Physica A 503 (2018) 1041–1053

Contents lists available at ScienceDirect

Physica A

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

A memetic algorithm for determining the nodal attacks with minimum cost on complex networks

Zhirou Yang, Jing Liu [*]

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

HIGHLIGHTS

- Practical attacks make networks fragmented rather than make each node isolated.
- An attack model considering the cost of attacking nodes is designed accordingly.
- A memetic algorithm MA-NA$_C$ is proposed to find the relatively low attack cost.
- The good performance of MA-NA$_C$ is validated on various networks.

ARTICLE INFO

Article history:
Received 17 August 2017
Received in revised form 16 March 2018
Available online xxxx

Keywords:
Attack cost
Nodal attack
Scale-free network
Complex network
Network robustness

ABSTRACT

Many real-world networks are exposed in complicated environments and may be destroyed easily by various kinds of attacks and errors. With no doubt it is of great significance to promote the anti-attack ability of systems. Besides, analyzing attack models is also of significance. The existing studies about network robustness conducted on weighted or unweighted networks have drawn the conclusion that scale-free networks are fragile under malicious attacks, where the precondition is that the cost of removing a node is equal. In fact, the cost of attacking different nodes is far from equal, thus, the removal cost should be taken into consideration when conducting attacks. In this paper, a malicious attack model considering the cost of attacking nodes, termed as Nodal Attack with Cost (NA$_C$), is first proposed to depict the tolerance of networks. Furthermore, the limitation of resources drives us to design an optimization algorithm based on memetic algorithm (MA), termed as MA-NA$_C$, to search for the optimal combination of nodes with the minimum cost which can destroy networks to the desired degree. The experimental results show that networks perform robust under the high degree adaptive (HDA) attack when there is a great difference between hub nodes and leaf nodes in the attack cost, yet the results are similar to previous studies on the condition that the attack cost gap is minor. In addition, MA-NA$_C$ is efficient in finding a relatively small attack cost. Based on the study of cost-optimized network structure and features of attacked nodes obtained by MA-NA$_C$, we find that MA-NA$_C$ selects the target nodes by taking into account their effect on network structure, which contributes to the good optimization ability of MA-NA$_C$.

[*] Corresponding author.
E-mail address: neouma@163.com (J. Liu).
URL: http://see.xidian.edu.cn/faculty/liujing (J. Liu).

https://doi.org/10.1016/j.physa.2018.08.132
0378-4371/© 2018 Elsevier B.V. All rights reserved.

1. Introduction

Many modern systems with different topologies in real life can be modeled as complex networks, such as water supplying systems, power grids, air transportation systems and World Wide Web [1–6]. Moreover, these networked systems are often exposed to intentional or unpredictable attacks, which may trigger great losses [7–9]. Therefore, improving the tolerance of networks to attacks on nodes and links, namely network robustness, is crucial. Over the last two decades, many existing researches have focused on designing robustness measures [10–12], analyzing the variation of network structure [10–13], presenting various types of attacks [10–14], and promoting network robustness [10–12,15–17]. Guided by robustness measures, the capacity of networks in defending attacks can be effectively enhanced by topological rewiring. Besides promoting robustness, the studies on analyzing attacks are also of immense significance. Modeling and simulating various kinds of attacks could help us find out their characteristics, which contributes to designing defense mechanisms and enhancing the robustness of networked systems.

Generally, the breakdown of nodes or links can be conducted randomly or maliciously. Nodes or links are removed with the same probability when conducting the former one, while the later one usually follows regularity and sequence, in which the nodes or links are removed according to their importance in systems. There are several kinds of importance measures, such as degree [10], clustering coefficient [11], betweenness [18], and eigenvector centrality [19]. The malicious attacks are quite harmful to some real facilities, which make the systems fall apart quickly. One of the most widely used attacks is the high degree adaptive attack (HDA) proposed by Schneider et al. [10], in which the importance of a node is measured by its degree. Therefore, the node with the highest degree is removed from the network first. Because scale-free (SF) networks are sensitive and vulnerable to malicious attacks, this kind of attacks is considered to be the most efficient destruction in previous studies.

In reality, the destroyers may not attack infrastructures by following the rules that remove the nodes sequentially based only on their degrees. They may take the effect of nodes on the network structure together with the required cost to conduct attacks into consideration simultaneously. For different kinds of networks, the role of important nodes on the structure is different. In the network with communities, the nodes with the highest degree are usually located in the inner of community. But in some circumstances, such as to separate these communities, cutting down the communication between communities is more effective. In other words, to adapt to different situations, adjusting the attack strategy is necessary.

It is generally agreed that tighter connection takes more cost to break [20,21], yet the cost of attacking different nodes in networks is equal. Actually, the facts seem to suggest this is not always the case; that is, it needs to take more cost to remove a hub node than a leaf node caused by larger link density. One example here can demonstrate the point. The importance of main engines or servers is different in the Internet. It is generally accepted that the public server is more important, such as the server of large-scale website, linking tens of thousands of other main engines and servers and carrying more confidential information. This kind of servers with high degree is amid tight security, including firewall and antivirus. However, for general users, their servers are of low importance and make few connections with others. Because lacking the funds and technology, these servers are under simple protection, or even no protection. Therefore, attacking public server may cause widespread influence, yet multi-connection makes it difficult in destruction. Oppositely, the destruction of unimportant server takes low cost, yet with little impact. Accordingly, multi-connected nodes may play an important role in network topology, but removing a node with high degree is at a costly price. Given limited resources, such as time, budgetary, human or material, we need to find a way to balance resources and attack effect in most realistic cases.

Learned from several nodal robustness measures, the process of attacking may not stop until the network completely collapses [10–12]. In the real world, once the main structure of modern facilities is broken, the system is supposed to be unworkable, which means it is unnecessary to make the whole networked system be completely knocked down. Redundant attacks are time-consuming and cost-consuming, which ought to be avoided. In fact, the process of removing nodes sequentially in HDA is a greedy way to find a set of nodes to attack, in which the node with the highest degree is selected in each step. Although this method would make serious damage to networks, the cost to perform this task may be enormous. Limited resources require us spend less cost to achieve the desired damage. Therefore, when we consider the objective of minimizing the attack cost, the HDA may not be the most malicious method to destruct networks. The examples are shown in the next section to confirm the viewpoint that the HDA is a kind of superfluous and costly attacks.

In this paper, we take the effect of nodes on the network structure and the attack cost into consideration synthetically. Therefore, we propose a new kind of malicious attack, named as Nodal Attack with Cost (NA_C), which can reach the desired damage on networks with the minimum cost. In addition, considering finding the minimum cost is an optimization problem guided by the degree of nodes being attacked, we redesign the objective function and use memetic algorithm (MA) with efficient improvements, named as MA-NA_C, to obtain a better solution. In the experiments, both synthetic and real-world networks are tested. We find that when attacking hub nodes versus leaf nodes makes a very large difference, the HDA is not the most malicious attack strategy. But if there is little difference in terms of attack cost between hub nodes and leaf nodes, the attack strategy of HDA is still advisable. In addition, MA-NA_C shows a good performance in getting less attack cost by removing a few important nodes instead of some unimportant nodes. Through further analyzing on the characteristics of network structure suffered from different attacks and the attacked nodes obtained by MA-NA_C, we can draw the conclusion that MA-NA_C can take the role of nodes in the topological structure and the attack cost into consideration simultaneously, promoting the attack efficiency to some extent. Moreover, we discuss the relation between attack cost and scaling exponent