Physica A xx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Physica A

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

A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks

Q1 Mingxing Zhou, Jing Liu *

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

HIGHLIGHTS

- A memetic algorithm is proposed for enhancing the robustness of scale-free networks.
- Malicious attacks are considered.
- The degree distribution of the networks is preserved.
- Effective global and local search operators are designed.
- The good performance of the new algorithm is validated using various networks.

ARTICLE INFO

Article history:
Received 2 January 2014
Received in revised form 26 March 2014
Available online xxxx

Keywords:
Robustness
Memetic algorithms
Scare-free networks
Malicious attacks

ABSTRACT

The robustness of the infrastructure of various real-life systems, which can be represented by networks and manifests the scale-free property, is of great importance. Thus, in this paper, a new memetic algorithm (MA), which is a type of effective optimization method combining both global and local searches, is proposed to enhance the robustness of scale-free (RSF) networks against malicious attacks (MA) without changing the degree distribution. The proposed algorithm is abbreviated as MA–RSF_{MA}. Especially, with the intrinsic properties of the problem of optimizing network structure in mind, a crossover operator which can perform global search and a local search operator are designed. In the experiments, both synthetic scale-free networks and real-world networks, like the EU power grid network and the real Internet at the level of autonomous system (AS), are used. MA–RSF_{MA} shows a strong ability in searching for the most robust network structure, and clearly outperforms existing local search methods.

1. Introduction

A wide range of systems in nature and society can be modeled by networks with complex topology [1–4]. One extremely important aspect of a network is its capability to withstand failures and fluctuations in the functionality of its nodes and links, namely the robustness. Of course, failures may occur in many different ways and to a different degree, depending on the complexity of the system under examination. Thus, the robustness of networks is of great importance to guarantee the security of network systems, such as the airports, the power grids, the transportation, the World Wide Web, and the disease control networks. Therefore, the robustness of different network structures has been studied intensively in the past decade [5–13].

There are several ways to define the robustness of a network [6,14,15]. Usually, a network is robust if their function is not affected by the attacks to nodes or links, which can be either random or malicious. In random attacks, nodes or links

* Correspondence to: P.O. Box 224, Xidian University, Xi'an 710071, China. Tel.: +86 29 88202661.
E-mail addresses: neouma@mail.xidian.edu.cn, neouma@163.com (J. Liu).

http://dx.doi.org/10.1016/j.physa.2014.05.002
0378-4371/

will be removed by the same probability. As for the malicious attacks, a widely studied one is the *high degree adaptive attack* (*HDA*) [6], which crashes down network nodes in a decreasing order of their nodal degrees. This is also the malicious attack we consider in this paper. Existing studies showed that only a few types of network are robust against both random and malicious attacks [16,17].

One particular class of complex networks—scale-free networks [1,4] has attracted much attention. As well known, one of the most important results about scale-free networks is that while scale-free networks are strongly tolerant against random failures, they are fragile under malicious attacks. Motivated by this result, many important related studies have been done. For example, Hooyberghs et al. in Ref. [18] performed a detailed study of biased percolation on scale-free networks and have shown that it is possible to tune a robust network fragile and vice versa. Due to the important role of the nodes with the largest degree in scale-free networks, Moreira et al. in Ref. [19] investigated the statistics of the most connected node in scale-free networks and have shown that the distribution of maxima follows the Gumbel statistics for a scale-free network model with homogeneous nodes.

In fact, the fragileness of the scale-free networks under the malicious attacks comes from their heavy-tailed property, causing loss of a large number of links when a hub node is crashed. The heavy loss of network links quickly makes the network to be sparsely connected and then fragmented. Thus, the major purpose of this work is to study how to improve the robustness of scale-free networks against malicious attacks. A simple solution for this problem is to add links, but additional links also increase the costs significantly. Therefore, we consider how to improve the network robustness against HDAs without changing the degree distribution of the initial networks.

A few studies have been proposed to tackle this problem. Xiao et al. in Ref. [20] designed a simple rewiring method which does not change any nodal degree, and showed that network robustness can be steadily enhanced at a slightly decreased assortativity coefficient. In Ref. [21], Schneider et al. introduced a new measure for robustness, which considers the size of the largest connected cluster during the entire attack process, and used this measure to devise a heuristic method to mitigate the malicious attacks. Based on the same measure, Buesser et al. in Ref. [22] proposed a simulated annealing algorithm and Louzada et al. in Ref. [23] proposed a smart rewiring method for this problem. All these methods manifest a good performance in improving the network robustness over the initial networks. However, these methods can still be improved by considering the possibility of global searches in the optimization algorithm. Thus, more powerful methods which can conduct both global and local searches are needed to optimize the network structure.

Evolutionary algorithms (EAs), which are a kind of stochastic global optimization method inspired by the biological mechanism of evolution and heredity, have been successfully used to solve various hard optimization problems. One popular branch in the field of EAs is memetic algorithms (MAs), where the concept of "memetic" came from Dawkin's concept of a meme, which represents a unit of cultural evolution that can exhibit local refinement [24,25]. In MAs, a meme is generally considered as an individual learning procedure capable of performing local refinements. Thus, MAs successfully combine global and local searches, and have been shown to be more efficient and more effective than traditional EAs for many problems [26–32].

Therefore, in this paper, we design a suitable memetic algorithm to improve the robustness of scale-free networks (RSF) against malicious attacks keeping the degree distribution and the connectivity of single node unchanged. The proposed algorithm is named as MA–RSF$_{MA}$, and a crossover operator which can perform global search and a local search operator are designed. We demonstrate its efficiency on both synthetic and real-world networks; that is, different types of networks are used as the initial state for our optimization procedure. The results show that MA–RSF$_{MA}$ can improve the network robustness against HDA dramatically while keeping the node degrees constant. Moreover, the comparison with existing local search methods also show that MA–RSF$_{MA}$ outperforms existing methods, and can obtain much more robust networks.

The rest of this paper is organized as follows. Section 2 introduces the robustness measure used in this paper. MA–RSF$_{MA}$ is described in detail in Section 3, while experiments are given in Section 4. Finally, conclusions and future work are given in Section 5.

2. Network robustness against malicious attacks

A network can be represented as a graph $G = (V, E)$, where $V = \{1, 2, \ldots, N\}$ is the set of N nodes, and $E = \{e_{ij} \mid i, j \in V \text{ and } i \neq j\}$ is the set of M links. In this study, we focus on targeted attacks on undirected and unweighted networks with a long-tailed degree distribution, namely undirected and unweighted scale-free networks. For this type of networks, targeted attacks are more interesting since they are fragile under this type of intentional damage. Moreover, scale-free networks have been found among many important networks in society and in biological systems, which mean that they are also important in practice.

To construct scale-free networks, the well-known Barabási–Albert model (BA model) [1,4] is used. The BA model starts with a small clique (a complete connected graph) of N_0 nodes. At each successive time step, a new node is added and M_0 edges are added to link this new node to M_0 existing nodes, where M_0 is smaller than the number of existing nodes. When a new node is connected to an existing node, it is assumed that the probability that an existing node is selected is proportional to its degree; that is, nodes that already have many links are more likely to be chosen over those that have few. This is called preferential attachment and is an effect that has been observed in real networks.

It is assumed that the malicious attack is the HDA, and works in this way [6,21,33]: at each time step, network nodes are sorted in decreasing degree order and the highest degree node is removed together with all its links. After removing that

Please cite this article in press as: M. Zhou, J. Liu, A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks, Physica A (2014), http://dx.doi.org/10.1016/j.physa.2014.05.002