A modal analysis based approach in studying robustness and vulnerability of complex networks

Irina Petreska, Igor Tomovski [†], Eugenio Gutierrez [‡], Ljupčo Kocarev [†], Flavio Bono, Karmen Poljansek [‡]

†Research Center for Energy, Informatics and Materials,Macedonian Academy of Sciences and Arts,
bul. Krste Misirkov 2, P. O. Box 428, 1000 Skopje, Republic of Macedonia
‡European Laboratory for Structural assessment,
Institute for the Protection and Security of the Citizen, Joint Research Center, European Commission, Ispra, Italy
Email: irina@manu.edu.mk, igor@manu.edu.mk, eugenio.gutierrez@jrc.it, lkocarev@manu.edu.mk,
f.bono@jrc.it, karmen.poljansek@jrc.it

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

In the last few decades complex networks having irregular structure and heterogeneity have been subject to very active researches. Topology and statistical physics play the major role in structure analysis of complex networks. 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[1-7]. In several papers by *Albert et al.* error and attack tolerance of complex networks are studied and some general conclusions, further confirmed through many other real-life networks analyses[2] were made. 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[6]. 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, which is a novel approach. 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

In this section we present the main aspects of the methodology used to simulate attacks and analyze the changes in the network properties. Several different networks topologies were investigated and their attack vulnerability was analyzed. Vulnerability (or contrarily robustness) of a network refers to the ability of a network to avoid malfunctioning when a damage is caused, which means a fraction of its constituents is removed. Speaking with the language of topology, modeling damages and failures of complex networks can be performed by deleting vertices or edges.

The issue of vulnerability has been actively studied in the last few decades and significant conclusions have been derived. The first numerical studies on network robustness refer to the Internet and a sample of the World Wide Web [2, 8]. *Albert et al.* have studied how the properties of the mentioned networks change when a fraction f of the nodes is removed[2]. 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) [9,10]. 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.

In the present paper we investigate the vulnerability of several different topologies, simulating attacks by removing nodes according to their degree, betweenness centrality and modal weight. First we were concentrated on analysis of some generic networks, for which the modal analysis has not been applied so far, thus we generated networks according to the ER model (random graphs) and scale-free networks according to the BA model.

2.1. Methods to assess busyness of nodes and lines

As it was mentioned above, attacks are simulated by preferential removal of nodes and lines. The problem of establishing quantitative criterion to rank the nodes and links of a network and to model attacks by preferential removal is still open in the scientific community. Thus, from the point of view of the mathematical modeling of network vulnerability, it is of great importance to develop methods for assessing node and line busyness. In the literature several methods for this are pointed out. Usually, statistical measures such as closeness and betweenness centrality are utilized for busyness assessment. In our work, partially presented in this paper, an attempt to apply modal analysis for nodes and lines assessment and their ranking according to the busyness will be undertaken. Ranking based on the modal analysis will be compare to the ranking according to centrality measures. A brief theoretical background on the spectral and modal analysis is given in the paragraph below.

2.2. 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:

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

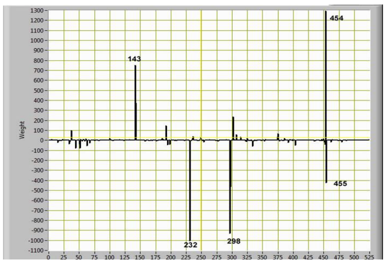

Figure 1: Nodal distribution of the modal weight for one of the possible modes obtained by the modal analysis

where $\mathbf{D}$ is a diagonal matrix whose elements are $D_{ii} = D_i$, where D_i stands for the degree of the corresponding node and $i = 1$ to n and $\mathbf{A}$ stands for the adjacency matrix[11].

Modal analysis, which is a method originating from structural dynamics, can be applied to assess the robustness of structures by analyzing oscillating modes. The idea to apply a similar approach to complex networks, was first introduced by *Gutierrez et al.* in a case study of vulnerability of a power grid segment [12]. We here give a brief mathematical background of the modal analysis. 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

$$\mathbf{\Gamma} = \mathbf{L}'\mathbf{\Phi} \tag{2}$$

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 $\gamma_{i,j}$, which represents the contribution of the j^{th} mode to the i^{th} node. Fig. 1 illustrates the nodal distribution of a particular mode for one of the considered networks.

Modal contributions to each node can now be determined as

$$w_i = \sum_{j=1}^{n} |\gamma_{i,j}|, \gamma_{i,j} \in \Gamma \tag{3}$$

for i=1 to 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. 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[13,14]

$$l_{i,j} = \sum_{k=1}^{n} |\gamma_{i,k} - \gamma_{j,k}| \tag{4}$$

3. Results and discussion

The modal analysis was first applied to random networks generated by Erdos-Renyi and Barabasi-Albert mod-

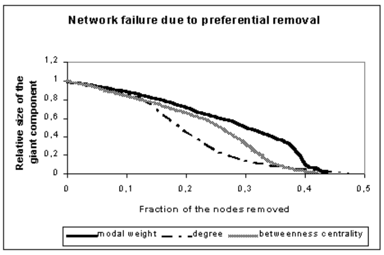

Figure 2: The dependence of the relative size of the giant component on the fraction of removed nodes for a random ER graph with 1000 nodes and average degree 3.5

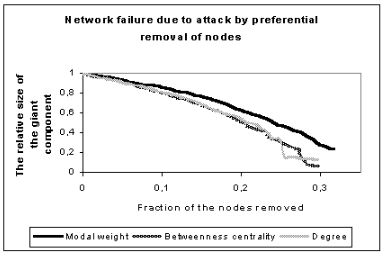

Figure 3: The dependence of the relative size of the giant component on the fraction of removed nodes for a random SF graph with 1000 nodes and average degree 3.5

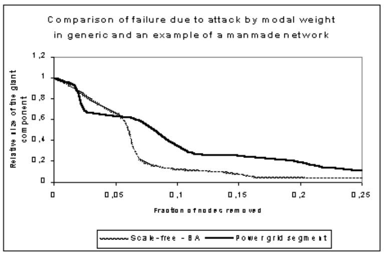

Figure 4: Attack vulnerability of a manmade network compared to an adequate generic BA graph, both networks has 524 nodes, average degree 3.5 and similar degree distribution

els. The latter represents scale-free networks that are usually a better description for real-life networks. Networks having 1000 nodes and average degree 3.5 and initially connected, were investigated. 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.

The rankings according to the node degree, betweenness centrality and modal weight were compared, which was further used to develop a strategy to simulate attacks on the networks. 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. Thus, we can conclude that there is no high correlation between these ranking criteria. However, we find that the modal weight of the nodes is 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. Therefore, we analyzed the vulnerability of complex networks by preferential removal of the nodes according to their modal weight and we compared the results with those obtained by preferential removal according to the standard measures.

We applied two different strategies to examine the attack vulnerability of the considered networks. First one, so called *non-adaptive strategy*, uses the initial ranking of the nodes, without recalculating the properties after a removal of a fraction of nodes. In the second *adaptive strategy*, the modal weight, as well as the betweenness centrality and nodes' degree were recalculated after each deletion of nodes, and the new ranking was utilized.

The dependence of number of clusters, the diameter and the relative size of the giant component on the fraction of deleted nodes was tracked in our simulation. 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. 2. The same analysis for the scale-free graph is given in the Fig. 3.

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.

The analysis was also applied to several examples of manmade networks, sectors of the European power grid were investigated from two perspectives. The first one was a basic topological analysis, which means the weights of the edges (power transmission lines) were neglected (set to one), and the second one involves also the weights of the lines. We here present the results from these investigations

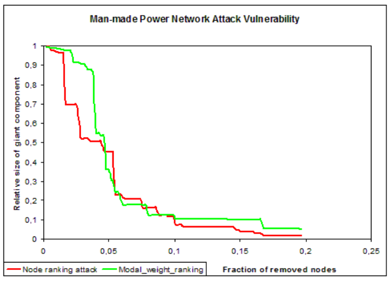

Figure 5: Attack vulnerability of a manmade network, simulated by an adaptive strategy, for unweighted graph, having 524 nodes and average degree of 2.4

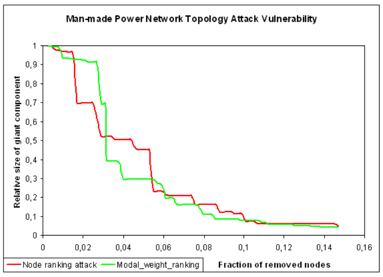

Figure 6: Attack vulnerability of a manmade network, simulated by an adaptive strategy, for weighted graph, having 524 nodes and average degree of 2.4

for only one of the considered sectors, since the results are rather similar. A non-adaptive strategy for a manmade network lead to the results, that are represented in comparison to those for an adequate BA scale-free network in Fig. 4, while the results obtained by the adaptive strategy are given in Fig. 5 and 6. As it is obvious from the presented analyses the modal weight based strategy could be an efficient method to disintegrate a manmade network by removing a small fraction of nodes (consider the range of the fraction of removed nodes between 0 and 0.06).

4. 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 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. A low correlation between the rankings according to the closeness and betweenness centrality and modal weight was found. 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 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] S. H. Strogatz, Nature 410 (2001) 268.

[2] R. Albert, A.-L. Barabasi, Rev. Mod. Phys.74 (2002)47.

[3] S. N. Dorogovtsev, J.F.F. Mendes, Adv. Phys. 51 (2002) 1079.

[4] D.J. Watts, Small worlds: The dynamics of Networks between order and randomness, Princeton University Press, Princeton, NJ, 1999.

[5] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.-U. Hwang, Complex networks: Structure and dynamics, Physics Reports 424 (2006) 175 - 308.

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

[7] B. Bollobas, Random Graphs, Academic Press, London, 1985.

[8] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, J. Wiener, Computer Networks 33 (2000) 309

[9] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Physics A 320 (2003) 622

[10] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Physics A 340 (2004) 388

[11] B. Bollobas, Modern Graph Theory, Graduate Texts in Mathematics, Springer, New York, 1998.

[12] E. Gutierrez, P. Caperan, S. Morris, 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

[13] Clough R.W, Penzien J, "Dynamics of Structures", Third Edition, Computers and Structures Inc, 1995.

[14] Chopra A.K. "DYNAMICS OF STRUCTURES - Theory and Application to Earthquake Engineering", Prentice-Hall International Series in Civil Engineering and Engineering Mechanics, Willliam J Hall - Editor, ISBN 0-13-855214-2, 1995.