# Multiscale vulnerability of complex networks

Stefano Boccaletti
*Embassy of Italy in Tel Aviv, 25 Hamered Street, 68125 Tel Aviv, Israel and CNR-Istituto dei Sistemi Complessi, Via Madonna del Piano, 10, 50019 Sesto Fiorentino (Fi), Italy*

Javier Buldú
*Departamento de Fisica Aplicada, Universidad Rey Juan Carlos, 28933 Mostoles, Spain*

Regino Criado and Julio Flores
*Departamento de Matematica Aplicada, Universidad Rey Juan Carlos, 28933 Mostoles, Spain*

Vito Latora
*Dipartimento di Fisica e Astronomia, Università di Catania, and INFN, Via S. Sofia 64, 95123 Catania, Italy*

Javier Pello and Miguel Romance
*Departamento de Matematica Aplicada, Universidad Rey Juan Carlos, 28933 Mostoles, Spain*

(Received 28 June 2007; accepted 28 September 2007; published online 26 October 2007)

We present a novel approach to quantify the vulnerability of a complex network, i.e., the capacity of a graph to maintain its functional performance under random damages or malicious attacks. The proposed measure represents a multiscale evaluation of vulnerability, and makes use of combined powers of the links' betweenness. We show that the proposed approach is able to properly describe some cases for which earlier measures of vulnerability fail. The relevant applications of our method for technological network design are outlined. © *2007 American Institute of Physics*.
[DOI: 10.1063/1.2801687]

**Many natural, technological, and social systems find a suitable representation as networks made of a large number of highly interconnected units. This is the case, for instance, of electric power grids, the Internet, neural networks, or networks of acquaintance or collaboration between individuals. Recent studies have revealed that such systems are all characterized by similar topological properties (such as relatively small characteristic path length, high clustering, and fat tailed degree distributions) and have started a new movement of interest and research in the study of complex networks.[1–3,13]**

A central issue in the analysis of complex networks is the assessment of their security and stability. The main aim is to understand, predict, and possibly even control the behavior of a networked system under attacks or dysfunctions of any type.

A central concept that is nowadays used to assess stability and robustness of the global behavior (or performance) of complex network dynamics under external perturbations (as failures or malicious attacks) is that of *vulnerability*.

Different approaches to properly define a measure for network vulnerability has been proposed so far, relating it to, for instance, percolation theory[4] (see also Refs. 2 and 3), variations of network efficiency,[5] some structural properties of the degree distribution,[6] and the bottlenecks of the network.[7] In this Letter, we show that all such methods are useless to properly describe the vulnerability of some networks, and we introduce a new approach to the concept of vulnerability that overcomes the encountered limitations.

In order to describe the concept of vulnerability of a network, one has first to discuss the issue of network malfunctioning. This may be done under two different points of view:

(i) By considering the deactivation (deletion) of a node, together with all the links having such a node as an extreme. This point of view is especially suitable when one deals, e.g., with computer networks.[4]
(ii) By considering the deactivation (deletion) of one or several edges, without deleting any node.[5] This is the case, for instance, of airline networks: if the pilots or the ground crew in an airport are on strike, all the links of the node representing that airport should be deleted, but neither the node (the airport) nor the passengers will disappear.

These two viewpoints are far from being equivalent, The approach (i) can give rise to some problems, as the following simple example shows. Consider the graph $G_1$ in Fig. 1. If we delete node 1 and its corresponding edge, we obtain the complete graph $K_4$, so the connectivity of our graph has improved. On the other hand, under the approach (ii) of only deleting the links, $G_2$ is obtained from $G_1$, with an obvious decrease in connectivity. For this reason, in the following we will consider only the approach (ii).

Let us now consider the two graphs depicted in Fig. 2, the so-called "bat" graph $G$ and the "umbrella" graph $G'$. It is easy to realize that the two graphs differ only by the fact that the links $\ell=(1,3)$ and $\ell=(4,6)$ in $G$ are substituted with the links $\ell=(1,6)$ and $\ell=(3,4)$ in $G'$. As a result, the two graphs display an identical degree distribution function, and all approaches based on degree distributions, such as those of

 © 2007 American Institute of Physics

Downloaded 28 Jan 2008 to 193.206.209.61. Redistribution subject to AIP license or copyright; see http://chaos.aip.org/chaos/copyright.jsp

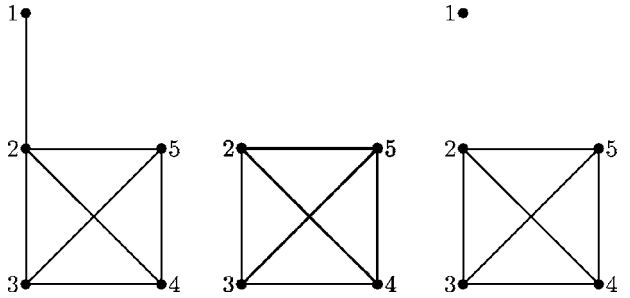


FIG. 1. From left to right: the initial graph $G_1$; the complete graph $K_4$ obtained from $G_1$ by deleting node 1 and its corresponding edges; the graph $G_2$ obtained from $G_1$ by deleting only the link emerging from node 1.

Ref. 6, would give the same value of vulnerability in both cases.

Moreover, by using the drop in the efficiency method proposed in Ref. 5, it is easy to verify that the vulnerabilities of $G$ and $G'$ under removal of single links coincide, $v(G)=v(G')=0.1951$. This is the maximal drop in the efficiency, obtained, in both networks, when the link $\ell=(7,8)$ is removed. Also, it can be easily checked that, despite the adjacency matrices of $G$ and $G'$ have different eigenvalues/eigenvectors, they share the eigenvectors corresponding to the maximal and minimal eigenvalues. This implies that measures of node centrality based on eigenvectors, like the one in Ref. 8, would be unable to distinguish between the two graphs. The question of when these two vulnerability measures fail to provide a sharp method to choose among graphs requires a deep understanding of their global structure. For example, when dealing with the eigenvalue vector vulnerability, just determining if two graphs have the same spectral radius is a central problem in graph spectrum analysis theory (see Ref. 9).

On the other hand, it is clear that the "bat" graph is more vulnerable than the "umbrella," because an attack involving the deletion of the links pertinent to node 7 would cut the graph $G$ into three disconnected components, while graph $G'$ would be cut into two disconnected components.

After careful inspection, one realizes that the difference between the "bat" and the "umbrella" graphs is in the way they distribute the load of pathways on their links. It is then evident that a proper measure of vulnerability should refer to measures of the link betweenness.[10–12]

A simple use of the standard measures of betweenness cannot, however, circumvent the problem. Indeed, if $G=(X,E)$ is a graph, for each link $\ell \in E$ one can define the edge betweenness as[10,11]

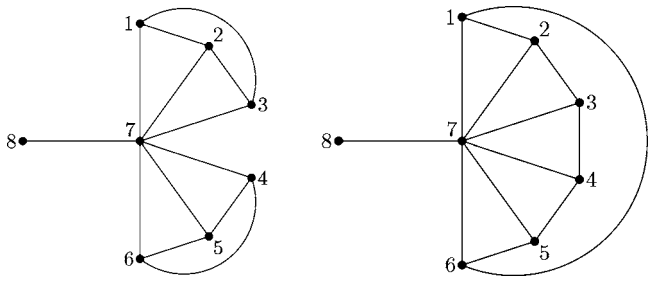


FIG. 2. The "bat" graph $G$ and the "umbrella" graph $G'$.

$$b_\ell = \sum_{j,k\in X} \frac{n_{jk}(\ell)}{n_{jk}}, \tag{1}$$

where $n_{jk}(\ell)$ is the number of geodesics from $j$ to $k$ that contain the link $\ell$ and $n_{jk}$ is the total number of geodesics from $j$ to $k$. One can then define the average edge betweenness of the graph $G$ as

$$b_1(G) = \frac{1}{|E|}\sum_{\ell\in E} b_\ell. \tag{2}$$

However, by evaluating Eq. (2) for the two graphs, one gets $b_1(G)=b_1(G')=43/13$. Actually, this equivalence is the direct consequence of a general property: For a generic network $G=(X,E)$ the parameter $b_1(G)$ is, up to normalization, the characteristic path length of $G$. Therefore $b_1(\cdot)$ gives no relevant new information about the vulnerability of the network.

Let us briefly demonstrate this property. One has

$$\begin{aligned} b_1(G) &= \frac{1}{|E|}\sum_{\ell\in E} b_\ell \\ &= \frac{1}{|E|}\sum_{\ell\in E}\left(\sum_{j,k\in X}\frac{n_{jk}(\ell)}{n_{jk}}\right) \\ &= \frac{1}{|E|}\sum_{j,k\in X}\frac{1}{n_{jk}}\left(\sum_{\ell\in E} n_{jk}(\ell)\right). \end{aligned}$$

Notice that if $\mathcal{P}_{jk}$ is the set of all geodesics joining $j$ and $k$ then one has

$$n_{jk}(\ell) = \sum_{g\in\mathcal{P}_{jk}} \chi_g(\ell),$$

where $\chi_g(\ell)$ is 1 if $\ell$ belongs to the geodesic $g$ and 0 otherwise. Hence if $d_{j,k}$ denotes the distance between $j$ and $k$ in the network, then

$$\begin{aligned} b_1(G) &= \frac{1}{|E|}\sum_{j,k\in X}\frac{1}{n_{jk}}\left(\sum_{\ell\in E} n_{jk}(\ell)\right) \\ &= \frac{1}{|E|}\sum_{j,k\in X}\frac{1}{n_{jk}}\left(\sum_{g\in\mathcal{P}_{jk}}\sum_{\ell\in E}\chi_g(\ell)\right) \\ &= \frac{1}{|E|}\sum_{j,k\in X}\frac{1}{n_{jk}}\left(\sum_{g\in\mathcal{P}_{jk}} d_{j,k}\right) \\ &= \frac{n(n-1)}{|E|}L(G) \end{aligned}$$

and, therefore, $b_1(G)$ measures essentially the same global properties than the characteristic path length $L(G)$.

In order to overcome such a limitation, we introduce here the coefficient

$$b_p(G) = \left(\frac{1}{|E|}\sum_{\ell\in E} b_\ell^p\right)^{1/|p|}, \tag{3}$$

for each value of $p>0$. Such a coefficient gives a *multiscale measure* of the vulnerability of a graph in the following sense: if one wants to distinguish between two networks $G$ and $G'$, one first computes $b_1$. If $b_1(G)<b_1(G')$, then $G$ is more robust that $G'$. On the other hand, if $b_1(G)=b_1(G')$,

Downloaded 28 Jan 2008 to 193.206.209.61. Redistribution subject to AIP license or copyright; see http://chaos.aip.org/chaos/copyright.jsp

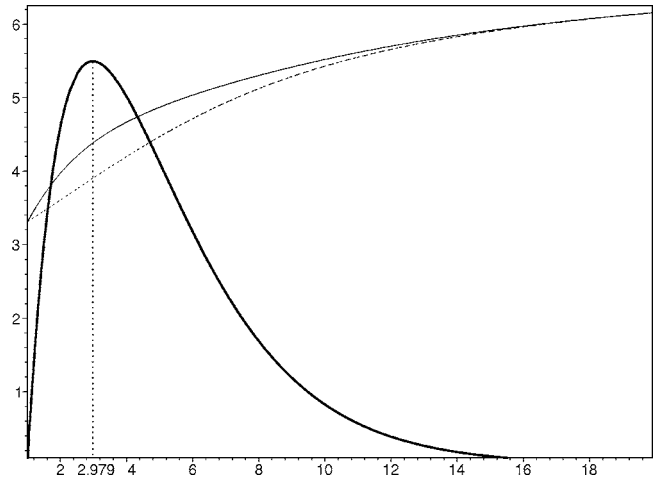


FIG. 3. $b_p(G)$ (thin line) and $b_p(G')$ (dashed line) as functions of $1 \leq p \leq \infty$. $50(b_p(G)-b_p(G'))/b_p(G)$ (thick line) as a function of $1 \leq p \leq \infty$ has a unique maximum at $p \simeq 2.979$.

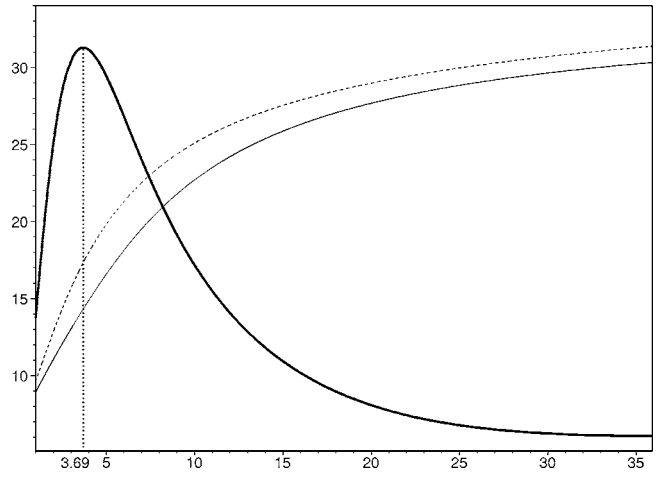


FIG. 4. $b_p$ for the Italian airline network (dashed line) and the Spanish airline (thin line) network as functions of $1 \leq p \leq \infty$. $180(b_p(G)-b_p(G'))/b_p(G)$ (thick line) as a function of $1 \leq p \leq \infty$ has a unique maximum at $p \simeq 3.699$.

then one takes $p>1$ and computes $b_p$ until $b_p(G) \neq b_p(G')$.

This, on its turn, introduces a scale $p$, at which the vulnerability measure of the networks is distinguishable. For instance, in the example of the "bat" and "umbrella" graphs, it can be easily verified that $b_2(G)>b_2(G')$ and therefore $p=2$ is already able to distinguish properly between $G$ and $G'$.

Despite the fact that $b_p(G) \leq b_q(G)$ if $p \leq q$, in general we have to consider the full multiscale sequence of betweenness coefficients $(b_p(G))_{p \geq 1}$ in order to get a sharp approach to the robustness of the network and we can not only consider the maximal extreme parameter $b_\infty(G)=\max\{b_\ell; \ell \in E\}$ [obtained as the limit of $b_p(G)$ as $p \to +\infty$], since some networks can be found, $G$ and $G'$ such that $b_1(G)=b_1(G')$, $b_\infty(G)=b_\infty(G')$, and $b_p(G)>b_p(G')$ for some $1<p<\infty$. As an example, in Fig. 3 we report the values of $b_p(G)$ (thin increasing line) and $b_p(G')$ (dashed thin line) as a function of $1 \leq p \leq \infty$, in the case of the "bat" and "umbrella." Notice that, despite the fact that $b_1(G)=b_1(G')=43/13$ and $b_\infty(G)=b_\infty(G')=7$, we have $b_p(G)>b_p(G')$ for all $1<p<\infty$, and therefore $G'$ comes out to be less vulnerable than $G$ at all scales.

Furthermore, in this particular case, the maximal relative difference $(b_p(G)-b_p(G'))/b_p(G)$ is obtained for $p \simeq 2.979$. Such a maximal difference is only reached once, as one can see from the plot of $(b_p(G)-b_p(G'))/b_p(G)$ as a function of $p$, reported in Fig. 3 (thick line).

On the other hand, if we consider the expression (3) for a network whose geodesic distribution concentrates strongly around a single link, the potential risk of a failure in this critical link is hidden in the formula by the average with the rest of minor links. However, if we go beyond the convexity frontier (as in the case of $p$-norms in the functional analysis context) and consider values of $p$ less than 1, we can avoid this difficulty and we are able to spot this kind of critical links in a network.

An easy computation shows that, in the range $0<p<1$, the properties of the $b_p$ function yield counterintuitive behaviors. If we consider negative values of $p$, then an adequate candidate should be the coefficient,

$$b_{-1}(G) = \frac{1}{|E|} \sum_{\ell \in E} \frac{1}{b_\ell}.$$

This formula is similar to the measure of global efficiency introduced in Ref. 14, and is obtained by replacing the role of distances by that of edge betweenness.

As a practical application of the proposed method we investigate the vulnerability of national airport networks. Airport networks are critical infrastructures having fundamental economic impact on local and national economies. Here, we compare the Italian and the Spanish airport networks. We have built the two networks by considering cities with airports as nodes, and assigning links to pairs of cities that are connected by nonstop domestic flights.[15] The Italian airport network, denoted by $G$ in the sequel, results in a graph with 33 nodes and 105 links, while the Spanish one, denoted by $G'$, has 35 nodes and 123 flights. If we calculate the average edge betweenness, we get $b_1(G) \simeq 9.657$ (for the Italian network), while $b_1(G') \simeq 8.919$ (for the Spanish one). The differences between the two graphs are more clear if one performs a multiscale approach. Hence, we have computed the shortest path betweenness for each link and then performed the $p$-means over all links and the results are shown in Fig. 4.

Notice that the difference between the two networks are maximal when we consider $p \simeq 3.699$, and this maximal discrepancy is only attained for this values as the plot of the function $f(p)=(b_p(G)-b_p(G'))/b_p(G)$, as it is shown in Fig. 4 (thick line).

In conclusion, we have introduced a novel approach to the measure of vulnerability for a complex network, that makes use of combined powers of the links' betweenness. The proposed approach is able to properly describe some cases for which earlier measures of vulnerability fail. Besides the assessment of the robustness of natural and biological networks against failures, the proposed approach is relevant for the design of technological (computer networks, power grids, etc.) secure graphs; given the number of nodes and links (and a desired degree distribution) the calculation of multiscale vulnerability would provide a solution to the problem of optimizing the placement of the links in order to ensure the

Downloaded 28 Jan 2008 to 193.206.209.61. Redistribution subject to AIP license or copyright; see http://chaos.aip.org/chaos/copyright.jsp

construction of a network with maximal resistance against malicious attacks.

[1]R. Albert and A. L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).
[2]S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Phys. Rep. **424**, 175 (2006).
[3]M. E. J. Newman, SIAM Rev. **45**, 167 (2003).
[4]R. Albert, H. Jeong, and A. L. Barabási, Nature (London) **406**, 378 (2000).
[5]V. Latora and M. Marchiori, New J. Phys. **9**, 188 (2007).
[6]R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, and M. Romance, Int. J. Math. Model. **4**, 307 (2005).
[7]R. Criado, J. Flores, M. I. Gonzalez-Vasco, and J. Pello, J. Comput. Appl. Math. **204**, 10 (2007).
[8]P. Bonacich, J. Math. Sociol. **2**, 113 (1972).
[9]D. M. Cetković, M. Dood, and H. Sachs, *Spectra of Graphs* (J Ambrosius Barth Verlag, Heildelberg, 1995).
[10]S. Wasserman and K. Faust, *Social Networks Analysis* (Cambridge University Press, Cambridge, 1994).
[11]M. E. J. Newman and M. Girvan, Phys. Rev. E **69**, 026113 (2004); S. Boccaletti, M. Ivanchenko, V. Latora, A. Pluchino, and A. Rapisarda, *ibid.* **75**, 045102 (2007).
[12]M. Chavez, D.-U. Hwang, A. Amann, H. G. E. Hentschel, and S. Boccaletti, Phys. Rev. Lett. **94**, 218701 (2005).
[13]R. Criado, A. García del Amo, B. Hernández-Bermejo, M. Romance, J. Comput. Appl. Math. **192**, 59 (2006).
[14]V. Latora and M. Marchiori, Phys. Rev. Lett. **87**, 198701 (2001).
[15]http://www.amadeus.net/

**Downloaded 28 Jan 2008 to 193.206.209.61. Redistribution subject to AIP license or copyright; see http://chaos.aip.org/chaos/copyright.jsp**