# The Structural Dimensions in the Security of Power Transmission Systems

**Tao Huang, Ettore Bompard, Marcelo Masera and Fei Xue**

**Abstract** This chapter discusses the security of power transmission systems from a structural perspective. It introduces a systematic concept of structural analysis for power grids security assessment applying extended topological approaches based on an adaptation of the theory of complex networks modified to capture the physical behavior of transmission networks as “flow networks”. The concept of structural analysis is introduced as an alternative approach for discussing the relation between structure and state of power grids. A general review of complex networks applied to power grids security serves as introduction to a discussion of the shortcomings of pure topological approaches. Finally, authors describe the proposed systematic extended topological approach. In this chapter, “entropic degree” and “T-betweenness” are used to provide a measure of the criticality of buses and lines of transmission networks. Then, authors proceed with a dynamic way to rank critical components. Third, integration the previous concepts as metrics for distinguishing important components from critical ones, and for indicating their correlations are done. Finally, taking an overall perspective, and departing from net-ability, authors discuss the concept of path-redundancy as a new metric for survivability.

**Keywords** Power system security · Power grid · Complex networks · Extended topological approach · Structural dimension

T. Huang · E. Bompard (✉)
Dipartimento Energia, Politecnico di Torino, Corso Duca Degli Abruzzi, 24,
10129 Turin, Italy
e-mail: ettore.bompard@polito.it

E. Bompard · M. Masera
Joint Research Centre, Institute for Energy and Transport, 2 1755 NL ZG Petten,
The Netherlands

F. Xue
Siemens Eco-City Innovation Technologies (Tianjin) Co., Ltd., Eco Business Park, Tianjin
Eco CityBinhai New Area, Tianjin, China

A. V. Gheorghe et al. (eds.), *Infranomics*, Topics in Safety, Risk,
Reliability and Quality 24, DOI: 10.1007/978-3-319-02493-6_20,

## PWRS Security Analysis Approaches and Practices

The contemporary society increasingly relies on a high integration of different interdependent systems [1]. Electricity, as a main energy source to other infrastructures, stands in the center and is essential to the operation of all other systems. Therefore, as a critical and fundamental infrastructure, power system's security problem is a global concern strongly associated with social stability and economic development. Hence, priorities for the secure operation of the power system have always been given by different authorities, organizations, and utilities at all levels.

As the power system is evolving in many directions, such as network interconnections between nations or regions, utilizations and deployment of new technologies and controls, and operation in highly stressed conditions, different academic/industrial organizations proposed various terminological definitions based on the scenarios of their own interest. For example, Table 1 lists definitions relevant for power system security from four academic/industrial organizations, namely the International Electrotechnical Commission (IEC), IEEE (the Institute of Electrical and Electronics Engineers), ENTSO-E (the European Network of Transmission System Operators for Electricity), and NERC (the North American Electric Reliability Corporation).

In order to unify the understanding of security issues to be addressed in this chapter, we propose our perspective on these terminologies.

*Reliability* refers to the ability to supply loads with a high level of probability for a certain time interval. It can be described by two attributes: security and adequacy. *Security* means the ability to withstand imminent disturbances or contingencies, such as electric short circuits or unanticipated loss of system elements, without interruption of customer service; and *adequacy* means the ability to supply power to customers in various conditions, taking into account operational constraints. As a sub-item of security, *stability* refers to the ability to maintain or to regain a state of equilibrium after disturbances or contingencies. Here *disturbance* refers to an unplanned incident producing an abnormal system condition; and *contingency* refers to an unexpected failure or outage of a system component. In addition, *vulnerability* and *robustness* are frequently used to qualify the low reliability and the high reliability of the power systems, respectively. Moreover, similar to the concept of reliability, availability refers to the ability to be in a state to perform a required function under given conditions, and is measured as the proportion of time the power system is in operable and committable condition over a given time interval.

In contemporary system operational practices, to verify the aspects of the above mentioned securities issues, simulations are employed to assure the secure operation of the power system as well as to devise and validate emergency planes after contingency. Security is commonly analyzed by using methods completely based on operational data and physical models such as static security assessment [13, 14], and dynamic security assessment [15] for different purposes. For example, steady state analysis is called every 15 min to conduct contingency analyses with "n − 1"

**Table 1** Definitions of security related terminologies from academic/industrial organizations

| | IEC | IEEE | ENTSO-E | NERC |
|---|---|---|---|---|
| Reliability | Probability that an electric power system can perform a required function under given conditions for a given time interval [2] | The probability of its satisfactory operation over the long run [3] | A general term encompassing all the measures of the ability of the system, generally given as numerical indices, to deliver electricity to all points of utilization within acceptable standards and in the amounts desired [4] | Able to meet the electricity needs of end-use customers even when unexpected equipment failures or other factors reduce the amount of available electricity [5] |
| Security | Ability of an electric power system to operate in such a way that credible events do not give rise to loss of load, stresses of system components beyond their ratings, bus voltages or system frequency outside tolerances, instability, voltage collapse, or cascading [6] | The degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service [3] | The ability to withstand sudden disturbances, such as electric short circuits or unanticipated losses of system components or load conditions together with operating constraints. Another aspect of security is system integrity, which is the ability to maintain interconnected operations [4] | The ability of the bulk power system to withstand sudden, unexpected disturbances such as short circuits, or unanticipated loss of system elements due to natural causes [5] |
| Adequacy | The ability of an electric power system to supply the aggregate electric power and energy required by the customers, under steady-state conditions, with system component ratings not exceeded, bus voltages and system frequency maintained within tolerances, taking into account planned and unplanned system component outages [7] | A system's capability to meet system demand within major component ratings and in the presence of scheduled and unscheduled outages of generation and transmission components or facilities [8] | The ability of a power system to supply the load in all the steady states in which the power system may exist considering standards conditions [4] | The ability of the electric system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements [9] |

(continued)

**Table 1** (continued)

| | IEC | IEEE | ENTSO-E | NERC |
|---|---|---|---|---|
| Stability | The ability of an electric power system to regain or to retain a steady-state condition, characterized by the synchronous operation of the generators and a steady acceptable quality of the electricity supply, after a disturbance due, for example, to variation of power or impedance [10] | The ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact [3] | The ability of an electric system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances [11] | The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances [9] |
| Availability | The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided [12] | – | A measure of time during which a generating unit, transmission line, ancillary service or another facility is capable of providing service, whether or not it actually is in service [11] | – |

criteria, verifying that for each configuration no line flow limits or voltage violations are expected. It is also used to check the adequacy of the system with the 4 typical operational scenarios (summer peak/off-peak, winter peak/off-peak) per year. In addition, when new plants or transmission lines are planned, it is called on demand to test the static security impacts on the system. In contrast, the dynamic state analysis is often used as an off-line resort to understand the dynamic cascading mechanisms after a severe failure or blackout happened. More often than usual, it is conducted to assess the dynamic impacts of new planned units on other rotating components in the system in terms of angle stability, oscillation, etc. Yet, although rarely, dynamic simulation is performed online when the system is very close to violate the constraints provided by the steady state.

As mentioned, these traditional methods evaluate the security relying on a given contingency and operating condition. It is computationally infeasible to check all possible combinations of contingencies that could cause serious blackouts in practical power grids; on the other hand, operating conditions of power systems change along time due to load variations, switching actions, etc. Therefore it is difficult to prevent the collapse of electrical power grids due to unforeseen operating conditions. Besides, due to the size of large-scaled power systems, physical behaviors and the interaction among many operators over power grid add difficulty to perform a comprehensive analytic analysis and simulation of the electromagnetic processes over the whole grid. Hence, in practice, reduced systems or some simplifying hypothesis are applied to these conventional methods to simulate the network's response to various external disturbances, yet the simulation results cannot reflect the exact response of power systems.

As a result, frequent blackouts occurred all over the world although advanced technologies and huge investments have been used in assuring the reliability and security of power systems. To deepen the insight into power systems, it is necessary to develop and complement the conventional analysis technology with new points of view and analytic capabilities.

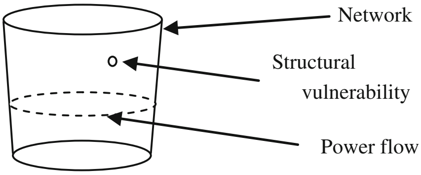
## Structural Analysis in Power Transmission Networks

### *Relation Between Structure and State of Power Grids*

In the assessment of power system security, we need to distinguish the influence of two different aspects, structure and operating states. If we only consider the vulnerability caused by structural factors or operating states, they will only represent a part, although important, of the problem. To explain the relationship between the two aspects, we give a conceptual example in Fig. 1.

As shown in Fig. 1, the cup can be considered as the transmission network, the water inside can be considered as the exact power flow depending on operative states of generators and loads. The volume of the cup can be considered as the

**Fig. 1** Conceptual example for structural vulnerability



aptitude of the network and indicates the capacity of the cup to take water. This capacity is fixed even there is no water inside the cup. A small hole as shown in the figure is a structural vulnerability for the cup. The outbreak of a problem (leaking water) induced by this vulnerability also depends on the level of water. Only when the level of water is higher than the hole, this vulnerability will affect the function of the cup. Similarly, structural vulnerabilities in power grids are caused by the network structure and may threaten the function of the network and power system. However, the outbreak of security problems will also depend on the operative states of generators/loads and corresponding power flow. For example, if currently there is no power flow in the network, there would of course be no security problem.

## *Complex Networks on Power Grids Structural Analysis*

A new approach, based on recent advances in the understanding of the structure of large complex networks, provides an emerging perspective to consider power grids security issues. By investigating the network model of the power grid from a topological perspective, it is possible to find properties and behaviors that have not been identified in traditional detailed model and analysis.

In Ref. [16], the authors built a network model based on data stored in the POWERmap mapping system developed by Platts [17]. This mapping system contains information about every power plant, major substation, and 115–765 kV power line of the North American power grid. The power from a generator is considered able to reach a consumer if there exists at least a path composed of transmission lines between them. In practice, the existence of a path between two substations does not always imply that power can be efficiently transferred through it by taking into account capacity or other constraints. Without consideration of the latter, the model only provides an idealized view.

As in general theory of CN, the node degree is a good indicator of topological importance (maybe not enough suitable for power grids, to be discussed later), the degree distribution of the power grid has been studied. Comparing the grid in Ref. [16] to scale-free and random networks (with the same number of nodes and edges), its cumulative degree distribution indicates that the probability of high-degree buses is less than in a scale-free network model, but higher than in a random network model [16].

In Ref. [18], the reliability of electric transmission systems is examined using a scale-free model of network topology and failure propagation. The topologies of the North American eastern and western electric grids were analyzed to estimate their reliability based on the Barabasi–Albert network model. A commonly used power system reliability index was computed using a simple failure propagation model. The results were compared to the values of power system reliability indices previously obtained from some standard power engineering methods, and they suggested that scale-free network models are unable to estimate aggregate electric grid reliability.

In Ref. [19], with the September 2003 actualization of the Union for the Coordination of Transport of Electricity (UCTE) power grid, the authors made an analysis of this topological structure and static tolerance to errors and attacks. Though every power grid in the study has exponential degree distributions, most of which without typical small-world topology, they were found to show patterns of reaction to node loss similar to those found in scale-free networks. Their observations stipulate that at the node removal behavior could be logarithmically related to the power grid size.

In Ref. [20], a cascading model was applied to the electrical power grid of the western United States. As a result, it was derived that global cascades are prone to be more probably triggered by load-based intentional attacks than by random or degree-based removal of nodes. The attack on a single node with large load may make the largest connected component decrease to less than half of its initial size, though the network is highly tolerant.

In Ref. [21], another cascading failure model was applied to the North American Power Grid. The model of the power grid used its actual topology and plausible assumptions about the load and overload of transmission substations. It was observed that the loss of a single substation can lead to a 25 % loss of transmission efficiency caused by an overload cascade in the network. A systematic study of the damage caused by the loss of a node suggested that the disruption of 40 % of the transmission substations may lead to cascading failures. While the loss of a single node can inflict primary substantial damage, the following removals have only incremental effects.

In Ref. [22], another cascading failure model was applied to the Italian power grid. The authors neglected the details of the electromagnetic processes and only focused on the topological properties of the grid. The objective of this study was to demonstrate that the structure of an electric power grid may provide important information about the vulnerability of the system under cascading failures. The Italian electric power grid network was built from the data on the 220 and 380 kV transmission lines of the GRTN web-site [23]. The network model has 341 nodes (substations) and 517 edges (transmission lines). Different kinds of nodes have been distinguished.

The network robustness is usually measured by the size of the largest connected component or by the average geometric distance as a function of the percentage of nodes/links removed. In the former works mentioned, the main attention has been on the number of removals needed to observe the serious decrease of system performance measured by these metrics. Nevertheless, in practical security analysis, it would be also meaningful to find what the critical components of the network are, i.e., the vertices/edges really crucial for the functioning of the network [24].

In Ref. [25], based on the general assessment of network performance in terms of efficiency, the drop of efficiency by cutting singular lines was applied to high-voltage electrical power grids to locate critical lines and best improvements. In Ref. [26], the topological properties of also high-voltage electrical power transmission networks of the Italian 380 kV, the French 400 kV and the Spanish 400 kV networks have been studied from available data. An assessment of the vulnerability of the networks has been implemented by analyzing the level of damage caused by a controlled removal of links. Such topological studies could be useful for the assessment of vulnerabilities and for designing specific actions to reduce topological weaknesses. As the analyzed grids are the same as the former case, some of their results are consistent.

## Pure Topological and Extended Topological Approaches

Power grids have been widely acknowledged as a typical complex network because of both their huge sizes and the complex interactions among components. However, former works only apply the methodology and metrics of CN directly to power grids and consider them from a pure topological perspective. Some specific physical properties and constraints of power grids not taken into account have serious impacts on the power systems security problems. Here we will introduce the main shortcomings of the pure topological approach we found for power system security assessment.

The distance between two vertices and the length of a path are critical concepts in the definition of several important metrics in CN, such as average distance, betweenness and global efficiency. In unweighted, undirected graphs, the number of edges in a path connecting vertices $i$ and $j$ is called the length of the path. A geodesic path (or shortest path) between vertices $i$ and $j$ is one of the paths connecting these vertices with minimum length; the length of the geodesic paths is the distance $d_{ij}$ between these two vertices [27].

However, from the perspective of engineering, distance should have a more practical meaning and should be a metric for the "cost" involved when a physical quantity is transmitted between the two nodes through the network. For electrical power grids, the cost of power transmission between two buses can be described from both an economic and a technological point of view, such as transmission losses or voltage drop. Therefore, in power system engineering, the description of distance by a pure topological approach cannot effectively reflect these related features and must be replaced by the description of "electrical distance" from an extended topological perspective.

In the general theory of CN, all elements are treated identically to avoid difficulties involved with their differentiation and dynamical behavior characterization [19]. Correspondingly, vertices are considered identical in the definition of several metrics, such as betweenness and global efficiency, where transmission of physical quantity was considered from any vertex to any other one, even for power grids [25].

Nevertheless, the essential function of power grids is to transmit electrical power from any generator bus to any load bus with eligible quality. Generally, we can classify the buses in power transmission networks as generation buses $B_g$, transmission buses $B_t$ and distribution buses $B_d$. From the point view of extended topological perspective, power transmission should only be considered from generation buses to load buses.

In the pure topological approach, edges are generally described in unweighted ways in the definition of several related metrics, such as distance, degree and betweenness [27].

However, in power system engineering, transmission lines have a very important feature that is a line flow limit, which restricts the ability of lines for power transmission according to several economic and technological factors. As this feature is critical for the network to perform its essential function, it cannot be neglected in the analysis related to security issues. In the extended topological view, different lines may have very different values of this parameter and therefore its distribution may also be important for security assessment.

As in the definition of distance, betweenness and global efficiency, the physical quantity transmission between two vertices is always supposed to be through the shortest path [27]. This assumption is still kept in some works on power grids [16, 22, 25].

This is the most unrealistic assumption from the point of view of power system engineering. Power transmission from a generator bus $g$ to a load bus $d$ will involve most lines or a huge number of paths with different levels of contribution. In a power flow linear model, the different contributions of lines in power transmission can be described by the Power Transmission Distribution Factors (PTDF). PTDF is a matrix that reflects the sensitivity of the power flow on the lines to the change in the injection power of buses and withdrawn at a reference bus. For a network with $N$ nodes and $Y$ lines, the matrix of PTDF can be written as:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ & & \vdots & \\ a_{Y1} & a_{Y2} & \cdots & a_{YN} \end{bmatrix} \tag{1}$$

where $a_{ij}$ is the change of power in line $i$ for a unit change of power injection at node $j$. The columns corresponding to node $g$ and node $d$ can be written as $\{a_{ig}\}i = 1,\ldots,Y$ and $\{\mathrm{a}_{id}\}i = 1,\ldots,Y$. Then the distribution factor $a_i^{gd}$ of the $i$th line corresponding to power injection at node $g$ and withdrawn at node $d$ can be calculated as:

$$a_i^{gd} = a_{ig} - a_{id} \quad (i = 1\ldots Y) \tag{2}$$

The network model in the pure topological description of CN is unweighted and undirected. The identification of possible paths connecting two nodes is based on graph theory where transmission lines are assumed bidirectional [22], whereas, as we have discussed, the power transmission behavior between two nodes completely depends on physical rules that can be reflected by the PTDF. As PTDF has signs, the lines connecting to one node should be classified as input or output lines. Therefore, some paths in the undirected model may be not valid in the directed power transmission networks.

With the shortcomings of pure topological approaches discussed above, it is obvious that new extended topological approaches with consideration of specific physical features in power system engineering would be necessary and promising.

## Metrics for Assessing the Criticality of the Network Components

### *Entropic Degree*

The connectivity of a node is traditionally measured by the degree in the unweighted topological model or strength in the weighted model. In an unweighted and undirected network model, according to traditional graph theory, the degree of a vertex $i$ is the number of edges connected to it (or the number of vertices adjacent to it), we rewrite it as:

$$k_i = \sum_{j \in B} c_{ij} \tag{3}$$

In a weighted graph, connectivity can also be described by strength as the sum of the weights of the corresponding edges, we rewrite it as:

$$s_i = \sum_{j \in B} w_{ij} \tag{4}$$

where $w_{ij}$ represents the weight of line connecting $i$ and $j$.

As a measurement of connectivity for a vertex, the definition of degree in a weighted network model should reflect the following factors:

- The strength of connections in terms of the weight of the edges;
- The number of edges connected with the vertex;
- The distribution of weights among edges.

It is obvious that the definition in (3) loses the information of the first factor and the definition in (4) loses information of the second factor. None of them can reflect the third factor.

For example, in Fig. 2, the results of (3) and (4) would be very different:

$$k_i(A) = 1; \quad k_i(B) = 2; \quad k_i(C) = 3$$
$$s_i(A) = s_i(B) = s_i(C) = 1$$

In Fig. 3, the results from (3) or (4) are all the same for both cases:

$$k_i(A) = k_i(B) = 2$$
$$s_i(A) = s_i(B) = 1$$

However, for case (A), both edges have the same importance for the node. For case (B), it is obvious that one edge is more important than another as it takes 90 % of the connection. Under a failure of the most important line, case (B) is more vulnerable than case (A).

We resort to the concept of entropy to define degree with consideration of all the three mentioned factors.

First, we consider $p_{ij}$ as the normalized weight of the edge between vertices $i$ and $j$ for each edge $l_{ij}$ connecting nodes $i$ and $j$:

$$p_{ij} = w_{ij} \sum_{j \in B} w_{ij} \tag{5}$$

It is obvious that $\sum_{j \in B} p_{ij} = 1$

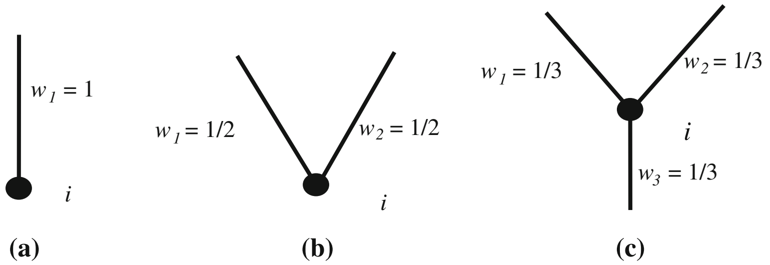
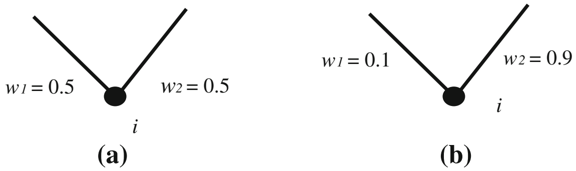


**Fig. 2** Same total weight with different connections

**Fig. 3** Different distribution of weights



Then, the entropic degree $g_i$ of vertex $i$ can be defined with entropy as:

$$g_i = \left(1 - \sum_{j \in B} p_{ij} \bullet \log p_{ij}\right) \sum_{j \in B} w_{ij} \tag{6}$$

As degree is a traditional concept in graph theory and widely applied for the analysis in complex networks, the proposed entropic degree may be a good replacement for research in weighted network models which include not only power grids but also other weighted networked systems. For power grids, it may directly give a quantitative measurement to indicate the importance of buses and their difference. The most important buses may need more resource to be protected or be more likely to be selected as targets of intentional attacks. If measured with the pure topological concept of degree, the corresponding results may be far from reality. Therefore, this entropic degree can give more reasonable evaluation of the importance of buses by taking into account not only the total strength of the connection but also the distribution of strength that may be sensitive for malicious attacks.

### *T-Betweeness for Buses*

In the traditional unweighted and undirected model, the betweenness of a component $u$ in the network Y has been defined as the number of shortest paths traversing the component $u$; we rewrite it as:

$$\Gamma_u = \sum_{\substack{i,j \in B \\ i \neq j}} \sigma(i, u, j) \tag{7}$$

where $\sigma(i, k, j)$ is the number of shortest paths between vertices $i$ and $j$.

This definition has several shortcomings for the application in power grids:

In the traditional definition, the flow in the network has been considered from whichever node $i$ to whichever node $j$. However, the essential function of power grids is to transmit electrical power from any generator bus to any load bus with eligible quality. Generally, we can classify the buses in power transmission networks as generation buses $B_g$, transmission buses $B_t$ and distribution buses $B_d$. Power transmission should be only considered from generation buses to load buses.

In the traditional definition, the transmission between any pair of nodes $i$ and $j$ or $g$ and $d$ is considered equally. However, since each transmission line has its own specific power flow limit, the capacities of the network to transmit power from $i$ to $j$ and from $g$ to $d$ may be quantitatively different due to the configuration of all lines with different power flow limits and to the distribution of the power flow among the lines.

In the traditional definition, the physical quantity transmission between two nodes is always supposed to be through the shortest path. This is the most unrealistic assumption from the point of view of power system engineering. Power transmission from a generator bus $g$ to a load bus $d$ will involve most lines or a huge number of paths with different extents of contributions.

When we consider power transmission from one generator bus $g$ to one load bus $d$, as PTDF has sign, we can divide the set of edges $\mathrm{L}^b$ connected to bus $b$ ($b \neq g$, $b \neq d$) into two subsets: $\mathrm{L}_{in}^b$ inputting power flow into $b$ and $\mathrm{L}_{out}^b$ outputting power flow from $b$. According to the theory of electrical circuits, as the total power injected into $b$ must be equal to the power output from $b$, we have:

$$\Gamma_b^{gd} = \sum_{l \in L_{in}^b} C_g^d \left| a_l^{gd} \right| = \sum_{l \in L_{out}^b} C_g^d \left| a_l^{gd} \right| = \frac{1}{2} \sum_{l \in L^b} C_g^d \left| a_l^{gd} \right| \tag{8}$$

*where* $C_g^d$ is the power transfer capacity of the transmission network from generator $g$ to load $d$.

If $b$ is only connected by one single line, it is obvious that $\Gamma_b^{gd} = 0$ in such situation since $b$ is neither a source nor a destination of power flow.

The new T-betweenness of bus $b$ can be defined as:

$$\Gamma_b^E = \sum_{g \in B_g} \sum_{d \in B_d} \Gamma_b^{gd} \tag{9}$$

## *T-Betweeness for Lines*

When we consider power transmission from one generator bus $g$ to one load bus $d$, as PTDF has sign, if we specify a reference direction for line $l$, the PTDF value $a_l^{gd}$ should be positive, negative or zero. Then we define the positive T-betweenness of $l$ as:

$$\Gamma_l^p = \sum_{g \in B_g} \sum_{d \in B_d} C_g^d a_l^{gd} \quad \left( \text{if } a_l^{gd} > 0 \right) \tag{10}$$

If there is no $a_l^{gd} > 0$, then $\Gamma_l^p = 0$.

The negative T-betweenness of $l$ can be defined as:

$$\Gamma_l^n = \sum_{g \in B_g} \sum_{d \in B_d} C_g^d a_l^{gd} \quad \left( \text{if } a_l^{gd} < 0 \right) \tag{11}$$

If there is no $a_l^{gd<0}$, then $\Gamma_l^n = 0$.

The T-betweenness of line $l$ can be defined as:

$$\Gamma_l^E = MAX\left[\Gamma_l^p, \left|\Gamma_l^n\right|\right] \tag{12}$$

As the power system can work at different configurations in terms of generation and load distributions, the positive power transmission and negative transmission along the same line *l* may not happen at the same time, so we use their maximum absolute value.

## Topological Approaches for Component Ranking

### *Efficiency*

Efficiency has been first introduced for small world networks, in which the average distance and the clustering coefficient define this property. Efficient networks are both highly clustered and closely connected averagely. The average geodestic distance is defined as:

$$D^Y = \frac{1}{B(B-1)} \sum_{\substack{i,j \in B \\ i \neq j}} d_{ij} \tag{13}$$

The definition of characteristic path length (or average distance) is valid only in a completely connected network Y where at least one path, composed by a finite number of edges, connecting any couple of vertices must exist; if two vertices *i* and *j* are not connected the relative distance $d_{ij} \to +\infty$, and the corresponding average distance, as defined in (13), tends to infinity [28]. In studying the network security, the removal of vertices and edges as a result of a failure is often considered and this may likely produce a non-connected network.

The concept of efficiency is closely related to that of distance. The distance, as we discussed, is generally assumed as a measure of the difficulty, cost or effort needed to transfer physical quantities over a network and so an efficiency $\varepsilon_{ij}$ can be associated to a pair of vertices *i* and *j* and defined as:

$$\varepsilon_{ij} = \frac{1}{d_{ij}} \quad (i,j \in B,\ i \neq j) \tag{14}$$

If no path exists between vertices *i* and *j*, $d_{ij} \to +\infty$ and, therefore, $\varepsilon_{ij}$= 0.

By averaging the efficiencies we can define the *global efficiency* $E^Y$ of the network Y as [29]:

$$E^Y = \frac{\sum\limits_{\substack{i,j \in B \\ i \neq j}} \varepsilon_{ij}}{B(B-1)} = \frac{1}{B(B-1)} \sum_{\substack{i,j \in B \\ i \neq j}} \frac{1}{d_{ij}} \tag{15}$$

The concept of efficiency can be used to assess the possible impacts of a fault or failure onto a network and its resilience; local efficiency is to quantify the performance of the connections of the vertices in the neighborhood of $i$ after a failure of $i$ and is a measure of the failure tolerance as well [29].

Resorting to the new metrics, small world network can be characterized by high global and local efficiencies that basically individuate the same situation pointed out by small average distance and high clustering coefficient.

The loss of a component would affect the global efficiency of the network and so the detection and ranking of the most critical components can be undertaken assessing the drop of efficiency $E_q^{\Delta}$ that each failure would cause.

$$E_q^{\Delta} = \frac{E^Y - E_{-q}^Y}{E^Y} \tag{16}$$

where $E^Y$ is the global efficiency of the original network and $E_{-q}^Y$ is the global efficiency after the removal of the component (vertex or edge) $q$.

A global metric for the network vulnerability is the maximum vulnerability for all of its vertices:

$$E_M^{\Delta} = \underset{q \in \mathscr{B} \cup \mathscr{L}}{MAX} E_q^{\Delta} \tag{17}$$

## *From Efficiency to Net-Ability*

The concept of distance within a network may be explained as the difficulty or cost to transfer physical quantities between a pair of nodes. Distance in general depends on the length of the path between the two nodes and thus should be defined as a function of the characteristics of the lines in the path. The economic and technical difficulties, which eventually amount to some sort of costs, for transmission of electrical power through a path depend on both the power flow through the lines and their impedance: with the same impedance, more power flow causes higher costs; with the same power flow, a bigger impedance causes higher costs. Consequently, the length of path $k$ from node $g$ to node $d$ is related not only to the impedance of each line of the path but also to the power flows through the lines of the path. As a result, we define the electrical length of a path $k$ as:

$$L^k = \sum_{l \in k} a_l^{gd} Z_l \tag{18}$$

where $a_l^{gd}$ is the Power Transmission Distribution Factor of line $l$ in path $k$ and $Z_l$ is its impedance.

Therefore, the net-ability based on topological efficiency with consideration of contributions from all paths (not only the shortest path as in pure topological approach) can be defined as:

$$A_{\mathscr{Y}} = \frac{1}{B_g B_d} \sum_{g \in \mathscr{B}_g} \sum_{d \in_d} C_g^d \sum_{k \in \mathscr{K}_g^d} p_k^{gd} \frac{1}{L^k} \tag{19}$$

where $B_g$ is the number of buses in $B_g$ and $B_d$ is the number of buses in $B_d$, $p_k^{gd}$ is the proportion of contribution in transmission of path $k$, $C_g^d$ will be defined later as the transmission capacity from $g$ to $d$. $K_g^d$ is the set of all paths between $g$ and $d$.

In the DC power flow equation, the definition of length for a path between $g$ and $d$ is just equal to the voltage angle difference between $g$ and $d$ when transmitting one unit power from $g$ to $d$. Therefore, as the voltage angle difference is fixed, the length $L^k$ is the same for any path $k$ in $K_g^d$ between $g$ and $d$. Hence, Eq. (19) can be developed further as (with consideration of $\sum_{k \in \mathscr{K}_g^d} p_k^{gd} = 1$):

$$A_{\mathscr{Y}} = \frac{1}{B_g B_d} \sum_{g \in \mathscr{B}_g} \sum_{d \in \mathscr{B}_d} C_g^d \frac{1}{L^k} \tag{20}$$

Then $L^k$ is just the electrical distance between $g$ and $d$.

We can define the generator bus $g$ together with all the involved paths $K_g^d$ from it to the distribution bus $d$ as an efficient power supply scheme $h(g, d)$ for power consuming on $d$. Then the capacity of scheme $h$ can be defined in the following way: the injection from $g$ is increased from zero to $C_g^d$ when the first line among all involved paths reaches its maximum power flow limit. $C_g^d$ is the capacity of the power supply scheme $h(g, d)$.

$$C_g^d = \underset{l \in L}{MIN} \left[ P_l^{\max} \Big/ \left| a_l^{gd} \right| \right] \tag{21}$$

where:

L is the set of all lines

$P_l^{max}$ is the power flow limit of line $l$

$a_l^{gd}$ is the PTDF of line $l$ for a power injection/withdrawal at buses $g/d$

We used the equivalent impedance to calculate the electrical distance $L_k$ from the point view of power system engineering. The definition of net-ability $A$ for a power grid Y is:

$$A_Y = \frac{1}{B_g B_d} \sum_{g \in B_g} \sum_{d \in B_d} C_g^d \frac{1}{Z_t} \tag{22}$$

$B_g$ is the number of buses in $B_g$ and $B_d$ is the number of buses in $B_d$.

$$Z_t = \frac{U_{gd}}{I_g} = U_{gd} \Rightarrow Z_t = (Z_{gg} - Z_{gd}) - (Z_{gd} - Z_{dd}) \tag{23}$$

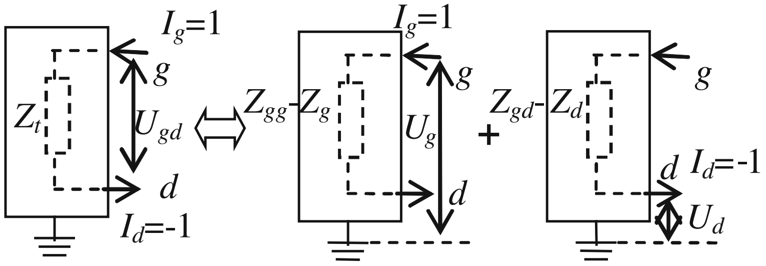


**Fig. 4** The computation of equivalent impedance

$Z_t$ is the equivalent impedance from generator bus $g$ to load bus $d$ as described in Fig. 4. $Z_t$ is an extended concept of electrical distance between $g$ and $d$ to reflect economic and technical cost for power transmission.

According to the DC power flow equation, the value of $Z_t$ is just equal to the voltage angle difference between $g$ and $d$ with one unit of power injected at $g$ and withdrawn at $d$. Then the value of $Z_t$ is just the value of $L_k$.

## ***Ranking by Drop of Net-Ability***

In Fig. 5, for the ideal 1-bus case (A), all generators and loads are connected by an ideal bus with infinite capacity and zero impedance (distance) and the net-ability is infinite. In case (C) where all generator buses and load buses are isolated, the connecting impedance or zero-power transfer capacity makes the net-ability null. In real cases (B) the net-ability, as defined in (22) is between infinite and zero.

Similar to the approach from efficiency, where critical components were identified according to the relative drop of global efficiency caused by the failure of each component, we can consider the failure of each line $l$ (removed one by one) and calculate the relative drop of net-ability, caused by each failure:

$$\Delta A^r = \frac{A_Y - A_{Y-l}}{A_Y} \tag{24}$$

The relative drop of net-ability will indicate which lines are the most critical ones for the operation of the network under current normal conditions. Furthermore, by locating critical transmission lines, it may also be useful to indicate how the performance of the network can be improved by re-enforcing its structure.

However, for a large power transmission network with real size of buses and lines, the calculation burden would be a critical issue. For calculation of net-ability, it has to calculate $B_g B_d$ times of PTDF between any generation bus and load bus. To calculate the relative drop of net-ability by removing each transmission line, if the total number of lines in Y is $L$, generally the calculation for

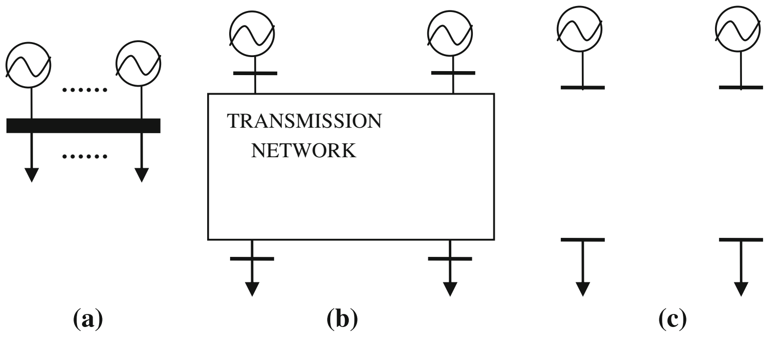


**Fig. 5** Reference cases

net-ability needs to be repeated for $L + 1$ times. For large-scale networks, such as the network of UCTE, the corresponding calculation burden may be unacceptable. Therefore, it is necessary to find valid methods to decrease the burden as later discussed.

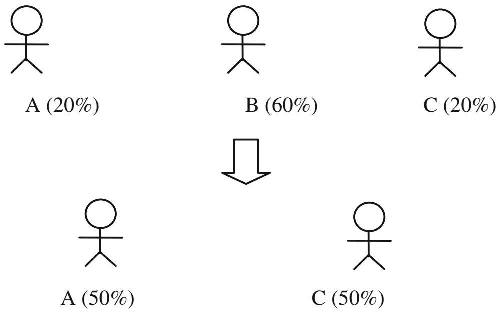
## Important and Critical Components in Transmission Network

### *What is Different Between Important and Critical Components?*

To give a clear definition and description between important and critical, we begin with an example about a team composed of a group of members as shown in the Fig. 6.

As we can see from Fig. 6, in the team, the member B takes sixty percent of the work of the whole team which is much higher than the work of the other two as twenty percent respectively. So we can say that the member B is an important

**Fig. 6** Example for important but no critical member



member for the team since he is responsible for most part of the work in the whole team. However, if the member B is removed from this team and the other two members have enough ability to take the work left by the member B as shown in the figure, the performance and the function of the team could be as the same as before. In such situation, although we can say that B is important, but we may not consider him as critical.

Another situation can also be described by this example where we change to another different scenario as shown in Fig. 7.

This time, the situation before removing B is the same as the last example, therefore we consider B still as an important member. However, if B is removed from this team, due to any reason (ability, resource or configuration), A and C can only take very small part of work left by B, only sixty percent of the work of the whole team can be done as shown in the figure. The absence of B can impact greatly on the performance and function of the whole team. In such situation, we would say that B is both important and also critical.

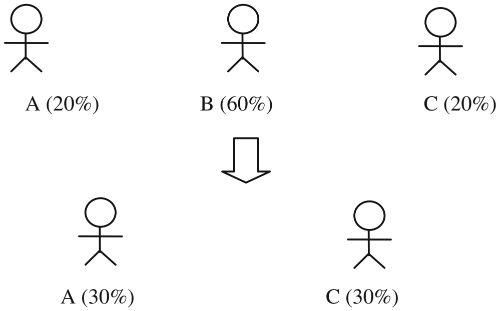
This logic can be easily transferred to the contexts of complex networks where we can give clear definitions as:

A component of the network is *important* if it takes remarkably higher proportion, quantitatively defined by the users, of responsibility for function of the whole network lying on the current configuration of the network compared with other components.

A component of the network is *critical* if its absence can have remarkable impact, quantitatively defined by the users, on the performance and function of the whole network lying on the change of the network configuration compared with other components.

From the discussion before, we can see that betweenness is a typical metric to measure how much responsibility a component takes for the function of the whole network in an unweighted and undirected pure topological model. This is a static measurement since it only depends on the current configuration of the network. The relative drop of global performance is to measure the impact on the network performance by the absence of a component. This is a dynamic measurement since it depends on the network configurations both before and after the failure of the component. Therefore, important and critical components all have their own specific definitions and meaning, and should not be confused.

**Fig. 7** Example for important but also critical member



## *Important and Critical Components in Power Grids*

According to the definition and analysis above, we can generally get a further conclusion in the contexts of complex networks: an important component may not necessarily be a critical component, however, a critical component must be an important component otherwise its absence cannot make serious impacts; or we can say that the critical components should be a subset of the important components. In a complex network, the quantity of important components may be more than the quantity of critical components.

With former definition of important components in CN, T-betweenness is an ideal indicator to reflect the responsibility of a component for the function of the whole power transmission network.

According to the definition proposed, a metric of performance is necessary to identify critical components in complex networks. Efficiency has been widely used as this type of metric in many research works, however as indicated in [30–32], it fails in describing specific features of power grids. Therefore, based on an extended topological approach, we have to resort to the concept of net-ability as the performance of power transmission networks.

The relative drop of net-ability in (24) will indicate which components (line and bus) are the most critical ones for the operation of the network under current normal conditions. Furthermore, by locating critical transmission lines, it may also be useful to indicate how the performance of the network can be improved by re-enforcing its structure.

According to what we have discussed, the important and critical components in power grids are respectively identified by their T-betweenness and relative drop of net-ability. Although T-betweenness and net-ability are two different metrics, they have deep interrelation caused by PTDF and equivalent impedance. As we can see from former definitions, both T-betweenness and net-ability depend greatly on the power transfer capacity $C_g^d$ which are exactly defined in the same way by PTDF and transfer capacity of the lines in the two metrics.

Furthermore, the PTDF in T-betweenness depend on the relative relation in impedance of transmission lines among the whole network. Therefore, suppose that the influence from transfer capacity $C_g^d$ can be neglected, we can generally judge that an important line should have relatively lower impedance or an important bus should connect to lines with relatively lower impedance, which cause higher PTDF compared with other lines. Meanwhile, if the absence of a critical component can cause incredibly decrease in equivalent impedance between many pairs of buses, this component must be related to lower impedance itself which may take them higher T-betweenness. However, conversely, the failure of an important line or bus described by absence of one or several lines with relatively lower impedance may not necessarily cause a serious drop in equivalent impedance between many pairs of buses because it also depends on the value and distribution of impedance in other lines. In summary, a critical component must be important, but an important component may not necessarily be critical.

Therefore, from the discussion above, we can generally conclude that the critical components in power grids should be a subset of their important components. This is important to decrease the calculation burden in ranking critical components by the relative drop of net-ability as we discussed in the last section. As the calculation burden for T-betweenness of all components is similar for calculation of net-ability for one time, we can make ranking of important components by the results of T-betweenness. Since the critical components are in subset of important components, limited top components in ranking of important components can be selected to perform calculation of (24) for relative drop of net-ability to identify critical components. In this way, the calculation burden can be greatly reduced.

## Metrics for the Overall Topological Assessment of the Grid

### *Introduction to Path-Redundancy*

Net-ability is originated from efficiency to indicate the aptitude of a network to perform its function in transmitting physical quantities between specified vertices based on current structure and physical conditions of the network. However, when we consider security, we may take care of the performance of the network after component failures or intentional attacks. Although to calculate the relative drop of net-ability in (24) can provide some detail information related to specific components, we still need a global metric as general assessment for ability of networks to survive from failures or attacks.

In a meshed system, for a given couple of buses, at least one path, composed by a sub-set of the lines of the system, can be identified. Higher is the number of paths connecting whichever couple of buses in the system higher would be the system resistance to attacks or failures.

As the PTDF indicates the contributions of all lines in power transmission from bus $g$ to bus $d$, it is possible to calculate the contribution of each path (the PTDF of a path) in power transmission according to the PTDF of the lines composing the path. If we consider the PTDF values of lines as DC power flow when transmitting one unit power from $g$ to $d$, we can get the power flow (i.e. PTDF) of a path by traversing the whole paths. The general procedure can be explained with the following steps:

1. Starting from the source bus $g$, follow an output line as the beginning of a path $p$ and consider the PTDF of the line as the initial PTDF of path $p$.
2. When path $p$ arrives at a new bus $i$ and if $i$ is not bus $d$, then partition path $p$ into multiple new paths according to the output lines of $i$ and recalculate the PTDF for each of them.
3. Continue to follow one of the new paths and repeat step 2 until the current path arrives at $d$.

4. Repeat to follow all possible paths until they all arrive at $d$.

In step 2, the recalculation of the PTDF should consider the three different cases shown in Fig. 8. As the path is a different concept from the line, multiple paths can go through the same line; we indicate paths by dashed lines and lines by solid lines.

For case (a), no matter how many input paths, since there is only one output line from node $i$, the PTDF of path $p$ still keeps unchanged. For case (b), since there is only one input path $p$, it would be partitioned as multiple new paths corresponding to the multiple output lines. Therefore, the PTDF for each new path is just equal to the PTDF of the corresponding output line. For case (c) where we have multiple input paths with multiple output lines, in a linear model, we suppose the power injected from different paths should be mixed completely uniformly at bus $i$. Therefore, we can summarize the three cases as: if node $i$ has $U$ output lines ($l_1$, $l_2$,…, $l_U$), each input path $p$ with PTDF $f_p$ would be partitioned as $U$ new paths. The PTDF $f_p^k$ of the new path from $p$ through line $l_k$ ($k = 1,\ldots,U$) can be calculated as:

$$f_p^k = f_p \bullet \left( a_{l_k}^{gd} \Big/ \sum_{s=1,\ldots,U} a_{l_s}^{gd} \right) \tag{25}$$

Assume that $K_g^d$ is the set of all valid paths from $g$ to $d$, we can get:

$$\sum_{p \in K_g^d} f_p = 1 \tag{26}$$

$f_p$ can be considered as a weight indicating how much path $p$ contributes to the power transmission from $g$ to $d$. According to Eq. (26), the paths redundancy $R_g^d$ from bus $g$ to $d$ can be defined as the entropy of the contributions (PTDF) of all paths involved in power transmission from bus $g$ to $d$:

$$R_g^d = -\sum_{p \in K_g^d} f_p \bullet \log f_p \tag{27}$$

The paths redundancy between two buses is related to the number of paths and the proportions for the power to be routed through those paths. The average paths redundancy of the whole network Y can be defined as:

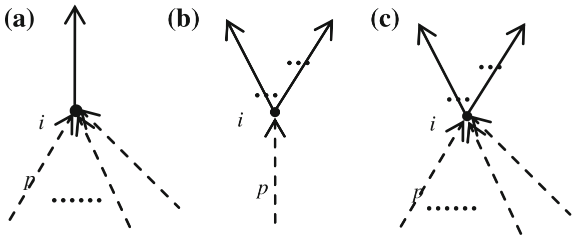


**Fig. 8** Different cases for recalculation of PTDF for paths

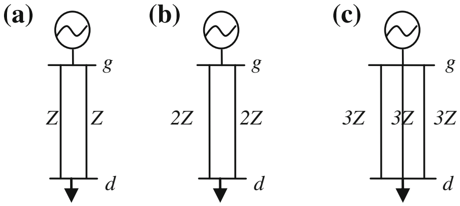


**Fig. 9** Comparison for net-ability and paths redundancy

$$R_Y = \frac{1}{B_g B_d} \sum_{g \in B_g} \sum_{d \in B_d} R_g^d \tag{28}$$

Paths redundancy is a concept independent of net-ability. In Fig. 9, assuming $C_g^d$ is the same for all cases, cases (a) and (b) have different net-ability due to different impedance. However, since for each case there are two paths with equal share of power transfer (50 %), their flow paths redundancies measured by (27) are same. The cases (b) and (c) have the same net-ability due to the same capacity and equivalent impedance. However, they have different paths redundancy defined in (27). The higher paths redundancy of the case (c) results in higher resilience to attacks or failures in transmission network. Even with the same number of paths, a more averaged distribution of the PTDF in paths causes higher entropy in (27), which means more resilience to malicious attacks to the most loaded path.

As shown in Fig. 5, the ideal 1-bus case (A) can be considered as composed of infinite paths with infinite capacity and zero impedance (distance) from whichever generator to whichever load. Obviously, the paths redundancy for this case is infinite. For the opposite extreme case (C), it is obvious that the paths redundancy is zero, since there is no path. Definition in (27) can give a quantitative measurement for case (B) between these two extreme cases.

## *From Net-Ability and Path-Redundancy to Survivability*

To make a new assessment of structural vulnerability for power grids with consideration of not only current static performance but also possible resilience to failures or attacks, we define here a new metric, called survivability, to indicate the capability of a network to keep on performing properly its function in the presence of limited attacks or failures on transmission paths. Therefore, this survivability depends on both net-ability and paths redundancy:

- With equal net-ability, more paths redundancy means higher survivability.
- With equal paths redundancy, more net-ability means higher survivability.

The survivability for a transmission network Y is defined as:

$$Sr_Y = \frac{1}{B_g B_d} \sum_{g \in B_g} \sum_{d \in B_d} R_g^d C_g^d \frac{1}{Z_t} \tag{29}$$

In Fig. 9, the survivability of case (a) is higher than that of case (b) since the former net-ability is higher and their paths redundancies are the same. The survivability of case (c) is higher than that of case (b) since the latter paths redundancy is higher and they have the same net-ability.

As shown in Fig. 5, the ideal 1-bus case (A) can be considered with infinite net-ability and infinite paths redundancy. Alternatively, since the survivability is only considered with reference to attacks and failures in transmission networks, the survivability of this case is infinite because there is no transmission network. For the opposite extreme case (C), with no net-ability and no paths redundancy, it is obvious that the survivability is zero. Definition in (29) can give a quantitative measurement for case (B) which is between these two extreme cases.

The relations among net-ability, paths redundancy and survivability can be explained still considering the cup in Fig. 1 as an example. While the volume represents net-ability, paths redundancy is corresponding to the strength of the cup (a cup being made of glass is more fragile than a cup being made of steel). The ability of a cup to survive from a crash (an attack) to continuously perform its function (holding water) depends on both its original volume and its strength. Therefore, survivability should take into account both net-ability and paths redundancy together to consider the both aspects.

An important problem in the calculation of survivability and paths redundancy is the calculation burden of PTDF of all paths for a transmission network of real scale. For a network with several hundred or several thousand of nodes, there may be millions of paths between two nodes. This may make the time of calculation unacceptable in practice. However, the distribution of PTDF in paths is very uneven in power transmission networks. Even with millions of paths, only a very small part of these paths (e.g. hundreds of) takes most of the power flow.

Therefore, for the calculation in (25), we can define a threshold $\theta$. Only when $a_l^{gd} > \theta$, line $l$ can be considered in calculation of (25). In this way, it is possible to get meaningful results within an acceptable time.

## Conclusions

Power systems play a pivotal role, as fundamentally critical infrastructures, in assuring the proper functioning of our societies. Therefore, the security of power systems has drawn attention since their inception. As a consequence, analysis approaches and tools have been developed to simulate the system response against any change, either internal or external. However, due to the Newtonian assumptions, they always depend on the given contingencies and operating conditions, which makes them not only computationally impractical but even impossible. As a fundamental change of ideology to combat the security problems in power systems, complex network theory, more specifically, topological analysis, was applied as a pioneer attempt. By abstracting the power system as a graph, the transmission network becomes the decisive factor. The trial showed some promising potentials in the arena, such as providing indices for overall characteristics of the system and identifying important structural components independent of the operating conditions. In any case those approaches showed some drawbacks. As the fact that, irrespective of the physical laws governing power systems, they ignore the engineering peculiarities of the system under study. All these shortcomings prompt the needs to reinforce the approach by considering aspects ignored by pure topological analysis.

We proposed a comprehensive framework composed of a set of metrics based on extended topological analysis derived from pure topological ones. The framework provides promising tools to analyze the general and overall security and identify vulnerabilities of the system determined by structural factors. More specifically, based on static assessment, “entropy degree” and “T-betweenness” can be used to measure the importance of a single component; while by ranking the drop of “net-ability” from dynamic assessment, the criticality of components can be observed. By considering both the static and dynamic results together, the correlations of the important and critical components can be revealed. In contrast, “path-redundancy” provides a global index indicating the ability of the network to survive from components failure. In light of considering the system resilience to limited failures on transmission paths, “survivability”, depends on both net-ability and path-redundancy was proposed.

Although progress and improvements have been made with respect to pure topological analysis, the extended topological analysis still faces many challenges when applying to power systems.

The first and foremost problem is how to validate the results in real systems. As the topology is only one of the two dimensions of the security problem, comparisons with system data or references that are strictly connected with features other than structure may not provide satisfactory feedbacks. Also, due to the statistical property of results given by the extended topological analysis, the vulnerable points spot by them may not show in real cases used as benchmark to evaluate the results. Therefore, it seems reasonable to compare the results with statistics from system operation. However, blackouts are not so frequent enough to build up meaningful statistic results for the comparison.

Another issue involves a more complicated consideration: dynamics. In the vocabulary of power systems, dynamic refers to the quantities (e.g. voltage/angular behaviors) changes over time with stability concerns rather than topology changes and corresponding power flow changes over transmission lines. A bad news to the topological analysis, including the extended one, is that most of the blackouts happened due to voltage, frequency, or angular instability rather than overloads. Therefore, new engineering features should be incorporated into the extended topological analysis to reflect the mechanism of blackouts in reality. However, it may force us to consider the operating conditions to reveal dynamic instabilities. Moreover, to consider the dynamic behaviors of rotating components (e.g. generators) and discrete elements (e.g. FACTS) will create mathematically and computationally dimensional disasters when facing large scale systems. Efforts then should be made to strike a balance between the details and usefulness of the extended topological analysis.

Last but not the least, complexity of power systems comes from the hectic interactions among different technical layers and various operational players. The network itself can hardly be a complex system. Although the proposed framework simply considered the interactions between power supply and demand, others are still missing, such as multiple heterogeneous decision makers at national levels and international level: policy makers, regulators, market participants, TSOs, etc. The most important revolution of intelligent grids (i.e. smart grids, super grids) in power systems pose a great challenge to the extended topological analysis to consider multiple levels of dependent systems.

## References

1. Rinaldi SM, Kelly TK (2011) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 21:11–25
2. The International Electrotechnical Commission (2009) IEV number 617-01-01. International Electrotechnical Vocabulary, Mar 2009
3. IEEE/CIGRE Joint Task Force on Stability Terms and Definitions (2004) Definition and classification of power system stability. IEEE Trans Power Syst 19:1387–1401
4. The European Network of Transmission System Operators for Electricity (2012) Glossary of terms, statistical glossary. Available at https://www.entsoe.eu/resources/data-portal/glossary/. Cited 9 Jul 2012
5. The North American Electric Reliability Corporation (2012) Company overview: FAQ. Available at http://www.nerc.com/page.php?cid=1%7C7%7C114. Cited 9 July 2012
6. The International Electrotechnical Commission (2009) IEV number 191-21-03. International Electrotechnical Vocabulary, Mar 2009
7. The International Electrotechnical Commission (2009) IEV number 191-21-01. International Electrotechnical Vocabulary, Mar 2009
8. IEEE Working Group (1978) Reliability indices for use in bulk power system supply adequacy evaluation. IEEE Trans Power Apparatus Syst PAS-97:1097–1103
9. The North American Electric Reliability Corporation (2012) Glossary of terms used in nerc reliability standards. Available at http://www.nerc.com/files/Glossary_of_Terms.pdf. Updated 25 May 2012, cited 9 July 2012
10. The International Electrotechnical Commission (2009) IEV number 617-01-03. International Electrotechnical Vocabulary, Mar 2009
11. The Union for the Coordination of the Transmission of Electricity, Glossary of terms, version 2.2; 2004 June
12. The International Electrotechnical Commission (2009) IEV number 191-02-05. International Electrotechnical Vocabulary, Mar 2009
13. Motto AL et al (2005) A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat. IEEE Trans Power Syst 20:1357–1365
14. Salmeron J et al (2004) Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst 19:905–912

15. Cai GW et al (2007) Identification of the vulnerable transmission segment and cluster of critical machines using line transient potential energy. Int J Electr Power Energy Syst 29:199–207
16. Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. Phys Rev E 69:025103 (R)
17. Platts Global Energy. http://www.platts.com
18. Chassin DP, Posse C (2005) Evaluating North American electric grid reliability using the Barabasi–Albert network model. Phys A 355:667–677
19. Rosas-Casals M, Valverde S, Sole RV (2007) Topological vulnerability of the European power grid under errors and attacks. Int J Bifurcat Chaos 17(7):2465–2475
20. Motter AE, Lai Y-C (2002) Cascade-based attacks on complex networks. Phys Rev E 66:065102 (R)
21. Kinney R, Crucitti P, Albert R, Latora V (2005) modeling cascading failures in the North American power grid. Eur Phys J B—Condens Matter Complex Syst 46(1)
22. Crucittia P, Latora V, Marchioric M (2004) A topological analysis of the Italian electric power grid. Phys A 338:92–97
23. GRTN S.p.A. CartograLa rete di trasmissione, http://www.grtn.it
24. Latora V, Marchiori M (2005) Vulnerability and protection of infrastructure networks. Phys RevE 71:015103(R)
25. Crucitti P, Latora V, Marchiori M (2005) Locating critical lines in high-voltage electrical power grids. Fluctuation Noise Lett 5(2):L201–L208
26. Rosato V, Bologna S, Tiriticco F (2007) Topological properties of high-voltage electrical transmission networks. Electric Power Syst Res 77:99–105
27. Costa LDF, Rodrigues FA, Travieso G, Villas Boas PR (2007) Characterization of complex networks: a survey of measurements. Adv Phys 56(1):167–242
28. Crucittia P, Latorab V, Marchioric M, Rapisardab A (2003) Efficiency of scale-free networks: error and attack tolerance. Phys A 320:622–642
29. Latora V, Marchiori M (2001) Efficient behavior of small-world networks. Physi Cal Rev Lett 87(19):5
30. Bompard E, Napoli R, Xue F (2010) Extended topological approach for the assessment of structural vulnerability in transmission networks. IET Gener Transm Distrib 4(6):716–724
31. Arianos S, Bompard E, Carbone A, Xue F (2009) Power grids vulnerability: a complex network approach. Chaos 19. 013119. doi:10.1063/1.3077229
32. Bompard E, Napoli R, Xue F (2009) Analysis of structural vulnerability in power transmission grids. Int J Crit Infrastruct Protection 2(1–2):5–12