Physica A 503 (2018) 503–515

Contents lists available at ScienceDirect

Physica A

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

A heuristic algorithm for enhancing the robustness of scale-free networks based on edge classification

Lei Rong, Jing Liu *

Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, Xidian University, Xi'an 710071, China

HIGHLIGHTS

- A heuristic algorithm based on edge classification, termed as EC-RSF$_{MA}$, is proposed.
- EC-RSF$_{MA}$ can enhance the robustness of scale-free networks.
- Two types of malicious attacks are studied.
- EC-RSF$_{MA}$ outperforms the existing algorithms in experiments.

ARTICLE INFO

Article history:
Received 13 August 2017
Received in revised form 11 January 2018
Available online 2 March 2018

Keywords:
Scale-free networks
Robustness
Malicious attacks
Edge classification

ABSTRACT

The essential of existing methods for promoting network robustness is randomly exchanging the edges of networks. Without considering the network structure, the performance of these algorithms is limited. Therefore, we put forward a way for classifying the edges of networks into three types, which are valid edges, invalid edges and flexible edges. Then, a heuristic optimization algorithm, which is designed based on the edge classification (EC) against malicious attacks (MA), is proposed to improve the robustness of scale-free (RSF) network termed as EC-RSF$_{MA}$. EC-RSF$_{MA}$ improves the robustness of scale-free networks by adjusting the number of edges of each type and changing the connection relation of the same type of edges under the constraint that the degree distribution remains to be unchanged. In the experiments, the performance of EC-RSF$_{MA}$ is validated on both synthetic and real-world networks. The results show that EC-RSF$_{MA}$ outperforms the existing algorithms.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

In reality, most nature and society systems can be represented by networks [1–5] to reflect their connectivity and improve the efficiency [6]. Most of these networks can be considered as scale-free networks [7], and many articles demonstrated that the scale-free network is robust against random attacks, but fragile when suffering from malicious attacks [8–10]. Power grids, whose degree distribution can be expressed by $P(k) \propto k^{-\gamma}$, is one of real-world networks that can be considered as scale-free networks. On Oct. 6, 2013, a man attacked a high-voltage transmission line near Cabot, Arkansas, USA. 10 000 customers lost power as a result [11]. This event shows that the fragility of scale-free networks against malicious attacks is likely to cause economic losses in the real-world network system. So the robustness of networks has been intensively studied in the past decade [12–17].

* Corresponding author.
E-mail address: neouma@mail.xidian.edu.cn (J. Liu).
URL: http://see.xidian.edu.cn/faculty/liujing (J. Liu).

https://doi.org/10.1016/j.physa.2018.02.173
0378-4371/© 2018 Elsevier B.V. All rights reserved.

Much attention has been paid on searching for the network topology with better robustness [18,19], however, the performance of existing methods are limited in optimizing the real-world networks. Because the degree distribution has been fixed, and a wide range of changes result in high maintenance costs. Therefore, to enhance the robustness of networks must ensure that the degree distribution be unchanged. Several methods have been proposed to optimize the robustness of scale-free networks, such as hill climbing [20], simulated annealing [21], and memetic algorithm [22,23]. The hill climbing algorithm and the simulated annealing algorithm are based on the random swap operator. The memetic algorithms in [22] uses a cross-operator to realize global search, which makes this algorithm has better performance. In these algorithms, the optimal strategies are based on some existing heuristic algorithms, and these algorithms do not find the factors that influence the robustness of networks. Moreover, these algorithms perform poorly when optimizing large-scale networks.

In this paper, we design a classification method to find out which type of edges affect the size of largest connected cluster in the current network. The principle of edge classification is based on the attribute of nodes connected through the edge, since the determination of robustness is the number of nodes in the largest connected cluster. The largest connected cluster is in the network after attacked, so these edges in this network can be discriminated from other edges. The edges connect removed nodes and the edges connect removed nodes to nodes in the network after attacked are two other types of edges. The proposed algorithm, termed as EC-RSF$_{MA}$, is based on the edge classification (EC) to enhance the robustness of scale-free network (RSF) against malicious attacks (MA) under the constraint that the degree distribution is unchanged. The idea of EC-RSF$_{MA}$ is to transform the type of edges, so as to adjust the number of edges with different type, and optimize the connection of each type of edges to enhance the robustness of networks. In EC-RSF$_{MA}$, we design five operators to realize the adjustment and optimization operation. The optimization operators are improved random swap operator with more constraint. In this operator, one of the swapped edge is fixed and the other one is randomly selected from the edges that satisfy the constraints. With different constraints, three modulation operators and two rehabilitation operators are proposed. Experiments on both synthetic and real-world networks are conducted, and the results show that EC-RSF$_{MA}$ outperforms the existing methods. Moreover, the performance of EC-RSF$_{MA}$ is not significantly declined when optimizing large-scale networks.

The rest of this paper is organized as follows. Section 2 introduces the construction of scale-free network and the robustness measures used in this paper. The edge classification measure and description of EC-RSF$_{MA}$ are given in Section 3. Section 4 shows the experimental results of EC-RSF$_{MA}$ on synthetic and real-world networks, together with the comparisons with other algorithms. Finally, the conclusions are given in Section 5.

2. Robustness measures

2.1. Scale-free network construction

Many real-world networks have the following common characteristics: most nodes have only a few links, and some nodes have a large number of links connected to other nodes, expressed in the degree of distribution is a power-law distribution [24–26]. These nodes with a large number of links are called "hubs", and the number of connections may be as high as several hundreds, thousands or even millions. The network containing such hubs is called a scale-free network. Barabási and Albert proposed a scale-free network model, known as the BA model [3,7], in order to explain the mechanism of power-law distribution. The network studied in this paper are undirected and unweighted BA networks, which are generated as follows:

Starting from N_0 connected nodes, each time a new node is introduced and connected to m already existing nodes, where $m < N_0$. The probability $\prod_i$ that a new node connects with an existing node v_i with k_i degree satisfies the following relation:

$$\prod_i = \frac{k_i + 1}{\sum_j (k_i + 1)} \tag{1}$$

The scale-free network has a preferential connection feature that the new nodes are more likely to connect to those nodes with higher degree.

2.2. Network robustness measure

This study is aimed at robustness under malicious attacks, and the malicious attacks used are high degree adaptive attack (HDA) [12,27,28], which is now widely used to evaluate the robustness of networks. HDA works as follows: each attack removes the node with the highest degree and all related links, recalculates the nodes' degree, and then executes the attack again until all nodes are removed.

In addition, the attack strategy based on betweenness centrality [12] is also studied. The betweenness centrality is the normalization parameter of betweenness, which can reflect the influence of node against the network. The betweenness B_i is defined as

$$B_i = \sum_{\substack{1 \le j < l \le N \\ j \ne i \ne l}} \left[\frac{n_{jl}(i)}{n_{jl}} \right] \tag{2}$$

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

- ✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
- ✓ امکان دانلود نسخه ترجمه شده مقالات
- ✓ پذیرش سفارش ترجمه تخصصی
- ✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
- ✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
- ✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
- ✓ دانلود فوری مقاله پس از پرداخت آنلاین
- ✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات