Physica A 414 (2014) 174–180

Contents lists available at ScienceDirect

Physica A

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

Efficiency of attack strategies on complex model and real-world networks

Michele Bellingeri [a,*], Davide Cassi [a], Simone Vincenzi [b,c]

[a] Dipartimento di Fisica, Università di Parma, via G.P. Usberti, 7/a, 43124 Parma, Italy

[b] Center for Stock Assessment Research (CSTAR) and Department of Applied Mathematics and Statistics, University of California Santa Cruz, 110 Shaffer Road, 95060 Santa Cruz, CA, United States

[c] Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Via Ponzio 34/5, I-20133 Milan, Italy

HIGHLIGHTS

- We investigated the efficiency of network attack strategies.
- We used the size of the largest connected component as a damage measure.
- We tested 3 attack strategies introduced in this work for the first time.
- Deletion according to betweenness centrality was the most efficient attack strategy.

ARTICLE INFO

Article history:
Received 18 March 2014
Received in revised form 10 June 2014
Available online 18 July 2014

Keywords:
Network robustness
Attack strategies
Immunization strategies

ABSTRACT

We investigated the efficiency of attack strategies to network nodes when targeting several complex model and real-world networks. We tested 5 attack strategies, 3 of which were introduced in this work for the first time, to attack 3 model networks (Erdos and Renyi, Barabasi and Albert preferential attachment network, and scale-free network configuration models) and 3 real networks (Gnutella peer-to-peer network, email network of the University of Rovira i Virgili, and immunoglobulin interaction network). Nodes were removed sequentially according to the importance criterion defined by the attack strategy, and we used the size of the largest connected component (*LCC*) as a measure of network damage. We found that the efficiency of attack strategies (fraction of nodes to be deleted for a given reduction of *LCC* size) depends on the topology of the network, although attacks based on either the number of connections of a node or betweenness centrality were often the most efficient strategies. Sequential deletion of nodes in decreasing order of betweenness centrality was the most efficient attack strategy when targeting real-world networks. The relative efficiency of attack strategies often changed during the sequential removal of nodes, especially for networks with power-law degree distribution.

1. Introduction

The resilience of real-world complex networks, such as Internet, electrical power grids, airline routes, ecological and biological networks [1–6] to "node failure" (i.e. node malfunctioning or removal) is a topic of fundamental importance for both theoretical and applied network science. Node failure can cause the fragmentation of the network, which has consequences in terms of system performance, properties, and architecture, such as transportation properties, information delivery efficiency and the reachability of network components (i.e. ability to go from a node of the network to another) [3].

* Corresponding author. Tel.: +39 0521 905674.
E-mail address: michele.bellingeri@nemo.unipr.it (M. Bellingeri).

http://dx.doi.org/10.1016/j.physa.2014.06.079
0378-4371/

Several studies [3,7–9] have investigated the resilience of model networks using a number of "attack strategies", i.e. a sequence of node removal according to certain properties of the nodes [2,3,7]. A widely applied attack strategy consists in first ranking the nodes with respect to an importance criterion (e.g. number of connections or some measure of centrality) and then removing the nodes sequentially from the most to the least important according to the chosen criterion until the network either becomes disconnected or loses some essential qualities [3,10]. However, little is known on how the efficiency of attack strategies (i.e. the fraction of nodes to be deleted for a given change in the network) varies when considering different real-world and model networks.

In this context, an underappreciated problem is how the relative efficiency of attack strategies may change during the attack to the network. For example, an attack strategy might be more efficient when the targeted (i.e. under attack) network is still pristine, while other strategies may be more efficient when the network has already been fragmented and some of its properties have been compromised. Testing the efficiency of the different attack strategies when targeting different networks may also allow us to identify the most important nodes for network functioning, and therefore which nodes should be primarily protected, as in the case of computer [11] or ecological networks [6,12–14], or removed, as in the case of immunization/disease networks [15].

In this work, we test the efficiency of both well-known attack strategies and new strategies introduced for the first time in this paper when targeting either model or real-world networks. We used the size of the largest connected component (*LCC*) (i.e. the largest number of nodes connected among them in the network, [2]) as a measure of network damage. We found for model networks that the best strategy to reduce the size of the *LCC* depended on the topology of the network that was attacked. For real-world networks, the removal of nodes using betweenness centrality as importance criterion was consistently the most efficient attack strategy. For some networks, we found that an attack strategy can be more efficient than others up to a certain fraction of nodes removed, but other attack strategies can become more efficient after that fraction of nodes has been removed.

2. Methods

2.1. Attack strategies

We attacked the networks by sequentially removing nodes following some importance criteria. We compared the efficiency of a pool of attack strategies, some of which have already been described in the literature while others are introduced in this work for the first time.

Most of the analyses on the robustness of network have investigated the effect of removing nodes according to their rank (i.e. number of links of the node) or some measures of centrality [3,10,16]. In this work, we introduce new attack strategies that focus entirely or in part on less local properties of a node, in particular its number of second neighbors, as explained in detail below.

Several indexes and measures have been proposed in order to describe network damage. We use the size of the largest connected component (*LCC*), i.e. the size of the largest connected sub-graph in the network [2,3], as a measure of network damage during the attack, where a faster decrease in the size of the *LCC* indicates a more efficient attack strategy. In order to compare attack strategies across networks, we normalized *LCC* size at any point during the attack with respect to the starting *LCC* size, i.e. the number of nodes in the *LCC* before the attack.

For each attack strategy, we applied both the recalculated and non-recalculated methods. With the recalculated method, the property of the node relevant for the attack strategy (e.g. number of links) was recalculated after each node removal. On the other hand, when applying the non-recalculated method the property of the node was measured before the first node removal and was not updated during the sequential deletion of nodes. With q we indicate the fraction of nodes removed during the sequential removal of nodes. An attack strategy is less efficient than another when a higher q is needed to reduce the *LCC* to zero (or any other size).

In this work, we used 2 attack strategies that have already been described in the literature. *First-degree neighbors (First)*: nodes are sequentially removed according to the number of first neighbors of each node (i.e. node rank). In the case of ties (i.e. nodes with the same rank), the sequence of removal of nodes is randomly chosen. *Nodes betweenness centrality (Bet)*: nodes are sequentially removed according to their betweenness centrality, which is the number of shortest paths from all vertices to all others that pass through that node [3,17].

We introduced in the present work the following new attack strategies. *Second-degree neighbors (Sec)*: nodes are sequentially removed according to the number of second neighbors of each node. Second neighbors of node j are nodes that have a node in common with – but are not directly connected to – node j. *First + Second neighbors* ($F + S$): nodes are deleted according to the sum of first and second neighbors of each node. *Combined first and second degree* (*Comb*): nodes are removed according to their rank. In the case of ties, nodes are removed according to their second degree.

For all the degree-based strategies, nodes were sequentially removed from most to least connected. In the case of *Bet*, nodes were sequentially removed from higher to lower betweenness centrality. For each network described in Section 2.2, we tested the relative efficiency of the five attack strategies in reducing the LCC to zero. In addition, we tested whether the relative efficiency of attack strategies changed along the removal sequence, i.e. whether an attack strategy was less efficient than another at the beginning of the attack, but more efficient after a fraction q of nodes was removed.