Physica A 501 (2018) 42–51

Contents lists available at ScienceDirect

Physica A

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

Optimization of cascading failure on complex network based on NNIA

Qian Zhu [a,b,*], Zhiliang Zhu [a], Yi Qi [a], Hai Yu [a], Yanjie Xu [a]

[a] *Software College, Northeastern University, Shenyang 110169, China*
[b] *School of Computer Science and Engineering, Northeastern University, Shenyang 110169, China*

HIGHLIGHTS

- We concentrate on how to improve the robustness of the networks from the perspective of intelligent optimization.
- Two multi-objective optimization models are established.
- The NNIA (Non-dominated Neighbor Immune Algorithm) is applied to solve the optimization models.
- We find the edges that can facilitate the propagation of cascading failure and the edges that can suppress the propagation of cascading failure.

ARTICLE INFO

Article history:
Received 27 October 2017
Received in revised form 29 December 2017
Available online 15 March 2018

Keywords:
Cascading failure
NNIA
The optimization of the network
Robustness

ABSTRACT

Recently, the robustness of networks under cascading failure has attracted extensive attention. Different from previous studies, we concentrate on how to improve the robustness of the networks from the perspective of intelligent optimization. We establish two multi-objective optimization models that comprehensively consider the operational cost of the edges in the networks and the robustness of the networks. The NNIA (Non-dominated Neighbor Immune Algorithm) is applied to solve the optimization models. We finished simulations of the Barabási–Albert (BA) network and Erdös–Rényi (ER) network. In the solutions, we find the edges that can facilitate the propagation of cascading failure and the edges that can suppress the propagation of cascading failure. From the conclusions, we take optimal protection measures to weaken the damage caused by cascading failures. We also consider actual situations of operational cost feasibility of the edges. People can make a more practical choice based on the operational cost. Our work will be helpful in the design of highly robust networks or improvement of the robustness of networks in the future.

1. Introduction

In our daily life, many key infrastructure networks such as communication networks, power networks, transport networks, and the Internet often have large cascading failures. The collapse of an entire network due to attacks or failure of certain key nodes in the network can seriously affects the daily life of people. For example, the major blackout accident in India in July 2012 [1], the crash of the China Southern Power Grid in January 2008 [2], or the global Internet failure on January 21, 2014. If large-scale cascading failures occur, they have devastating influence on the entire network. Timely, accurate and targeted response is the key to control the spread of disasters and reduce economic losses when coping

* Corresponding author.
E-mail address: zhuq@mail.neu.edu.cn (Q. Zhu).

https://doi.org/10.1016/j.physa.2018.02.138
0378-4371/

with infrastructure network disasters initiated by cascading failures; it is also the key to the management of infrastructure networks.

Complex network theory is a very powerful tool for evaluating and improving infrastructure networks. The robustness of a network is largely related to the topology of the network. Recently, many scholars have proposed more general models for cascading failures of complex networks [3–7]; these models are progressively better at showing cascading failures on actual networks from different perspectives. A number of valuable prevention and control strategies are proposed based on these models.

Among them, the research of Motter et al. showed that if the betweenness centrality or degree of the networks is more homogeneous, the networks are more robust. The effective way to prevent networks from cascading failures is to protect nodes with larger betweenness centrality and nodes with larger degree or to make the load distribution on the networks more uniform [3]. This research inspired many researchers to study the prevention and control strategies of complex network cascading failures. Motter et al. [8] proposed that after a scale-free network suffered intentional attack, the cascading failures can be controlled by removing a portion of the nodes with low load or edges with high load in advance. Based on this idea of changing network topology, some researchers have further studied how to effectively control cascading failures [9–12]. Modifications of network topology include adding edges, removing edges, reconnecting edges, and so on.

In these studies, the rules to change the network topology were often designed and the effectiveness of the rules were verified by simulations. There is another way to improve the network robustness, which is to optimize the maximum capacity of the networks [13,14]. Many of these studies designed initial loads according to topological characteristics of the nodes, such as betweenness centrality and degree, and the initial load is multiplied by a redundancy factor to get the node capacity. On this basis, we need to design a number of strategies to allocate node capacity in a more rational way that can enhance the robustness of the networks. The spread of cascading failures can be better controlled by designing a better global or local routing strategy [15–17]. Wang Jian et al. [17] constructed cascading failure models on the Internet network by introducing the congestion function of nodes. They consider the effects on the cascading spread caused by the shortest path routing strategy and the extent of congestion of all the nodes on the paths. Safe and efficient cascade-oriented routing strategies are designed to ensure the relative security of the networks.

This paper studies the improvement of network robustness from the perspective of network topology. Different from previous research, this paper proceeds from the aspect of intelligent optimization and establishes two multi-objective combination optimization problems based on network robustness and the operational cost of connecting the network edges. These two operational problems are used to determine the two types of edge sets that facilitate or suppress the spread of cascading failures in the networks. At present, there are many methods of solving the multi-objective optimization problem. The typical cases are: bare-bones multi-objective particle swarm optimization algorithm [18–20], the particle swarm optimization (PSO) is a heuristic search technique that is inspired by the behavior of bird flocks, the concept of bare-bones particle swarm optimization (BBPSO) was used in some early literatures to deal with the single-objective problems. Afterwards, people extend the idea of the BBPSO to solve the multi-objective optimization problems; multi-objective differential evolution algorithm [21], Evolutionary algorithm is a method of simulating natural selection and natural adaptation. It is commonly used in solving a high dimensional, dynamic, complex, multi-objective optimization problem; Multi-Objective Immune Algorithm [22], etc. Multi-Objective Immune Algorithm is an intelligent method to imitate the function of a natural immune system. It learns from the function, principle and model of a biological immune system and is improved from the evolutionary algorithm. Luh et al. [22] proposed a Multi-Objective Immune Algorithm (MOIA) and then proposed a Constrained Multi-Objective Immune Algorithm (CMOIA). MOIA is a complex algorithm with a strong biological background, which utilizes biological theories and models including the clonal selection theory, the establishment of DNA libraries, and the difference between heavy and light protein chains in antibodies and other immune models. Lu et al. [23] proposed an Immune Forgetting Multi-Objective Optimization Algorithm (IFMOA) based on the dynamic process of immune response and the clonal selection theory. This algorithm combines antigen and antibody affinity assignments based on Pareto intensity, clonal selection operation and a method of simulating immune tolerance processes.

Chen et al. [24] used the clonal selection and immune network theory to design a Population-Based Adaptive Immune Algorithm (PAIA), in which the population size and clone scale were adaptively adjusted by the searching process and the problems. Based on the concept of immune domination and the clonal selection theory, the Jiao Licheng research group proposed the Immune Domination Clone Multi-Objective Algorithm (IDCMA [25]) and the Nondominated Neighbor Immune Algorithm (NNIA [26]). Among these immune multi-objective algorithms, NNIA is more representative and simulates the phenomenon of diverse antibody symbiosis and minority antibody activation in immune response. By using the individual selection method of nondominated neighborhood and cloning proportionally according to the degree of crowding, this algorithm can obtain an evenly distributed Pareto optimal solution with low computational complexity, which is a very effective multi-objective algorithm. Multi-objective immune optimization algorithms are used to optimize the established multi-objective problems in the model. On this basis, we take the best protective measures to reduce the network damage caused by cascading failures. Simulations are carried out on two kinds of network topology, the BA network and the ER network.