Commun Nonlinear Sci Numer Simulat 18 (2013) 2722–2732

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

A scoring mechanism for the rank aggregation of network robustness

Alireza Yazdani *, Leonardo Dueñas-Osorio, Qilin Li

Department of Civil and Environmental Engineering, Rice University, Houston, TX 77005, USA

ARTICLE INFO

Article history:
Received 1 August 2012
Received in revised form 23 December 2012
Accepted 6 March 2013
Available online 16 March 2013

Keywords:
Complex graphs
Network topology
Rank aggregation
System vulnerability

ABSTRACT

To date, a number of metrics have been proposed to quantify inherent robustness of network topology against failures. However, each single metric usually only offers a limited view of network vulnerability to different types of random failures and targeted attacks. When applied to certain network configurations, different metrics rank network topology robustness in different orders which is rather inconsistent, and no single metric fully characterizes network robustness against different modes of failure. To overcome such inconsistency, this work proposes a multi-metric approach as the basis of evaluating aggregate ranking of network topology robustness. This is based on simultaneous utilization of a minimal set of distinct robustness metrics that are standardized so to give way to a direct comparison of vulnerability across networks with different sizes and configurations, hence leading to an initial scoring of inherent topology robustness. Subsequently, based on the inputs of initial scoring a rank aggregation method is employed to allocate an overall ranking of robustness to each network topology. A discussion is presented in support of the presented multi-metric approach and its applications to more realistically assess and rank network topology robustness.

1. Introduction

Many complex systems in nature, society and technology are networks consisting of multiple elements joined by different types of connections and links. Examples of different types of such networks include social networks consisting of the people and their contacts, information networks such as the World Wide Web consisting of the web pages and links between them, and technological networks such as the Internet consisting of the computers and physical connections between them [1]. In general, a network is an abstract mathematical structure which consists of a set of objects and their connections (known as a graph), as well as information associated with the function or attributes of these objects and the type of connections between them [2].

One important observation giving rise to the broader studies of the topology of networks is that "the structure affects function" [3]. In other words, there exist a large extent of interactions between network architecture and its dynamics that makes the study of the network topology crucial. In particular, this is true in the case of technological and physical networks where system topology is formed (i.e. evolved or designed) to support certain activities towards operational and service objectives. Subsequently, any changes in the network topology (e.g. due to operational constraints, the failure of a fraction of components or retrofit activities) will have consequences in terms of system operation and its ability to function.

* Corresponding author.
E-mail address: alireza.yazdani@rice.edu (A. Yazdani).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.03.002

Studying the relationship between network topology and performance with focus on assessing robustness to failures allows the identification of structural holes (nodes whose neighboring nodes are not connected), indicates the presence and location of high-flux regions and single points of failure such as the hubs and bridges, and enables measuring network vulnerability to random failures or malicious attacks on system components [4–12]. In addition, network design improvement strategies may be devised and implemented in the same context to reduce the vulnerability of certain configurations such as scale-free networks [6] to targeted attacks on their hubs and other centrally positioned nodes [8]).

Two distinct but related approaches to assessing robustness include estimating the probability of network connectivity subject to various component failure scenarios, and examining pure graph connectivity for assessing robustness inherent in network topology [13]. In the later context, failure is modeled by the removal of components which may take place once or consecutively either randomly or as a result of a targeted attack. In general, conducting the probabilistic analysis of network reliability while incorporating different failure scenarios involves highly data-dependent and computationally intensive simulations even for relatively simple networks [14]. Hence, the second approach, hereafter referred to as robustness analysis, simply develops or employs inexpensive graph metrics to quantify network topology and interprets their values toward network robustness.

To conduct robustness analysis of networks, closed-form analytical metrics have been proposed based on the direct application or modification of simpler graph topology metrics which indicate robustness properties inherent to network topology. For example, the betweenness centrality of an edge has been used as an (approximate) indicator of the component's critical role in the passage of network flow [4,9], or it has been used along with the other edge betweenness values to compute an integrated metric called "multiscale vulnerability" [15,16] that approximates network-level vulnerability to failures for a diverse selection of network layouts.

However, in spite of offering a computationally inexpensive methodology, it will be demonstrated later in this work that a major drawback of the described robustness analyses is that they fail to fully capture the vulnerability of generic network configurations to random failures and targeted attacks, particularly when relying on the use of a single metric only. Moreover, the described metrics only allow comparing topology robustness for networks of the same order and size. In reality, however, there exist situations when comparing robustness across networks with different sizes and layouts is required. These comparisons may become necessary to study the effects of network size (and its increase due to expansion) on overall robustness, or to assess the long-term cost and benefits of network topology modifications and alternative design strategies. Subsequently, it is increasingly important to improve the existing robustness analysis methods to overcome such limitations.

A potential way to overcome the mentioned problem of the inadequacy of single-metric approach to characterizing network topology robustness is via undertaking a "multi-metric" approach to assessing the robustness of the topology of an "ensemble" of networks. This implies the use of a selection of relevant robustness metrics simultaneously, rather than using one single metric in isolation, and applying them to an ideally large and diverse selection (realization) of network layouts. In theory, the selected set of metrics must be sufficiently large and be comprehensive to capture different aspects of network topology robustness against multiple types of potential failures and mishaps, including random failures and targeted attacks taking place in isolation or in sequence. In addition, the chosen ensemble of network models must be sufficiently large and diverse to incorporate a variety of different network sizes and layouts, and to yield a wide range of different values for each metric.

This work demonstrates the construction and application of such a multi-metric approach by utilizing a selection of frequently used metrics of robustness analysis and exploring their usefulness in characterizing the robustness (or vulnerability) inherent in the topology of a number of purposefully synthesized network models. These network models are generated in such a fashion to offer diversity through the size and layout, and are grouped into two main categories of hierarchically organized and distributed layouts. This grouping is meant to offer an intuitive and simple yet practical guideline for the replication and categorization of the real world networks, according to a set of layout constraints and a number of perceived modes of system operation to support optimal flow distribution across networks in practice.

The robustness metrics are briefly studied for their scope and discriminatory power in capturing different aspects of network topology robustness to random failures and targeted attacks, and they are used to separately quantify the robustness of each studied network. To enable direct comparisons across networks, a standardization of the metrics is proposed and an initial ranking of network robustness by each individual metrics is formed. Subsequently, the existence of correlation between metrics is investigated in order to determine the possibility of using them interchangeably and, in particular, to detect correlation and redundancy among them. After eliminating such redundancies, a minimal set of standardized discriminant metrics is obtained which is used to generate an aggregate ranking of network robustness based on the input of initial rankings generated by each individual metric. The thus generated aggregate ranking is subsequently adopted as a new superior combined multi-faceted scoring mechanism to address the issue of inadequacy of single-metric approach to characterizing network topology robustness.

The remainder of this paper is structured as follows. Section two introduces some of the most important and commonly used metrics of network topology robustness. In section three, the hierarchical and distributed network models are constructed and their topology specifications are studied as a way to emphasize the critical role of certain intricate configurations in overall robustness of many real world technological networks. In section four the topology of a number of case study networks are studied, their vulnerability to different types of failures are quantified by using the introduced metrics, and their overall robustness is directly compared through introducing a standardization of individual metrics following the elimination of redundancies and correlation among metrics. Then in section five, a rank aggregation process is proposed to