1st Hispano-Moroccan Days on Applied Mathematics and Statistics
17-19 December 2008
Tetouan, Morocco

Some approaches to complex networks vulnerability: results and relationships

*** Regino Criado[1] and Miguel Romance[1]**

[1] Departamento de Matemática Aplicada (URJC)
C/Tulipán s/n, 28933-Móstoles (Madrid)
regino.criado@urjc.es; miguel.romance@urjc.es

Key Words: *complex networks; betweeness; robustness; efficiency; network's vulnerability.*

ABSTRACT

The main target of this extended abstract is to give a panoramic view about different approaches to the concept of complex network's vulnerability. The study of structural properties of complex networks (the vulnerability is one of them) has become one of the paradigms of the science of complexity as well as a fascinating branch of research in applied mathematics, science and engineering, because there are a wide range of relevant properties and systems in the real world which can be modeled by complex networks: From Internet to food webs going through fields as disparate as sociology (social networks, acquaintances or collaborations between individuals), biology (metabolic and protein networks, neural networks) or technology (phone call networks, computers in telecommunication networks) [2, 6, 13, 23, 24, 25, 27, 29, 32, 33].

These systems are held to have behavioral and structural characteristics in common, and they can be studied by using non-linear mathematical models and computer modeling approaches. The interest for complex networks has certainly been promoted by the optimized rating of computing facilities, and by the availability of data on large real networks (World Wide Web, cortical networks, citation networks from Scientific Citation Index).

The study of the structural properties of the underlying network has promoted a revival of network modelling, because this kind of properties are very important not only to quantify the strategic importance of a node (or a set of nodes) in order to preserve the best functioning of the network as a whole but to give a sufficiently rich and complete picture of the problem under investigation.

The concept of vulnerability in a network quantifies the capacity of a network to maintain its functional performance under random damages, malicious attacks or disfunctions of any type. Several different approaches have been introduced to measure the vulnerability of a complex network (see, for instance [1, 3, 8, 9, 11, 18, 22, 26, 27]).

Considering that different types of networks and different applications suggest different approaches to the concept of network's vulnerability, it is obvious that there exist several ways of measuring the drop of performance of a network under malicious attacks or random damages, depending on the aspect we focus on. Some of these approaches are related to the following contexts:

- Network's connectivity loss (see, for example, [19, 30]). This approach relates the concept of vulnerability to the loss of connectivity when we remove some nodes and links in terms of potentially disconnecting the network. Under this point of view, the more homogeneous a network is (i.e., with all the nodes and links playing a similar roll) the more robust that network is. This approach is particularly interesting for military purposes and military networks or for civilian networks facing possibly terroristic activity. An alternative approach, under this point of view, is given in [13, 14, 11, 15].

- Variation of the network performance (see, for example,[18, 22, 25, 26]). This approach relates the measure of vulnerability of a network $G = (X, E)$ to the fall of its efficiency when a damage occurs.

- Betweenness' measures ([3, 4, 10, 12, 30]). This approach attend to the strategic importance of specific links and nodes in order to preserve the functioning and performance of the network as a whole.

- Centrality measures ([20, 21]) or percolation theory ([1, 6, 28]).

Each one of these approaches has its advantages and disadvantages, and the most suitable approach for a specific problem may depends on the size of the network and of the nature of the problem under investigation. It is important to remark that all of these approaches can be submerged in a general framework, the (ψ, p, q)-vulnerability, which give us a new perspective and formalism to this concept (see [17]).

In the following, we will consider a complex network $G = (X, E)$ of n nodes and m links, where X is the set of nodes and E is the set of edges. If $i, j \in X$ are nodes of G, d_{ij} will denote the geodesic distance between i and j in the network G and n_{ij} is the number of different geodesics that join i and j. If $\ell \in E$ is a link and $v \in X$ is a node, then $n_{ij}(v)$ and $n_{ij}(\ell)$ will denote the number of geodesic that join i and j passing through v and ℓ respectively.

Definition 1 *Let $G = (X, E)$ be a complex network, Y be a subset of ordered pairs of nodes or links and Z be a subset of nodes or links. If $\psi : Y \times Z \longrightarrow [0, +\infty)$ is a function and $p, q \in (0, \infty)$, then we define the (ψ, p, q)-vulnerability of G as*

$$V_{\psi,p,q}(G) = \left[\frac{1}{|Z|} \sum_{z \in Z} \left(\frac{1}{|Y|} \sum_{(i,j) \in Y} \psi(i,j,z)^p \right)^{q/p} \right]^{1/q}.$$

Most of the different definitions for the vulnerability of a complex network are particular cases for the (ψ, p, q) -vulnerability, as we can see in the following examples (see [17]). If we consider

$$Y = \{(i,j);\ \ i \neq j \in X\},$$

$Z = X$ and we take $\psi_1 : Y \longrightarrow [0, 1]$ defined for every $i, j, v \in X$ $(i \neq j)$ by

$$\psi_1(i,j,v) = \begin{cases} \frac{1}{n(n-1)} \frac{1}{d_{ij}} - \frac{1}{(n-1)(n-2)} \frac{1}{d'_{ij}}, & \text{if } i \neq v \neq j, \\ \frac{1}{n(n-1)} \frac{1}{d_{ij}}, & \text{otherwise,} \end{cases}$$

where d'_{ij} is the geodesic distance in $G \setminus \{v\}$, then the vulnerabilities based on the fail of efficiency (see [25]) $\overline{V}(G)$ and $V_{\max}(G)$ are the $(\psi_1, 1, 1)$ -vulnerability of G and $V_{\max}(G)$ the $(\psi_1, 1, \infty)$ - vulnerability of G respectively. Moreover, $V_{\psi_1,1,q}(G)$ interpolates between $\overline{V}(G)$ and $V_{\max}(G)$ in the range $q \in [1, \infty]$.

A similar phenomenon occurs if we consider the network's vulnerability is based in the concentration of the geodesic structure throughout the network (see [3]), which can be introduced as

$$V_{E,q}(G) = \left(\frac{1}{m}\sum_{\ell\in E} b_\ell^q\right)^{1/q},$$

for any $q \in [1, +\infty)$, where b_ℓ is the betweenness of the link $\ell \in E$ given by

$$b_\ell = \frac{1}{n(n-1)} \sum_{\substack{i,j\in X\\ i\neq j}} \frac{n_{ij}(\ell)}{n_{ij}}.$$

Another related concept of vulnerability was introduced in [16], where it was considered the node-based multi-scale vulnerability of a complex network given for any $q \in [1, +\infty)$ as

$$\begin{aligned} V_{X,q}(G) &= \left(\frac{1}{n}\sum_{v\in X} b_v^q\right)^{1/q} \\ &= \left(\frac{1}{n}\sum_{v\in X}\left[\frac{1}{n(n-1)}\sum_{\substack{i,j\in X\\ i\neq j}}\frac{n_{ij}(v)}{n_{ij}}\right]^q\right)^{\frac{1}{q}}. \end{aligned}$$

In these cases, if we take $Y = \{(i,j);\ i \neq j \in X\}$, $Z = E$ and we consider $\psi_2 : Y \times Z \longrightarrow [0,1]$ defined for every $i, j \in X$ $(i \neq j)$ and $\ell \in E$ by

$$\psi_2(i,j,\ell) = \frac{n_{ij}(\ell)}{n_{ij}},$$

then $V_{E,q}(G) = V_{\psi_2,1,q}(G)$, while if we consider the same set Y, but now bay taking $Z = X$ and $\psi_3 : Y \times Z \longrightarrow [0,1]$ given for every $i, j, v \in X$ $(i \neq j)$ by

$$\psi_3(i,j,v) = \frac{n_{ij}(v)}{n_{ij}},$$

then $V_{X,q}(G) = V_{\psi_3,1,q}(G)$ for every $q \in [1, +\infty)$ (see [17]).

It is pointed out in the literature that the last two vulnerability functions are correlated (see [16]), but by using this unified approach, the following result can be proven (see [17]):

Theorem 2 *Let $G = (X, E)$ be a network with n nodes and m links. If $1 \le q < \infty$, then*

$$\left[\left(\frac{1}{2}\left(\frac{2m}{n}\right)^{1/q} V_{\psi_2,1,q}(G) + \frac{1}{n^{1+\frac{1}{q}}}\right)^q + \frac{n-1}{n^{q+1}}\right]^{\frac{1}{q}} \le V_{\psi_3,1,q}(G)$$

$$V_{\psi_3,1,q}(G) \le 2^{\frac{1}{q}-1}\left(\frac{m}{n}\right)^{1/q}(gr_{\max})^{1-1/q}\, V_{\psi_2,1,q}(G) + \frac{1}{n}.$$

Other examples, such as the bottleneck type vulnerabilities are particular cases of (ψ, p, q) -vulnerability functions and this new framework help to show new correlations and interpolations between different approaches. For example, it can be proven that $V_{\psi_1,p,q}(G) \le V_{\psi_3,p,q}(G)$, for all $1 \le p, q \le \infty$ and similar results occur for the bottleneck type vulnerabilities (see [17]).

References

[1] R. Albert, H. Jeong, A. L. Barabási, Nature **406**, 378 (2000).

[2] Y. Bar-Yam, *Dynamics of Complex Systems*, Addison-Wesley, 1997.

[3] S. Boccaletti, J. Buldú, R. Criado, J. Flores, V. Latora, J. Pello, M. Romance, Chaos **17**, 043110 (2007).

[4] S. Boccaletti, R. Criado, J. Pello, M. Romance, M. Vela-Pérez, to appear in IJBC , (2009).

[5] S. Boccaletti, M. Ivanchenko, V. Latora, A. Pluchino, A. Rapisarda, Phys. Rev. E **75**, 045102 (2007).

[6] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D. U. Hwang, Physics Reports **424**, 175 (2006).

[7] C. Boyd, A. Mathuria, *Protocols for Authentication and Key Establishment (Information Security and Cryptography)*, Springer, 2003.

[8] R. Cohen, K. Erez, D. ben-Avraham and S. Havril, Phys. Rev. Lett. **85 (21)**, 4626 (2000).

[9] R. Cohen, K. Erez, D. ben-Avraham and S. Havril, Phys. Rev. Lett. **86 (16)**, 3682 (2001).

[10] R. Criado, J. Flores, M.I. Gonzalez-Vasco, J. Pello, Journal of Computational and Applied Mathematics **204**, 10 (2007).

[11] R. Criado, J. Flores, B. Hernández-Bermejo, J. Pello, M. Romance, J. Math. Modelling and Algorithms **4**, 307 (2005).

[12] R. Criado, J. Flores, J. Pello, M.Romance, EPJ, Special Topics **146**, 145-157 (2007).

[13] R. Criado, A. García del Amo, B. Hernández-Bermejo, M. Romance, J. Comput. Appl. Math. **192**, 59 (2006).

[14] R. Criado, B. Hernández-Bermejo, J.Marco-Blanco,M. Romance, J. Comput. Appl. Math. **204**, 166 (2007).

[15] R. Criado, B. Hernández-Bermejo and M. Romance, IJBC **17 (7)**, 2289 (2007).

[16] R. Criado, J. Pello, M. Romance, M. Vela-Pérez, To appear in IJBC , (2008).

[17] R. Criado, J. Pello, M. Romance, M. Vela-Pérez, Preprint , (2008).

[18] P. Crucitti, V. Latora, M. Marchiori and A. Rapisarda, Physica A **320**, 622 (2003).

[19] A. H. Dekker and B. D. Colbert, "Network Robustness and Graph Topology", *Proceedings of ACSC04, the 27th Australasian Computer Science Conference* (18-22 January 2004), Dunedin, New Zealand.

[20] E. Estrada, J. Rodríguez-Velázquez, Phys. Rev. **E71**, art. no. 056103 (2005).

[21] J. Rodríguez,E. Estrada and A. Gutiérrez, Linear and Multilinear Algebra **55 (3)**, 293–302 (2007).

[22] P. Holme, Beom Jun Kim, Chang No Yoon and Seung Kee Han, Phys. Rev. **E65**, 056109 (2002).

[23] P. Holme, J.-H. Kim, Phys. Rev. **E65**, 066109 (2002).

[24] H. Jeong, S. Mason, A. L. Barabási and Z. N. Oltvai, Nature **411**, 41 (2001).

[25] V. Latora, M. Marchiori, Phys. Rev. Lett. **87**, 198701 (2001).

[26] V. Latora, M. Marchiori, Chaos, Solitons and Fractals **20**, 69 (2004).

[27] V. Latora, M. Marchiori, New J. Phys. **9**, 188 (2007).

[28] M. E. J. Newman, SIAM Rev. **45**, 167–256 (2003).

[29] M. E. J. Newman, M. Girvan, Phys. Rev. E **69**, 026113 (2004).

[30] M. E. J. Newman, G. Goshal, Phys. Rev. Lett. **100**, 138701 (2008).

[31] W. Rudin, *Real and complex analysis (3th. Ed.)*, McGraw-Hill, 1987.

[32] O. Sporns, Complexity **8**, 56 (2002).

[33] S. H. Strogatz, Nature **410**, 268 (2001).

[34] S. Wasserman, K. Faust, *Social Networks Analysis*, Cambridge University Press, 1994.