Physica A 408 (2014) 134–148

Contents lists available at ScienceDirect

Physica A

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

Damage attack on complex networks

Hui Wang [a], Jinyuan Huang [b], Xiaomin Xu [c], Yanghua Xiao [c,*]

[a] School of Economics and Management, Shanghai University of Electric Power, Shanghai 200090, PR China
[b] School of Management, University of Shanghai for Science of Technology, Shanghai 200090, PR China
[c] School of Computer Science, Fudan University, Shanghai 200433, PR China

HIGHLIGHTS

- Damage characterizes the vertex importance to maintain the integrity of a network.
- In damage attack adversaries select the vertex causing the most damage to attack.
- We systematically investigated a new attack model: damage attack.
- Damage attack is more destructive than degree attack.

ARTICLE INFO

Article history:
Received 18 February 2014
Received in revised form 25 March 2014
Available online 13 April 2014

Keywords:
Complex network
Damage attack
Degree attack
Network robustness

ABSTRACT

Behaviors of complex networks under intentional *attacks guided by degree* (degree attack) have been extensively studied. However, little is known about the behaviors of these networks under intentional *attacks guided by damage* (damage attack), in which adversaries choose the vertex with the largest damage to attack. In this article, we systematically investigate damage attack and behaviors of real networks as well as synthetic networks against damage attack. Empirical study shows that for real networks in a wide range of domains there exists a critical-point before which damage attack is more destructive than degree attack. This is further explained by the fact that degree attack tends to produce networks with more heterogeneous damage distribution than damage attack. Results in this article strongly suggest that damage attack is one of the most destructive attacks and deserves additional study. Our understanding about damage attack may also shed light on efficient solutions to protect real networks against damage attack.

1. Introduction

In the last decade, there has been a large effort dedicated to research on the resilience of real-world networks or synthetic networks against random failures or intentional attacks [1–15]. Random failure can be considered as a special case of intentional attack when no information of vertex importance in the sense of maintaining the integrity of the network is available to an adversary. If certain structural information of the network is available, a rational adversary tends to select the most important vertices to attack, maximizing the destructive effect. Usually, the attack continues step by step until the adversary believes that the desired destructive objective is achieved. Thus, from an adversary's perspective, ranking the importance of vertices in the network is one of the fundamental steps towards destroying the network.

A real network can be precisely modeled as a graph $G(V, E)$, where V represents the entities in the network and E represents relations among these entities. A variety of measurements are available to rank the vertex importance in a graph.

* Corresponding author.
E-mail address: shawyh@fudan.edu.cn (Y. Xiao).

http://dx.doi.org/10.1016/j.physa.2014.04.001
0378-4371/

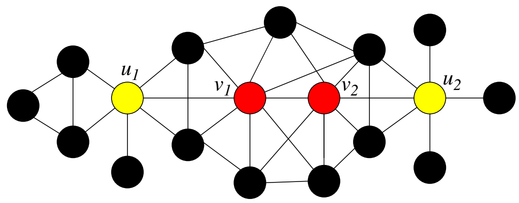

Fig. 1. (Color online) Damage attack on a hypothetical network. u_1 and u_2 are the top two of the largest damages, which are 4 and 3, respectively. v_1 and v_2 are the top two of the largest degrees, which are 8 and 7, respectively.

Among them, *degree* and *betweenness*, have been widely investigated in previous studies about network robustness [10,6]. Degree quantifies the number of connections to a vertex. Because vertices with a large degree dominate the connections of the whole network they are commonly regarded as the most important to maintaining network integrity. Betweenness counts the fraction of shortest paths going through a given vertex. Hence, vertices with high betweenness are important in maintaining the communication functionality of the network [16–18].

Aside from betweenness and degree, little research into other methods of characterizing vertex importance is found in the literature. One promising method is *damage*, which characterizes the damage caused by the removal of a vertex and usually is quantified as the decrease of the largest component size when the vertex and its incident edges are removed. Intuitively, a vertex causing larger damage leads to more destructive effect on the network performance. Damage plays a vital role in characterizing the essentiality of components in biological networks. Vertices (proteins or enzymes) that cause large damage are essential or important in protein interaction networks or metabolic networks [19,20].

When the destructive effect is measured by damage, damage attack is more destructive by definition than any other attack. An example is shown in Fig. 1, where vertex u_1 has the largest damage value 5. The removal of u_1 isolates itself and four other vertices from the major component. In contrast, if we remove the vertex with the largest degree, i.e., vertex v_1, v_1 will be the only vertex isolated from the major component. This example shows that *attack guided by damage* or simply *damage attack* (attacking the vertex with the largest damage) yields a non-trivial destructive effect.

Despite its destructive effect, the fundamental characteristics of damage attack and the response of real networks as well as synthetic networks to damage attack have been rarely studied. In this article, we systematically investigate damage attack and the performance of real networks and synthetic networks including Barabasi–Albert (BA) [21] networks and Erdös–Rény (ER) [22] networks against damage attack. Attack guided by degree is investigated as a comparison.

The structure of the remainder of the paper is as follows. In Section 2, we systematically investigate statistical properties about damage, damage distribution, correlation between damage and degree. In Section 3, we present the empirical results about the behaviors of real networks and synthetic networks against damage attack. Additionally we compare these results to degree attack and show that *there exists a cross point before which damage attack is more destructive than degree attack*. In Section 4, these results are further explicated. Finally, in Section 5, we briefly summarize major findings and results of this article. We also give in Appendix section the key concepts of intentional attack on complex networks and previous attacking model. Readers may refer to this section for background knowledge.

2. Damage of networks

In general, the network functionality can be measured by different mechanisms (Please refer to Appendix for more information). One of them is the size (usually vertex number) of the largest connected component in a network, denoted by $S_{\max}$. If the network functionality is measured by $S_{\max}$, then the most destructive approach is removing vertices one by one in the descending order of damage value. In this section, we will systematically revisit vertex damage for real networks and synthetic networks.

2.1. Damage of graphs

Let $G(V, E)$ be an undirected graph (not necessarily a connected graph). The damage of a vertex $v \in V$, $D(v)$ is defined as $S_{\max} - S'_{\max}$, where $S_{\max}$ and $S'_{\max}$ are the largest connected component sizes before removing v and after removing v, respectively. For a vertex v in a connected graph, its damage $D(v)$ lies in the range $[1, N-1]$ [23]. $D(v)$ is 1 when the induced subgraph of $V - \{v\}$ is a connected component. $D(v) = N - 1$ when v is the central vertex of a *star-like network* (that is the graph with $N-1$ vertices of degree 1 being connected to a central vertex of degree $N-1$). If the degree of v, $d(v)$, is given, a tighter upper bound of $D(v)$ can be given by:

$$N - \frac{N}{d(v)} = N\left(1 - \frac{1}{d(v)}\right). \quad (1)$$

The upper bound is reachable when v connects to $d(v)$ clusters that have the same size and have no connections among each other. Since damage is computed in linear time (i.e., $O(M)$), it can also be used by adversaries as a lightweight ranking.