Power Grids' Dynamic Enlargement Calculus Using Petri Nets

Radu MUNTEANU[1], Vasile DUB[2]
[1]*Technical University of Cluj-Napoca,Romania*
[2]*Petru Maior University of Tirgu-Mures, Romania*
dub_laci@yahoo.com

***Abstract*—The robustness of power grids characterizes the behavior of grids in situations of serial failures and/or human errors. A coherent method of evaluating vulnerability is to quantify this attribute in terms of the scale-free graph theory. One way of increasing power grid robustness consists of adding new electric lines between the existing nodes. Once the target scale-free network is found, the real network must be enlarged to the graph of the target network. The choice of a reasonable solution is made difficult by the great number of topological solutions, because this number increases as the number of the network nodes becomes bigger. Thus, the first aim is to make an inventory of all these solutions. The second necessary step is to build correct algorithms able to find the nodes of the real grid which will be connected respecting economical criteria. In continuation of our previous research, our paper proposes a Petri net-based method of building all enlargement variants, starting from non-robust networks to the nearest free-scale, robust network. Starting from some distinctive characteristics of elementary enlargements introduced in our earlier works, this allows us to obtain a mathematically unique, robustness-oriented enlargement solution.**

Index Terms—**topological vulnerability, Petri nets, power grids, scale-free graphs.**

I. INTRODUCTION

We begin with a short presentation of the topological description of the networks. The basics of PN are exposed in the Appendix with the purpose of understanding our Petri nets (PN) model of network enlargement dynamic.

I.1 Graphs' topological quantifiers

The main elements used to describe large systems by their graphs are presented in [1],[2].

The graphs' quantifiers used in our paper are the following:

- The nod's degree *k*, which is an indicator of how many links the node has to other nodes.

- The degree distribution *P(k)* representing the probability that a selected node has exactly *k* links:

- The critical fraction f_C quantifies the robustness of the network faced with random series of removed nodes (random attacks). The result of these complex events is a strong reduction of the grid dimension, by the appearance of giant clusters, [1], [3], [4], characterized by high dimension in contrast to other clusters. In our paper, the power flow processes are neglected, the target being the static robustness, in opposition to the dynamic robustness thoroughly presented in [5]. The power flow approach leads to finding the most critical components in a network, by analytical or topological methods.

A suggestive illustration of the difference between a topological (nearest-neighbor) model of cascading failure [6] and one based on Kirchhoff's laws is presented in [7]. So, in a topological approach, the clusters formation, known as percolation, is the main event in the random (or intentional) destroying dynamics 8], and it has been the subject of many mathematical studies. An accepted criterion in determining the percolation threshold in the destroying process dynamics is when: $c = <k^2> / <k> \to 2$. The critical fraction f_c^{theor}, representing the deleted nodes' percentage producing the percolation, is defined and computed in [2]. For one ordinary graph described by its probability function $\begin{pmatrix} k \\ P(k) \end{pmatrix}$, the f_c value is:

$$f_c^{theor} = 1 - \frac{1}{\frac{<k^2>}{<k>} - 1} \tag{1}$$

where $<>$ is the average symbol.

Unlike the theoretical critical fraction, the real critical fraction f_c^{theor} is evaluated by random destroying experiences.

A special random graph class is the scale-free (SF) *s* graphs, with a power law degree distribution:

$$P(k) = Ak^{-b}, \quad k = m, m+1, ..., K \tag{2}$$

Observe that in logarithmic coordinates, (2) is a straight line.

If $2 < b < 3$ we estimate the critical threshold f_c with :

$$f_c = 1 - \frac{1}{2b-1} \tag{3}$$

In addition, for SF graphs, $c = b/2$

Note that the smaller the network's *N* node number, the bigger the error between the theoretical and the empirical values of f_c is. The reason is that by using such formulae as (1) and (3), for $K >> m$, *k* is considered as a continuous variable. In [9], the authors make a difference between the theoretical and the real values of the critical fraction in the analysis of some European power grids.

On the other hand, the SF graphs "steady" properties have a relevant sense [10], examining their evolution as random processes. What is random in the power grids' enlargement? The mathematical approach to the random graphs offers other very attractive models of the real networks: in [11], the presented Watts–Strogatz network model describes networks between a regular network and a random one. The last is defined in a particular manner, allowing the modeling

Digital Object Identifier 10.4316/AECE.2011.02012

of different random behaviors, one of them conducting to the SF graphs. A very simple node-addition algorithm, presented in [12], [13] and used in [14], allows us to build SF graphs: starting with a small sized initial graph, a new node with *k* edges is added step-by-step in such a way that the probability to be connected to an existing node is proportional to the connection degree of this node, thus we establish a preferential attachment with the highest connected nodes. But in power grids, we follow the similar idea, because it makes no sense to introduce low connected new nodes and, at the same time, assure an elevated reliable power flow for the enlarged network, thus at first sight, the power grids should become SF graphs.

II. Networks Enlargements by New Edges Addition

The networks' extension policy can assume various targets: a reliability approach, [15], or, the power flow growth for some customers, all these with the purpose of reducing the network vulnerability facing random failure events. Thus, the first step is the risk assessment of power grids. The reliability approach is focused on a few well-defined points of the network. A very interesting and necessary enterprise is to identify the quantitative equivalences between the reliability and the topological approach. In [15], the reliability of electric transmission systems is analyzed in terms of the topological properties of scale-free graphs, and failure propagation. A power system reliability index is compared to the scale-free network models robustness-derivate quantifiers. The topological approach is very attractive, because it can reveal relevant properties of the structure of a power grid, emphasizing the role played by its components, role which escapes a local, reliability centered analysis and offers the instrument to perform vulnerability assessments based on the simulation of random or intentional faults [15]. In [16], the authors present two extension algorithms to generate the minimum distance graph, in terms comparable with our works, but using the bisection technique by introducing the bisection cost parameter .and maintaining the grid's exponential degree distribution character. In [17] it is emphasized that in critical infrastructure systems, such as electric power grids, there is a significant influence on the network structure of the new links. In order to measure the power networks vulnerability, the response of networks is tested in a variety of disturbance scenarios, measuring the relationship between the disturbance size and the economic aspect of the disturbances [18].

In our paper we assume that the enlargement is performed only by new connections, and in addition, we change the exponential degree distributions to a desired SF distribution. To this purpose, we will model the extension process by dedicated Petri nets, associated with vulnerability quantifiers introduced in Section I.

We consider a network graph with the empirical degree distribution $P^0(k)$.

Thus we must obtain the objective graph G^F, from the initial G^0 graph of the studied power grid.

Let the initial network and its graph G^0 histogram be:

$$G^0\begin{bmatrix} i \\ N_i \end{bmatrix} = \begin{bmatrix} k & k+1 & \dots & i & \dots & j & \dots & K \\ N_k & N_{k+1} & \dots & N_i & \dots & N_j & \dots & N_K \end{bmatrix} \tag{4}$$

An elementary enlargement [19] is made by adding a single new edge, denoted by the operation:

$$G^{r+1} = e_{ij}(G^r),\ k \le i \le j \le K \tag{5}$$

where:

- G^r, G^{r+1} are two successive graph histograms;
- e_{ij} - connection of one nodes with *i* edges with the other one, with *j* edges.

The new graph's histogram will be:

$$G^{r+1} = \begin{cases} \begin{bmatrix} k \dots\dots i. & i+1 \dots\dots\dots j & j+1 \dots\dots\dots\dots K \\ N_k \dots N_i - 1 & N_{i+1} + 1 \dots N_j - 1 & N_{j+1} + 1 \dots N_K \end{bmatrix} & if\ \ j > i+1 \\ \begin{bmatrix} k \dots\dots\dots i\ . & i+1 & i+2 \dots\dots\dots\dots K \\ N_k \dots N_i - 1 & N_{i+1} & N_{i+2} + 1 \dots . N_K \end{bmatrix} & if\ \ j = i+1 \\ \begin{bmatrix} k \dots\dots\dots i & i+1 & \dots\dots\dots K \\ N_k \dots N_i - 2 & N_{i+1} + 2 & \dots\dots N_K \end{bmatrix} & if\ \ j = i+1 \end{cases} \tag{6}$$

Thus, one edge removal between a node with *i* edges and another one, with *j* edges is defined, according to (5), as a negative enlargement "$-e_{ij}$". Of course, this operation can be made only if there is a connection between the selected nodes.

A. *Properties of elementary enlargements:*

We attach critical fractions f_c^r and f_c^{r+1} to G^r and G^{r+1}:

Prop.1 We accept as obvious for any enlargement that:

$$f_c^{r+1} \ge f_c^r \tag{7}$$

Prop.2 Let $m \le x, y, z, t \le K$. Hence, there are equivalence relationships between distinct elementary extensions pairs:

$$e_{xy} + e_{zt} = e_{xz(t)} + e_{yt(z)} \tag{8}$$

There is a S_{eq} system of n_{eq} distinct, (8)-form equations. For $K - m > 3$,

$$n_{eq} = \begin{pmatrix} 2 \\ K - m + 1 \end{pmatrix} + 2\begin{pmatrix} 4 \\ K - m + 1 \end{pmatrix} \tag{9}$$

Prop.3 The number $\boldsymbol{z}$ of the linear independent elementary extensions is:

$$z = rank(S_{eq}) \tag{10}$$

According to the convention for the signs associated to the elementary enlargements, in (8) we can move the terms following usual algebraic rules.

III. Analyzing The Power Grid's Vulnerability

There are more approaches to the power grids' vulnerability evaluation, depending on the risk source [20], [21]. Here, our approach is based on the terms of the SF graph theory. The proposed network is the IEEE-30 bus system, and our choice is motivated by the adequacy of the network dimension to some networks studied in [22]. The relatively small sized dimension is imposed with the purpose of illustrating the enlargement process by a tolerable complexity of the Petri net coverability tree. In Fig.1, the transformers are not explicitly figured, therefore the buses' voltage can be different (i.e. 110 kV, 220kV): also, performing the random destroying experiences to find the empirical value for the critical fraction, no differences were observed between generator nodes and the other nodes of the network. The single line diagram of the IEEE 30-bus test system [23] is shown in Fig. 1

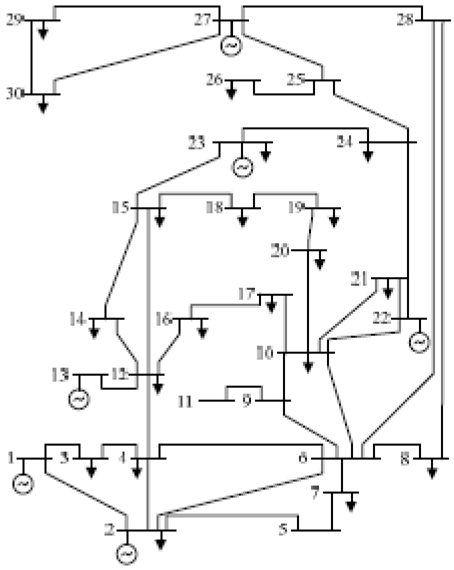

Figure 1. The IEEE 30-bus test system

The network's degree distribution and histogram are:

$$G^0 \equiv \left| \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 16 & 6 & 3 & 0 & 1 & 1 \end{matrix} \right| \tag{11}$$

The graph's quantifiers are: $c = 3.081$, $f_c^{theor} = 0.51$, $f_c^{real} = 0.27$. By representing *log(N(k))*, which in logarithmic coordinates has a similar form as *log(N(k))*, it is obvious that the analyzed network is not SF (Fig.2): we must eliminate the 1-edge connected nodes, build 5- edge connected and increase 2-edge connected node number.

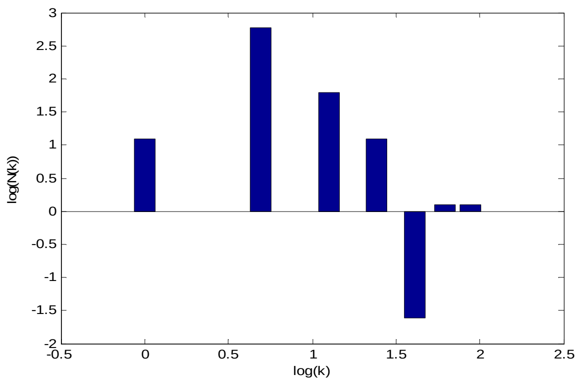

Figure 2. The graph's degree distribution

By imposing a needed $f_c^{theor} \geq 0.65$, a target degree distribution, obtained by a linear regression method is found:

$$G^F \equiv \left| \begin{matrix} 2 & 3 & 4 & 5 & 6 & 7 \\ 11 & 8 & 5 & 3 & 2 & 1 \end{matrix} \right| \tag{12}$$

The new graph's quantifiers are: $c = 3.92$, $f_c^{theor} = 0.66$, and an expected $f_c^{real} = 0.42$.

IV. The Solvability of the Problem

Thus, we intend to transform G^0 in G^F ($G^0 \to G^F$) by adding new edges, keeping the nodes' number constant. Observe that for any real network's histogram, we have:

$$\sum_{i=m}^{K} iN_i^0 = 2L^0 \tag{13}$$

where L^0 is the vertices' number. Therefore, the sum is always an even number. We will nominate this (4) form matrix as graph matrix (GM).

We associate to G^0 and G^F a Petri net (PN) with the subsequent structure: the P set of places: $P = \{p_m, p_{m+1}, ..., p_K\}$; the T set of transitions: $T = \{t_{m,m}, t_{m,m+1}, ..., t_{K,1,K-1}\}$; the W function of arcs' weight: $w(p_i, t_{i,i}) = 2$, $w(t_{ii}, p_{i+1}) = 2$, else, $w_{ij} = 1$, according with the elementary enlargement definitions (6).

The maximal indices for the transition set was limited to K-1 so as not to generate nodes with edge number over *K*

The PN's states, as the places' marking, are equal to the second row G_{II}^F of the successive $G^r \big|_{r=1:(L^F - L^0)}$, the initial state being $M_0 = G^0(2,:)$

The transitions must have the same task as the elementary transitions defined by (6):

$$t_{ij} \equiv e_{ij}, \; i = 2:5 \tag{14}$$

With these notes, we affirm that:

If G^0 and G^F are GM - form, in *the previously defined PN, there is always a transition set conducting from G^0 and G^F, or more precisely, G^F is always accessible from G^0.*

Proof:

Without reducing the generality of our proof, we consider G^0 and G^F as:

$$G^{0(F)} = \begin{bmatrix} 1 & 2 & 3 \\ N_1^{0(F)} & N_2^{0(F)} & N_3^{0(F)} \end{bmatrix}$$

The associated PN is depicted in Fig. 3:

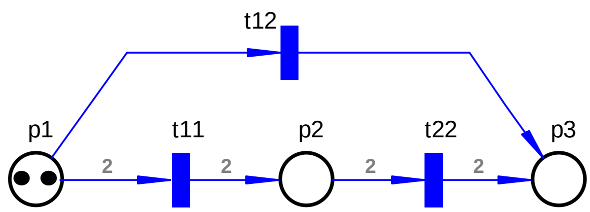

Figure 3. The PN for the accessibility proof

The PN's incidence matrix A and the $\Delta M = M^F - M^0$ are:

$$A = \begin{bmatrix} -2 & 2 & 0 \\ 0 & -2 & 2 \\ -1 & 0 & 1 \end{bmatrix}, \; \Delta M = \begin{bmatrix} N_1^F - N_1^0 \\ N_2^F - N_2^0 \\ N_3^F - N_3^0 \end{bmatrix}$$

We have successively:

$rank(A^T) = 2$,

$$\left[A^T \ \Delta M\right] = \begin{bmatrix} -2 & 0 & -1 & N_1^F - N_1^0 \\ 2 & -2 & 0 & N_2^F - N_2^0 \\ 0 & 2 & 1 & N_3^F - N_3^0 \end{bmatrix}$$

Let us check the rank of the matrix having any two columns of A^T and the ΔM . By adding the matrix rows, we will obtain only zeros, because $\sum_i N_i^F = \sum_i N_i^F$, hence $rank\left(\left[A^T \ \Delta M\right]\right) = 2$, satisfying the accessibility condition (A.2).

V. Application: Building The Petri Net- Model of The Enlargement Dynamics

We will return to model the IEEE 30-bus test system enlargement with a PN built in accordance with section IV. Thus:

- The places of this PN will be associated with the nodes' number having k connections. Thus, the number of the places will be: $n = K - m + 1$. The initial state M_0 is associated with the starting network's graph G^0 and we expect to find in the proposed PN the state M^F corresponding to the target graph G^F, so as to have: $M_F(p_k) = G_{II}^F(k), k = m : K$. The M_F is not necessary a deadlock state.

We assume we will not use negative enlargements:

At first sight, according to (9), (10) we can build two distinct type of PNs:

a) with *z* transitions; b).with $|E|$ transitions.

The main differences is the convergence mode from G^0 to G^F: if we opt for b), knowing $z < |E|$, the simultaneous transition conflict solving becomes decisive.

Thus, we will choose the a) variant. Also, to reduce the coverability tree dimension, the first three enlargements steps are chosen in the beginning: e_{11}, e_{14} and e_{22}, and in the same line, observe that the 7-edge nodes number must not be affected: thus, the initial and the final state marking will be: $M_0(17,8,2,1,1)$, $M_F(11,8,5,3,2)$, so we will work with a PN having : $P = \{p_2, p_3, p_4, p_5, p_6\}$.

The proposed PN is shown in Fig. 4:

The accessibility condition (A.2) is satisfied, because:

$$rank(A^T) = rank([A^T][M_F - M_0]^T) = 4$$

The PN's dynamic is described by the coverability tree from where we will retain some ways conducting from M_0 to M_F, (Fig. 5). Here, the boxes are the states of the enlargement process and the labels of the edges are, in accordance with the enlargement-transition equivalence (14), the elementary enlargement indices.

The proposed PN's state capacities were fixed to have $K(p_{4,5,6}) = G_{II}^F(k = 4,5,6)$, and for p_2 and p_3, to assure the PN's repetitiveness property, thus:

$$K(p_2) = 19, K(p_3) = 14, K(p_4) = 5,$$
$$K(p_5) = 3, K(p_6) = 2$$

To obtain the solutions containing all the elements of $T = [t_{22}, t_{23}, t_{24}, t_{25,} t_{34}, t_{35}, t_{45}]$, we would start from a PN with $z = 7$ independent transitions (9). In our example, for space economy, we will reduce the T set of transitions, renouncing t_{45}, thus we will have a 6-transition PN. Note that a PN with all the elements of T produces a coverability tree with 193 state, the target states having the label 185; Therefore, reducing the T set elements number, we'll obtain less complex coverability trees,. but with the price to lose the trajectories containing the eliminated transitions.

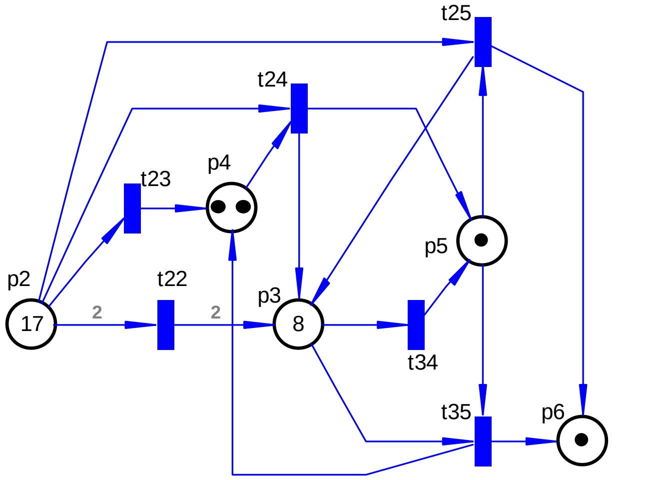

Figure 4. The 6-transition PN

In Fig.5, we present only a section of the entire coverabily tree. Here, the signification of the edges' label, according to (14), is: $label \equiv t_{label}$

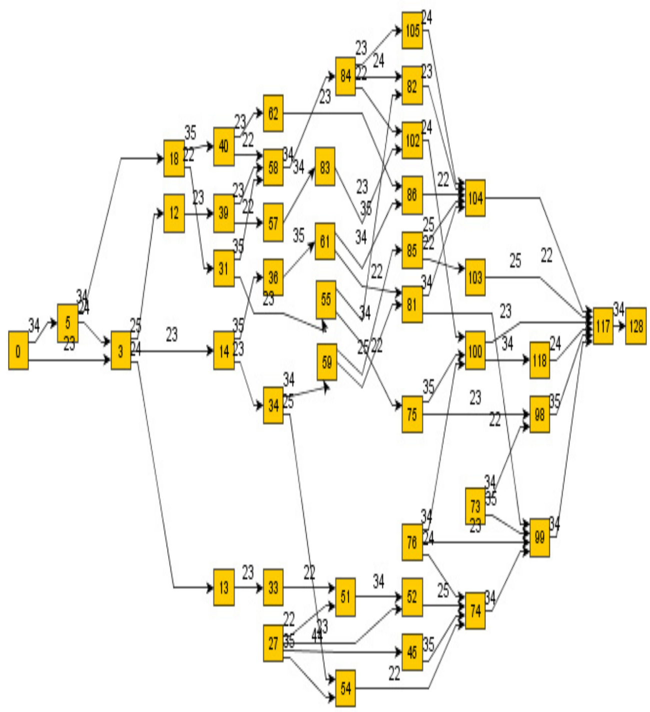

Figure 5. A partial coverability tree view for the 6-transition PN

The $M_n, n = 1:128$ states legend is presented in Table I:

Now, for all the states of table I, we add the theoretical critical fraction computed with (1) to the coverability tree.

For purposes of space saving, we will do it only for the predecessor states of the 117 labeled state (Table II).

In this way, we have the essential information based on which to choose the optimal enlargement trajectories.

TABLE I - THE STATES'LABEL LEGEND

S	**P2,3,4,5,6**	**S**	**P2,3,4,5,6**	**S**	**P2,3,4,5,6**
0	17 8 2 1 1	51	12 11 5 0 1	83	14 8 2 3 2
3	16 8 3 1 1	52	12 10 5 1 1	85	14 6 5 3 1
5	17 7 2 2 1	54	13 9 5 0 2	86	15 5 5 5 2
12	15 9 3 0 2	55	14 8 3 3 1	98	11 10 4 3 1
13	15 9 4 0 1	57	14 9 2 2 2	99	11 10 5 1 2
14	15 8 4 1 1	58	15 7 3 2 2	100	12 9 4 2 2
15	16 7 3 2 1	59	14 7 5 2 1	102	13 8 3 3 2
18	17 6 2 3 1	61	15 6 5 1 2	103	12 8 5 3 1
27	13 10 4 1 1	62	16 5 4 2 2	104	13 7 5 2 2
31	15 8 2 3 1	64	17 4 3 3 2	105	14 6 4 3 2
33	14 9 5 0 1	73	11 11 4 2 1	117	11 9 5 2 2
34	1 4 8 5 1 1	74	11 11 5 0 2	118	12 8 4 3 2
36	15 7 5 0 2	75	12 10 3 3 1	128	**11 8 5 3 2**
39	16 7 2 2 2	76	12 10 4 1 2		
40	17 5 3 2 2	81	13 8 5 1 2		
45	11 12 4 1 1	82	14 7 4 2 2		

TABLE II THE CRITICAL FRACTIONS OF SOME FINAL STATES

State No	98	99	100	103	104	118
f_c^{theor}	0.633	0.636	0.641	0.636	0.644	0.664

In our example, with the exception of 118, the state 104 is the best predecessor of 117. We immediately obtain relevant information: we can practically stop the enlargement arriving in 104, thus reducing the new connections' number by two.

Thus, the convenient solutions from *0* to *128* labeled states are trajectories such as:

- $M_0, M_5, M_{18}, M_{40}, M_{62}, M_{86}, M_{104}, M_{117}, M_{128}$
- $M_0, M_3, M_{14}, M_{34}, M_{59}, M_{85}, M_{104}, M_{117}, M_{128}$

or the associated enlargement sets:

$E_1 = \{e_{11}, e_{14}, e_{22}, e_{34}, e_{34}, e_{35}, e_{23}, e_{23}, e_{22}, e_{22}, e_{34}\}$,

$E_2 = \{e_{11}, e_{14}, e_{22}, e_{23}, e_{23}, e_{23}, e_{34}, e_{25}, e_{25}, e_{22}, e_{34}\}$

In the case of the IEEE 30-bus test system, the first solution may be in join nodes 11 and 26 for t_{11}, join nodes 1 and 10 , for t_{14}, etc., all the enlargement being applied to the successively modified power grids.

The final enlargement solution depends on the cost matrix of all the new possible connections of the IEEE 30-bus test system.

VI. CONCLUSION

The ideas presented in our paper offers an attractive tool to find enlargement solutions of a vulnerable network to the nearest robust network. The first advantage of this algebraic method is to answer the question of accessibility analysis of the target grid. One of advantages of the Petri nets' used in the graphs' enlargement strategies study is that instead of computing them; we have a comprehensive presentation of all the solutions of the problems, by a suggestive graphical diagram of the enlargement process. Another advantage is the possibility of choosing the elementary enlargement set in which we would solve the enlargement process. Based on the coverability tree inspection, the enlargement process can be stopped before realizing the theoretical scale-free character, by attaching the critical fraction value to the coverability tree. Therefore we can formulate criteria for optimal enlargement solutions, with the purpose of reducing the choice space of economically eligible variants.

APPENDIX A

Petri nets (PNs)

PNs (defined by Petri in 1962) is a graphical tool, mathematically based on matrix algebras. Classical PNs are identified by a quintuple (P, T, F, W, M_0), in which:

- $P = \{p_1, p_2, ..., p_m\}$ is the set of places;
- $T = \{t_1, t_2, ..., t_n\}$ is a set of transitions;
- $F \subseteq (P \times T) \cup (T \times P)$ is a set of arcs;
- $W : F \rightarrow (1,2,3,...)$ is the arcs' weight function;
- $M_0 : P \rightarrow (0,1,2,3,...)$ is the initial mark

Mathematically, a PN is a directed bipartite graph with two different types of nodes called *places* and *transitions*. The nodes are connected through directed *arcs*. Input places are a set of places that can fire a transition, while output places are a set of places that are associated with the results (outputs) from a transition. Only the static properties of a system are presented by a PN structure and dynamic system properties result from PN execution. The execution of a PN may affect the number of tokens in a place. A transition is called *enabled* when each of its input places has enough tokens. A transition can be *fired* only if it is enabled. When a transition is fired, tokens from input places are used to produce tokens in output places.

A PN with all arcs' unitary weight is an ordinary PN.

A 1-bounded PN is a safe-called PN.

A. Transition enabling rule

A transition t_j is said to be enabled in a marking M if and only if $M(p_i) \geq w(p_i, t_j)$ for all p_i, elements of the t_j's input places set.

B. Transition firing rule.

Only an enabled transition can be fire.

The firing execution of t_j has as effect the remove of $W(p_i, t_j)$ tokens from all input places of t_j and add $W(t_j, p_i)$ tokens to every output places of t_j.

C. The state equation

Any PN can be specified in matrix form as incidence matrix A, $A = A^+ - A^-$, with *m* rows and *n* columns, where *m* is the number of *transitions* and *n* is the number of *places* in the PN, and:

- $a_{ij}^+ = W(t_i, p_j)$ is the weight of the arc from t_i to its output place p_j;
- $a_{ij}^- = W(p_j, t_i)$ is the weight of the arc to t_i from its input place p_j;

We consider two M_0 and M_d states of a PN dynamics, consisting of a succession of states from an initial M_0 to a

M_d marked, present state. A state is defined by a line matrix containing the places' instantaneous marking. That dynamics can be described by the matrix equation:

$$M_d = M_0 + A^T X \qquad \text{(A.1)}$$

where X is the possible firing number matrix.

The necessary, but insufficient accessibility condition is the subsequent equality:

$$rank(A^T) = rank([A^T][M_n - M_0]^T) \qquad \text{(A.2)}$$

For further information, please consult [24], [25].

References

[1] R Albert, A. L Barabási , "Statistical mechanics of complex networks", in Reviews of Modern Physics, volume 74, January, 2002, pag.47-97.

[2] A. L Barabasi, E. Ravasz, T. Vicsek, "Deterministic Scale-Free Networks", in Physica A 299, (3-4) (2001), pp. 559-564.

[3] R. Cohen, S. Havlin, D. Avraham, "Structural Properties of Scale-Free Networks", WILEY-VCH Verlag Berlin GmbH, August 18, 2002.

[4] D. S. Callaway, M. E. J. Newman,2,3 S. H. Strogatz, and D. J. Watts, "Network Robustness and Fragility: Percolation on Random Graphs", in Physical Review Letters, volume 85, number 25 , 2000, Pages 5468-5471.

[5] A. Pinar, J. Meza, V. Done, B. Lesieutre, "Optimization strategies for the vulnerability analysis of the electric power grid", in SIAM J. OPTIM. Society for Industrial and Applied Mathematics, Vol. 20, No. 4, pp. 1786–1810.

[6] L. Zhao, K. Park, Y.C. Lai1, "Attack vulnerability of scale-free networks due to cascading breakdown", in PHYSICAL REVIEW E 70, (2004), , Pages 035101-4.

[7] P. Hines, S. Blumsack, E. Cotilla Sanchez, C. Barrows, "The Topological and Electrical Structure of Power Grids," in HICSS, pp.1-10, 2010 43rd Hawaii International Conference on System Sciences, 2010.

[8] S.Arianos, E.Bompard, A.Carbone, F.Xue, "Power grids vulnerability: a complex network approach", in Chaos 19, 013119 (2009), DOI: 10.1063/1.3077229, pages 1-16.

[9] R.V. Solé, M. Rosas-Casals, B.Corominas-Murtra,1 and S. Valverde, "Robustness of the European power grids under intentional attack",in Physical review e 77, 026102 _2008, pp. 026102-2-7.

[10] P Crucittia, M. Marchioric, A. Rapisarda, "Efficiency of scale-free networks: error and attack tolerance", in Physica A, Volume 320, 15 March 2003, Pages 622-642.

[11] Y. W. Chen1, L F Zhang1,J P Huang1, "The Watts–Strogatz network model including degree distribution: theory and computer simulation," in J. Phys. A: Math. Theor. 40 (2007), Pages 8237–8246.

[12] Albert-László Barabási , "Linked: The New Science of Networks:" Perseus Publishing, April 2002.

[13] H. Wang, Y. Guo, "Consensus on scale-free network", in Proceedings of the American Control Conference,Washington, USA, 2008, Pages 748-752.

[14] B. J Kim, C. N. Yoon , S. K. Han, H Jeong, "Path finding strategies in scale-free networks" in PHYSICAL REVIEW E, VOLUME 65, 2003, DOI: 10.1103/PhysRevE.65.027103, Pages 65 027103-1-4.

[15] D P. Chassin, C. Posse "Evaluating North American electric grid reliability using the Barabási–Albert network model", in Physica A: Statistical Mechanics and its Applications, Volume 355, Issues 2-4, 15 September 2005, Pages 667-677.

[16] T. Rigole, G. Deconinck , "A Survey on Modeling and Simulation of Interdependent Critical Infrastructures", 3rd IEEE Benelux Young Researchers Symposium in Electrical Power Engineering, paper no. 44, pag.1-9, 27-28 April 2006, Ghent, Belgium.

[17] E. Zio, W. Kröger, "Vulnerability assessment of critical Infrastructures", in IEEE Reliability Society 2009 Annual Technology Report, pag.1-7.

[18] P.Hines, E. Cotilla-Sanchez, S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?", in Proceeding of CHAOS 20, 2010, published online 28 September 2010,pag 033122-1-5.

[19] V. Dub, D. Sarchiz , "Power networks' robustness oriented Extension", in PowerTech 2009 IEEE Bucharest, Digital Object Identifier: 10.1109/PTC.2009.5281871 , 2009 , Page(s): 1 – 4.

[20] O. A. Mousavi, M. S. Farashbashi-astaneh, G. B. Gharehpetian, "Improving Power System Risk Evaluation Method Using Monte Carlo Simulation and Gaussian Mixture Method," Advances in Electrical and Computer Engineering, vol. 9, no. 2, pp. 38-44, 2009. [Online]. Available: http://dx.doi.org/10.4316/AECE.2009.02007

[21] G. Grigoras, G. Cartina, E. C. Bobric, "Strategies for Power/Energy Saving in Distribution Networks," Advances in Electrical and Computer Engineering, vol. 10, no. 2, pp. 61-64, 2010. [Online]. Available: http://dx.doi.org/10.4316/AECE.2010.02010

[22] M. Rosas-Casals, S. Valverde, R. V. Sole, "Topological vulnerability of the european power grid under errors and attacks", in International Journal of Bifurcation and Chaos, World Scientific Publishing Company, Vol. 17, No. 7 (2007), pp. 2465–2475.

[23] P. Cesarz, P., G.M. Pomann, G., L. Torre, and al.., "Detecting Network Vulnerabilities Through Graph Theoretical Methods", pag.1-20, October2007.

[24] T. Murata, Petri nets: Properties, "Analysis and Applications", in Proceedings of the IEEE, vol.77, No. 4, April 1989, Pag.541-580.

[25] Octavian Pastravanu - Sisteme cu evenimente discrete (Discrete event systems), Matrixrom Publishing Bucarest, 1997.