Robustness Quantification of Hierarchical Complex Networks under Targeted Failures

Kashif Bilal[a,b] , Marc Manzano[c], Aiman Erbad[a], Eusebi Calle[c], and Samee U. Khan[d]

[a] Qatar University, Qatar

[b] COMSATS University Islamabad, Abbottabad, Pakistan

[c] University of Girona, Spain

[d] North Dakota State University, Fargo ND, USA

Abstract

Robustness is one of the key properties in complex networks to ensure the expected level of performance and service availability in case of perturbations and failures. Network robustness is generally quantified using various classical metrics. However, whether the robustness quantification of the networks in various types of failures can be proved to be valid or not? Moreover, how does the hierarchy of a network impacts the robustness, is still not a well-explored domain. This paper presents the robustness quantification of hierarchical complex networks under targeted attacks. We analyze ten different real-world networks with varying graph characteristics using the classical robustness metrics. The level of the hierarchy of the considered networks is computed using the Global Reaching Centrality (GRC) measure. To depict the targeted attacks, we remove (decommission) specific network nodes based on the nodal degree and node betweenness centrality. Moreover, to compare various networks with varying size and characteristics, we employ deterioration strategy to evaluate the effect of the failures on hierarchical networks. Our results reveal a strong relationship between hierarchy and robustness of the networks. Moreover, the presented results reveal that the robustness inferences based on the classical robustness measures may be inaccurate. It can be inferred from the analysis that the classical robustness metrics may not be able to quantify the structural robustness of hierarchical complex networks appropriately, which lay down a need for new robustness metrics for robustness quantification.

Keywords: Network robustness, hierarchical complex network, data center networks, targeted attacks.

1. Introduction

The society today is more dependent than ever on complex networks, such as the transportation and power networks, Internet, and Data Center Networks (DCNs) (s). Natural structures, such as biochemical networks modules (metabolic, protein interaction, and genetic regulatory networks), brain network, food webs, or social networks also exhibit the complex network characteristics [1-6]. A complex network is generally denoted by the structural complexity, network evolution characteristics, network hierarchy, connection diversity, dynamical complexity, and node diversity. One of the key characteristics of complex networks is network hierarchy. Most of the complex networks are inherently hierarchical in the organization [7, 8]. Hierarchy involves several descriptors, such as *order*, *levels*, *inclusion*, or *control*, leading to various types of hierarchies [8-10]. Mones *et al.* discussed three types of network hierarchies within the complex systems, namely: flow, nested, and order hierarchy [8]. Murtra *et al.* classified hierarchy in three types, i.e., treeness, feedforwardness, and orderability [9]. Zhang *et al.* compared different techniques for quantification of multi-level hierarchies, presenting the features, and drawbacks of various approaches [10].

Hierarchy is one of the ubiquitous organization principles in various complex networks [2]. Network hierarchies can be exploited in the development of new drugs [3]. Similarly, hierarchies in the synaptic structure of the nervous system helps to understand the working of the brain [11, 12]. Hierarchies are used to map human dynamics. e.g., purchase patterns of customers [13] or the hiring process of universities [14]. Network hierarchy is a crucial component to gauge the controllability of the system [7]. In human engineering complex networks, such as road, railway, power line, and computer networks, studying the impact of hierarchy on robustness plays a critical role to sustain and deliver the

expected services in case of perturbations and failures, which is the main target of this study. A 3-D morphological framework has been proposed to characterize quantitatively the concept of *hierarchy* [9]. However, the framework cannot be applied to undirected networks. Several quantitative hierarchy measures can be found in the literature [7, 8, 15]. The Global Reaching Centrality (GRC) metric is considered as a critical measure because the GRC is applicable to any type of complex networks, such as directed, undirected, weighted, or unweighted [8]. The GRC is based on the *Local Reaching Centrality* (LRC) that denotes the portion of nodes that can be reached via outgoing edges of a node. The GRC measure is computed as the difference between the maximum and average values of the LRCs within the network. The GRC values lie within the interval [0-1]. A directed tree network has the GRC value close to one; whereas, the GRC value of a homogeneous network, such as a lattice is near to zero. Table I summarizes the abbreviations used in this paper.

Robustness is the ability of a network to deliver an anticipated level of performance, while sustaining component failures and system parametric perturbations [16, 17]. For instance, the DCNs need to be robust against failures and system parametric perturbations for the successful and timely delivery of cloud services [18]. Minor performance degradation may result in enormous financial and reputation loss, as reported by Google and Amazon. Therefore, the robustness analysis of the complex networks that represent the foundations of our modern society is extremely crucial. In general, the network robustness is evaluated by using the classical graph metrics [16]. Some of the well-known network robustness metrics are discussed in [16]. Various studies have been conducted for the robustness analysis of complex networks, such as biological, technological, and social networks. Our contribution is to study the impact of network hierarchy on the robustness of networks in case of intentional (or targeted) failures.

1.1. Contributions and Paper Organization

Our study specifically focuses to answer the following questions in the study: **(a)** what is the relationship between the hierarchy of the network and its robustness? **(b)** what is the behavior of popular robustness metrics in the robustness quantification of hierarchical networks? **(c) w**hat is the impact of targeted failures on robustness of hierarchical networks and how does the robustness metrics behave in case of targeted attacks? and **(d)** are current robustness metrics applicable and adequate to quantify the robustness of hierarchical complex networks? To answer these questions, we analyze ten real-world networks for the robustness analysis using GRC measure to find the extent of hierarchy in the complex networks. The networks are then categorized into two classes based on the GRC values: **(a)** highly hierarchical (high GRC valued networks) and **(b)** low hierarchical (low GRC valued networks). To observe the behavior of classical metrics in robustness quantification of hierarchical networks, we employ various classical robustness metrics to measure the network robustness and find the relationship between GRC value (i.e., the extent of the hierarchy) and robustness. To evaluate the accuracy of the robustness measure, we employ node failures within a network to fail (remove) nodes based on the highest nodal degree and betweenness centrality of the nodes representing the worst-case scenarios. The failures are performed from 1% to 5% of the nodes within each network. To quantify the robustness of the networks after failures, we use the *deterioration* procedure to find the percentage change in the value of the metrics for the network [18]. Our analysis reveals a strong relationship between the hierarchy and the robustness of a network calculated by the classical metrics. However, the targeted failures show that the highly hierarchical networks are more vulnerable to the targeted attacks than the low hierarchical networks, illustrating the inadequacy of classical metrics. The results show that the robustness quantification using classical metrics may be inaccurate and therefore, there is a need for new robustness metrics specifically designed for hierarchical networks under various types of attacks.

Our major contributions can be summarized as:

- evaluate the hierarchy of various real-world complex networks using the GRC measure,
- evaluate the relationship between network hierarchy and robustness,

Table I: Abbreviation used in the paper

Abbreviation	Description	Notion	Description
GRC	Global Reaching Centrality	LRC	Local Reaching Centrality
AS	Autonomous System	$\mu \mid \nu \mid -1$	Algebraic connectivity
$\langle l \rangle$, ASP	Average shortest path length	D	Deterioration
DCN	Data Center Networks	GC	Giant Cluster

- evaluate the behavior of classical metrics to quantify robustness on the network (without failure) and when targeted failures are employed,
- evaluate the network robustness after targeted failures using *deterioration* procedure,
- investigate the correlation between the hierarchy and the robustness of a network under targeted failures.

The rest of this paper is organized as follows. A brief discussion related to the considered networks, robustness metrics, and the GRC measure is presented in Section 2. Section 3 details the deterioration metric and robustness analysis of the networks without failure. The network analysis under the targeted failures and the correlation between the network hierarchy and robustness is presented in Section 4. Finally, Section 5 concludes the paper.

2. Related Work

It has been shown in the recent studies that the operation, formation, and evolution of complex systems reflect hierarchical appearance [10]. Mones *et al.* characterized hierarchies within the complex systems into flow, nested, and order hierarchy [8]. In a flow hierarchy, the nodes are organized and connected as a layered graph having multiple layers. The nodes in the lower layer are influenced by the nodes in the upper layer. Most of the complex networks within the domain of computer science and engineering, such as DCNs [19] that form the backbone of the cloud computing, exhibit flow hierarchy. Conversely, a nested hierarchy is composed of high level and lower level elements, where high-level elements contain lower level elements [20]. The ordered hierarchy is based on an ordered set, where the ordering is made up of the values of the variables in the set of elements. Clauset *et al.* presented hierarchical networks as a group of multiple nodes with different functionalities, which are divided to subgroups leading to network hierarchy [21]. Clauset *et al.* presented a generic technique to infer hierarchy from the network structure. The study revealed that the hierarchy is the central organization concept in complex networks [21]. Mengistu *et al.* tried to explore the reasons for a hierarchical organization in evolutionary biology [2]. The authors presented the biological network hierarchy as recursively organized modules, such as neural networks. The results of the studies explained that in man-made complex networks, hierarchy generally evolves because of the cost and resource constraints. Murtra *et al.* also classified hierarchy in three types, i.e., treeness, feedforwardness, and orderability [9]. Aerts *et al.* studied the robustness in human brain to examine the extent of damage the brain can withstand and what distortions are expected after injuries [4]. Csermely *et al.* studied the role of hierarchy in pharmacology and drug discovery [3]. The authors detailed the drug effects considering robustness and hierarchy of the cellular network. Peng and Wu studied the robustness from natural connectivity perspective to find the optimal network structure [22]. The authors proposed a tabu search algorithm using assortative rewiring for an optimal network topology. Shahrivar *et al.* studied the robustness of

random interdependent networks and characterized the algebraic connectivity of such networks [23]. Li *et al.* measured the network robustness based on the Hamiltonian function using the critical threshold of resolution parameter [24]. Zhang *et al.* compared different techniques for quantification of multi-level hierarchies, presenting the features and drawbacks of various approaches [10].

The robustness of complex networks has been extensively studied in the past decade. The studies discuss the physical connectivity of a network and the effects of random and targeted failures using the classical graph metrics. Various new metrics to capture the advanced robustness characteristics were also proposed in [17]. The correlations of traditional graph metrics were also considered and various interesting observations were made about the strong correlation between the average shortest path length and clustering coefficient [25]. Recently, several metrics have been proposed to consider the performance of a network under failure scenarios [17, 26]. Zamani *et al.* investigated the stability in hierarchical networks [1]. The study revealed that hierarchy has a considerable impact on stability. Higher level of hierarchy increases the stability, however, may have a negative impact in case of perturbations, where low hierarchical networks perform better. The targeted attacks on hierarchical networks may have paradoxical outcomes. The authors study the impact of targeted attacks on the stability of the hierarchical networks. However, the authors used random graphs with different number of edges instead of real-world networks. Coscia explained the hierarchy as influence of a node in upper level over the nodes in a lower level leads to hierarchy [7]. Coscia presented a model to estimate the hierarchy of a directed network based on arborescence score. The model estimates the hierarchy based on the directed link from an upper-level node to a lower level node to compute the score and significance of hierarchy. However, the aforementioned studies do not focus on the relationship between the robustness of a network under targeted failures. Moreover, the underlying hierarchical structure of the network has not been considered in detail in terms of robustness. Furthermore, the accuracy of the robustness quantification using a different metric is not considered in various studies, which are the main objectives of this study.

3. Methods and Data Set

3.1. Measure of Network Hierarchy

Several measures have been proposed to measure the network hierarchy [7, 9, 15]. Some of the hierarchical metrics require the definition of free parameters that are unknown for many networks. Some of the proposals only quantify the deviation from the pure tree structure to measure the hierarchy of the network , or are only applicable to fully directed graphs [7, 9, 15]. The Global Reaching Centrality (GRC) measure is chosen because it is applicable to any type of complex network, such as undirected and unweighted [8].

Local Reaching Centrality (LRC) is defined by Mones *et al.* as, "The LRC of node i is the proportion of all nodes in the graph that can be reached from node i via outgoing edges." It is equivalent to the closeness centrality for disconnected graphs measure proposed by Opsahl *et al.* in [27]. Classical Closeness centrality is the invers of the average of the sum of the shortest paths between two nodes,

$$Closeness(i) = \frac{1}{\sum_j d_{ij}},$$

where d_{ij} is the length of the shortest path from the node *i* to *j*. To avoid dividing by infinite in the case where nodes not connected to the rest of the graph (disconnected graphs), Opsahl *et al.* propose a change in the formula:

$$Closeness(i) = \sum_j \frac{1}{d_{ij}}$$

If we normalize to the nodes in the network N we obtain the Local Reaching Centrality measure, as

Table II: The GRC values of the Networks.

High GRC valued Networks	**ASN25K**	**ASN26K**	**PowerlawN400**	**ThreeTierN2K**	**FatTreeN2K**
GRC Value	0.24336	0.19728	0.18713	0.17199	0.14343
Low GRC Valued Networks	**USmotorway**	**ATTN383**	**EuroPGN1400**	**SprintN300**	**DCellN2K**
GRC Value	0.05559	0.04579	0.04319	0.0413	0.00715

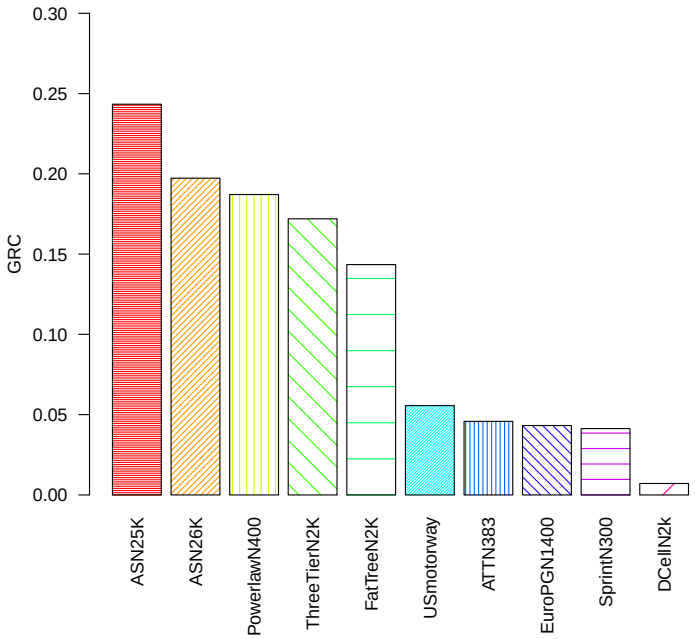

Fig. 2: The GRC values of the networks.

$$C_R(i) = \frac{1}{N-1} \sum_{j:0<d(i,j)<\infty} \frac{1}{d_{ij}},$$

This measure can easily be extended to weighted networks by introducing Dijkstra's algorithm as proposed in the average shortest distance in weighted networks.

Given a graph G, the GRC can be defined as follows:

$$GRC = \frac{\sum_{i \in V}[C_R^{max} - C_R(i)]}{N-1},$$

where V denotes the set of nodes, N is the number of nodes within G, $C_R(i)$ is the *Local Reaching Centrality* (LRC) of the node i, and C_R^{max} is the highest LRC value among all of the nodes within G. The GRC values lie within the interval [0,1]. A higher GRC value depicts a higher hierarchy of the network.

Fig. 2 illustrates the GRC measures for the set of ten networks considered in this work. As can be observed, there are five networks that have the value of GRC greater than 0.14, while the other five present the GRC values below 0.05. For the ease of the analysis and comparison, we classify the considered networks into two categories. The network with the GRC value greater than 0.14, such as the ASN25K, ASN26K, Powerlaw400, ThreeTierN2K, and FatTreeN2K, fall under the former category

(referred as *high GRC valued* networks in the paper). Alternatively, the network with the GRC value less than 0.05, such as the ATTN383, EuroPGN1400, Sprint200, USmotorway, and DCellN2K, fall under the latter category (referred as *low GRC valued* networks in the paper). The GRC values of the networks are reported in Table II.

Therefore, we aim to analyze the effect of the hierarchy on the robustness of a network in response to targeted attacks. To do so, we define the following case study for a set of ten different complex networks, where the authors:

- consider the GRC measure to quantify the hierarchy of complex networks.
- define two scenarios of node targeted attacks using the nodal degree and node betweenness centrality.
- Failures are instigated from 1% to 5% of the nodes within the networks.
- calculate the GRC value for each of the considered networks, and classify the networks into highly hierarchical and low hierarchical network.
- use six classical graph metrics to evaluate the robustness of each of the networks in each of the failure scenarios.
- study the relationship between the GRC metric and the robustness of networks using the deterioration procedure when incremental and irreversible attacks occur.

The rest of this section is dedicated to present the networks and define the different measures that are used in our subsequent analysis.

3.2. Deterioration

In this section, a procedure for the quantification of the network robustness and comparison between various heterogeneous networks (in terms of size), named *deterioration,* based on the percentage change in the metric values. The deterioration can be calculated as the difference between the initial value (without failure) of the robustness metric M and the average of the metric values at various failure percentages, divided by the initial value. The average metric value is considered to minimize the effect of a critical point and phase transition for various networks [28]. Some of the networks studied exhibit a phase transition after a specific number of failures. For instance, the FatTree network exhibits a phase transition at 1.9% of targeted failures based on the betweenness centrality failures [18]. For targeted failures up to 1.8%, the FatTree holds around 98% of the nodes in the largest connected cluster. However, the total number of nodes within the largest cluster drops to 2% of the original network size, when targeted failures percentage reaches 1.9%. Therefore, we use the average of the metric values for the entire failure range to minimize the impact of phase change at a specific percentage of failure. Moreover, various metrics, such as diameter and shortest path length can only be calculated for a connected component of the graph. Therefore, the resultant values of the aforementioned metrics may be misleading for a specific percentage of failure. For instance, the ThreeTierN2K network totally segregates after 5% of targeted failures, where the size of the largest connected component is two. Therefore, the resultant diameter and path length is equal to one. Similarly, the size of the largest connected component after 5% of targeted failures in the ASN26K network was 35, compared to the initial network size of 26,475. Therefore, the resultant value for the diameter and average path length was 16 and 2.3, respectively. However, for 3% of the failures for the ASN26K network, the values for the largest connected component, diameter, and average path length was 718, 46, and 15.55, respectively. Consequently, considering only the final values after 5% of failure will be misleading. Therefore, we take the average for all of the percentages of failures for calculating the percentage change within the metric value. The deterioration can be presented as:

$$\sigma_M = \left| \frac{\mathbf{1}}{M_{\mathbf{0}}} \left(\frac{\sum_{i=1}^{n} M_i}{n} - M_0 \right) \right|,$$

where M_0 is the initial value of a metric M without failures, and M_i is the value of the metric when i percent of the nodes fail ($1 \leq i \leq n$). The lower the value of deterioration, the higher is the robustness

of the network, indicating that the network has undergone the minimum number of changes. On the contrary, the larger the change in values of the various metrics of a network, the higher the deterioration is, depicting less robustness of the network. To demonstrate the validity of the proposed procedure, we calculate σ_M for the: diameter, algebraic connectivity, spectral radius, nodal degree, largest connected cluster size, and average shortest path length. Fig. 3 – Fig. 8 present the deterioration results for the considered metrics with respect to the nodal degree and betweenness centrality based targeted failures. For both of the failures scenarios (nodal degree and betweenness centrality), it can be observed that the low GRC valued networks exhibit lower deterioration in most of the cases depicting the higher robustness to targeted failures.

3.3. Networks

In this study, we consider ten networks. The details of the networks are discussed below.

- EuroPGN1400: an approximated model of the European power grid network.
- ASN25K: an Autonomous System (AS) network of the year 2012.
- ASN26K: the largest AS connected graph from the network set available in November 2007 in the Cooperative Association for Internet Data Analysis (CAIDA) repository.
- USmotorway: the US interstate highway topology.
- ATTN383: a physical fiber network of AT&T.
- SprintN300: a physical fiber network of Sprint.
- ThreeTierN2K: commonly used network topology within data centers.
- FatTreeN2K: Clos based network topology proposed for data centers.
- DCellN2K: hierarchical server-centric topology proposed for data centers.
- PowerlawN400: a power-law network that has been generated using the Barabási Albert (BA, preferential attachment mechanism) model.

Table III depicts the main features of the networks. As observed, our set of networks is heterogeneous with respect to size, number of edges, average nodal degree, and maximum nodal degree.

3.4. Classical Robustness Metrics

Here, we define the six classical robustness measures that we use in our analysis:

- **Diameter:** is the longest path among all of the shortest paths of the network. Generally, low diameter represents a higher robustness of a network [29].
- **Cluster size (largest/giant cluster size):** depicts the size of the largest connected component of the network. The giant cluster size is typically used to analyze the fragmentation of a network under incremental and irreversible failures. The lower the value of the giant cluster size for a specific failure, the more vulnerable is the network.
- **Average shortest path length (⟨l⟩):** is the average of all of the shortest paths among all of the node-pairs of the network [30]. Small ⟨l⟩ values exhibit better robustness because such networks are likely to lose fewer connections in response to different types of failures (random or targeted).
- **Average nodal degree:** is one of the coarse robustness measures [29]. Networks having high average nodal degree value are considered more robust and "better-connected" on average.

- **Algebraic connectivity ($\mu|\nu|-1$):** depicts how difficult it is to break the network into islands or individual components. Such a metric is obtained from the second smallest eigenvalue of the Laplacian matrix of a network. The higher the value of the algebraic connectivity, the better is the robustness.
- **Spectral radius:** is the largest eigenvalue of the adjacency matrix of a network [29]. Generally, the networks with the higher eigenvalues have a small diameter and higher node distinct paths. Moreover, networks with high spectral radius denote more initial resistance to the epidemic-like spreading of failures. Therefore, the networks with high spectral radius are considered more robust.

4. Results and Robustness Analysis

4.1. Initial Network Analysis

The robustness of the ten complex networks is analyzed considering the classical robustness metrics. Table IV presents the values of the classical metrics for the networks without any failures. Table IV is sorted based on the decreasing GRC values to depict the relation between hierarchy and robustness estimation of the network. As can be observed from the table, the networks with high GRC values (highly hierarchical networks) depict better robustness in most of the cases without failures. The average diameter value for the high and low GRC valued networks was 11 and 36.2, respectively. The average diameter is calculated to highlight the difference of the initial metric values for both of the network groups.

As discussed in Section 2.3, the networks with low average shortest path lengths (denoted as ASP) are considered more robust. It can be observed from the metrics results presented in Table IV that in general, the high GRC valued networks have low average path lengths. On the contrary, low GRC valued networks exhibit high average path length values. The average of the high GRC valued networks is 4.84; whereas, the low GRC valued networks have 13.97 as the average value for the path length metric. The networks with high spectral radius are considered more robust. A similar trend of high GRC valued networks to exhibit better robustness can also be observed when considering the spectral radius metric. The ASN25K and ASN26K with the highest GRC value also exhibit the highest spectral ratio values of 103.36 and 69, respectively. Alternatively, the spectral radius values of the low

Table III: Network characteristics

Network	Number of nodes	Number of edges	Average nodal degree	Maximum nodal degree
ASN25K	25,357	74,999	5.91	3,781
ASN26K	26,475	53,381	4.03	2,628
PowerlawN400	400	399	2	47
ThreeTierN2K	2,562	2,740	2.1389	40
FatTreeN2K	2,500	6,000	4.8	20
USmotorway	411	553	2.69	7
ATTN383	383	488	2.54	8
EuroPGN1400	1,494	2,154	2.88	13
SprintN300	264	313	2.37	6
DCellN2K	2,709	4,515	3.3333	4

GRC valued networks group are comparatively very low. The average spectral radius values for high and low GRC valued network groups are 41.53 and 3.87, respectively.

An analogous trend of robustness estimation based on the algebraic connectivity metric can also be observed in both of the network groups. The high GRC valued networks exhibit high algebraic connectivity values than the low GRC valued networks. The only exception is the DCellN2K network that has a high algebraic connectivity value, almost equal to the ASN25K network. However, the algebraic connectivity value of the DCellN2K is three times less than the FatTreeN2K network. In general, high GRC valued networks exhibit high algebraic connectivity values with an average of 0.0942 than the low GRC valued networks having an average value of 0.0256. The DCellN2K and PowerlawN400 networks are to be considered as the exceptions in both of the network groups while considering the algebraic connectivity values. The networks with high average nodal degrees are considered more robust. The networks having a high GRC value in general, exhibit high average nodal degrees. The average value of the nodal degree for high and low GRC valued groups was 3.77 and 2.76, respectively.

In general, one may infer from the initial metric values that the higher the hierarchy, more robust is the network. However, we will see in Section 4 that the aforementioned assumption does not hold true in case of targeted failures where low GRC valued networks exhibit better robustness than the higher GRC valued networks, leading to the fact that the initial robustness estimation of the hierarchical networks using the classical robustness metrics may be misleading and erroneous.

Table IV: Classical metric values for the considered network topologies.

Network	GRC	Diameter	Nodal Degree	ASP	Cluster Size	Algebraic Connectivity	Spectral Radius
High GRC valued Networks							
ASN25K	0.243	10	5.9154	3.3984	25,357	0.10768	103.361
ASN26K	0.197	17	4.0325	3.8756	26,475	0.02043	69.642
PowerlawN400	0.187	16	1.995	6.0065	400	0.00463	7.01347
ThreeTierN2K	0.171	6	2.1389	5.7247	2,562	0.02307	10.25044
FatTreeN2K	0.143	6	4.8	5.2106	2,500	0.31526	17.4186
Average	0.188	11	3.776	4.8432	11,458.8	0.094214	41.5371
Low GRC valued Networks							
USmotorway	0.055	42	2.6909	13.654	411	0.00547	4.2156
ATTN383	0.045	39	2.5483	14.129	383	0.00554	3.7069
EuroPGN1400	0.043	48	2.8835	18.888	1494	0.00169	5.0272
SprintN300	0.041	37	2.3712	14.704	264	0.00535	2.9317
DCellN2K	0.007	15	3.3333	8.5106	2709	0.11021	3.475
Average	0.038	36.2	2.765	13.977	1052.2	0.0256	3.871

4.2. Robustness Analysis under Targeted Failures

To analyze the effect of the failures and the validity of the robustness metrics, we evaluate the considered networks by instigating targeted failures, and removing the nodes based on the highest nodal degree and the highest node betweenness centrality values. The aforementioned targeted failure criteria are used in various studies. The nodal degree represents the number of outgoing physical connections of a node with its neighbors. The betweenness centrality is used to estimate the prestige of a node, and is measured as the number of the shortest paths between all of the node pairs within the network that pass through that node [16]. Therefore, the two failure criteria consider the structural as well as the operational aspects of the network. The failures are introduced within the network from within a range of 1% – 5% of the total number of the nodes.

The values of the largest connected cluster size and deterioration (D) under the targeted failures for the considered networks are reported in Table V and Table VI, for the nodal degree and betweenness centrality based failures, respectively. The reported values represent the cluster size and deterioration values for the metric results obtained after instigating 1% – 5% of the failures within the network. The values for the shortest path length, diameter, algebraic connectivity, and spectral radius, are calculated from the largest connected cluster of the resulting network after targeted failure. For an ease of

comparison and observation, the initial size of the network without failure (labeled as Initial in the second column), the resultant largest connected cluster size obtained after 5% of the node failures (labeled as 5% F), and the deterioration value (labeled as D) are reported in the Table V and Table VI, respectively. The rows in the tables are sorted based on the decreasing GRC values to highlight the relation between the GRC value and deterioration. It can be observed from the tables that the networks with high GRC values exhibit more deterioration in contrary to the initial observations obtained from the robustness metric values without failure, as reported in Section 4.1. The detailed analysis of various metric results and deterioration is presented below.

4.3. Robustness Analysis considering the Classical Metrics

4.3.1. Cluster Size

The largest connected cluster (giant cluster) is one of the simplest robustness measures. A network with high robustness must retain most of the nodes in the giant cluster depicting a minimum deterioration and segregation. Such a behavior of the network having high giant cluster size after failures is a natural and easy estimation of the network's robustness. We argue that the networks depicting higher hierarchical organization and high GRC values exhibit low robustness in terms of the giant cluster size. It can be observed from the initial and after 5% failure size of the giant cluster (see Table V and Table VI) that the high GRC valued networks get segregated in very small sized clusters where the giant cluster has a very little number of nodes as compared to the initial graph. For instance, the ASN25K, SN26K, PowerlawN400, ThreeTierN2K, and FatTreeN2K, show 82%, 89%, 94%, 97%, and 18% deterioration in the giant cluster size for the nodal degree based targeted failures, respectively. The FatTreeN2K network exhibits better connectivity in case of the nodal degree failures. However, for the betweenness centrality based failures, the FatTreeN2K networks exhibits 39% deterioration. This is due to the fact that all of the nodes in the upper three layers of the FatTreeN2K topology have the same nodal degree [18]. Therefore, the nodal degree based failures have little effect on network connectivity in case of the FatTree2K network.

Conversely, the networks with low hierarchy and GRC values, such as the USmotorway, ATTN383, SprintN300, EuroPGN1400, and DCellN2K depict low deterioration in the giant cluster size, respectively. The deterioration results observed in the considered hierarchical networks depict that the networks with the low GRC values exhibit more tolerance to the targeted failures and show a small variation in the giant cluster size. Therefore, a major portion and most of the nodes within the network stay connected even after 5% of the failed/removed nodes. Conversely, the networks with high GRC values depict very high deterioration values, and the networks get fragmented and isolated in many small networks with a very little number of the nodes in the giant cluster. A similar behavior and resultant values can be observed in Table VI for the betweenness centrality based targeted failures as depicted by the nodal degree based failures. Such a behavior of the high GRC valued networks depicts weak tolerance against targeted attacks. The deterioration in size of the largest connected cluster illustrated in Fig. 3, also affirms that the high GRC valued networks are more prone to targeted failures and exhibit low robustness.

Table V: Deterioration values for 1% – 5% of Nodal Degree based failures.

Network	Cluster Size			Diameter	Nodal Degree	ASP	Algebraic Connectivity	Spectral Radius
	Initial	5%F	D					
ASN25K	25,357	51	0.83	1.933	0.867	1.756	0.941	0.936
ASN26K	26,475	35	0.90	0.716	0.854	1.238	0.658	0.936
PowerlawN400	400	9	0.95	0.573	0.415	0.593	22.189	0.592
ThreeTierN2K	2,562	2	0.97	0.528	0.680	0.527	19.365	0.543
FatTreeN2K	2,500	1,901	0.18	0.194	0.243	0.017	0.315	0.127
USmotorway	411	376	0.07	0.122	0.088	0.266	0.403	0.152
ATTN383	383	328	0.12	0.208	0.102	0.219	0.370	0.037
EuroPGN1400	1,494	1,037	0.18	0.272	0.134	0.164	0.443	0.182
SprintN300	264	237	0.07	0.149	0.061	0.180	0.395	0.050
DCellN2K	2,709	2,572	0.04	0.052	0.036	0.027	0.085	0.017

Table VI: Deterioration values for 1% – 5% of Betweenness Centrality based failures.

Network	Cluster Size			Diameter	Nodal Degree	ASP	Algebraic Connectivity	Spectral Radius
	Initial	5%F	D					
ASN25K	25,357	51	0.80	2.32	0.85	2.17	0.91	0.78
ASN26K	26,475	35	0.88	0.87	0.84	1.61	0.89	0.88
PowerlawN400	400	9	0.94	0.55	0.39	0.58	22.19	0.59
ThreeTierN2K	2,562	2	0.97	0.43	0.62	0.53	19.37	0.55
FatTreeN2K	2,500	120	0.39	0.13	0.23	0.13	0.03	0.26
USmotorway	411	337	0.06	0.08	0.07	0.22	0.51	0.15
ATTN383	383	324	0.10	0.11	0.08	0.12	0.37	0.04
EuroPGN1400	1,494	1,036	0.15	0.29	0.12	0.18	0.51	0.19
SprintN300	264	232	0.08	0.33	0.06	0.31	0.47	0.03
DCellN2K	2,709	2,572	0.03	0.05	0.03	0.02	0.08	0.02

4.3.2. Average Shortest Path Length

The networks with small average shortest path length are considered more robust. However, the deterioration values observed in the case of the nodal degree based targeted attacks for the high GRC valued networks are quite high. Conversely, the networks with low hierarchical values, the deterioration value of the aforementioned networks are comparatively low for the nodal degree based failures. A similar trend can be observed in Table VI for the betweenness centrality based failures. The aforementioned results depict that the average path length based robustness analysis of hierarchical networks may be misleading and inadequate for robustness quantification of hierarchical networks. Fig 4. depicts the results for the average path length deterioration for the nodal degree and betweenness centrality based failures. The deterioration values in Fig. 4 are capped at value 1.0 to show a better comparison.

4.3.3. Diameter

The networks with low diameter are considered more robust. The diameter of a disconnected graph is infinite. Therefore, the diameter of the largest connected cluster is calculated in case of disconnected networks. The high GRC valued networks have low diameter than the networks with low GRC values. However, as can be observed in the Table V and Table VI, and as shown in Fig. 5, the deterioration values of the high GRC valued networks are very high as compared to the networks with low GRC values. Similar to the average shortest path length, it can be inferred that the diameter based robustness estimation of the hierarchical networks may be misleading and wrong as well.

4.3.4. Algebraic Connectivity

A network with high algebraic connectivity values is considered more robust. Most of the high GRC valued networks depict high algebraic connectivity values without failure, leading to the fact that such networks should be more robust. However, the giant cluster size deterioration values for all of the aforementioned networks depict conflicting behavior to the initial robustness estimation based on the algebraic connectivity values. Most of the high algebraic connectivity valued based networks that were expected to be more robust illustrated low resilience to the targeted attacks, and the low algebraic connectivity value-based network described better resilience and high robustness opposite to the initial robustness estimation. The algebraic connectivity based deterioration is illustrated in Fig. 6.

4.3.5. Spectral Radius

Spectral radius is another robustness measure where high spectral radius presents higher robustness of the network. However, in the case of hierarchical networks, spectral radius based robustness estimation of hierarchical networks is misleading as well. Low spectral radius values show better robustness and high giant cluster size, and the network with high spectral radius values depict higher deterioration. The deterioration values for spectral radius are illustrated in Fig. 7.

4.3.6. Average Nodal Degree

The nodal degree depicts the average connectivity of the nodes within a network, so the higher the average nodal degree, the more robust the network is. A similar trend can also be observed for deterioration values for targeted node failures depicted in Table VI. It can be observed from the aforementioned nodal degree and deterioration values after 5% of the node failures that the low valued GRC networks exhibit better robustness to the targeted failures as compared to the highly hierarchical networks. The deterioration trend illustrated in Fig. 8 also affirms the claim.

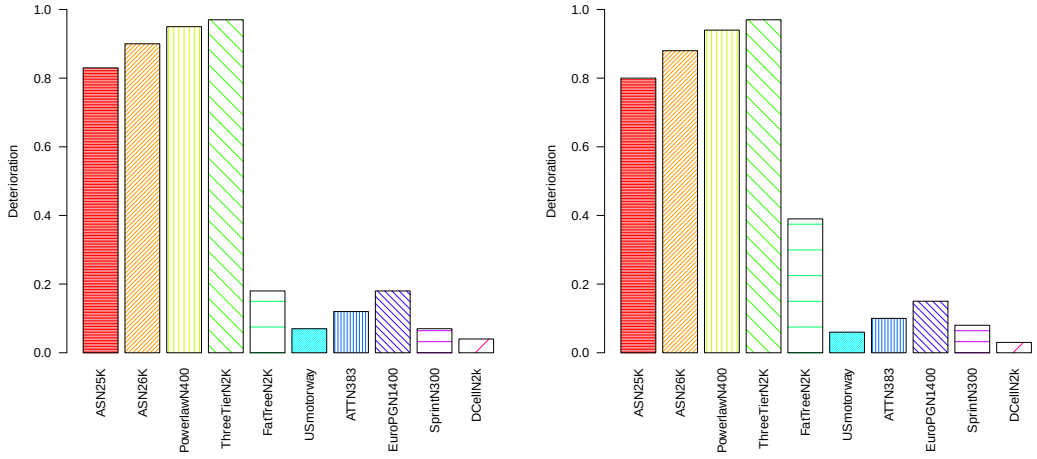

Fig. 3: Deterioration in Largest Connected Cluster size based on: Nodal degree (left) and Betweenness centrality (right).

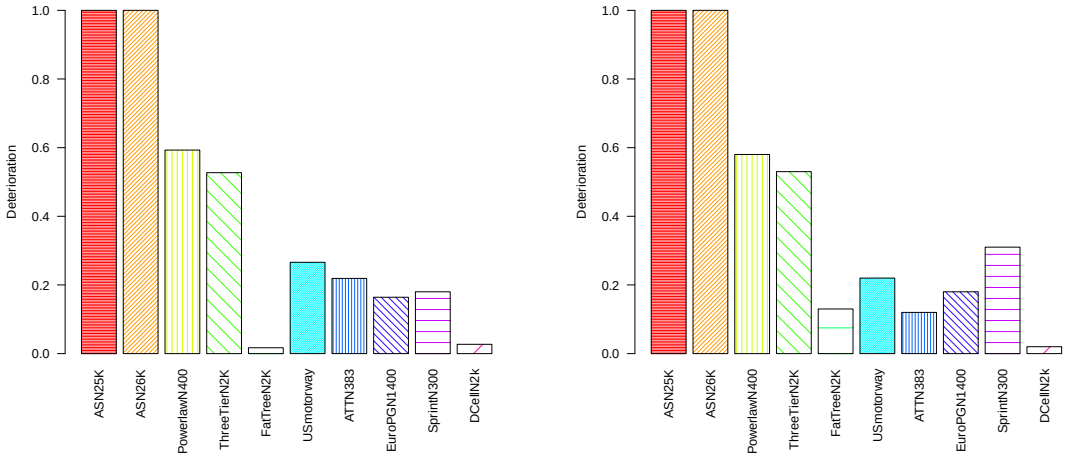

Fig. 4: Deterioration in Average Path Length based on: Nodal degree (left) and Betweenness centrality (right).

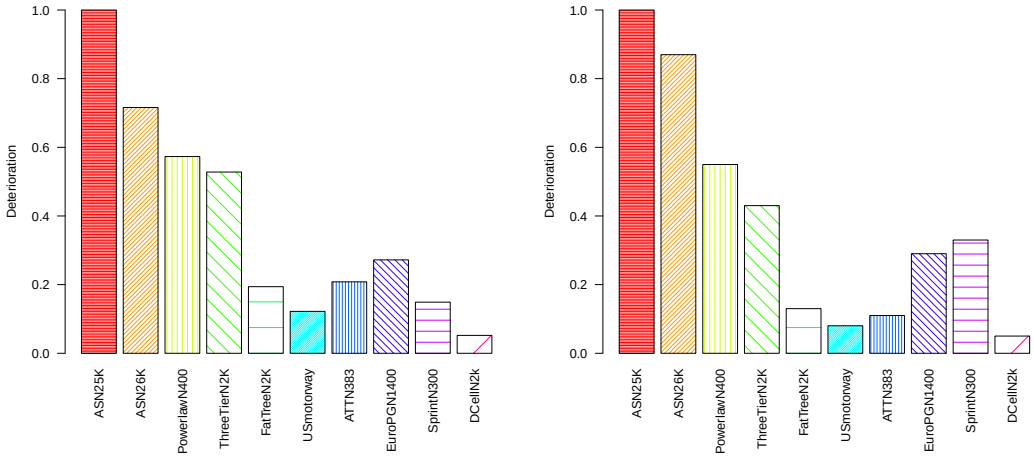

Fig. 5: Deterioration in Diameter based on: Nodal degree (left) and Betweenness centrality (right).

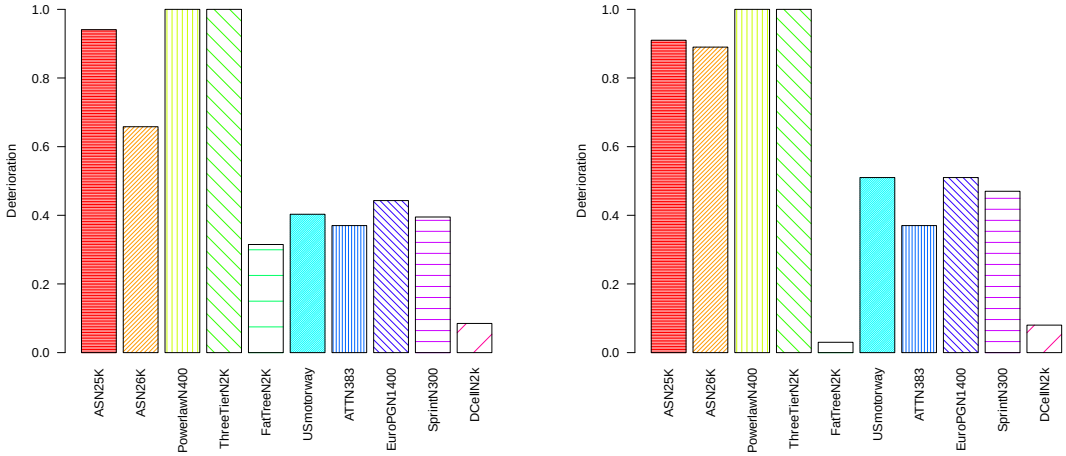

Fig. 6: Deterioration in Algebraic Connectivity based on: Nodal degree (left) and Betweenness centrality (right).

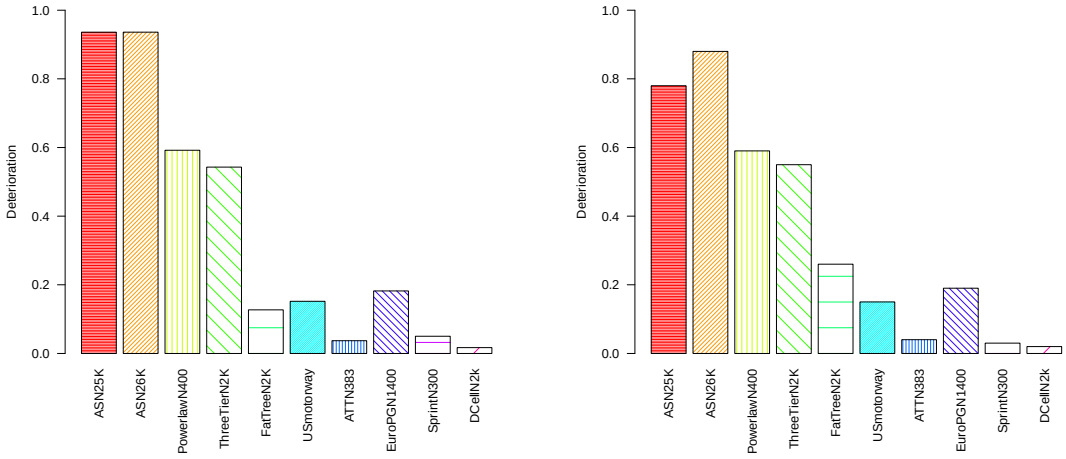

Fig. 7: Deterioration in Spectral Radius based on: Nodal degree (left) and Betweenness centrality (right).

Summarizing, the results depict that the high GRC valued networks undergo more segregation and deterioration. In most of the cases, the initial metric results for the networks with higher hierarchy values show comparatively high robustness as compared to low GRC valued network. However, based on the giant cluster size and deterioration analysis, one can infer that the low GRC valued networks retain connectivity, exhibit large giant cluster size, and report low deterioration values contradicting the initial robustness estimation. Therefore, it can be argued that the initial robustness estimation of the hierarchical networks using most of the classical robustness measures may be misleading and inadequate.

4.4. Correlation between network hierarchy and deterioration

To quantify the relationship between the network hierarchy and the deterioration in case of failures, we use the Pearson correlation coefficient. Fig. 9 illustrates the Pearson correlation coefficient between the GRC values and the deterioration for the nodal degree and betweenness centrality based failures. As can be observed there exists a strong correlation between network hierarchy and deterioration. For most of the metrics, such as the cluster size, diameter, nodal degree, and spectral radius, the correlation value is above 80% depicting a strong correlation. The correlation value for the algebraic connectivity

in case of the betweenness centrality based failures is around 70%. However, in the case of the nodal degree based failures, the value of the correlation for the algebraic connectivity is 82%. Therefore, it can be inferred that the network hierarchy is closely related to deterioration in case of intentional attacks. The more hierarchical a network, the less robustness it exhibits in case of targeted attacks.

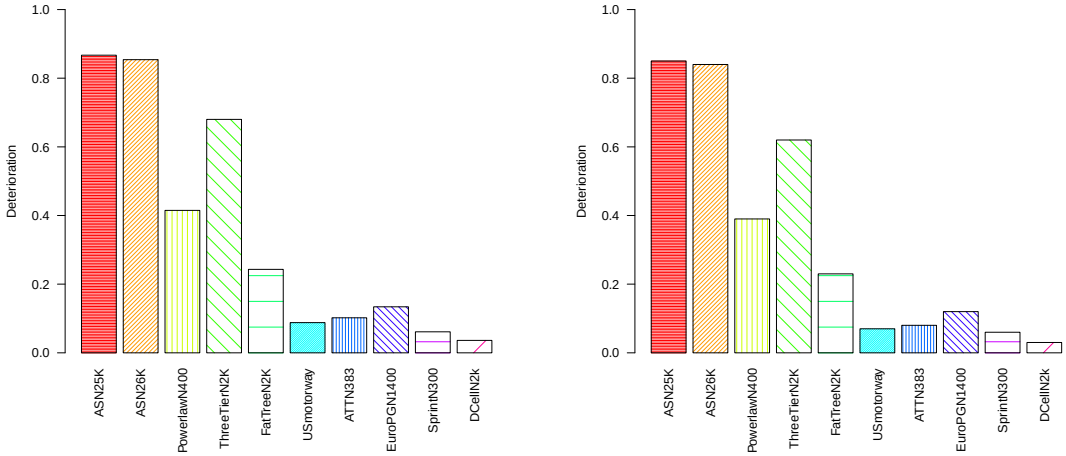

Fig. 8: Deterioration in Average Nodal Degree based on: Nodal degree (left) and Betweenness centrality (right).

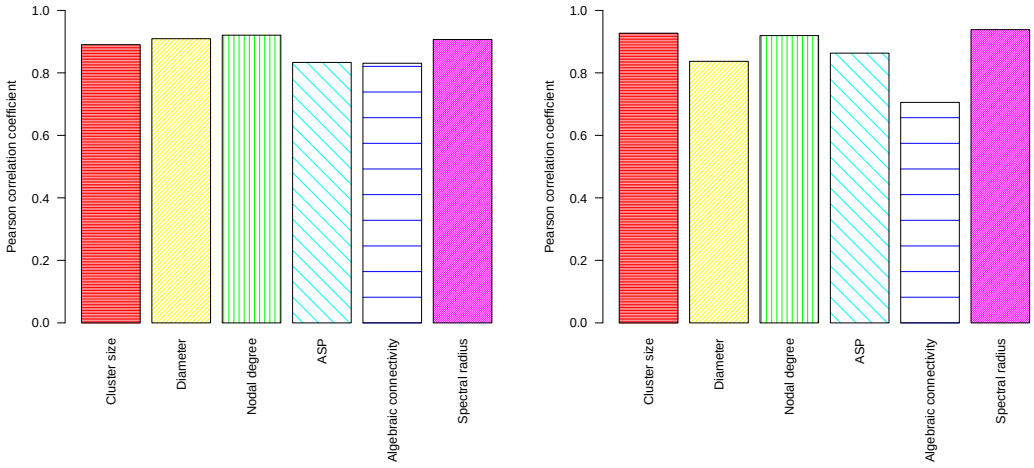

Fig. 9: Correlation between the network hierarchy and deterioration observed in classical metrics, for the nodal degree (left) and betweenness centrality-based (right) attacks.

5. Conclusions

This work presented a study of the relationship between the network hierarchy and robustness. Our study revealed a strong correlation between the network hierarchy and robustness. We first calculated the robustness using classical metrics on the whole network. The results illustrated that the classical metrics show a directly proportional relationship between the network hierarchy (GRC value) and robustness. Initial results estimate that the higher the GRC value, more failures and perturbations it should be able to sustain. However, a targeted failure analysis falsifies the estimate where highly hierarchical networks are seen as more vulnerable to targeted attacks. So, it can be observed that the classical metrics' robustness estimation may not be fully applicable to hierarchical complex networks. *Classical metrics are useful to estimate robustness in the various types of networks under different attacks, however, in the case of hierarchical complex networks, classical metrics are observed to behave inefficiently.*

Therefore, our study instigates a need for the development of new robustness metrics, specifically designed considering the hierarchical nature of complex networks and various possible attacks, to more precisely quantify the hierarchical complex networks robustness. In future, we will propose a robustness metrics designed for hierarchical complex networks considering various types of networks, under different failure models, such as random and targeted failures.

Acknowledgment

This publication was made possible by NPRP grant # [8-519-1-108] from the Qatar National Research Fund (a member of Qatar Foundation). The findings achieved herein are solely the responsibility of the author[s].

References

[1] M. Zamani, L. Camargo-Forero, T. Vicsek. Stability of glassy hierarchical networks. New Journal of Physics. (2018).
[2] H. Mengistu, J. Huizinga, J.-B. Mouret, J. Clune. The evolutionary origins of hierarchy. PLoS computational biology. 12 (2016).
[3] P. Csermely, T. Korcsmáros, H.J.M. Kiss, G. London, R. Nussinov. Structure and dynamics of molecular networks: A novel paradigm of drug discovery: A comprehensive review. Pharmacology & Therapeutics. 138 (2013) 333-408.
[4] H. Aerts, W. Fias, K. Caeyenberghs, D. Marinazzo. Brain networks under attack: robustness properties and the impact of lesions. Brain. 139 (2016) 3063-83.
[5] H.-J. Li, J.J. Daniels. Social significance of community structure: Statistical view. Physical Review E. 91 (2015).
[6] H.-J. Li, Z. Bu, A. Li, Z. Liu, Y. Shi. Fast and accurate mining the community structure: integrating center locating and membership optimization. IEEE Transactions on Knowledge and Data Engineering. 28 (2016) 2349-62.
[7] M. Coscia. Using arborescences to estimate hierarchicalness in directed complex networks. PloS one. 13 (2018).
[8] E. Mones, L. Vicsek, T. Vicsek. Hierarchy measure for complex networks. PloS one. 7 (2012) e33799.
[9] B. Corominas-Murtra, J. Goñi, R.V. Solé, C. Rodríguez-Caso. On the origins of hierarchy in complex networks. Proceedings of the National Academy of Sciences. 110 (2013) 13316-21.
[10] Y. Zhang, Z. Wang, Y. Wang. Multi-hierarchical profiling: an emerging and quantitative approach to characterizing diverse biological networks. Briefings in bioinformatics. (2016).
[11] S. Li. Griffiths phase on hierarchical modular networks with small-world edges. Physical Review E. 95 (2017).
[12] X. Liao, A.V. Vasilakos, Y. He. Small-world human brain networks: Perspectives and challenges. Neuroscience & Biobehavioral Reviews. 77 (2017) 286-300.
[13] D. Pennacchioli, M. Coscia, S. Rinzivillo, F. Giannotti, D. Pedreschi. The retail market as a complex system. EPJ Data Science. 3 (2014) 33.
[14] A. Clauset, S. Arbesman, D.B. Larremore. Systematic inequality and hierarchy in faculty hiring networks. Science advances. 1 (2015).
[15] M. Zamani, T. Vicsek. Glassy nature of hierarchical organizations. Scientific Reports. 7 (2017) 1382.
[16] M. Manzano, E. Calle, D. Harle. Quantitative and qualitative network robustness analysis under different multiple failure scenarios. Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on. IEEE, 2011. p. 1-7.
[17] T.A. Schieber, L. Carpi, A.C. Frery, O.A. Rosso, P.M. Pardalos, M.G. Ravetti. Information theory perspective on network robustness. Physics Letters A. 380 (2016) 359-64.
[18] K. Bilal, M. Manzano, S.U. Khan, E. Calle, K. Li, A.Y. Zomaya. On the characterization of the structural robustness of data center networks. IEEE Transactions on Cloud Computing. 1 (2013).
[19] M. Manzano, K. Bilal, E. Calle, S.U. Khan. On the connectivity of data center networks. IEEE Communications Letters. 17 (2013) 2172-5.

[20] E.T. Wimberley. Nested ecology: the place of humans in the ecological hierarchy. JHU Press, 2009.
[21] A. Clauset, C. Moore, M.E.J. Newman. Hierarchical structure and the prediction of missing links in networks. Nature. 453 (2008) 98.
[22] G.-s. Peng, J. Wu. Optimal network topology for structural robustness based on natural connectivity. Physica A: Statistical Mechanics and its Applications. 443 (2016) 212-20.
[23] E.M. Shahrivar, M. Pirani, S. Sundaram. Robustness and Algebraic Connectivity of Random Interdependent Networks. 48 (2015) 252-7.
[24] H.-J. Li, H. Wang, L. Chen. Measuring robustness of community structure in complex networks. EPL (Europhysics Letters). 108 (2015).
[25] C. Li, H. Wang, W. De Haan, C. Stam, P. Van Mieghem. The correlation of metrics in complex networks with applications in functional brain networks. Journal of Statistical Mechanics: Theory and Experiment. 2011 (2011).
[26] M. Manzano, E. Calle, V. Torres-Padrosa, J. Segovia, D. Harle. Endurance: A new robustness measure for complex networks under multiple failure scenarios. Computer Networks. 57 (2013) 3641-53.
[27] T. Opsahl, F. Agneessens, J. Skvoretz. Node centrality in weighted networks: Generalizing degree and shortest paths. Social networks. 32 (2010) 245-51.
[28] B. Luque, R.V. Solé. Phase transitions in random networks: simple analytic determination of critical points. Physical Review E. 55 (1997) 257.
[29] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, A. Vahdat. The Internet AS-level topology: three data sources and one definitive metric. ACM SIGCOMM Computer Communication Review. 36 (2006) 17-26.
[30] C. Shannon, D. Moore. The spread of the witty worm. IEEE Security & Privacy. 2 (2004) 46-50.

Biography

Kashif Bilal completed his PhD from North Dakota State University, ND USA. He is serving as Assistant Professor at COMSATS University, Pakistan. His research interests include cloud computing, data center networks, green computing, and distributed systems. He has published more than 40 research papers in peer reviewed conferences and journals. He also is a co-author of four book chapters.

Marc Manzano received his PhD in Computer Networks Security by the University of Girona in 2014. He has been an active member in the research community with more than 25 publications in international conferences and first tier journals. Since 2014, Marc has been working in the field of Cryptography Engineering where he has continued his research career.

Aiman Erbad is assistant professor at Computer Science and Engineering department at Qatar University, Qatar. He received his PhD from British Columbia University, Canada. He regularly serves as a technical program committee member in international conferences related to multimedia systems and networking (ACM Multimedia, ACM Multimedia Systems, NOSSDAV, MoVid).

Eusebi Calle obtained his PhD. in 2004, from University of Girona. He is an Associated Professor at the Computer Architecture Department in UdG. His current research interests are design of reliable and robust networks, networks science and telecommunications networks. He has published 100+ papers in international journals and relevant conferences and led/participate different national and international research projects.

Samee U. Khan is an associate professor of electrical and computer engineering at the North Dakota State University. Samee's research interests include optimization, robustness, and security of: cloud, grid, cluster and big data computing, social networks, wired and wireless networks, power systems, smart grids, and optical networks. His work appears in over 250 publications.