ARTICLE IN PRESS

Physica A ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Physica A

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

Optimal defense resource allocation in scale-free networks

Xuejun Zhang [a,b,c], Guoqiang Xu [a,b,c], Yongxiang Xia [d,*]

[a] School of Electronic and Information Engineering, Beihang University, Beijing 100191, China
[b] Beijing Key Laboratory for Network-based Cooperative Air Traffic Management, Beijing 100191, China
[c] Beijing Laboratory for General Aviation Technology, Beijing 100191, China
[d] College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China

HIGHLIGHTS

- A specific PSO algorithm was proposed to optimize the resource allocation.
- The PSO based strategy outperforms other traditional strategies.
- The optimal resource allocation pattern was investigated.
- We considered real-world network to verify the efficiency of PSO based strategy.

ARTICLE INFO

Article history:
Received 3 May 2017
Received in revised form 1 September 2017
Available online xxxx

Keywords:
Complex networks
Robustness
Defense resource allocation
Particle swarm optimization

ABSTRACT

The robustness research of networked systems has drawn widespread attention in the past decade, and one of the central topics is to protect the network from external attacks through allocating appropriate defense resource to different nodes. In this paper, we apply a specific particle swarm optimization (PSO) algorithm to optimize the defense resource allocation in scale-free networks. Results reveal that PSO based resource allocation shows a higher robustness than other resource allocation strategies such as uniform, degree-proportional, and betweenness-proportional allocation strategies. Furthermore, we find that assigning less resource to middle-degree nodes under small-scale attack while more resource to low-degree nodes under large-scale attack is conductive to improving the network robustness. Our work provides an insight into the optimal defense resource allocation pattern in scale-free networks and is helpful for designing a more robust network.

1. Introduction

The infrastructure of complex systems, such as World-Wide Web, power grid, transportation systems and communication systems, plays an increasingly significant role in our daily life [1]. However, they may fall into abnormal operation under the random malfunction or external attacks and cause serious consequence such as blackouts [2], flight delays [3] or communication outages [4].

These infrastructures can be modeled as networks and studied by using the complex network theory. One interesting and significant research field is to study the network robustness [5–8]. Albert et al. [5] found that scale-free networks present a surprisingly high degree of tolerance against random failures, but sensitive to malicious attacks through the numerical simulation results. Subsequently, Cohen et al. [6] studied the robustness of scale-free networks against random attack by theoretical analysis and found the critical percolation threshold of the Internet. In the research of network robustness models,

* Corresponding author.
E-mail address: xiayx@zju.edu.cn (Y. Xia).

https://doi.org/10.1016/j.physa.2017.11.135
0378-4371/

different attack strategies were investigated, including random attack, high-degree attack, and high-centrality attack. Holme et al. [7] investigated the network robustness under four different attack strategies: removals by the descending order of the degree and the betweenness centrality, calculated for either the initial network or the updated network during the removal procedure. It is found that the recalculated attack strategy is often more effective than the attack strategies based on the initial network. These studies are mainly focused on the case of isolated networks. However, many real networked infrastructures are actually coupled with each other. Buldyrev et al. [9] analyzed the electrical blackout in Italy, and studied the robustness of the interdependent networks with a cascading failures framework. Brummitt et al. [10] investigated the sandpile model on modular random graphs and power grids, and found that some connectivity is beneficial but too much interconnectivity becomes detrimental. Tan et al. [11] found the robust-yet-fragile nature of interdependent scale-free networks.

Most previous works have the same assumption that an attacker pays equal attack cost to remove different nodes. However, this assumption is unrealistic for the fact that the hub nodes often have a stronger ability to resist attacks than the other nodes in practice. In other words, different nodes have different resource to defend themselves. Based on this fact, Zheng et al. [12] investigated the robustness of the scale-free networks under the selective node attack with different node defense resource. Hong et al. [13] assumed that the node defense resource is positively correlated to the degree of nodes and studied the effect of attack cost on network robustness. It is found that the performance of different attack strategies is sensitive to the total attack cost. Therefore, the defense resource allocation plays a crucial role to determine the network robustness under different attack strategies.

How to effectively allocate limited defense resource to each node is a significant issue to improve the network robustness. Actually, the essence of node defense resource allocation in scale-free networks is an optimization problem. Recently, the intelligent optimization algorithms have been applied to the network optimization [14–17]. Zhou et al. [14] proposed an adaptive memetic algorithm (MA) to enhance the robustness of scale-free networks against malicious attack without changing the degree distribution. Chen et al. [15] applied particle swarm optimization (PSO) to search the most favorable pattern of node capacity allocation to improve the network robustness with minimum cost. Motivated by their works, in this paper, we apply a specific PSO algorithm to optimize the node resource allocation for improving the network robustness in scale-free networks. It is found that assigning less resource to middle-degree nodes under small-scale attack while more resource to low-degree nodes under large-scale attack is helpful for improving the network robustness.

The paper is organized as follows. In Section 2 we describe the network model as well as the optimization model in detail. In Section 3, the specific PSO algorithm is presented. Section 4 shows the simulation results and the corresponding analysis. The work is summarized in Section 5.

2. Model

2.1. Network model

Many real-world networks, such as the World-Wide Web, communication networks and airline networks, are found to be with scale-free property [18–20]. Thus, we adopt the well-known Barábasi–Albert (BA) [21] model to build the scale-free network. The BA model starts with a small number (m_0) of completely connected vertices, and at every time step a new vertex is added with $m(\leq m_0)$ edges that link the new vertex to m different vertices already present in the network. In the following, the BA model are set to $m_0 = m = 2$. And we assume that the BA network is undirected and unweighted network.

To resist external attacks, each node i in the network is assigned some defense resource r_i. And the resource allocation of the network can be represented as $\vec{r} = (r_1, r_2, \ldots, r_N)$. To mimic the fact that the defense resource of each node may be heterogeneous due to the various practical properties, the resource allocation can be modeled as $r_i = k_i^{\alpha}$, where α is a tunable parameter. Here $\alpha = 0$ corresponds to the uniform allocation; $\alpha = 1$ corresponds to the allocation proportional to node's degree; and $\alpha = 1.6$ corresponds to the allocation proportional to node's betweenness based on the results of betweenness centrality shown in previous studies [22–24].

2.2. Node removal strategies and network robustness measure

From previous studies, there are three common node removal strategies to the network, namely Random removal strategy (RRS), High-degree removal strategy (HDRS) and Low-degree removal strategy (LDRS) [13].

Random removal strategy. As to the system random malfunction, every node in the network has the same probability with failure, and the nodes are removed randomly.

High-degree removal strategy. As to the malicious attack in the center, high-degree nodes are more inclined to be attacked, and the nodes are removed with the descending order of nodes' degrees.

Low-degree removal strategy. As to the attack from periphery to the center, low-degree nodes are attacked at first, and the nodes are removed with the ascending order of nodes' degrees.

The total cost an attacker has to pay is defined as the proportion

$$\rho = \frac{\sum_{m \in V} r_m}{\sum_{i=1}^{N} r_i} \tag{1}$$

Please cite this article in press as: X. Zhang, et al., Optimal defense resource allocation in scale-free networks, Physica A (2017), https://doi.org/10.1016/j.physa.2017.11.135.