Physica A 446 (2016) 82–91

Contents lists available at ScienceDirect

Physica A

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

# Tabu Search enhances network robustness under targeted attacks

Shi-wen Sun*, Yi-lin Ma, Rui-qi Li, Li Wang, Cheng-yi Xia

*Key Laboratory of Computer Vision and System (Ministry of Education), Tianjin University of Technology, Tianjin 300384, China*
*Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology, Tianjin University of Technology,*
*Tianjin 300384, China*

## HIGHLIGHTS

- The problem of improving the robustness of complex networks is concerned.
- An optimization model is established to maximize the robustness measure $R$.
- An efficient optimization method based on Tabu Search is provided.
- Numerical simulation results verify the effectiveness of proposed algorithm.

## ARTICLE INFO

*Article history:*
Received 26 May 2015
Received in revised form 25 September 2015
Available online 30 November 2015

*Keywords:*
Network robustness
Attack
Combinatorial optimization
Tabu Search
Complex networks

## ABSTRACT

We focus on the optimization of network robustness with respect to intentional attacks on high-degree nodes. Given an existing network, this problem can be considered as a typical single-objective combinatorial optimization problem. Based on the heuristic Tabu Search optimization algorithm, a link-rewiring method is applied to reconstruct the network while keeping the degree of every node unchanged. Through numerical simulations, BA scale-free network and two real-world networks are investigated to verify the effectiveness of the proposed optimization method. Meanwhile, we analyze how the optimization affects other topological properties of the networks, including natural connectivity, clustering coefficient and degree–degree correlation. The current results can help to improve the robustness of existing complex real-world systems, as well as to provide some insights into the design of robust networks.

## 1. Introduction

Attack robustness (or resilience) is one of the most important properties of complex networked systems [1–3]. A network is said to be *robust* if as many as possible elements of the system remain globally connected even after a fraction of nodes or edges have been removed. Firstly, Albert et al. [4] found the "*robust yet fragile*" generic property of scale-free networks: scale-free networks display an unexpected degree of robustness to random failure; however, they are extremely vulnerable to intentional attack on high-degree nodes. Cohen et al. [5,6] theoretically studied the resilience of scale-free networks with power-law degree distribution $p(k) \sim k^{-\gamma}$ under random node removal; it was found that for network with exponent $\gamma \leq 3$, the critical fraction $f_c$ of nodes, which need to be removed before the network disintegrates, tends to 1 if the

[*] Corresponding author at: Key Laboratory of Computer Vision and System (Ministry of Education), Tianjin University of Technology, Tianjin 300384, China.
*E-mail address:* sunsw80@126.com (S.-w. Sun).

http://dx.doi.org/10.1016/j.physa.2015.10.086
0378-4371/© 2015 Elsevier B.V. All rights reserved.

network size $N \to \infty$. The result indicates that this kind of networks is impressively robust to random attacks. Furthermore, much attention had been paid to the effects of different topological properties on attack robustness, including the degree distribution, centrality, assortativity, the interaction strength of the edges and so on [7–14]. Meanwhile, the subject of network robustness against attacks has also attracted considerable interest in terms of other important dynamical behaviors occurred on networks [15,16].

However, given an existing networked system, how and at which cost can one improve the robustness against random and/or malicious attacks? Many researchers have devoted a great deal of efforts to this topic. Valente et al. [17] found that given a network with fixed numbers of nodes and links the optimal configuration which can maximize the percolation threshold under attacks and/or random failures has at most three distinct node degrees. Paul et al. [18] found that networks with bimodal degree distributions, i.e. $q \sim \sqrt{N}$ hub nodes and $N - q$ nodes of degree 1, are most robust to random breakdowns. Also, many methods have been developed to reconstruct the networks with small modifications in topologies, including link rewiring [19,20], link adding [21], link deleting [22] and link repairing [23]. By maximizing the network efficiency while keeping the number of links constant, Wang et al. [19,20] developed a link-rewiring method, combining the Tabu Search heuristic algorithm, to modify the structure of a random network with a Poisson degree distribution. Shi et al. [21] proposed a method to significantly increase the robustness of scale-free complex networks by allocating a few redundant links among key nodes. Motter [22] introduced a costless strategy based on a selective further removal of nodes and edges right after the initial attack or failure on highly loaded nodes, thus preventing the cascade from propagating through the entire network. Chi et al. [23] studied the stability of random networks under the evolution of attack and repair, that is, after the attacks on the key nodes, the removed links are repaired with a predefined probability.

Recently, Schneider et al. [24] proposed a new robustness measure $R$ and developed an efficient method to generate robust networks against malicious attacks. The robustness of a given network can be improved significantly with small changes in the network structure at low cost. Furthermore, all the final networks after optimization exhibit a novel type of "onion-like" topology in which high-degree nodes form a core surrounded by rings of nodes with decreasing degree.

In our study, we concentrate on the optimization of network robustness against intentional attacks. From a different perspective, the problem of improving the robustness of an existing network can be considered as a typical combinatorial optimization problem. As a result, motivated by the optimization methods proposed in Refs. [19,20,24], an efficient method is developed to greatly enhance network robustness with relatively minor modifications on the topology. Different from the local-search method, a heuristic Tabu Search strategy [25,26] is introduced to improve the efficiency of the optimization. Through numerical simulations, the optimization method is applied to two typical real-world networks as well as one artificial Barabási–Albert (BA) scale-free network [27]. Furthermore, we investigate the effect of the optimization on other topological properties [28], including natural connectivity [29], clustering coefficient [30] and degree–degree correlation [31].

The rest of this paper is organized as follows. In Section 2, the optimization model aiming at maximizing the robustness measure $R$ is presented, followed by the description of the optimization algorithm based on Tabu Search. In Section 3, through numerical simulations, the optimization method is applied to BA scale-free network and two air transport networks, moreover, the effect of optimization on several important topological properties is investigated numerically. We conclude the whole paper in Section 4.

## 2. Models and optimization algorithm

### 2.1. Optimization model

When nodes are gradually damaged due to random failures or targeted attacks, a network may be split into several unconnected parts. In percolation theory, the robustness of networks is usually measured by the percolation threshold $f_c$, the critical fraction of nodes attacked, at which the whole network collapses completely. However, in realistic cases, this measure overlooks situations in which the networks suffer from a big damage but they are not completely collapsing. Recently, Schneider et al. [24] proposed a novel measure, node robustness $R$, to evaluate the robustness of networks under attacks considering the size of the largest connected component during all possible malicious attacks, namely,

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

where $N$ is the total number of nodes in the initial network and $S(q)$ denotes the relative size of the largest connected component after removing $q$ nodes with the highest degrees. The normalization factor $1/N$ ensures $1/N \le R \le 0.5$. Two special cases exist: $R = 1/N$ corresponds to star-like networks while $R = 0.5$ to the case of fully-connected network. Generally, the larger the value of $R$, the more robust the network resisting intentional attacks on high degree nodes.

With the robustness criterion $R$ in mind, the network optimization problem can be regarded as a standard single-objective combinatorial optimization problem which can be defined as follows: given a network $G$ with the predefined