Computers and Electrical Engineering 72 (2018) 112–124

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Robustness quantification of hierarchical complex networks under targeted failures☆

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

[a] Qatar University, Doha, Qatar
[b] COMSATS University Islamabad, Abbottabad, Pakistan
[c] University of Girona, Girona, Catalonia, Spain
[d] North Dakota State University, Fargo, ND, USA

ARTICLE INFO

Article history:
Received 31 March 2017
Revised 6 September 2018
Accepted 7 September 2018

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

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.

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

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. G. Martinez Perez.

* Corresponding author at: Qatar University, Al Jamiaa St., Doha, Qatar.
E-mail address: kashif@qu.edu.qa (K. Bilal).

https://doi.org/10.1016/j.compeleceng.2018.09.008
0045-7906/

Table 1
Abbreviation used in the paper.

Abbreviation	Description	Notion	Description
GRC	Global reaching centrality	LRC	Local reaching centrality
AS	Autonomous system	$\mu\|v\|-1$	Algebraic connectivity
⟨l⟩, ASP	Average shortest path length	D	Deterioration
DCN	Data center networks	GC	Giant cluster

[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 1 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: