IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Power grids as complex networks: Resilience and reliability analysis

Ali Moradi Amani[1], Member, IEEE, Mahdi Jalili[1], Senior Member, IEEE
[1]School of Engineering, RMIT University, Melbourne, VIC 3001, Australia

Corresponding author: Mahdi Jalili (e-mail: mahdi.jalili@ rmit.edu.au).

This research was supported by Australian Research Council through projects DP200101199 and LP180101309.

ABSTRACT Power grids are cyber-physical systems and can be modelled as network systems where individual units (generators, busbars and loads) are interconnected through physical and cyber links. Network components (nodes/edges) may undergo intentional and/or random failures. In catastrophic cases, a failure initiating from a small set of these components can quickly propagate through the whole network, leading to a cascade of failures that might force a deep whole-grid blackout. Often network components have different vitality and protecting some is more critical than others. This manuscript aims to provide a focused overview of modelling power grids as complex networks and their resilience and reliability analysis. We also perform a critical review of vitality metrics and their precision in power grid resilience analysis. The review is accompanied by some simulations on benchmark and real power grids to show the applicability of these concepts in studying resilience.

INDEX TERMS Power grids, resilience and reliability, complex networks.

I. INTRODUCTION

Many natural and man-made systems can be modelled as network systems where individual units interact over connection links. Network science, which was first started within the physics community, is now a mature field of interdisciplinary science with many potential applications [1]. Real networks share a number of common structural properties, such as scale-free degree distribution, small-worldness, and community structure [2]. This indicates that insights provided by model networks can have significant interpretations of real systems.

Power grids are perhaps the most important engineering systems that can be modelled as networks. They are among the most critical infrastructures and daily lives are disrupted without their proper functioning. Grid failure may lead to significant socio-economic consequences [1, 2]. The existing power grids have been developed based on resilience principles to deal with known critical events. This has made them one of the most reliable complex infrastructures of the current century [3]. However, in recent years, social and environmental concerns have pushed for cleaner energy generation. This, along with advances in renewable energy sources, is changing the structure of power grids towards complex systems comprised of many distributed generations [4-6], which does not necessarily inherits the resilience or reliability. Modern power grids are indeed cyber-physical systems composed of interacting physical power grid, and cyber and communication networks [7]. Such a complex infrastructure requires a new interdisciplinary paradigm for control and optimisation [8, 9] as well as for resilience and reliability analysis [3, 10].

Despite all advances in the design, installation and operation of power grids, failures in power grids are unavoidable [11, 12]. Power grids, like any other network systems, may undergo random and/or intentional failures in their components. These failures may happen because of electrical and/or mechanical faults, extreme weather events, or faulty components [13]. In some cases, because of the improper reaction of protective devices, a single or partial failure may quickly propagate to other parts [14-16]. If no effective action is taken to limit and clear these failures, a cascaded failure happens which may result in a wide-spread blackout over a significant portion of loads [17-23].

To quantify damages in a power grid, as a consequence of a failure or attack, different yet related concepts have been proposed in the literature, such as *resilience*, *reliability*, *robustness*, *fragility,* and *vulnerability* [24]. A network is called *robust* if it can maintain its normal operation against a class of unexpected events. *Vulnerability* is defined as how a network can continuously provide its main

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

functionalities under random failures or intentional attacks [25]. *Resilience* was first defined by C.S. Holling in 1973 as a measure of "the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables." [3]. The resilience of infrastructures can be studied either in the short-term, i.e. before, during and after an event, or in the long-term where the resilience enhancement, using the information and experiences from the past events, is of interest [3, 13, 26]. For instance, an integrated resilience-enhancement framework has been proposed in the form of a robust optimisation model, which provides effective and efficient responses in both preventive and emergency states of a power grid [27].

The resilience of systems has been studied from both control systems and network sciences perspectives [28, 29], where the latter mainly focuses on the complex networks paradigm [30]. The *Complex Network* (CN) concept provides a promising framework for the analysis and control of complex power grids, in which generators and loads can be considered as nodes connected over power cables or communication links [31-36]. The study of complex networks has been mainly a branch of applied mathematics known as *graph theory* [37]. One of the interesting topics in this field is *centrality* (*or vital entities*), which is mainly about identifying nodes and edges with the maximum influence on a desired performance [38-40]. It has been shown that networks may disintegrate considerably faster when their nodes are removed deliberately rather than randomly [41]. Therefore, the identification of central components is interesting for network operators aiming for resilient performance. It is also fascinating for attackers as they may result in maximum disruption. Although many centrality measures have been introduced in the literature, they need to be modified to include physical and electrical properties and limitations for power grid applications [42, 43].

The aim of this manuscript is twofold. First, we review the existing techniques to model modern power grids as networks and study their unique properties as compared to model networks. We then provide a comprehensive review of the latest state-of-the-art in resilience and reliability of power networks and the role of different centrality measures in studying them. The manuscript is organised as follows. The models applicable to large-scale power grids are introduced in Section II. In Section III, a detailed review on the events that affect reliability and resilience of power grids is provided. A literature review on different methods of measuring reliability and resilience of power grids, including flow-based and CN-based techniques, is provided in Section IV. Simulation results in Section V compare the performance of these centrality metrics when applied to some benchmark and real power grids. Finally, concluding remarks and the future outlook are provided in Section VI.

II. POWER GRIDS MODELING

The resilience and reliability of conventional power grids against small perturbations as well as severe faults have been heavily studied in the literature [3, 44-48]. However, with the increased penetration of renewable energy resources, the complex networks approach has recently attracted much attention in modelling and control of power grids [32, 34, 49, 50]. In this section, two main approaches in modelling modern power grids, namely 'complex networks' and 'cyber-physical systems, are reviewed. These models facilitate reliability and resilience studies of power grids through identification of vulnerable points and predicting potential failures [51]. We see that both of these potentially correlated approaches have their own drawbacks in providing practical models for modern power grids which is indeed a gap for further research.

A. COMPLEX NETWORKS AND GRAPH THEORY

In the context of graph theory, a complex network is modelled as a graph of nodes connected over a number of links. It is shown as $G = (V, E)$ where V is the set of N nodes having either static or dynamical behaviours. The set $E \subset V \times V$ includes links that establish a network among nodes. The network may contain directed/undirected and weighted/unweighted links. The pair (i, j) or a_{ij} denotes the edge between nodes i and j. The matrix $A = [a_{ij}]$ is called the adjacency matrix in which a_{ij} takes a non-zero value if there is a link from node i to node j. Two nodes connected by an edge are referred to as adjacent or neighbouring nodes. The set of adjacent nodes to the i^{th} node is defined as $N_i = \{j \in V;\ a_{ij} \neq 0\}$. In unweighted graphs, $a_{ij} \in \{0,1\}$ resulting in a binary adjacency matrix. In weighted graphs, each edge (i, j) is labelled with a weight $w_{ij} \in \mathbb{R}^+$. These weights may quantify the strength of interactions between nodes using parameters such as distance, force, and impedance. $L = [l_{ij}]$ is the Laplacian matrix, which is a zero-row sum matrix with off-diagonal elements equal to $-w_{ij}$ (-1 in unweighted graphs), if there is a link, and 0 otherwise [52]. The diagonal elements of L are the corresponding degree of the nodes. The topology of the network can be either static or evolving. The *degree* of i^{th} node of a network is defined as the number of edges connected to that node, i.e. $d_i = \Sigma_j a_{ij}$. If the network is directed, we have in-degree $d_i^{in} = \Sigma_j a_{ji}$ which shows the number of edges coming into i^{th} node, and the out-degree $d_i^{out} = \Sigma_j a_{ij}$ which is the number of edges going out of it. The degree distribution shows the information on how links are distributed among nodes of the network.

A *walk* from node i to node j is a series of nodes and edges starting from node i and ending to node j. The length of a walk is defined as the number of edges in it. A walk which does not pass through a node more than once is called a *path*. A path between nodes i and j, with the minimum number of edges, is referred to as the shortest path between these nodes and is shown by d_{ij} in this paper. The average shortest path $\bar{S}$ of a network is defined as

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

$$\overline{S} = \frac{1}{N(N-1)} \sum_{i,j \in V} d_{ij} \quad (1)$$

The average path length typically shows how separate the nodes of a network are. In this paper, all networks are supposed to be connected, i.e. there is a path between any two distinct nodes of the network. The existence of closed walks, or the cycle structure in a network, is conveyed by the "clustering coefficient". This feature shows the presence of triangles or loops in a network and quantifies the efficiency of the network in transferring information locally.

B. POWER GRIDS AS COMPLEX NETWORKS

The study of real-world network systems often requires sophisticated network models to mimic their properties. Traditionally, these systems used to be modelled as "random graphs". This approach, proposed by two mathematicians Paul Erdős and Alfréd Rényi in 1960, lies at the intersection of the graph theory and the probability theory, and considers a set of random edges placed between the nodes of a graph [53, 54]. They proposed a model for homogenous networks where nodes are connected with the probability p. Random graphs were the only model to deal with network systems for a long time.

The last two decades, however, witnessed tremendous progress in uncovering generic properties of different kinds of complex networks. It was discovered that many real-world networks have some common properties, such as small-world effect or scale-free degree distribution. Social networks and power grids have small-world property where any two nodes are connected through a path of a rather small length, that scales logarithmically with the network size [55]. Watts and Strogatz investigated this feature in their seminal Nature article [56]. They proposed a model for networks with this feature which starts from a lattice, and then at each step, a link is rewired with a probability p. Thus, it covers networks from a completely regular to a completely random topology as p varies. For some values of the rewiring probability, the produced networks have both small-world property and high clustering coefficient, two properties that are observed simultaneously in real systems.

Although networks with Watts-Strogatz (WS) topology are often more realistic than the Erdős-Rényi (ER) random model, both of them show almost the same degree distribution [54]. This means that many of the nodes have almost the same number of connections, a feature observed in *homogenous networks*. However, many real networks, such as the World Wide Web and the Internet, do not follow such a degree distribution. To address these heterogeneous networks, Barabasi and Albert proposed a model resulting in networks with power-law degree distribution which are often called Scale-Free (SF) networks [57]. In these networks, nodes with higher degrees have more chance to receive connections from newly added nodes than those with lower degrees. The following algorithm is proposed in [58, 59] to generate SF networks. Starting with a fully connected graph of small size, at each step, a new node is added to the network and creates m links with the already existing nodes. The probability of creating an edge between the newly added nodes and an existing node i is $(d_i+B)/\sum_j(d_j+B)$, where d_i is the degree of node i and B is a constant controlling the heterogeneity of the network; as B increases, heterogeneity of the network decreases [58, 59].

Graph-theoretic tools, developed in the context of complex networks, have been applied to study different phenomena in power grids [25]. These research activities have mainly studied topological properties, such as degree distribution and efficiency, of a power grid to identify whether it shows WS, SF, or ER behaviours [24, 60]. A review on the topological properties of the American and the European high-voltage networks (the whole or parts of them) as well as the Chinese, South Korean, and Indian ones revealed that their degree distributions tend to be exponential with some minor exemptions [61-63]. Although they might be considered as power-law at first sight, many of these power networks show features of the small-world networks. For example, clustering coefficients and average shortest paths of these networks are significantly larger than ER and SF networks [41]. These research works concluded that power grids are generally resilient to random breakdowns because of their small-world feature, while they are extremely vulnerable against targeted attacks [61]. A similar study showed that the Iranian high-voltage power grid is a small-world network with a relatively poor performance against cascaded failures [64]. There exists a notable correlation between the degree distribution of the European electricity transmission system and its reliability [65]. The fragility of the European high-voltage network depends only on its size, where it increases logarithmically with the size of the network [66]. The topology of a power grid also impacts failure propagation. For example, the propagation failure rate decreases in sparse networks [67]. Evolutionary algorithms can be applied to design a power grid topology with maximum robustness to suppress cascading failure propagation [68]. It has also been shown that networks with a high average clustering coefficient together with a large size are highly sensitive to dispatch scenarios [69]. Table I summarizes some of these achievements.

TABLE I: MODELLING OF DIFFERENT REAL-WORLD POWER GRIDS

REF.	NETWORK	RESULT
[61, 62]	The American, European, Chinese and Indian high-voltage networks	These networks show small-world features. They are generally resilient to random breakdowns, but extremely vulnerable against targeted attacks.
[65]	European transmission system	There is a notable correlation between degree distribution and reliability of the network.
[64]	Iranian high-voltage power grid	This grid is a small-world network with a relatively poor performance against cascading failures.
[66]	European high-voltage network	Fragility increases logarithmically with the size of the network and is not related to other topological measures.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

Power grids as multi-agent systems: The concept of Multi-Agent Systems (MAS) provides another abstraction of large-scale systems in the context of 'systems engineering' [70]. Although CN and MAS were originated in physics and engineering disciplines, respectively, they address almost similar problems and can be viewed from a unified approach [71]. With the paradigm shift from centralised power generation to Distributed Energy Resources (DERs) as well as advancements in communication technologies, power grid modelling and analysis using MAS-based approaches is of high interest within the power system community [72-74]. Conventionally, monitoring and control of power grids were implemented over centralised Supervisory Control and Data Acquisition (SCADA) systems [75]. Based on MAS strategy, different monitoring, protection and control requirements can be distributed among power units and can be managed in a fast and intelligent way [76, 77]. Agents can perform different algorithms collaboratively, such as load-shedding [78], protection [79], voltage and frequency control [80-82], energy sharing and trading [83, 84], electric vehicle management in distribution grids [85], fault and attack tolerant mechanisms [86, 87], optimisation [88], resource allocation and scheduling [89], and power system restoration [90, 91]. This makes MAS a strong tool for the analysis and control of micro and smart grids [92].

The MAS approach has been heavily studied in different engineering disciplines, including computer and control engineering, and has a solid mathematical background that supports its applications in power grids [93]. Unlike CN-based approaches, which are mainly designed to manipulate large-scale grids by focusing mainly on the topology, the focus of MAS-based approaches is on dynamical behaviours of small-scale power grids. Therefore, there is still a gap in modelling large-scale dynamical power grids for analysis and control purposes, especially in the presence of renewable resources, which indeed requires combining MAS- and CN-based approaches [94].

C. POWER GRIDS AS CYBER-PHYSICAL SYSTEMS

In recent decades, the capabilities of power grids are expanded by integrating communication, computation and control technologies, resulting in so-called smart grids. Although promising to deliver reliable power to loads, they are technically complicated Cyber-Physical Systems (CPS) [95]. In a CPS, a physical system, such as a power network, is monitored and controlled using processing modules and control loops in the cyber layer [96]. CPS is a structurally multi-layer system. For example, [96] proposes a three-layer model by augmenting 'information' and 'user' layers to the 'physical' one. A two-layer model for power grids, including physical and cyber layers and considering linearized swing equations and DC power flow, is proposed in [97] as,

$$E\dot{\boldsymbol{x}}(t) = \bar{L}\boldsymbol{x}(t) + P(t)$$
$$\boldsymbol{x} = \begin{bmatrix} \boldsymbol{\delta} \\ \boldsymbol{f} \\ \boldsymbol{\phi} \end{bmatrix}, E = \begin{bmatrix} I & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & 0 \end{bmatrix}, \bar{L} = -\begin{bmatrix} 0 & -I & 0 \\ L_g & D & L_{gc} \\ L_{cg} & 0 & L_c \end{bmatrix} \quad (2)$$

The state vector $\boldsymbol{x}$ includes the rotor angles $\boldsymbol{\delta}$ and frequencies $\boldsymbol{f}$ for n generation busses, and voltage angles $\boldsymbol{\phi}$ for all loads. $P(t)$ is the real power demand. $\bar{L}$ is an augmented Laplacian matrix and includes the Laplacian of the network among generators L_g, among loads L_c, and interaction between them L_{gc} and L_{cg}. Diagonal matrices M and D include generator inertia and damping coefficients, respectively. In addition to this model, which is useful for the analysis and design of control strategies, different frameworks for assessing features of a CPS have been proposed, see e.g. [98] for security.

A comprehensive CPS framework for power grids is proposed in Fig. 1. This model contains generation units and loads connected over physical and cyber links. It has been widely used in the design and optimisation of the distributed control algorithms in power grids [99-101]. Physical cables, that connect generators to loads, form the physical layer. Each physical load or generator has a corresponding cyber node. These nodes can communicate with each other or with a control centre to implement different algorithms for distributed control [102], optimisation [101], fault/attack detection [103], and attack tolerance [99].

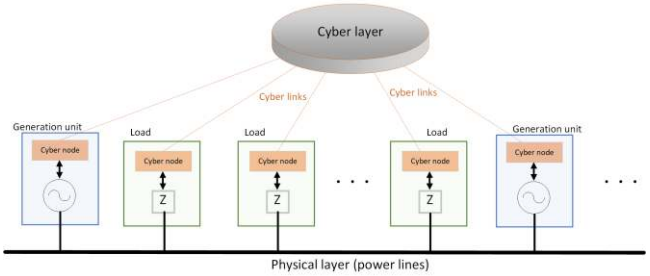

Figure 1. A CPS model framework for modelling power grids.

Cyber-physical interactions result in complicated scenarios in the reliability analysis of power grids. There have been several research activities to model these interactions. For example, different mathematical tools such as Petri Nets [104-106], stochastic graphs [107], and complex networks [108, 109] have been used to extract the interaction model. In this context, power grids are also hybrid systems containing a mixture of continuous and discrete-time events [110]. Continuous-time dynamics, represented by frequency, current and voltage, describe the physical processes of this hybrid system. The discrete event dynamics include those cyber components for monitoring, analysis and control [110]. Hybrid system theory [111] is an approach to the analysis and design of these systems and has been applied to power grids. For example, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

reachability analysis of a hybrid system in the presence of constraints is applied to study the stability of a power grid [110]. A hybrid automaton model is also used to design a supervisory control system for microgrids [112].

The appearance of the network topology, in the form of Laplacian matrices, in the state-space equation (2) sparks the brain to hire complex networks tools for analysis and control problems. Indeed, state-space approaches to study these problems in modern large-scale power grids suffer from dimensional issues and computational complexity. Techniques inspired by the graph theory, such as the one proposed in [35] to identify the frequency control leader unit, can bring innovative and computationally efficient solutions to this problem.

Modelling of blackouts and cascading failures: Blackout prevention is an important strategy in improving the reliability of power grids [113]. Several research studies have been conducted in both academia and industry on how the blackout risk, especially through cascading events, can be reduced [114]. For example, a study on the blackout in Italy, that happened in 2003, shows that while a significant number of nodes should be randomly failed to cause a breakdown in an isolated network, interdependent networks are generally highly sensitive to these failures [115, 116]. A precise model which includes the dynamical behaviour of cascading failures can facilitate these studies [114]. Research studies on the propagation of cascading failures can be performed using dynamical transient complex network model proposed in [117], or network-based stochastic models [118, 119]. A stochastic cascading failure model based on the MAS approach is proposed in [120] considering interdependencies between physical and cyber networks. In addition to model-based approaches, data-driven machine learning techniques have been also applied to study cascading failures [121, 122].

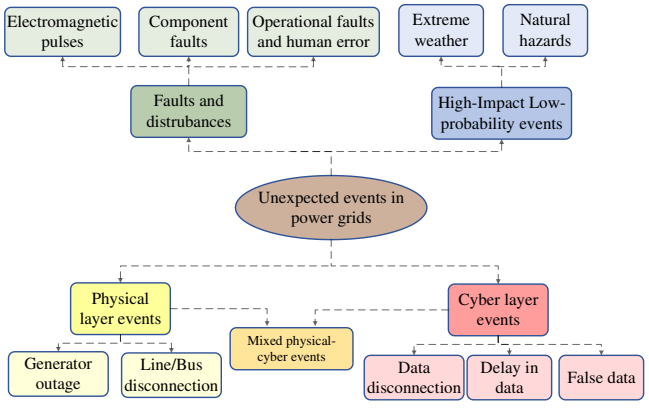

Figure 2. Unexpected events in a power grid

III. RELIABILITY AND RESILIENCE ANALYSIS OF POWER GRIDS

Resilience and reliability are two interconnected subjects, but with different meanings, in the context of power grids. IEEE 1366 standard defines reliability from a demand-side perspective: A reliable power grid can deliver enough power with high quality to consumers with minimum interruption [128]. The standard introduces the 'System Average Interruption Frequency Index (SAIFI)' which quantifies the number of interruptions, and 'System Average Interruption Duration Index (SAIDI)' for measuring the duration of interruption for consumers. On contrary, the main concern of resilience study is how rapidly the power grid can recover after a disruptive event [129]. Indeed, a power grid may meet all reliability standards while it is not resilient to major events [130].

A. RELIABILITY OF POWER GRIDS

In the reliability analysis of power grids, different types of events may be considered in physical and cyber layers (see Fig. 2). Physical power networks are naturally subject to line faults, generator/load outages, and sometimes electromagnetic pulse disturbances [131-133]. Communication in the cyber layer may be impacted by variable delay or packet dropouts during normal operation or after attacks [134-136]. In this section, the impacts of these events on the reliability of power grids are surveyed.

Operational reliability: Although several automation technologies have been augmented to power grids for effective monitoring and control purposes, reliability of power grids is still sensitive to operators' decisions [137]. Events like what happened in Southwest US in 2011 [138] clearly shows the contribution of operators' actions in a blackout. Human reliability is also important in a high-quality maintenance [139]. To embed the operators' behaviours into models of cascaded failures, a probabilistic approach based on Markov chains has been proposed in [140]. [141] studied the impact of frequency of inspections of the system components on the reliability of power grid, and suggested one inspection per year as optimal using a mathematical modelling.

Appropriate grid segmentation is also important to help operators to quickly identify possible risks and act accordingly, thus increasing reliability of the grid. To this end, Wide Area Monitoring Systems (WAMP), mainly based on Phasor Measurement Units (PMU), have been extensively studied to increase controllability and stability of the grid [142]. Intermittence and uncertainty of renewable resources have encouraged researchers to apply data-driven approaches, such as those based on machine learning, for segmentation [143, 144]. For example, load pattern segmentation can be performed in residential power grids using clustering techniques [145]. Besides, appropriate segmentation of AC system through DC links in HVDC grids can reduce the risk of blackout [146], and improve the performance of the whole system [147].

Cyber issues and attacks: Rapid penetration of new technologies, such as renewable generation and AMI, in the grid has made the power grids very dynamic. Reliable operation of such as dynamic system needs continuous adjustments based on real-time data, which indeed results in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

a complicated real-time cyber layer [148]. A vulnerable communication system may cause abnormal operation of power grids, and even cascading failure [149, 150]. Therefore, advanced data routing and switching algorithms are required for a reliable operation [151]. Attacks against intelligent protection devices, which is normally performed through the SCADA systems, can also severely disrupt the operation of power grid [107, 152].

In addition to individual components and services, interconnections between physical and cyber layers make reliability analysis of power grids complicated since failure or attack in one of the layers affects other layers as well [153-155]. Different types of threats in physical and cyber networks can be defined, including cyber-physical, cyber-cyber, physical-cyber, and physical-physical [156]. The origin of a cyber-physical threat may be in the cyber network, which may then impacts the characteristics of the physical network as well. These threats require various prevention and mitigation approaches [156]. For instance, a communication failure led to a serious impact on the Hydro-Quebec power grid in 1988 [157]. A mixed physical/cyber attack on the Ukrainian power grid in 2015 [158] revealed that any combination of physical and cyber components should be considered in the reliability analysis of a power grid. Li et al. [159] proposed a bilevel model for the case that physical line disconnections are accompanied by a false data injection in the cyber layer. The reliability of power grids against mixed physical and cyber attacks and failures still needs further research.

Reliability in distribution grids: Commitment to mitigate greenhouse emission has not only pushed the power generation environment towards renewable energy resources, but has also impacted the demand side by introducing new intermittent and unpredictable electrical consumers such as Electric Vehicles (EV). Lack of coordination of these new technologies can significantly weaken the reliability of distribution grid by overloading distribution transformers [160] or reducing the quality of voltage regulation [161]. With the massive increase in Photovoltaic (PV) and energy storage batteries in distribution grids, new local technologies, such as demand-response [162, 163], load shifting [164] and coordination strategies [165], have emerged to improve the reliability. These technologies are well supported by real time data over the AMI. In addition, demand-side ancillary services for voltage and frequency regulations are under development [166-168]. Besides supply-load balancing, a reliable distribution grid requires advanced data-driven algorithms for detection of anomalies and illegal consumers [169, 170].

B. RESILIENCE OF POWER GRIDS

The resilience of an infrastructure can be assessed using the "resilience triangle" [171]. Figure 4(a) shows the loss of functionality caused by any events, as well as the restoration pattern. Resilience-enhancing algorithms aim to reduce the size of this triangle, see e.g. [172] and [173]. This approach is enhanced to a so-called "resilience trapezoid" [47], which considers the disturbance progress period after the event happens as well as the post-event degradation period before restoration (Fig. 4(b)). In this context, *operational* and *infrastructure* resilience are defined in a power grid. Operational resilience shows how secure the power can be delivered to loads, while infrastructure resilience refers to the success of the power grid to mitigate failure or collapse in its components [47]. For example, Fig. 4(b) shows that both operational and infrastructure resilience is 100% before the event time t_{oe}, meaning that all demand is successfully supplied and there is no non-functional component in the power grid. In the case of an event at t_{oe}, the resilience of the power grid drops to R_{pdo} (for operational resilience) and R_{pdi} (for infrastructure resilience). Recovery of the operational resilience normally happens earlier than the infrastructure one, as shown in Fig. 4(b). Based on the resilience trapezoid, different time-dependent metrics for operational and infrastructure resilience can be defined. For example, $\Phi = (R_{pdo} - R_{0o})/(t_{ee} - t_{oe})$ shows the slope of resilience degradation, and $\Lambda = R_{pdo} - R_{0o}$ shows the resilience degradation level during Phase I of Fig. 4(b) [47].

Restoration of power grids: Both resilience triangle and trapezoid methods show that a quicker restoration process results in a more resilient system. The idea of restoration of power grids has recently attracted a lot of interests among researchers. A power grid maybe restored from the negative impact of faults [174] or attacks [175], or after a blackout using black-start strategies [176]. A successful power system restoration may require an optimal start-up sequence, reconfiguration of the transmission network [177] or appropriate distribution network strategies [178]. In the presence of uncertain renewable energy resources in the generation side and uncertain and almost uncontrollable generation/demand caused by DERs, advanced restoration strategies for future power grids are required [178, 179]. In this context, new restoration approaches have been proposed including agent-based and learning-based [180-182], and probability-based ones [183].

Extreme weather events: Increasing the frequency of extreme weather events, such as floods, high temperature and wildfires, as well as sudden failures and intentional attacks in recent years has made the resilience study of power grids a hot research topic [26, 45, 184-186]. A model of the impact of these events on the performance of a power grid is a crucial part of such studies. For the case of extreme weather, the comprehensive modelling framework of Fig. 3 has been proposed [187]. It includes models of the weather, components, and the whole power grid in obtaining desired resilience indices, such as expected but not served energy and loss of load probability [188]. Using this framework, [184] proposed a fragility model for components of the grid, such as towers and lines, and augmented them to achieve a model for the whole transmission system. The

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

model describes the probability of failure in a component considering the intensity of a hazard, e.g. probability of getting a tower broken conditional to the wind speed. These probability curves can be derived from local long-term statistical analysis. This framework can help to make the power grids proactively resilient against high-impact low-probability extreme weather events [189, 190]. It can also help to optimise capital investments in resilient power networks [191, 192]. Among different approaches that make the power grids robust against unexpected events, the performance of microgrids is promising, especially when they are networked [189, 193-196]. They can reduce the undesired effects of these events or facilitate the restoration of power supply to critical loads after events if they are optimally located to support fragile points [197-199].

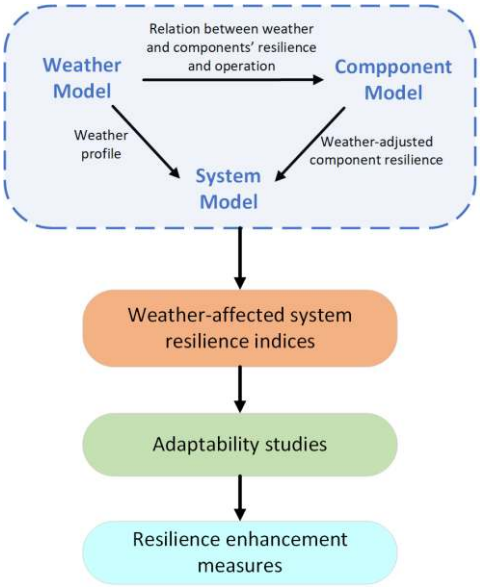

Figure 3. A comprehensive modelling framework to study the impact of extreme weather on the resilience of power grids [187].

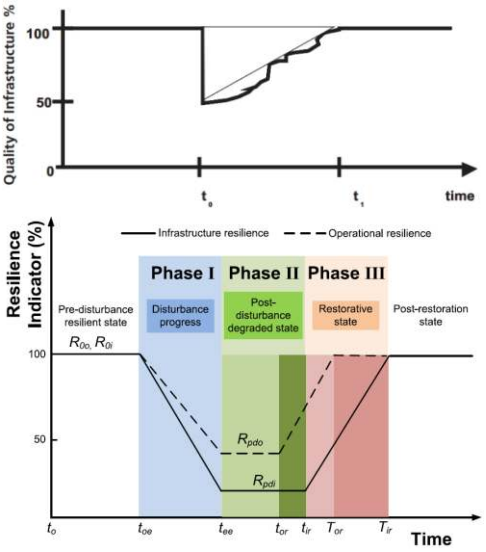

Fig. 4. (a) The resilience triangle [171], (b) the resilience trapezoid [47].

In addition to these model-based approaches, data-driven techniques based on Artificial Intelligence (AI) methods have shown a strong capability in studying large datasets, which are gathered in monitoring systems, and evaluating the resilience of a power grid [200, 201]. Machine learning, one of the popular AI-based techniques in power grid studies, has been applied to predict power outages [202, 203], vulnerable points [204, 205], and power outage duration [206]. AI-based techniques can be also used as a decision-making engine in the post-event control and restoration of the system [207-209]. The application of AI-based techniques in resilience studies in power transmission and distribution systems is a field of future research activities.

IV. MEASURES FOR RESILIENCE AND RELIABILITY OF POWER GRIDS

Resilience and reliability assessments have been among major topics in engineering [188] and non-engineering disciplines such as ecology [210]. Appropriate metrics have been introduced to measure these features in a system. For example, [211] proposes an availability-based metric to measure resilience of an engineering system based on the system design and maintenance resources. The code-based metric, proposed in [212], receives the current state of a power distribution grid as well as other information such as weather, and quantify the system capability to supply critical loads. One strategy in increasing resilience and reliability of a power grid is to first identify weak points. To this end, suitable metrics to identify vulnerable point of the grid are required. In this context, two main sets of measures have been developed: "Flow-based measures" which are based on the load-flow study of the grid, and "Centrality-based measures" which are inspired from the centrality concept in complex networks. These two sets are reviewed in this section.

A. FLOW BASED MEASURES

In addition to the study of the resilience of the whole power grid, identifying vulnerable busses and power lines is of high interest for both network operators and attackers. Approaches based on "load-flow study" and "complex networks" have been developed to answer this question and are reviewed in the section.

The load-flow analysis is an important approach in studying power grids. It includes calculating node voltages and branch power flow in a specific operational condition. Mathematically, this problem solves a system of nonlinear algebraic equations of active and reactive power balances at each operating point [213]. More precisely, the objective of the load-flow study in a power grid is to calculate voltage magnitude V_i and angle δ_i of each bus i, knowing the amount of injected active and reactive powers (P_i and Q_i, respectively). The relationship between these parameters of a power grid is generally nonlinear,

$$\begin{aligned} P_i &= f_i(\boldsymbol{V}, \boldsymbol{\delta}) \\ Q_i &= h_i(\boldsymbol{V}, \boldsymbol{\delta}) \end{aligned}, \tag{3}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

where, $\boldsymbol{V} = [V_1, V_2, \ldots V_n]$ and $\boldsymbol{\delta} = [\delta_1, \delta_2, \ldots, \delta_n]$ include voltage magnitudes and angles of all busses, respectively. It means that a system of nonlinear algebraic equations may need to be solved at each time step or in the case of any changes in generation, consumption, or network topology because of failures. Therefore, this study is computationally expensive, especially when large-scale power grids are studied in the presence of uncertain and unpredictable renewable generation units. To reduce the complexity, a DC load flow study is proposed which is a non-iterative approach focusing only on calculating the active power flow [214, 215]. It simplifies calculations by assuming identical 1 p.u. voltage at all nodes and neglecting the resistance of the transmission lines.

Both AC and DC power-flow analyses have been applied to the study of cascading failure and blackout caused by unexpected events. An intuitive estimation of the impact of line $l = (i,j)$ on a power grid can be derived using a flow-based approach. If F_l is the power flow through the line l in the normal operation, then

$$V(l) = \frac{F_l}{\max\{F_l\}} \tag{4}$$

can rank all links. The line margin metric [216] augments the line capacity (thermal rating) C_l to define a margin for the line l as,

$$M(l) = \frac{C_l - |F_l|}{C_l} \tag{5}$$

It indicates how much the power flow through line l is close to its maximum capacity. Therefore, lines with smaller margins would be more vulnerable than others [216]. The Oak Ridge–PSERC–Alaska (OPA) model proposed in [217] uses DC load-flow to study cascaded failures while [218] applies AC load-flow to the same problem. To include realistic uncertainties, such as variations in load demand, a stochastic (probabilistic) load-flow study [219, 220] is also considered. For example, [221] develops probability distribution functions for bus voltages and power transmissions over lines to assess how they violate limits. This assessment is done more quantitively in [222]. The main drawback of the flow-based metrics is that they need computationally complex load-flow studies.

Maximum flow method: The maximum flow problem is about finding the maximum amount of flow between two desired nodes, called 'source' and 'sink', of a network [223]. This approach is inspired from the traditional maximum-flow minimum-cut problem in the network community. In a directed graph G, where each link l has the flow F_l and the capacity C_l, the Ford-Fulkerson theorem [224] states that the maximum flow is equal to the sum of the flows across the "minimum-cut" links. This problem can be solved using the following algorithm [225].

1. Reset the flow of all links in the augmenting path set, i.e. $F_l = 0$. An augmenting path is an acyclic path between source and sink which links satisfy $F_l < C_l$.
2. Set residual $r = \infty$ for all links mentioned in item 1.
3. For each link l in an augmenting path, set $r = \min(r,(C_l-F_l))$.
4. Update the flow of edge $F_l = F_l + r$.
5. Repeat items 3 and 4 until no augmenting path remains.

Max-flow Min-cut theorem has been applied to the vulnerability analysis of power grids [225, 226]. The maximum power flow F in a power grid should be calculated subject to the following restrictions [226].

$$\begin{aligned} &0 \le f_{uv} \le C_{uv} \\ &\sum_{k \in L_u^o} f_{uk} = \sum_{s \in L_u^i} f_{su} \\ &|F| = \sum_{\substack{g \in S \\ j \in N_g}} f_{gj} = \sum_{\substack{d \in D \\ k \in N_d}} f_{kd} \end{aligned} \tag{6}$$

The links adjacent to node u are defined as L_u^i (L_u^o), based on whether the power flow is coming into (going out of) this node, and F represents the network power flow. S and D are the sets of generators and loads, respectively. The first equation guarantees that the flow over power lines between any pair of nodes (u,v) is in the admissible range, the second equation shows the inflow and outflow of each node u are equal, and the third equation represents that the network flow is equal to the flow injected by generation units, which is indeed the flow consumed by loads. In addition to these equations, two more constraints should be considered to make the results realistic [227]. First, capacity limitation only on the links is not enough since generators have also practical constraints in the power they can supply. Second, multiple maximum flows between all possible source-sink pairs should be considered simultaneously since a specific load is not necessarily fed from only a specific generator in a power network. In addition to conventional techniques, such as linear programming, this optimisation problem is solved using a modified maximum flow algorithm [227]. Both of these methods benefit from the following normalised maximum flow centrality index for the link l [228]:

$$F_l = \frac{\sum_{u \in S} \sum_{v \in D} f_{uv}^l}{\sum_{u \in S} \sum_{v \in D} \bar{f}_{uv}} \tag{7}$$

in which, $\bar{f}_{uv}$ shows the maximum flow from a source node u to a sink node j, and f_{uv}^l is the portion of the power flow between nodes u and v which passes through the link l.

Study of the blackout size: The importance of a node or link can be defined as the size of the blackout that may happen if that node or link fails [229]. The network assessment algorithm starts by removing a generation node randomly or based on a feature such as degree of the node. A DC load-flow study is used to re-calculate the network flow. It is supposed that each line is equipped with a protective

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

relay that trips the line if its load exceeds 50% of its capacity for 5 seconds. If such a cut happens, the DC load-flow study is repeated. It is also supposed that generation units can compensate up to 10% of their adjusted output to achieve generation/consumption balance in the grid. The process continues until when a balance between generation and loads happens and flows on lines are all in their admissible capacity. Finally, the blackout size Δ_i caused by a failure in node i is defined [229]:

$$\Delta_i = 1 - \frac{\sum P'_d(i)}{\sum P_d} \tag{8}$$

where P_d and $P'_d(i)$ represent consumption loads before and after the generator failure, respectively. Clearly, large values of Δ_i show that failure of node i results in a severe outage in loads, i.e. i is a vulnerable node.

Comparing with pure topological metrics, [229] concludes that evaluating vulnerability using these metrics may be misleading since their results show only a mild correlation with the achieved blackout size. A similar study has been reported in [230] where the percentage of noncritical links is introduced as a metric for network vulnerability. The percentage of unserved nodes $P^u(l)$ is calculated for the case of failure in link l. If it is less than a specific threshold, then the link is tagged as noncritical:

$$\delta(l) = \begin{cases} 1; & P^u(l) < threshold \\ 0; & otherwise \end{cases} \tag{9}$$

Finally, the percentage of noncritical links P_n of the network is calculated as:

$$P_n = \frac{1}{m} \sum_{l \in E} \delta(l) \tag{10}$$

Therefore, a power grid with a large P_n is robust against link failures. Interestingly, [230] concludes that the average shortest path and the loads' accessibility to generators are two parameters that significantly affect the robustness of a power grid. To quantify the accessibility of a load to generators, the resistive distance between node i and its nearest generation is considered as

$$d(i) = \min(R_{is}); \quad s \in S \tag{11}$$

where R_{is} is the resistance between the node i and the generator s. If the number of generation units in a network is high enough and they are evenly distributed, the load imposed on transmission lines is reduced and the network will be robust [230]. Therefore, the average effective resistance to the nearest generator, calculated for all loads, is defined as the vulnerability metric

$$\beta = \frac{1}{N - N_S} \sum_{i \in N \setminus S} d(i) \tag{12}$$

The smaller the β is, the more robust the network will be [230].

B. COMPLEX NETWORK BASED MEASURES

Traditional models of power grids mainly consider structural features of power grids. That means elements of the adjacency matrix are a_{ij} = 1 if there is a cable connecting substation i to j, otherwise a_{ij} = 0. To study vulnerability, a subset of nodes or links of the graph is removed selectively or randomly. Then, the variation of a topological feature of the graph is assessed, such as diameter or the size of the largest connected component [66, 231], network disintegration [232], the efficiency of the network [233], and decrease of the average number of generation substations connected to nodes, called connectivity loss [234]. These studies clearly show how failure in a subset of nodes or links impacts power grid stability and performance. However, a more accurate study of the power grid requires a dynamical complex network model that considers *i*) dynamics of loads/generators connected to substations, *ii*) evolution of the failure effect in the network [235]. The first research activities on the vulnerability of power systems assumed that electricity flow between substations i and j mainly happens through the shortest path d_{ij} between them. This was a motivation to apply the betweenness centrality metric in power grids [236]. It also attracted attention to the *efficiency* of a network as a vulnerability criterion. Efficiency is traditionally defined as how well a network exchanges data and is strongly related to topological properties [237]. The efficiency of a network G is measured based on the shortest path d_{ij} between any two nodes i and j, as

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{13}$$

Indeed, efficiency is an extension of the average shortest path measure to account for unconnected nodes [238]. The relationship between efficiency and vulnerability of power grids is reported in [239, 240]. Later studies show that efficiency is not still an accurate metric to study power networks because power flow between two nodes does not necessarily happen through the shortest path. It is extended to electrical power systems in different ways. For example, [241] introduced a 'directed global efficiency' by augmenting physical network and fault features into the model. To augment the dynamical behaviour of the power grid into efficiency analysis, the 'load' L_k of the k^{th} node is defined as the number of shortest paths passing through it [242]. Therefore, the load of all nodes in the network may change if a node fails. This may cause nodes to become even overloaded if a practical maximum capacity is considered. A similar load redistribution approach has been applied to the robustness analysis of the Western US grid [243]. Algorithm 1 shows how this dynamic modelling works in identifying vulnerable nodes [240]. Based on this algorithm, an evolutionary technique is proposed to create resilient networks against cascading failure [244]. This

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

algorithm can be empowered by embedding a DC power flow model into it [245]. An algorithm similar to Algorithm 1 has been proposed to identify vulnerable nodes of a power grid using dynamic power flow studies [246]. Modified versions of efficiency for power network applications are reviewed in the next section.

Another approach in the study of resilience and reliability of large network systems, including power grids, emerges from the centrality concept in complex networks. "Central (or vital)" nodes or links of a complex network are those with the highest influence on a specific behaviour. Several centrality metrics have been introduced to identify influential components of a network [39, 247, 248]. In the next section, some of these centrality measures, which show promising performances or have been customised for power grids, are reviewed.

ALGORITHM 1. IDENTIFYING VULNERABLE NODES USING NETWORK EFFICIENCY

Initialisation.
Calculate the load $L_k(0)$ for all nodes, i.e. $k = 1, 2, \ldots, N$.
Define a capacity $C_k = \alpha L_k(0)$ for each node k choosing $0 < \alpha \leq 1$.
For all nodes $i = 1, 2, \ldots, N$
  Remove node i.
  For all remaining nodes
    Calculate the load L_k for all nodes, i.e. $k = 1, 2, \ldots, N$.
    For all nodes, if $L_k > C_k$ then multiply weights of its adjacent links by L_k/C_k.
  End
  Calculate network efficiency E_i using Eq. (13).
  Reset the network to the original version.
End
Output
The most vulnerable node = $\underset{i}{\operatorname{argmin}}\, E_i$

C. CENTRALITY-BASED MEASURES

The topology of a power grid has an evident impact on its robustness [66, 249]. In the context of complex networks, topology-based centrality metrics can be used to study how networks are resilient when failures happen in the central nodes. Among them, Degree Centrality (DC), Betweenness Centrality (BC), Closeness centrality (CC), and Eigenvector Centrality (EC) are popular. DC considers hubs, i.e. nodes with the highest degrees, as central nodes. The BC of each node (link) of the network is the number of shortest paths that pass through that. The CC measures how close a node is to the other nodes of the network. Closeness C_i of node i of a network is defined as the inverse of the average length of the shortest path between node i and all other nodes in the network. It is computed as

$$C_i = \frac{N-1}{\sum_{i,j \in V} d_{ij}} \tag{14}$$

EC defines node centrality based on the importance of its neighbours [250]. The EC of node i of a network is shown by $e_i > 0$ and is proportional to the sum of ECs of its neighbours. More precisely, the ECs of nodes of a network are defined as the elements of the eigenvector of the adjacency matrix associated with its dominant eigenvalue. EC is interestingly related to some dynamical behaviours of networks [251]. The concept of DC is also expanded into power system vulnerability studies using a so-called 'pseudo degree' [252].

Complex Dynamical Networks (CDNs) are a class of complex networks whose nodes have internal dynamics. Many large-scale real-world systems can be modelled as CDN, such as social networks [253] and power grids [1]. In addition to the aforementioned centrality measures, which sometimes do not work well in CDNs [40], Spectral Centrality (SC) metrics have been introduced using eigen-decomposition of the original or a modified version of the adjacency or Laplacian matrices of the network. It is shown that the spectrum of these matrices has a significant impact on collective behaviours in CDNs [38, 254-256]. For example, the variation of frequency in a distributed generation system is a function of the spectrum of its graph [109, 257]. Network spectrum is also important in the control of a CDN [101, 254, 258].

Research studies have shown that pure topological metrics, such as global efficiency, degree and betweenness centrality, may fail to capture the physical properties and operational constraints of power grids and needs to be customised [17, 132, 241, 259, 260]. Therefore, centrality measures should be extended to power grid applications. To get the benefits of the well-developed centrality concept, researchers have been focused on extending these measures to power grids. In this section, CN-inspired centrality metrics which are customised for power grid applications are reviewed. Considering correlations between some of these measures, such as average shortest path and efficiency [261, 262], the independent metrics are addressed here.

LINE CENTRALITY MEASURES

Vulnerable power lines, i.e. those with the maximum impact on the power grid performance if failed, can be considered as central links on CN model. Therefore, edge centrality measures are suitable for this study [263]. In the following, we provide a review of a number of edge centrality metrics in the context of power grids.

Geodesic link vulnerability: In power grids, since the power flow is always from generator nodes to loads, a modified version of efficiency, called source–demand efficiency E_{SD}, has been proposed [261]:

$$E_{SD}(PG) = \frac{1}{N(N-1)} \sum_{i \in S, j \in D} \frac{1}{d_{ij}} \tag{15}$$

where S and D are sets of supply and demand nodes in the power grid PG, respectively. Based on E_{SD}, the geodesic vulnerability G_l of the power line l is defined as the drop in efficiency when the link l fails [235].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

$$G_l = 1 - \frac{\sum_{i \neq j} \frac{1}{d_{ij}^l}}{\sum_{i \neq j} \frac{1}{d_{ij}}} \quad (16)$$

G_l takes large values when the network is not resilient against the failure of line l.

Net-ability: Applying the efficiency metric defined in Eq. (15) to the vulnerability study of power grids is problematic since electric current does not only flow through a specific path, like the shortest path [17]. Transmission capabilities between any pair of generators and loads should also be considered when studying flow-based networks like power grids. Net-ability is a metric inspired by efficiency to consider these operational constraints [17]. The weight w^l_{ij} of the link l in path k between generator i and load j shows the difficulty of the power transfer through that link. This weight is defined by:

$$w_{ij}^l = \sum_{l \in k} f_{ij}^l Z_l \quad (17)$$

Z_l shows the impedance of line l and the Power Transmission Distribution Factor (PTDF) of line l in path k is shown by f_{ij}^l. Elements of the PTDF matrix F = $[f_{ij}]$ express the change in the power over the line l caused by a unit change of power injection at bus j. Therefore, $f_{ij}^l = f_{li} - f_{lj}$ reflects the sensitivity of power flow in the line (i,j) to injection at bus i and delivery at bus j. The net-ability of the power grid is defined as [17],

$$\eta = \frac{1}{N_S N_D} \sum_{i \in S} \sum_{j \in D} C_{ij} \sum_{k \in H_{ij}} p_{ij}^k \frac{1}{w_{ij}^k} \quad (18)$$

where S and D are sets of N_S generators and N_D loads, respectively. H_{ij} is the set of paths from generator i to load j where each path has a power transmission capacity C_{ij}, and p^k_{ij} is the power share of path k in power transfer from node i to j. In the DC load flow study, $w^k_{ij} = Z_{ij}$, which simplifies Eq. (18) to

$$\eta = \frac{1}{N_S N_D} \sum_{i \in S} \sum_{j \in D} \frac{C_{ij}}{Z_{ij}} \quad (19)$$

Therefore, the vulnerability of line l of a grid can be defined as the drop of net-ability of the grid when the line is failed and removed from the grid:

$$V(l) = \frac{\eta - \eta_l}{\eta} \quad (20)$$

Close to PTDF, the concept of "line correlation" is introduced in [264] and applied to identify vulnerable transmission lines. Two transmission lines are called 'correlated' if the failure of one of them results in the change of power flow in another one.

Edge betweenness: The betweenness centrality measure is also defined based on the shortest path concept. It was introduced by Linton Freeman as a measure to quantify the control of a person on the communication between other people in a social network [265]. The edge betweenness centrality for the link l of the network is defined as:

$$B(l) = \sum_{k,j \in V} \frac{d_{kj}^l}{d_{kj}} \quad (21)$$

where d^l_{kj} shows the number of shortest paths between nodes k and j which passes through the link l. Although this is a pure topological and computationally expensive metric, it is still of interest in error and attack tolerance analysis of power grids [229, 266-268].

Electrical edge betweenness: The electrical betweenness of line l has been proposed to compensate for the lack of electrical information in the original edge betweenness centrality [267]. It is defined as

$$B_l = \sum_{i \in S} \sum_{j \in D} w_{ij} \left| I_{ij}^l \right| \quad (22)$$

where I^l_{ij} is the current of line l when a unit current is injected in generator bus i to be delivered to load j. That is,

$$I_{ij}^l = Y_l (V_i - V_j) \quad (23)$$

where Y_l shows the admittance of line l, and V_i and V_j are voltages at generation and load buses, respectively. We have $w_{ij} = \min\{S_i, D_j\}$ where S_i is the capacity of generator i and D_j is the maximum load at bus j. The electrical betweenness of line l can be transformed to,

$$B_l = \max\{B_l^p, \left| B_l^n \right|\} \quad (24)$$

using the PTDF concept, where B_l^p is calculated as

$$B_l^p = \sum_{i \in G} \sum_{j \in D} C_{ij} f_{ij}^l \quad (25)$$

and is the positive electrical betweennesses of line l, i.e. for links with $f^l_{ij} > 0$. Those link with $f^l_{ij} < 0$ results in B_l^n, the negative electrical betweenness, which is calculated using the same equation as (25). It is worth noting that $f^l_{ij} > 0$ ($f^l_{ij} < 0$) means that injecting power at bus i, which should be delivered to bus j, increases (decreases) the electrical flow of line l. Finally, Eq. (24) picks the one with the maximum absolute value as the electrical betweenness centrality of the link l.

BUS CENTRALITY MEASURES

Node centrality metrics in the study of complex networks can be extended to identify vital buses of power grids.

Geodesic node vulnerability: In the same way as section A, the geodesic vulnerability of bus v of a power grid can be defined as,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

$$G_v = 1 - \frac{\sum_{i \neq j} \frac{1}{d_{ij}^v}}{\sum_{i \neq j} \frac{1}{d_{ij}}} \tag{26}$$

where d^v_{ij} is the shortest path between busses i and j of the network when bus v is failed.

Node betweenness centrality: Similar to the edge betweenness metric, the node betweenness centrality for node v of a network is defined as:

$$B(v) = \sum_{\substack{k,j \in V \\ k,j \neq v}} \frac{d^v_{kj}}{d_{kj}} \tag{27}$$

where d^v_{kj} shows the length of shortest paths between nodes k and j which passes through the node v.

Electrical node betweenness: If C_{ij} represents the maximum power which can be injected at bus i to be delivered to bus j, the electrical betweenness of bus u is redefined as,

$$B_u = \sum_{i \in S} \sum_{j \in D} \underbrace{\left[\frac{C_{ij}}{2} \sum_{l \in L^u} | f^l_{ij} | \right]}_{\kappa} \tag{28}$$

where L^u is the set of lines connected to bus u and $f^l_{ij} = f_{li} - f_{lj}$ is derived from the PTDF matrix. κ represents the transmission power taken by bus u where i and j are generation and consumption busses, respectively. Another form of electrical node betweenness is defined using Kirchhoff's law for bus v as [267],

$$B_u = \sum_{i \in S} \sum_{j \in D} w_{ij} I^u_{ij} \tag{29}$$

where the current through node u can be calculated as,

$$I^u_{ij} = \frac{1}{2} \left[\sum_{l \in L^u} \left| I^l_{ij} \right| + \Delta_u \right] \tag{30}$$

when a unit of electric current is transmitted from i to j. $\Delta_u = 1$ if $u = i$ or $u = j$, otherwise $\Delta u = 0$. This metric needs information about current in all branches of the network. It is also extended to study cascading failures in power networks [269].

Node electrical centrality: Node electrical centrality has been introduced as a combination of the electrical betweenness and the eigenvector centrality metrics [270]. The electrical centrality of node u is defined as

$$N_u = \varepsilon \bar{B}_u + (1 - \varepsilon) e_u \tag{31}$$

where e_u is the eigenvector centrality of node u and $\bar{B}_u$ is the normalised electrical betweenness of node u, derived from Eq. (29) as,

$$\bar{B}_u = \frac{B_u}{\sum_{i \in S} \sum_{j \in D} \sqrt{C_i C_j}} \tag{32}$$

where C_i is the rated active power of i^{th} generator and C_j is the actual load at bus j. The parameter ε tunes the trade-off between betweenness and eigenvector centralities.

Entropic Degree: The concept of entropy in complex networks has been used to define the entropic degree to study the vulnerability of busses in a power grid. The entropy of a given distribution p_i is computed by

$$H = \sum_{i=1}^{L} p_i \log p_i \tag{33}$$

where L refers to the number of sample values in the distribution. The idea is to extend the definition of entropy to include the number of connections to a node, their strengths, and the distribution of weights. Suppose that $\bar{w}_{ij}$ is the normalized weight of the power line between i^{th} generator and j^{th} load, i.e.

$$\bar{w}_{ij} = \frac{w_{ij}}{\sum_j w_{ij}} \tag{34}$$

The entropic degree of bus u is defined as [132, 271],

$$G_u = \left(1 - \sum_j \bar{w}_{uj} \log \bar{w}_{uj} \right) \sum_j w_{uj} \tag{35}$$

Other weighted entropy metrics are applied to vulnerability analysis, see e.g. [272]. Table II summarizes the centrality metrics discussed above.

TABLE II: SUMMARY OF METRICS WHICH ARE COMPARED IN THIS PAPER

NO.	METRIC	EQ. NUMBER	REF.
LINE CENTRALITY			
1	Geodesic link vulnerability	(16)	[235]
2	Net-ability	(19)	[17]
3	Edge betweenness	(21)	[265]
4	Electrical Edge betweenness	(24), (25)	[267]
BUS CENTRALITY			
1	Geodesic node vulnerability	(26)	[235]
2	Node betweenness	(27)	[265]
3	Electrical node betweenness	(28)	[267]
4	Node electrical centrality	(31), (32)	[270]
5	Entropic degree	(34), (35)	[132, 271]

V. CASE STUDIES

To assess the performance of centrality metrics in identifying the important power lines and generation buses correctly, they are applied on six benchmark networks (Table III). We compare performances of the centrality metrics in the three different scenarios. Scenarios 1 and 2 compare the performance of link centrality measures, while Scenario 3 focuses on bus centrality ones. In Scenario 1, the load protection on the power lines, which is normally implemented in power grids, are omitted. Instead, we measure how much the power lines are overloaded due to a failure. This is helpful to compare the performance of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

centrality measures in an unconstrained environment although. Scenario 2 repeats this comparison when practical constraints on the capacities of power lines are considered. In this case, it is assumed that the overloaded cables will be disconnected from the grid by the protection system, which indeed impacts the topology and dynamics of the system. The same practical constraint is considered in Scenario 3.

Scenario 1: *Line failure happens when overload protections of lines are ignored*

In this scenario, link centrality measures including geodesic vulnerability, net-ability, edge betweenness and Electrical edge betweenness are compared. To achieve the ground truth, we first rank the power lines based on the impact of their failure on the overload of other lines. To this end, we remove the lines one by one and perform a DC load flow study, using MATPOWER® [273], after each line is removed. At each step, we calculate the following total line margin (L_l) after removal of the l^{th} line,

$$L_l = \sum_{l \in E} \frac{C_l - |F_l|}{C_l} \tag{37}$$

where C_l is the power capacity of line l and F_l is its power flow. Therefore, small L_l means that power lines become close to overload if the line l is removed. In other words, line l with the smallest L_l is the most influential (central) line. We determine the ground truth by sorting the power lines, such that the line with the minimum L_l is on the top (let's name this value as L_{min}). Then, we calculate the most central line predicted by the above-mentioned centrality metrics and find its related load (L') from the ground truth. The precision of each metric in finding the most central power line is defined as $P = (L_{min}/L') \times 100$. For example, P = 40% for a centrality metric means that if the link predicted by that metric is failed, the reduction in L_l becomes 40% of the maximum possible reduction which may happen because of a line failure. Therefore, P shows how precise these metrics can identify the most influential link in the grid. Fig. 5(A) compares P(%) for all metrics in IEEE57, IEEE118, IEEE300, 200-I, 1354-ETS and 2868-VHV (see Table III). Although electrical betweenness works perfectly in IEEE57, Net-ability shows the best performance in networks with rather large sizes. The Performance of the efficiency and the betweenness measures are nearly the same.

TABLE III: INFORMATION ABOUT CASE STUDIES

MODEL	BUS	BRANCH	GENERATOR	REF.	LABEL
IEEE 57-bus	57	80	7		IEEE57
IEEE 118-bus	118	186	54		IEEE118
IEEE 300-bus	300	411	69		IEEE300
200-bus Illinois model	200	245	49	[274]	200-I
1354-bus European transmission systems	1354	1991	260	[275, 276]	1354-ETS
2868-bus VHV French transmission systems	2868	3808	600	[275]	2868-VHV

A similar study is performed considering the number of lines that become overloaded because of a line failure. Here, the ground truth contains the number of overloaded links caused by a failure in a specific link. Then, the prediction of the metric is compared with the maximum possible number of overloaded links to calculate the accuracy L(%). For example, if a metric suggests removal of a particular link causes overload in 4 other links while the maximum possible number of overloaded links in the ground-truth is 5, then the accuracy of this centrality metric is L = 4/5 = 80%. Fig. 5(B) compares the accuracy of all centrality metrics in the same networks as Fig. 5(A). Here, net-ability works perfect regardless of the grid size. Once again, the efficiency and betweenness measures show almost the same precision. However, the performance of electrical betweenness is not consistent.

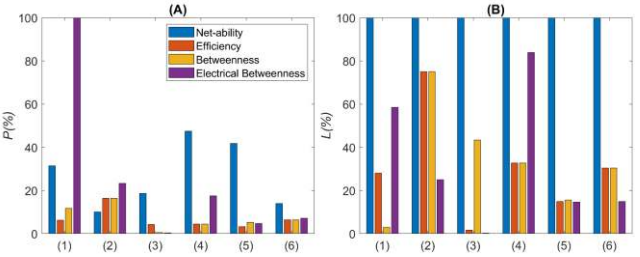

Figure 5. Accuracy of different metrics in finding the link which failure causes (A) the minimum total line margin, and (B) the maximum number of overloaded links in the following networks for Scenario 1: (1) IEEE57, (2) IEEE118, (3) IEEE300, (4) 200-I, (5) 1354-ETS and (6) 2868-VHV.

Pearson correlations ρ between rankings obtained by the centrality metrics and the ground-truth ranking for the case of total line margin is shown in Table IV. The p-value less than 0.05 means the correlation is significant. It shows that the ranking based on net-ability is more correlated to the ground truth than those based on other centrality metrics.

To further study rankings obtained by different centrality metrics, we measure the impact of a sequential link failure on the total line margin. Links are first removed based on the ranking obtained by each centrality metric. Then, a DC load flow analysis is performed to update the total line margin. Fig. 6 shows the variation of the total line margin when the top-l_f (%) of links of the grid are sequentially removed using different metrics. Once again, net-ability works more precise in large networks (panels C and D) resulting in the highest reduction. However, no consistent result performance is shown in small networks.

Scenario 2. *Line failure happens when overload protections of lines are active*

In the real world, power transmission lines are protected against getting overloaded. If an overload remains on a line for more than a specific (short) time, then the protection system isolates it from the grid. This may result in further overload on other lines, potentially leading to a cascade of failures and large-scale blackout. To compare the performance of different centrality metrics, the top-1% of links suggested by each metric is first removed and a DC

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

load flow is performed. The overloaded lines are removed, and the DC load flow analysis is repeated. This process continues until no further line overload happens. Finally, the total number of overloaded lines (that are tripped) is obtained. This process is then repeated for top-2% links, top-3% links, up to top-l_f% of links. Fig. 7 compares the percent of lines $T(\%)$ failed because of this sequential line removal based on different metrics. It shows that in large grids, net-ability works more precisely than others. For example, in 2868-VHV (panel D in Fig. 7), failure of top-6% of links proposed by the net-ability metric results in 100% of power lines being tripped, i.e. a total blackout. However, the failure of even the top-10% of links sorted by electrical betweenness does not have such a disruptive impact. In small networks, no consistent performance can be seen.

From the results of our study in scenarios 1 and 2, we conclude that net-ability can often identify vulnerable links in the large network more precisely than other metrics.

Scenario 3. *Generator failure happens, the reference bus compensates for lack of supply (i.e., no load shedding is required), and overload protections of power lines are active.*

In this scenario, buses are ranked using five node centrality measures: Geodesic node vulnerability, node betweenness, electrical node betweenness, node degree centrality and entropic degree. To achieve the ground truth, a DC load flow analysis is repeated once after removing each bus. Then, the buses are ranked with those resulting in the highest reduction in the total line margin on top. The above node centrality metrics are also applied to rank these buses and identify the most critical ones. Figure 8(A) compares the precision P of rankings obtained by each metric. For example, the entropic degree shows a precision of almost 90% for 2868-VHV. It means that if the highest-ranked node by the entropic degree is failed in this network, the amount of reduction in the total line margin will be 90% of the maximum possible reduction that can happen because of failure in a single bus. Fig. 8(A) shows that the entropic degree performs precisely in large networks while geodesic node vulnerability works better in small ones. For further analysis, we also consider the number of overloaded links when a bus is failed. Again, we find the ground truth by performing consecutive DC load flow analysis to rank buses based on the number of overloaded links which failure cause. Then, the bus that each metric suggests as the most vulnerable one is compared with the maximum possible case to derive $L(\%)$. Fig. 8(B) shows L for different metrics, where again the entropic degree and geodesic node vulnerability show better precision in predicting the most vulnerable bus.

The correlation between rankings of the node centrality metrics with the ground-truth is shown in Table V. It shows that entropic degree performs better than others in finding the most influential bus in large grids. In a complementary study, a consecutive failure scenario on busses is performed. The generation buses are failed one after another according to the ranking obtained by each metric. After each failure, the number of tripped lines (due to being overloaded) is calculated from a DC load flow analysis. Figure 9 shows how the number of the tripped line increases when the top-$B_f(\%)$ of the generation buses are removed based on different metrics. In the European transmission system, failure in less than top-10% of buses ranked by either entropic degree or geodesic node vulnerability results in 100% of lines to trip and a total blackout. In the high voltage French transmission system, removing buses based on entropic degree or node electrical centrality degrades the network performance faster than other metrics. Therefore, the entropic degree performs more precisely in large networks which support the correlation shown in Table V.

TABLE IV: PEARSON CORRELATION ρ BETWEEN RESULTS OF LINK CENTRALITY MEASURES AND THE GROUND TRUTH. DATA IS IN $\rho[p\text{-value}]$

	NET-ABILITY	EFFICIENCY	BET.	ELEC. BET.
IEEE57	0.39[3×10^{-4}]	0.06[0.62]	0.06 [0.56]	0.50 [2×10^{-6}]
IEEE118	0.12[0.09]	0.39[$<10^{-7}$]	0.06 [0.4]	0.06 [0.38]
IEEE300	0.21[1×10^{-5}]	-.01[0.89]	-.01[0.89]	0.14 [3×10^{-3}]
200-I	0.04[0.54]	0.18[0.004]	0.05[0.004]	-0.09 [0.15]
1354-ETS	0.21[$<10^{-19}$]	0.15[$<10^{-10}$]	0.13[$<10^{-8}$]	0.13 [$<10^{-7}$]
2868-VHV	0.23[$<10^{-47}$]	0.17[$<10^{-25}$]	0.14[$<10^{-19}$]	0.22 [$<10^{-45}$]

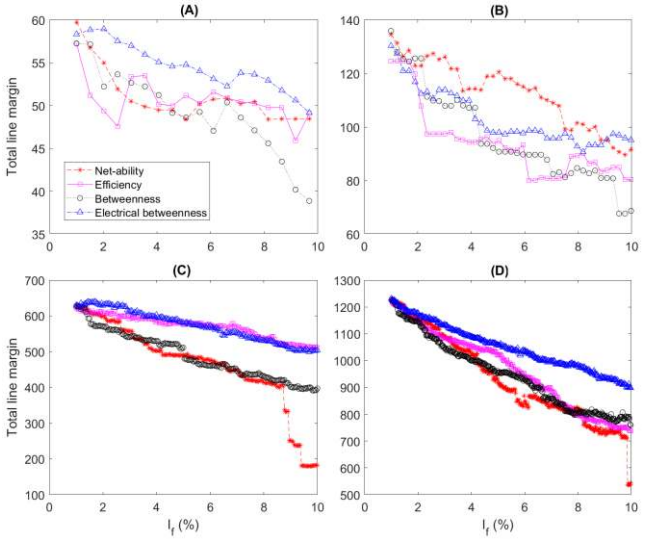

Figure 6. Reduction of the total line margin of the grid when l_f(%) of the top-ranked links based on different metrics are failed. Grids are (A) IEEE118, (B) IEEE300, (C) 1354-ETS and (F) 2868-VHV.

VI. CONCLUSIONS AND OUTLOOK

Power grids are among critical infrastructures which have supported us towards the current modern lifestyle. Although they have shown to be rather resilient against unexpected events, the paradigm shift towards distributed generation has increased sources of attacks and failures in the grid, and thus makes the vulnerability analysis important once again. The structure of modern power grids is considerably more complicated than before and requires advanced tools for vulnerability study. In the paper, different approaches for this analysis was reviewed. Among different approaches, complex networks and centrality analysis have shown promising performance in the study of distributed generation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3107492, IEEE Access

grids. As pure topological centrality metrics do not cover the dynamical nature of power grids, this paper mainly reviewed those metrics extended for power grid applications. We compared the performance of these metrics by applying them on benchmark and real power grid networks. Simulation results show that net-ability can often identify vulnerable links in large power grids more precisely than other line centrality metrics. To identify the most vulnerable busses, "entropic degree" showed better results.

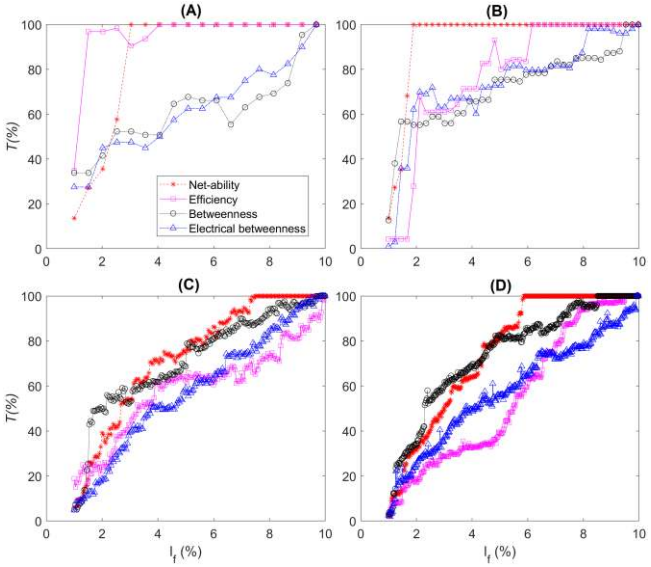

Figure 7. Cascading failure caused by the failure of the top l_f(%) of links ranked by different metrics. Grids are (A) IEEE118, (B) IEEE300, (C) 1354-ETS and (D) 2868-VHV.

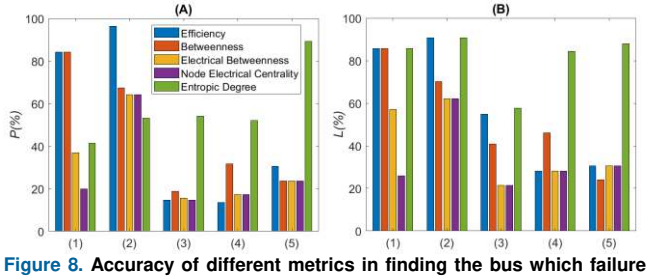

Figure 8. Accuracy of different metrics in finding the bus which failure causes (A) maximum reduction in total line margin, and (B) the maximum number of overloaded links in the following networks for Scenario 1: (1) IEEE57, (2) IEEE118, (3) IEEE300, (4) 1354-ETS and (5) 2868-VHV.

TABLE V: PEARSON CORRELATION ρ BETWEEN RESULTS OF BUS CENTRALITY MEASURES AND THE GROUND TRUTH. DATA IS IN ρ[p-value]

	IEEE 57	IEEE 118	IEEE 300	1354-ETS	2868-VHV
GEODESIC NODE VUL.	0.23 [0.09]	0.26 [0.004	0.33 [*]	0.38 [**]	0.15 [***]
BETWEENNESS	0.12 [0.38]	0.22 [0.015]	0.28 [*]	0.45 [**]	0.15 [***]
ELECTRICAL BETWEENNESS	**0.4** [0.002]	0.01 [0.88]	0.35 [*]	0.4 [**]	0.1 [***]
NODE ELEC. CENTRALITY	0.35 [0.009]	**0.31** [0.0007]	**0.37** [*]	0.41 [**]	0.15 [***]
ENTROPIC DEGREE	0.1 [0.43	-0.05 [0.6]	0.23 [*]	**0.48** [**]	**0.18** [***]

* $<1\times10^{-4}$, ** $<1\times10^{-46}$, *** $<1\times10^{-3}$

Developing precise models, using either model-based or data-driven approaches, is the key step towards analysis and control of future power grids, especially for reliability and resilience studies. These models should consider the intermittence and uncertainty of renewable units, dynamical behaviours of power grids, and practical limitations and constraints. Although CN-based modelling approaches can manage large-scale power grids, they mainly focus on the topology of the grid. On the other hand, CPS and MAS models normally target dynamical behaviour of the grid and have difficulties in modelling large systems. Therefore, there is a lack of a comprehensive model which addresses the dimension problem, dynamics, and real-world constraints of power grids simultaneously.

Modelling electricity distribution networks is also important because the future smart grids will likely include local energy trading over medium- or low-voltage networks. The emergence of disruptive DERs, such as batteries, photovoltaics, and electric vehicles, has made the planning and control problems complicated, which indeed require appropriate models. Despite the efforts in modelling these systems as a small-world CN [123] or a MAS [124], the management of several unpredictable and uncertain parameters in the future distribution grids requires a comprehensive modelling framework to be developed.

Human decisions and errors play important roles in reliability of power grids. Therefore, the CPS models should be leveraged to Cyber-Physical-Human ones [127] in which, actions of system operators and consumers' behaviours are also augmented. This is crucial for reliability analysis specifically, since people's decisions in future power grids, with a huge amount of uncertainties and unpredictability, can be more disruptive than that in conventional ones.

Resilience against extreme weather events and cyberattacks has attracted a lot of researchers during recent decades. With the advancement of sensor and communication technologies, a huge amount of data from different parts of a power grid is now available with a high resolution. This data can be used for different applications, such as vulnerability study, for which, advanced data-drive and AI-based algorithms are should be developed. A review of this field in the paper showed that it is still a young field of research and a lot of progress is expected in the future.

On the other hand, the vulnerability study has been mainly focused on the generation and transmission levels of a power grid. However, changing the nature of distribution power grids with the emergence of DERs makes their resilience study very important since they were not originally designed to face local generation units. Data-driven algorithms can also be applied to problems in distribution power grids, especially in residential areas, thanks to the huge amount of consumption data collected by smart meters through Advanced Metering Infrastructure (AMI). This can be done using either time-series analysis techniques [125] or machine learning classification approaches [126]. This revolution

makes the resilience analysis in distribution power grids in the presence of DER a very hot research topic.

Finally, we require to update resilience and reliability measures and make them appropriate for future power grids. Flow-based metrics, which are based on load-flow studies, are precise, but computationally expensive. In contrary, easy to calculate CN-based measures have not been well customised for future power grid applications yet. Therefore, developing computationally efficient metrics which simultaneously address dynamical performance and practical constraints of power grids is a subject of further research. Particularly, these metrics should appropriately consider limitations of renewable energy resources, such as limited availability, minimum/maximum rate and level of supply and their limitations in VAR control.

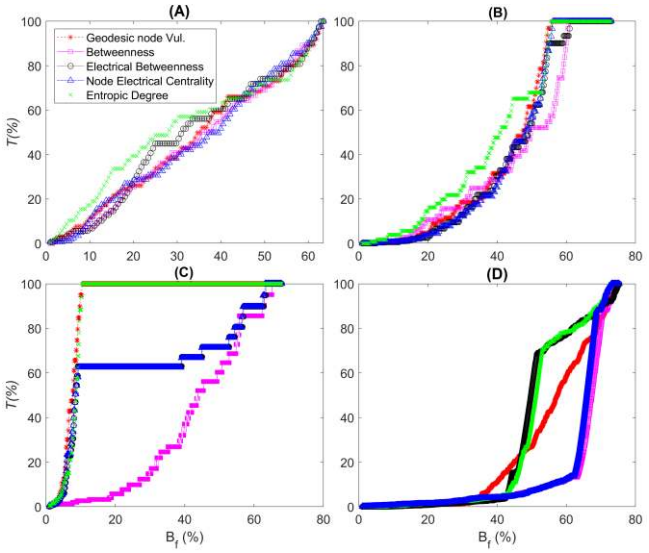

Figure 9. Percent *T* of failed links caused by the failure of the top B_f(%) of busses ranked by different metrics. Grids are (A) IEEE118, (B) IEEE300, (C) 1354-ETS and (D) 2868-VHV.

REFERENCES

[1] X. Yu, C. Cecati, T. Dillon, and M. G. Sim, "The new frontier of smart grids," *IEEE Control Syst. Mag.,* vol. 5, no. 3, pp. 49-63, 2011.

[2] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research,* vol. 81, no. 7, pp. 1334-1340, 2011.

[3] M. Panteli and P. Mancarella, "The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience," *IEEE Power Energy Mag.,* vol. 13, no. 3, pp. 58-66, 2015.

[4] M. S. Hossain, N. A. Madlool, N. A. Rahim, J. Selvaraj, A. K. Pandey, and A. F. Khan, "Role of smart grid in renewable energy: An overview," *Renew. Sustain. Energy Rev.,* vol. 60, pp. 1168-1184, 2016.

[5] M. L. Tuballa and M. L. Abundo, "A review of the development of Smart Grid technologies," *Renewable and Sustainable Energy Reviews,* vol. 59, pp. 710-725, 2016.

[6] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and Sustainable Energy Reviews,* vol. 66, pp. 499-516, 2016.

[7] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1058-1070, 2016.

[8] O. Palizban and K. Kauhaniemi, "Hierarchical control structure in microgrids with distributed generation: Island and grid-connected mode," *Renewable and Sustainable Energy Reviews,* vol. 44, pp. 797-813, 2015.

[9] T. L. Vandoorn, J. C. Vasquez, J. D. Kooning, J. M. Guerrero, and L. Vandevelde, "Microgrids: Hierarchical Control and an Overview of the Control and Reserve Management Strategies," *IEEE Industrial Electronics Magazine,* vol. 7, no. 4, pp. 42-55, 2013.

[10] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on CPS," presented at the ACM Int. Conf. High confidence networked syst., USA, 2013.

[11] A. Bernstein, Bienstock, D., Hay, D., Uzunoglu, M., & Zussman, "Sensitivity analysis of the power grid vulnerability to large-scale cascading failures," *ACM SIGMETRICS Performance Evaluation Review,* vol. 40, pp. 33-37, 2012.

[12] O. P. Veloza and F. Santamaria, "Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes," *The Electricity Journal,* vol. 29, no. 7, pp. 42-49, 2016.

[13] F. H. Jufri, V. Widiputra, and J. Jung, "State-of-the-art review on power grid resilience to extreme weather events: Definitions, frameworks, quantitative assessment methodologies, and enhancement strategies," *Applied Energy,* vol. 239, pp. 1049-1065, 2019.

[14] L. M. Shekhtman, M. M. Danziger, and S. Havlin, "Recent advances on failure and recovery in networks of networks," (in English), *Chaos Soliton Fract,* vol. 90, pp. 28-36, Sep 2016.

[15] R. Ghanbari, M. Jalili, and X. H. Yu, "Analysis of Cascaded Failures in Power Networks using Maximum Flow based Complex Network Approach," presented at the IEEE Industrial Electronics Conference (IECON), 2016.

[16] Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," *Science,* vol. 358, no. 6365, 2017.

[17] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: a complex network approach," *Chaos,* vol. 19, no. 1, p. 013119, Mar 2009.

[18] R. Carareto, M. S. Baptista, and C. Grebogi, "Natural synchronization in power-grids with anti-correlated units," (in English), *Communications in Nonlinear Science and Numerical Simulation,* vol. 18, no. 4, pp. 1035-1046, 2013.

[19] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos,* vol. 12, no. 4, pp. 985-994, Dec 2002.

[20] I. Dobson, B. A. Carreras, V. E. Lynch, B. Nkei, and D. E. Newman, "Estimating failure propagation in models of cascading blackouts," (in English), *Probability in the Engineering and Informational Sciences,* vol. 19, no. 4, pp. 475-488, 2005.

[21] M. Vaiman *et al.*, "Mitigation and Prevention of Cascading Outages: Methodologies and Practical Applications," in *IEEE Power and Energy Society General Meeting (Pes)*.

[22] R. Ghanbari, M. Jalili, and X. Yu, "Selective load reduction in power grids in order to minimise the effects of cascade failures " presented at the The 43rd Annual Conference of IEEE Industrial Electronics Society (IECON), Beijing, China, 2017.

[23] R. Ghanbari, M. Jalili, and X. Yu, "Correlation of cascade failures and centrality measures in complex networks," *Future Generation Computer Systems,* 2017.

[24] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. Geem, "A Critical Review of Robustness in Power Grids Using Complex Networks Concepts," *Energies,* vol. 8, no. 9, pp. 9211-9265, 2015.

[25] C.-C. Chu and H. H.-C. Iu, "Complex Networks Theory For Modern Smart Grid Applications: A Survey," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.,* vol. 7, no. 2, pp. 177-191, 2017.

[26] Y. Lin, Z. Bie, and A. Qiu, "A review of key strategies in realizing power system resilience," *Global Energy Interconnection,* vol. 1, no. 1, pp. 70-78, 2018.

[27] G. Huang, J. Wang, C. Chen, J. Qi, and C. Guo, "Integration of Preventive and Emergency Responses for Power Grid Resilience

Enhancement," *IEEE Trans. Power Syst.,* vol. 32, no. 6, pp. 4451-4463, 2017.
[28] S. M. Dibaji, M. Pirani, D. B. Flamholz, A. M. Annaswamy, K. H. Johansson, and A. Chakrabortty, "A systems and control perspective of CPS security," *Annual Rev. Control,* vol. 47, pp. 394-411, 2019.
[29] J. Gao, B. Barzel, and A. L. Barabasi, "Universal resilience patterns in complex networks," *Nature,* vol. 530, no. 7590, pp. 307-12, Feb 18 2016.
[30] M. Newman, *Networks: an introduction*. Oxford university press, 2010.
[31] A. Bidram, F. L. Lewis, Z. Qu, and A. Davoudi, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission & Distribution,* vol. 7, no. 8, pp. 822-831, 2013.
[32] M. Rohden, A. Sorge, D. Witthaut, and M. Timme, "Impact of network topology on synchrony of oscillatory power grids," *Chaos,* vol. 24, no. 1, p. 013123, Mar 2014.
[33] W. Yu, G. Wen, X. Yu, Z. Wu, and J. Lu, "Bridging the gap between complex networks and smart grids," *Journal of Control and Decision,* vol. 1, no. 1, pp. 102-114, 2014.
[34] G. A. Pagani and M. Aiello, "Power grid complex network evolutions for the smart grid," *Physica A: Statistical Mechanics and its Applications,* vol. 396, pp. 248-266, 2014.
[35] A. Moradi Amani, N. Gaeini, M. Jalili, and X. Yu, "Which generation unit should be selected as control leader in secondary frequency control of microgrids?," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems,* vol. 7, no. 3, pp. 393-402, 2017.
[36] F. Wenli, L. Zhigang, H. Ping, and M. Shengwei, "Cascading failure model in power grids using the complex network theory," *IET Gen. Trans. Dist.,* vol. 10, no. 15, pp. 3940-3949, 2016.
[37] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. Hwang, "Complex networks: Structure and dynamics," *Physics Reports,* vol. 424, no. 4-5, pp. 175-308, 2006.
[38] J. G. Restrepo, E. Ott, and B. R. Hunt, "Characterizing the dynamical importance of network nodes and links," *Physical Review Letters,* vol. 97, no. 9, p. 094102, 2006.
[39] D. Chen, L. Lü, M.-S. Shang, Y.-C. Zhang, and T. Zhou, "Identifying influential nodes in complex networks," *Physica a: Statistical mechanics and its applications,* vol. 391, no. 4, pp. 1777-1787, 2012.
[40] A. Moradi Amani, M. Jalili, X. Yu, and L. Stone, "Finding the most influential nodes in pinning controllability of complex networks," *IEEE Trans. Circuits Syst. II, Exp. Briefs,* vol. 64, no. 6, pp. 685-689, 2017.
[41] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Anal,* vol. 26, no. 4, pp. 955-69, 2006.
[42] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power system," *Reliability Engineering & System Safety,* vol. 183, pp. 153-172, 2019.
[43] Y.-S. Li, D.-Z. Ma, H.-G. Zhang, and Q.-Y. Sun, "Critical Nodes Identification of Power Systems Based on Controllability of Complex Networks," *Applied Sciences,* vol. 5, no. 3, pp. 622-636, 2015.
[44] M. Panteli and P. Mancarella, "Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events," *IEEE Syst. J.,* vol. 11, no. 3, pp. 1733-1742, 2017.
[45] Y. Wang, C. Chen, J. Wang, and R. Baldick, "Research on Resilience of Power Systems Under Natural Disasters—A Review," *IEEE Trans. Power Syst.,* vol. 31, no. 2, pp. 1604-1613, 2016.
[46] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the Extreme: A Study on the Power System Resilience," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1253-1266, 2017.
[47] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," *IEEE Trans. Power Syst.,* vol. 32, no. 6, pp. 4732-4742, 2017.
[48] N. M. Tabatabaei, S. N. Ravadanegh, and N. Bizon, *Power systems resilience: Modeling, analysis and practice*. Springer, 2018.
[49] A. M. Amani, N. Gaeini, M. Jalili, and X. Yu, "Voltage control in distributed generation systems based on complex network approach," *Energy Procedia,* vol. 110, pp. 334-339, 2017.
[50] X. Yu and Y. Xue, "Smart grids: A cyber physical systems perspective," *Proceedings of the IEEE,* vol. 104, no. 5, pp. 1058-1070, 2016.
[51] M. Chertkov, F. Pan, and M. G. Stepanov, "Predicting failures in power grids: The case of static overloads," *IEEE Transactions on Smart Grid,* vol. 2, no. 1, pp. 162-172, 2010.
[52] P. V. Mieghem, *Graph Spectra for Complex Networks*. Cambridge University Press, 2011, p. 362.
[53] P. Erdős and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hungar. Acad. Sci,* vol. 5, pp. 17-61, 1960.
[54] X. F. Wang and G. Chen, "Complex networks: Small-world, scale-free and beyaond," *IEEE Circuits Syst. Mag.,* vol. 3, no. 1, pp. 6-20, 2003.
[55] L. Cui, S. Kumara, and R. Albert, "Complex Networks: An Engineering View," *IEEE Circuits and Systems Mag.,* vol. 10, no. 3, pp. 10-25, 2010.
[56] Duncan J.Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature,* vol. 393, pp. 440-442, 1998.
[57] A.-L. s. Barabasi and R. k. Albert, "Emergence of Scaling in Random Networks," *Science,* vol. 286, 1999.
[58] K. -I. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale-free networks," *Physical Review Letters,* vol. 87, no. 27, p. 278701, 2001.
[59] M. Chavez, D. U. Hwang, A. Amann, H. G. Hentschel, and S. Boccaletti, "Synchronization is enhanced in weighted complex networks," *Physical Review Letters,* vol. 94, no. 21, p. 218701, Jun 3 2005.
[60] Tian Xu, Jie Chen, Yue He, and Da-Ren He, "Complex network properties of Chinese power grid," *Int. J. Modern Physics B,* vol. 18, no. 17-19, pp. 2599-2603, 2004.
[61] G. A. Pagani and M. Aiello, "The Power Grid as a complex network: A survey," *Physica A,* vol. 392, no. 11, pp. 2688-2700, 2013.
[62] Y. Xu, A. J. Gurfinkel, and P. A. Rikvold, "Architecture of the Florida power grid as a complex network," *Physica A,* vol. 401, pp. 130-140, 2014.
[63] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, "Network topology and resilience analysis of South Korean power grid," *Physica A,* vol. 465, pp. 13-24, 2017.
[64] M. A. Saniee Monfared, M. Jalili, and Z. Alipour, "Topology and vulnerability of the Iranian power grid," *Physica A,* vol. 406, pp. 24-33, 2014.
[65] M. Rosas-Casals and B. Corominas, "Assessing European power grid reliability by means of topological measures," *WIT Trans. ecology environment,* vol. 121, pp. 527-537, 2009.
[66] M. Rosas-Casals, S. Valverde, and R. Solé, "Topological vulnerability of the European power grid under errors and attacks," *Int. J. Bifurcation Chaos,* vol. 17, no. 07, pp. 2465-2475, 2007.
[67] P. Dey, R. Mehra, F. Kazi, S. Wagh, and N. M. Singh, "Impact of Topology on the Propagation of Cascading Failure in Power Grid," *IEEE Trans. Smart Grid,* vol. 7, no. 4, pp. 1970-1978, 2016.
[68] H. Tu, Y. Xia, H. H.-C. Iu, and X. Chen, "Optimal robustness in power grids from a network science perspective," *IEEE Trans. Circuits Syst. II, Exp. Briefs,* vol. 66, no. 1, pp. 126-130, 2018.
[69] J. M. Reynolds-Barredo, D. E. Newman, B. A. Carreras, and I. Dobson, "The interplay of network structure and dispatch solutions in power grid cascading failures," *Chaos,* vol. 26, no. 11, p. 113111, 2016.
[70] M. Herrera, M. Pérez-Hernández, A. Kumar Parlikad, and J. Izquierdo, "Multi-agent systems and complex networks: Review and applications in systems engineering," *Processes,* vol. 8, no. 3, p. 312, 2020.
[71] Z. Li, Z. Duan, G. Chen, and L. Huang, "Consensus of multiagent systems and synchronization of complex networks: A unified viewpoint," *Transactions on Circuits Systems I: Regular Papers,* vol. 57, no. 1, pp. 213-224, 2009.
[72] M. Pipattanasomporn, H. Feroze, and S. Rahman, "Multi-agent systems in a distributed smart grid: Design and implementation," in

2009 IEEE/PES Power Systems Conference and Exposition: IEEE, pp. 1-8.

[73] A. Sujil, J. Verma, and R. Kumar, "Multi agent system: concepts, platforms and applications in power systems," *Artificial Intelligence Review,* vol. 49, no. 2, pp. 153-182, 2018.

[74] V. N. Coelho, M. W. Cohen, I. M. Coelho, N. Liu, and F. G. Guimarães, "Multi-agent systems applied for energy systems integration: State-of-the-art applications and trends in microgrids," *Applied energy,* vol. 187, pp. 820-832, 2017.

[75] K. Barnes, B. Johnson, and R. Nickelson, "Review of supervisory control and data acquisition (SCADA) systems," *Idaho National Engineering*
Environmental Laboratory, 2004.

[76] A. A. Shobole and M. Wadi, "Multiagent systems application for the smart grid protection," *Renewable and Sustainable Energy Reviews,* vol. 149, p. 111352, 2021/10/01/ 2021.

[77] J. Ansari, A. Gholami, and A. Kazemi, "Multi-agent systems for reactive power control in smart grids," *International Journal of Electrical Power & Energy Systems,* vol. 83, pp. 411-425, 2016/12/01/ 2016.

[78] Y. Xu, W. Liu, and J. Gong, "Stable multi-agent-based load shedding algorithm for power systems," *IEEE Transactions on Power Systems,* vol. 26, no. 4, pp. 2006-2014, 2011.

[79] V. Telukunta, J. Pradhan, A. Agrawal, M. Singh, and S. G. Srivani, "Protection challenges under bulk penetration of renewable energy resources in power systems: A review," *CSEE journal of power energy systems,* vol. 3, no. 4, pp. 365-379, 2017.

[80] H. Shahbazi, F. J. J. o. M. P. S. Karbalaei, and C. Energy, "Decentralized voltage control of power systems using multi-agent systems," *Journal of Modern Power Systems Clean Energy,* vol. 8, no. 2, pp. 249-259, 2020.

[81] Z. Yan and Y. Xu, "A multi-agent deep reinforcement learning method for cooperative load frequency control of a multi-area power system," *IEEE Transactions on Power Systems,* vol. 35, no. 6, pp. 4599-4608, 2020.

[82] W. Liu, W. Gu, W. Sheng, X. Meng, Z. Wu, and W. Chen, "Decentralized multi-agent system-based cooperative frequency control for autonomous microgrids with communication constraints," *IEEE Transactions on Sustainable Energy,* vol. 5, no. 2, pp. 446-456, 2014.

[83] Y. Zhou, J. Wu, and C. Long, "Evaluation of peer-to-peer energy sharing mechanisms based on a multiagent simulation framework," *Applied energy,* vol. 222, pp. 993-1022, 2018.

[84] F. Luo, Z. Y. Dong, G. Liang, J. Murata, and Z. Xu, "A distributed electricity trading system in active distribution networks based on multi-agent coalition and blockchain," *IEEE Transactions on Power Systems,* vol. 34, no. 5, pp. 4097-4108, 2018.

[85] M. Nizami, M. Hossain, S. Rafique, K. Mahmud, U. B. Irshad, and G. Town, "A Multi-agent system based residential electric vehicle management system for grid-support service," in *2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*: IEEE, pp. 1-6.

[86] W. He, X. Gao, W. Zhong, and F. Qian, "Secure impulsive synchronization control of multi-agent systems under deception attacks," *Information Sciences,* vol. 459, pp. 354-368, 2018.

[87] C. Chen *et al.*, "Resilient adaptive and H∞ controls of multi-agent systems under sensor and actuator faults," *Automatica,* vol. 102, pp. 19-26, 2019.

[88] M. W. Khan and J. Wang, "The research on multi-agent system for microgrid control and optimization," *Renewable Sustainable Energy Reviews,* vol. 80, pp. 1399-1411, 2017.

[89] A. S. Nair *et al.*, "Multi-agent systems for resource allocation and scheduling in a smart grid," *Technology Economics of Smart Grids Sustainable Energy,* vol. 3, no. 1, pp. 1-15, 2018.

[90] R. F. Sampaio, L. S. Melo, R. P. Leão, G. C. Barroso, and J. R. Bezerra, "Automatic restoration system for power distribution networks based on multi-agent systems," *IET Generation, Transmission Distribution,* vol. 11, no. 2, pp. 475-484, 2017.

[91] W. Li *et al.*, "A full decentralized multi-agent service restoration for distribution network with DGs," *IEEE Transactions on Smart Grid,* vol. 11, no. 2, pp. 1100-1111, 2019.

[92] A. Kulasekera, R. Gopura, K. Hemapala, and N. Perera, "A review on multi-agent systems in microgrid applications," in *ISGT2011-India*: IEEE, pp. 173-177.

[93] M. Woolridge and M. J. Wooldridge, *Introduction to multiagent systems*. John Wiley & Sons, Inc., 2001.

[94] S. Mei, N. Zarrabi, M. Lees, and P. M. Sloot, "Complex agent networks: An emerging approach for modeling complex systems," *Applied Soft Computing,* vol. 37, pp. 311-321, 2015.

[95] S. K. Khaitan, J. D. McCalley, and C. C. Liu, *Cyber physical systems approach to smart electric power grid*. Springer, 2015.

[96] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica,* vol. 4, no. 1, pp. 27-40, 2017.

[97] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *50th IEEE Conference on Decision and Control and European Control Conference*, pp. 2195-2201.

[98] K. R. Davis *et al.*, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2464-2475, 2015.

[99] Chen *et al.*, "A Game Theory-Based Approach for Vulnerability Analysis of a Cyber-Physical Power System," *Energies,* vol. 12, no. 15, 2019.

[100] A. Bidram, F. L. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks," *IEEE Control Syst. Mag.,* vol. 34, no. 6, pp. 56-77, 2014.

[101] N. Gaeini, A. M. Amani, M. Jalili, and X. Yu, "Optimization of Communication Network Topology in Distributed Control Systems Subject to Prescribed Decay Rate," *IEEE Transactions on Cybernetics,* 2019.

[102] Y. Sun, C. Zhong, X. Hou, J. Yang, H. Han, and J. M. Guerrero, "Distributed cooperative synchronization strategy for multi-bus microgrids," *International Journal of Electrical Power & Energy Systems,* vol. 86, pp. 18-28, 2017.

[103] M. Mola, A. Afshar, N. Meskin, and M. Karrari, "Distributed Fast Fault Detection in DC Microgrids," *IEEE Systems Journal,* pp. 1-12, 2020.

[104] K. Schneider, C. C. Liu, and J. P. Paul, "Assessment of Interactions Between Power and Telecommunications Infrastructures," *IEEE Transactions on Power Systems,* vol. 21, no. 3, pp. 1123-1130, 2006.

[105] X. Liu, J. Zhang, and P. Zhu, "Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory," *International Journal of Critical Infrastructure Protection,* vol. 16, pp. 13-25, 2017.

[106] H. Tu, Y. Xia, C. K. Tse, and X. Chen, "A Hybrid Cyber Attack Model for Cyber-Physical Power Systems," *IEEE Access,* vol. 8, pp. 114876-114883, 2020.

[107] Y. Zhang, Y. Xiang, and L. Wang, "Reliability analysis of power grids with cyber vulnerability in SCADA system," in *2014 IEEE PES General Meeting| Conference & Exposition*: IEEE, pp. 1-5.

[108] N. Gaeini, A. Moradi Amani, M. Jalili, and X. Yu, "Cooperative secondary frequency control of distributed generation: The role of data communication network topology," *Int. J. Elec. Power & Energy Systems,* vol. 92, pp. 221-229, 2017.

[109] A. M. Amani, N. Gaeini, M. Jalili, and X. Yu, "Effect of disconnection of generation units on the rate of change of frequency in distributed power systems," in *2017 Australian and New Zealand Control Conference (ANZCC)*: IEEE, pp. 127-132.

[110] Y. Susuki *et al.*, "A Hybrid System Approach to the Analysis and Design of Power Grid Dynamic Performance," *Proceedings of the IEEE,* vol. 100, no. 1, pp. 225-239, 2012.

[111] R. Goebel, R. G. Sanfelice, and A. R. J. I. c. s. m. Teel, "Hybrid dynamical systems," vol. 29, no. 2, pp. 28-93, 2009.

[112] E. Foruzan, S. Asgarpoor, and J. M. Bradley, "Hybrid system modeling and supervisory control of a microgrid," in *2016 North American Power Symposium (NAPS)*, pp. 1-6.

[113] S. C. Savulescu, *Real-time stability in power systems: techniques for early detection of the risk of blackout*. Springer, 2014.

[114] H. Haes Alhelou, M. E. Hamedani-Golshan, T. C. Njenda, and P. Siano, "A survey on power system blackout and cascading events:

Research motivations and challenges," *Energies,* vol. 12, no. 4, p. 682, 2019.
[115] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature,* vol. 464, no. 7291, pp. 1025-8, Apr 15 2010.
[116] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," in *IEEE Global Comm. Conf.*, pp. 2164-2169.
[117] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids," *Nature communications,* vol. 9, no. 1, pp. 1-13, 2018.
[118] X. Zhang, C. Zhan, and K. T. Chi, "Modeling the dynamics of cascading failures in power systems," *IEEE Journal on Emerging Selected Topics in Circuits Systems,* vol. 7, no. 2, pp. 192-204, 2017.
[119] Z. Wang, A. Scaglione, and R. J. Thomas, "A Markov-transition model for cascading failures in power grids," in *2012 45th Hawaii International Conference on System Sciences*: IEEE, pp. 2115-2124.
[120] H. Guo, S. S. Yu, H. H. C. Iu, T. Fernando, and C. Zheng, "A complex network theory analytical approach to power system cascading failure-From a cyber-physical perspective," *Chaos,* vol. 29, no. 5, p. 053111, May 2019.
[121] R. A. Shuvro, P. Das, M. M. Hayat, and M. Talukder, "Predicting cascading failures in power grids using machine learning algorithms," in *2019 North American Power Symposium (NAPS)*: IEEE, pp. 1-6.
[122] R. Pi, Y. Cai, Y. Li, and Y. Cao, "Machine learning based on bayes networks to predict the cascading failure propagation," *IEEE Access,* vol. 6, pp. 44815-44823, 2018.
[123] G. A. Pagani and M. Aiello, "Power grid complex network evolutions for the smart grid," *Physica A,* vol. 396, pp. 248-266, 2014.
[124] S. Baghali and Z. Guo, "Impacts of Privately Owned Electric Vehicles on Distribution System Resilience: A Multi-agent Optimization Approach," *arXiv preprint arXiv:.03828,* 2021.
[125] R. S. Tsay and R. Chen, *Nonlinear time series analysis*. John Wiley & Sons, 2018.
[126] L. Blakely, M. J. Reno, and W.-c. Feng, "Spectral clustering for customer phase identification using AMI voltage timeseries," in *2019 IEEE Power and Energy Conference at Illinois (PECI)*: IEEE, pp. 1-7.
[127] S. K. Sowe, K. Zettsu, E. Simmon, F. de Vaulx, and I. Bojanova, "Cyber-Physical Human Systems: Putting People in the Loop," (in eng), *IT Prof,* vol. 18, no. 1, pp. 10-13, Jan-Feb 2016.
[128] "IEEE Guide for Electric Power Distribution Reliability Indices," *IEEE Std 1366-2012 (Revision of IEEE Std 1366-2003),* pp. 1-43, 2012.
[129] A. Clark-Ginsberg, "What's the Difference between Reliability and Resilience," *Department of Homeland Security,* March 2016.
[130] J. M. Cainey, "Resilience and reliability for electricity networks," *Proceedings of the Royal Society of Victoria,* vol. 131, no. 1, pp. 44-52, 2019.
[131] S. N. Islam, Z. Baig, and S. Zeadally, "Physical layer security for the smart grid: vulnerabilities, threats, and countermeasures," *IEEE Trans. Ind. Informat.,* vol. 15, no. 12, pp. 6522-6530, 2019.
[132] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *Int. J. Critical Infrastructure Protection,* vol. 2, no. 1-2, pp. 5-12, 2009.
[133] D. Wang, Y. Li, P. Dehghanian, and S. Wang, "Power grid resilience to electromagnetic pulse (EMP) disturbances: A literature review," in *North American Power Symposium*: IEEE, pp. 1-6.
[134] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications," *IEEE Access,* vol. 8, pp. 151019-151064, 2020.
[135] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks,* vol. 57, no. 5, pp. 1344-1371, 2013.
[136] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," *Int. J. Elec. Power Energy Syst.,* vol. 99, pp. 45-56, 2018.
[137] M. Rahnamay-Naeini and M. M. Hayat, "Impacts of operating characteristics on sensitivity of power grids to cascading failures," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*: IEEE, pp. 1-5.
[138] "Arizona-southern california outages on september 8, 2011: Causes and recommendations," FERC and NERC, Apr. 2012.
[139] M. Tavakoli and M. Nafar, "Reduce maintenance costs by improving human reliability in power grids," *Electrical Engineering,* pp. 1-11, 2021.
[140] Z. Wang *et al.*, "Impacts of operators' behavior on reliability of power grids during cascading failures," *IEEE Transactions on Power Systems,* vol. 33, no. 6, pp. 6013-6024, 2018.
[141] M. Borecki, M. Ciuba, Y. Kharchenko, and Y. Khanas, "Substation reliability evaluation in the context of the stability prediction of power grids," *Bulletin of the Polish Academy of Sciences: Technical Sciences,* pp. 769-776-769-776, 2020.
[142] A. Nageswara Rao, P. Vijaya Priya, M. Kowsalya, and R. Gnanadass, "Wide area monitoring for energy system: a review," *International Journal of Ambient Energy,* vol. 40, no. 5, pp. 537-553, 2019.
[143] A. Marot, S. Tazi, B. Donnot, and P. Panciatici, "Guided machine learning for power grid segmentation," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*: IEEE, pp. 1-6.
[144] D.-I. Kim, L. Wang, and Y.-J. Shin, "Data driven method for event classification via regional segmentation of power systems," *IEEE Access,* vol. 8, pp. 48195-48204, 2020.
[145] A. Rajabi, M. Eskandari, M. J. Ghadi, L. Li, J. Zhang, and P. Siano, "A comparative study of clustering techniques for electrical load pattern segmentation," *Renewable Sustainable Energy Reviews,* vol. 120, p. 109628, 2020.
[146] G. J. C. Santos and P. R. da Silva Jota, "HVDC grid segmentation analysis for blackouts reduction," *J Journal of Power Energy Engineering,* vol. 5, no. 03, p. 36, 2017.
[147] H. Huang, Z. Xu, and X. Lin, "Improving performance of multi-infeed HVDC systems using grid dynamic segmentation technique based on fault current limiters," *IEEE Transactions on power systems,* vol. 27, no. 3, pp. 1664-1672, 2012.
[148] J. Yin, P. Sharma, I. Gorton, and B. Akyoli, "Large-scale data challenges in future power grids," in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*: IEEE, pp. 324-328.
[149] Q. Wang, M. Pipattanasomporn, M. Kuzlu, Y. Tang, Y. Li, and S. Rahman, "Framework for vulnerability assessment of communication systems for electric power grids," *IET Generation, Transmission Distribution,* vol. 10, no. 2, pp. 477-486, 2016.
[150] L. Martins, R. Girao-Silva, L. Jorge, A. Gomes, F. Musumeci, and J. Rak, "Interdependence between power grids and communication networks: A resilience perspective," in *DRCN 2017-Design of Reliable Communication Networks; 13th International Conference*: VDE, pp. 1-9.
[151] R. R. Vaz, R. A. Franco, H. P. Corrêa, F. H. Vieira, and S. G. Araújo, "Algorithms for selecting and interconnecting switches to automate power grids considering continuity indexes and reliability," *Journal of Control, Automation Electrical Systems,* vol. 30, no. 6, pp. 1059-1068, 2019.
[152] M. Bahrami, M. Fotuhi-Firuzabad, and H. Farzin, "Reliability evaluation of power grids considering integrity attacks against substation protective IEDs," *IEEE Transactions on Industrial Informatics,* vol. 16, no. 2, pp. 1035-1044, 2019.
[153] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-Physical Modeling and Cyber-Contingency Assessment of Hierarchical Control Systems," *IEEE Transactions on Smart Grid,* vol. 6, no. 5, pp. 2375-2385, 2015.
[154] B. Falahati and Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies," *IEEE Transactions on Smart Grid,* vol. 5, no. 4, pp. 1677-1685, 2014.
[155] K. Marashi, S. S. Sarvestani, and A. R. Hurson, "Consideration of cyber-physical interdependencies in reliability modeling of smart grids," *IEEE Transactions on Sustainable Computing,* vol. 3, no. 2, pp. 73-83, 2017.

[156] C. Neuman and K. Tan, "Mediating cyber and physical threat propagation in secure smart grid architectures," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 238-243.
[157] "Analysis of the Hydro-Québec System Blackout on April 18th 1988," May 30, 1988.
[158] D. U. J. E. I. S. Case and A. Center, "Analysis of the cyber attack on the Ukrainian power grid," vol. 388, 2016.
[159] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems," *IEEE Transactions on Smart Grid,* vol. 7, no. 5, pp. 2260-2272, 2016.
[160] S. Shao, M. Pipattanasomporn, and S. Rahman, "Challenges of PHEV penetration to the residential distribution network," in *2009 IEEE Power & Energy Society General Meeting*: IEEE, pp. 1-8.
[161] R. Godina, E. M. Rodrigues, J. C. Matias, and J. P. Catalão, "Smart electric vehicle charging scheduler for overloading prevention of an industry client power distribution transformer," *Applied Energy,* vol. 178, pp. 29-42, 2016.
[162] X. Yan, Y. Ozturk, Z. Hu, and Y. Song, "A review on price-driven residential demand response," *Renewable Sustainable Energy Reviews,* vol. 96, pp. 411-419, 2018.
[163] B. Parrish, P. Heptonstall, R. Gross, and B. K. Sovacool, "A systematic review of motivations, enablers and barriers for consumer engagement with residential demand response," *Energy Policy,* vol. 138, p. 111221, 2020.
[164] S. M. H. Ali, M. Lenzen, and J. Huang, "Shifting air-conditioner load in residential buildings: benefits for low-carbon integrated power grids," *IET Renewable Power Generation,* vol. 12, no. 11, pp. 1314-1323, 2018.
[165] Z. Luo, Z. Hu, Y. Song, Z. Xu, and H. Lu, "Optimal coordination of plug-in electric vehicles in power grids with cost-benefit analysis—Part I: Enabling techniques," *IEEE Transactions on Power Systems,* vol. 28, no. 4, pp. 3546-3555, 2013.
[166] H. Wang, S. Wang, and K. Shan, "Experimental study on the dynamics, quality and impacts of using variable-speed pumps in buildings for frequency regulation of smart power grids," *Energy,* vol. 199, p. 117406, 2020.
[167] A. Mohammad, R. Zamora, and T. T. Lie, "Integration of electric vehicles in the distribution network: A review of PV based electric vehicle modelling," *Energies,* vol. 13, no. 17, p. 4541, 2020.
[168] A. Zecchino, K. Knezović, and M. Marinelli, "Identification of conflicts between transmission and distribution system operators when acquiring ancillary services from electric vehicles," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*: IEEE, pp. 1-6.
[169] C. Niddodi, S. Lin, S. Mohan, and H. Zhu, "Secure integration of electric vehicles with the power grid," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*: IEEE, pp. 1-7.
[170] A. Bin-Halabi, A. Nouh, and M. Abouelela, "Remote detection and identification of illegal consumers in power grids," *IEEE Access,* vol. 7, pp. 71529-71540, 2019.
[171] K. Tierney and M. Bruneau, "Conceptualizing and measuring resilience: A key to disaster loss reduction," *TR news,* no. 250, 2007.
[172] M. Ouyang and L. Duenas-Osorio, "Time-dependent resilience assessment and improvement of urban infrastructure systems," *Chaos,* vol. 22, no. 3, p. 033122, 2012.
[173] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a Consensus on the Definition and Taxonomy of Power System Resilience," *IEEE Access,* vol. 6, pp. 32035-32053, 2018.
[174] R. Dantas, J. Liang, C. E. Ugalde-Loo, A. Adamczyk, C. Barker, and R. Whitehouse, "Progressive fault isolation and grid restoration strategy for MTDC networks," *IEEE Transactions on Power Delivery,* vol. 33, no. 2, pp. 909-918, 2017.
[175] S. N. Edib, Y. Lin, V. Vokkarane, F. Qiu, R. Yao, and D. Zhao, "PMU and Communication Infrastructure Restoration for Post-Attack Observability Recovery of Power Grids," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*: IEEE, pp. 1-6.
[176] E. Lu, N. Wang, Z. Qin, H. Liu, and Y. Hou, "Black-start strategy for power grids including fast cut thermal power units," in *2013 IEEE Power & Energy Society General Meeting*: IEEE, pp. 1-5.
[177] Y. Liu, R. Fan, and V. Terzija, "Power system restoration: a literature review from 2006 to 2016," *Journal of Modern Power Systems Clean Energy,* vol. 4, no. 3, pp. 332-341, 2016.
[178] D. Fan, Y. Ren, Q. Feng, Y. Liu, Z. Wang, and J. Lin, "Restoration of smart grids: Current status, challenges, and opportunities," *Renewable Sustainable Energy Reviews,* vol. 143, p. 110909, 2021.
[179] D. Sharma, C. Lin, X. Luo, D. Wu, K. Thulasiraman, and J. N. Jiang, "Advanced techniques of power system restoration and practical applications in transmission grids," *Electric Power Systems Research,* vol. 182, p. 106238, 2020.
[180] Y. Ren, D. Fan, Q. Feng, Z. Wang, B. Sun, and D. Yang, "Agent-based restoration approach for reliability with load balancing on smart grids," *Applied energy,* vol. 249, pp. 46-57, 2019.
[181] D. Ye, M. Zhang, and D. Sutanto, "A hybrid multiagent framework with Q-learning for power grid systems restoration," *IEEE Transactions on Power Systems,* vol. 26, no. 4, pp. 2434-2441, 2011.
[182] Y. Zhang, J. Wu, Z. Chen, Y. Huang, and Z. Zheng, "Sequential node/link recovery strategy of power grids based on q-learning approach," in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*: IEEE, pp. 1-5.
[183] R. B. Duffey and T. J. I. T. o. p. S. Ha, "The probability and timing of power system restoration," *IEEE Transactions on power Systems,* vol. 28, no. 1, pp. 3-9, 2012.
[184] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures," *IEEE Trans. Power Syst.,* vol. 32, no. 5, pp. 3747-3757, 2017.
[185] N. Bhusal, M. Abdelmalak, M. Kamruzzaman, and M. Benidris, "Power System Resilience: Current Practices, Challenges, and Future Directions," *IEEE Access,* vol. 8, pp. 18064-18086, 2020.
[186] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews,* vol. 58, pp. 1060-1069, 2016.
[187] M. Panteli and P. Mancarella, "Influence of extreme weather and climate change on the resilience of power systems: Impacts and possible mitigation strategies," *Electric Power Systems Research,* vol. 127, pp. 259-270, 2015.
[188] W. Li, *Reliability assessment of electric power systems using Monte Carlo methods*. Springer Science & Business Media, 2013.
[189] M. A. Mohamed, T. Chen, W. Su, and T. Jin, "Proactive Resilience of Power Systems Against Natural Disasters: A Literature Review," *IEEE Access,* vol. 7, pp. 163778-163795, 2019.
[190] E. Brugnetti, G. Coletta, F. De Caro, A. Vaccaro, and D. Villacci, "Enabling Methodologies for Predictive Power System Resilience Analysis in the Presence of Extreme Wind Gusts," *Energies,* vol. 13, no. 13, 2020.
[191] C. D. Zamuda, P. H. Larsen, M. T. Collins, S. Bieler, J. Schellenberg, and S. Hees, "Monetization methods for evaluating investments in electricity system resilience to extreme weather and climate change," *The Electricity Journal,* vol. 32, no. 9, 2019.
[192] Y. Fang and G. Sansavini, "Optimizing power system investments and resilience against attacks," *Reliability Eng. Syst. Safety,* vol. 159, pp. 161-173, 2017.
[193] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked Microgrids for Enhancing the Power System Resilience," *Proceedings of the IEEE,* vol. 105, no. 7, pp. 1289-1310, 2017.
[194] H. Farzin, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing Power System Resilience Through Hierarchical Outage Management in Multi-Microgrids," *IEEE Trans. Smart Grid,* vol. 7, no. 6, pp. 2869-2879, 2016.
[195] T. Ding, Y. Lin, Z. Bie, and C. Chen, "A resilient microgrid formation strategy for load restoration considering master-slave

distributed generators and topology reconfiguration," *Applied Energy,* vol. 199, pp. 205-216, 2017.

[196] B. Chen, J. Wang, X. Lu, C. Chen, and S. Zhao, "Networked microgrids for grid resilience, robustness, and efficiency: a review," *IEEE Trans. Smart Grid,* 2020.

[197] R. Eskandarpour, H. Lotfi, and A. Khodaei, "Optimal microgrid placement for enhancing power system resilience in response to weather events," in *North American Power Symposium (NAPS)*, pp. 1-6.

[198] J. Wang, N. Xie, W. Wu, D. Han, C. Wang, and B. Zhu, "Resilience enhancement strategy using microgrids in distribution network," *Global Energy Interconnection,* vol. 1, no. 5, pp. 537-543, 2018.

[199] A. Hussain, V.-H. Bui, and H.-M. Kim, "Microgrids as a resilience resource and strategies used by microgrids for enhancing resilience," *Applied energy,* vol. 240, pp. 56-72, 2019.

[200] J. Xie, I. Alvarez-Fernandez, and W. Sun, "A Review of Machine Learning Applications in Power System Resilience," in *IEEE Power & Energy Society General Meeting*, pp. 1-5.

[201] C. Nauck, "Prediction of Power Grid Vulnerabilities using Machine Learning," Master's thesis, RWTH Aachen University, 2020.

[202] H. Sun, Z. Wang, J. Wang, Z. Huang, N. Carrington, and J. J. I. T. o. S. G. Liao, "Data-driven power outage detection by social sensors," vol. 7, no. 5, pp. 2516-2524, 2016.

[203] R. Eskandarpour and A. J. I. T. o. P. S. Khodaei, "Leveraging accuracy-uncertainty tradeoff in SVM to achieve highly accurate outage predictions," *IEEE Trans. Power Syst.,* vol. 33, no. 1, pp. 1139-1141, 2017.

[204] R. Eskandarpour, A. Khodaei, A. Paaso, and N. Abdullah, "Artificial Intelligence Assisted Power Grid Hardening in Response to Extreme Weather Events," *arXiv:.02866,* 2018.

[205] C. Haseltine and E. E.-S. Eman, "Prediction of power grid failure using neural network learning," in *IEEE Int. Conf. on Machine Learning and Applications*, pp. 505-510.

[206] A. Jaech, B. Zhang, M. Ostendorf, and D. S. J. I. T. o. P. S. Kirschen, "Real-time prediction of the duration of distribution system outages," *IEEE Trans. Power Syst.,* vol. 34, no. 1, pp. 773-781, 2018.

[207] M. A. Karim, J. Currie, and T.-T. Lie, "Distributed Machine Learning on Dynamic Power System Data Features to Improve Resiliency for the Purpose of Self-Healing," *Energies,* vol. 13, no. 13, p. 3494, 2020.

[208] M. H. Amini, A. Imteaj, and J. Mohammadi, "Distributed Machine Learning for Resilient Operation of Electric Systems," in *IEEE Int. Conf. Smart Energy Syst. Tech.*, pp. 1-6.

[209] B. Zohuri and F. M. Rahmani, "Artificial Intelligence Driven Resiliency with Machine Learning and Deep Learning Components," *Int. J. Nanotechnology Nanomedicine,* vol. 4, no. 2, pp. 1-8, 2019.

[210] L. E. Cole, S. A. Bhagwat, and K. Willis, "Recovery and resilience of tropical forests after disturbance," *Nature communications,* vol. 5, no. 1, pp. 1-7, 2014.

[211] B. Cai, M. Xie, Y. Liu, Y. Liu, and Q. Feng, "Availability-based engineering resilience metric and its corresponding evaluation methodology," *Reliability Engineering & System Safety,* vol. 172, pp. 216-224, 2018/04/01/ 2018.

[212] S. Chanda, A. K. Srivastava, M. U. Mohanpurkar, and R. Hovsapian, "Quantifying power distribution system resiliency using code-based metric," *IEEE Transactions on Industry Applications,* vol. 54, no. 4, pp. 3676-3686, 2018.

[213] "Load Flow Analysis," in *Modern Power Systems Analysis*. Boston, MA: Springer US, 2008, pp. 71-128.

[214] H. Saadat, *Power system analysis*. McGraw-Hill, 1999.

[215] H. Seifi and M. S. Sepasian, *Electric power system planning: issues, algorithms and solutions*. Springer Science & Business Media, 2011.

[216] J. Yan, Y. Tang, Y. Zhu, H. He, and Y. Sun, "Smart Grid Vulnerability under Cascade-Based Sequential Line-Switching Attacks," in *IEEE Glob. Comm. Conf. (GLOBECOM)*, pp. 1-7.

[217] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization," *Chaos,* vol. 17, no. 2, p. 026103, 2007.

[218] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *Int. J. Elec. Power Energy Syst.,* vol. 28, no. 9, pp. 627-633, 2006.

[219] J. Dopazo, O. Klitin, and A. Sasson, "Stochastic load flows," *IEEE Trans. Power App. Syst.,* vol. 94, no. 2, pp. 299-309, 1975.

[220] B. Marah and A. Ekwue, "Probabilistic load flows," in *Int. Universities Power Eng. Conf.*: IEEE, pp. 1-6.

[221] J. Ma, Z. Huang, P. C. Wong, and T. Ferryman, "Probabilistic vulnerability assessment based on power flow and voltage distribution," in *IEEE PES T&D 2010*, pp. 1-8.

[222] P. Zhang and S. Lee, "Probabilistic load flow computation using the method of combined cumulants and Gram-Charlier expansion," *IEEE Trans. power syst.,* vol. 19, no. 1, pp. 676-682, 2004.

[223] S. Han, Z. Peng, and S. Wang, "The maximum flow problem of uncertain network," *Inf. Sciences,* vol. 265, pp. 167-175, 2014.

[224] V. K. Balakrishnan, *Schaum's outline of theory and problems of graph theory*. McGraw-Hill, 1997.

[225] A. Dwivedi and X. Yu, "A Maximum-Flow-Based Complex Network Approach for Power System Vulnerability Analysis," *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 81-88, 2013.

[226] W. Fan, S. Huang, and S. Mei, "Invulnerability of power grids based on maximum flow theory," *Physica A,* vol. 462, pp. 977-985, 2016.

[227] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, "Power System Structural Vulnerability Assessment Based on an Improved Maximum Flow Approach," *IEEE Trans. Smart Grid,* vol. 9, no. 2, pp. 777-785, 2018.

[228] A. Dwivedi, X. Yu, and P. Sokolowski, "Analyzing power network vulnerability with maximum flow based centrality approach," in *IEEE Int. Conf. Indust. Informatics*, pp. 336-341.

[229] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?," *Chaos,* vol. 20, no. 3, p. 033122, 2010.

[230] X. Zhang and C. K. Tse, "Assessment of Robustness of Power Systems From a Network Perspective," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.,* vol. 5, no. 3, pp. 456-464, 2015.

[231] Re´ka Albert, Hawoong Jeong, and A.-L. s. Baraba´si, "Error and attack tolerance of complex networks," *Nature,* vol. 406, p. 5, 2000.

[232] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," *Physical review letters,* vol. 85, no. 21, p. 4626, 2000.

[233] A. E. Motter, T. Nishikawa, and Y.-C. Lai, "Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon?," *Phys. Rev. E,* vol. 66, no. 6, p. 065103, 2002.

[234] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Phys Rev E,* vol. 69, no. 2 Pt 2, p. 025103, Feb 2004.

[235] G. Chen, Z. Y. Dong, D. J. Hill, and G. H. Zhang, "An improved model for structural vulnerability analysis of power networks," *Physica A,* vol. 388, no. 19, pp. 4259-4266, 2009.

[236] A. B. M. Nasiruzzaman and H. R. Pota, "Transient stability assessment of smart power system using complex networks framework," in *IEEE Power and Energy Society General Meeting*, pp. 1-7.

[237] P. Crucitti, V. Latora, M. Marchoori, and A. Raposarda, "Efficiency of scale-free networks: error and attack tolerance," *Physica A,* vol. 320, pp. 622-642, 2003.

[238] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys Rev Lett,* vol. 87, no. 19, p. 198701, 2001.

[239] H. Zhao and Z. Y. Gao, "Cascade defense via navigation in scale free networks," *Eur. Phys. J. B,* vol. 57, no. 1, pp. 95-101, 2007.

[240] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys Rev E,* vol. 69, no. 4 Pt 2, p. 045104, Apr 2004.

[241] H. Bai and S. Miao, "Hybrid flow betweenness approach for identification of vulnerable line in power system," *IET Gen. Trans. Dist.,* vol. 9, no. 12, pp. 1324-1331, 2015.

[242] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A,* vol. 340, no. 1-3, pp. 388-394, 2004.

[243] J.-W. Wang and L.-L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Safety Science,* vol. 49, no. 6, pp. 807-812, 2011.
[244] J. Ash and D. Newth, "Optimizing complex networks for resilience against cascading failure," *Physica A,* vol. 380, pp. 673-683, 2007.
[245] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A,* vol. 389, no. 3, pp. 595-603, 2010.
[246] Y. Cao, Y. Li, X. Liu, and C. Rehtanz, "Modeling and Analysis Techniques of Interdependent Network," in *Cyber-Physical Energy and Power Systems: Modeling, Analysis and Application*. Singapore: Springer Singapore, 2020, pp. 17-35.
[247] E. Estrada and J. A. Rodriguez-Velazquez, "Subgraph centrality in complex networks," *Phys. Rev. E,* vol. 71, no. 5, p. 056103, 2005.
[248] M. Jalili and M. Perc, "Information cascades in complex networks," *J. Complex Net.,* vol. 5, no. 5, pp. 665-693, 2017.
[249] Z. Wang, A. Scaglione, and R. J. Thomas, "The node degree distribution in power grid and its topology robustness under random and selective node removals," in *IEEE Int. Conf. Comm. Workshops*, pp. 1-5.
[250] M. E. Newman, "The mathematics of networks," vol. 2, pp. 1-12, 2008.
[251] M. E. Newman, *Networks: An Introduction.* Oxford University Press., 2010.
[252] P. Chopade and M. J. I. J. o. C. I. P. Bikdash, "New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts," *Int. J. Critical Infrastructure Protection,* vol. 12, pp. 29-45, 2016.
[253] P. J. Górski, K. Kułakowski, P. Gawroński, and J. A. Hołyst, "Destructive influence of interlayer coupling on Heider balance in bilayer networks," *Scientific reports,* vol. 7, no. 1, pp. 1-12, 2017.
[254] A. Moradi Amani, M. Jalili, X. Yu, and L. Stone, "Controllability of complex networks: Choosing the best driver set," *Phys. Rev. E,* vol. 98, no. 3, p. 030302, 2018.
[255] M.-Y. Zhou, R.-Q. Xu, X.-Y. Li, and H. Liao, "Identifying influential nodes to enlarge the coupling range of pinning controllability," *J. Statistical Mechanics,* vol. 2020, no. 9, p. 093401, 2020.
[256] F. Sorrentino, M. di Bernardo, F. Garofalo, and G. Chen, "Controllability of complex networks via pinning," *Physical Review E,* vol. 75, no. 4, p. 046103, 2007.
[257] N. Gaeini, A. M. Amani, M. Jalili, X. J. I. J. o. E. P. Yu, and E. Systems, "Cooperative secondary frequency control of distributed generation: The role of data communication network topology," vol. 92, pp. 221-229, 2017.
[258] F. Sorrentino, "Effects of the network structural properties on its controllability," *Chaos: An Interdisciplinary Journal of Nonlinear Science,* vol. 17, no. 3, p. 033101, 2007.
[259] A. Nasiruzzaman, H. Pota, and M. Mahmud, "Application of centrality measures of complex network framework in power grid," in *Annual Conf. IEEE Ind. Elec. Society (IECON)*, pp. 4660-4665.
[260] Y. Koç, M. Warnier, R. E. Kooij, and F. M. T. Brazier, "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety Science,* vol. 59, pp. 126-134, 2013.
[261] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Physica A,* vol. 396, pp. 204-211, 2014.
[262] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Elec. Power Syst. Research,* vol. 101, pp. 71-79, 2013.
[263] Y.-j. Cao, X.-g. Chen, and K. Sun, "Identification of vulnerable lines in power grid based on complex network theory," *Electric power automation equipment,* vol. 26, no. 12, pp. 1-5, 2006.
[264] F. Wenli, Z. Xuemin, M. Shengwei, H. Shaowei, W. Wei, and D. Lijie, "Vulnerable transmission line identification using ISH theory in power grids," *IET Gen. Trans. Dist.,* vol. 12, no. 4, pp. 1014-1020, 2017.
[265] L. C. Freeman, "A Set of Measures of Centrality Based on Betweenness," *Sociometry,* vol. 40, no. 1, pp. 35-41, 1977.
[266] E. Bompard, E. Pons, and W. Di, "Extended Topological Metrics for the Analysis of Power Grid Vulnerability," *IEEE Syst. J.,* vol. 6, no. 3, pp. 481-487, 2012.
[267] K. Wang, B.-h. Zhang, Z. Zhang, X.-g. Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A,* vol. 390, no. 23-24, pp. 4692-4701, 2011.
[268] Z. Wang, A. Scaglione, and R. J. Thomas, "Electrical centrality measures for electric power grid vulnerability analysis," presented at the IEEE Conf. Decision Control, USA, 2010.
[269] J. Yan, H. He, and Y. Sun, "Integrated Security Analysis on Cascading Failure in Complex Networks," *IEEE Trans. Inf. Forensics Security,* vol. 9, no. 3, pp. 451-463, 2014.
[270] B. Liu, Z. Li, X. Chen, Y. Huang, and X. Liu, "Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality," *IEEE Trans. Circuits Syst. II, Exp. Briefs,* vol. 65, no. 3, pp. 346-350, 2018.
[271] C. Wu *et al.*, "Evaluation of Buses in Power Grids by Extended Entropic Degree," in *37th Chinese Control Conference*, Wuhan.
[272] R. Fang, R. Shang, Y. Wang, and X. Guo, "Identification of vulnerable lines in power grids with wind power integration based on a weighted entropy analysis method," *Int. J. Hydrogen Energy,* vol. 42, no. 31, pp. 20269-20276, 2017.
[273] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. power syst.,* vol. 26, no. 1, pp. 12-19, 2010.
[274] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Trans. power systems,* vol. 32, no. 4, pp. 3258-3265, 2016.
[275] C. Josz, S. Fliscounakis, J. Maeght, and P. J. a. p. a. Panciatici, "AC power flow data in MATPOWER and QCQP format: iTesla, RTE snapshots, and PEGASE," 2016.
[276] S. Fliscounakis, P. Panciatici, F. Capitanescu, and L. Wehenkel, "Contingency ranking with respect to overloads in very large power systems taking into account uncertainty, preventive, and corrective actions," *IEEE Trans. Power Systems,* vol. 28, no. 4, pp. 4909-4917, 2013.

Ali Moradi Amani (M'16) has completed graduate and post-graduate studies all in Electrical Engineering (control systems). He is now with the School of Engineering at RMIT University, Melbourne, Australia. His research interests include control of complex networks, fault tolerant control systems, and stability and control of future power systems.

Mahdi Jalili (M'09–SM'16) received the Ph.D. degree in computer and communications sciences from the Swiss Federal Institute of Technology Lausanne, Lausanne, Switzerland, in 2008. He was an Assistant Professor with the Sharif University of Technology, Tehran, Iran. He is currently an associate professor with the School of Engineering, RMIT University. He was an Australian Research Council DECRA Fellow and an RMIT Vice-Chancellor Research Fellow. His current research interests include network science and dynamical systems.