Physica A 390 (2011) 4684–4691

Contents lists available at SciVerse ScienceDirect

Physica A

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

Rethinking failure and attack tolerance assessment in complex networks

Cinara G. Ghedini *, Carlos H.C. Ribeiro

Technological Institute of Aeronautics, Computer Science Division, São José dos Campos, SP, Brazil

ARTICLE INFO

Article history:
Received 30 April 2010
Received in revised form 1 May 2011
Available online 20 July 2011

Keywords:
Vulnerability in complex networks
Failure and attack tolerance
Network connectivity

ABSTRACT

Studies have revealed that real complex networks are inherently vulnerable to the loss of high centrality nodes. These nodes are crucial to maintaining the network connectivity and are identified by classical measures, such as degree and betweenness centralities. Despite its significance, an assessment based solely on this vulnerability premise is misleading for the interpretation of the real state of the network concerning connectivity. As a matter of fact, some networks may be in a state of imminent fragmentation before such a condition is fully characterized by an analysis targeted solely on the centrally positioned nodes. This work aims at showing that, in fact, it is basically the global network configuration that is responsible for network fragmentation, as it may allow many other lower centrality nodes to seriously damage the network connectivity.

© 2011 Elsevier B.V. All rights reserved.

1. Introduction

It is increasingly recognized that organizing principles operate in most real networks [1]. These networks form and evolve in an *ad hoc* manner, being naturally self-organizing and self-adaptive. Examples can be found in nature, such as in ecological food webs [2], *Escherichia coli* [3], and neuronal topologies in *Caenorhabditis Elegans* worms [4]. Such network structures may also serve as models for social [5,6] and technological networks, such as P2P, overlay, sensor, and communication networks [7–10].

Although real network formations are targeted to achieve specific goals in diverse contexts and applications, most networks in fact exhibit similar organizational principles [4,11,1,12]. In general, this implies similar topological properties. The best-known property is that, on average, pairs of nodes can be connected by short path lengths (the so-called *small-world phenomenon*) [11]. Another property is a high clustering coefficient, which means that there is a high likelihood of any two nodes with a common neighbor being connected. Moreover, the degree distribution of many real networks follows a power-law tail, which, in a simplified way, means that a few nodes have many connections. However, networks exhibiting uniform and exponential degree distributions have also been reported [13].

As these networks do not rely on any fixed or predefined infrastructure and are not supported by any central management, nodes are usually autonomous to leave or join the network, causing frequent changes in the network topology. Besides, topological changes can also be induced by node failure (e.g., in sensor networks). Despite such variability, these networks are often able to maintain their main topological properties. However, this is not necessarily the case when such topological variability is biased to nodes of high centrality that either leave or fail. In fact, attacks on high centrality nodes are frequently considered (e.g., in communication networks) as a means to seriously harm the network operation, for instance by increasing the average path length.

Several researchers have studied the impact that both failures and targeted attacks have on the network efficiency and connectivity [14,15]. This assessment has been made through simulations of node disconnections based on two main criteria: (a) at random, and (b) choosing the high centrality nodes, to mimic, respectively, failures and targeted attacks.

* Corresponding address: Instituto Tecnológico de Aeronáutica, Divisão de Ciência da Computação, Praça Mal. Eduardo Gomes, 50, 12228-900, São José dos Campos, SP, Brazil. Tel.: +55 12 3947 6887; fax: +55 12 3947 5989.
E-mail addresses: cinara@ita.br, cinarag@gmail.com (C.G. Ghedini), carlos@ita.br (C.H.C. Ribeiro).

0378-4371/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2011.07.006

Despite high centrality nodes playing a crucial role regarding network connectivity, we argue that an assessment considering only this aspect misinterprets the role of the actual network configuration as far as the possibility of disconnection is concerned. In fact, some networks may reveal an imminent state of disconnection before it is characterized through standard centrality measurements.

The imminent state of disconnection is related to the concept of *vulnerability* in several areas, from biology [16], sociology and ecology [17–19] to network engineering and computer science [20–22].

This paper aims at showing that, in general, the main feature that is responsible for network fragmentation is the global network configuration. In this sense, nodes of relatively low centrality can also seriously damage network connectivity.

The rest of the paper is organized as follows. A brief theoretical background is presented in Section 2. Section 3 states the problem addressed herein, namely the impact of topological changes induced by failures and attacks on network efficiency and connectivity, and the usual approach adopted to assess it. In Section 4, we explore another point of view concerning this problem, and show the results of experiments conducted to support the argument of the existence of a global state of imminent disconnection.

2. Background

Two major branches of research on complex networks are the development of methods for network analysis and for network modelling, as the combination of modelling and measurement tools provides a benchmark to simulate network dynamics and allows a targeted analysis. This section addresses the main analytical measures and network models which are of interest for the approach reported in this paper.

2.1. Measuring network properties

Regarding the topological properties of complex networks, both global and local characteristics are relevant. Global assessment is often performed – especially in settings where information transmission is at stake – by computing the average of the shortest distance between any two nodes in the network, the so-called characteristic path length L [11]:

$$L = \frac{1}{\frac{1}{2}n(n+1)} \sum_{i \geq j} d_{ij}, \tag{1}$$

where d_{ij} is the geodesic distance from vertex i to vertex j. The characteristic path length (L) indicates how far apart the nodes are from each other, in other words, how efficient a network is with respect to information dissemination through its elements.

However, L is not an appropriate metric to deal with disconnected networks. Lattora et al. [14,23] introduced the efficiency E, which measures how efficiently the nodes exchange information in a local or global scope, independently of whether the network is disconnected, weighted, or topological. Consider a graph G where d_{ij} is the smallest sum of the physical distances through every possible path between nodes i and j. The efficiency E_{ij} is inversely proportional to the shortest distance: $E_{ij} = \frac{1}{d_{ij}}$. If there is no path between them, the distance d_{ij} is $+\infty$, and therefore $E_{ij} = 0$. Thus, the global efficiency of a graph G may be defined as

$$\begin{aligned} E_{glob}(G) &= \frac{\sum_{i \neq j \in G} E_{ij}}{n(n-1)} \\ &= \frac{1}{n(n-1)} \sum_{i \neq j \in G} \frac{1}{d_{ij}}. \end{aligned} \tag{2}$$

Notice that E_{glob} range is $[0, \infty]$. To normalize it, consider the ideal case G_{ideal} where all the possible $n(n-1)/2$ edges are in the graph; this is the case when E_{glob} assumes its maximum value. The normalized efficiency is then defined as $\frac{E_{glob}(G)}{E_{glob}(G_{ideal})}$.

The same idea can be extended to estimate the local efficiency (3). A local perspective provides mechanisms to quantify the existence of tightly linked subgraphs and may express the structure of the cluster a given node takes part in. The average over all network nodes represents the cohesion of the nodes (4):

$$E_{loc}(G) = \frac{1}{n} \sum_{i \in G} E(G_i) \tag{3}$$

where

$$E(G_i) = \frac{1}{k_i(k_i-1)} \sum_{l \neq m \in G_i} \frac{1}{d_{lm}} \tag{4}$$

and G_i is the subgraph containing all nodes directly connected to i (k_i is its degree). If the nearest neighborhood of i was part of a clique, there would be $k_i(k_1 - 1)/2$ edges among them [1].

Download English Version:

https://daneshyari.com/en/article/7383160

Download Persian Version:

https://daneshyari.com/article/7383160

Daneshyari.com