Comparing topological and reliability-based vulnerability analysis of Iran power transmission network

Zohre Alipour[1], Mohammad Ali Saniee Monfared[2] and Enrico Zio[3,4]

Abstract

Power grids are one of the most important and critical infrastructures which societies rely upon for well-being. Their topological (structural) characteristics related to vulnerability can be analyzed from the viewpoint of complex network theory. In this article, we incorporate into this viewpoint some relevant reliability properties and apply the analysis framework to study the high-voltage power grid in Iran. To identify weak points in the structure, we look at four different centrality measures, namely, degree, betweenness, information and closeness, and analyze their correlation properties. This allows providing a more comprehensive picture of the vulnerability characteristics of the power grid structure. By our analysis, we show that reliability-based characteristics are different from purely topological ones as they are mostly uncorrelated. We also use a voting aggregation method, the Borda Count method, to perform an overall ranking of the most vulnerable nodes, considering both intentional attacks and random failures.

Keywords

Topological analysis, vulnerability, reliability, centrality measures, networks, power grids

Date received: 10 May 2012; accepted: 24 June 2013

Introduction

With the fast development of modern societies, power grids are continually growing in complexity and size, and have become one of the largest engineered complex systems.[1–6] They comprise a large number of units connected in a complex web of structural and physical interactions from which correlations among events emerge, often in unexpected ways.[7,8] For example, it is a common experience that power grids are subject to cascading failures, whose probability and size often are found to obey a characteristic power law distribution.[9]

The functionality of a system like this depends on its structure,[7] the installed capacity in each substation, the lines capacity, their forced outage rates, the load and generation levels and the types of operational protocols in existence between them.[10–12]

It has been argued that conventional reliability, availability, maintainability, and safety (RAMS) methodologies may be inadequate to analyze the complexity of the failure and repair behavior of these systems.[9,13–15]

Furthermore, many power grids today are open systems with given energy flux boundary conditions crossing to neighboring countries. This allows energy to flow in and out to the extent that countries can share energies, which give the boundary conditions to every other neighboring country's networks. These inter- and intra-dependency conditions add potential vulnerability but also robustness depending on how the networks are managed.[16]

In this extended operational scenario, methods to assess the vulnerability of networks are needed. Traditional, probabilistic safety assessment (PSA) methods can help systematically analyze the risk of complicated systems, identifying the most unreliable components, and correspondingly dimensioning the adequate redundancies.[17–19] PSA has been originally developed for the safety analysis of nuclear power plants, and to a certain extent, it is suitable for studying power grid protection systems.[20] However, vulnerability analyses of

[1]Department of Industrial Engineering, College of Engineering, University of Tehran, Tehran, Iran
[2]Department of Industrial Engineering, School of Engineering, Alzahra University, Tehran, Iran
[3]European Foundation for New Energy-Electricite' de France, at Ecole Centrale Paris–Suplec, Châtenay-Malabry Cedex, France
[4]Dipartimento di Energia, Politecnico di Milano, Milano, Italy

Corresponding author:
Mohammad Ali Saniee Monfared, School of Engineering, Alzahra University, Vanak Street, P.O. Box 1993891167, Tehran, Iran.
Email: mas_monfared@alzahra.ac.ir; mas_monfared@yahoo.com

complex networks have to go beyond the conventional cause-and-effect and fault tree analyses to be able to capture spillover clusters of failures and cascading when strong interdependencies exist. In fact, it is well known that the behavior that emerges in a complex network can hardly be described as the sum of the behaviors of its components, whereas conventional risk analysis techniques are founded on a premise that a system can be broken into parts and parts into smaller parts, in order to enable quantification.[21,22]

A partial response to the analysis challenges brought by the complexity of these systems comes from recent advances in information science, statistical and nonlinear physics, applied mathematics, and their integration into the relatively new inter-disciplinary field of complex systems, and is a sub-field of network science. Within this framework for looking at complex, distributed and highly interconnected systems, approaches are developed to study the vulnerability of large-scale complex networks whose components are facing random faults and malevolent attacks.[19,23–25]

In this article, we extend topological measures to include information about failure rates, and call them "reliability-based" measures to stress the fact that they differ from those defined in the Reliability and Electrical Engineering communities.

From the system structure analysis point of view, local and global topological centrality measures have been proposed such as degree, betweenness, eigenvector, closeness, and information centrality measures.[25] Recently, Sole et al.[26] have attempted to correlate network reliability-based measures with structural-based and topological-based measures with application to 33 European power grids, suggesting that topology might be capturing some of the problems of robustness or fragility of the real network.

They presented evidence of a plausible relation between these two classes of measures: their results indicate a positive correlation between topological-based measures and reliability-based measures. The latter were energy not supplied, normalized by the gross electricity consumption; total loss of power, normalized by the peak load and equivalent time of interruption known as Average Interruption Time (AIT), which is the ratio between the total energy not supplied at the average power demand per year, measured in minutes per year and is normalized by definition.

Topological-based centrality measures have also been extended to enable accounting for reliability characteristics, giving rise to the so-called reliability efficiency centrality measures, first adopted in social network contexts.[27] In the engineering context, Zio[28] proposed an integrated framework for vulnerability and reliability analysis of critical infrastructures. The conjecture was that by considering the probabilities of malfunctioning of the interconnected nodes and links, one can gain additional and more realistic insights into the reliability-based vulnerability of power grids, for use in optimal design, operation, and maintenance.

One outcome of the analysis performed is the identification of the critical components of the system, which if hit by a failure or attack event can give rise to cascading failures and significant consequences at system level.

The proposed framework was implemented first on a reference Institute of Electrical and Electronics Engineers (IEEE) system, a power grid with 14 bus bars and 20 transmission lines,[19,29] and then on the Swiss power grid,[22] but also on road networks.[30] Bompard et al.[31] analyzed the vulnerability of the Italian power grids using the entropic degree, the net-ability and efficiency measures. Also, Zio et al.[32] analyzed the vulnerability of the Italian high-voltage (380 kV) power grid for the identification of groups of most critical links using a multiobjective optimization model, and Zio et al.[33] extended an optimization cascading failures model to a mid-size network (380-kV Italian power grid). Zio et al.[34] used load flow and random walk betweenness centrality measures to analyze power transmission network performance. Li et al.[35] improved the optimization of the cascading failure protection algorithm and applied that to the Italian high-voltage transmission power grid.

In our work, we adopt the integrated topological and reliability framework of analysis, and extend it for application to the high-voltage power grid of Iran. The framework extension goes in the following directions: vulnerable nodes (i.e. buses or substations) are considered (only links have been considered in previously cited work); four different centrality measures (rather than two as in previously cited work) are used to study the robustness of the power grid from two different standpoints, topological and reliability; correlations between the topological measures and reliability measures are analyzed; and the Borda Count method is used to aggregate the different measures. As a result, those nodes that are most important with respect to the measure of network reliability efficiency are identified, and network robustness analysis with respect to both intentional attacks and random failures is studied.

From the complex system theory point of view, the type of analysis undertaken here can be called reliability-based vulnerability analysis. This article is organized as follows: section "Structural characteristics of Iran power transmission network" describes the main technical characteristics of the power grid in Iran, section "Centrality measures" defines the topological and reliability measures considered, section "Centrality measure analysis of Iran's power transmission network" applies such measures to Iran's power grid, section "Network robustness" illustrates the network analysis based on the measures; and section "Conclusion" concludes this article.

Structural characteristics of Iran power transmission network

It has been reported that 34% of power outage in Iran in 2009 is associated with problems in transmission

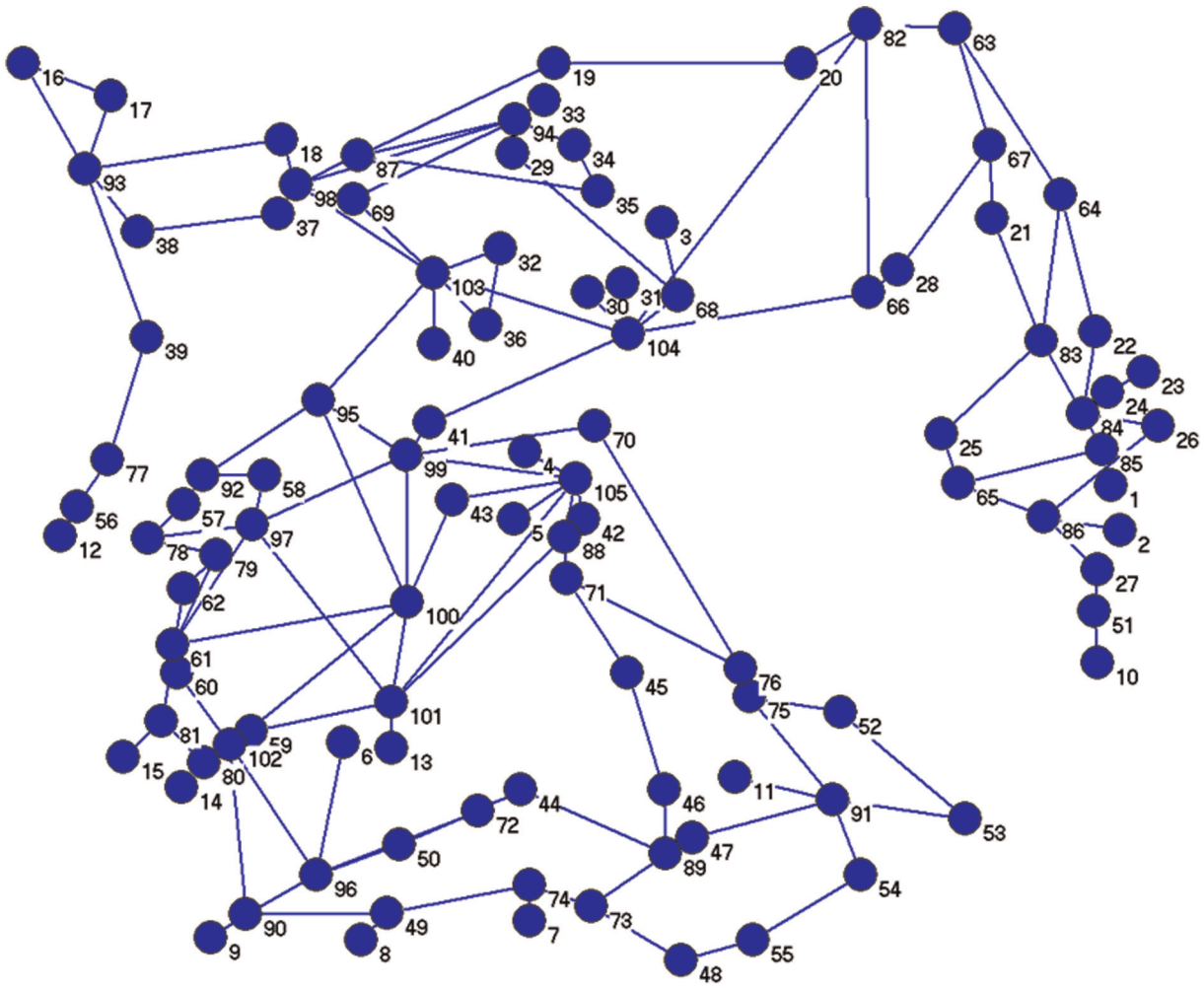

Figure 1. Full graph representation of Iran's power grid.

lines, 55% is due to problems in power generation, and 11% is due to unexpected events in distribution networks.[36]

The data for our analysis are extracted from an official document updated in 2011, containing the detailed description of the whole power grid comprising lines from 400 kV down to 33 kV (http://www.igmc.ir). According to the data, the power transmission network in Iran has 419 bus bars (or nodes), that is, power-generating stations and substations, including transformers, switching stations, reactive power compensators, and 546 edges, that is, transmission lines summing up to more than 108,960 km. The transmission lines in Iran's grids operate at different voltage levels, including 400, 230, 132, 63, and 33 kV. Among them, it is the 400-kV system that constitutes the test system for which the analyses are carried out.

In Figure 1, a graph of the ultrahigh voltage (400 kV) network comprising 105 generation/transmission substations or nodes and 142 transmission lines (links) is shown.[36] The indicated graph is undirected, and the weights of the edges are unitary to represent the system from a topological point of view. However, considering the reliability point of view, each edge in the graph should be assigned a weight equal to its probability of failure.[22]

In Table 1, we provide some statistical properties[37] of the structure of Iran's power grid, including the mean node degree $< k >$, the maximum node degree $k_{\max}$, the graph diameter d, the clustering coefficient C, and the mean shortest path $< l >$.

The data reported in Table 1 indicate that Iran's high-voltage grid is a sparse network with an average degree of 2.7048, low with respect to the maximum degree of 7. The sparsity feature is confirmed by the fact that $L = 142 \ll N^2 = 11,025$. We also note that Iran's power grid is heterogeneous (a network is homogeneous, for example, regular or random if the nodes degrees are similar and heterogeneous, for example, small world or scale free if few nodes, that is, the hubs are linked to many other nodes, but a large number of nodes are poorly connected[37]).

The relatively moderate value of the clustering coefficient of 0.1097 is larger than that of random networks, and also the value 6.8817 of the path length is larger than that of random networks; this leads to conclude that Iran's power grid is a small-world network.[38]

Table 1. Some topological characteristics of the 400-kv power grid.

Transmission network	N	L	$< k >$	$< l >$	C	k_{max}	d
400 kV	105	142	2.7048	6.881	0.1097	7	19

N: number of nodes; L: number of edges; $< k >$: mean degree; $< l >$: mean shortest path; C: clustering coefficient; k_{max}: maximum degree; d: graph diameter.

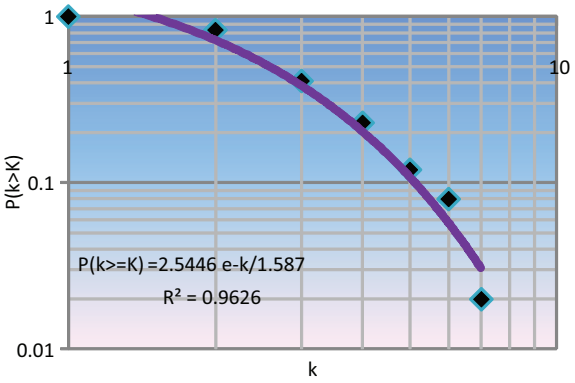

Figure 2. Cumulative distribution.

Degree distribution

Other insights on the structural properties of the 400-kV power grid can be drawn from the analysis of the degree distribution. The results show that the degree distribution can be approximated by an exponential function $P(k \geqslant K) = 2.5446e-k/1.587$ with a (fitting) coefficient of determination $R^2 = 0.9626$ (Figure 2). This is in agreement with the characteristics found by Rosato et al.[38] in their study of the topological properties of the high-voltage electrical power transmission network in three European Union (EU) countries (Italian 380-kV and French and Spanish 400-kV networks). Similar results have been found also by Casals et al.[39] in their analysis of Union for the Coordination of Transmission of Electricity (UCTE) power grids, involving 33 different networks. The implication is that power grids are not scale-free networks (characterized by power law degree distributions).

An additional result has been found by Sole et al.[26] related to the assumption that the node degree distributions for all 33 European power grids follow exponential distributions of the type $P(k \geqslant K) = C\exp(-k/\gamma)$ in which C is a normalization parameter, k is the node degree and γ is a characteristic parameter. Based on the positive correlation found between topological measures and a reliability measure, they have suggested a dichotomous criterion for robustness or fragility of a real network: if $\gamma < 1.5$, the real network would be more robust, whereas if $\gamma > 1.5$, it is more fragile.

Accordingly, for Iran power grids, we have that $\gamma = 1.5870 > 1.5$; hence, they are fragile just like those in Slovak Republic, Poland, Portugal, Switzerland, Czech Republic, France, Hungary, Spain, and Serbia.[26]

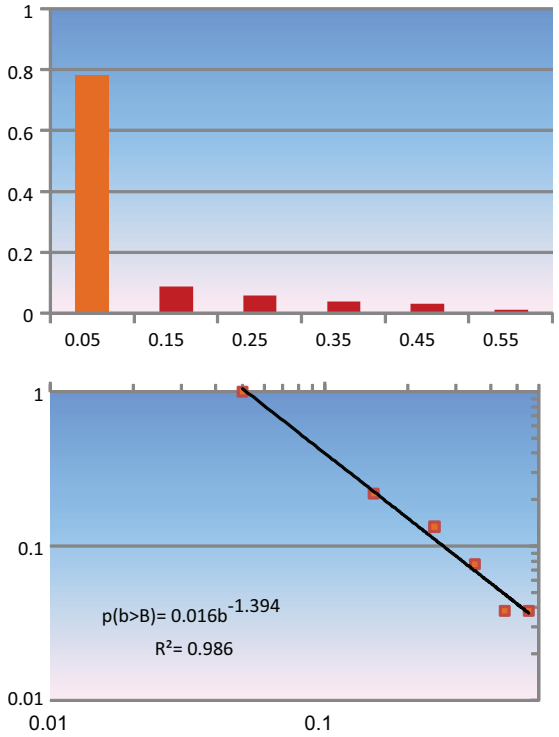

Figure 3. Node betweenness distribution for Iran's 400-kV power grid: frequency distribution (top) and cumulative distribution (bottom).

Betweenness centrality distribution

In a recent work,[40] simulation results of the IEEE-118 bus system and the central China power grid was used to show that the cumulative distributions of node electrical betweenness centrality follow a power law. For Iran's power grids, the node betweenness distribution is shown in Figure 3 (top). Indeed the log–log distribution of node betweenness follows a power law with coefficient of determination $R^2 = 0.986$. The fact that the degree centrality follows an exponential distribution, but the node betweenness centrality follows a power law distribution shows that Iran's power grid belongs to the class of small-world networks of Watts and Strogatz,[41] that is, being a mix between random and regular networks.

Centrality measures

To identify, from the structural point of view, the system elements that are critical for the system's overall

Table 2. Topological- and reliability-based centrality measures.

Centrality measures	Topological	Reliability
Degree	$C_i^D = \frac{\sum_{j \in G} a_{ij}}{N-1}, \quad 0 \leqslant C_i^D \leqslant 1$	$RC_i^D = \frac{\sum_{j} a_{ij} \sum_{j \in G} p_{ij}}{(N-1)^2}, \quad 0 \leqslant RC_i^D \leqslant 1$
Closeness	$C_i^C = \frac{N-1}{\sum_{j \in G} d_{ij}}, \quad 0 \leqslant C_i^C \leqslant 1$	$RC_i^C = \frac{N-1}{\sum_{j \in G} rd_{ij}}, \quad 0 \leqslant RC_i^C \leqslant 1$
Betweenness	$C_i^B = \frac{1}{(N-1)(N-2)} \sum_{j,k \in G, j \neq k \neq i} \frac{n_{jk}(i)}{n_{jk}}, \quad 0 \leqslant C_i^B \leqslant 1$	$RC_i^B = \frac{1}{(N-1)(N-2)} \sum_{j,k \in G, j \neq k \neq i} \frac{rn_{jk}(i)}{rn_{jk}}, \quad 0 \leqslant RC_i^B \leqslant 1$
Information	$C_i^I = \frac{\Delta E(i)}{E} = \frac{E(G) - E(G'(i))}{E(G)}, \quad 0 \leqslant C_i^I \leqslant 1$	$RC_i^I = \frac{\Delta RE(i)}{RE} = \frac{RE(G) - RE(G'(i))}{RE(G)}, \quad 0 \leqslant RC_i^I \leqslant 1$
Efficiency	$E(G) = \frac{1}{N(N-1)} \sum_{i,j \in N, i \neq j} \frac{1}{d_{ij}}$	$RE(G) = \frac{1}{N(N-1)} \sum_{i,j \in N, i \neq j} \frac{1}{rd_{ij}}$

G: the graph descriptive of the structure of the real network with N nodes; $G'(i)$: graph that results from removing the edges of node (i); $A = [a_{ij}]$: $N \times N$ adjacency matrix whose generic element a_{ij} is 1 if node i is connected to node j, and 0 otherwise; $P = [p_{ij}]$: the $N \times N$ reliability matrix whose generic element p_{ij} is the overall (here "r" stands for reliability-based $n_{jk}(i)$).probability of connection from node i to node j; $D = [d_{ij}]$: $N \times N$ shortest path matrix whose generic element d_{ij} is the shortest path from node i to node j; $RD = [rd_{ij}]$: $N \times N$ most reliable path matrix whose generic element rd_{ij}, is the most reliable path connecting node i to node j; n_{jk}: the number of shortest paths from node k to node j; $n_{jk}(i)$: the number of shortest paths that contain i; rn_{jk} and $rn_{jk}(i)$: defined analogously to n_{jk} and $n_{jk}(i)$, respectively.

vulnerability for both intentional attacks and random failures,[25,42] the degree centrality measure (C_i^D) has been used in Boccaletti et al.[37] In addition, the betweenness centrality measure (C_i^B) has been shown to be useful to explore the vulnerability of complex systems.[40] Both measures are relevant for power grids, as the former one accounts for the transmission lines (links) which are attached to a substation (node), so that a high-degree node is more vulnerable than a low-degree one, whereas the latter one can account for the flows in the network and identify those which most influence system vulnerability if interrupted.[19,25,39,42,43]

Most previous studies have considered only two centrality measures at most (e.g. local and global efficiency in Eusgeld et al.[22] and betweenness centrality and network efficiency in Zio et al.[32]) for identifying critical elements in network systems. However, in the perspective of future (smart) power grids with physical automation and control, supervision and management, and strategic and policy layers,[43] it is important to provide insights on other aspects of the system, for example, regarding the mechanisms of communication among the consumers and utilities for end-users to actively participate in the network operation by tailoring energy consumption based on individual preferences. Cadini et al. introduced new reliability centrality measures, but these measures have not been used simultaneously in previous works. In this view, information and closeness centrality measures, C_i^I and C_i^C, could be considered for representing structural properties of the network related to the importance of its elements with respect to information exchange capability and communication mechanisms. It should be noted that the future information exchange will most likely not be done through the power grid but with a separate telecommunication system (as is the case for transmission systems, only some distribution systems (up to 20 kV) use to the power grid for communication), but in our study, we are only considering the transmission system. Consideration of the communication system and its interconnection with the transmission system is the subject of future research work.

For completeness, Table 2 reports the definition of the five topological measures used here. Centrality measures have been extended to account for the reliability characteristics of the system elements.[19,28] In this view, while the *topological degree centrality measure* (C_i^D) gives highest score of importance to the node with the largest number of first neighbors, the *reliability degree centrality measure* (RC_i^D) gives highest importance to the node with overall largest reliability of its first links. The *topological node betweenness centrality* (C_i^B) is based on the idea that a node is central if it structurally lies between many other nodes, in the sense that it is traversed by many of the shortest paths connecting pairs of nodes. The measure is extended into the *reliability node betweenness centrality* (RC_i^B), with the meaning that a node is central if it reliably lies between many other nodes in the sense that it is traversed by many of the most reliable links connecting pairs of nodes. The *topological closeness centrality measure* (C_i^C) captures the idea of speed of communication among nodes in a way that the central nodes are those which on average need fewer steps to communicate with the others (and not just the first neighbors). The measure is extended into the *reliability closeness centrality measure* (RC_i^C) according to which a node i is near to all others along the most reliable links. Also, the *topological information centrality measure* (C_i^I), that relates a node importance to the ability of the network to respond to the deactivation of the node (relative drop in the network topological efficiency caused by the removal of the edges incident to it), is extended into the *reliability information centrality measure* (RC_i^I).

Finally, as a global network structure property, the network reliability efficiency $RE[G]$ represents the

Table 3. Sample of transmission links and their reliabilities.

From node	To node	Distance in km	Failure rate (1.0858 occurrence/ year for 100 km)	Reliability $R = e^{-\lambda T}$, $T = 1$ year
3	68	62	0.6732	0.5101
20	82	91	0.9880	0.3722
21	83	186	2.0195	0.1327
22	84	162	1.7589	0.1722
30	31	25	0.2714	0.7622
41	99	76	0.8252	0.4381
42	88	11	0.1194	0.8874
50	72	88	0.9555	0.3846
51	10	154	1.6721	0.1878
63	67	107	1.1618	0.3129
70	99	134	1.4549	0.2334
71	45	200	2.1716	0.1139
80	102	55	0.5971	0.5503
81	15	7	0.0760	0.9268
90	102	257	2.7905	0.0613
91	75	296	3.2139	0.0401
104	41	252	2.7362	0.0648
105	42	43	0.4668	0.6269

extension of the topological efficiency $E[G]$ calculated with reference to the inverse of the shortest path between nodes. In Table 2, the definitions of the centrality measures are given.

Centrality measure analysis of Iran's power transmission network

We have computed the structural and reliability centrality measures, that is $(C_i^D, C_i^C, C_i^B, C_i^I)$ and $(RC_i^D, RC_i^C, RC_i^B, RC_i^I)$, for all 105 nodes (buses or substations) of Iran's power transmission network. For the reliability measures, we adopted the formalism of weighted networks, where the weight is p_{ij}, that is, the probability of the connection link between the pair of nodes i and j (or the probability that is working well in period T). In our case, it is assumed that $p_{ij} = e^{-\lambda_{ij}T}$, where λ_{ij} is the failure rate of edge ij linking nodes i and j, and T is the reference time of analysis that is chosen equal to 1 year. From Table 3, we see that the failure frequency is considered 1.085/100 km/year for all power lines. Furthermore, the lengths of the power lines are actual lengths.[19]

Figure 4 shows the values of the centrality measures. Some of these values are also numerically reported in Table 4.

Correlation analysis

Given the similarity of definition, one may question the degree of correlation among topological and reliability measures in terms of the final importance rankings. In Table 5, we report some ranking results. It can be seen, for instance, that node 103 ranks first from a topological degree centrality standpoint, while node 105 ranks first when reliability degree centrality is considered; however, node 104 stands second in both measures.

In Figure 5, we have plotted the pairs of topological and reliability centrality measures, C_i^D versus RC_i^D, C_i^C versus RC_i^C, C_i^B versus RC_i^B and C_i^I versus RC_i^I: the correlation coefficients are 0.2898, 0.0536, 0.3870, and 0.3065, which shows that the measures are only weakly correlated, at most. This is in contrast with the results by Eusgeld et al.[22] on the Swiss power grid, where the four lines ranked most vulnerable were actually the same for the topological and reliability measures considered. However, in that case, the authors argued that the results might be due to the assumption of equal failure rates for all lines. On the contrary, Bompard et al.[31] used entropic degree, net-ability, and efficiency measures to rank the most vulnerable lines and found that these measures led to completely different sets of most important lines.

Borda Count Method

To aggregate the information from different centrality measures and rank the nodes with respect to their role in the network, we use the Borda Count Method.[44] The analysis is carried out considering the four different reliability centrality measures. In all generality, the Borda Count Method is a voting method in which voters rank candidates in order of preference. Each candidate is given a certain number of points corresponding to the position in which the candidate is ranked by each voter; the candidate with the most points is the winner. Since the Borda Count Method elects a candidate with broadest acceptance, it is often considered as a consensus-based method rather than a majoritarian one.

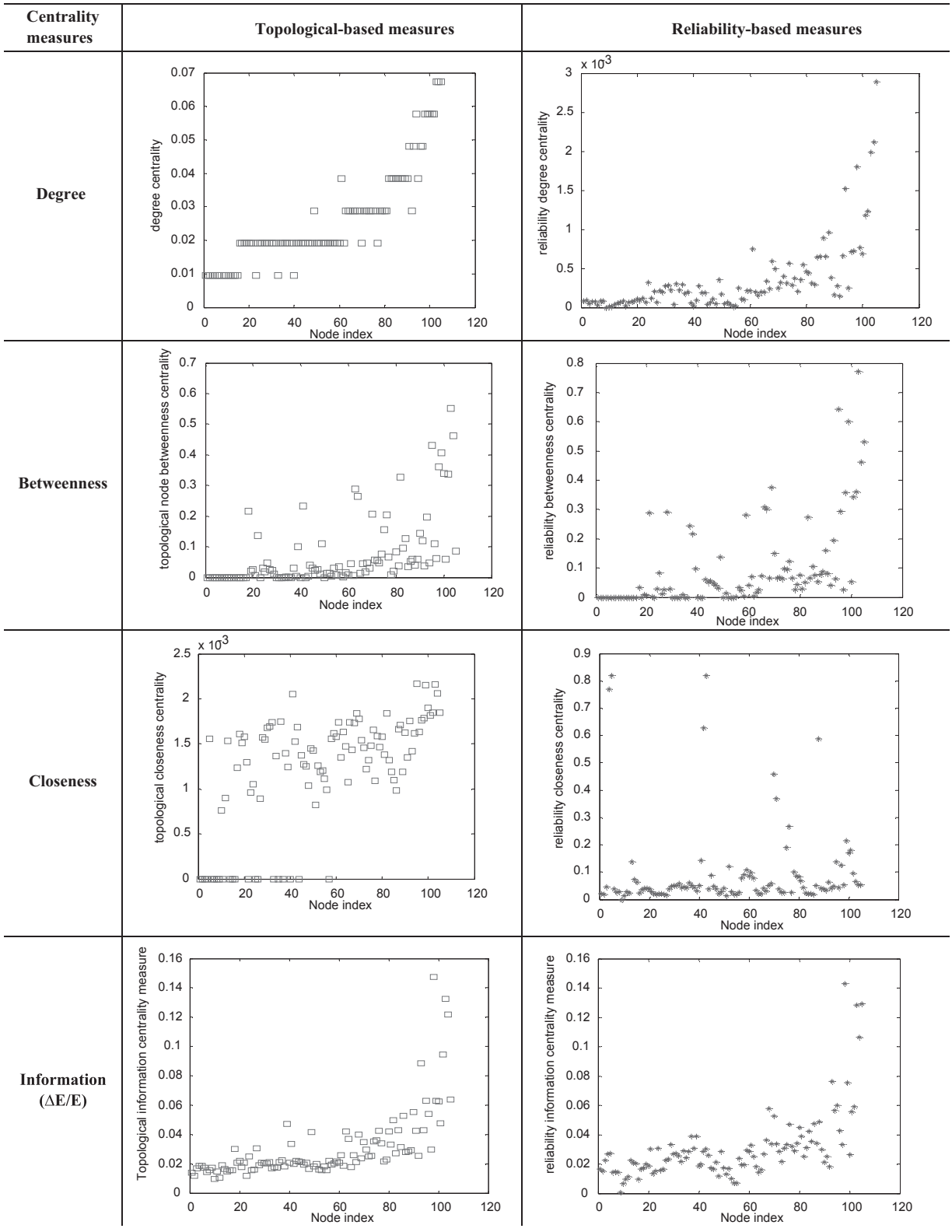

Figure 4. Topological and reliability-based centrality measures.

In our case, the buses are the candidates, and the centrality measures are the voters. The maximum number of points that can be assigned is equal to the number of buses to be ranked, that is, 105—a bus will receive 105 points, each time it is ranked first by one of the centrality measures vote. Then, 104 points are given to a bus that is ranked second by one of the centrality measures and so on, until 1 point is assigned to a bus ranked last. For example, bus number 105 is ranked 1st, 38th, 25th, and 2nd with respect to the four

Table 4. Sample of topological- and reliability-based centrality measure values.

Reliability information $\Delta E/E$	Information $\Delta E/E$	Reliability betweenness	Betweenness	Reliability closeness	Closeness	Reliability degree	Degree	Node index
0.0166	0.0136	0	0	0.0212	0.1111	8.12E−05	0.0096	1
0.0272	0.0187	0	0	0.818	1	7.56E−05	0.0096	5
0.0068	0.0095	0	0	0.0127	0.0769	1.74E−05	0.0096	10
0.0203	0.0146	0	0	0.0629	0.1666	8.57E−05	0.0096	15
0.0187	0.0218	0.0073	0.0264	0.0383	0.2	0.0001	0.0192	20
0.0156	0.0156	0.0819	0.0185	0.0219	0.125	0.0001	0.0192	25
0.0269	0.0204	0	0	0.0507	0.25	0.0002	0.0192	30
0.0243	0.0174	0	0.0021	0.0439	0.1666	0.0002	0.0192	35
0.0189	0.0208	0	0	0.0507	0.25	2.13E−05	0.0096	40
0.0176	0.0211	0.0557	0.0298	0.0870	0.3333	4.22E−05	0.0192	45
0.0175	0.0182	0	0	0.0411	0.2	0.0001	0.0192	50
0.0072	0.0155	0.0003	0.0092	0.0177	0.1428	2.42E−05	0.0192	55
0.0285	0.0206	0.0410	0.0081	0.0861	0.25	0.0002	0.0192	60
0.0160	0.0176	0.0722	0.0124	0.0207	0.1111	0.0002	0.0288	65
0.0527	0.0348	0.1505	0.2063	0.4576	0.5	0.0002	0.0192	70
0.0332	0.0359	0.0945	0.1547	0.1896	0.25	0.0002	0.0288	75
0.0450	0.0420	0.0749	0.0826	0.0822	0.25	0.0004	0.0288	80
0.0355	0.0314	0.1053	0.0352	0.0217	0.125	0.0006	0.0384	85
0.0210	0.0552	0.1593	0.1443	0.0379	0.25	0.0001	0.0384	90
0.0599	0.0629	0.6417	0.4317	0.1379	0.5	0.0002	0.0384	95
0.0262	0.0625	0.0540	0.3394	0.1710	0.5	0.0006	0.0576	100
0.1292	0.0636	0.5309	0.0860	0.0545	0.3333	0.0028	0.0673	105

Table 5. The 20 most vulnerable substations ranked according to the four different reliability measures.

Rank	Degree	Betweenness	Closeness	Information
1	105	103	5	98
2	104	104	43	105
3	103	95	4	103
4	98	99	42	104
5	94	98	88	93
6	102	100	70	99
7	101	102	71	95
8	88	82	76	102
9	86	63	99	68
10	99	64	75	94
11	61	41	101	101
12	97	18	100	70
13	96	70	41	88
14	100	76	13	86
15	93	93	95	76
16	85	75	97	80
17	87	90	52	96
18	84	22	59	84
19	68	84	78	81
20	74	91	61	39

reliability centrality measures, respectively; the total points assigned to such bus is 105 + 68 + 81 + 104 = 358. Figure 6 shows the cumulative number of points for each of the 105 nodes of Iran's power grid.

Table 6 and Figure 7 show the vulnerable nodes categorized for representation purposes in 8 different grades: grade 8 for the most vulnerable nodes with total points between 350 and 400 down to grade 1 for the least vulnerable nodes with total points between 0 and 50. It appears that less vulnerable nodes are often outsiders, with less links, connecting the transmission network to the consumer (grades 1 and 2 in Figure 7). From grades 3 to 8, we see that the vulnerable nodes are often insider nodes (see grades 3–8 in Figure 7). Figure 8, aggregates all grades to show the general map of vulnerable nodes across Iran's power grids.

Network robustness

In network theory, robustness refers to the ability of a network to continue functioning even though a fraction of its components are failed.[37] We can investigate the robustness of a network according to two paradigms of analysis, static and dynamic. In the static analysis of robustness, we remove a node from a network without any redistribution of its loads (or flows). In the dynamic analysis, flows are redistributed in the network after a node or link failure. For example, see Casals et al.[39] for a static investigation of the robustness of the European power grid, and Newman et al.[9] and Chen et al.[42] for a study of the robustness of the power grid from the system dynamics point of view.

In this section, we investigate the robustness of Iran's high-voltage power grids with respect to node removals in a static setting of analysis, that is, without load redistribution. Figure 9 displays the network global efficiency E_{glob}[37,45,46] as a function of the fraction of nodes removed. This measure is a global indicator of the traffic capacity of a network,[37] and the reliability efficiency in the transmission between two substations i and j is defined to be inversely proportional to the distance of the shortest (most reliable) path linking them.[22]

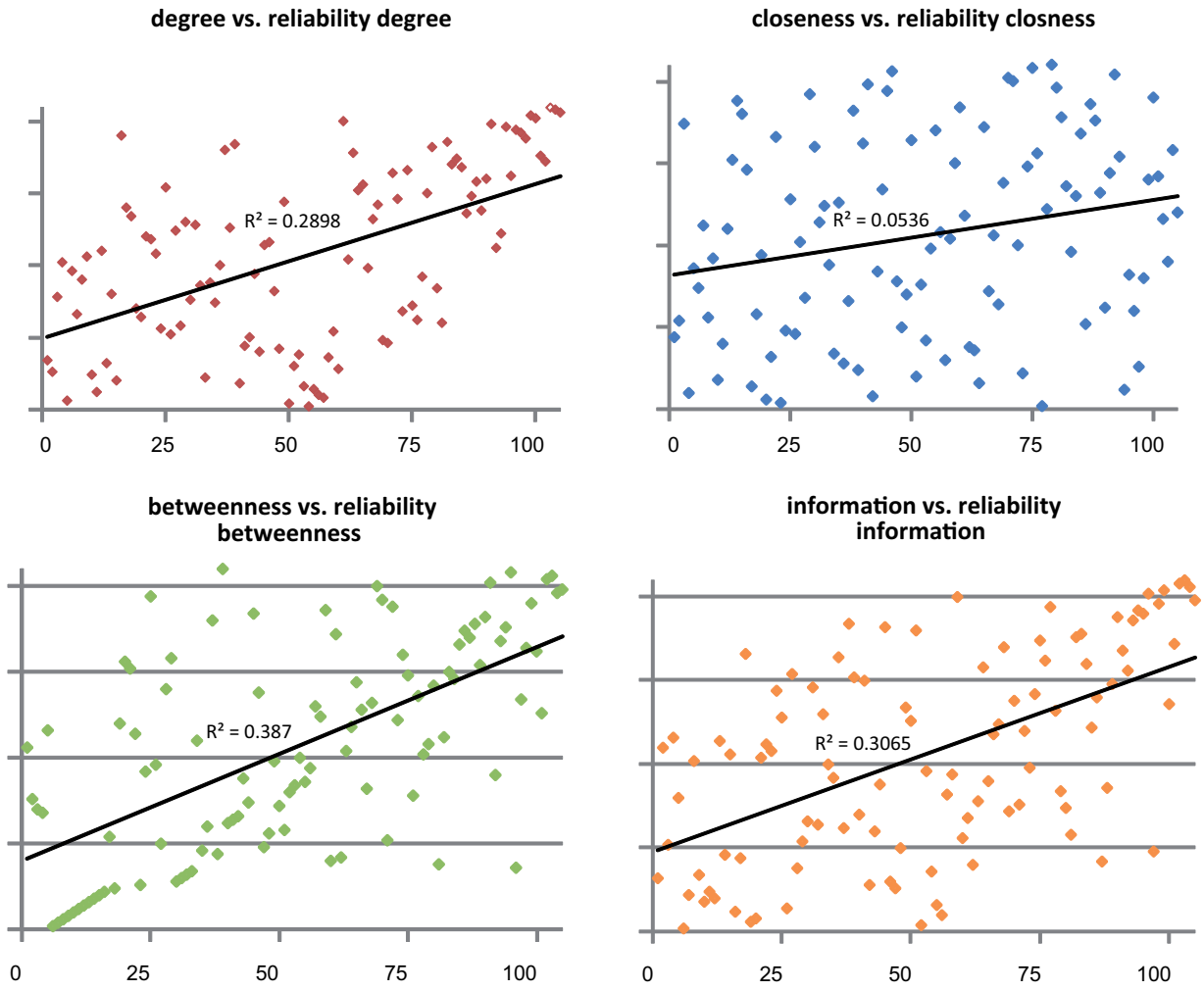

Figure 5. Topological versus reliability-based measures correlation: degree measure (top-left), closeness measure (top-right), betweenness measure (bottom-left) and information measure (bottom-right).

Table 6. Vulnerable nodes in eight different grades.

Node index at different grades of vulnerability							
Grade 1 Point: 0–50	Grade 2 Point: 50–100	Grade 3 Point: 100–150	Grade 4 Point: 150–200	Grade 5 Point: 200–250	Grade 6 Point: 250–300	Grade 7 Point: 300–350	Grade 8 Point: 350–400
9	1	3	13	4	37	59	76
10	2	17	14	5	38	61	88
53	6	18	15	21	43	68	95
54	7	20	19	24	49	69	98
	8	26	25	28	60	70	99
	11	27	35	29	66	71	101
	12	30	41	31	67	75	102
	16	32	44	34	72	79	103
	22	33	45	36	74	80	104
	23	40	46	39	78	93	105
	48	50	47	42	81	94	
	51	52	56	62	83	96	
	55	63	57	73	84	97	
		64	58	77	85	100	
			65	82	86		
			92	90	87		
				91	89		
4	13	14	16	17	17	14	10
Total number of nodes in a grade							

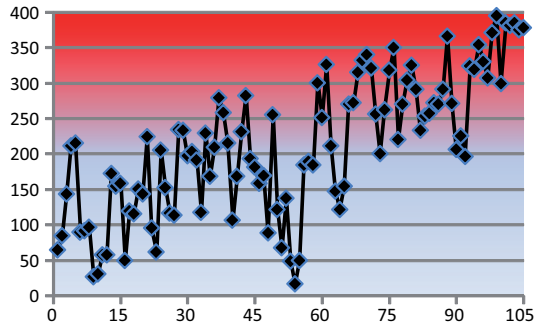

Figure 6. Total cumulated points according to the Borda Count Method for nodes indexed 1–105.

We see from Figure 9 that by removing only 2% of nodes in a random fashion, the network loses only 2% of its efficiency, whereas by attacking 2% of the most central nodes, the loss of efficiency is 42%. Furthermore, by randomly removing 20% of the nodes, the network loses 50% of efficiency, whereas by attacking 20% of the most central nodes, 80% of the efficiency is lost. The network is thus highly sensitive to attacks targeting nodes with high centrality. When removing one node at a time, the analysis allows pointing out those nodes which can affect mostly the efficiency of the network (Figure 10).

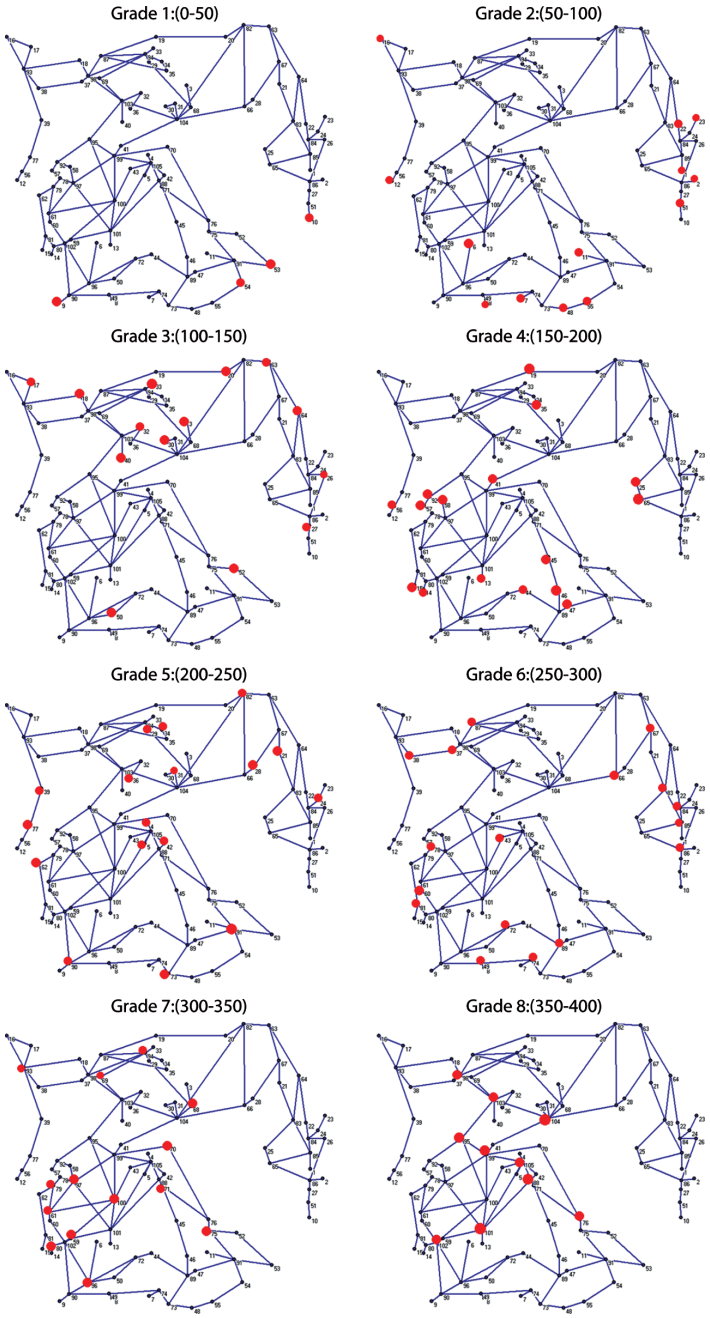

Figure 7. Vulnerable nodes (buses or substations) ranked by the Borda Count Method at different grades: grade 8 with total points between 350 and 400 as the most vulnerable nodes and grade 1 with total points of 0–50 as the least vulnerable nodes. The most vulnerable nodes are shown by larger nodes in red color.

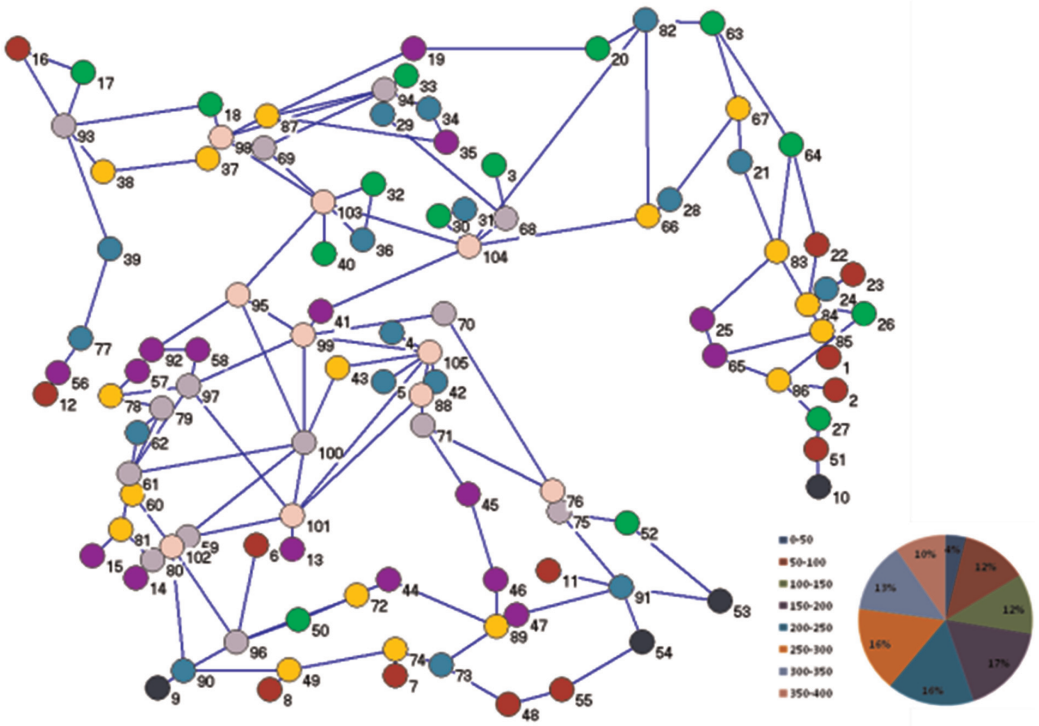

Figure 8. Eight grades of vulnerable nodes in Iran's 400-kV power grids.

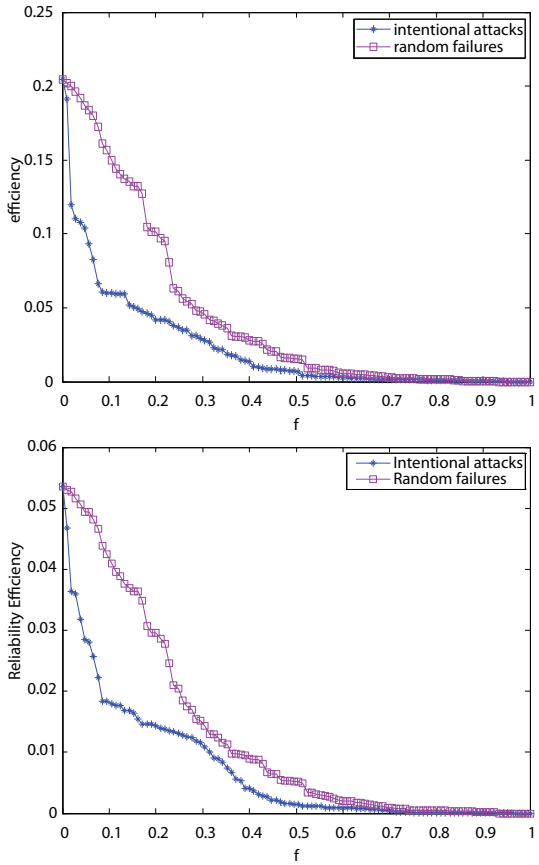

Figure 9. Robustness against random errors or intentional attacks: topological (top) and reliability-based (bottom).

Conclusion

This article concludes by discussing how different reliability-based measures can be used to improve the design and management of real-world power systems. We have considered four different centrality measures, that is, betweenness, closeness, degree, and information to provide insights to the complexity of interrelations among the components of power grids from the purely topological point of view and also considering their reliability characteristics. We have shown that reliability characteristics are different from topological results, as they are mostly uncorrelated. We have also proposed to use a voting aggregation method like the Borda Count Method to rank the nodes (buses or substations) of power grids by aggregation of the rankings provided by the four different centrality measures. The ranking results can then drive the analysis of the robustness of the network to intentional attacks and random failures.

Based on the results obtained from our investigations on the specific case study of Iran's power network, we draw the following conclusions:

1. Viewing the results of our analysis with respect to the criterion suggested in Sole et al.,[26] we can classify the transmission network of Iran as a fragile network.
2. As Iran's power grid is homogeneous with respect to degree distribution and heterogeneous with respect to betweenness distribution, robustness

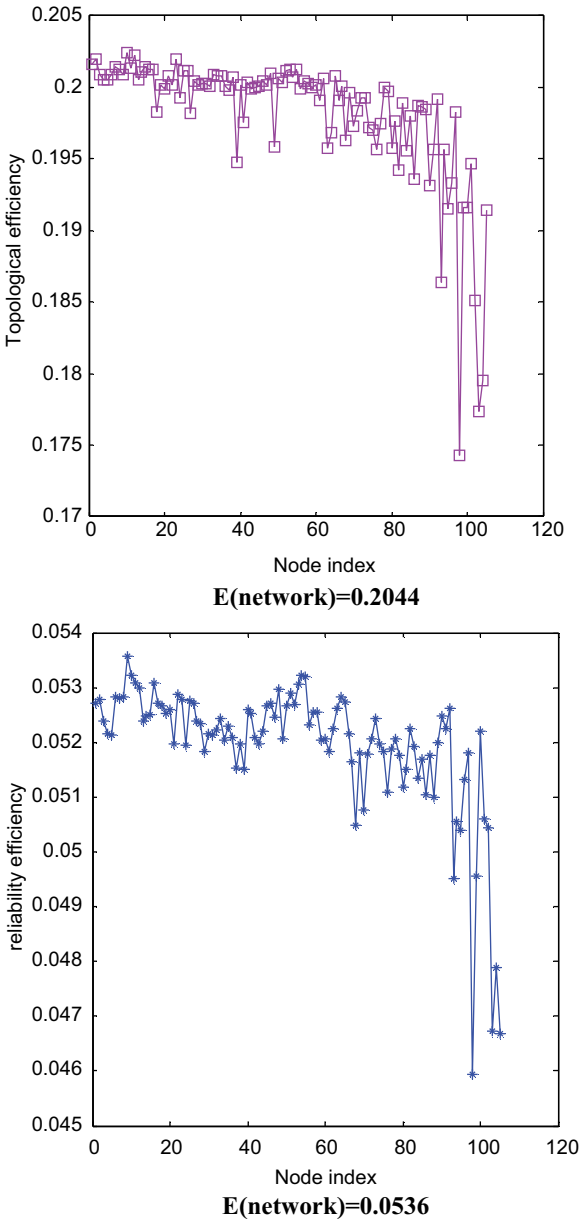

Figure 10. Topological efficiency (top) and reliability efficiency (bottom) values when removing one node at a time.

could be gained if it were possible to dispatch the actual loads/flows homogeneously, that is, so that they follow an exponential distribution; thus, the network would behave more like an Erdos-Renyi random network which is known to perform better with respect to both random failures and intentional attacks. This result is somewhat a logical extension of the analysis provided in Crucitti et al.[47] and Xia et al.[48]

Finally, in future work, we consider improving the structural and reliability modeling of power grids by accounting for aging and sudden shocks due to overloads (currents or voltages). Also, the communication system will be considered explicitly.

Declaration of conflicting interests

The authors declare that there is no conflict of interest.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. Hughes TP. *Networks of power*. London: The Johns Hopkins University Press, 1983.
2. Constable G and Somerville B. *A century of innovation: twenty engineering achievements that transformed our lives*. Washington, DC: Joseph Henry Press, 2003.
3. Wood AJ and Wollenberg BF. *Power generation, operation and control*. New York: John Wiley & Sons, Inc., 2005.
4. Houston G and Johnson C. *EPRI-GTC overhead electric transmission line siting methodology*. Palo Alto, CA: Electric Power Research Institute, 2006.
5. Casals MR. Topological complexity of the electricity transmission network, implications in the sustainability paradigm. Barcelona: Universitat Politècnica de Catalunya, 2009.
6. Mohammadpour J and Grigoriadis KM. *Efficient modeling and control of large-scale systems*. New York: Springer, 2010.
7. Strogatz SH. Exploring complex networks. *Nature* 2001; 410: 268–276.
8. UCTE. *Final Report System Disturbance on 4 November 2006*, 2007, UCTE: UCTE Members (European Countries).
9. Newman DE, Carreras BA, Degala NS, et al. Risk metrics for dynamic complex infrastructure systems such as the power transmission grid. In: *45th Hawaii international conference on system science* 2012, Maui, Hawaii: IEEE.
10. Billinton R and Li W. *Reliability assessment of electric power systems using Monte Carlo methods*. New York: Plenum Press, 1992.
11. Zhu J. *Optimization of Power system Operation*. 2009, Hoboken, New Jersey: John Wiley & Sons.
12. Milano F. *Power system modelling and scripting*. London: Springer-Verlag Ltd, 2010.
13. Zio E. Review: reliability engineering 2008: old problems and new challenges. *Reliab Eng Syst Safe* 2009; 94: 125–141.
14. Kastenberg WE. Assessing and managing the security of complex systems: shifting the RAMS paradigm. In: *Proceedings of the 29th ESReDA seminar on systems analysis for a more secure world*, 2005. Ispra, Italy: JRC-IPSC.
15. Érdi P. *Complexity explained*. Heidelberg: Springer-Verlag, 2008.
16. Dorogovtsev SN and Mendes JFF. *Evolution of networks*. New York: Oxford University Press, 2001.
17. Koonce AM. Bulk power risk analysis: ranking infrastructure elements according to their risk significance. In: *Massachusetts Institute of Technology. Dep. of Nuclear Science and Engineering* 2006, Massachusetts Institute of Technology: USA.

18. Kiureghiana AD and Song J. Multi-scale reliability analysis and updating of complex systems by use of linear programming. *Reliab Eng Syst Safe* 2008; 93: 288–297.
19. Cadini F, Zio E and Petrescu CA. Optimal expansion of an existing electrical power transmission network by multi-objective genetic algorithms. *Reliab Eng Syst Safe* 2010; 95: 173–181.
20. Haarlaa L, Pulkkinenb U, Koskinenc M, et al. A method for analysing the reliability of a transmission grid. *Reliab Eng Syst Safe* 2008; 93: 277–287.
21. Pottonen L. *A method for the probabilistic security analysis of transmission grids*. Espoo: Helsinki University of Technology, 2005.
22. Eusgeld I, Kroger W, Sansavani G, et al. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliab Eng Syst Safe* 2009; 94: 954–963.
23. Albert R and Jeong H. Error and attack tolerance of complex networks. *Nature* 2000; 406: 378–382.
24. Amin M. Toward self-healing energy infrastructure systems. *IEEE Comput Appl Pow* 2001; 14(1): 20–28.
25. Chen G. Attack structural vulnerability of power grids: a hybrid approach based on complex networks. *Physica A* 2010; 389: 595–603.
26. Sole RV, Casals MR, Murta BC, et al. Robustness of the European power grids under intentional attacks. *Phys Rev E* 2008; 77(2): p.026102.
27. Zemljica B and Hlebecb V. Reliability of measures of centrality and prominence. *Soc Networks* 2005; 27: 73–88.
28. Zio E. From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures. *Int J Crit Struct* 2007; 3: 488–508.
29. Zio E, Petrescu A-C and Sansavani G. *Vulnerability analysis of a power transmission system*. Milan: Department of Energy, Polytechnic of Milan, 2008.
30. Zio E, Sansavani G, Maja R, et al. *Analysis of the safety efficiency of a road network: a real case study*. R&RATA, 2008b. **1**(2): p. 172–179.
31. Bompard E, Napoli R and Xue F. Analysis of structural vulnerabilities in power transmission grids. *Int J Crit Infrastruct Prot* 2009; 2: 5–12.
32. Zio E, Golea LR and Rocco SCM. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms. *Reliab Eng Syst Safe* 2012; 99: 172–177.
33. Zio E, Golea LR and Sansavani G. Optimizing protections against cascades in network systems: a modified binary differential evolution algorithm. *Reliab Eng Syst Safe* 2012; 103: 72–83.
34. Zio E, Piccinelli R, Delfanti M, et al. Application of the load flow and random flow models for the analysis of power transmission networks. *Reliab Eng Syst Safe* 2012; 103: 102–109.
35. Li YF, Sansavini G and Zio E. Non-dominated sorting binary differential evolution for the multi-objective optimization of cascading failures protection in complex networks. *Reliab Eng Syst Safe* 2013; 111: 195–205.
36. Monfared MAS and Alipour Z. Structural Properties and Vulnerability of Iranian 400kv Power Transmission Grid: A Complex Systems Approach. *Industrial Engineering & Management*, 2013. 2(3).
37. Boccaletti S, Latora V, Moreno Y, et al. Complex networks: structure and dynamics. *Phys Rep* 2006; 424: 175–308.
38. Rosato V, Bologna S and Tiriticco F. Topological properties of high-voltage electrical transmission networks. *Electr Pow Syst Res* 2007; 77: 99–105.
39. Casals MR, Valverde S and Sole RV. Topological vulnerability of the European power grid under errors and attacks. *Int J Bifurcat Chaos* 2007; 17(7): 2465–2475.
40. Wang K, et al. An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load. *Physica A* 2011; 390: 4692–4701.
41. Watts DJ and Strogatz SH. Collective dynamics of "small-world" networks. *Nature* 1998; 393: 440–442.
42. Chen G, Dong ZY, Hill D, et al. An improved model for structural vulnerability analysis of power networks. *Physica A* 2009; 388: 4259–4266.
43. Crucitti P, Latora V, Marchiori M, et al. Error and attack tolerance of complex networks. *Physica A* 2004; 340: 388–394.
44. Zwicker W. The voters' paradox, spin, and the Borda count. *Math Soc Sci* 1991; 22: 181–227.
45. Latora V and Marchiori M. Efficient behavior of small-world networks. *Phys Rev Lett* 2001; 87(19): 1–4.
46. Latora V and Marchiori M. Economic small-world behavior in weighted networks. *Eur Phys J B* 2003; 32: 249–263.
47. Crucitti P, Latora V and Marchiori M. A topological analysis of the Italian electric power grid. *Physica A* 2004; 338: 92–97.
48. Xia Y, Fan J and Hill D. Cascading failure in Watt-Strogatz small-world networks. *Physica A* 2010; 389: 1281–1285.