Physica A 466 (2017) 295–309

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

A study of the impacts of flow direction and electrical constraints on vulnerability assessment of power grid using electrical betweenness measures

Di Wu [a,*], Feng Ma [b], Milad Javadi [a], Krishnaiya Thulasiraman [c], Ettore Bompard [d], John N. Jiang [a]

[a] School of Electrical and Computer Engineering, University of Oklahoma, Norman, OK, 73019, USA
[b] OGE Energy Corporation, Oklahoma, OK, 73172, USA
[c] School of Computer Science, University of Oklahoma, Norman, OK, 73019, USA
[d] Department of Energy, Polytechnic University of Turin, Turin, 10129, Italy

HIGHLIGHTS

- We analyze the effect of electrical properties on assessment of grid vulnerability.
- Flow direction impacts the identification of critical elements.
- Line limits also affect the identification of critical elements.
- Flow direction and line limits have more significant effects than node constraints.
- Combined electrical betweenness is more effective for detecting critical elements.

ARTICLE INFO

Article history:
Received 5 January 2016
Received in revised form 22 August 2016
Available online 27 September 2016

Keywords:
Power grid vulnerability
Complex network
Betweenness centrality

ABSTRACT

In this paper, we analyze the impacts of major electrical properties, including node constraints, line limits, and flow direction, on vulnerability assessment of power grid using several types of electrical betweenness measures. Specifically, we first propose a set of new electrical betweenness measures, which takes into account flow direction in power grids. Then, the impacts of major electrical properties on vulnerability assessment of power grid are analyzed by comparing the identification results of critical components based on the proposed electrical betweenness measures with those based on the other two types of electrical betweenness measures reported in the literature, which take into consideration node constraints and line limits, respectively. Analysis results show the important impact of flow direction on the identification of critical components. The results lead us to introduce a set of combined electrical betweenness measures that take into account node constraints, line limits, and flow direction together. Simulation results on the IEEE 300-bus system and the Italian power grid show that the combined electrical betweenness measures are superior in identifying critical components and more useful in assessing power grid vulnerability.

* Corresponding author.
E-mail address: dee.d.wu@ou.edu (D. Wu).

http://dx.doi.org/10.1016/j.physa.2016.09.029
0378-4371/

1. Introduction

Network scientists have applied network theory to the vulnerability analysis of power grid. Various measures have been used for this purpose. Betweenness centrality is one of the widely used measures. The betweenness measures are typically calculated based on the shortest paths between node pairs, assuming that information spreads along shortest paths between node pairs in a network. The betweenness measures have been used to identify critical components in real power grids such as North American power grid [1], Italian electric power grid [2], Dutch electric power grid [3], and East China power grid [4]. Also, these measures have been used to develop models for cascading failure analysis in real power grids such as Italian electric power grid [5], Western US power grid [6], North American power grid [7], and Northern China power grid [8].

However, the betweenness measures may not be directly applied to power grid vulnerability analysis. Since they do not take into account essential electrical properties of power grids, analysis results based on the betweenness measures may not accurately describe the characteristics of real power grids [9–13]. In Ref. [10], the betweenness measures have been modified with electrical betweenness measures in which the shortest paths between node pairs are replaced with the electrical paths. Recently, some new electrical betweenness measures have been proposed by taking into account additional electrical properties of power grids. For instance, the electrical betweenness measures reported in Ref. [11] take into consideration node constraints including generation capacity and maximum load demand; the electrical betweenness measures proposed in Ref. [12] include line limits, i.e., line power transmission limits. In these papers, the importance of the electric properties, i.e., node constraints and line limits, in power grid vulnerability analysis has been shown.

In this paper, we first introduce new electrical betweenness measures by taking into account flow direction in power grids. Then, we analyze the impacts of major electrical properties, including node constraints, line limits, and flow direction, on vulnerability assessment of power grid by performing comparative studies of the proposed electrical betweenness and those electrical betweenness reported in Refs. [11,12]. Analysis results show the important impact of flow direction on the identification of critical components. Thus, we further propose a set of combined electrical betweenness measures by including the electrical properties of node constraints, line limits, and flow direction together. We show the effectiveness of the combined electrical betweenness measures in the identification of critical components by performing vulnerability analysis on the IEEE 300-bus system and the Italian power grid.

The rest of the paper is organized as follows. In Section 2, we summarize recent works on the application of complex network concepts in the vulnerability analysis of power grids. In Section 3, models and measures for power grid vulnerability analysis are presented. In Section 4, new electrical betweenness measures with flow direction are introduced, and comparative studies based on simulations are provided. In Section 5, we further propose a set of integrated electrical betweenness measures and provide comparative studies. We conclude in Section 6.

2. A review of power grid vulnerability analysis using complex network concepts

Cascading failures are common in large complex networks such as internet networks, transportation networks, and power grids [6,14–17]. In a power grid, a cascading outage may affect a wide area or even the whole power grid, which causes catastrophic consequences. Thus, the study of cascading failures has become a vibrant research topic in power grid vulnerability analysis [18–23]. Recently, complex network concepts have been used to analyze the vulnerability of power grids against cascading failures. Following the recent reviews presented in Refs. [24,25], we classify related works in the area into two different categories: the purely topological approach and the hybrid approach.

The purely topological approach is mainly based on topological concepts. In this approach, the measures that are used to analyze large complex networks are directly applied to power grids to identify critical components and assess topological vulnerability [26]. This approach has been used to investigate various power grids such as European power grids [27–29], the North American power grid [1], the US Western power grid [30], and the New York power grid [31]. The investigations show that the power grids have a behavior similar to scale-free networks when nodes are removed. That is, the power grids are vulnerable to attacks on the most connected nodes but are robust against random loss of nodes. Thus, the failure of one of the small number of nodes may trigger large-scale blackouts in the power grids. In addition, the purely topological approach has also been used to analyze the structure of power grids. The research in Ref. [32] points out that the US Western power grid seems to be a small-world network. The nature of small-world networks is also found in other power grids such as the Shanghai Power Grid [33], the Italian 380 kV, the French 400 kV and the Spanish 400 kV power grids [34] and the Nordic power grid [30]. The work in Ref. [35] suggests that the degree distribution of the power grid seems to be scale-free following a power law distribution function, but exponential cumulative degree distribution functions are found in Californian power grid [36], the whole US power grid [1], and thirty-three different European transmission power grids [28]. While the purely topological approach is widely used to analyze the vulnerability of power grids, it may lead to inaccurate results since the purely topological approach does not capture electrical properties of power grids [24,25].

To improve the purely topological approach, the hybrid approach has been developed by combining the electrical properties with the topological concepts. In the hybrid approach, various topological measures in complex network analysis have been extended as electrical measures by incorporating the electrical properties [25]. For example, topological measures, such as efficiency, betweenness, and degree, were extended as net-ability, electrical betweenness, and entropy degree in Refs. [13,37–39]. It has been found that the extended electrical measures are more effective to identify critical components in power grids than topological measures. The work in Ref. [40] shows the connection between the analysis results of

the extended electrical measures and real blackout data of German, Italian, French and Spanish power grids. In Ref. [10], a number of other electrical centrality measures have been presented and used to analyze the New York transmission network. It has been found that the electrical centrality measures provide information different from the one based solely on the topological measures and are more effective to identify critical components than topological centrality measures. Additionally, in the hybrid approach, the power flow models of power grids are combined with complex network concepts to analyze the vulnerability of several power grids such as the North China power grid [41], the North American power grid [42] and the Swiss power grid [43].

In the framework of the hybrid approach, it is important to understand how electrical properties of power grids affect vulnerability assessment of power grid. This understanding is useful to effectively extend topological measures for power grid vulnerability analysis. In this paper, we analyze the impacts of major electrical properties of power grids on vulnerability assessment of power grid using several types of electrical betweenness measures. The major electrical properties and these electrical betweenness measures will be described in the following sections.

3. Models and measures for power grid vulnerability analysis

3.1. Power network model

Power flows in a power grid follow laws of physics including Kirchhoff's laws and Ohm's law. The power flow in a power grid with $N_b + 1$ nodes and N_l transmission lines can be described by the following network equations,

$$\mathbf{I}_b = \mathbf{Y}_b \mathbf{V}_b \tag{1}$$

where $\mathbf{I}_b$ is an $N_b \times 1$ vector in which each element is the current injected into a node; $\mathbf{V}_b$ is an $N_b \times 1$ vector in which each element is the voltage at a node; $\mathbf{Y}_b$ is an $N_b \times N_b$ matrix and is called network admittance matrix in which non-diagonal element Y_{ij} is the negative of the admittance of line l_{ij} connecting node i to node j and diagonal element Y_{ii} is the sum of line admittances connected to node i. In (1), the equation corresponding to the voltage reference node is not included. For the transmission network of a power grid, the imaginary part of the admittance of each line is usually much larger than its real part. For the sake of simplicity, in this paper we only consider the imaginary part of the admittance of each line for calculation of power or current flow in a power grid.

In addition to the network equations above, a power grid also has the following essential electrical properties:

- Node constraints: Power or current that is injected into and withdrawn from nodes in a power network is subject to node constraints. The nodes can be classified as three types: generation nodes, load nodes, and transmission nodes. A generation node is a node connected to a generator, where power or current is injected and is subject to generation capacity constraint. A load node is a node connected to a load, where power or current is withdrawn and is subject to maximum load constraint. A transmission node, such as a transfer bus, is a node which is not connected to a generator or a load.
- Line limits: Power flowing through lines is subject to transmission limits. In a power network, power is transmitted along electric paths between nodes, unlike topological paths in social networks, since power flow in a power network is governed by Kirchhoff's laws and Ohm's law. In power transmission, the power through each line is subject to power transmission limit.
- Directional flow: Power flowing through each line is directional. When power or current is transmitted between two nodes, the flow can be in one or other direction depending upon the operating condition of generation and load.

3.2. Measures of vulnerability and approaches

The concept of vulnerability in complex networks usually refers to the extent to which a network performance decreases following a sequential removal of nodes or links. Many topology-based measures have been proposed to quantify vulnerability, such as efficiency [44], size of giant component [45], and cluster coefficient [32]. However, it is found that the direct use of existing topological-based measures may not be sufficient for power grid vulnerability analysis [46–48].

3.2.1. Grid vulnerability measure

In some recent publications, the extent of availability of power supply (PS) following a sequential removal of nodes or links is used to represent vulnerability. For example, in Ref. [48], the PS-based measure below is proposed and used for vulnerability analysis.

$$V_{PS} = \frac{PS_{norm} - PS_{damg}}{PS_{norm}} \tag{2}$$

where PS_{norm} represents the power supply of a power grid in the normal state; PS_{damg} represents the power supply of a power grid after the removal of nodes or links. V_{PS} in (2) is referred to as loss of load in Ref. [11].

V_{PS} can be calculated using direct current (DC) power flow equations

$$\mathbf{P}_l = \mathbf{FP} \tag{3}$$

where $\mathbf{P}_l$ is an $N_l \times 1$ vector in which each element is the power flowing through a line; $\mathbf{F}$ is a constant matrix in which each element is derived by the reactance of a line; and $\mathbf{P}$ is an $N_b \times 1$ vector in which each element is the power injected into a node, and the node connected to reference generator is not included. More details on (3) are provided in Ref. [49].

3.2.2. Approach for assessing grid vulnerability

An approach for assessing grid vulnerability in terms of V_{PS} in (2) is summarized as follows: the vulnerability can be assessed by computing the decrease of V_{PS} following a sequential removal of components, i.e., nodes or links. Due to the loss or removal of certain number of its components, the power grid may break into several parts or sub-grids. In such a case, the PS_{damg} in (2) is the sum of power supplies in each sub-grid. For a sub-grid, the following three scenarios are considered [48]: (1) if the sub-grid does not have any generators or loads, the power supply is zero. (2) If the sum of the supplies from generators is larger than the sum of the demands from loads, then the output of each generator is uniformly reduced to balance the total supply and total demand. Then, (3) is used to calculate the power flow through each line and line flow constraints are checked. If there are violations, the power withdrawn at load nodes is reduced in the order of magnitude of load demands, until there are no violations. (3) If the sum of supplies from all generators is smaller than the sum of loads, the power withdrawn at load nodes is reduced in the order of magnitude of load demands to balance the total supply and total demand, and then line flow limits are checked with (3), which is similar to the one in scenario (2).

3.2.3. Fault mode

In complex networks, vulnerability is usually studied by removing nodes or links to represent the results of fault. The following two major fault modes are often considered:

- In random failures, a given number of nodes or links are selected at random and then removed from the network one by one.
- In intentional attacks, a given number of critical nodes or links are selected according to some measures and then removed from the network one by one in descending order of their criticality.

One of the key actions in intentional attacks is to identify the set of critical components, so that the network performance will drop quickly after these components are removed in descending order of their criticality. Many studies showed that node or link betweenness can be used for the identification of critical components, which will be discussed next.

3.2.4. Topological betweenness measures and electrical betweenness measures

Various betweennesses measures have been used to study the importance of nodes and links in a network. Betweenness is typically calculated based on the shortest paths between node pairs. For a graph $\mathcal{G}(\mathbf{V}, \mathbf{L})$ composed of node set $\mathbf{V}$ and link set $\mathbf{L}$, the betweenness of node m can be represented as [50],

$$TB(m) = \sum_{i \in \mathbf{V}} \sum_{j \in \mathbf{V}} \frac{\sigma_{ij}(m)}{\sigma_{ij}} \quad i \in \mathbf{V},\ j \in \mathbf{V},\ i \neq j \tag{4}$$

and the betweenness of link l_{mn} can be represented as [51],

$$TB(l_{mn}) = \sum_{i \in \mathbf{V}} \sum_{j \in \mathbf{V}} \frac{\sigma_{ij}(l_{mn})}{\sigma_{ij}} \quad i \in \mathbf{V},\ j \in \mathbf{V},\ i \neq j,\ l_{mn} \in \mathbf{L} \tag{5}$$

where σ_{ij} is the number of the shortest paths from node i to node j; $\sigma_{ij}(m)$ is the number of shortest paths from node i to node j that pass through node m; $\sigma_{ij}(l_{mn})$ is the number of shortest paths from node i to node j that pass through the link l_{mn} connecting node m to node n. Eqs. (4) and (5) show that a node or a link is more important if it is passed through more shortest paths between other nodes. That is, the importance of a node or a link in a network can be quantified with the betweenness measures.

The betweenness measures in (4) and (5) quantify the importance of a component based on topological information of a network. In this paper, they are referred to as topological betweenness measures (*TB*).

Recent works showed that *TB* may not be directly applied to the vulnerability analysis of power grid since it does not take into consideration essential electrical properties of power grids such as node constraints and line limits. Rather than relying on *TB*, several electrical betweenness measures have been proposed. Next, two most recently electrical betweenness measures are summarized.

Electrical betweenness measures with node constraints: Electrical betweenness measures taking node constraints into consideration have been presented in Ref. [11]. We refer to these measures as type I electrical betweenness measures (EB_l) in this paper. EB_l of link l_{mn} is represented as,

$$EB_l(l_{mn}) = \sum_{i \in \mathbf{G}} \sum_{j \in \mathbf{D}} \omega_{ij} |I_{ij}(l_{mn})| \tag{6}$$

where **G** is the set of generation nodes; **D** is the set of load nodes; $\omega_{ij} = \min(S_i, S_j)$ is a weight, which represents power transmitted from the generator at node i to the load at node j; S_i is the capacity of the generator at node i; S_j is the maximal demand of the load at node j; $I_{ij}(l_{mn})$ is the current through the link l_{mn} (from node m to node n) for a unit of current transmitted from the generation node i to the load node j.

Based on (6), EB_I of node i is represented as

$$EB_I(i) = \begin{cases} \left(\sum_{j\in\mathbf{F}(i)} EB_I(l_{mn}) + \sum_{k\in\mathbf{D}} \omega_{ik}\right) \Big/ 2 & i \in \mathbf{G} \\ \left(\sum_{j\in\mathbf{F}(i)} EB_I(l_{mn}) + \sum_{m\in\mathbf{G}} \omega_{mi}\right) \Big/ 2 & i \in \mathbf{D} \\ \left(\sum_{j\in\mathbf{F}(i)} EB_I(l_{mn})\right) \Big/ 2 & i \in \mathbf{T} \end{cases} \tag{7}$$

where **T** is the set of transmission nodes; $\mathbf{F}(i)$ is the set of nodes connected to node i; $\sum_{k\in\mathbf{D}} \omega_{ik}$ represents the sum of the total power that is transmitted from generation node i to all load nodes. $\sum_{m\in\mathbf{G}} \omega_{mi}$ represents the sum of the total power that the load at node i withdraws from all generation nodes; coefficient 1/2 is used since the power entering into a node i along links is equal to the power leaving from node i.

In Ref. [11], it has been demonstrated that EB_I is more useful to identify critical nodes and links since it takes into consideration node constraints including generation capacity and maximal load demand.

Electrical betweenness measures with line limits: Electrical betweenness measures taking into account line power transmission limits have been reported in Ref. [12]. We refer to these measures as type II electrical betweenness measures (EB_{II}) in this paper. EB_{II} of link l_{mn} is represented as,

$$EB_{II}(l_{mn}) = \max\left[\sum_{i\in\mathbf{G}}\sum_{j\in\mathbf{D}} C_{ij} f_{ij}(l^+_{mn}), \sum_{i\in\mathbf{G}}\sum_{j\in\mathbf{D}} C_{ij} f_{ij}(l^-_{mn})\right] \tag{8}$$

where $f_{ij}(l_{mn})$ is the power through the link l_{mn} for a unit of power transmitted from generation node i to load node j; $f_{ij}(l^+_{mn})$ represents the power through link l_{mn} along the given direction of link l_{mn}; $f_{ij}(l^-_{mn})$ represents the power through link l_{mn} against the given direction of link l_{mn}. Note that for a given pair of generation and load nodes, either $f_{ij}(l^+_{mn})$ or $f_{ij}(l^-_{mn})$ is zero since the power through link l_{mn} only has one direction for the power transmission between a pair of generation and load nodes. C_{ij} is a weight, which represents the maximum power that can be transmitted from generation node i to load node j without violating the power transmission limits of the lines. C_{ij} can be represented as,

$$C_{ij} = \min_{l_{mn}\in\mathbf{L}} \left(\frac{P_{\max}(l_{mn})}{|f_{ij}(l_{mn})|}\right) \tag{9}$$

where $P_{\max}(l_{mn})$ is the power transmission limit of link l_{mn}.

EB_{II} of node m is represented as,

$$EB_{II}(m) = \frac{1}{2}\sum_{i\in\mathbf{G}}\sum_{j\in\mathbf{D}} C_{ij} \sum_{n\in\mathbf{F}(m)} |f_{ij}(l_{mn})| \quad m \neq i \text{ and } m \neq j \tag{10}$$

where $\mathbf{F}(m)$ is the set of lines connected to node m; $C_{ij}\sum_{n\in F(m)} |f_{ij}(l_{mn})|$ represents the sum of the power through all lines connected to node m when the power equal to C_{ij} is transmitted from generation node i to load node j; coefficient 1/2 is used since the power entering into a node m equal to the power leaving from node m. Eq. (10) is only used for transmission nodes. For generation nodes, an additional term $\sum_{k\in\mathbf{D}} C_{mk}/2$ is included in (10) while for load nodes, (10) has an additional term $\sum_{k\in\mathbf{G}} C_{km}/2$.

4. Electrical betweenness measures with flow direction

EB_I and EB_{II} presented in previous section take into consideration two essential electrical properties of power grids, i.e., node constraints and line limits. However, another important electrical characteristic of power grids – flow direction – is not taken into consideration appropriately. In this section, a new set of electrical betweenness measures with flow direction is proposed.

4.1. Electrical betweenness measures with flow direction

As mentioned in Section 2, directional flow through a link is another important electrical property of power grids. When the power is transmitted between a pair of generation and load nodes, the power through a link may flow along its given reference direction. But the direction of power through the same link may be reversed for the power transmission between another pair of generation and load nodes. When the power is transmitted between multiple pairs of generation and load nodes, the actual power is the difference between the total power transmitted in one direction and the total power transmitted in the other direction. Thus, we propose a set of electrical betweenness measures with flow direction. We refer to these measures as type III electrical betweenness measures (EB_{III}) in this paper. EB_{III} of link l_{mn} can be written as,

$$EB_{III}(l_{mn}) = \left| \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{+}) + \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{-}) \right| \tag{11}$$

where $\sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{+})$ represents the total power through link l_{mn} along the reference direction of link l_{mn}; $\sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{-})$ represents the power through link l_{mn} against the reference direction.

Based on (11), EB_{III} of node i is given below.

$$EB_{III}(i) = \begin{cases} \left(\sum_{j\in\mathbf{F}(i)} EB_{III}(l_{mn}) + N_D \right) \Big/ 2 & i \in \mathbf{G} \\ \left(\sum_{j\in\mathbf{F}(i)} EB_{III}(l_{mn}) + N_G \right) \Big/ 2 & i \in \mathbf{D} \\ \left(\sum_{j\in\mathbf{F}(i)} EB_{III}(l_{mn}) \right) \Big/ 2 & i \in \mathbf{T} \end{cases} \tag{12}$$

where $\sum_{j\in\mathbf{F}(i)} EB_I(l_{mn})$ represents the sum of the power through all links connected to node i when the power is transmitted between all pairs of generation nodes and load nodes; N_D is the total number of load nodes; N_G is the total number of generation nodes. Since a unit of power is assumed to be transmitted between each pair of generation node and load node, N_D also represents the total power transmitted from a generation node to all load nodes, and N_G represents the total power that a load withdraws from all generation nodes.

To further explain flow direction taken into account in EB_{III}, let us consider a simple network as shown in Fig. 1. In this network, each link has its given reference direction of flow, which is indicated with black arrow. The red arrow indicates the direction of flow through each link when the power is transmitted from generation node 1 to load node 3. The blue arrow indicates the direction of flow through each link when the power is transmitted from generation node 2 to load node 3. From Fig. 1, it can be seen that for the power transmission from generation node 1 to load node 3, link l_{12} has a positive power $f_{13}(l_{12}^{+})$, which means the flow is in the reference direction; for the power transmission from generation node 2 to load node 3, link l_{12} has a negative power $f_{23}(l_{12}^{-})$, which means the flow is against the reference direction. When the power is transmitted from the two generation nodes to the load node, the actual power through link l_{12} is equal to $f_{12}(l_{12}^{+}) + f_{23}(l_{12}^{-})$.

$EB_{III}(l_{mn})$ defined in (11) takes flow direction into consideration since it is defined as the absolute value of the sum of the total power through a link in two different directions (i.e., $\left| \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{+}) + \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} f_{ij}(l_{mn}^{-}) \right|$). However, both $EB_I(l_{mn})$ described in (6) and $EB_{II}(l_{mn})$ described in (8) do not take flow direction into account.

4.2. Illustration

To illustrate the differences in the calculations and identification results of EB_I–EB_{III}, a simple case study is now presented. As shown in Fig. 2, two generators are connected to a load via three transmission lines. The constraints on generation and load as well as line power transmission limits are also provided. The weight factors of EB_I, i.e., w_{ij} in (6), are $w_{13} = w_{23} = 1$ MW. The weight factors of EB_{II}, i.e., C_{ij} in (9) are $C_{13} = 8.75$ MW and $C_{23} = 5.83$ MW.

In Tables 1–5, we summarize the differences in calculation and identification results of EB_I–EB_{III}. Table 1 shows the power through each line when a unit power is transmitted between each pair of generation node and load node. Tables 2 and 3 demonstrate the difference in the calculations of EB_I–EB_{III}. Tables 4 and 5 compare identification results of EB_I–EB_{III}.

It can be seen from Tables 4 and 5 that EB_I–EB_{III} have the same identification results of critical nodes; however, they have different identification results of critical lines. Specifically, both $EB_I(l_{mn})$ and $EB_{II}(l_{mn})$ indicate that line l_{23} is the most critical line, and line l_{12} and line l_{13} are second and third most critical ones. However, $EB_{III}(l_{mn})$ indicates line l_{13} and line l_{12} as the second and third critical lines.

With the above identification results of critical lines, the vulnerability of the system can be evaluated in two steps. First, two sets of intentional attacks, i.e., l_{23}, l_{12}, l_{13} and l_{23}, l_{13}, l_{12} are constructed based on the results shown in Table 3. Then, the vulnerability is evaluated using V_{PS} defined in (2) and the approach described in Section 3.2.2. Fig. 3 shows the changes in V_{PS}.

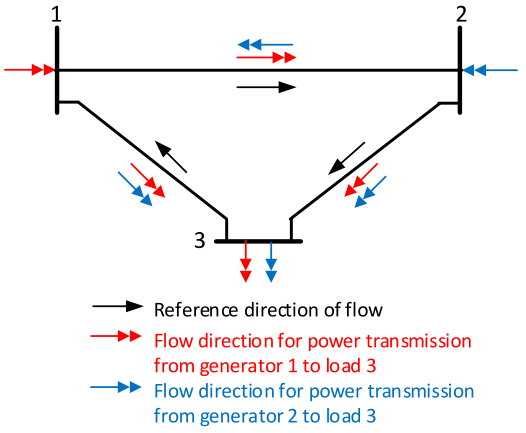

Fig. 1. Illustration of flow direction in a simple network. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

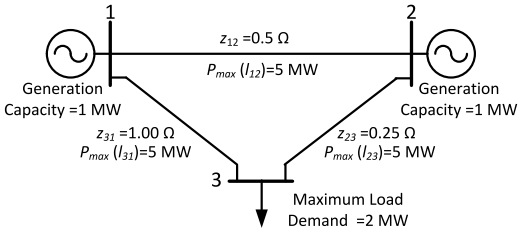

Fig. 2. A simple power system.

Table 1
Power flows on lines for a unit power transmitted between each pair of generation and load nodes.

Power transmission	$f_{ij}(l_{12})$		$f_{ij}(l_{23})$		$f_{ij}(l_{13})$	
	$f_{ij}(l_{12}^{+})$	$f_{ij}(l_{12}^{-})$	$f_{ij}(l_{23}^{+})$	$f_{ij}(l_{23}^{-})$	$f_{ij}(l_{13}^{+})$	$f_{ij}(l_{13}^{-})$
From nodes 1 to 3	0.57	0	0.57	0	0	−0.43
From nodes 2 to 3	0	−0.14	0.86	0	0	−0.14

Table 2
Calculations of $EB_I(l_{mn})$, $EB_{II}(l_{mn})$, and $EB_{III}(l_{mn})$.

Line	$EB_I(l_{mn})$	$EB_{II}(l_{mn})$	$EB_{III}(l_{mn})$
l_{12}	$w_{13} \times \|0.57\| + w_{23} \times \|-0.14\| = 0.71$	$\max[C_{13} \times 0.57, C_{23} \times \|-0.14\|] = 4.99$	$\|0.57 - 0.14\| = 0.43$
l_{23}	$w_{13} \times \|0.57\| + w_{23} \times \|0.86\| = 1.43$	$\max[C_{13} \times 0.57 + C_{23} \times 0.86, 0] = 10.00$	$\|0.57 + 0.86\| = 1.43$
l_{13}	$w_{13} \times \|-0.43\| + w_{23} \times \|-0.14\| = 0.57$	$\max[0, C_{13} \times \|-0.43\| + C_{23} \times \|-0.14\|] = 4.58$	$\|-0.43 - 0.14\| = 0.57$

Table 3
Calculations of $EB_I(i)$, $EB_{II}(i)$, and $EB_{III}(i)$.

Node	$EB_I(i)$	$EB_{II}(i)$	$EB_{III}(i)$
1	$0.5 \times (EB_I(l_{12}) + EB_I(l_{13}) + w_{13}) = 1.14$	$0.5 \times C_{13} \times (0.57 + \|-0.43\|) + 0.5 \times C_{23} \times (\|-0.14\| + \|-0.14\|) + 0.5 \times C_{13} = 9.58$	$0.5 \times (EB_{III}(l_{12}) + EB_{III}(l_{13}) + 1) = 1$
2	$0.5 \times (EB_I(l_{12}) + EB_I(l_{23}) + w_{23}) = 1.57$	$0.5 \times C_{13} \times (0.57 + \|-0.57\|) + 0.5 \times C_{23} \times (\|-0.14\| + \|-0.86\|) + 0.5 \times C_{23} = 10.82$	$0.5 \times (EB_{III}(l_{12}) + EB_{III}(l_{13}) + 1) = 1.43$
3	$0.5 \times (EB_I(l_{23}) + EB_I(l_{13}) + w_{13} + w_{23}) = 2$	$0.5 \times C_{13} \times (0.57 + \|-0.43\|) + 0.5 \times C_{23} \times (0.86 + \|-0.14\|) + 0.5 \times C_{13} + 0.5 \times C_{23} = 14.58$	$0.5 \times (EB_{III}(l_{13}) + EB_{III}(l_{23}) + 2) = 2$

From Fig. 3, it can be observed that V_{PS} of the system under the intentional attacks based on $EB_{III}(l_{mn})$ increases faster than under those based on $EB_I(l_{mn})$ or $EB_{II}(l_{mn})$. Under $EB_{III}(l_{mn})$-based attacks, V_{PS} increases to 1 after the removal of two critical lines (line l_{23} and line l_{13}). However, under the attacks based on $EB_I(l_{mn})$ or $EB_{II}(l_{mn})$, V_{PS} only increases to 0.5 after the removal of two critical lines (line l_{23} and line l_{12}). This observation implies that flow direction affects the identification results of critical lines since the main difference between EB_{III} and the other two EBs is that EB_{III} takes flow direction into consideration.

Table 4
Comparison of identification results of critical lines of $EB_I(l_{mn})$, $EB_{II}(l_{mn})$, and $EB_{III}(l_{mn})$.

Rank	$EB_I(l_{mn})$	$EB_{II}(l_{mn})$	$EB_{III}(l_{mn})$
1	l_{23}	l_{23}	l_{23}
2	l_{12}	l_{12}	l_{13}
3	l_{13}	l_{13}	l_{12}

Table 5
Comparison of identification results of critical nodes of $EB_I(i)$, $EB_{II}(i)$, and $EB_{III}(i)$.

Rank	$EB_I(i)$	$EB_{II}(i)$	$EB_{III}(i)$
1	3	3	3
2	2	2	2
3	1	1	1

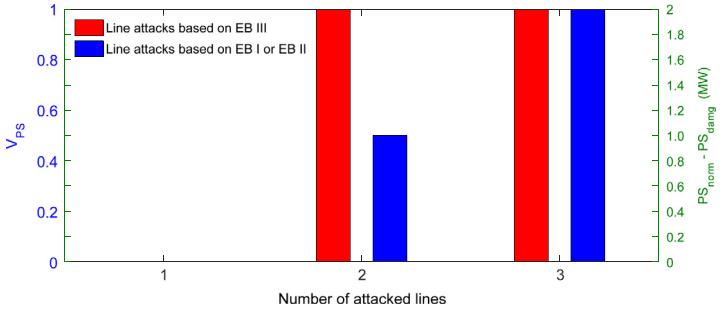

Fig. 3. Changes in V_{PS} of the 3-bus system under two sets of intentional line attacks.

4.3. Case studies on IEEE 300-bus system and Italian power grid

The above observation on the important impact of flow direction on the identification results of critical components is further demonstrated with case studies on the IEEE 300-bus system and the Italian power grid. The IEEE 300-bus system consists of 411 lines and 300 nodes including 69 generation nodes and 164 load nodes [52]. For this system, line limits and generator capacities are obtained from Refs. [53,54], respectively; the maximum demand of each load is assumed to be 1.5 times its original load demand. The Italian power grid is composed of 641 lines and 521 nodes including 158 generation nodes and 205 load nodes. In the Italian power grid, line limits and generation capacities are given in its data and the maximum demand of each load is also assumed to be 1.5 times its original load demand.

Intentional attacks on lines and nodes as well as random failures on lines and nodes are constructed to evaluate the vulnerability of the IEEE 300-bus system and the Italian power grid. Figs. 4 and 6 show the changes in V_{PS} of these two power systems under random line failures and three sets of intentional line attacks based on EB_I–EB_{III}. Figs. 5 and 7 show the changes in V_{PS} of the 300-bus system and the Italian power grid under random node failures and three sets of EB-based intentional node attacks. In Figs. 4 and 6, the changes in V_{PS} under random line failures are the average under 50 different sets of randomly selected lines. Similarly, in Figs. 5 and 7, the changes in V_{PS} under random node failures are the average under 50 different sets of randomly selected nodes.

It can be observed from Figs. 4 and 5 that V_{PS} of the system always increases faster under EB-based intentional attacks than that under random failures, which, as one would expect, suggests that the system is more vulnerable under intentional attacks than under random failures.

Also, it can be observed from Figs. 4 and 5 that the attacks based on EB_{III} are more effective in increasing V_{PS} than the attacks based on EB_I and EB_{II} in the middle stage of attacks, i.e., the stage after a moderate number of nodes or lines is removed but before a loss of substantial number of nodes or lines.

In the initial stage, when a small number of lines or nodes are removed (such as about 50 lines or 30 nodes), there are relatively small changes in V_{PS} of the system under the attacks based on EB_I–EB_{III} since an appropriately designed power system can usually maintain its ability of power supply when a small number of components are under fault conditions. In this stage, it is observed that V_{PS} increases faster under the attacks based on EB_{II} than under those based on EB_I and EB_{III}, which suggests that line limits more significantly affect the identification of critical components since only EB_{II} takes line limits into account.

In the middle stage, when an additional number of lines or nodes are removed (the number of removed lines in this case study increases from 50 to 230 while the number of removed nodes increases from 30 to 120), V_{PS} increases quickly. The removal of additional lines or nodes starts separating the system into multiple sub-grids. In the sub-grids, some generators

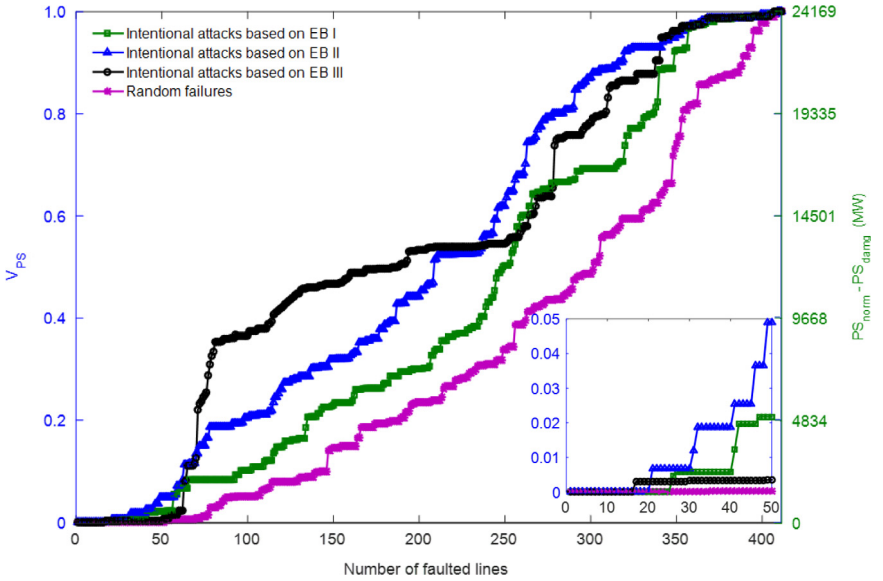

Fig. 4. Changes in V_{PS} of the IEEE 300-bus system under random line failures and three sets of intentional line attacks.

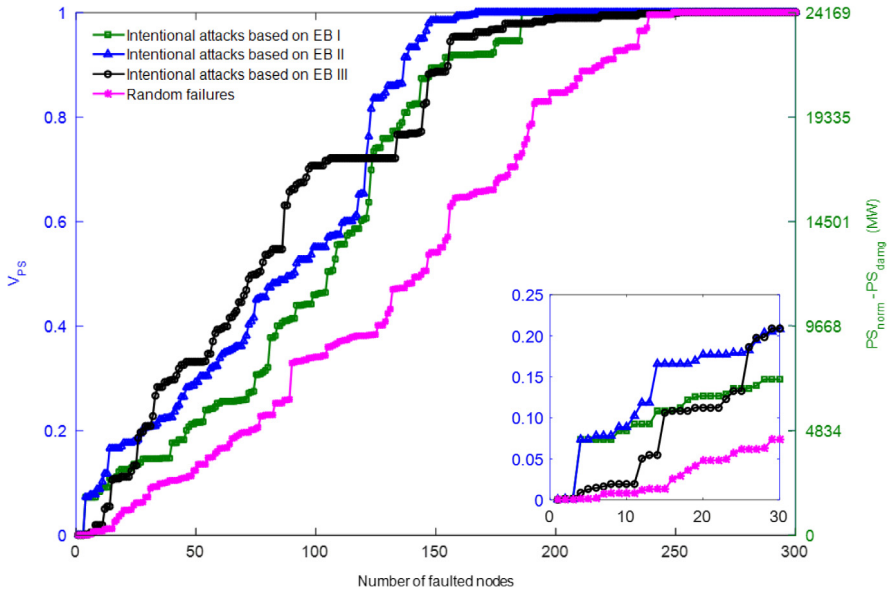

Fig. 5. Changes in V_{PS} of the IEEE 300-bus system under random node failures and three sets of intentional node attacks.

are disconnected. Thus, generation may not meet load demand, and some loads may be shed in order to balance generation and load demand. For this stage, it is observed that V_{PS} increases much faster under the attacks based on EB_{III} than under those based on EB_I and EB_{II}. This suggests that flow direction plays an important role in the identification of critical components because only EB_{III} appropriately takes flow direction into consideration. In addition, it is observed that the system is more vulnerable under EB_{II} and EB_{III}-based attacks than under EB_I-based attacks since V_{PS} increases faster under the attacks based on EB_{II} and EB_{III} than under those based on EB_I. This implies that internal properties of networks with flow direction and line limits may have more significant impacts on the identification of critical components than external limits such as node constraints.

In the last stage, a large number of lines or nodes are removed (the number of removed lines increases from 230 to 409 while the number of removed nodes increases from 120 to 300). As a result, a substantial number of sub-grids are formed, more generators are isolated, and much less loads are supplied. For this last stage, it is observed that V_{PS} increases faster under intentional attacks based on EB_{II} than under those based on EB_I and EB_{III}. This implies that line limits impact the identification of critical components significantly when a substantial number of critical components are removed.

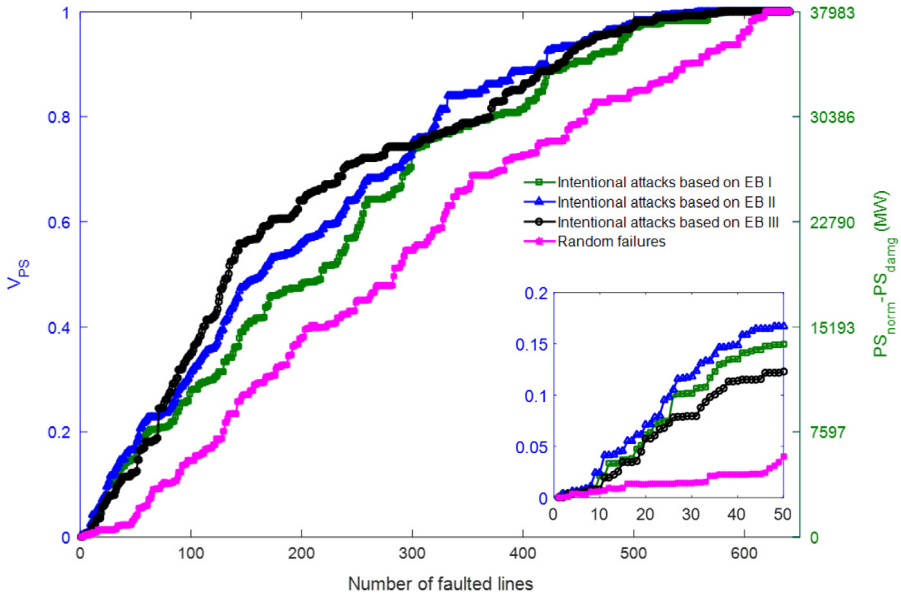

Fig. 6. Changes in V_{PS} of the Italian power grid under random line failures and three sets of intentional line attacks.

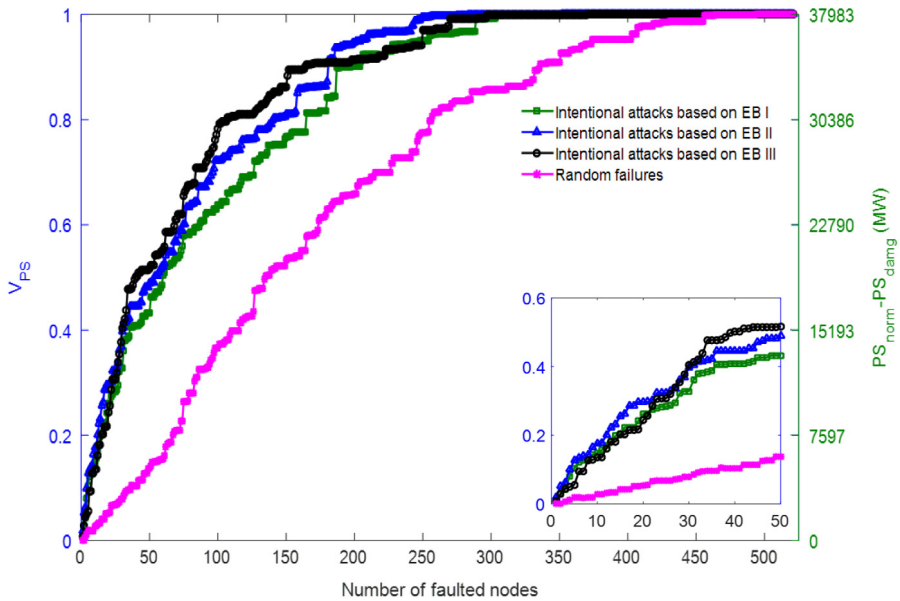

Fig. 7. Changes in V_{PS} of the Italian power grid under random node failures and three sets of intentional node attacks.

The observations from Figs. 6 and 7 in the Italian power grid are similar to those from Figs. 4 and 5 in the IEEE 300-bus system. Based on the above comparative studies of EBs, we know that the essential electrical properties of power grids, i.e., node constraints, line limits, and flow direction, play important roles in the identification of critical components. However, each EB only takes into consideration an electrical property individually in its measure. In the next section, we will analyze power grid vulnerability with a new set of electrical betweenness measures that integrate all the three essential electrical properties.

5. Combined electrical betweenness measures

In this section, we propose a way to integrate three essential electrical properties of power grids into a set of combined electrical betweenness measures. With the combined measures to identify critical components, we also provide comparative case studies of power grid vulnerability under intentional attacks.

5.1. Combined electrical betweenness measures

First, we redefine a weight. For a given pair of generation node i and load node j, the weight represents a specified power, which satisfies the following two conditions: (1) when the specified power is transmitted from generation node i to load node j, no lines violate their power transmission limits; (2) the specified power is not larger than either the generation capacity of the generator at node i or the maximum load at node j. To satisfy the two conditions, the weight for a given pair of generation node i and load node j can be represented as,

$$\alpha_{ij} = \min\left(C_{ij}, S_i, S_j\right) \tag{13}$$

where C_{ij} represents the maximum power that can be transmitted from generation node i to load node j without violating line power transmission limits; S_i is the generation capacity of generator at node i; and S_j is the maximal load at node j.

Then, with (13), we redefine $EB_{III}(l_{mn})$ and obtain a combined electrical betweenness measure of link l_{mn} ($CEB(l_{mn})$) as follows.

$$CEB(l_{mn}) = \left| \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} \alpha_{ij} f_{ij}(l_{mn}^{+}) + \sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} \alpha_{ij} f_{ij}(l_{mn}^{-}) \right| \tag{14}$$

where $\sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} \alpha_{ij} f_{ij}(l_{mn}^{+})$ is the total power through link l_{mn} along the reference direction of link l_{mn} when the power equal to α_{ij} is transmitted between generation node i and load node j; $\sum_{i\in\mathbf{G}} \sum_{j\in\mathbf{D}} \alpha_{ij} f_{ij}(l_{mn}^{-})$ is the total power through link l_{mn} against the reference direction of link l_{mn} when the power equal to α_{ij} is transmitted between generation node i and load node j.

Further, with $CEB(l_{mn})$, the corresponding combined electrical betweenness measure of node i ($CEB(i)$) is defined below.

$$CEB(i) = \begin{cases} \left(\sum_{j\in\mathbf{F}(i)} CEB(l_{mn}) + \sum_{k\in\mathbf{D}} \alpha_{ik} \right) \Big/ 2 & i \in \mathbf{G} \\ \left(\sum_{j\in\mathbf{F}(i)} CEB(l_{mn}) + \sum_{m\in\mathbf{G}} \alpha_{mi} \right) \Big/ 2 & i \in \mathbf{D} \\ \left(\sum_{j\in\mathbf{F}(i)} CEB(l_{mn}) \right) \Big/ 2 & i \in \mathbf{T} \end{cases} \tag{15}$$

where $\mathbf{F}(i)$ is the set of nodes connected to node i; $\sum_{j\in\mathbf{F}(i)} CEB(l_{mn})$ represents the sum of the power through all links connected to node i when the power is transmitted between all pairs of generation nodes and load nodes; $\sum_{k\in\mathbf{D}} \alpha_{ik}$ represents the sum of the total power that is transmitted from generation node i to all load nodes; and $\sum_{m\in\mathbf{G}} \alpha_{mi}$ represents the sum of the total power that the load at node i withdraws from all generation nodes.

In the definition of CEB, the shortcomings of EB_I–EB_{III} are overcome:

- EB_I does not take into consideration line limits. Thus, the power transmission limits for some lines may be violated. Also, flow direction is not included in EB_I.
- EB_{II} does not take into account node constraints. Thus, the power generated at generation node and power consumed at load node may violate their limits. In addition, flow direction is not appropriately considered in EB_{II}.
- EB_{III} does not take into account node constraints and line limits. Thus, it does not consider the effects of node constraints and line limits.

5.2. Results of analysis of IEEE 300-bus system and Italian power grid

In the analysis, the critical lines and nodes are identified by CEB and EB_I–EB_{III}. Based on the identification results, four sets of intentional line attacks and four sets of intentional node attacks are constructed to evaluate the vulnerability of the IEEE 300-bus system and the Italian power grid. Figs. 8 and 9 show the changes in V_{PS} of the IEEE 300-bus system under intentional line attacks and intentional node attacks, respectively. Figs. 10 and 11 show the changes in V_{PS} of the Italian power grid under intentional line attacks and intentional node attacks, respectively.

It can be observed from Figs. 8 and 9 that V_{PS} increases much faster under CEB-based attacks compared to the ones based on the three EBs in all stages, which implies that CEB is much more effective for identifying critical components.

In the initial stage, when a small number of lines or nodes (such as 30 lines or 10 nodes) are removed, V_{PS} quickly jumps to 0.2 under the CEB-based line and node attacks, but under the EBs-based line attacks, V_{PS} slightly changes, and under the EBs-based node attacks, V_{PS} increases slowly to less than 0.2.

In the middle stage, when additional number of lines or nodes are removed (the number of removed lines increases from 30 to 230, and the number of removed nodes increases from 10 to 120), V_{PS} dramatically increases to about 0.65 under the CEB-based line attacks and V_{PS} even increases to more than 0.85 under the CEB-based nodes attacks. However, under the EBs-based line attacks, V_{PS} increases only to 0.5, and under EBs-based node attacks, V_{PS} increases only to about 0.7.

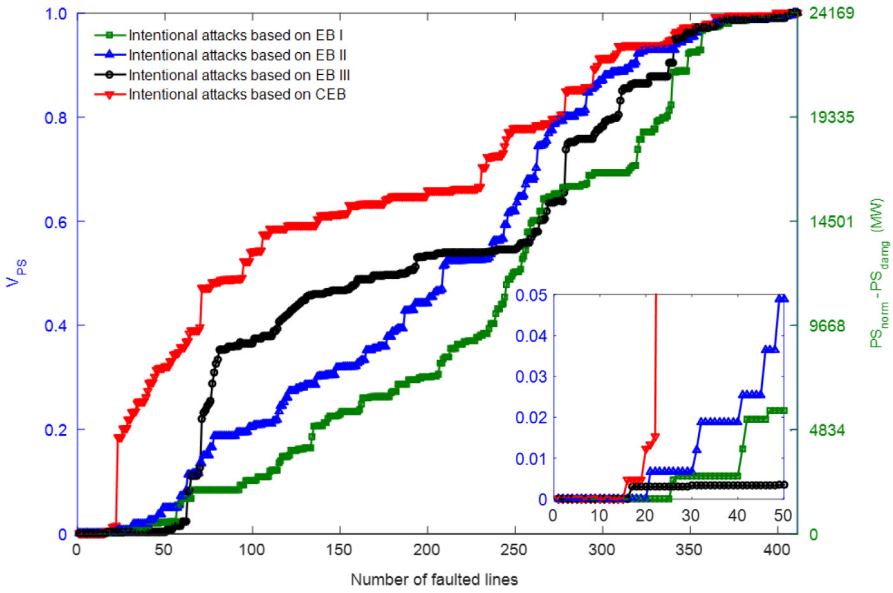

Fig. 8. Changes in V_{PS} of the IEEE 300-bus system under four sets of intentional line attacks.

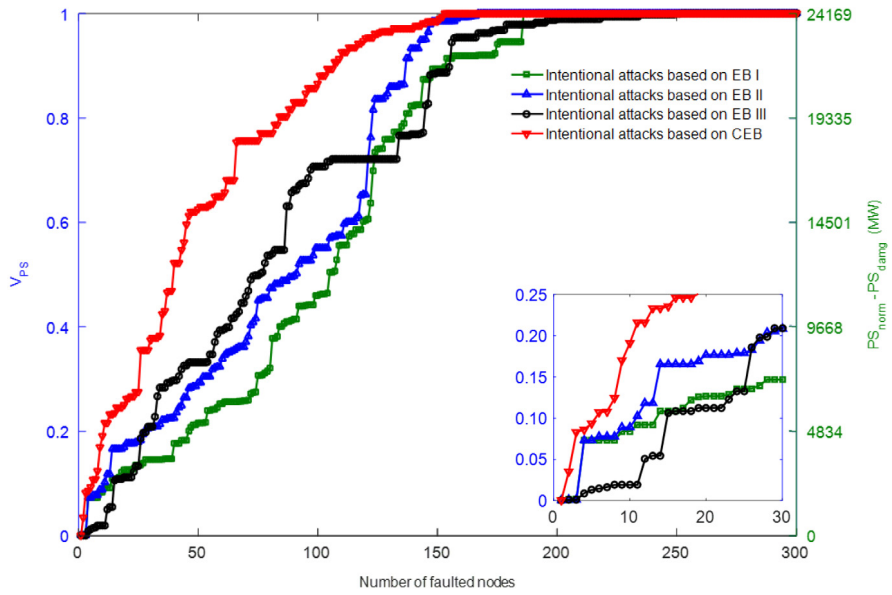

Fig. 9. Changes in V_{PS} of the IEEE 300-bus system under four sets of intentional node attacks.

In the last stage, when a large number of lines or nodes are removed (the number of removed lines increases from 230 to 409, and the number of removed nodes increases from 120 to 300), V_{PS} quickly increases to 1 under the CEB-based attacks, but under the EBs-based attacks, the increase of V_{PS} is very slow.

The observations from Figs. 10 and 11 in the Italian power grid are similar to those from Figs. 8 and 9 in the IEEE 300-bus system, and they further verify that CEB is much more effective for the identification of critical components in the Italian power grid.

6. Conclusion

In the literature, various topological measures in complex network analysis have been used to analyze the vulnerability of power grids. However, these measures are not readily applicable for vulnerability analysis of power grid because they do not take into consideration electrical properties of power grids. In this paper, we studied the impact of essential electrical properties, including node constraints, line limits, and flow direction, on vulnerability assessment of power grid using

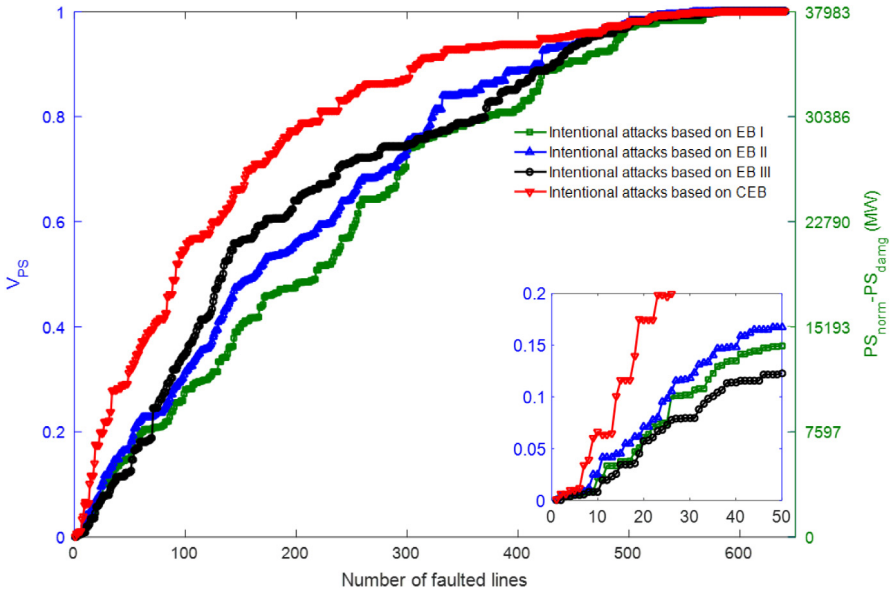

Fig. 10. Changes in V_{PS} of the Italian power grid under four sets of intentional line attacks.

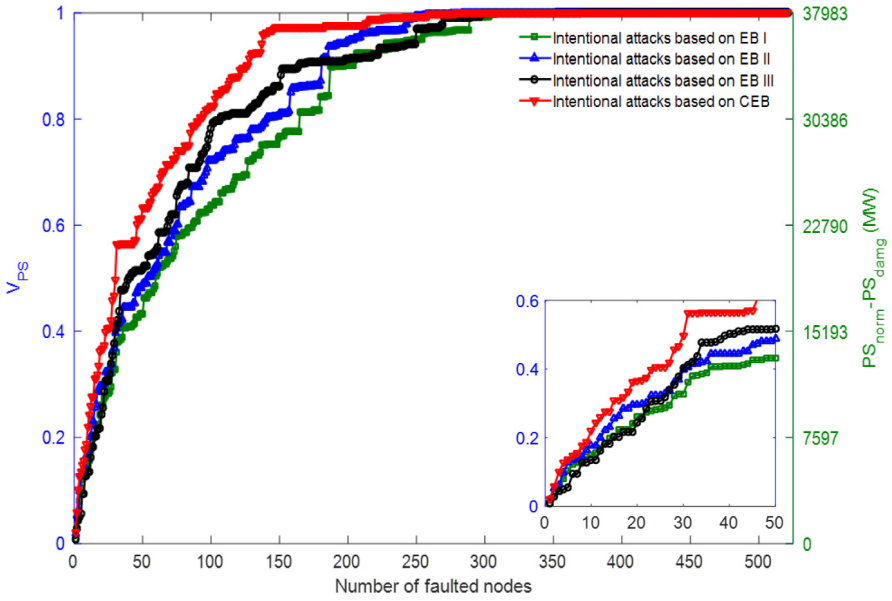

Fig. 11. Changes in V_{PS} of the Italian power grid under four sets of intentional node attacks.

electrical betweenness measures EB_I–EB_{III}. EB_I reported in Ref. [11] took node constraints into account while EB_{II} presented in Ref. [12] took line limits into consideration. Different from EB_I and EB_{II}, EB_{III} was proposed in this paper by taking into account flow direction in a power grid. Simulation analysis on the IEEE 300-bus system and the Italian power grid shows the important impact of flow direction on vulnerability assessment of power grid. Thus, we further proposed a new set of combined electrical betweenness measures (i.e.,*CEB*) by taking into consideration all the essential electrical properties that are included individually in EB_I–EB_{III}. The identification results of *CEB* and EB_I–EB_{III} were compared by performing vulnerability studies on the IEEE 300-bus system and the Italian power grid.

The analysis results of the impacts of essential electrical properties on vulnerability assessment of power grid and the comparison results of *CEB* and EB_I–EB_{III} are summarized below:

- Flow direction plays a significant role in impacting the identification of critical components. It is observed that the system is more vulnerable under EB_{III}-based attacks than under EB_I- and EB_{II}-based attacks in the middle stage of attacks (i.e., when a moderate number of nodes or lines are removed due to attacks).

- Line limits impact the identification of critical components. It is observed that the system is more vulnerable under EB_{II}-based attacks than under EB_I- and EB_{III}-based attacks in the initial stage of attacks (i.e., when a large number of nodes or lines are removed under attacks) and in the last stage of attacks (i.e., when a large number of nodes or lines are removed under attacks).
- The internal properties of networks with flow direction and line limits may have more significant impacts on the identification of critical components than external limits such as node constraints. It is observed that the system is more vulnerable under EB_{II} and EB_{III}-based attacks than under EB_I-based attacks in the middle stage of attacks (i.e., when a moderate number of nodes or lines are removed due to attacks).
- *CEB* is more effective than EB_I–EB_{III} for identifying critical components. It is observed that the system is more vulnerable under CEB-based attacks than under the attacks based on EB_I–EB_{III} in all stages of attacks including the initial stage, the middle stage, and the last stage.

References

[1] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the north American power grid, Phys. Rev. E 69 (2) (2004) 025103.
[2] V. Rosato, L. Issacharoff, G. Gianese, S. Bologna, Influence of the topology on the power flux of the italian high-voltage electrical network, arXiv preprint arXiv:0909.1664.
[3] G.A. Pagani, M. Aiello, Towards decentralization: A topological investigation of the medium and low voltage grids, IEEE Trans. Smart Grid 2 (3) (2011) 538–547.
[4] M. Ding, P. Han, Reliability assessment to large-scale power grid based on small-world topological model, in: 2006 International Conference on Power System Technology, IEEE, 2006, pp. 1–5.
[5] P. Crucitti, V. Latora, M. Marchiori, A topological analysis of the italian electric power grid, Physica A 338 (1) (2004) 92–97.
[6] A.E. Motter, Y.-C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (6) (2002) 065102.
[7] R. Kinney, P. Crucitti, R. Albert, V. Latora, Modeling cascading failures in the north American power grid, Eur. Phys. J. B 46 (1) (2005) 101–107.
[8] L. Zongxiang, M. Zhongwei, Z. Shuangxi, Cascading failure analysis of bulk power system using small-world network model, in: 2004 International Conference on Probabilistic Methods Applied to Power Systems, IEEE, 2004, pp. 635–640.
[9] P. Hines, S. Blumsack, A centrality measure for electrical networks, in: Hawaii International Conference on System Sciences, Proceedings of the 41st Annual, IEEE, 2008, pp. 1–8.
[10] Z. Wang, A. Scaglione, R.J. Thomas, Electrical centrality measures for electric power grid vulnerability analysis, in: 49th IEEE Conference on Decision and Control, (CDC), IEEE, 2010, pp. 5792–5797.
[11] K. Wang, B.-h. Zhang, Z. Zhang, X.-g. Yin, B. Wang, An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load, Physica A 390 (23) (2011) 4692–4701.
[12] E. Bompard, D. Wu, F. Xue, Structural vulnerability of power systems: A topological approach, Electr. Power Syst. Res. 81 (7) (2011) 1334–1340.
[13] E. Bompard, E. Pons, D. Wu, Extended topological metrics for the analysis of power grid vulnerability, IEEE Syst. J. 6 (3) (2012) 481–487.
[14] A.E. Motter, Cascade control and defense in complex networks, Phys. Rev. Lett. 93 (9) (2004) 098701.
[15] Y. Moreno, J. Gmez, A. Pacheco, Instability of scale-free networks under node-breaking avalanches, Europhys. Lett. 58 (4) (2002) 630.
[16] G. Caldarelli, A. Vespignani, Large Scale Structure and Dynamics of Complex Networks, World Scientific, 2007.
[17] M. Sachtjen, B. Carreras, V. Lynch, Disturbances in a power transmission system, Phys. Rev. E 61 (5) (2000) 4877.
[18] J. Yan, Y. Tang, H. He, Y. Sun, Cascading failure analysis with dc power flow model and transient stability analysis, IEEE Trans. Power Syst. 30 (1) (2015) 285–297.
[19] P. Henneaux, Probability of failure of overloaded lines in cascading failures, Int. J. Electr. Power Energy Syst. 73 (2015) 141–148.
[20] J. Qi, K. Sun, S. Mei, An interaction model for simulation and mitigation of cascading failures, IEEE Trans. Power Syst. 30 (2) (2015) 804–819.
[21] A. Scala, S. Pahwa, C.M. Scoglio, Cascade failures and distributed generation in power grids, Int. J. Crit. Infrastruct. 11 (1) (2015) 27–35.
[22] B. Shi, J. Liu, Decentralized control and fair load-shedding compensations to prevent cascading failures in a smart grid, Int. J. Electr. Power Energy Syst. 67 (2015) 582–590.
[23] G. Zhang, Z. Li, B. Zhang, W.A. Halang, Understanding the cascading failures in indian power grids with complex networks theory, Physica A 392 (15) (2013) 3273–3280.
[24] E. Bompard, L. Luo, E. Pons, A perspective overview of topological approaches for vulnerability analysis of power transmission grids, Int. J. Crit. Infrastruct. 11 (1) (2015) 15–26.
[25] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jimnez-Fernndez, Z.W. Geem, A critical review of robustness in power grids using complex networks concepts, Energies 8 (9) (2015) 9211–9265.
[26] G.A. Pagani, M. Aiello, The power grid as a complex network: a survey, Physica A 392 (11) (2013) 2688–2700.
[27] R.V. Sol, M. Rosas-Casals, B. Corominas-Murtra, S. Valverde, Robustness of the European power grids under intentional attack, Phys. Rev. E 77 (2) (2008) 026102.
[28] M. Rosas-Casals, S. Valverde, R.V. Sol, Topological vulnerability of the European power grid under errors and attacks, Int. J. Bifurcation Chaos 17 (07) (2007) 2465–2475.
[29] P. Crucitti, V. Latora, M. Marchiori, Locating critical lines in high-voltage electrical power grids, Fluct. Noise Lett. 5 (02) (2005) L201–L208.
[30] J. Holmgren, Using graph models to analyze the vulnerability of electric power networks, Risk Anal. 26 (4) (2006) 955–969.
[31] Z. Wang, A. Scaglione, R.J. Thomas, The node degree distribution in power grid and its topology robustness under random and selective node removals, in: 2010 IEEE International Conference on Communications Workshops, IEEE, 2008, pp. 1–5.
[32] D.J. Watts, S.H. Strogatz, Collective dynamics of small-worldnetworks, Nature 393 (6684) (1998) 440–442.
[33] S. Mei, X. Zhang, M. Cao, Power Grid Complexity, Springer Science & Business Media, 2011.
[34] V. Rosato, S. Bologna, F. Tiriticco, Topological properties of high-voltage electrical transmission networks, Electr. Power Syst. Res. 77 (2) (2007) 99–105.
[35] A.-L. Barabsi, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[36] L.A.N. Amaral, A. Scala, M. Barthelemy, H.E. Stanley, Classes of small-world networks, Proc. Nat. Acad. Sci. 97 (21) (2000) 11149–11152.
[37] E. Bompard, R. Napoli, F. Xue, Analysis of structural vulnerabilities in power transmission grids, Int. J. Crit. Infrastruct. Prot. 2 (1) (2009) 5–12.
[38] E. Bompard, D. Wu, F. Xue, The concept of betweenness in the analysis of power grid vulnerability, in: Complexity in Engineering, 2010, COMPENG'10, IEEE, 2010, pp. 52–54.
[39] S. Arianos, E. Bompard, A. Carbone, F. Xue, Power grid vulnerability: A complex network approach, Chaos 19 (1) (2009) 013119.
[40] L. Luo, M. Rosas-Casals, Correlating empirical data and extended topological measures in power grid networks, Int. J. Crit. Infrastruct. 11 (1) (2015) 82–96.
[41] Z. Guohua, W. Ce, Z. Jianhua, Y. Jingyan, Z. Yin, D. Manyin, Vulnerability assessment of bulk power grid based on complex network theory, in: Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies, 2008, DRPT 2008, IEEE, 2008, pp. 1554–1558.
[42] P. Hines, S. Blumsack, E.C. Sanchez, C. Barrows, The topological and electrical structure of power grids, in: 2010 43rd Hawaii International Conference on System Sciences, (HICSS), IEEE, 2010, pp. 1–10.
[43] E.I. Bilis, W. Krger, C. Nan, Performance of electric power systems under physical malicious attacks, IEEE Syst. J. 7 (4) (2013) 854–865.

[44] V. Latora, M. Marchiori, Efficient behavior of small-world networks, Phys. Rev. Lett. 87 (19) (2001) 198701.
[45] B. Bollobas, Random Graphs, Academic Press, New York, 1985.
[46] P. Hines, E. Cotilla-Sanchez, S. Blumsack, Do topological models provide good information about electricity infrastructure vulnerability? Chaos 20 (3) (2010) 033122.
[47] M. Ouyang, Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability, Chaos 23 (2) (2013) 023114.
[48] M. Ouyang, Z. Pan, L. Hong, L. Zhao, Correlation analysis of different vulnerability metrics on power grids, Physica A 396 (2014) 204–211.
[49] B.A. Carreras, V.E. Lynch, I. Dobson, D.E. Newman, Critical points and transitions in an electric power transmission model for cascading failure blackouts, Chaos 12 (4) (2002) 985–994.
[50] L.C. Freeman, A set of measures of centrality based on betweenness, Sociometry 40 (1) (1977) 35–41.
[51] M. Girvan, M.E. Newman, Community structure in social and biological networks, Proc. Nat. Acad. Sci. 99 (12) (2002) 7821–7826.
[52] Power systems test case archive. http://www.ee.washington.edu/research/pstca/.
[53] Matpower. http://www.pserc.cornell.edu/matpower/.
[54] A.Z.-u. Rahman, An ex ante probabilistic study of market power with emphasis on the transmission constraints (Master thesis), Royal Institute of Technology (KTH), 2011.