A Complex Network Approach to Power System Vulnerability Analysis based on Rebalance Based Flow Centrality

Alma Ademovic Tahirovic, David Angeli and Goran Strbac
Department of Electrical and Electronic Engineering
Imperial College London
SW7 2AZ London, United Kingdom
{a.ademovic14, d.angeli, g.strbac}@imperial.ac.uk

***Abstract*—The study of networks is an extensively investigated field of research, with networks and network structure often encoding relationships describing certain systems or processes. Critical infrastructure is understood as being a structure whose failure or damage has considerable impact on safety, security and wellbeing of society, with power systems considered a classic example. The work presented in this paper builds on the long-lasting foundations of network and complex network theory, proposing an extension in form of *rebalance based flow centrality* for structural vulnerability assessment and critical component identification in adaptive network topologies. The proposed measure is applied to power system vulnerability analysis, with performance demonstrated on the IEEE 30-, 57- and 118-bus test system, outperforming relevant methods from the state-of-the-art. The proposed framework is deterministic (guaranteed), analytically obtained (interpretable) and generalizes well with changing network parameters, providing a complementary tool to power system vulnerability analysis and planning.**

***Index Terms*—centrality, complex networks, graph/network theory, network flow, power system vulnerability analysis.**

I. INTRODUCTION

The study of networks is an extensively investigated field of research [1], with networks and network structure often encoding relationships between subsystems composing certain systems or processes [2]-[4]. The mathematical concepts developed as part of the corresponding frameworks are used extensively in understanding *complex network* behavior [5]. Complex networks correspond to a branch of network theory concerned with structural properties of real-world networks (physical or abstract), which often interchangeably exhibit both random [6] and/or ordered features [7], [8], making them hard to generalize and study.

A network can thereby correspond to an infrastructure, a collection of basic physical and organizational structures and facilities, needed for the operation of a society or organization [9]. A critical infrastructure is understood as being a structure whose failure or damage has considerable impact on safety, security, wellbeing, health and economy of a society [10], [11]. A power system is considered a classic example of a critical infrastructure, with current *power system vulnerability* assessment involving four major methodological classes [10]: *topological methods*, methods based on geodesic centrality [12]-[14], which have the intuition of critical component identification, however, have no regard of the underlying processes and are concerned with topological properties only; *flow based methods*, methods based on flow betweeness centrality [15]-[17], which explore network utilization limits based on residual capacity, however, have certain limitations addressed in more detail in this paper; *logical methods*, such as hierarchical clustering techniques [18]-[20], which reduce network complexity and identify critical elements in different failure scenarios, however, may fail to generalize and adapt to changing network parameters, since driven by data; *functional methods*, methods based on energy functions and dynamic modeling [21], [22], which most closely simulate dynamic system behaviour, however, they are computationally intractable and hardly applicable to larger systems.

Flow based methods, specifically those based on flow betweenness (max-flow) centrality [23], have been considered in some recent work related to power system vulnerability assessment [15]-[17]. Their benefit, in contrast to some other power system vulnerability assessment methods, is that they generalize well with changing network parameters. The max-flow model formulation, however, is only valid under the assumption that the system operational limits are reached. The approach does not take adequate consideration of the max-flow context, namely that: max-flow optimal solutions are not uniquely determined (apart for the min-cut or bottleneck); max-flow based centrality and ranking is consequently not consistent for all network components; max-flow only explores residual capacity of a network and has no capability of reallocating capacity limits (failing to account for network rebalance and rewiring, where applicable). Where the system disposes of a certain type of control mechanism, such as unused fast response reserve, demand response, or some form

of switching capability [24], the approach presented in [15]-[17] is not sufficient, as will be presented in this paper.

To address the idea of a changing network topology and the corresponding changes in network flow, a *rebalance based flow centrality* measure is proposed. The proposed framework incorporates the idea of an *adaptive topology*, which is a form of structural response to changing network parameters, derived with respect to the flow balance condition, where network flow is defined with respect to a flow circulation (i.e. supply and demand are mapped into the network structure and treated as flows [2], [3]). Network flow is here derived as a classic Laplacian flow [25], with network transformation enabling incorporation of arc capacity constraints [2], [3]. The result is an updated ranking, with better correspondence to outcomes obtained in assessment of flexible topologies, as will be demonstrated in the section related to application potential of the proposed framework.

The remainder of this paper is organized as follows. Section II provides a brief overview of preliminaries. The proposed framework and mathematical formulation are presented in Section III. Case studies, results and discussion are provided in Section IV. In Section V conclusions and key findings are summarized.

II. Preliminaries

This section contains a brief introduction of preliminaries, an overview of key background concepts, as well as details to the mathematical foundation of the proposed framework.

A. Preliminaries

To obtain a general understanding of the presented work, basic graph and network theoretic terminology is recalled. Further reference is made to well-established literature, such as [1]-[3]. A graph G is an ordered tuple $G = (V, E)$, with a vertex set V of cardinality n (graph order) and edge set E of cardinality m (graph size). The edge set E is a subset $E \subseteq [V]^2$, where $[V]^2$ denotes all two-element subsets of V defining distinct pairs of adjacent vertices, incident to their relevant edge. The adjacency matrix is a matrix $A \in \mathbb{R}^{n \times n}$ encoding all distinct vertex pairs of graph G, while incidence matrix $A_t \in \mathbb{R}^{n \times m}$ is a matrix encoding all incidence pairs of vertices and edges. The graph can be weighted ($\omega: E \to \mathbb{R}$) or unweighted, where ω denotes the corresponding weighting coefficient. The graph is assumed connected, or otherwise decomposed into the union of its connected graph components. A disconnected edge is denoted with zero weight. A graph G represents the underlying topology of a network. A directed graph or digraph is defined as an ordered tuple $G_D = (V, A_N)$. A flow network N_f is a digraph defined on an ordered tuple $N_f = (G_D, c, s, t) \equiv (V, A_N, c, s, t)$. The digraph consist of an arc set $A_N \subseteq V \times V$ of ordered vertex pairs or node pairs. A flow network comprises furthermore of an arc capacity function $c: A_N \to \mathbb{R}^+ \backslash \{0\}$, and a single-source s and single-sink t, which reduce the flow network to a flow circulation, by mapping exogenous flow b into the network.

B. Centrality

A notion of particular interest in network theory is *centrality* [26]-[28], an algebraic concept aimed at quantifying importance, impact or influence of objects composing a network [26]. It originated in social sciences [27], [28], and proceeded to follow two perspectives [23], [26]: closeness perspective, where an object of importance has a high level of impact or status (as a result of its ability to influence), and mediation perspective, where an object of importance provides access to such status (as a result of its ability to control). The most commonly used centrality measures to date follow a shortest path intuition. In most networks, however, transition or flow does not unfold along geodesic trajectories [26]. This motivated a new approach to centrality research, incorporating aspects of flow in the assessment. The following three types of flow based centralities are addressed in this paper, namely: flow betweenness [23], random walk betweenness [29], and potential based vulnerability [30], with more details provided in the following subsections.

III. Mathematical Formulation

In this section an overview of key mathematical concepts is presented, including details and mathematical formulation of the proposed framework. Details to the relevant state-of-the-art reference approach are presented as well.

A. Flow Betweenness (Max Flow)

Flow based methods, specifically those based on flow betweenness (max-flow) centrality [23], have been considered in some recent work related to power system vulnerability assessment [15]-[17]. The latest approach, presented in [17], corresponds to transforming the network to a flow circulation [2], [3], then finding the maximum throughput in line with the notion of flow betweenness centrality [23], as

$$C_M(i,j) = \sum_{\tilde{s} \in S_N} f_m^{\tilde{s}}(i,j) / f_{max}^{\tilde{s}}, \quad \forall (i,j) \in E \qquad (1)$$

where $C_M(i,j)$ stands for the max-flow based centrality of edge $(i,j) \in E$, $f_m^{\tilde{s}}(i,j)$ stands for the corresponding max-flow and $f_{max}^{\tilde{s}}$ stands for the maximum st-flow, under scenario $\tilde{s}$. To deduce the strain on the power system and obtain different network configuration scenarios $\tilde{s} \in S_N$, a PCA transformation is performed to extract the most representative coordinates (principal components) from a historical data set of supply and demand data. Extreme operating conditions are obtained at the boundary of the convex hull of a transformed data set.

In [17] authors conclude that: flow betweenness identifies critical lines of the power system efficiently; the measure is consistent with system operator's network planning strategy (which is expert and simulation based); the measure is more sensitive to intentional attacks, as verified by a series of simulated attacks. The max-flow model formulation, however, is only valid under the assumption that the system capacity or operational limits are reached. Adequate consideration of the max-flow context is not taken into account, namely that: max-flow obtained flows f_m are not uniquely determined, except for the min-cut (which may result in inconsistent findings); and that max-flow based algorithms explore residual capacity of a network only, having no capability of reallocating capacity limits (failing to account for rebalance and rewiring, where applicable). Flexibility in a max-flow based circulation would have to be introduced in the form of arc capacity buffers to source/sink arcs, which cannot be optimized or adequately assessed with a max-flow.

B. Rebalance Based Flow Centrality (Proposed Framework)

To address the idea of a changing network topology and the corresponding changes in network flow, a *rebalance based flow centrality* measure is proposed. The measure corresponds to an integrated component participation assessment based on some auxiliary flow centrality, e.g.: random walk betweenness (importance) [29] or potential based vulnerability (impact) [30], with consideration of rebalance and topological rewiring. By corresponding network transformation [2], [3], the use of random walk centrality in a capacity constrained network flow model is justified. The proposed framework incorporates the idea of an *adaptive topology*, a form of structural response to changing network parameters, derived with respect to the flow balance condition. It corresponds to a flow rebalance and topological rewiring, where network flow is defined with respect to a circulation (i.e. supply and demand are mapped into the network structure and treated as flows [2], [3]). Network flow is here derived as a classic Laplacian flow [25], with network transformation enabling incorporation of arc capacity constraints [2], [3]. Random walk centrality C_{RW} is obtained directly, in the limit of the corresponding evolution process [29], while potential based vulnerability C_{PB} is derived with respect to resistance distance of the respective edge [30]. The rebalance based flow centrality C_R is obtained as summarized in Algorithm 1.

Algorithm 1: Rebalance Based Flow Centrality C_R - Ranking

Input: Flow network N_f, auxiliary centrality $C^*_{h,0}$, $*: \{V, E: RW, E: PB\}$, score matrix $S_{h,0} \leftarrow C^*_{h,0}(h)$, initial failure $F_{h,0} = \{h\}$, $\forall h \in H$, $H \in \{\{V\}, \{E\}\}$, k failures.

for each $h \in H$ **do**
  Compute $F^*_{h,0} \leftarrow F_{h,0}$, $H^* \leftarrow H$, $d_h \leftarrow 0$, $i \leftarrow 0$.
  while $F_{h,i} \neq \emptyset$ **do**
    Remove faulty component $F^*_{h,i}$, $H^* = H \backslash F^*_{h,i}$, $H^* \in \{\{V^*\}, \{E^*\}\}$.
    Rebalance supply/demand to meet network flow balance condition $\sum_{v \in V^*} b_{h,i}(v) = 0$ [2],[3].
    if $\sum_{v \in V^*} b_{h,i}(v) = 0$ **then**
      Compute $C^*_{h,i+1}(\tilde{h})$, $\forall \tilde{h} \in H^*$, $S_{h,i+1} \leftarrow \max_{\tilde{h} \in H^*} C^*_{h,i+1}(\tilde{h})$, $F_{h,i+1} \leftarrow \text{argmax}_{\tilde{h} \in H^*} C^*_{h,i+1}(\tilde{h})$, $F^*_{h,i+1} \leftarrow F^*_{h,i} \cup F_{h,i+1}$.
    else update $d_h \leftarrow \sum_{v \in V^*} b_{h,i}(v)$, $F_{h,i+1} = \emptyset$.
    $i \leftarrow i + 1$
Compute $\tilde{S} \leftarrow diag(d)\, S$, $C_R(h) \leftarrow \max_{i \in \{1,\dots,k\}} R_i(h)$, $R_i(h)$: $\max\{\tilde{S}_{\tilde{h},i}: F_{\tilde{h},i} = \{h\}\}$.
Sort components $h_1, h_2, \dots, h_z$, $z = |H|$, where $p \leq q$ iff $C_R(h_p) \geq C_R(h_q)$.
return h_p, $p = \overline{1,z}$, $z = |H|$.

Each network component $h \in H$ is considered at least once, as initial cause of failure. Auxiliary centrality (importance [29] or impact [30]) is derived with each rebalance and rewiring, where components are sequentially removed according to the highest centrality score. The output is an $(|H| \times |H|)$ matrix S of centrality scores by removal stage (columns), over $|H|$ initiating components (rows). The second output is an $|H|$ size flow imbalance vector d for each row sequence. Entries are normalized by respective row and vector sums (to account for individual participation). The final score $\tilde{S}$ is obtained as

$$\tilde{S} = diag(d)\, S. \tag{2}$$

The rebalance based flow centrality C_R is obtained with respect to the maximum score $\tilde{S}$, i.e. severity R of component participation in a corresponding removal stage i (column), as

$$C_R = \max_{i \in \{1,\dots,k\}} R_i(h)\,. \tag{3}$$

The result is an updated ranking, with better correspondence to outcomes obtained in assessment of flexible adaptive topologies, as demonstrated in the following section.

IV. Case Studies

In this section an overview of three different case studies is presented, to demonstrate application potential of the proposed framework. Performance is assessed on an IEEE 30-, 57- and 118-bus test system [31]. Assessments are performed on an Intel Xeon E5 2.4GHz CPU, with 64GB RAM.

A. Problem Formulation

The case studies correspond to a problem of power system vulnerability assessment, with respect to an $(n-k)$ security criterion (the problem of finding the smallest k-combination of network components whose removal will cause a flow imbalance by discontinuing a sustained supply of demand). The optimum power flow scheduling model is formulated as in [24]. Comparative assessment is provided with respect to: a benchmark enumerative search as baseline (BC), the max-flow approach (MF) as adopted in [17], and the proposed rebalance based flow centrality approach (RF). Analysis is performed for an $(n-3)$ security criterion (an outage of a k-combination of at most $k = 3$ components out of n), which is considered sufficient for power system applications [10]. Performance is assessed on an IEEE 30-, 57- and 118-bus test system [31]. Line capacity is taken as a 20% increment on nominal line flow (nominal test condition). Flexibility is introduced in form of two types of control mechanisms, namely: post-contingency generation rescheduling (as in [24]) and demand response with a 30% margin (by means of a set of relations comparable to flexible supply). The ranking is presented graphically, as share of demand supplied (Yield), corresponding to a k-component outage by rank (k-rank).

B. IEEE 30-Bus Test System

The results obtained for the IEEE 30-bus test system are presented in Fig. 1a-b. From both figures it can be observed that the proposed rebalance based centrality measure is in better correspondence to benchmark results, as opposed to the max-flow approach adopted in [17]. Furthermore, from Fig. 1b it can be observed that max-flow remains insensitive to any form of system flexibility (it ultimately retains the same ranking as in Fig. 1a) and therefore fails to capture any type of control mechanism, as opposed to the proposed framework which follows the benchmark more closely.

C. IEEE 57-Bus Test System

The results obtained for the IEEE 57-bus test system are presented in Fig. 1c-d. The case study corresponds to the problem of a system reaching operating limits. The max-flow approach performs well under such conditions, however, any form of system flexibility is still not captured. The result is an unaltered ranking for two entirely different outcome scenarios (see MF, Fig. 1c-d), as opposed to the proposed framework.

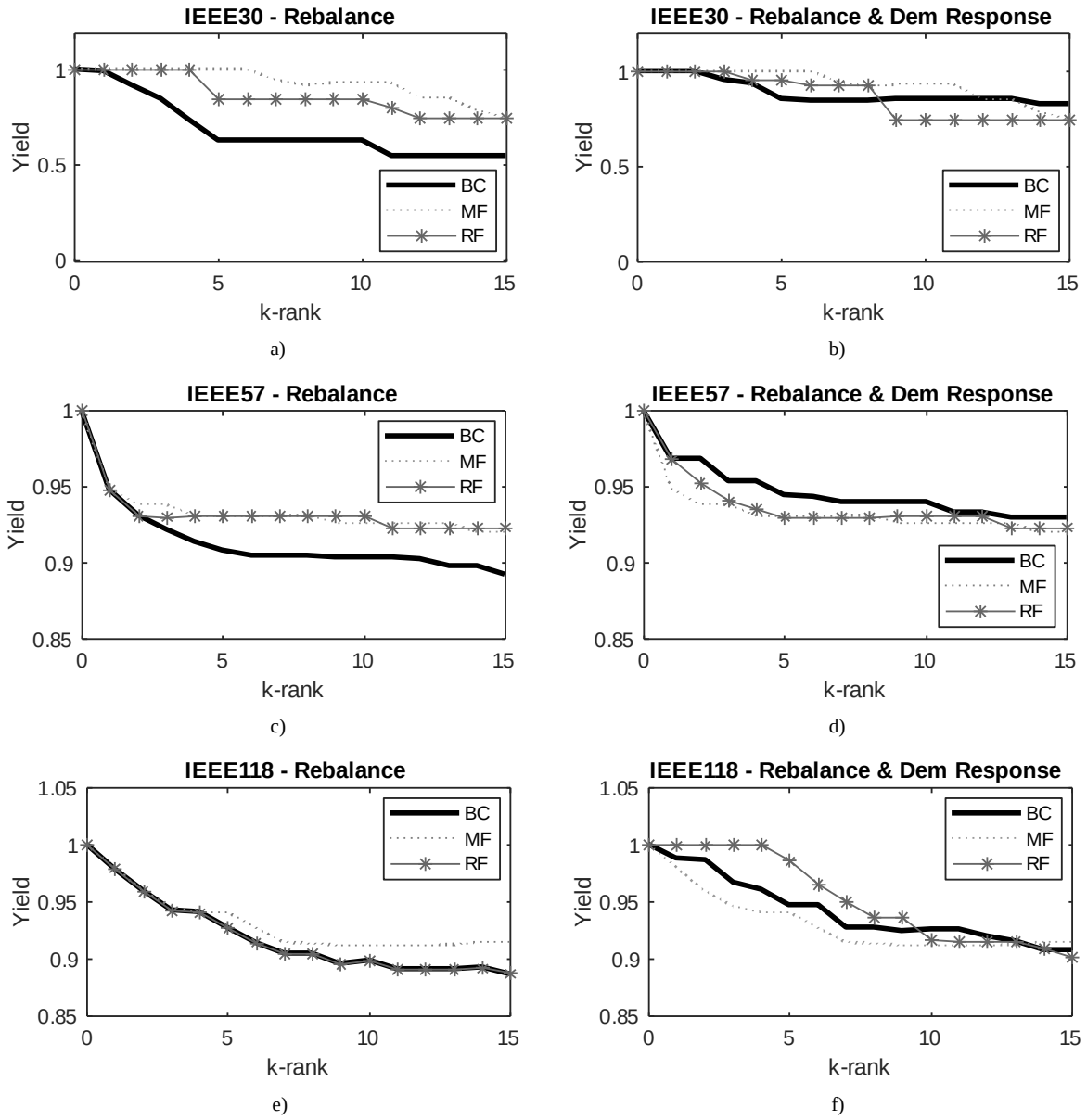

Figure 1. Graphical representation of the top k most critical components by rank: obtained for the highest criticallity $(n-3)$ security criterion [10], with benchmark enumerative search (BC), max-flow adopted in [17] (MF) and proposed rebalance based flow centrality (RF), presented in form of a share of demand supplied (Yield), corresponding to a k-component outage by rank (k-rank), with ranks obtained for two types of control mechanisms - rebalance (one degree of freedom) and rebalance & demand response (two degrees of freedom). Yield is calculated with respect to rebalance only, for comparability of rankings, with individual graphs corresponding to: a) IEEE 30-bus - rebalance, b) IEEE 30-bus - rebalance & demand response, c) IEEE 57-bus - rebalance, d) IEEE 57-bus - rebalance & demand response, e) IEEE 118-bus - rebalance, f) IEEE 118-bus - rebalance & demand response.

D. IEEE 118-Bus Test System

The performance of the proposed rebalance based centrality measure is most visible from the results obtained for the IEEE 118-bus test system, presented in Fig. 1e-f. The proposed framework produces a ranking with identical correspondence to the benchmark enumerative search (Fig 1e). It executes, however, in 26 min time as opposed to 47 days required for a full enumerative assessment (Table I). A good response is obtained with additional demand driven flexibility as well (Fig. 1f), as opposed to max-flow, which again results in an identical, entirely unaffected ranking.

TABLE I. CASE STUDY - EXECUTION TIME

Time [s]	**Methodological Approach**		
	BC	***MF***	***RF***
IEEE 30-bus	52,699.4	3.7	64.8
IEEE 57-bus	377,444.9	46.5	106.1
IEEE 118-bus	4,067,905	807.2	1,915.1

E. Discussion

From the results presented in Fig. 1a-f it can be observed that the proposed rebalance based centrality measure has a better correspondence to the benchmark result and responds to changes in outcomes more closely than the max-flow approach adopted in [17]. The max-flow approach has no regard of system flexibility and fails to capture any type of control mechanism, thereby always retaining the same ranking. The $k = 3$ most critical components identified in the benchmark assessment, are found in the top 1.7%-37.5% of the ranking for max-flow, as opposed to 1.1%-24.7% for the proposed framework. The proposed framework serves as an auxiliary tool, facilitating structural vulnerability and critical component identification, by reducing the search space and decreasing computational time considerably. It is thereby particularly convenient for planning applications, where parameters are optimized, not a priori known or changing. The proposed framework is deterministic (guaranteed), analytically obtained (interpretable) and generalizes well with changing network parameters, providing a complementary tool to power system vulnerability analysis and planning.

V. Conclusions

The study of networks is an extensively investigated field of research, with networks and network structure often encoding relationships describing certain systems or processes. The work presented in this paper builds on the long-lasting foundations of network and complex network theory, proposing an extension in form of a rebalance based flow centrality for structural vulnerability assessment and critical component identification in adaptive network topologies. The proposed measure is applied to power system vulnerability analysis, with performance demonstrated on the IEEE 30-, 57- and 118-bus test system. The proposed framework outperforms relevant methods from the state-of-the-art and is particularly convenient for planning applications, where parameters are optimized, not a priori known or changing. It facilitates assessment and reduces the search space, decreasing computational time considerably. The proposed framework is deterministic (guaranteed), analytically obtained (interpretable) and generalizes well with changing network parameters, providing a complementary tool to power system vulnerability analysis and planning.

Acknowledgment

The authors would like to thank anonymous reviewers for their valuable comments.

References

[1] R. Diestel, *Graph theory*. Ed. 2. Springer: New York, 2000.
[2] D.P. Bertsekas, *Network optimization: continuous and discrete models. Belmont*, MA: Athena Scientific, 1998.
[3] R.K. Ahuja, T.L. Magnanti, and J.B. Orlin, *Network flows: theory, algorithms, and applications*. Harlow, 2014.
[4] V. Latora, and M. Marchiori, Vulnerability and protection of infrastructure networks. Physical Review E. 2005 Jan 20;71(1):015103.
[5] E. Estrada, *The structure of complex networks: Theory and applications*. Oxford University Press: New York, 2012.
[6] P. Erdos, and A. Renyi, On the evolution of random graphs. Publ. Math. Inst. Hung. Acad. Sci. 1960 Jan;5(1):17-60.
[7] D.J. Watts, and S.H. Strogatz, Collective dynamics of 'small-world' networks. Nature. 1998 Jun;393(6684):440.
[8] A.L. Barabasi, and R. Albert, Emergence of scaling in random networks. science. 1999 Oct 15;286(5439):509-12.
[9] A. Stevenson, editor. *Oxford dictionary of English*. Oxford University Press, USA; 2010 Aug 19.
[10] A. Abedi, L. Gaudard, and F. Romerio, Review of major approaches to analyze vulnerability in power system. ELSEVIER - Reliability Engineering & System Safety. 2019 Mar 1;183:153-72.
[11] E. Zio, Challenges in the vulnerability and risk analysis of critical infrastructures. ELSEVIER - Reliability Engineering & System Safety. 2016 Aug 1;152:137-50.
[12] A. Dwivedi, X. Yu, and P. Sokolowski, Identifying vulnerable lines in a power network using complex network theory. In2009 IEEE International Symposium on Industrial Electronics 2009 Jul 5 (pp. 18-23). IEEE.
[13] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z.W. Geem, A critical review of robustness in power grids using complex networks concepts. Energies. 2015 Sep;8(9):9211-65.
[14] G.A. Pagani, and M. Aiello, The power grid as a complex network: a survey. Physica A: Statistical Mechanics and its Applications. 2013 Jun 1;392(11):2688-700.
[15] A. Dwivedi, X. Yu, and P. Sokolowski, Analyzing power network vulnerability with maximum flow based centrality approach. In2010 8th IEEE International Conference on Industrial Informatics 2010 Jul 13 (pp. 336-341). IEEE.
[16] A. Dwivedi, and X. Yu, A maximum-flow-based complex network approach for power system vulnerability analysis. IEEE Transactions on Industrial Informatics. 2011 Oct 28;9(1):81-8.
[17] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, Power system structural vulnerability assessment based on an improved maximum flow approach. IEEE Transactions on Smart Grid. 2016 May 10;9(2):777-85.
[18] E. Ferrario, N. Pedroni, and E. Zio, Evaluation of the robustness of critical infrastructures by Hierarchical Graph representation, clustering and Monte Carlo simulation. ELSEVIER - Reliability Engineering & System Safety. 2016 Nov 1;155:78-96.
[19] C. Gomez, M. Sanchez-Silva, L. Dueñas-Osorio, and D. Rosowsky, Hierarchical infrastructure network representation methods for risk-based decision-making. Structure and Infrastructure Engineering. 2013 Mar 1;9(3):260-74.
[20] J. Agarwal, D. Blockley, and N. Woodman, Vulnerability of structural systems. Structural Safety. 2003 Jul 1;25(3):263-86.
[21] N. Tsolas, A. Arapostathis, and P. Varaiya, A structure preserving energy function for power system transient stability analysis. IEEE Transactions on Circuits and Systems. 1985 Oct;32(10):1041-9.
[22] P. Bhui, and N. Senroy, Real-time prediction and control of transient stability using transient energy function. IEEE Transactions on Power Systems. 2016 May 10;32(2):923-34.
[23] L.C. Freeman, S.P. Borgatti, and D.R. White, Centrality in valued graphs: A measure of betweenness based on network flow. Social networks. 1991 Jun 1;13(2):141-54.
[24] G. Ayala, and A. Street, Energy and reserve scheduling with post-contingency transmission switching. Electric Power Systems Research. 2014 Jun 1;111:133-40.
[25] F. Bullo, *Lectures on Network Systems*. Version 0.96, January 2018. With contributions by J. Cortes, F. Dorfler, and S. Martınez. URL: http://motion.me.ucsb.edu/book-lns.
[26] S.P. Borgatti, Centrality and network flow. Social networks. 2005 Jan 1;27(1):55-71.
[27] S. Wasserman, and K. Faust, *Social network analysis: Methods and applications*. Cambridge university press; 1994 Nov 25.
[28] J. Scott, *Social network analysis: A handbook*. 2nd edn sage publications.
[29] M.E. Newman, A measure of betweenness centrality based on random walks. Social networks. 2005 Jan 1;27(1):39-54.
[30] S. Soltan, D. Mazauric, and G. Zussman, Analysis of failures in power grids. IEEE Transactions on Control of Network Systems. 2015 Nov 5;4(2):288-300.
[31] Power Systems Test Case Archive. [Online]. Available: http://www.ee.washington.edu/research/pstca/.