Physica A 478 (2017) 63–68

Contents lists available at ScienceDirect

Physica A

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

Efficient calculation of the robustness measure R for complex networks

Chen Hong [a], Ning He [a], Oriol Lordan [b,*], Bo-Yuan Liang [c,d,e], Nai-Yu Yin [c,d,e]

[a] College of Information Technology, Beijing Union University, Beijing 100101, PR China
[b] Universitat Politècnica de Catalunya-BarcelonaTech, Colom 11, Terrassa 08222, Spain
[c] School of Electronic and Information Engineering, Beihang University, Beijing 100191, PR China
[d] Beijing Key Laboratory for Network-based Cooperative Air Traffic Management, Beijing 100191, PR China
[e] Beijing Laboratory for General Aviation Technology, Beijing 100191, PR China

HIGHLIGHTS

- We propose a measure R' to improve the calculation efficiency of network robustness measure R.
- We confirm the reasonability of R' on three types network models and three real networks.
- The relationships between R' and the network size and the network average degree are investigated.

ARTICLE INFO

Article history:
Received 20 November 2016
Received in revised form 22 January 2017
Available online 28 February 2017

Keywords:
Network robustness
Robustness measure
Malicious attack
Complex networks

ABSTRACT

In a recent work, Schneider et al. (2011) proposed a new measure R for network robustness, where the value of R is calculated within the entire process of malicious node attacks. In this paper, we present an approach to improve the calculation efficiency of R, in which a computationally efficient robustness measure R' is introduced when the fraction of failed nodes reaches to a critical threshold q_c. Simulation results on three different types of network models and three real networks show that these networks all exhibit a computationally efficient robustness measure R'. The relationships between R' and the network size N and the network average degree $\langle k \rangle$ are also explored. It is found that the value of R' decreases with N while increases with $\langle k \rangle$. Our results would be useful for improving the calculation efficiency of network robustness measure R for complex networks.

1. Introduction

A wide range of systems in nature and society can be described as complex networks, such as the World Wide Web, neural networks and air transportation networks, etc. In the past decades, the study of complex networks has given rise to great achievements in many fields [1–4], such as network modeling [5–7], cascading failures [8–12], evolutionary games [13–16], optimization [17–19] and traffic dynamics [20–22] and so on.

Large infrastructure networks such as the Internet, power grids and transportation systems [23,24] play a significant role in the modern world. As the robustness of infrastructure networks is becoming more and more important, the robustness of

* Corresponding author.
E-mail address: oriol.lordan@upc.edu (O. Lordan).

http://dx.doi.org/10.1016/j.physa.2017.02.054
0378-4371/

complex networks has attracted many researchers in recent years [25–29]. Albert et al. [30] found that complex networks with scale-free character are robust to random failures but vulnerable under malicious attacks. Cohen et al. [31] explored the robustness of the Internet and proposed an analytical approach to find the critical percolation threshold on random networks. Holme et al. [32] investigated the effect of four attacking strategies: removal by descending order of betweenness and degree, calculated for either the current network during the removal process or the initial network. It is found that adaptive attack strategies are more effective than attack strategies based on the initial network.

Recently, Schneider et al. [33] proposed a new measure R for network robustness and investigated optimal network structure against high-degree node removal with respect to this measure. They found that the final robust networks exhibit an onion structure in which highly connected nodes form a core surrounded by rings of nodes with decreasing degree. Following the pioneering work of Schneider et al., many researchers have used this new robustness measure and onion-like structure to explore the robustness of networks [34–37]. Wu et al. [38] proposed a generative algorithm to efficiently produce synthetic scale-free networks with onion structure and validated the robustness of their generated networks against malicious attacks and random failures. Complementary to the node-robustness measure, Zeng et al. [39] proposed a link-robustness index and designed a hybrid greedy algorithm to against both node and link attacks. The results show that network robustness can be significantly improved. In previous works, the value of network robustness measure R is calculated within the whole process of malicious attacks, resulting in a time-consuming calculation process. In modern society, there are many large networks such as the World Wide Web and the Internet, hence the computation cost of network robustness measure on large networks needs to be considered. This calls for a quicker, smarter method to calculate the value of network robustness measure R. In this paper, we propose a computationally efficient robustness measure corresponding to the critical fraction of attacked nodes and confirm its reasonability on three types of network models and three real complex networks.

The paper is organized as follows. In the next section we demonstrate the computationally efficient robustness measure and attacking strategies in detail. In Section 3, simulation results and correspondent theoretical analysis are provided. Finally, the work is summarized in Section 4.

2. The model

The unique network robustness measure proposed by Schneider et al. is defined as [33]

$$R = \frac{1}{N}\sum_{q=1/N}^{1} s(q), \tag{1}$$

where N is the number of nodes in the network, q is the fraction of removed nodes and $s(q)$ is the fraction of nodes in the largest connected component after removing qN largest degree nodes. The normalization factor $1/N$ ensures the comparability of network robustness of different sizes. The range of possible values of R is between 0 and 0.5, where $R = 0$ corresponds to a star network, in which all nodes in the network are isolated after removing the hub node. If $R = 0.5$, the original network is a fully connected network and the largest connected component decreases only one node at each node attack step [34]. Obviously, networks with higher value of R are of stronger resistance to targeted node attacks.

Since the robustness measure R captures the effects on the network over the entire attack sequence, it is especially time-consuming when the size of the network is huge. From the definition of R, we can see that R is strongly correlated with the size of the largest connected component. It is known that network robustness can also be measured by the critical percolation threshold q_c, which is the minimum value of the remaining node fraction required for a unique giant component to be of the order of the entire network under attacks [30–32]. For huge networks, since the change of $s(q)$ is relatively small after the giant component completely collapses, it is reasonable that the calculation efficiency of R will be efficiently improved if the calculation process is stopped at $q = q_c$.

To estimate the calculation efficiency of R, we define a cost-based function

$$R(t) = \frac{1}{N}\sum_{q=1/N}^{t} s(q) \approx t - \frac{t(tN+1)}{2N}, \tag{2}$$

where $t(1/N \le t \le 1)$ is the cost indicator of the calculation process and $R = R(1)$. Obviously, the smaller the value of t, the lower the calculation cost of $R(t)$. If the network is fully connected and the largest connected component decreases only one node at each node attack step, we can get $R(t) \approx \frac{1}{N}(\frac{N-1}{N} + \frac{N-2}{N} + \cdots + \frac{N-tN}{N}) = t - \frac{t(tN+1)}{2N}$. Consequently, $R(1) \approx (N-1)/2N \approx 0.5$, $R(1/N) \approx (N-1)/N^2$ and $R(1/N) \approx 0$ for large N values, indicating that the range of $R(t)$ values is the same as that for R.

Based on above analyses, we propose a computationally efficient robustness measure which is defined as

$$R' = R(q_c) = \frac{1}{N}\sum_{q=1/N}^{q_c} s(q) \approx q_c\left(1 - \frac{1}{2N}\right) - \frac{q_c^2}{2}, \tag{3}$$