted attacks, the network centralization based on *degree centrality* (d_c) is the most appropriate metric to measure the network robustness owing to nodes being removed by their degree centrality values. Similar to structural metrics, centrality-based metrics allow network robustness to be compared to no more than 20 % of failures.

Figure 3 shows the robustness results of network centralization based on *degree centrality* (d_c). As can be seen, it is possible to identify three subsets of networks: the first has two networks with the highest robustness (TISCALI_L3 and CESNET), the second has four networks with an intermediate robustness (GEANT, RENATER, GARR and GPENI_L2) and the third has the least robust networks e.g. SPRINT_L1, ATT_L1, US_MW and KDL. The topological properties of these subsets of networks are similar i.e. the most robust networks have high values of $\langle k \rangle$, and low values of $\langle l \rangle$ and D, whereas the least robust networks have low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D (see Table 2).

5.3 Robustness Analysis Under Sequential Targeted Attacks

This section presents the robustness analysis of the real telecommunication networks when nodes are removed under the sequential targeted attack. In this scenario the most effective technique for removing nodes is *nodal betweenness centrality* (b_c) [4]. As can be observed in Fig. 4a, the *average two-terminal reliability* (ATTR) results show that all networks are more robust under sequential targeted attacks than when compared to simultaneous targeted attacks. A similar robustness behavior for both attacks can be found in [4]. Figure 4a also shows that when the percentage of removed nodes (P) is between 1 and 5, 50 % of the network connections are lost. At 15 % of P, most of the networks reduce their connections to <20 % and, at 20 % or more networks are near to being completely disconnected.

By comparing this robustness result to robustness results in simultaneous targeted attacks, in sequential targeted attacks the TISCALI_L1 network moves up from

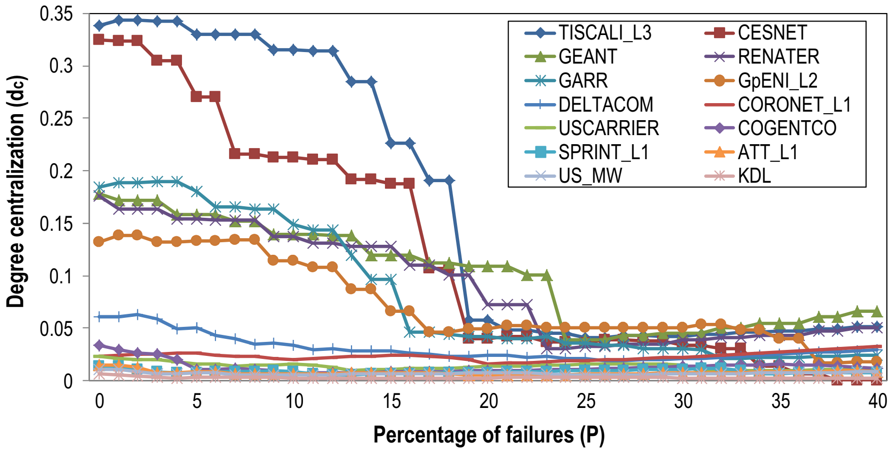


Fig. 3 Network centralization results for simultaneous targeted attack

fourth to first place in the rankings of most robust networks, whereas CORONET_L1 descends to eighth place. TISCALI_L1 has a high *average nodal degree* ($\langle k \rangle$) value (5.0588) and a low *average shortest path length* ($\langle l \rangle$) value (2.4298) which can explain this result. In contrast to the CORONET_L1 network, TISCALI_L3 is one the most disassortative network ($r = -0.3614$). This means that disassortative networks are less vulnerable to sequential targeted attacks by nodal betweenness centrality and assortative networks show more robustness under simultaneous targeted attacks by nodal degree centrality. This result for *assortativity coefficient* (r) analysis is the same as was found in [4]. In both targeted attacks, KDL is the least robust network.

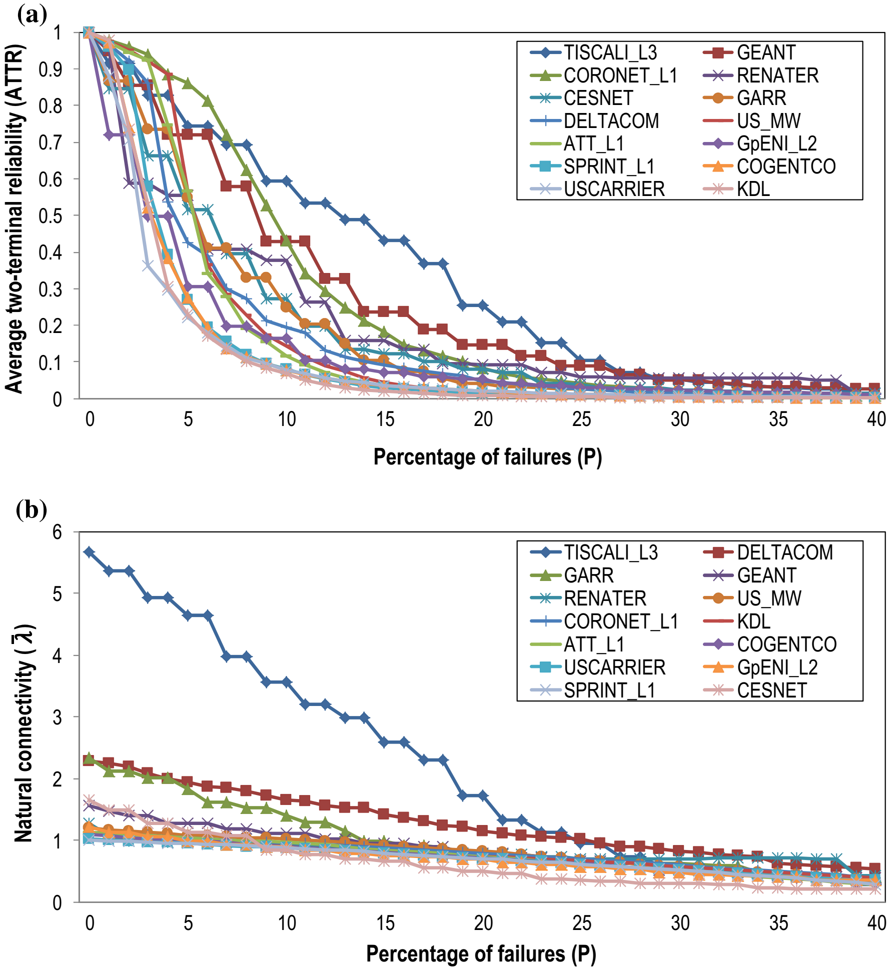


Fig. 4 Structural results for sequential targeted attack. **a** Average two-terminal reliability (ATTR) results and **b** natural connectivity ($\bar{\lambda}$) results

In Fig. 4b the robustness results for *natural connectivity* ($\bar{\lambda}$) metric are presented. The $\bar{\lambda}$ metric allows networks to be identified that are the most robust to <25 % of P. In this sense, TISCALI_L3 presents the best robustness and USCARRIER the poorest. The *largest eigenvalue* (λ_1) metric exhibit similar robustness behavior to $\bar{\lambda}$. In both cases, the robustness degradation is lower than the results found in the simultaneous targeted attacks.

For centrality-based metrics, the most robust networks are also those which have high centralization values. In contrast with simultaneous targeted attack results, for sequential targeted attacks these metrics allow network robustness to be compared to no more than 35 % of failures. In this failure scenario, network centralization based on *nodal closeness centrality* (c_c) and *nodal betweenness centrality* (b_c) are the most effective metrics to measure the network robustness in sequential targeted attacks due to the nodes being removed by their betweenness centrality values. As shown in Fig. 5, in the range of 1–10 % of P, the shortest paths are quickly lost, then, the length of the shortest path between nodes quickly increases. Therefore, networks have fewer nodes with high values of betweenness or closeness centrality which generate the increases of network centralization values.

Figure 5 shows the robustness results according to the network centralization based on b_c. As can be observed, in the range of 1–10 % of failures, it is not easy to identify which networks are most robust due to the high variability produced by the increase of $\langle l \rangle$. Nonetheless, when P is between 10 and 30 %, it can be seen that TISCALI_L3 is most robust network, followed by the group encompassing the CESNET, RENATER, GEANT and GARR networks and lastly by a set of least robust networks e.g. SPRINT_L1, USCARRIER and KDL. Similarly to robustness results presented in sequential targeted attacks, the most robust networks have high values of $\langle k \rangle$, and low values of $\langle l \rangle$ and D, whereas the least robust networks have low values of $\langle k \rangle$ and high values of $\langle l \rangle$ and D.

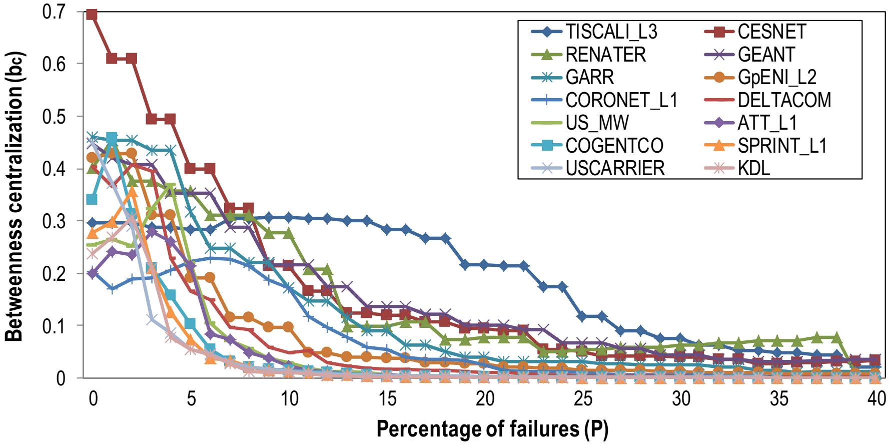


Fig. 5 Network centralization results for sequential targeted attack

5.4 Robustness Analysis Under Random Failures Results

In this section, the real telecommunication networks' robustness, when nodes are removed under random failures, is presented. In Fig. 6, the robustness results according to *average two-terminal reliability* (ATTR) for random node failures are presented. As can be seen, all networks are more robust under random failures as compared to both types of targeted attacks. This is because in random attacks it is less likely that most central nodes are removed in first percentages of failures.

Figure 6 shows that network connections are over 50 % from 1 to 10 % of failures, whereas all of them reduce their connections to <50 % in the range of 10–25 % of P. At 68 % or more failures, all networks have <5 % of connections. In this case, TISCALI_L3 is the most robust network and KDL is the least robust. The set of networks with high robustness to random node failures has low values of *average shortest path length* ($\langle l \rangle$) and *diameter* (D), and they are the most disassortative networks ($r < 0$). Furthermore, it can be observed that networks with high *average nodal degree* ($\langle k \rangle$) show robustness to random attacks, which is in accordance with the results found in [30].

6 Conclusions and Future Work

In this paper a robustness analysis of 15 real telecommunication networks under multiple failure scenarios (random and targeted attacks) was carried out. Through this analysis the common topological proprieties that can be used to group networks with similar robustness behavior are identified. Furthermore, a taxonomy of robustness metrics in telecommunication networks has been extended from previous work and a classification of multiple failure scenarios has been made.

In accordance with the results presented here, some conclusions can be drawn. First, robustness analysis based on structural metrics shows that the subset of real

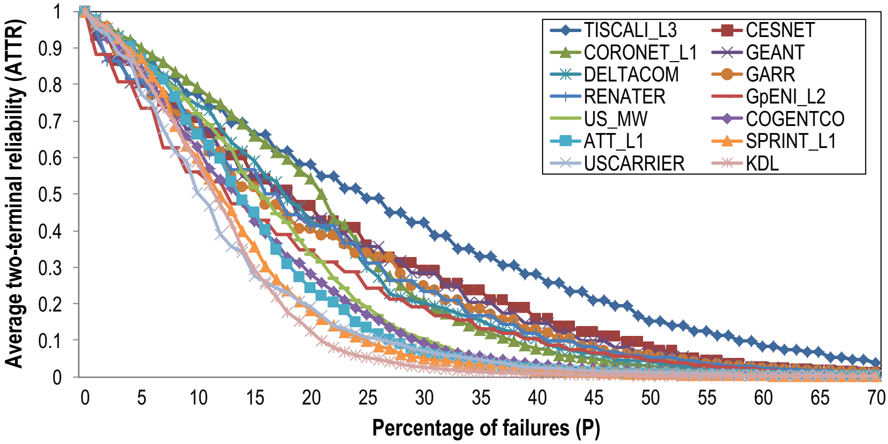


Fig. 6 Structural results for random failures

telecommunication networks most robust under targeted attacks have high values of *average nodal degree* ($\langle k\rangle$), low values of *average shortest path length* ($\langle l\rangle$) and *diameter* (D), whereas the subset of networks least robust have the opposite results for $\langle k\rangle$, $\langle l\rangle$ and D. Similar to previous studies, for disassortative networks ($r < 0$) simultaneous targeted attacks by *nodal degree centrality* is the most effective method of degrading a network. However, in sequential targeted attacks by *nodal betweenness centrality*, assortative networks ($r > 0$) are more vulnerable. These results are a consequence of disassortative networks having an excess of links connecting nodes of dissimilar degrees, which in simultaneous targeted attacks are removed rapidly according to their degree centrality value.

The second round of conclusions is focused on the robustness comparison using the centrality-based metrics. The subset of real telecommunication networks with high values for the network centralization metrics based on *nodal degree centrality* (d_c), *nodal closeness centrality* (c_c) and *nodal betweenness centrality* (b_c) shows robustness under targeted attacks as more central nodes must be removed to affect network performance. Networks with low results in centralization metrics are less robust. Moreover, robustness analysis according to centrality-based metrics can be carried out by selecting the appropriate metric to identify the impact of nodal failures. Hence, in simultaneous targeted attacks by nodal degree centrality, the centralization metric based on d_c should be used to measure the robustness. However, in case of sequential targeted attacks by nodal betweenness centrality, network robustness should be measured by the centralization metric based on b_c.

As to the results of nodal random failures, the subset of more robust real telecommunication networks have low values of *average shortest path length* ($\langle l\rangle$) and *diameter* (D), and these are the most disassortative networks ($r < 0$). Also, similar to previous studies, topologies with high *average nodal degree* ($\langle k\rangle$) show robustness to random failures as there are more nodes available to maintain connections. Additionally, in random failures the probability of affecting central nodes at first values of percentage of removed nodes (P) is low compared to targeted attacks. Therefore, a lot of nodes would have to be removed to degrade the network structure to the same affectation levels reached by targeted attacks.

As future work, a more in-depth study focused on the relationship between robustness metrics under multiple failure scenarios could be made. This would allow those properties of the networks which must be strengthened to maintain desirable network robustness to be identified.

Acknowledgments This work is partiality supported by the Spanish Ministerio de Economía y Competitividad and the DURSI consolidated research group (CSI Ref. SGR-1469) through the RoGER project (TEC 2012-32336) being developed in the Broadband Communications and Distributed Systems (BCDS) research group at the Universitat de Girona (Spain).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Maniadakis, D., Balmpakakis, A., Varoutas, D.: On the temporal evolution of backbone topological robustness. In: Proceedings of the 18th European Conference on Networks and Optical Communications (NOC 2013), Graz (2013)
2. Manzano, M., Marzo, J.L., Calle, E., Manolova, A.: Robustness analysis of real network topologies under multiple failure scenarios. In: Proceedings of the 17th European Conference on Networks and Optical Communications (NOC 2012), Vilanova i la Geltru (2012)
3. Van der Meer, E.: Comparing Measures of Network Robustness. Research Paper Business Analytics. VU University Amsterdam, Amsterdam (2012)
4. Iyer, S., Killingback, T., Sundaram, B., Wang, Z.: Attack robustness and centrality of complex networks. PLoS ONE **8**(4), 1–17 (2013)
5. Trajanovski, S., Martín-Hernández, J., Winterbach, W., Van Mieghem, P.: Robustness envelopes of networks. J. Complex Netw. **1**(1), 44–62 (2013)
6. Sydney, A., Scoglio, C., Youssef, M., Schumm, P.: Characterising the robustness of complex networks. Int. J. Internet Technol. Secur. Trans. **2**(3/4), 291–320 (2010)
7. Bilal, K., Manzano, M., Khan, S.U., Calle, E., Li, K., Zomaya, A.Y.: On the characterization of the structural robustness of data center networks. IEEE Trans. Cloud Comput. **1**(1), 64–77 (2013)
8. Manzano, M., Bilal, K., Calle, E., Khan, S.U.: On the connectivity of data center networks. IEEE Commun. Lett. **17**(11), 2172–2175 (2013)
9. Couto, R.S., Secci, S., Campista, M.E.M., Costa, L.H.M.K.: Reliability and survivability analysis of data center network topologies. J. Netw. Syst. Manag. **24**(2), 346–392 (2015)
10. Lewis, R.G.: Network Science: Theory and Practice. Wiley, Hoboken (2009)
11. Mahadevan, P., Krioukov, D., Fomenkov, M., Huffaker, B., Dimitropoulos, X., Vahdat, A.: The internet AS-level topology: three data sources and one definitive metric. SIGCOMM Comput. Commun. Rev. **36**(1), 17–26 (2006)
12. Wang, Y., Wang, C., Faloutsos, C., Chakrabarti, D.: Epidemic spreading in real networks: an eigenvalue viewpoint. In: Proceedings of the 22nd International Symposium on Reliable Distributed Systems (SRDS'03), Florence (2003)
13. Jamakovic, A., Uhlig, S.: Influence of the network structure on robustness. In: Proceedings of the 2007 15th IEEE International Conference on Networks (ICON 2007), Adelaide (2007)
14. Zhang, X.-K., Wu, J., Tan, Y.-J., Deng, H.-Z., Li, Y.: Structural robustness of weighted complex networks based on natural connectivity. Chin. Phys. Lett. **30**(10), 108901–108904 (2013)
15. Ellens, W., Spieksma, F.M., Van Mieghem, P., Jamakovic, A., Kooij, R.E.: Effective graph resistance. Linear Algebra Appl. **10**(435), 2491–2506 (2011)
16. Rohrer, J.P., Sterbenz, J.P.G.: Predicting topology survivability using path diversity. In: Proceedings of the 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT 2011), Budapest, Hungary (2011)
17. Long, X., Tipper, D., Gomes, T.: Measuring the survivability of networks to geographic correlated failures. Opt. Switch. Netw. **14**(2), 117–133 (2014)
18. Neumayer, S., Modiano, E.: Network reliability with geographically correlated failures. In: Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA (2010)
19. Neumayer, S., Zussman, G., Cohen, R., Modiano, E.: Assessing the vulnerability of the fiber infrastructure to disasters. In: Proceedings of the 2009 IEEE INFOCOM, Rio de Janeiro (2009)
20. Youssef, M., Kooij, R., Scoglio, C.: Viral conductance: quantifying the robustness of networks with respect to spread of epidemics. J. Comput. Sci. **2**(3), 286–298 (2011)
21. Freeman, L.C.: Centrality in social networks conceptual clarification. Soc. Netw. **1**(1978/1979), 215–239 (1979)
22. Tang, L., Liu, H.: Community Detection and Mining in Social Media. Morgan and Claypool, San Rafael (2010)
23. Kitsak Maksim, M., Gallos, L., Havlin, S., Liljeros, F., Muchnik, L., Stanley, H.E., Makse, H.A.: Identification of influential spreaders in complex networks. Nat. Phys. **6**(11), 888–893 (2010)
24. Manzano, M., Calle, E., Harle, D.: Quantitative and qualitative network robustness analysis under different multiple failure scenarios. In: Proceedings of the 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT 2011), Budapest, Hungary (2011)

25. Van Mieghem, P., Doerr, C., Wang, H., Martin-Hernandez, J., Hutchison, D., Karaliopoulos, M., Kooij, R.E.: A Framework for Computing Topological Network Robustness. Technical Report 20101218, Networks Architectures and Services. Delft University of Technology (2010)
26. Manzano, M., Calle, E., Torres-Padrosa, V., Segovia, J., Harle, D.: Endurance: a new robustness measure for complex networks under multiple failure scenarios. Comput. Netw. **57**(17), 3641–3653 (2013)
27. Manzano, M., Sahneh, F., Scoglio, C., Calle, E., Marzo, J.L.: Robustness surfaces of complex networks. Sci. Rep. **4**, 1–4 (2014)
28. Topology Zoo. www.topology-zoo.org (2015). Accessed 3 Mar 2015
29. ResiliNets Topology Map Viewer. www.ittc.ku.edu/resilinets/maps (2015). Accessed 3 Mar 2015
30. Sydney, A., Scoglio, C., Schumm, P., Kooij, R.E.: Elasticity: topological characterization of robustness in complex networks. In: Proceedings of the 3rd international conference on bio-inspired models of network, information, and computing systems (BIONETICS 2008), Awaji City, Japan (2008)

Diego F. Rueda received the master degree in Telecommunications Engineering in 2013 at Universidad Nacional de Colombia. He is currently a Ph.D. student within the Broadband Communications and Distributed Systems (BCDS) research group at the Universitat de Girona, Spain. His research interests include network management, quality of service (QoS), multimedia services, and large-scale failures in complex and interdependent networks.

Eusebi Calle is an Associate Professor at the Universitat de Girona (UdG), where he received his doctorate degree in computer science in 2004. Since 1998 he has been a member of the Broadband Communications and Distributed System Group at the UdG. He has co-authored more than 100 papers in international journals and international conferences. He develops his research in fault management, optical networks, QoS routing, and network science.

Jose L. Marzo is a full Professor at the Computer Architecture and Technology Department at the Universitat de Girona (UdG). He is also adjunct Professor at the Department of Electrical and Computer Engineering, Kansas State University, USA. He leads the Broadband Communications and Distributed Systems. His research interests are in the fields of communication networks, complex networks control and management, adaptive hypermedia systems.