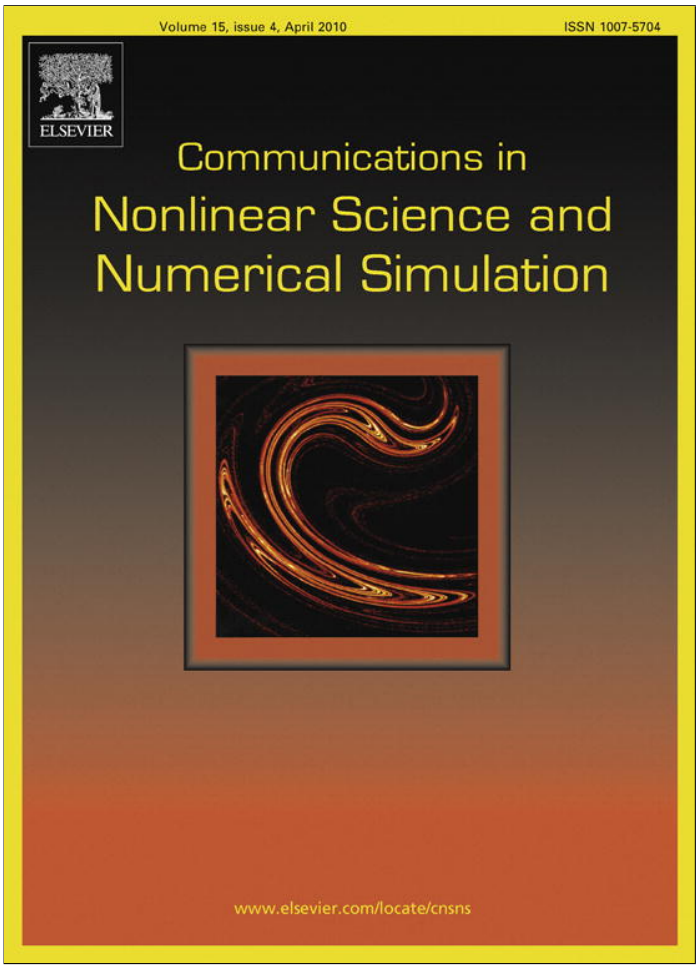

Commun Nonlinear Sci Numer Simulat 15 (2010) 1008–1018

Contents lists available at ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

Application of modal analysis in assessing attack vulnerability of complex networks

Irina Petreska [a,b,*], Igor Tomovski [a], Eugenio Gutierrez [c], Ljupčo Kocarev [a], Flavio Bono [c], Karmen Poljansek [c]

[a] Research Center for Energy, Informatics and Materials, Macedonian Academy of Sciences and Arts, bul. Krste Misirkov 2, P.O. Box 428, 1000 Skopje, Macedonia
[b] Faculty of Natural Sciences and Mathematics, Institute of Physics, P.O. Box 162, 1000 Skopje, Macedonia
[c] European Laboratory for Structural Assessment, Institute for the Protection and Security of the Citizen, Joint Research Center, European Commission, Ispra, Italy

ARTICLE INFO

Article history:
Received 16 February 2009
Received in revised form 3 May 2009
Accepted 3 May 2009
Available online 10 May 2009

PACS:
89.75.−k
02.10.Ox

Keywords:
Vulnerability
Modal analysis
Modal weight
Generic networks
Manmade networks

ABSTRACT

In this paper we propose an alternative way to study robustness and vulnerability of complex networks, applying a modal analysis. The modal weights of the network nodes are considered as a measure for their busyness, which is further used for preferential removal of nodes and attack simulation. Analyses of the attack vulnerability are carried out for several generic graphs, generated according to ER and BA algorithms, as well as for some examples of manmade networks. It was found that a modal weight based attack causes significant disintegration of manmade networks by removing a small fraction of the busiest nodes, comparable to the one based on the node degree and betweenness centrality.

1. Introduction

Vulnerability of complex networks is an issue that has been studied from various aspects. The definition of vulnerability itself is still a subject of discussion. As a concept, vulnerability has been introduced in several fields including psychology, sociology, political science, economics, epidemiology, biology, environmental and geosciences, and engineering [1]. In dictionary definitions of "vulnerable", a common denominator is references to deliberate actions (threats), e.g., "susceptible to attack", and "open to attack or assault by armed forces" [2]. However, there is no generally accepted definition of the concept vulnerability even if we only consider technical, or engineering applications. Below we will give a few examples of possible definitions of vulnerability in relation to technical systems. Einarsson and Rausand [3] study industrial systems, and define vulnerability as the properties of an industrial system; its premises, facilities, and production equipment, including its human resources, human organization and all its software, hardware, and net-ware, that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries. Berdica defines vulnerability in the road transportation system as a susceptibility to incidents that can result in considerable reductions

* Corresponding author. Address: Research Center for Energy, Informatics and Materials, Macedonian Academy of Sciences and Arts, bul. Krste Misirkov 2, P.O. Box 428, 1000 Skopje, Macedonia. Tel.: +389 23249999.
E-mail addresses: irina@manu.edu.mk, irina.petreska@pmf.ukim.mk (I. Petreska), igor@manu.edu.mk (I. Tomovski), eugenio.gutierrez@jrc.it (E. Gutierrez), lkocarev@manu.edu.mk (L. Kocarev), f.bono@jrc.it (F. Bono), karmen.poljansek@jrc.it (K. Poljansek).

1007-5704/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.cnsns.2009.05.002

in road network serviceability [4]. In the field of information security, vulnerability is commonly thought of as a weakness in the security system that might be exploited to cause harm or loss. Morakis et al. [5] define vulnerability as a measure of the exploitability of a weakness". In structural engineering, the term vulnerability is often used to capture the susceptibility of a component or a system to some external action. Thus, a structure is vulnerable if any small damage produces disproportionately large consequences [6]. Finally, vulnerability is also a topic in mathematics. In the branch of discrete mathematics called graph theory, vulnerability implies a lack of resistance of the graph to the deletion of nodes and edges [7].

When investigating the issues related to system functionality, under special circumstances, some authors tend to speak of reliability, rather then vulnerability of the system. IEEE defines reliability as the ability of a system or component to perform its required functions under stated conditions for a specified period of time [8]. Though it might be understood that vulnerability is marly a complement of vulnerability, it is not the case, since the reliability takes into consideration both the failure of certain segment of the system as well as the system as a whole, when the segment of the system fails, while the vulnerability considers only the later.

In complex infrastructure networks nodes are entities that produce, transform or consume a resource (e.g., generators, substations or loads in electricity networks), while the edges are physical or virtual entities linking the nodes and enabling flow of a physical quantity, information or influence. Many years of experience have generated a consistent system of statistical measures describing properties that are common to most of the real-life networks. Several generic models such as Erdos–Renyi (ER random graph), Watts–Strogatz (WS small world), and Barabasi–Albert (BA scale-free) models have been established and investigated [9–16]. In several papers by Albert et al. error and attack tolerance of complex networks were studied and some general conclusions, further confirmed through many other real-life examples [2], were derived. The preferential removal of nodes and edges, which is a way to model attacks, in the aforementioned papers was based on the centrality measures. Thus, the effects of nodes removal according to their degree and betweenness centrality on the network fragmentation, giant component size, the diameter of the network, average shortest path and efficiency were investigated [15]. It was shown in heterogenous networks (scale-free) that the diameter increases dramatically when they're the subject of attacks, while in the homogenous networks there is no significant difference as to whether the nodes are chosen randomly (removals referred to as errors) or preferentially according to their connectivity or betweenness centrality. In real-life networks, such as power grids, urban networks, communication networks, centrality measures are not always the best way to assess the nodes or edges busyness. In this work we apply the methods from structural dynamics based on modal analysis to investigate complex networks and their vulnerability. We make an attempt to find the different modes of flow in a complex structure and to assign modal weight to each node and edge. We further use this data to rank the nodes and edges by their modal weight and to simulate attacks based on the modal rank.

2. A brief description of the methodology

The investigations of the complex networks attack vulnerability are usually carried out by tracking the changes in topological measures after a network is subjected to attacks. Numerical studies on network robustness were first applied to the Internet and a sample of the World Wide Web [11,17]. Albert et al. have studied how the properties of the mentioned networks change when a fraction f of the nodes is removed [11]. The nodes are randomly deleted to simulate errors, or in decreasing order of their degree to simulate attacks. It was shown that both the Internet and WWW are persistent for high rates of random node removal, i.e., persistent to errors, but sensitive to attacks. This corresponds to the mathematical predictions for scale-free networks, confirming once more that most of the real-life examples of networks are most adequately described by the scale-free model.

Crucitti et al. examined the dependence of average shortest path and the global efficiency of BA scale-free network and ER random graph on the fraction of the removed nodes. It was shown that the differences between scale-free networks become less pronounced as the fraction of removed nodes increases. The scale-free networks are the most affected by attacks, even if a small fraction of nodes is removed (sometimes a single one) [18,19]. It is worth mentioning that as a network becomes unconnected (larger fraction of nodes are removed), the global efficiency is a better quantity to describe the system than the average shortest path.The preferential removals, which simulate attacks are based on the measures that generally describe connectivity of the network components, such as degree and centrality.

In this work we introduce another measure of the nodes and lines busyness, that originate from structural dynamics. Looking at the complex networks from the structural dynamics view point, one finds analogy between a graph and a system of point-like oscillators connected by elastic springs. Such a system has several possible vibrating modes, that can be determined by applying a so called modal analysis – a linear algebra approach enabling to find the normal vibrational modes of an elastic oscillating system. Thus, employing the modal analysis for the purposes of vulnerability studies has two major justifications. First, the topological entities have analogs in dynamical structures. Second, the transport of a physical quantity through a complex network can be described in a similar way as a spreading of oscillations in a mass–spring system of oscillators.

As a first step we utilize the modal weights as a measure of the busyness or the load of nodes and lines, and explore the correlation between the modal parameters and topological measures such as degree and centrality. For this purpose we rank the nodes and lines according to their busyness, quantified by various criteria. Afterwards, we simulate attacks by preferential removal of nodes according to their rank by degree, modal weight and betweenness centrality, and analyze the network

fragmentation, relative size of the giant component and diameter. Aforementioned analysis is applied on networks having different topologies.

2.1. Spectral and modal analysis – brief theoretical background

Much relevant information about complex networks can be obtained by analyzing the topological properties of the graph which represents the network. One of the most frequently utilized methods to examine the topological properties of a graph is based on the analysis of the eigenvalues of the graph Laplacian, given by:

$$\mathbf{L} = \mathbf{D} - \mathbf{A} \tag{1}$$

where $\mathbf{D}$ is a diagonal matrix whose elements are $D_{ii} = D_i$, where D_i $(i = 1 - n)$ stands for the degree of the corresponding node and $\mathbf{A}$ stands for the adjacency matrix[11]. The adjacency matrix entries a_{ij} get value 1 if a link exists between the nodes i and j, or 0 if the link does not exist. Note that in the case of weighted graph, the diagonal degree matrix elements D_{ii} are calculated as a sum of the weights of all the links emerging from the node i, while the adjacency matrix entries are in fact, the line weights [20–26]. The eigenvalues of the Laplacian are very often used to classify a network.

But, where is the analogy with the structural dynamics? If we consider a graph as a system of mass–spring oscillators, employing an analogy between the spring constants and the link weights, the net force acting on each node would be given by:

$$f_i = \sum_{j=1}^{N} a_{ij}(x_j - x_i) = -\left(\sum_{j=1}^{N} a_{ij}x_i - \sum_{j=1}^{N} a_{ij}x_j\right) \tag{2}$$

Note that the first sum in the equation above gives the node degree d_i, thus the net force acting on the node i can be expressed as

$$f_i = -\left(d_i x_i - \sum_{j=1}^{N} a_{ij}x_j\right) \tag{3}$$

Stacking up the equations for each node, in the complete system of equations, the Laplacian appears:

$$\mathbf{F} = -(\mathbf{D} - \mathbf{A})\mathbf{X} = -\mathbf{L}\mathbf{X} \tag{4}$$

This system of equations plays a major role in Structural dynamics, since it governs the dynamics of a mass–spring grid and is a base of the method known as modal analysis. The idea to apply this approach to complex networks, was first introduced by Gutierrez et al. in a case study of vulnerability of a power grid segment [27] and further investigated in [28]. We here give a few details on the modal analysis application. If we express the force in terms of mass as $\mathbf{F} = \omega_i^2\mathbf{M}\mathbf{X}$, it is obvious that the equation above can be used to determine the normal vibrational frequencies. In order to quantify the influence of each oscillating mode on each network node, one should determine the modal connectivity matrix $\mathbf{\Gamma}$. The $\mathbf{\Gamma}$ matrix is defined as

$$\mathbf{\Gamma} = \mathbf{L}'\mathbf{\Phi} \tag{5}$$

where $\mathbf{L}'$ stands for the transposed Laplacian and $\mathbf{\Phi}$ is a matrix composed of the Laplacian eigenvectors. Let us denote the modal connectivity matrix elements by $\gamma_{i,j}$. Modal contributions to each node can now be determined as

$$w_i = \sum_{j=1}^{n} |\gamma_{i,j}|, \quad \gamma_{i,j} \in \Gamma \tag{6}$$

for $i = 1$–n. The modal contribution is a measure of the load each node receives, thus the modal contribution w_i can be used to rank the nodes according to their busyness. In our work the modal ranking of the nodes was used to develop a strategy for each theoretical study of the power grid vulnerability. The modal spectral analysis can be also applied to assess busyness of lines. The modal load of a line is given by the sum of the absolute values of the differences between modal contributions of neighboring nodes [27,29,30]

$$l_{i,j} = \sum_{k=1}^{n} |\gamma_{i,k} - \gamma_{j,k}| \tag{7}$$

One important question in modeling manmade networks is the way of assigning line weights. Various physical quantities can be used to quantify the line weight. For example in a power grid those can be voltages, power transmitted through the lines, capacity of the line etc. In our study the weights in terms of line voltages were utilized.

Applying the methodology described above we investigate the attack vulnerability of topologically different networks, including samples generated by Erdos–Renyi and Barabasi–Albert models, as well as segments of the EU power grid, as representatives of manmade networks (processing of the datasets used to generate power grid graphs is described in the next

chapter) [9,11]. Modal analysis and ranking of the nodes according to their modal weight was carried out by a programming code developed for the purposes of this work.

3. Network collation

As it was mentioned before, attacks on several segments of the EU power grid are simulated in this work. The European electricity network is composed of four main independent AC synchronized zones. Each single zone is managed by a transmission system operator (TSO) that ensures the stability of the grid and coordinates the operations between power suppliers and distribution companies: UCTE, covering the main part of continental Europe, NORDEL, covering Scandinavia, and UKTSOA, consisting of the island of Great Britain. ATSOI for Ireland; other islands, like Iceland, Corsica, and Crete have their own power grids without AC connections to the main continental network. The UCTE and NORDEL member countries which border with the synchronous system of the ex-USSR republics are not synchronously connected and are managed by a separated TSO (BALTSO). This leaves the three EU Baltic states effectively disconnected from other EU states.

As it was mentioned before, attacks on several segments of the EU power grid are simulated in this work. The European electricity network is composed of four main independent AC synchronized zones. Each single zone is managed by a transmission system operator (TSO) that ensures the stability of the grid and coordinates the operations between power suppliers and distribution companies: UCTE, covering the main part of continental Europe, NORDEL, covering Scandinavia, and UKTSOA, consisting of the island of Great Britain. ATSOI for Ireland; other islands, like Iceland, Corsica, and Crete have their own power grids without AC connections to the main continental network. The UCTE and NORDEL member countries which border with the synchronous system of the ex-USSR republics are not synchronously connected and are managed by a separated TSO (BALTSO). This leaves the three EU Baltic states effectively disconnected from other EU states.

For the purposes of this paper, we investigate the NORDEL, UKTSOA, and ATSOI electricity transmission grid networks (see Figs. 1 and 2).

4. Results and discussion

4.1. Correlation between the different ranking criteria

Rankings according to connectivity, betweenness centrality and modal weight were compared and further used in developing a strategy to simulate attacks on the network.

The correlation between the ranking according to degree and betweenness centrality, as well as the modal weight and betweenness centrality was estimated by the Spearman's correlation coefficient. This correlation coefficient between two lists of numerical values x and y can be calculated as follows:

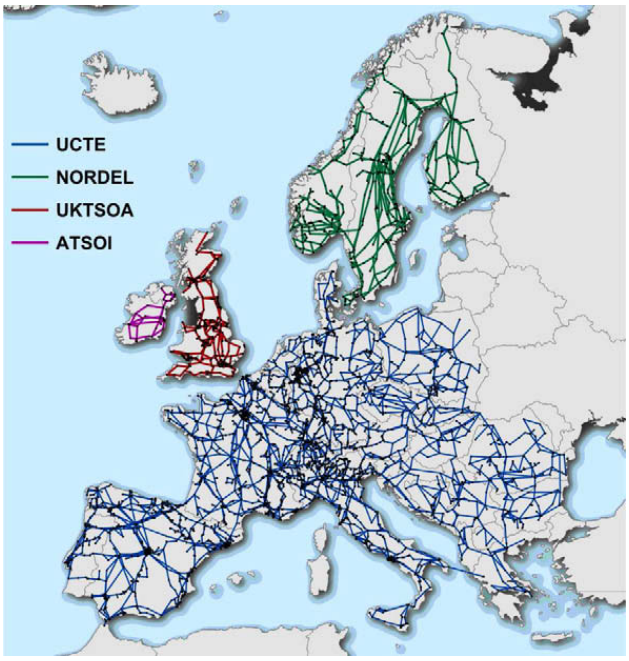

Fig. 1. European electricity independent grid networks.

Electricity independent grid	Number of edges	Number of Vertices
UCTE	5305	4200
NORDEL	641	524
UKTSOA	492	393
ATSOI	60	49

Fig. 2. Basic statistics on the extracted independent electricity networks.

$$\frac{(n^3-n)/6-T_x-T_y-\sum_i r_i^2}{\sqrt{((n^3-n)/6-2T_x)((n^3-n)/6-2T_y)}} \tag{8}$$

where n is the length of the lists of values, r_i is the rank difference between x_i and y_i, T_x is the correction term for ties in x-list and T_y is the correction term for ties in y-list. We examine the correlation between the lists of nodes' degrees and betweenness centralities, and the lists of modal weights and betweenness centralities for several BA scale-free and ER random graph realizations. The average correlation coefficient for the investigated BA realizations between the degree and betweenness centrality rankings is found to be 0.765502, while for the random ER graphs 0.67274.

The Spearman's correlation coefficient between the rankings according to the modal weight and the betweenness centrality is about 0.56462, while the correlation between modal ranking and closeness centrality is about 0.5. The correlation between the centrality measures and modal weights is graphically represented in Figs. 3–5.

Obviously there is a positive, but relatively low linear correlation between the rankings, so it will be of significant importance to apply these different assessing criteria complementary, taking into account parameters that are related with the connectivity, centrality, and load.

Throughout our research we found the modal weight of the nodes a reliable measure for a node utilization and busyness especially for manmade networks (power grids, urban networks, internet), where the flow of the physical quantity transported through the network is of importance. This is what motivate us to analyze the attack vulnerability of complex networks by preferential removal of the nodes according to their modal weight and to compare the results with those obtained by preferential removal according to the standard measures.

4.2. Attack vulnerability

The attack vulnerability of the considered networks is examined by two different strategies. First one, so called *non-adaptive strategy*, uses the initial ranking of the nodes, without recalculating the properties after each removal of nodes. In the second *adaptive strategy*, the modal weight, as well as betweenness centrality and nodes' degree are recalculated after each deletion of nodes, and the new ranking is utilized. The adaptive strategy gives more reliable results, since a deletion of a node that is strongly connected by several other nodes in a certain mode causes transition to some other flowing mode. Usually in the other flowing mode, new nodes are activated and the ranking changes.

The attack vulnerability in this analysis is measured through the dependence of the number of clusters, network diameter, and relative size of the giant component on the fraction of deleted nodes. Giant component of a graph is the largest

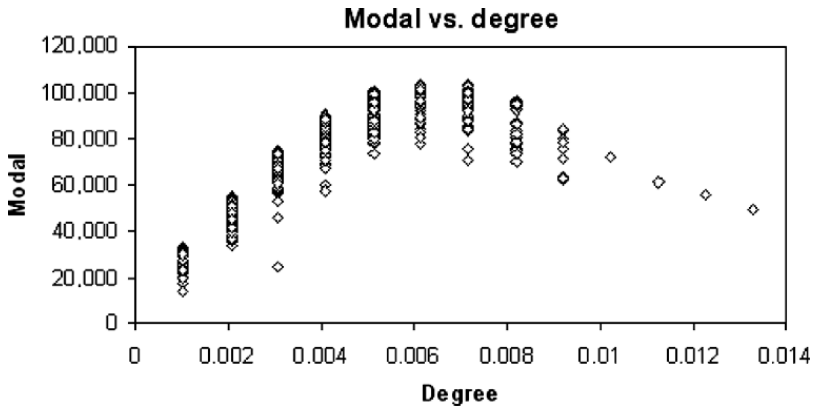

Fig. 3. Correlation between the modal weight and degree of the nodes in an ER graph (1000 nodes, average degree 3.5).

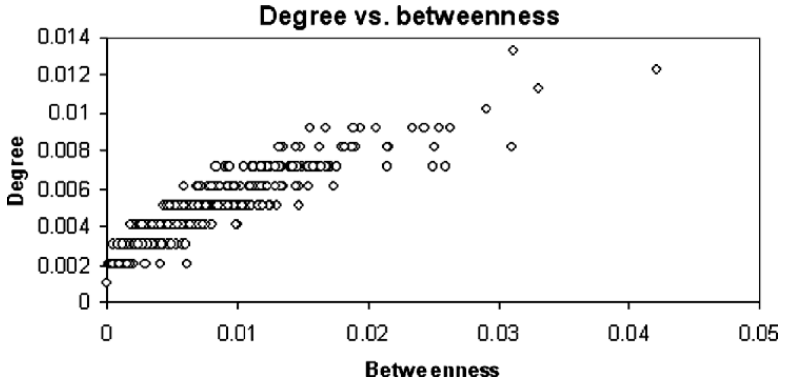

Fig. 4. Correlation between the betweenness and degree of the nodes in an ER graph (1000 nodes, average degree 3.5).

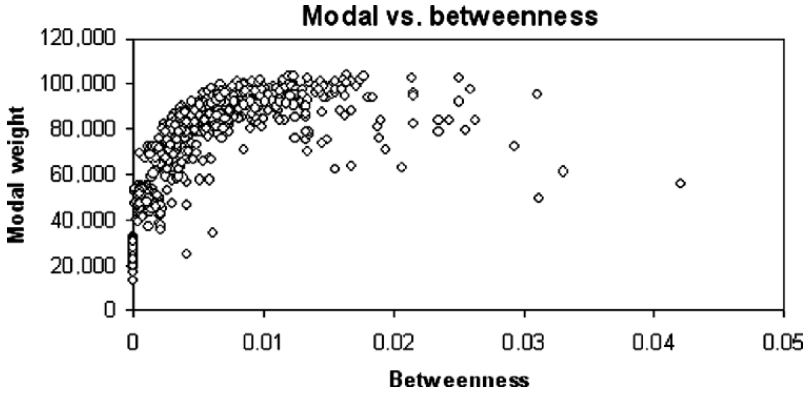

Fig. 5. Correlation between the modal weight and betweenness of the nodes in an ER graph (1000 nodes, average degree 3.5).

subgraph, that is still connected. The ratio of the size (number of nodes) of the giant component to the total number of nodes of the considered graph is known as a relative size of the giant component.

The failure of the random ER network considered in this work, tracked by the decrease in the relative size of the giant component with the deletion of nodes is represented in Fig. 6. The same analysis for the scale-free graph is given in Fig. 7.

In agreement with the recent findings [2,8–10], our results confirm that the scale-free networks are more vulnerable than ER networks, when submitted to attacks (preferential removal of nodes). Analyzing the graphs, one can notice that deletion of nodes of the considered scale-free and ER networks according to their connectivity and betweenness centrality is a more efficient strategy to disintegrate a generic network than a modal weight based strategy.

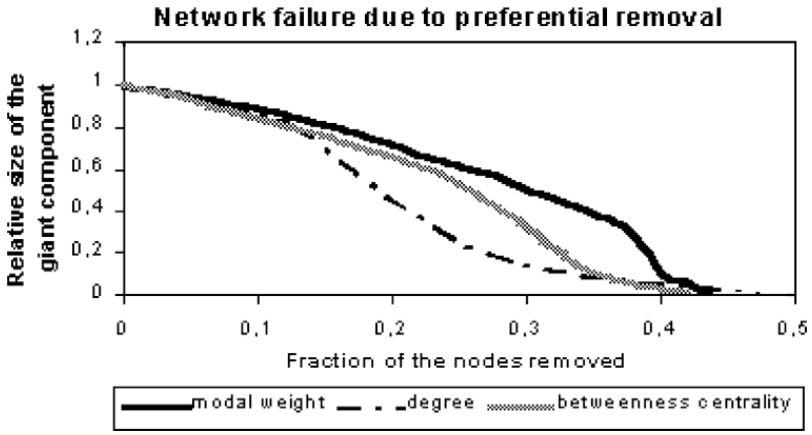

Fig. 6. The dependence of the relative size of the giant component on the fraction of removed nodes for a random ER graph with 1000 nodes and average degree 3.5 – non-adaptive strategy.

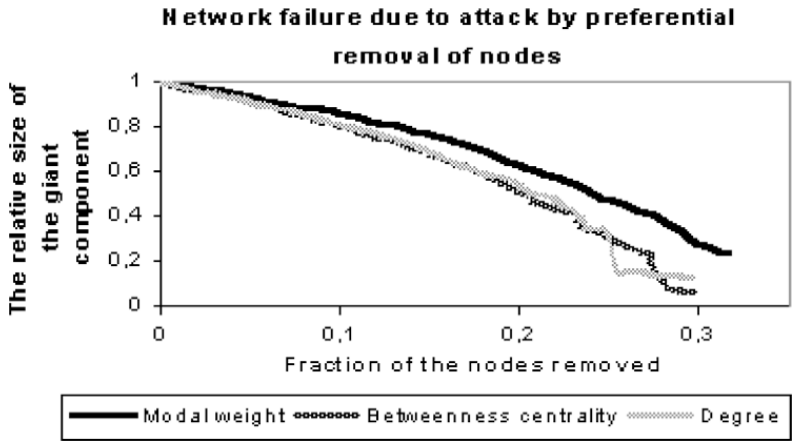

Fig. 7. The dependence of the relative size of the giant component on the fraction of removed nodes for a random SF graph with 1000 nodes and average degree 3.5 – non-adaptive strategy.

The examples of manmade networks, represented by NORDEL, UKTSOA, and Ireland synchronized zones of the European power grid are also subjected to this analysis. Modal weight distribution among the nodes for a certain mode for one of the investigated sectors is shown in Fig. 8, just as an illustration.

Two approaches are implemented on the power grid segments. The first one is a basic topological analysis, carried out by neglecting – setting to one the weights of the edges, and the second one includes the weights of the lines.

Fig. 9 shows the dependence of the giant component relative size on the fraction of the removed nodes, by the adaptive approach for unweighted NORDEL synchronized zone. Neglecting the weights of power transmission lines allows only a topological analysis of manmade networks. For comparison, the results obtained by simulating attacks based on the nodes degree and their modal weight are represented on the same graph. Obviously, the preferential removal based on the nodes degree is more efficient for small fractions of removed nodes (0—0.03) and as the fraction of the removed nodes increases the both strategies have nearly the same efficiency, except for some regions where either strategy leads faster disintegration (see the interval between 0.03 and 0.05, where modal weights based strategy is more efficient). For example, in the interval between 0.03 and 0.05, the attacks based on modal weight are more successful.

Fig. 10 presents the attack vulnerability, measured by the changes of the relative size of the giant component for the same synchronized zone, but considering the weights of lines as well. The general conclusion that the deletion by degree is more efficient at the beginning of the attack, and after several removals the strategies are equally efficient still stands. Similarity between the results obtained through pure topological analysis and physical analysis indicates that one can assess a manmade network vulnerability, at least qualitatively, even with a limited knowledge on the physical properties of the network.

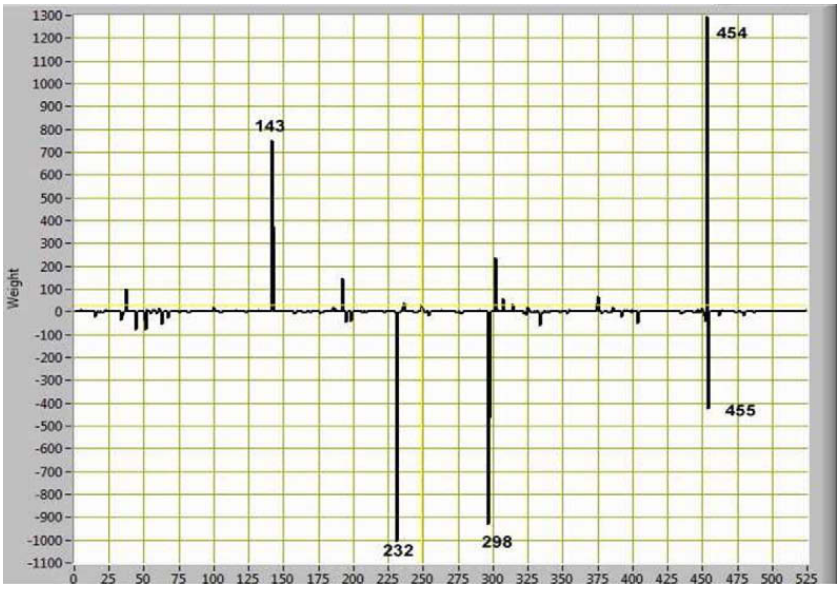

Fig. 8. Modal weights of the nodes for one of the possible modes obtained by the modal analysis.

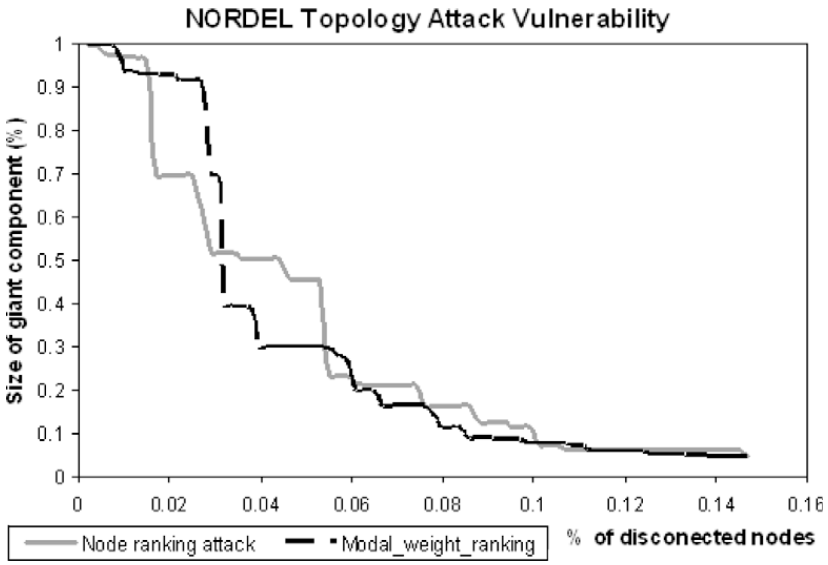

Fig. 9. Topological assessment of the attack vulnerability of a power grid segment (unweighted), having 524 nodes and 641 links, simulated by an adaptive strategy.

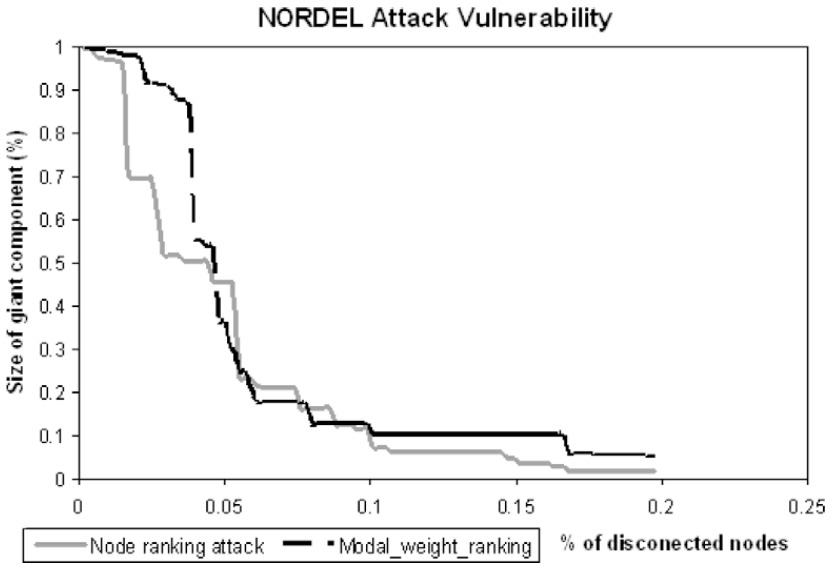

Fig. 10. Attack vulnerability of a power grid segment (weighted), having 524 nodes and 641 links, simulated by an adaptive strategy.

Results for the rest two synchronized zones, UK and Ireland, analyzed through our simulations are shown in Figs. 11–14. Fig. 11 illustrates the giant component relative size versus the fraction of removed nodes for UK synchronized zone, modeled by unweighted graph, while Fig. 12 gives the same analysis for the weighted graph. Comparison of network disintegration by applying degree of the nodes and modal weights as measures of the nodes busyness leads to similar conclusions as in the case of NORDEL zone, elaborated in the previous paragraphs. The topological analysis of the attack vulnerability for Ireland synchronized zone, represented in Fig. 13, as well as the analysis including line weights (Fig. 14) indicates higher efficiency of the modal weights based strategy in wider range of removed nodes fraction, compared to previous cases. Probably the only reason for this result is the size of the network.

To summarize, analyzing the attack vulnerability, measured through the decrease of the giant component relative size with preferential removals of nodes by the two adopted criteria (Figs. 9–14) suggest that the modal weight could be an efficient method to disintegrate a manmade network.

5. Conclusions

In this paper a modal analysis based study of the attack vulnerability of generic and manmade networks was presented. The modal analysis was for the first time applied to random graphs generated by the basic Erdos–Renyi and scale-free

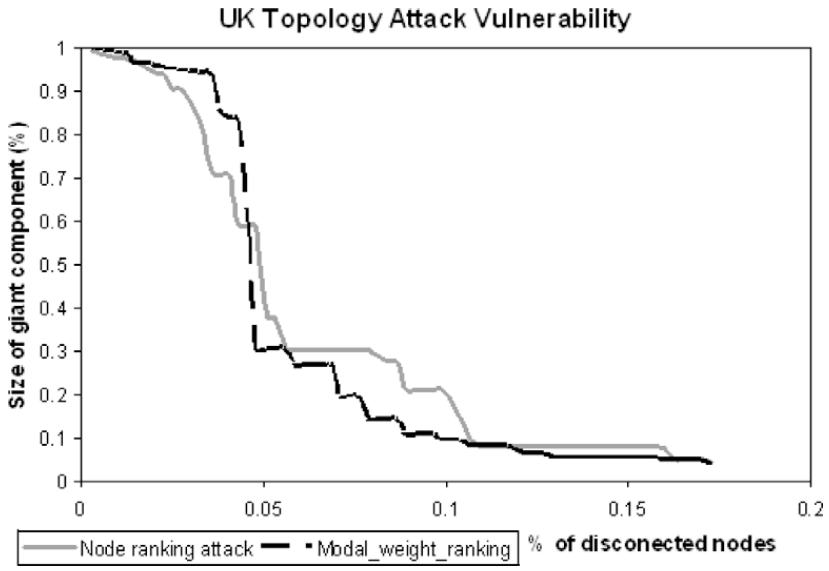

Fig. 11. Topological assessment of the attack vulnerability of a power grid segment (unweighted), having 393 nodes and 492 links, simulated by an adaptive strategy.

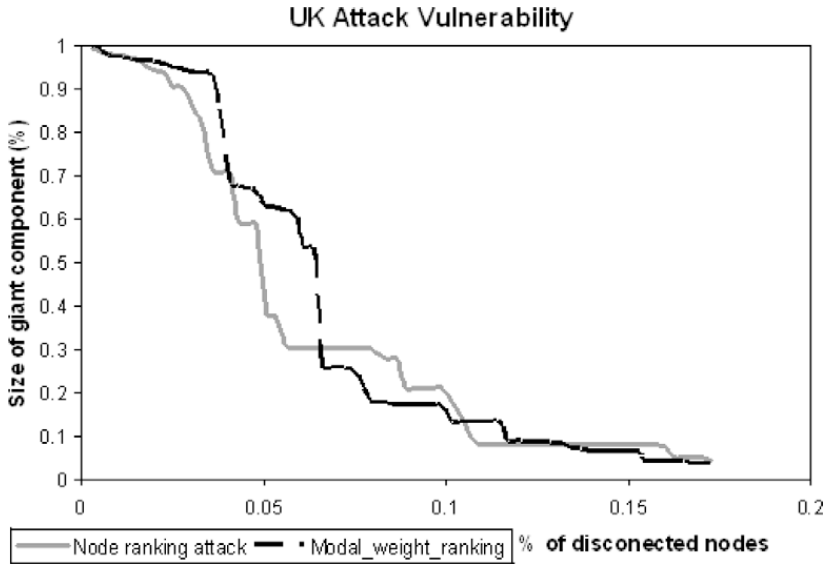

Fig. 12. Attack vulnerability of a power grid segment (weighted), having 393 nodes and 492 links, simulated by an adaptive strategy.

Barabasi–Albert algorithms. The modal weight was introduced as an assessment criterion of the nodes and lines busyness, which was further used to rank the nodes. Spearman's correlation coefficients between the rankings based on centrality measures at one side, and modal weights on the other, indicate low correlation. Attack simulations were carried out by using two different strategies – *adaptive* and *non-adaptive*. The preferential removal of the fractions of nodes was based on the three different criteria (the nodes connectivity, betweenness centrality, and modal weight).

It was confirmed once more that the scale-free BA graphs are more sensitive to attacks than random ER graphs, even when the attacks are planned using the results of modal analysis. In addition, the attack vulnerability analysis was also applied to several examples of manmade networks. From the topological point of view attacking the network according to the node degree proved to be the most efficient strategy, especially for generic networks. However, the disintegration of the manmade networks caused by a modal weight based attack at initial steps is as significant as a disintegration based on the node degree or betweenness centrality. The low correlation between the node degree and modal weight shows that the most connected nodes are not at the same time the most loaded nodes, so the modal analysis could be sufficient to detect the busiest nodes. Even though the rate of fragmentation is higher when the attacks are planned by the node degree, a busiest node deletion can cause overloading of the neighboring nodes and provoke a cascading

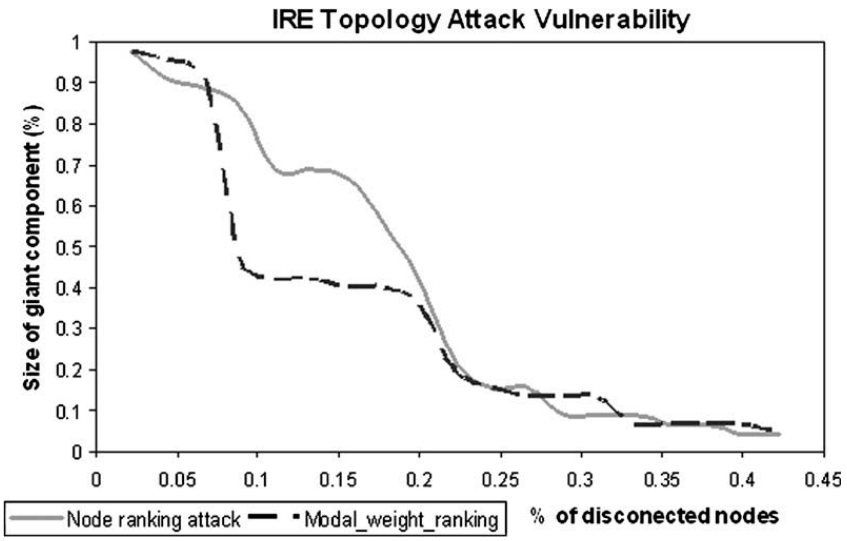

Fig. 13. Topological assessment of the attack vulnerability of a manmade network, simulated by an adaptive strategy, for unweighted graph, having 49 nodes and 60 links.

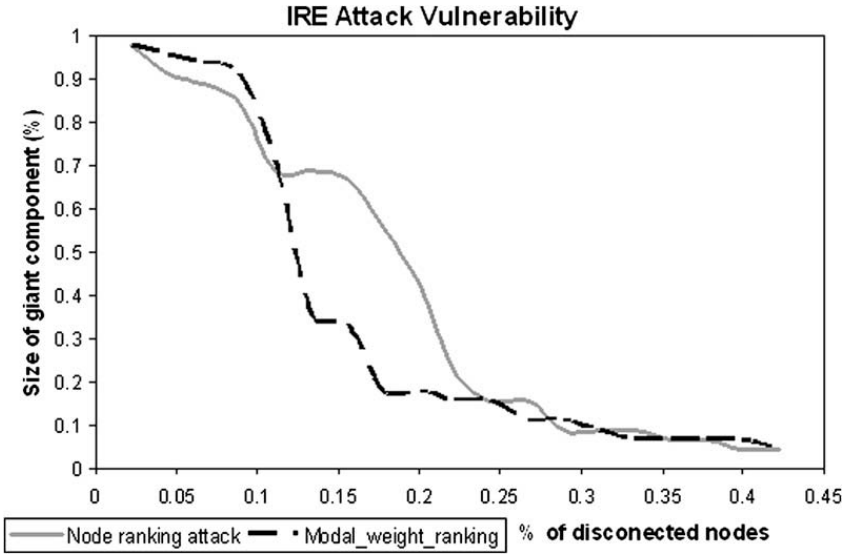

Fig. 14. Attack vulnerability of a manmade network, simulated by an adaptive strategy, for weighted graph, having 49 nodes and 60 links.

failure. Thus, a modal analysis could be a complementary method for vulnerability assessment to the methods based on centrality measures, aiming at detection, protection, and safety of the busiest components.

References

[1] McEntire DA. Why vulnerability matters: exploring the merit of an inclusive disaster reduction concept. Disaster Prev Manage 2005;14:206–22.
[2] Merriam-Webster. Merriam-Webster online dictionary: http://www.m-w.com/; 2006.
[3] Einarsson S, Rausand M. An approach to vulnerability analysis of complex industrial systems. Risk Anal 1998;15:535–46.
[4] Berdica K. An introduction to road vulnerability: what has been done, is done and should be done. Transp Policy 2002;9:117–27.
[5] Morakis E, Stylianos V, Blyth A. Measuring vulnerabilities and their exploitation cycle. Inf Secur Tech Rep 2003;8:45–55.
[6] Agarwal J, Blockley D, Woodman N. Vulnerability of structural systems. Struct Saf 2003;25:263–86.
[7] Barefoot CA, Entringer R, Swart H. Vulnerability in graphs – a comparative survey. J Comb Math Comb Comput 1987;1:13–22.
[8] Wikipedia – http://en.wikipedia.org/wiki/Reliability.
[9] Erdös P, Rènyi A. On random graphs. I. Publ Math 1959;6:290–7.
[10] Strogatz SH. Exploring complex networks. Nature 2001;410:268.
[11] Albert R, Barabasi AL. Statistical mehcanics of complex networks. Rev Mod Phys 2002;74:47.
[12] Dorogovtsev SN, Mendes JFF. Evaluation of networks. Adv Phys 2002;51:1079.
[13] Watts DJ. Small worlds: the dynamics of networks between order and randomness. Princeton, NJ: Princeton University Press; 1999.
[14] Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang D-U. Complex networks: structure and dynamics. Phys Rep 2006;424:175–308.
[15] Wasserman S, Faust K. Social networks analysis. Cambridge: Cambridge University Press; 1994.
[16] Bollobas B. Random graphs. London: Academic Press; 1985.

[17] Broder A, Kumar R, Maghoul F, Raghavan P, Rajagopalan S, Stata R, et al. Graph structure in the WEB. Comput Netw 2000;33:309.
[18] Crucitti P, Latora V, Marchiori M, Rapisarda A. Efficiency of scale-free networks: error and attack tolerance. Physics A 2003;320:622.
[19] Crucitti P, Latora V, Marchiori M, Rapisarda A. Error and attack tolerance of complex networks. Physics A 2004;340:388.
[20] Bollobas B. Modern graph theory, graduate texts in mathematics. New York: Springer; 1998.
[21] Biggs N. Algebraic graph theory. Cambridge University Press; 1993.
[22] Kirchhof F. Über die Auflösung der Gleichungen, auf welche man bei der Untersuchung der linearen Verteilung galvanischer Ströme geführt wird. Ann Phys Chem 1847;72:497–508.
[23] Chung FRK. Spectral graph theory. Providence, RI: American Mathematical Society; 1997.
[24] Cvetkovič DM, Doob M, Sachs H. Spectra of graphs, theory and applications. Heidelberg: Johann Ambrosius Barth Verlag; 1995.
[25] Merris R. Laplacian matrices of graphs: a survey. Linear Algebra Appl 1994;197:143–76.
[26] Mohar B. The Laplacian spectrum of graphs. In: Alavi Y, Chartrand G, Oellermann OR, Schwenk AJ, editors. Graph theory, combinatorics, and applications, vol. 2. Wiley; 1991. p. 871–98.
[27] Gutierrez E, Caperan P, Morris S. T.N.I.05.59, IPSC-JRC, European Commission. A case study in vulnerability analysis of high-voltage electricity transmission system from a sector of the European grid; July 2005.
[28] Petreska I, Tomovski I, Gutierrez E, Kocarev Lj, Bono F, Poljansek K. A modal analysis based approach in studying robustness and vulnerability of complex networks. In: Proceedings of the 2008 international symposium on nonlinear theory and its applications NOLTA'08, Budapest, Hungary, September 7–10, 2008. p. 253–6.
[29] Clough RW, Penzien J. Dynamics of structures. 3rd ed. Computers and Structures Inc; 1995.
[30] Chopra AK. Dynamics of structures – theory and application to earthquake engineering. In: Hall William J., editor. Prentice-Hall international series in civil engineering and engineering mechanics, ISBN 0-13-855214-2; 1995.