Chaos, Solitons and Fractals 106 (2018) 61–66

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

Multi-node attack strategy of complex networks due to cascading breakdown

Fu Chaoqi[*], Wang Ying, Wang Xiaoyang, Gao Yangjun

Equipment Management and Safety Engineering College, Air Force Engineering University, Xi'an 710038, China

ARTICLE INFO

Article history:
Received 8 January 2017
Revised 27 August 2017
Accepted 7 November 2017

Keywords:
Cascading failure
Multi-node attack
Average avalanche scale
Tolerance coefficient

ABSTRACT

Studying attack strategy of complex networks is the basis of investigating network characteristics such as robustness, invulnerability, and network security. Knowing means of attack can help us take more effective measures to ensure network security. Presently, most research conclusions focus on a single vertex being attacked, and the choice of a set of attack nodes is also limited to a complete understanding of network information. In this paper, considering the effect of cascading failure, we focus on the multi-node attack strategy. Our results showed that the distance between attack targets has a great effect on the attacking effect. Taking both the average avalanche scale and maximum destruction size into account, when the distance between attack targets was 2, the network suffered the most serious damage. If the information about the network was unclear, we presented 3 kinds of conditional attack strategies. Under the condition of different tolerance coefficients and different degrees of known information, each strategy had its own unique advantages. In conclusion, the research in this paper supports the easy and quick selection of attack targets under the condition of incomplete information.

1. Introduction

Complex networks arise in natural systems and are an essential part of modern society. They have caught the attention of many scholars [1], and seen specific application in many fields, such as the sociology of information dissemination, spreading of rumors [2,3], the biology of virus infection [4,5], interactions between proteins [6], urban subway planning, and reasonable partitioning of bus systems [7,8]. Complex networks can abstract components in complex systems into corresponding nodes and edges, which express the relationship between nodes, and then we can study optimal network design [9,10] and network security issues [11,12] through topological structure [13] and network dynamics. If we want to ensure network security and reliability, first of all, we must clearly understand how the network may be attacked. Since different network structures may have different results under different means of attack [14], we can allocate limited resources to where it is most needed by understanding how the networks will fail. Originating from studies of complex networks vulnerability, Albert et al. [15] was the first to pay close attention to the relationship between topological network structure and network invulnerability. Until now, there were 3 main kinds of attack modes: (1) Random attack, where nothing about the network is known, and we do not have the ability to distinguish which nodes or edges are more important; therefore, each node has the same probability of being attacked. (2) Intentional attack, where we fully understand the network and can choose the most important nodes or edges to remove (which may otherwise cause great damage). The research of Holme et al. [16] was relatively comprehensive, as they divided attack strategies into 4 types by defining the following strategies: removals by descending order of link degrees and betweenness centrality, calculated for either the initial network or current network during the removal procedure. Results showed that removals by the recalculated degrees and betweenness centrality were often more harmful. In the study of vital nodes identification [17], vital nodes identified by connection-sensitive [18] and stability-sensitive [19] criteria also provided an idea for the selection of attack targets, and a better attack effect was usually obtained. (3) Conditional attack, of which random and intentional attacks are 2 extreme cases and are rare in reality, means that one can preferentially attack only the most important vertex (edge) among a local region of a network. Gallos et al. [20] studied the stability and topology of scale-free networks under attack and defense strategies, they regard incomplete information as uncertain information, which meaning that one can obtain the information of all nodes but that information may be uncertain. Wu et al. [21] obtained attack information using probability sampling without return, with indicators α and β to describe the attack information.

The aforementioned attack strategies are limited to static network and do not consider network breakdown caused by cascad-

[*] Corresponding author.

https://doi.org/10.1016/j.chaos.2017.11.009
0960-0779/© 2017 Elsevier Ltd. All rights reserved.

ing failure [22–24], such as the power network failure in southern China in 2008, Internet congestion, the pipeline explosion in Qingdao, and so on. These accidents have shown that a small initial attack or failure has the potential to trigger a global cascade. In 2002, Motter and Lai [25] established a linear model about capacity and initial load (ML model). Since then, some scholars further presented varieties of a nonlinear load-capacity model [26,27]. Chen et al. [28] proposed a local-capacity optimal relationship model, where they defined node redundant capacity as a maximum redistribution load from a single neighbor failure node. Additionally, Wang [29] proposed a partial protection strategy, where the vertex could invoke redundant capacity from its neighbor nodes to share a redistribution load and greatly reduce the capacity threshold. The best network structure and optimal parameter configurations aimed at reducing the impact of cascading failure addresses failure caused by a single vertex under attack [22–30]. However, in real life, there are often multiple nodes under attack simultaneously. In this case, what kind of network design is more stable? Precise knowledge of self and precise knowledge of the threat leads to victory. Till far, many studies have investigated the influence maximization problem (IMP) [17], where a set of vital nodes could be determined as causing the greatest damage, no matter determined by the topology, mechanisms, or dynamical processes [31,32]. Many advanced algorithms have also been proposed to find the most influential group of nodes, such as greedy algorithms [32] and heuristic algorithms [33]. However, the realization of these methods has a basic premise: since the network is completely known, especially for the algorithm, they test one by one to find the best combination. Hu et al. [34] have demonstrated a very fundamental and exciting result, that is, a node's or a group of nodes' global influence can be exactly measured by using purely local network information. However, the local network information is specially selected from the global information, there are strict limits on connectivity and component size. As the enemy, we can usually obtain only part of the network information, even the known structure of network is disconnected. If we cannot accurately calculate the impact of the removal of nodes on the network, perhaps we can narrow down the range of options with some characteristics. For example, whether the destruction of a focused attack is more serious than a dispersed attack? Therefore, through considering such issues, in this paper we studied cascading failure caused by multi-node attack. We aimed to find some rules that could aid us in limited information conditions when determining the targets that could cause more serious damage. We hope that our study of multi-node attack strategy can be helpful to network security.

The remainder of this paper is organized as follows: in Section 2, we study the characteristics of multi-node attack, and determine the impact of distance between attack targets; in Section 3 we propose 3 kinds of attack strategies under incomplete network information, and conduct analysis of application scopes; finally, some summaries and conclusions are presented in Section 4.

2. Characteristics of multi-node attack

2.1. Modeling and parameter selection

The classical load-capacity model was established by Motter and Lai in 2002 [25], but it is difficult to apply to large-scale networks due to the large amount of calculations. Wang et al. [30] defined a new model, where the initial load of the node i is correlated with its link degree k as $L_i = k_i^{\theta}$, the load-capacity linear model is $C_i = T \times L_i$, and the expression of load local preferential redistribution rule is as follows:

$$\Delta L_{ij} = L_i \frac{L_j}{\sum\limits_{n\in\Gamma_i} L_n}, \tag{1}$$

where Γ_i is set of nodes adjacent to failure node i, θ is the load parameter, and T is the tolerance coefficient.

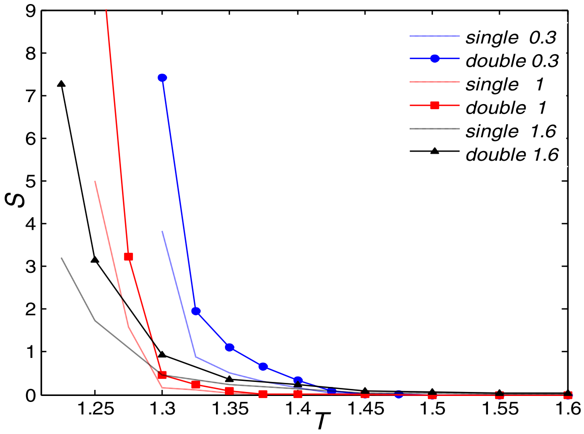

Fig. 1. Average avalanche scale as a function of tolerance coefficient for several values of θon BA scale-free networks, under the condition of single vertex removal (dotted line) and two nodes removal (solid line). Each curve was obtained by averaging over experiments on 20 independent networks.

Tolerance coefficient determines whether there is a cascading failure phenomenon, which can be completely avoided when T is sufficiently large. However, in reality, T is limited by cost constraints, and much work has been done to prove the case that, with a load coefficient $\theta = 1$, the network has the strongest robustness under the same T when only a single vertex is attacked [30]. Therefore, we are interested in whether there is a similar phenomenon under the condition of multi-node attack. Here, we simulated the case that only two nodes were initial failure nodes, and built a BA scale-free network [35] with total number of nodes $N = 1000$ and average connectivity degree $\langle k \rangle \approx 4$. We initially deactivated two nodes simultaneously and calculated avalanche sizes S_i, which is the total number of broken nodes induced by initial failure nodes after cascading failure. We adopted the average avalanche scale $S = \sum\limits_{i=1}^{M} S_i / M$, obtained via summation over all avalanche sizes, by deactivating a couple of nodes at each time, divided by the total number of couples $M = C_N^2$. According to the attack types, we obtained 6 curves with increasing T and under the situations of $\theta = 0.3$, $\theta = 1$, and θ=1.6.

Fig. 1 shows that multi-node attack had the same trend as when a single vertex was attacked, and when $\theta = 1$, the network had the strongest robustness against cascading failure. To clarify this observed phenomenon, we now provide some theoretical analysis. If a set of nodes fails simultaneously, and no cascading failure occurs, the following condition should be satisfied:

$$\Delta L_{il} + \cdots + \Delta L_{jl} + L_l < C_l, \tag{2}$$

where node i and j are the failure nodes, and node l is the object that impacted by redistribution load.

According to the attack mode, the analysis is divided into 2 different situations:

(1) Focused attack (the distance among initial failure nodes satisfies $d = 1$). The adjacent nodes suffer from the redistribution load of multiple failure nodes.

Assuming that the number of initial failure nodes is q, node l inherits the redistribution load. Combining Eqs. (1) and (2),