# D4.3 Topological analysis of selected EU synchronous grid systems and report on risk and fragmentation analysis of EU grid networks

**SIXTH FRAMEWORK PROGRAMME**

**Project contract no. 043363**

**ManMade**
**Diagnosing vulnerability, emergent phenomena and volatility in man-made networks**

**SPECIFIC TARGETED PROJECT**
**NEST PATHFINDER**
**Sub-Priority Tackling Complexity in Science**

**Lead authors for this deliverable:**
**I. Mishkovski, I. Trpevski, A. Kanevce, L. Kocarev, L. Grcev, D. Trajanov**

**Start date of project: 1st of January 2007** **Duration: 36 months**

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)

Dissemination Level: Restricted to a group specified by the consortium (including the Commission Services)

# I. SUMMARY

This report deals with topological analysis of selected EU synchronous grid systems and report on risk and fragmentation analysis of EU grid networks. The report should consider the following tasks:

- T4.4 Topological analysis of EU synchronously connected electricity grids.
- T4.5 Modal analysis of selected of EU electricity grid sectors.
- T4.6 Network fragmentation studies of EU grid.

Since the above tasks have already been covered in other reports from and journal papers, see I. Petreska, I. Tomovski, E. Gutierrez, L. Kocarev, F. Bono, K. Poljansek, Application of modal analysis in assessing attack vulnerability of complex networks, Vol. 15, pages: 1008–1018, 2010, and I. Mishkovski, L. Kocarev, and M. Biey, Vulnerability of Complex Networks, Communications in Nonlinear Science and Numerical Simulation (submitted for publication), here we only briefly discuss a novel metric for vulnerability analysis of real networks. We argue that normalized average edge betweenness together with is relative difference when certain number of nodes and/or edges are removed from the network is a novel network vulnerability metric, called vulnerability index. Real-world networks for which vulnerability index is calculated include: two human brain networks, there urban networks, one collaboration network, and tow power grid networks. We find that WS model of small-world networks and biological networks (human brain networks) are the most robust networks among all networks studied in the report.

## II. INTRODUCTION

Different approaches to address network robustness and vulnerability have recently been proposed by research community. The first approach is related to structural robustness [1–5]: how different classes of network topologies are affected by the removal of a finite number of links and/or nodes. It was concluded that the more heterogeneous a network is in terms of, e.g., degree distribution, the more robust it is to random failures, while, at the same time, it appears more vulnerable to deliberate attacks on highly connected nodes. The second approach concerns dynamical robustness [6–9]. For networks supporting the flow of a physical quantity, the removal of a node or link will cause the flow to redistribute with the risk that some other nodes or links may be overloaded and failure prone. Hence, a triggering event can cause a whole sequence of failures due to overload, and may even threaten the global stability of the network. Such behavior is termed cascading failure.

In general, the vulnerability of complex networks can be either node or edge vulnerability. One method of measuring node vulnerability is proposed in [10]. Latora and Marchiori measure the vulnerability of a node $V(i)$ as relative drop in performance after removal of the $i-th$ node together with all the edges connected to it. Then they argue that the maximal value $V$ of $V(i)$ over all $i$ corresponds to the network vulnerability. As an addition to this, authors in [11] introduce an additional parameter called the relative variance $h$. This parameter is a measure of the fluctuation level and it is used to describe the hierarchical properties of the network, and thus its vulnerability.

In this report we consider the normalized average edge betweenness as a metric for network vulnerability. Recently a multi-scale measure for vulnerability of a graph is suggested by Boccaletti and his co-workers in [12]. In special case, when the multi-scale coefficient equals 1, it reduces to the average edge betweenness. We discuss relations of this metric to some graph characteristics. We also investigate how the normalized average edge betweenness fluctuates when certain nodes or edges are removed from the network. We measure the vulnerability of different real world networks: the Erdős collaboration network, logical network of the brain, physical network of the brain, and EU and US power grid networks. The same analysis is also carried out for three urban transport networks: Turin's, Milan's and London's road network.

## III. NETWORK VULNERABILITY

We consider networks that can be modeled as simple graphs. A graph is an ordered pair $G = (V, E)$ comprising a set $V$ of vertices or nodes together with a set $E$ of edges or lines, which are 2-element subsets of $V$. A simple graph is an undirected graph that has no loops and no more than one edge between any two different vertices. Average edge betweenness of the graph $G$ is defined as [12]:

$$b(G) = \frac{1}{|E|} \sum_{l \in E} b_l \tag{1}$$

where $|E|$ is the number of the edges, and $b_l$ is the edge betweenness of the edge $l$, defined as:

$$b_l = \sum_{i \neq j} \frac{n_{ij}(l)}{n_{ij}} \tag{2}$$

where $n_{ij}(l)$ is the number of geodesics (shortest paths) from node $i$ to node $j$ that contain the edge $l$, and $n_{ij}$ is the total number of shortest paths. The average edge betweenness of graph $G$ is related to the characteristic path length $L(G)$ as [12]:

$$b(G) = \frac{N(N-1)}{2|E|} L(G). \tag{3}$$

where $N$ is the number of nodes in the graph.

Recently a multi-scale measure for vulnerability of a graph is suggested in [12]:

$$b_p(G) = \left[ \frac{1}{|E|} \sum_{l \in E} {b_l}^p \right]^{1/|p|} \tag{4}$$

for each value of $p > 0$. In order to compare 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 $b_1(G) = b_1(G')$, then one takes $p > 1$ and computes $b_p$ until $b_p(G) \neq b_p(G')$. For typical (both synthetic and real) graphs $b_1(G) \neq b_1(G')$, so in the following we adopt $b_1(G) = b(G)$ as a measure of vulnerability.

We first evaluate $b(G)$ for some particular networks. A complete graph is a simple graph in which every pair of distinct vertices is connected by an edge. The complete graph on $N$ vertices has $N(N-1)/2$ edges. For a complete graph, we have $b(G_{complete}) = 1$. A path graph is a particularly simple example of a tree, namely one which is not branched at all, that is, contains only nodes of degree two and one. In particular, two of its vertices have degree 1 and all others (if any) have degree 2. For a path graph with $N$ nodes, $|E| = N - 1$, and therefore:

$$b(G_{path}) = \frac{N(N+1)}{6} \tag{5}$$

It is easy to see that $b(G_{complete}) \leq b(G) \leq b(G_{path})$. As a consequence, we can define normalized average edge betweenness of a network as:

$$b_{nor}(G) = \frac{b(G) - b(G_{complete})}{b(G_{path}) - b(G_{complete})} = \frac{b(G) - 1}{\frac{N(N+1)}{6} - 1}. \tag{6}$$

Clearly $0 \leq b_{nor}(G) \leq 1$; if normalized average edge betweenness is close to 0 it means that the network is more robust, when is close to 1, then network is more vulnerable.

We define two quantities related to average edge betweenness, namely relative difference of the average edge betweenness when a finite number of nodes are removed from the network as

$$D_{node}(G) = \frac{b_{nor}(G') - b_{nor}(G)}{b_{nor}(G)}, \tag{7}$$

where $G' = (V \setminus \{v_1, v_2, \ldots, v_m\}, E \setminus E_v)$ is graph obtained from $G$ by removing nodes $v_1, v_2, \ldots, v_m \in V$ and all edges incident to the nodes $v_1, v_2, \ldots, v_m$ (the set $E_v$). In a similar way, we define relative difference of the average edge betweenness when a finite number of edges are removed from the network as

$$D_{edge}(G) = \frac{b_{nor}(G') - b_{nor}(G)}{b_{nor}(G)}, \tag{8}$$

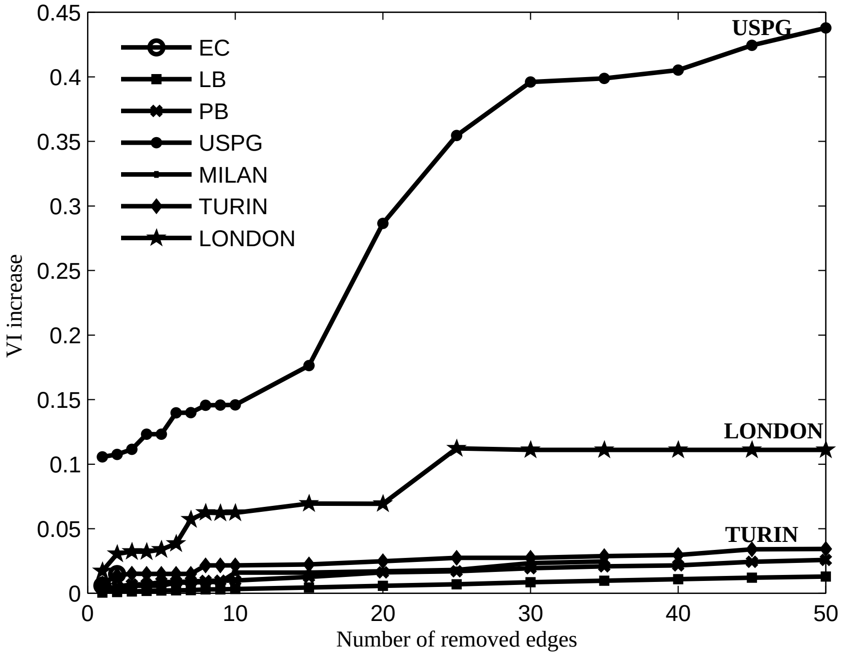

FIG. 1: Relative difference of the $b_{nor}$ after some of the edges are removed (using edge betweenness

where $G' = (G, E \setminus \{e_1, e_2, \ldots, e_n\})$ is graph obtained from $G$ by removing edges $e_1, e_2, \ldots, e_n \in E$. When using the equations (7) and (8) we assume that both networks $G$ and $G'$ are connected. There are two questions to be addressed when using the equations (7) and (8). The first one is how to choose nodes and edges to be removed? When removing a node (or an edge) from a network, one can remove a random node (edge) or a node which is the highest ranking node according to some ranking method, such as: PageRank [25], node degree, and node betweenness, or edge betweenness, when an edge is removed. The second question is how small or large the number of removed nodes (edges) should be? If $m, n$ are small (for example, $m = 1$ and $n = 1$), then the relative differences $D_{node}$ and $D_{edge}$ could be vary small numbers (statistically insignificant). On the other hand, for large $m$ and $n$ the network can be disconnected.

We think that the robustness and/or vulnerability of a network $G$ should be measured with the triple $(b_{nor}(G), D_{node}(G), D_{edge}(G))$. Thus, for example, the network is robust when all three quantities $b_{nor}$, $D_{node}$, and $D_{edge}$ are small. We call the triple $(b_{nor}, D_{node}, D_{edge})$ *vulnerability index* of the network.

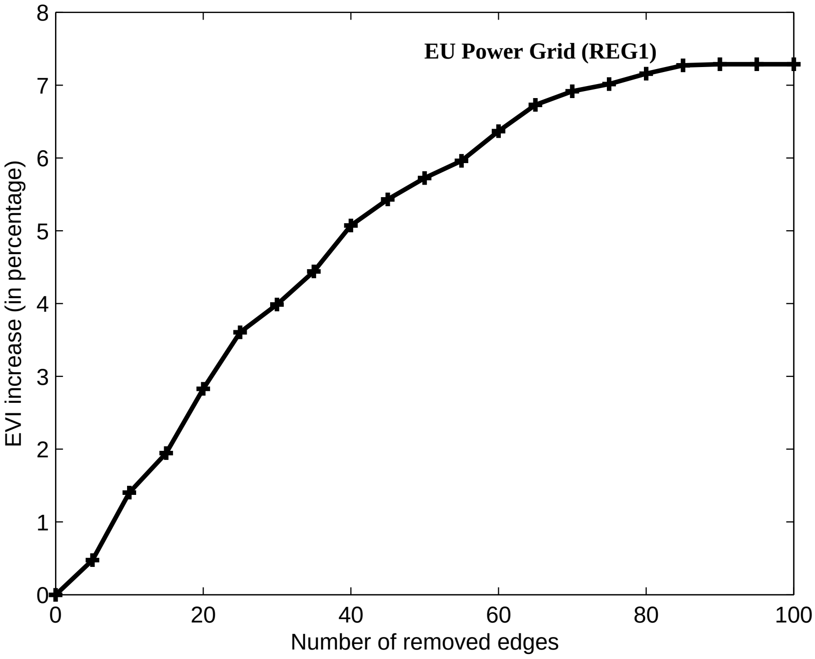

FIG. 2: Relative difference of the $VI$ after some of the edges were removed (using edge betweenness) for the region 1 of the EU Power Grid

## IV. VULNERABILITY INDEX FOR REAL NETWORKS

In this section we consider several real-world networks.

- Human brain network – It represents the structural connectivity of the entire human brain. The data are obtained by a diffusion magnetic resonance imaging (MRI) scan [24]. The network has two layers: physical and logical. The logical layer consists of connections in the gray matter in the brain, while the physical layer reflects the axonal wiring used to establish the logical connections. The logical brain network (LB) is consisted of 1013 nodes and 30738 edges whilst the average node degree is 30.343 and the average clustering coefficient is 0.456. The physical brain network (PB) is larger and it has 4445 nodes and 41943 nodes whilst the average node degree is 9.436 and the average clustering coefficient is 0.373.

- US power grid network – US power grid (USPG) network is provided in [27]. This network has 4941 nodes and 13188 edges. The average node degree is 2.669 and the clustering coefficient is 0.107.

- Collaboration network – As a collaboration network, we consider a network whose edges are the collaboration between Paul Erdős and other mathematicians. Erdős network [27] has 472 nodes and $2,628$ edges (collaborations). Additionally, the average node degree for this network is 5.568 and the clustering coefficient is 0.347.

- Urban transport networks – The transport networks are focused on the urban street networks in the towns: Turin, Milan and London. The urban network for Milan consists of 21553 nodes and 29980 edges (roads). The average node degree is 1.391 and the average clustering coefficient is 0.0231. The Turin network consists of 18147 nodes connected with 26120 edges. In addition, the average node degree for this network is 1.439 and the average clustering coefficient is 0.0193. The London network has 8518 nodes and 15495 edges. It has average node degree of 1.819 and average clustering coefficient of 0.0794.

- EU power grid network – The experimental dataset contains the electricity lines above 200kV grouped by disconnected regions: Main Europe, Nordic Countries, Ireland, and UK. In our simulations only region Main Europe is analyzed. For this networks, the number of nodes is 4335 and the network has 11102 edges. The average node degree is equal to 2.561 and the average clustering coefficient is equal to 0.0508.

| | $b_{nor}(G)$ | $D_{node}(G)$ | $D_{edge}(G)$ |
|---|---|---|---|
| PB | 0.0125 | 0.0011 | 0.002 |
| LB | 0.0165 | 0.0035 | 0.001 |
| EC | 0.042 | 0.1282 | - |
| Lo | 0.0366 | 0.0067 | 0.012 |
| Tu | 0.0040 | - | 0.03 |
| Mi | 0.0044 | - | 0.025 |
| USPG | 0.0231 | 0.0010 | 0.040 |
| EUPG | 0.0001 | 0.0801 | 0.004 |

TABLE I:

We calculate $b_{nor}(G)$, $D_{node}(G)$, and $D_{edge}(G)$ for all networks. The relative difference $D_{node}(G)$ is calculated when 10 nodes with the largest PageRank scores are removed from the network. The relative difference $D_{edge}(G)$ is calculated when 30 edges with the largest edge betweenness are removed from the network. The results are shown in Table I. Two networks with the largest normalized average edge betweenness $b_{nor}$ are EC and Lo, two networks with the largest $D_{node}$ are EC and EUPG, and two networks with the largest $D_{edge}$ are USPG and Mi. No data in the table means that the corresponding network is disconnected. Considering vulnerability index as a measure of network vulnerability, we may conclude that the most robust real-world networks are biological networks represented here with PB and LP networks. The increase of the normalized average edge betweenness when a certain number of edges are removed (using edge betweenness) is shown in Fig.1.

Figure 2 presents the trend-line of the relative increase of the edge vulnerability of the EU Power Grid, when some of the edges with the highest edge betweenness are removed. From the Fig. 2 one can see that by removing 100 of the most important edges the vulnerability index increases by around 7%. In addition, the vulnerability increases with the same trend when removing from 5 to 70 edges, then in the range between 70 and 100 edges it increases with a smaller rate. From this analysis we might conclude that the first 70 edges with the highest edge betweenness value influence the vulnerability of the EU power grid the most.

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

[2] R. Albert, A. L. H. Jeong, and A.-L. Barabasi, Nature (London) 406, 378 (2000).

[3] D. J. Watts, Proc. Natl. Acad. Sci. U.S.A. 99, 5766 (2002).

[4] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Phys. Rev. E 65, 056109 (2002).

[5] R. Albert, I. Albert, and G. L. Nakarado, Phys. Rev. E 69, 025103(R) (2004).

[6] A. E. Motter and Y.-C. Lai, Phys. Rev. E 66, 065102(R) (2002).

[7] A. E. Motter, Phys. Rev. Lett. 93, 098701 (2004).

[8] P. Crucitti, V. Latora, and M. Marchiori, Phys. Rev. E 69, 045104(R) (2004).

[9] L. Huang, L. Yang, and K. Yang, Phys. Rev. E 73, 036102 (2006).

[10] V. Latora and M. Marchiori, “Vulnerability and protection of critical infrastructures”, Physical Review E 71, 015103(R) (2005)

[11] V. Gol’dshtein, G. A. Koganov, and G. I. Surdutovich, “Vulnerability and hierarchy of complex networks”, cond-mat/0409298, 2004.

[12] S. Boccaletti, J. Buldu, R. Criado, J. Flores, V. Latora, J. Pello, and M. Romance, “Multi-scale vulnerability in complex networks”, Chaos 17, 043110, 2007.

[13] D. J. Watts and S. H. Strogatz, Nature 393, 440, 1998.

[14] A.-L. Barabasi and R. Albert, R., “Emergence of scaling in random networks”, Science, 286:509-512, October 15, 1999

[15] Freeman, L. C. Centrality in social networks: Conceptual clarification. Social Networks 1, 215-239, 1979.

[16] J. von Neumann, O. Morgenstern, Theory of Games and Economic Behavior. Princeton University Press, 1944.

[17] Fronczak, A., Fronczak, P., Holyst, J. A., July 2004. Average path length in random networks. URL http://arxiv.org/abs/cond-mat/0212230.

[18] L. A. N. Amaral, A. Scala, M. Barthe lemy, H. E. Stanley, Classes of small-world networks, PNAS 97:11149-11152

[19] M. Jalili, A. Ajdari RAd, and M. Hasler, International Journal of Circuit Theory and Applications 35, 611, 2007.

[20] Mathew Penrose: Random Geometric Graphs, Oxford University Press, New York, 2004.

[21] Michael Karonski and Adrzej Rucinski: The Origins of the Theory of Random Graphs, The Mathematics of Paul Erdos, Berlin, Springer, 1997.

[22] Mohar B., ”Eigenvalues, diameter and mean distance in graphs”, Graphs Comb. 7, 53-64, 1991.

[23] P. Bork et al. ”Protein interaction networks from yeast to human”, Current Opinion in Structural Biology, 14(3):292-299, 2004.

[24] P. Hangmann, M. Kurant, X. Gigadent, P. Thiran, V. J. Weeden, R. Meuli and J. P. Thiran, “Mapping Human Whole-Brain Structural Networks with Diffusion MRI,” Plos ONE, 2007.

[25] S. Brin and L. Page, ”The anatomy of a large-scale hyper- textual Web search engine”, Proceedings of the 7th inter-national conference on World Wide Web 7, 107, 1998.

[26] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill, 2001. ISBN 0-262-03293-7. Chapter 1: Foundations, pp.3-122.

[27] http://www.cise.ufl.edu/research/sparse/matrices/Pajek/.