Vulnerability of networks of interacting Markov chains

By L. Kocarev, N. Zlatanov, and D. Trajanov

Macedonian Academy for Sciences and Arts, Skopje, Macedonia

The concept of vulnerability is introduced for a model of random, dynamical interactions on networks. In this model, known as influence model, the nodes are arranged in an arbitrary network, while the evolution of the status at a node is according to an internal Markov chain, but with transition probabilities that depend not only on the current status of that node, but also on the statuses of the neighboring nodes. Vulnerability is treated analytically and numerically for several networks with different topological structures, as well as for three real networks: network of infrastructures, power grid, and WWW, identifying the most influential nodes of these networks.

Keywords: vulnerability, VulnerabilityRank, Markov chains, networks

1. Introduction

In everyday life we are surrounded, and increasingly dependent on engineered network structures. Therefore, reliability of a network is a crucial for its design and operation. The impact of component (link or node) failure on the performance of the network as a whole depends in part on network topology and in part on the flow occurring along the links. This impact is measured by network reliability. Traditionally, there are two approaches to evaluate the reliability of a stochastic network (Sanso & Soumis 1991):

1. Static approach: network is considered as a graph. In this case, reliability of the network is related to some measure of connectivity of the network (Biechelt & Tittman 1991).

2. Dynamic approach: network is considered as a flow network that carries commodities from origin to destination nodes to satisfy a demand. In this case, reliability of the network is related to the ability of the network to transmit a level of flow (Chan *et al.* 1997; Kishimoto 1997).

Related to the concept of reliability is a concept of vulnerability, which has been introduced in several fields including psychology, sociology, political science, economics, epidemiology, biology, environmental and geosciences, and engineering (McEntire 2005). 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" (Merriam-Webster 2006). 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 (1998) 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 (2002) defines vulnerability in the road transportation system as "a susceptibility to incidents that can result in considerable reductions in road network serviceability". 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.* (2003) 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" (Agarwal 2003). 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 vertices and edges (Barefoot *et al.* 1987).

In the network literature there are different approaches to the concept of vulnerability. One trend relates the vulnerability or robustness of a network with its connectivity (Albert *et al.* 2000; Paul *et al.* 2005; Newman & Ghoshal 2008), while others relate it with the decrease of efficiency when some vertices or edges are under attack (Holme *et al.* 2002; Crucitti *et al.* 2003; Crucitti *et al.* 2004). This paper proposes to study vulnerability of networks of interacting Markov chains. The concept of interactions on networks is not new, and has appeared in various forms in a variety of fields. The influence model (Asavathiratham 2000) differs from other previous models of interactions (such as stochastic Ising model, cellular automata, infinite particle system, voter model, interactive Markov chain) in several ways, two most important are (1) each site (node) may contain an arbitrary (finite) local chain and (2) the network may have an arbitrary (finite) graph and influence structure. The influence model (Asavathiratham 2000; Asavathiratham *et al.* 2001; Roy *et al.* 2002) is a simple (and mathematically tractable) model of random, dynamical interactions on networks. It consists of a network of nodes, each with a status that evolves over time. The evolution of the status at a node is according to an internal Markov chain, but with transition probabilities that depend not only on the current status of that node, but also on the statuses of the neighboring nodes.

In this paper, we introduce a new concept called *VulnerabilityRank*: it takes into account the network topology, node dynamics, and potential node interactions in calculating nodes' influence and their relative priority. The behavior of the influence model depends strongly on the so called *influence matrix* (to be defined precisely bellow). We define *vulnerability* of the network as the stationary distribution π of its influence matrix, which is the normalized left eigenvector of the influence matrix associated with the eigenvalue 1. For binary influence model, it measures a steady-state probability of the node failure. The vector π is called VulnerabilityRank: it shows what are the most influential (vulnerable) nodes in the network. VulnerabilityRank is treated analytically and numerically for several networks with different topological structures. We compute VulnerabilityRank for interdependency matrix of a infrastructures network and EU power grid, showing the most influential (vulnerable) nodes. Our work differs from two most relevant for this paper concepts of

PageRank (Brin & Page 1998) and SecureRank (Miura-Ko & Bambos 2007) in the following: in both (Brin & Page 1998; Miura-Ko & Bambos 2007) nodes are static and do not change in time, while in our work dynamics of each node is governed by an arbitrary (finite) Markov chain.

2. Preliminaries: Influence model

The influence model is suggested in (Asavathiratham 2000) as a model of random, dynamical interactions on networks. We refer the reader to (Asavathiratham 2000) for a full account of the model and its properties; here we give a brief description of the model. Define the directed graph of a $n \times n$ matrix A, denoted by $\Gamma(A)$, as the directed graph on nodes 1 to n, where a directed edge from i to j, denoted by (i, j), exists if and only if $a_{ij} \neq 0$. The edge weight is given by a_{ij}. Consider a graph with n nodes, referred to as sites; each site has a *status* value that varies over time as it is 'influenced' by the neighbors. Assume that we are given an $n \times n$ matrix $D = [d_{ij}]$ ($d_{ij} \geq 0$). We further assume that D is a stochastic matrix, that is $\sum_j d_{ij} = 1$ for each i. The graph $\Gamma(D^T)$ will be called the *network influence graph*. An edge (i, j) exists on this graph if the status of j can be influenced by the status of i. The weight on edge (i, j) can be interpreted as the amount of influence that i exerts on j relative to the total amount of influence that j receives. The total amount of influence received by any site is equal to the sum of incoming edge weights, which is 1, because D is stochastic matrix. Let m_i be the order of the local Markov chain at the site i for $1 \leq i \leq n$. Let $s_i(k)$ and $p_i(k)$ be the status vector and the next-status probability mass-function (PMF) vector of site i at time k. Let $\mathbf{s}(k) = [s_1 \dots s_n]^T$ and $\boldsymbol{p}(k) = [p_1 \dots p_n]^T$ denote the state and probability vectors of length $(m_1 + \dots + m_n)$. For each pair of i and j, the state transition matrix A_{ij} is an $m_i \times m_j$ nonnegative matrix whose rows sum to 1. The *influence matrix* is defined as $H = D^T \otimes \{A_{ij}\}$, where $\otimes$ denotes Kronecker product. The evolution equations of the influence model are defined as:

$$\begin{aligned} \boldsymbol{p}^T(k+1) &= \mathbf{s}^T(k)H, & (2.1)\\ \mathbf{s}^T(k+1) &= MultiRealize[\boldsymbol{p}^T(k+1)], & (2.2) \end{aligned}$$

where the operation $MultiRealize[\boldsymbol{p}(k+1)]$ treats each block of PMF's within $\boldsymbol{p}^T(k+1)$ separately, independently realizing the new status vectors block by block.

The influence matrix H is, in general, not stochastic. However, its dominant eigenvalue is one. Assuming for simplicity that all its eigenvalues are distinct, the state-state value of the evolution of the status PMF approaches the left eigenvector π corresponding to eigenvalue 1, that is

$$E(\mathbf{s}^T(k)) = E(\mathbf{s}^T(0))H^k \to \pi$$

as $k \to \infty$, where the notation $E(\cdot)$ is used for expectation or expected value. In what follows we discuss in more detail the binary influence model.

3. VulnerabilityRank

Binary influence model is the special case of influence model for which each A_{ij} is equal to the 2×2 identity matrix I_2, $A_{ij} = I_2$. For the binary influence model,

the status of the site i is represented by s_i, $s_i \in \{0,1\}$. The values 0 or 1 may represent any two different statuses such as 'on' vs. 'off', 'healthy' vs. 'sick', or 'normal' vs. 'failed'. Let $\mathbf{s} = [s_1 \dots s_n]^T$. The *binary influence model* refers to the following equation:

$$\boldsymbol{p}(k+1) = D\mathbf{s}(k), \tag{3.1}$$

$$\mathbf{s}(k+1) = Bernoulli[\boldsymbol{p}(k+1)]. \tag{3.2}$$

Since D is stochastic matrix, it follows that $p_i(k) \leq 1$ for each k and i. The operation $Bernoulli[p(k+1)]$ in (3.2) can be thought of as flipping n independent coins to realize the entries of $\mathbf{s}(k+1)$, where the probability of the i-th coin turning up heads (status 1) is $p_i(k+1)$. If $\Gamma(D^T)$ is an ergodic (irreducible and aperiodic) graph, then the only recurrent states in a binary influence model are the all-ones and all-zeros consensus states. In this case,

$$\lim_{k\to\infty} D^k = \mathbf{1}\pi^T \tag{3.3}$$

where π is the left eigenvector corresponding to the eigenvalue 1, which is normalized so that $\pi^T\mathbf{1} = 1$, and $\mathbf{1}^T = [1 \dots 1]$ is vector of length n.

Definition 1. *For binary influence model, we call the vector π VulnerabilityRank for the network $\Gamma(D^T)$.*

The following theorem explains why the vector π is called VulnerabilityRank.

Theorem 3.1. *Let $\pi = [\pi_1, \dots, \pi_n]^T$ and let $\pi_j = \max_{1\leq i\leq n} \pi_i$. Assume for the binary influence model that the matrix D is ergodic. Assume further that $s_j(0) = 1$ and $s_i(0) = 0$ for all $i \neq j$. Then the probability of reaching the all-ones consensus state is π_j and the node j is the most influential node.*

The proof od the theorem is straightforward. Since D is ergodic $p_i > 0$; moreover $\sum \pi_i = 1$. From Eq.(3.3) we conclude that

$$\lim_{k\to\infty} E(\mathbf{s}(k) \mid \mathbf{s}(0)) = \lim_{k\to\infty} D^k\mathbf{s}(0) = \mathbf{1}\pi^T\mathbf{s}(0) = \sum_i s_i(0)\pi_i.$$

The last equation indicates that all sites have the same probability of $\pi^T s(0)$ of reaching the status 1. Let $s_j(0) = 1$ and $s_i(0) = 0$ for all $i \neq j$. Then, the last equation reduces to π_j. Assuming, for simplicity only, that $\pi_i \neq \pi_j$ for all i, j, and since $\pi_j > \pi_i$, for all $i \neq j$, the site j is the most *influential site*. Therefore, if the value 1 represents failed status of the network, the *VulnerabilityRank* describes what is the influence of each cite i to the failure of the network – it is exactly the value π_i.

Remark 1. *For the case of heterogenous Markov chains, the VulnerabilityRank is defined as the left eigenvector π corresponding to eigenvalue 1 of the influence matrix H. We will deal with heterogenous influence mode in a forthcoming paper.*

It is easy to see that if $s_{j_1}(0) = \dots = s_{j_k}(0) = 1$ and $s_i(0) = 0$ otherwise, then

$$\lim_{k\to\infty} E(\mathbf{s}(k) \mid \mathbf{s}(0)) = \pi_{j_i} + \dots + \pi_{j_k}.$$

Therefore, if $\pi_{j_1} + \ldots \pi_{j_k} > 0.5$, then the probability of reaching the all-ones consensus state for the binary influence model with initial conditions $s_{j_i}(0) = \ldots = s_{j_k}(0) = 1$ and $s_i(0) = 0$ otherwise, is greater than 0.5.

As an example, we consider a binary influence model with a fully connected network of 6 nodes and the influence matrix D given by

$$D = \begin{bmatrix} 1/60 & 7/15 & 7/15 & 1/60 & 1/60 & 1/60 \\ 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \\ 19/60 & 19/60 & 1/60 & 1/60 & 19/60 & 1/60 \\ 1/60 & 1/60 & 1/60 & 1/60 & 7/15 & 7/15 \\ 160 & 1/60 & 1/60 & 7/15 & 1/60 & 7/15 \\ 1/60 & 1/60 & 1/60 & 11/12 & 1/60 & 1/60 \end{bmatrix}. \tag{3.4}$$

It is easy to compute the eigenvector π,

$$\pi^T = \begin{bmatrix} .03721 & .05396 & .04151 & .3751 & .206 & .2862 \end{bmatrix}.$$

Therefore, the site 4 is the most vulnerable site and $\pi_4 + \pi_6 > 0.5$.

(*a*) *VulnerabilityRank for different network topologies*

In this subsection we address the following problem: given a graph how to define corresponding network influence graph. Let G be a finite simple undirected connected graph with n nodes, so that its adjacency matrix $A = (a_{ij})$ is a symmetric (0,1)-matrix with zeros on its diagonal. We suggest two approaches to correspond network influence graph to an arbitrary graph G.

For the first approach, called node-degree influence model, we define the influence matrix $D = (d_{ij})$ such that $d_{ij} = a_{ij}/\sum_i a_{ij}$. The second model, called betweenness-centrality influence model, is defined as follows. Recall that the edge betweenness centrality is defined as

$$c_{ij} = \sum_{s \neq i, s \neq t} \frac{\sigma_{st}(e_{ij})}{\sigma_{st}},$$

where e_{ij} is the edge between nodes i and j, $\sigma_{st}(e_{ij})$ is the number of shortest paths from node s to node t that edge e_{ij} lies on and σ_{st} is the total number of shortest paths from node s to node t. Shortest path is the minimum distance between two nodes. The distance between two nodes is the sum of edge weights on that path. For this model the matrix $D = (d_{ij})$ is defined as $d_{ij} = c_{ij}/\sum_i c_{ij}$.

Figures 1–3 show the *VulnerabilityRank* for several networks with different topologies using node-degree influence model. The most vulnerable site is in the scale free network: its vulnerability is 10 times larger than the maximum vulnerabilities of small world and Erdös–Rényi (ER) graphs. The distribution of vulnerabilities of a scale free network follows power-low distribution. For example, for a scale free graph with 2048 nodes and a minimum node degree 2, we found that distribution of vulnerabilities fits well the power-law distribution with exponent 1.8943.

Figures 4–6 show the *VulnerabilityRank* for the same networks shown in the previous figures, but using now betweeness-centrality influence model. The average

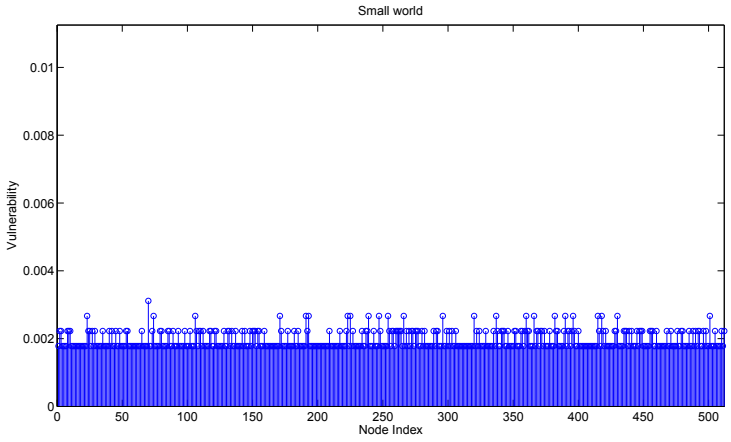

Figure 1. VulnerabilityRank for node-degree binary influence model on small world graph.

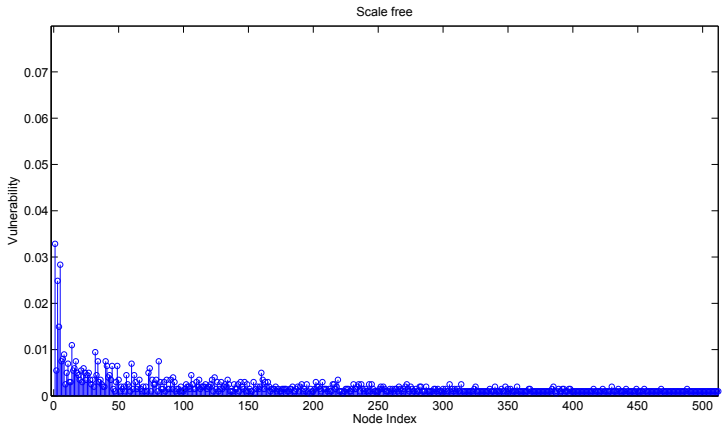

Figure 2. VulnerabilityRank for node-degree binary influence model on scale free graph.

maximum values for VulnerabilityRank for three graphs, scale free, small world and ER, when node-degree influence model is used, are 0.0513, 0.0078, and 0.0067, respectively. The same values for betweenness-centrality influence model are 0.1138, 0.0182, and 0.0079. We have also computed the average percentage of the nodes that need to be in the status off at time $k = 0$ so that, when time goes to infinity ($k \to \infty$), the probability of the whole network (all sites) to be in the status 1 (off) is greater or equal to 0.5. These numbers for node-degree influence model and scale free, small world, and ER graphs are 21.24, 40.71, and 41.09, respectively. For betweenness-centrality influence model we have 9.73 for scale free networks, 24.27 for small world networks, and 40.04 for ER graphs. For both models: node-degree and betweenness-centrality influence models, scale free graph is the most vulnerable graph, while random ER graph is the most robust graph.

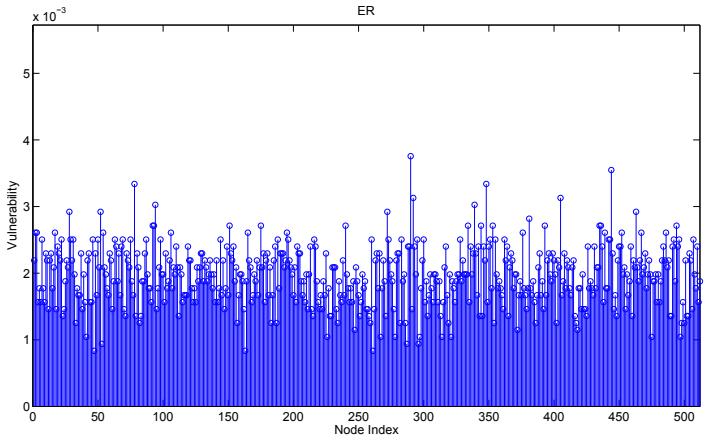

Figure 3. VulnerabilityRank for node-degree binary influence model on ER graph.

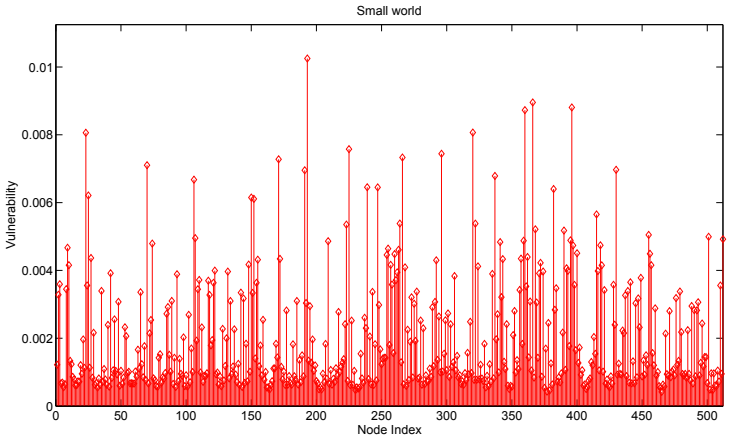

Figure 4. VulnerabilityRank for betweenness-centrality binary influence model on small world graph.

(*b*) *VulnerabilityRank for reducible graphs*

Irreducibility is a desirable property because it is precisely the feature that guarantees that a Markov chain possesses a unique (and positive) stationary distribution vector π. When $\Gamma(D^T)$ is an ergodic graph, then computation of VulnerabilityRank for the graph G is easy. However, when $\Gamma(D^T)$ is reducible further adjustment is necessary in order ensure irreducibility. We first compute the following quantity $\pi_i = (1/n)\sum_{i=1}^{n} \lim_{k\to\infty} D^k \mathbf{s}_i(0)$, where $\mathbf{s}_i(0) = [s_{i1}(0) \dots s_{in}(0)]^T$ such that $s_{ii} = 1$, otherwise $s_{ij} = 0$. The *VulnerabilityRank* for this graph is $\pi = [\pi_1 \dots \pi_n]^T$. Next, following (Brin & Page 1998), we make every state directly reachable from

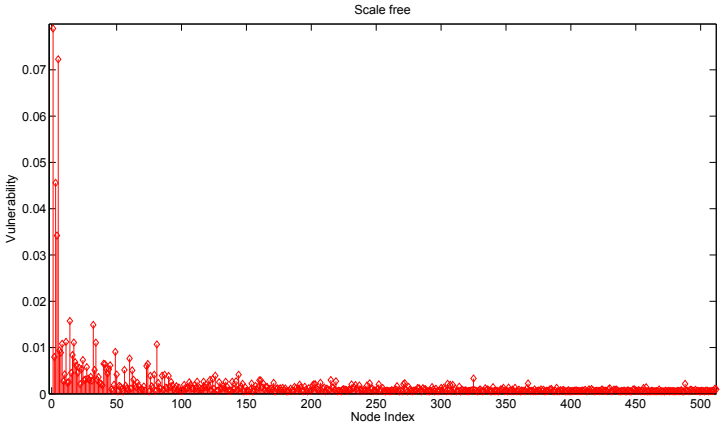

Figure 5. VulnerabilityRank for betweenness-centrality binary influence model on scale free graph.

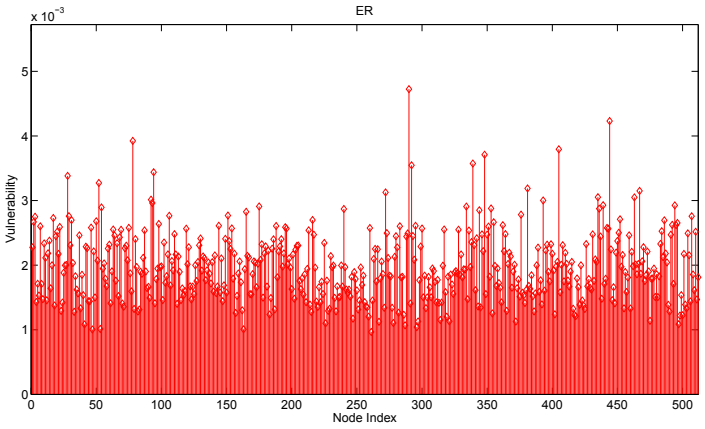

Figure 6. VulnerabilityRank for betweenness-centrality binary influence model on ER graph.

every other state by adding a perturbation matrix to D so that:

$$D^* = \alpha D + (1-\alpha)\frac{\mathbf{1}\mathbf{1}^T}{n}.$$

It is easy to show that if the respective spectrums of D and D^* are $\sigma(D) = \{1, \mu_2, \ldots, \mu_n\}$ and $\sigma(D^*) = \{1, \lambda_2, \ldots, \lambda_n\}$, then $\lambda_k = \alpha\mu_k, \quad k = 2, \ldots, n$. It should be noted here that the matrix D^* in the context of Web's hyperlink structure is generally called "the Google matrix" and its stationary distribution is the real PageRank vector. Let π^* be the left eigenvector corresponding to the eigenvalue 1 of the matrix D^*. Numerically we found that $\pi^* \approx \pi$ for values of α close to 1.

We now present example. Let

$$\boldsymbol{D} = \begin{bmatrix} 0 & 1/2 & 1/2 & 0 & 0 & 0 \\ 1/6 & 1/6 & 1/6 & 1/6 & 1/6 & 1/6 \\ 1/3 & 1/3 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

This matrix is stochastic, but it is reducible, so it cannot have a unique positive stationary distribution. To force irreducibility, choose $\alpha = 0.9$; thus, one obtains the matrix given with Eq. (3.4), for which we have already found that the node 4 is the most influential node.

(*c*) *VulnerabilityRank for SIR model*

In this subsection we study VulnerabilityRank for a stochastic susceptible-infected-removed (SIR) model. Let G be a finite simple undirected connected graph with n nodes, so that its adjacency matrix $A = (a_{ij})$ is a symmetric (0,1)-matrix with zeros on its diagonal. Let $\left[p_i^S(k) \;\; p_I^1(k) \;\; p_R^1(k)\right]$ be 3-dimensional probability vector of node i at time k. $p_i^S(k)$, $p_i^I(k)$, and $p_R^1(k)$ are the probabilities that node i at time k is in status susceptible, infected, and removed, respectively. Further, let $\left[s_j^S(k) \;\; s_j^I(k) \;\; s_j^R(k)\right]$ be 3-dimensional status vector of node i at time k. The status vector can only have one element equals to 1; the other elements are equal to 0. For $s_j^S(k) = 1$, the node i is in status susceptible, if $s_j^I(k) = 1$ then the node i is in status infected, and for $s_j^R(k) = 1$, the node i is in status removed. We consider the following version of the SIR model, for which the node equations are:

$$p_i^S(k+1) = 1 - p_i^I(k+1) - p_i^R(k+1) \tag{3.5}$$

$$p_i^I(k+1) = s_i^S(k)\left[1 - \prod_{j=1}^{N}(1 - \beta a_{ij} s_j^I(k))\right] \tag{3.6}$$

$$p_i^R(k+1) = s_i^I(k) + s^R(k). \tag{3.7}$$

where β is the probability that the infection attempt is successful, and $A = (a_{ij})$ is the adjacency matrix of the graph. Each node that is infected at time k attempts to infect each of its neighbors; each infection attempt is successful with probability β independent of other infection attempts. Each infected node at time k is removed at time $k + 1$.

We consider epidemic spreading on graphs starting with one node initially infected, all other nodes are susceptible. In this section we address the following problem: given a graph, what is the most important (influential, vulnerable) node. Intuitively, the node is most influential, if when is initially infected, the spreading is most dominant (the average number of infected nodes when time goes to infinity is the largest or the time needed the nodes to be infected is the largest). For SIR model we compute the VulnerabilityRank for node-degree influence model. VulnerabilityRank gives answer to our problem: indeed, the most vulnerable node computed with VulnerabilityRank is also the most important (influential) node for

the SIR dynamics on the graph G. As an example, we show on Figure 7 the average number of infected nodes for small-world graph versus time for two different values of β when the most influential, the least influential, and random node are initially infected.

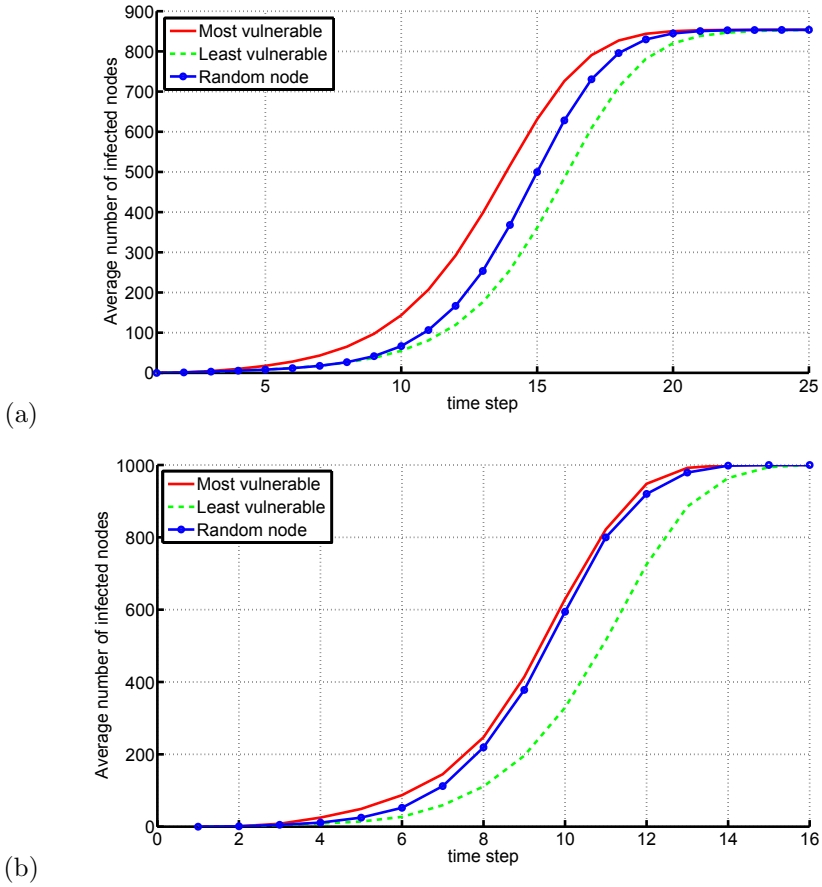

Figure 7. Average number of infected nodes versus time for three different initially infected nodes: (a) $\beta = 0.5$ (b) $\beta = 1$.

4. Applications

(*a*) *Network of infrastructures*

Infrastructures are vital for the operation of our society. A mathematical model that might be applied for assessment of the compound risk of failure of interdependent infrastructure networks, is provided by Sivonen et al. (Sivonen 2004), in the frames of which the following groups of inter-operating items have been considered: technical infrastructure (energy supply, communications, information systems), basic services and supplies (food supply, transport logistics, mass media, health care,

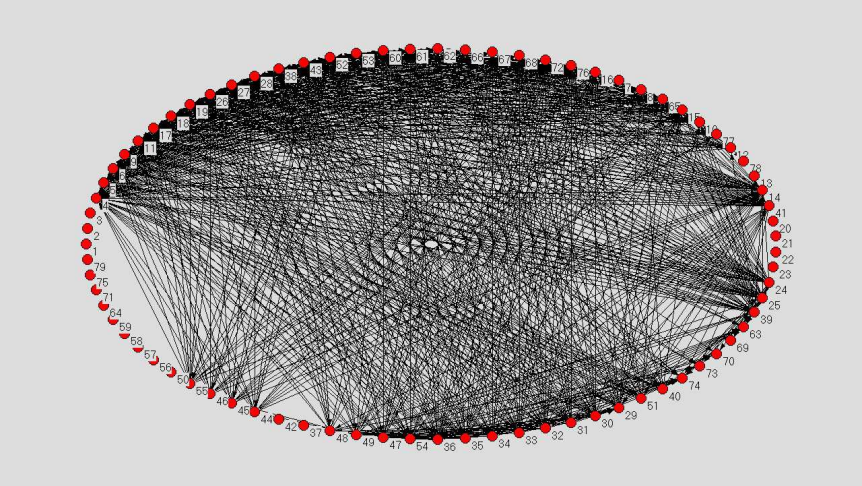

Figure 8. Network influence graph for the network of infrastructures.

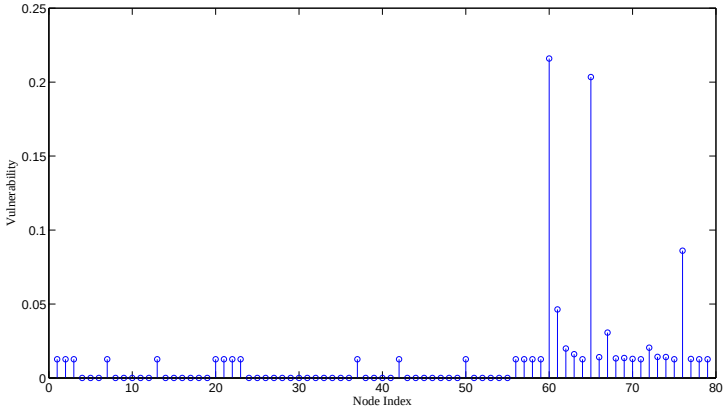

Figure 9. VulnerabilityRank for infrastructure network influence graph shown in Figure 8.

financial services) and threats (threats to data system, illegal immigration, threats to food and health, threats to environment, economic threats, crime and terrorism, disasters, international tension, war and warlike situations). For each of the items the frequency, duration and effects of failures are studied, as well as the dependency of a failure of one item on the failures in other items. An example of a network influence graph $\Gamma(D^T)$ obtained in this way using real data from the web page of the National Emergency Supply Agency of Finland: www.nesa.fl, is shown in Figure 8.

Figure 9 shows the *VulnerabilityRank* for infrastructure network influence graph shown in Fig. 8. The most vulnerable sites are the sites representing the following threats (out of 17 threats grouped in 4 groups: Causes for severe disturbances, Economic threats, Environment and health treats, Political security threats) : 1. Weather phenomenon, 2. Threats to data systems, 3. Crime and terrorism, 4. Strike, and 5. International logistics crisis. The threats 1 and 4 belong to the same group:

'Causes for severe disturbances', threats 2 i 5 to the group 'Economic threats' and 3 to 'Political security threats'. Since the influence graph in this example is reducible, we compute the VulnerabilityRank using approach described in the previous section with $\alpha = 0.9$.

(*b*) *Power grid*

Our next example is the EU power grid. The "Union for the Co-ordination of Transmission of Electricity" (UCTE) is the association of transmission system operators in continental Europe; different data can be found at UCTE web page: www.ucte.org. For this paper, we consider the physical energy flows for the month January 2007. The data can be organized as a directed weighted graph with $N = 26$ nodes. Each node represents a country (or region) in EU as follows: 1 represents Austria, 2 Bosnia, 3 Belgium, 4 Bulgaria, 5 Switzerland, 6 Czech Republic, 7 Germany, 8 Spain, 9 France, 10 Greece, 11 Croatia, 12 Hungary, 13 Italy, 14 Luxembourg, 15 Monte Negro, 16 Macedonia, 17 Netherland, 18 Poland, 19 Portugal, 20 Romania, 21 Serbia, 22 Slovenia, 23 Slovakia, 24 Denmark West, 25 Ukraine West, and 26 represents others (Albania, Belarus, Denmark East, Great Britain, Morocco, Republic of Moldavia, Norway, Sweden, Republic of Turkey and Ukraine). The weight $a_{i,j}$ represents a value (in GWh) that country i exports to country j. For example, $a_{1,5} = 906$, $a_{1,7} = 227$, $a_{1,12} = 104$, $a_{1,13} = 121$, and $a_{1,22} = 72$ means that Austria exported during January 2007 906 GWh energy to Switzerland, 227 GWh to Germany, and so on.

We compute the VulnerabilityRank for the influence model defined on this graph using both approaches: node-degree and betweenness centrality. The results are shown in Fig. 10 and Fig. 11. For the node-degree influence model the most vulnerable node is 9 (corresponding to France), while for the betweenness- centrality influence model the most influential node is 7 (corresponding to Germany).

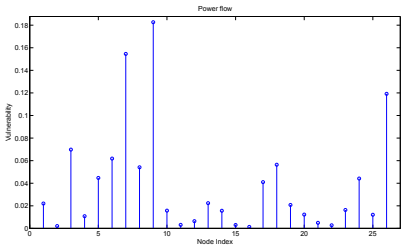

Figure 10. VulnerabilityRank for node-degree binary influence model for the physical energy flows for the month January 2007.

(*c*) *World Wide Web*

The World Wide Web (commonly shortened to the Web) is a system of interlinked hypertext documents accessed via the Internet. Suppose the web of interest contains n pages, each page indexed by an integer k, $1 \leq k \leq n$. The web is an example of a directed graph: an arrow from page i to page j indicates a link from

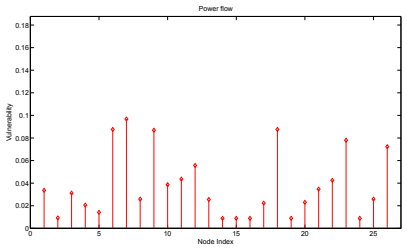

Figure 11. VulnerabilityRank for betweenness-centrality binary influence model for the physical energy flows for the month January 2007.

page i to page j. We will use the phrase "importance score" (also page rank) for any quantitative rating of a web page's importance. The importance score for any web page will always be a non-negative real number. Let x_k denote the importance score of page k in the web, and $L_k \subset \{1, \ldots, n\}$ denote the set of pages with a link to page k. For each k importance score is defined as $x_k = \sum_{j \in L_k} \frac{x_j}{n_j}$, where n_j is the number of outgoing links from page j. Finding the importance score for nodes (web pages) reduce to finding solutions of the linear equation $A\boldsymbol{x} = \boldsymbol{x}$, where A, so called link matrix, is square column-stochastic $n \times n$ matrix. Thus, the problem of finding importance score for the web pages is equivalent to finding the eigenvector, called PageRank, that corresponds to eigenvalue 1, of the matrix A. Assuming that the matrix A is the influence matrix for the binary influence model, we may conclude that the vector VulnerabilityRank for the binary influence model defined on the web is equal to the vector PageRank.

5. Conclusions

We have suggested a method for calculating the VulnerabilityRank for networks of interacting Markov chains. The method is readily applicable for huge matrices and heterogenous Markov chains. The method can be applied to any network, including most of the infrastructure networks, such as power grid, gas network, transportation network, as well as to network of infrastructures. It can also be extended to biological and social networks provided that each node can be described with a Markov chain. We stress that our concept of VulnerabilityRank is different than both recently introduced concepts of PageRank and SecureRank – it reduces to these concepts only when we consider node-degree binary influence model. More general treatment of VulnerabilityRank for heterogenous influence model will be a subject of interest in our future work.

Acknowledgment – We thank Hannu Sivonen for sending us the data describing the interdependencies of critical infrastructures in Finland. This work is partially supported by the EU Commission (project MANMADE).

References

Agarwal, J., Blockley, D. & Woodman, N. 2003. "Vulnerability of structural systems". Structural Safety 25, pp. 263–286.

Albert, R., Jeong, H. & Barabási,A.L. 2000. "Error and attack tolerance of complex networks", Nature, Volume 406, 2000, Pages: 378-382.

Asavathiratham, C. 2000. "Influence Model: A tractable Representation of Networked Markov Chains," PhD thesis, Massachusetts Institute of Technology.

Asavathiratham, C., Roy, S., Lesieutre, B. & Verghese, G. 2001. "The influence model" IEEE Control Systems Magazine, Volume 21, Issue 6, Page(s): 52 – 64.

Barefoot, C. A., Entringer, R. & Swart, H. 1987. "Vulnerability in graphs – a comparative survey". Journal of Combinatorial Mathematics and Combinatorial Computing 1, pp. 13–22.

Berdica, K. 2002. "An introduction to road vulnerability: what has been done, is done and should be done". Transport Policy 9, pp. 117–127.

Biechelt, F. & Tittman, P. 1991. "A generalized reduction method for the connectedness probability of stochastic networks," IEEE Trans. Rel., vol. 40, no. 2, pp. 199-203.

Brin, S. & Page, L. 1998. "The anatomy of a large-scale hypertextual Web search engine", Proceedings of the 7th international conference on World Wide Web 7, Pages: 107–120.

Chan, Y., Yim, E., & Marsh, A. 1997. "Exact and approximate improvement to the throughput of a stochastic network," IEEE Trans. Rel., vol. 46, no. 4, pp. 473-486.

Crucitti, P. , Latora, V. & Marchiori, M. 2004. Phys. Rev. E 69, 045104(R).

Crucitti, P., Latora,V., Marchiori, M. & Rapisarda,A. 2003. Physica A 320, 622.

Einarsson, S. & Rausand, M. 1998. "An approach to vulnerability analysis of complex industrial systems". Risk Analysis 15, pp. 535–546.

Holme, P., Kim, B.J., Yoon, C.N. & Han S.K. 2002. "Attack vulnerability of complex networks", Phys. Rev., E 65, art. no. 056109.

Holme, P., Kim, B. J., Yoon, C. N. & Han, S. K. 2002. Phys. Rev. E 65, art. no. 056109.

Kishimoto, W. 1997. "Reliable flows with failures in a network," IEEE Trans. Rel., vol. 46, no. 3, pp. 308-315.

Latora, V. & Marchiori, M. 2001. "Efficient behavior of small-world networks", Phys. Rev. Lett. 87(19), Page: 1-198701-4.

Latora, V. & Marchiori, M. 2003. "Economic small-world behavior in weighted networks", Eur. Phys. J. B 32, Pages: 249–263.

McEntire, D. A. 2005. "Why vulnerability matters: exploring the merit of an inclu-sive disaster reduction concept", Disaster Prevention and Management 14, pp. 206–222.

Merriam-Webster 2006. Merriam-Webster Online Dictionary: http://www.m-w.com/

Miura-Ko, R. A., and Bambos, N. 2007. "SecureRank: A Risk-Based Vulnerability Management Scheme for Computing Infrastructures", IEEE International Conference on Communications, Page(s): 1455 – 1460.

Morakis, E., Stylianos, V. & Blyth, A. 2003. "Measuring vulnerabilities and their exploitation cycle". Information Security Technical Report 8, pp. 45–55.

Newman, M. E. & Ghoshal, G. 2008. Phys. Rev. Lett. 100, 138701 (2008).

Paul, G., Sreenivasan, S. & Eugene, H.S. 2005. Phys. Rev. E 72, 056130 (2005).

Roy, S., Lesieutre, B.C. & Verghese, G.C. 2002. "Resource allocation in networks: a case study of the influence model", Proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002, Page(s): 875 – 884

Sanso, B. & Soumis, F. 1991. "Communication and transportation network reliability using routing models," IEEE Trans. Rel., vol. 40, no. 1, pp. 29-37.

Sivonen, H. 2004. "Calculating Compound Risk of Failure Based on Interdependencies of Critical Infrastructures", EAPC / PfP Workshop on Critical Infrastructure Protection and Civil Emergency Planning.

Vardi,Y., & Zhang, C.H. 2007. " Measures of Network Vulnerability" IEEE Signal Processing Letters, Volume 14, Issue 5, Page(s): 313–316.