IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 5, 2019, accepted December 19, 2019, date of publication December 25, 2019, date of current version January 6, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2962139

A MDP-Based Vulnerability Analysis of Power Networks Considering Network Topology and Transmission Capacity

CLAUDIA CARO-RUIZ[1,3], (Member, IEEE), AMEENA SAAD AL-SUMAITI[2], SERGIO RIVERA[3], (Senior Member, IEEE), AND EDUARDO MOJICA-NAVA[3], (Member, IEEE)

[1]Department of Electronic Engineering, Universidad Manuela Beltrán, Bogotá 110231, Colombia
[2]Advanced Power and Energy Center, Electrical Engineering and Computer Science Department, Khalifa University, Abu Dhabi, United Arab Emirates
[3]Department of Electrical and Electronic Engineering, Universidad Nacional de Colombia, Bogotá 111321, Colombia

Corresponding author: Claudia Caro-Ruiz (clccaroru@unal.edu.co)

This work was supported in part by the Universidad Nacional de Colombia and Colciencias (Departamento Administrativo de Ciencia, Tecnologia e Innovacion) under Grant 647-2014, and in part by the Khalifa University under Award FSU-2018-25.

ABSTRACT This paper aims to study the vulnerability of the network to sequential cascading failures attacks where the attack strategy integrates network theory and discounted reward with Markov decision process (MDP) in the target selection process. A control strategy is designed to maximize the attack's long-term expected reward while reducing the attack sequence duration. The attack model identifies the most suitable targets by prediction through a Markov process for predicting the propagation and consequences of the failure. The state transition probabilities through a hidden failure model embedded in an independent edge-dependent network evolution model is estimated. Value iteration algorithms are used to identify targets at every attack stage. Target selection is updated depending on network changes. The results provide an optimal attack strategy based on network congestion with maximum damage, considering congestion as a cascade propagation mechanism. Reward functions based on increasing congestion and immediate power loss are compared. Strategies designed with network congestion as the attack reward function produce more vulnerability of the network to sequential attacks.

INDEX TERMS Cascading failures, complex networks, Markov decision process, network congestion, system vulnerability, transmission capacity.

I. INTRODUCTION

As power grids expand and integrate new technologies, their ability to respond and recover from hazards events plays a major role in system planning and operation. Models for anticipating adverse events, as well as their immediate and long-term resulting consequences, are required to assess the extent to which the network is prepared for the threats it faces [1]. In this context, three main issues have gained considerable interest: network-based vulnerability analysis [2]–[5], cascading failures [6]–[8], and the power network robustness to attacks [9], [10].

Vulnerability analysis frameworks integrating cascading failures and attacks have been proposed in the literature. Game theory [11] and stochastic games combined with machine learning methods are used to propose the vulnerability assessment frameworks [9]. In [12], a similar approach is presented to assess the vulnerability in cyber-physical systems. Optimization approaches based on N-K contingency are used in [13] to identify the operational conditions affecting the vulnerability of the network to cascading failures. An attack strategy under limited network information is introduced in [14]. All these approaches integrated attacks with cascading failures into a vulnerability analysis framework. However, the network properties and their influence on the vulnerability are not considered. Network structural vulnerability is roughly related to the fraction of the elements affected (from failures or external attacks) required to produce cascading failures.

For the external adversary, the finding of such a set of fragile components whose removal would cause severe damage to the network would be rather valuable [10]. For a network

The associate editor coordinating the review of this manuscript and approving it for publication was Ziang Zhang.

operator, the information about this set of elements at risk and the set relation to network topological properties would serve to plan effective strategies that enhance the network resilience [15], [16]. In this way, when this small number of elements is attacked, network vulnerability in terms of cascading failures is revealed. An alternative to identify these elements and obtain an efficient attack can be formulted by combining electric and network properties into the metrics for the identification of critical elements.

In particular, the problem of vulnerability to sequential attacks can offer beneficial information about how sensible the network is to the influence of a sophisticated adversary able to assess and select the best target sequence to affect the network [17]. The sequential attack can be described as the removal of multiple elements in the network at different time stages. Targets could be nodes [18], edges [19], or a combination of both. The main issue on the attack strategy is the selection of the appropriate targets and the corresponding sequence of disturbances to be applied. Electrical and topological metrics are used in the literature to identify targets [17]; however, most of the works are related to single-stage attacks [20]. For sequential attacks, properties such as degree distribution [18] and cut-sets [21] are used. Electrical properties such as power flow, load, and generation placement are also used to identify elements to be attacked according to their relevance in operation [22]. More sophisticated strategies try to optimize the target selection to maximize the reward obtained by the attacker. Random search and learning algorithms are used to identify the optimal attack [23], but information for estimating failure probabilities and transitions between states seems to be usually approximated without the use of a specific criterion. In addition, topological information on the network evolution and congestion estimation due to this process can be used to estimate and to identify the target elements that seem to produce more vulnerability of the network to target attacks [20], [21].

This paper proposes a different view of the vulnerability of the network to sequential attacks. It integrates network theory and discounted reward with Markov decision processes in the model of sequential attacks. A strategy is designed to maximize the attack's long-term expected reward while reducing the attack sequence duration. The attack model identifies the most suitable targets by using a Markov process to predict the propagation and consequences of the failure. The state transition probabilities is estimated through a hidden failure model embedded in an independent edge-dependent network evolution model. As long as the network configuration varies in time as a consequence of network attacks and cascading failures, value iteration algorithms are used to identify targets at every attack stage. Targets are updated depending on network configuration at each step of the attack sequence. The results provide an optimal attack strategy with the maximum damage, considering congestion as a cascade propagation mechanism. A case study is evaluated for two different damage metrics: power loss and flow congestion. The results show that the network is more vulnerable when the failure estimation is related to a network structure and flow congestion than a single power loss. On the other hand, target control of the transmission capacity of some selected elements can reduce the vulnerability of the network to sequential attacks.

The paper is organized as follows: Section II presents the system model and attacker model. Section IV develops the sequential attack problem, including failure probability estimation and target selection. Section V presents the Markov decision process designed to obtain the solution to the problem of the sequential attack. A case study of an IEEE 30-bus test system with different attack scenarios is analyzed in Section VI. The conclusions and recommendations on future research are provided in Section VII.

II. SYSTEM MODEL

The power system is modeled as a flow graph $\mathcal{G}$ as follows:

$$\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathbf{c}), \tag{1}$$

where the node set $\mathcal{V}$, with cardinality $|\mathcal{V}| = n$, represents the power system buses and the edge set $\mathcal{E}$, with cardinality $|\mathcal{E}| = m$, represents the transmission lines. In addition, $\mathbf{c}^t \in \mathbb{R}^m$ is a vector with edge transmission capacities. This model equates capacities with edge weights. Parallel circuits between buses are represented by a single edge with the sum of their respective capacities. For the power network in (1), let $\mathcal{V}_s \subset \mathcal{V}$ be the set of supply nodes and let $\mathcal{V}_d \subset \mathcal{V} \setminus \mathcal{V}_s$ be the set of demand nodes in the network. Transmission nodes without supply or demand are $\mathcal{V}_b \subset \mathcal{V}$. Consider a node associated with supply/demand vector $\mathbf{p}$ where $\mathbf{p} \in \mathbb{R}^n$; $p_v > 0$ for $v \in \mathcal{V}_s$, $p_v < 0$ for $v \in \mathcal{V}_d$, and $p_v = 0$ for $v \in \mathcal{V}_b$ and $\sum_{v \in \mathcal{V}} p_v = 0$.

Also consider a flow vector $\mathbf{f} \in \mathbb{R}^m$ where f_e is the flow at edge e and meets capacity constraint $|f_e| < c_e$ on every link $e \in \mathcal{E}$ and flow conservation $\sum_{e \in \mathcal{E}_v} f_e = p_v$ for every node v, where $\mathcal{E}_v \subseteq \mathcal{E}$ is the set of all incident edges to the node v. The vector flow $\mathbf{f}$ is defined by a routing policy Ξ. The routing policy defines the magnitude and direction of every edge flow in the network. Consider a linear routing policy such that

$$\mathbf{f} = \Xi \mathbf{p}, \tag{2}$$

where Ξ is an $m \times n$ matrix. The matrix Ξ maps the supply/demand profile $\mathbf{p}$ into the power flows going through each edge. The flow routing will depend on the electric and topological properties of the power system. In this study, a routing policy based on the DC power flow is used.

Consider the power system modeled as a flow network in (1) with supply/demand vector $\mathbf{p}$ and flows in (2) evolving in time. Let $\mathcal{G}^t = (\mathcal{V}^t, \mathcal{E}^t, \mathbf{c}^t)$ and $\mathbf{f}^t$ describe the state of the system at every time $t = 0, 1, \ldots$, where $\mathcal{V}^t \subseteq \mathcal{V}$ and $\mathcal{E}^t \subseteq \mathcal{E}$ are the active nodes and links at time t [24].

For the initial condition of the system $\left(\mathcal{G}^0, \mathbf{f}^0\right)$, all the elements of the node and edge set start active, i.e., $\mathcal{V}^0 = \mathcal{V}$, $\mathcal{E}^0 = \mathcal{E}$, and $\mathbf{f}^0$ is the initial flow. At every time t, the network $\mathcal{G}^t$ should be connected. Define $\hat{\mathcal{G}}^t$ as the largest connected

component in $\mathcal{G}^t$ and $\hat{\mathcal{G}}^0 \equiv \mathcal{G}^0$. The largest connected component of the network refers to the biggest connected part of the entire set of nodes where a feasible flow exists. Considering the largest connected component, we are modeling the network in its natural dynamical behavior. Edge disconnection produced by cascade propagation may generate uncontrolled component islanding. Uncontrolled islanding or redispatch is considered during the cascade propagation. In this way, the small connected components could have only load nodes or unbalanced supply-demand nodes that collapse during the cascade evolution.

Attack-defender threat models could include controlled actions, but defender actions are out of the scope of this model. The network changes its state as follows. Edges become overloaded when their current flow exceeds the transmission capacity. All the overloaded edges are disconnected along with all the edges in small subcomponents isolated from the largest connected component, $\hat{\mathcal{G}}^t$.

Next, all active nodes v that have no incident edges, along with all those not included in the large connected component become inactive.

In addition, the capacity vector $\mathbf{c}^t$ is changed by a disturbance $\delta^t \in \mathbb{R}^m$:

$$c_e^{t+1} = c_e^t - \delta^t, \quad e \in \mathcal{E}^t. \tag{3}$$

Disturbance δ^t is defined according to the selected attack strategy. The initial equilibrium flows $\mathbf{f}^0$ are generated by the given routing policy. The network state does not change as long as $\delta^t = 0$. The initial line transmission capacity $\mathbf{c}^0$ is defined by $\mathbf{c}^0 = \alpha \mathbf{f}^0$, where α is a tolerance parameter and $\alpha \geq 1$.

III. ATTACKER MODEL

The model assumes a single intruder threatening the network. The attack is repeated in time; for every stage the attacker has to choose an element e to attack thereby producing a disturbance in the network. Consider the sequence $\Delta =: (\delta^1, \delta^2, ...)$ of progressive disturbances representing the external adversary intervention against the power network. At each stage, the disturbance δ^t is modeled by $\delta^t = \Gamma^t \mathbf{c}^t$, where Γ^t is an $m \times m$ matrix and $\Gamma^t = \text{diag}\,(\gamma_1, \gamma_2, \ldots, \gamma_m)$. Disturbance δ^t is applied in (3) simulating the loss of line transmission capacity or a severe transmission damage by defining the element γ_e^t as follows:

$$\gamma_e^t = \begin{cases} 1, & \text{if edge } e \text{ is attacked;} \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

$\mathcal{D}$ refers to the set of all the feasible attack sequences possible in the network. The attacker problem is discussed in the following section and related to how to select elements e to be attacked at every stage.

IV. PROBLEM FORMULATION

Most of the approaches consider an attacker that selects its targets according to a reward function $S(e, \hat{\mathcal{G}})$ that depends on the targets e selected at every stage t when the network configuration is $\hat{\mathcal{G}}$. The reward function measures the damage that can be obtained from the attack at stage t. Different approaches can be used to define the reward obtained by the attacker. This function represents an immediate reward and can be useful to select targets when one single-stage attack is performed. For sequential target attack case, a long-term reward function is a better approach to obtain an adequate selection of targets. In addition, rewards of attacks' actions at different stages of the attack will not have the same impact on the system. Then, the time preference in a long-term reward, assuming that future rewards are discounted at some rate, can be modeled by a rate of discount $\beta \in (0, 1]$, whose value discounts the value of the damage produced by the attack depending on the time stage at which this occurrs. Then, the long-term reward for the attack sequence is defined by (5):

$$\sum_{t=0}^{\infty} \beta^t E[S(e, \hat{\mathcal{G}})]. \tag{5}$$

A strategy that can trigger blackouts with a minimum of sequential attacks is studied herein. This strategy is accomplished by increasing the estimated risk of the network cascading failures. For a given set of attacks' actions, a defined supply/demand, network topology, and flow routing strategy over an infinite horizon, the optimal sequence of attacks that maximizes the damage triggered by the attack with the minimum number of attacks is given by the optimization problem in (6):

$$\max_{e^1, \ldots, e^t} \sum_{t=0}^{\infty} \beta^t E[S(e^t, \hat{\mathcal{G}})], \quad e^t \in \mathcal{E}^t, \tag{6}$$

for e^t being the edge selected for the attacker to attack at stage t. The risk is higher if the damage of the networks during the first attacks is stronger. Maximizing the risk estimation metric included in the cumulative sum of the objective function and discounted by the rate of discount β implies an efficient attack where the targets are selected to increase the damage and to trigger the propagation of failures thereby reducing the number of attacks required. The severity of the attack depends not only on its duration but also on the risk of producing cascading failures at each stage. As is evident in the previous results, if the attacker manages to increase the cascading failure risk as soon as possible by using a precisely formulated attack sequence, it can cause very fast and significant damage to the network. To cause a significant impact, the attack's magnitude and damage should be optimized at the same time. In this way, the solution of the optimization problem in (6) must achieve a balance between the attack's magnitude and the damage. A Markov Decision Process (MDP) approach is proposed in the following section as a method to solve the optimization problem in (6) [25].

The long-term expected reward function should be defined in order to select the best targets for the attack. First, we define

a function for estimating the risk of cascading failures due to the attack of a specific target e in terms of the hidden failures model and the independent edge dependent model for the transition probability function. Attack severity is estimated by calculating the damage of the cascading failures produced by the attack targeted. Two different measures for the severity of the attack are proposed. First, the power loss produced by the cascading propagation triggered by the attack and another defined in terms of the network congestion produced by the attack. Both measures are also defined in the following subsection.

A. RISK ESTIMATION

A standard model of the failure estimation due to the network congestion is the hidden failures model [15]. In this model the function $\omega(e)$ is the probability of failure for an edge e. This probability changes depending on the capacity limits for each edge and the power flow routed along the edge. If power flow is close to the capacity limits, probability of failure is higher than probability for edges with power flow far from capacity limits.

A rising function of the power flow on edge e models the failure probability function for each edge in the network, as shown in (7),

$$\omega(e) = \begin{cases} 1 & \text{for } f_e^t \geq \alpha f_e^0 \\ \dfrac{1}{f_e^0(\alpha - 1)} f_e^t & \text{for } f_e^0 \leq f_e^t \leq \alpha f_e^0 \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

Fig. 1 shows the failure probability function. Initially, the probability is below the line security limit and changes linearly to one when the edge flow is α times of the security limit.

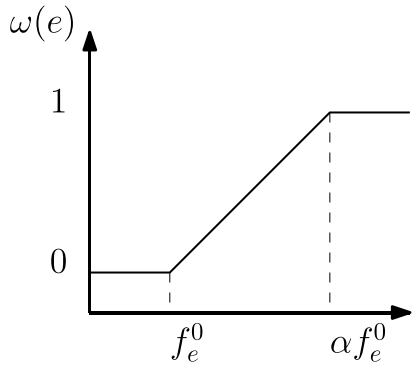

FIGURE 1. The probability distribution of an edge tripping by a cascading failure propagation effect.

Probability $\omega(e)$ defines the chance to obtain a failure in the edge but does not consider the probability of failure related to previous exogenous failures or attack events. To estimate the risk of edge lost triggered by neighboring edges' contingency during attacks, an independent edge-dependent network evolution model based in [26] is proposed. Assume that a random process governs the failure of each individual edge and it independent of all the other edges, i.e. $Pr(e_1 \cap e_j) = Pr(e_i)Pr(e_j) = \omega(e_i)\omega(e_j)$. The function $\omega(e)$ denotes the probability that any edge e, which is part of the network at time t, will be removed over the next time step as a result of cascade propagation. Let $P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}})$ denote the probability that $\hat{\mathcal{G}}_{j+1} = \hat{\mathcal{G}}'$ given that $\hat{\mathcal{G}}_j = \hat{\mathcal{G}}$, for any pair $\hat{\mathcal{G}}, \hat{\mathcal{G}}'$. Then, the independent edge-dependent model allows the graph-to-graph transition probability in (8):

$$P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) = \prod_{e \notin \mathcal{E}', e \in \mathcal{E}} \omega(e) \prod_{e \in \mathcal{E}', e \in \mathcal{E}} (1 - \omega(e)). \tag{8}$$

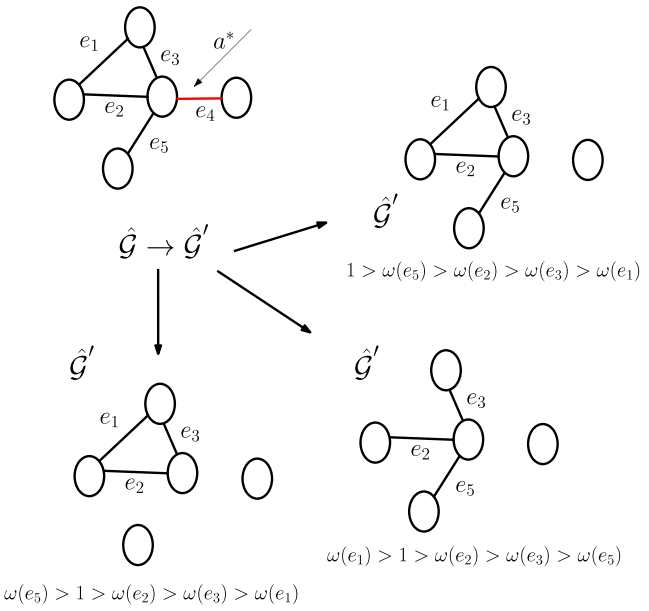

FIGURE 2. Depending on the selected target, the network will evolve to a new state with an independent probability related to the hidden failures model in (7).

At the beginning, all the network edges are active, and there are no failures produced by the attacker. Then, when the attacker chooses an edge to attack e^*, the power network probability to move to another state, where the edge e^* and the other edges e are down, is $P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}})$. Fig. 2 explains how the transition probability $P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}})$ between the same states are different depending on the action taken by the attacker at stage $\hat{\mathcal{G}}$ and the power flow routed through each edge, network topology, and trigger event. Considers the network in the state $\hat{\mathcal{G}}$, where an action a^* is taken by the attacker. After the action, the network evolves to a state where edge e_4 and other edges are disconnected. The transition to the new state depends on the power flow in the edges, probability $\omega(e)$, and at the same time, it depends on flow saturation of the edges. If a new power flow value is far from its limits in all the edges, the probability of transition is going to be lower than probability in cases where other edges are in its capacity limits and produce a probability $\omega(e) = 1$. In this way, transition probability depends directly on the topology and the power flow conditions after the action a^* is applied. It is also defined $S(e^*, \hat{\mathcal{G}})$ as a measure of severity of the

failures proceeding from an arbitrary attack e^* to the network at a particular state $\hat{\mathcal{G}}$. Then, the risk of the cascading failure due to attack the edge e^* is

$$R(e^*, \hat{\mathcal{G}}) = P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) S(e^*, \hat{\mathcal{G}}). \tag{9}$$

Consider $\mathcal{E}^t$ as the set of all the possible targets to attack at stage t. Then the cascading failure network risk under a defined target attack is:

$$R(\hat{\mathcal{G}}) = \sum_{\forall e \in \mathcal{E}} R(e, \hat{\mathcal{G}}) = \sum_{\forall e \in \mathcal{E}} P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) S(e^*, \hat{\mathcal{G}}) = E[S(e^*, \hat{\mathcal{G}})]. \tag{10}$$

Therefore, $S(e^*, \hat{\mathcal{G}})$ is a variable that maps an event e^* to its severity and interprets $R(\hat{\mathcal{G}})$ as the expected value of $S(e^*, \hat{\mathcal{G}})$, i.e. $E[S(e^*, \hat{\mathcal{G}})]$.

B. SEVERITY OF THE CASCADING FAILURES

The severity of the attack for the selection of a target e^* at each stage of the attack defined by $S(e^*, \hat{\mathcal{G}})$ is measured considering two parameters: power loss and flow bottleneck. The power loss is used to define the severity of the attack against e^* as:

$$S(e, \hat{\mathcal{G}}) = \lambda^t = \sum_{v \in \mathcal{I}^t \cap \mathcal{V}_d} p_v, \tag{11}$$

where $\mathcal{I}^t$ is the isolated node-set resulting from the cascading failures at stage t, and the target action a^* is the disconnection of edge e. On the other hand, the flow bottleneck can also be used to measure the severity of an attack by indicating the increase in network congestion due to the targeted attack against e. The severity of the attacks in terms of flow bottleneck is defined as follows:

$$S(e, \hat{\mathcal{G}}) = \Delta q_e^t = q^t - q_e, \tag{12}$$

where q_e represents the change in the bottleneck when the edge e is attacked and q^t is its pre-contingency state. The flow bottleneck is defined as follows.

Definition 1: The flow bottleneck parameter q^t measuring the ratio between the maximum transmission capacity of the network and the power demand is defined as follows:

$$q^t = \frac{W\left(\mathcal{S}^t\right)}{\sum_{v \in \mathcal{V}_d \wedge v \notin \mathcal{I}^t} p_v}, \tag{13}$$

where $W\left(\mathcal{S}^t\right)$ is the minimum cut set between the generation and the load and $\mathcal{I}^t$ is the set of isolated nodes at time t and each of its components is a node with degree 0.

The flow bottleneck parameter q^t is defined based on [27], where a flow-based Cheeger constant is proposed to identify Laplacians for flow networks. The parameter q^t measures the rate of deliverable demand on the component connected. For the existence of a flow path able to transport the power required from elements in $\mathcal{V}_d$ from $\mathcal{V}_s$, a necessary condition can be defined in terms of q^t as $q^t \geq 1$. If $q^t < 1$, then the demand exceeds the transmission capacity of the network. For values of $q^t > 1$ close to 1 (close from above), the network presents a flow congestion. This means that the power demand value is close to the transmission capacity limit of the network, which in general is subject to the structure of the network and the placement of supply and demand nodes on it. Higher values of q^t (i.e., $q^t \gg 1$) represent the non existence of congestion. The MCS weight represents an upper limit for transmission in the established network configuration. The flow congestion parameter q^t defined in (13) is used to measure the state of the flow bottleneck in the network.

V. MARKOV DECISION PROCESS SOLUTION TO MULTISTAGE ATTACK

In this section, we cast the sequential attacks problem proposed in (6) as a markov decision process and solving it by using a value iteration algorithm.

A. MARKOV DECISION PROCESS MODEL

A state s in the MDP corresponds to the network configuration $\hat{\mathcal{G}}$ and the action a corresponds to the attackers' target edge selection e. The set of all the possible actions that the attacker can take at state s is denoted by $A(s)$. The approach is to map the independent edge-dependent network dynamics modeled by (8) to the state transition probabilities, the risk estimation in (11) or (12) to the MDP immediate reward, and the objective function of (6) to the MDP's long-term expected reward. Formally, the MDP is defined by a tuple $(\mathbf{S}, A, q, r)$, where $\mathbf{S}$ is the set of all possible states. A is the action space of the attacker. $q(s, s', a)$ is the probability of transiting from state s to state s' under an action $a \in A$ of the attacker. $r(s, s', a)$ is the immediate expected reward for the attacker when it takes an action $a \in A$ in state $s \in \mathbf{S}$.

1) MDP STATE TRANSITIONS PROBABILITIES

Consider an initial state s^0 corresponding to the initial network configuration before an attack corresponding to the network $\hat{\mathcal{G}}$. States $s^1, \ldots, s^e, \ldots, s^m$, where m is the cardinality of $\mathcal{E}$ at time t, correspond to the network configurations $\hat{\mathcal{G}}'$ where it is asumed to be inactive $e \notin \hat{\mathcal{E}}'$. Then, the state transition probability $q(s, s', a)$, with $s = \hat{\mathcal{G}}$ and $s' = \hat{\mathcal{G}}'$, is:

$$q(s, s', a) = P(\hat{\mathcal{G}}' \mid \hat{\mathcal{G}}) \tag{14}$$

The probability of failure for each edge in (7) is calculated for the state s and attacker action a.

2) MDP IMMEDIATE REWARD

Now, the damage model (either (11) or (12)) is mapped to the MDP immediate reward function. Accordingly, the immediate expected reward of the MDP is given by $r(s, s', e) = S(e, \hat{\mathcal{G}})$, where the actions selected is $a = e$.

3) DISCOUNTED REWARD STATE VALUE FUNCTION AND MDP POLICY

The solution of the MDP corresponds to a policy π, which maps from a state to action. Let $\{r_t\}_{t=0}^{\infty}$ the sequence of

rewards of the attacker, with r_t being the reward of the stage t of the attack. The expectation of r_t is also denoted by $\mathbb{E}_{s\pi}[r_t] := \mathbb{E}_{\pi}[r_t|S_0 = s]$. The overall discounted value of the strategy $\pi = (\pi(1), \ldots, \pi(s), \ldots, \pi(N))$, selected by the attacker form the initial state s, is defined by:

$$V_\beta(s, \pi) := \sum_{t=0}^{\infty} \beta^t \mathbb{E}_{s\pi}[r_t] \tag{15}$$

where β is the discounted factor.

To evaluate the long-term expected reward, the attacker has an immediate expected reward $r(\pi) = (r(1, \pi), r(2, \pi), \ldots, r(N, \pi))^T$, where for each $s \in S$ $r(s, \pi) := \sum_{a \in A(s)} r(s, a)\pi(s, a)$. Also, consider the $t-$step transition probability between states as:

$$Q^t(\pi) = \left(q_t(s, s', \pi)\right)_{s,s'=1}^{N} \tag{16}$$

Then, the value of the strategy is finaly defined as:

$$\mathbf{V}_\beta(\pi) = \sum_{t=0}^{\infty} \beta^t Q^t(\pi) r(\pi) \tag{17}$$

The previous equation captures the fact that the reward output of 1 unit at time $t + 1$ is worth only by $\beta < 1$ of what it was worth at time t. Then, $\pi(s, a)$ will be the probability that the attacker chooses action $a \in A(s)$ in the state $s \in S$ whenever s is visited. In this case, the strategy will be pure, i.e., $\pi(s, a) \in \{0, 1\}$ for all $a \in A(s)$ and $s \in S$.

4) OPTIMAL POLICY

The optimal policy maximizes the total expected reward, $\pi^* = \text{argmax}_\pi \mathbf{V}_\beta(\pi)$, and the optimal value is V^*. Finally, the attacker strategy at each stage is the solution of the discounted optimal Markov decision problem:

$$\begin{aligned} &\max \mathbf{V}_\beta(\pi) \\ &\text{s.t. } \pi \in P_s, \end{aligned} \tag{18}$$

where P_s is the space of strategies, $\pi(s) = \pi(s, 1), \pi(s, 2), \ldots, \pi(s, m(s))$ and

$$\sum_{a=1}^{m(s)} \pi(s, a) = 1 \tag{19}$$

B. SOLVING THE MDP

The attack problem in (18) is solved by dynamic programming. The algorithm stores two arrays indexed by state: long-term reward value V and attack policy π. The algorithm randomly initiates the reward value function V and repeats the following steps for each state s until no further changes take place:

$$\pi(s) := arg \max_a \left\{ \sum_{s'} Q(s, s', a) \left(r(s, \pi) + \beta V(s')\right) \right\} \tag{20}$$

$$V(s) = \sum_{s'} Q(s, s', \pi(s)) \left(r(s, \pi) + \beta V(s')\right) \tag{21}$$

The optimal policy π, obtained by a backward recursion of (20) and (21), shows the best targets to select for each possible state of the network. Attacks are applied sequentially. Then, the attack with the highest long-term reward value is selected and applied to the network. With the new state of the network, the next attack is recalculated and applied.

VI. RESULTS AND DISCUSSION

This section evaluates the performance of the MDP attack in the IEEE 30-bus case study.

A. CASE STUDY - IEEE 30-BUS POWER NETWORK

In this work, the case study comprises the IEEE 30-bus test system shown in Fig. 3. The system consists of 6 generators and an initial total power demand of $\lambda_{init} = 179.2\ p.u.$ with p.u. base equal to 100 MVA. To evaluate the vulnerability of the test system in Fig. 3, the method in Fig. 4 is applied.

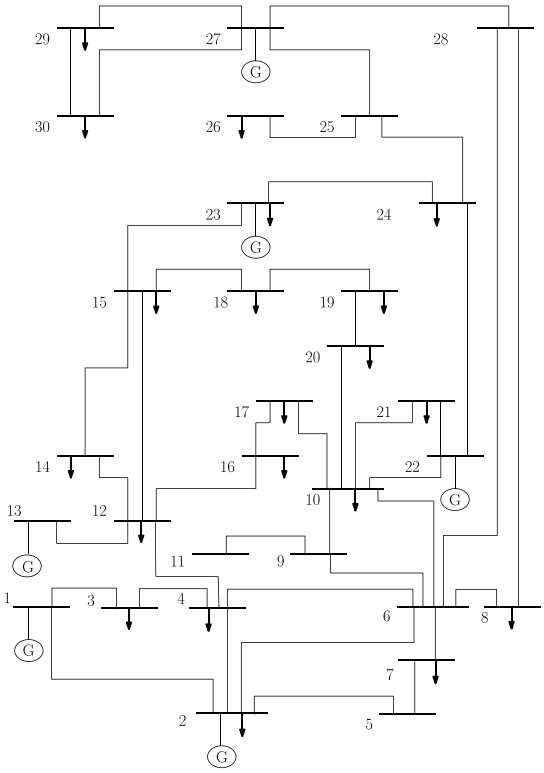

FIGURE 3. IEEE 30-bus system.

First, the test system is modeled as a network following the procedure in Section III. The system is modeled by the graph containing 41 edges and 30 nodes. The power flow initial conditions for the system is calculated by using the routing policy matrix (2). The transmission capacity for each line is calculated through this initial condition. A capacity for each edge in terms of the parameter $\alpha = 5$ is defined. Table 1 summarizes the value of the transmission capacity for each edge.

In the second step of the methodology, the attack target using the MDP strategy is identified. First, the action set A and state set S for the case study are identified. The action set includes all the posible elements that an attacker can interdict

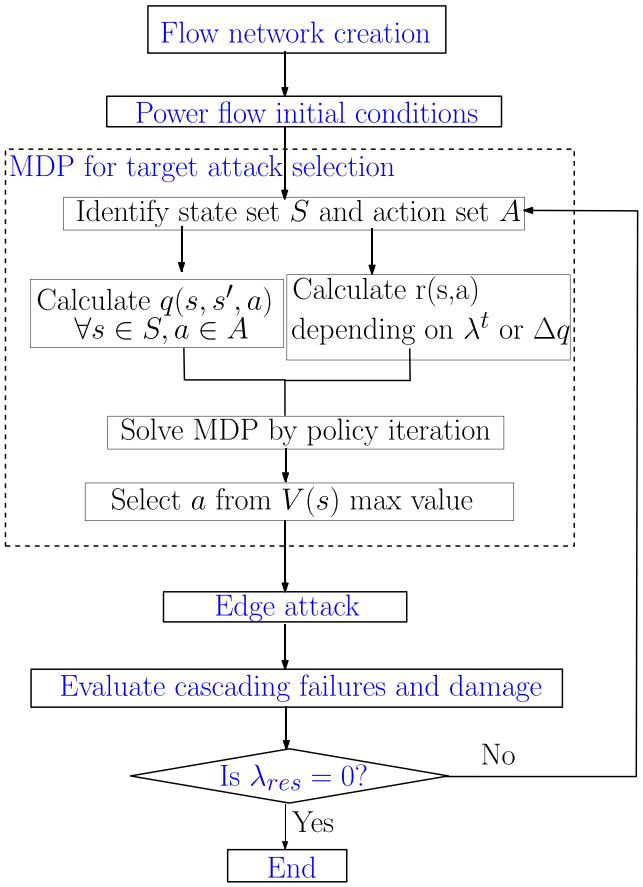

FIGURE 4. Algorithm for the MDP attack strategy.

TABLE 1. The values of the transmission capacities of the IEEE-30 bus system.

e	(from-to)	capacity(p.u.)	e	(from-to)	capacity(p.u.)
1	(1, 2)	130	22	(15, 18)	16
2	(1, 3)	130	23	(18, 19)	16
3	(2, 4)	65	24	(19 ,20)	32
4	(3, 4)	130	25	(10, 20)	32
5	(2, 5)	130	26	(10 ,17)	32
6	(2, 6)	65	27	(10, 21)	32
7	(4, 6)	90	28	(10, 22)	32
8	(5, 7)	70	29	(21, 22)	32
9	(6, 7)	130	30	(15, 23)	16
10	(6, 8)	32	31	(22 ,24)	16
11	(6, 9)	65	32	(23, 24)	16
12	(6,10)	32	33	(24, 25)	16
13	(9, 11)	65	34	(25, 26)	16
14	(9, 10)	65	35	(25, 27)	16
15	(4, 12)	65	36	(28, 27)	65
16	(12,13)	65	37	(27 ,29)	16
17	(12,14)	32	38	(27, 30)	16
18	(12, 15)	32	39	(29, 30)	16
19	(12, 16)	32	40	(8, 28)	32
20	(14, 15)	16	41	(6 ,28)	32
21	(16, 17)	16			

at stage t. At the initial stage, the set A is composed of all edges with weights as in Table 1. For the IEEE 30 case, the initial action set has m elements. By applying action $a \in A$, the network will be at state of edge contingency $m-1$ where an edge is missing. The state set S corresponds to the set of network representation for all posible edge contingencies $m-1-1$ produced as a consecuence of action a generating contingency $N-1$. The initial state set have $m-1$ elements. Once the first attack stage is produced, the network will evolve as a product of failures' propagation. Then, the number of edges in network will reduce $N^t \leq N^{t-1} \leq \cdots \leq N^1 \leq N$. Thus, the state set and action set should be identified at every stage. Next, the transition probability matrix defined in (16) is calculated for each posible state in S at stage t through the failure probability in (7) and the graph-to-graph transition probability in (8). In addition, the risk estimation (10) and the severity of the cascading failure risk are calculated. Severity of the attack is used to evaluate the immediate reward in the system. Two metrics are used. The metrics are the power loss in (11) and the flow congestion change in (12). Once all previous elements are defined, then the Markov decision process in Section V-A is established. In order to solve the MDP corresponding to the attack, the policy iteration in Section V-B is used. According to the solution obtained for the MDP, the first stage of the MDP actions obtained are applied, the cascading failure and the power loss produced by the attack are evaluated; if the network has not collapsed completely, then, considering this new initial condition, all the parameters are calculated again to find the element to be attacked at the next stage.

During the attack stages, cascading failures could occur as a consequence of the attack. Also, power losses occur as a consequence of the attacks. A good target for the attack is the element whose interdiction generates a high power loss as a consequence of a cascading failure phenomena. The algorithm in 1 evaluates the cascading failure process for each attack and measures its damage in terms of the power loss. Network vulnerability is finally calculated by the proposed metric evaluated for the results of the attacks.

To determine the relative efficiency of attacking a particular set of network and comparing it with other attacks, a function of the number of elements required to attack the network and the corresponding damage produced by their interdiction are calculated. Consider the cumulative fraction of attacked edges ρ^t after t attack stages when a single edge is targeted at each stage, defined as:

$$\rho^t = t/m. \tag{22}$$

Then, consider the attack damage obtained after t attack stages measured as the residual load λ^t_{res} given by:

$$\lambda^t_{res} = 1 - \frac{\lambda^t}{\lambda_{init}}, \tag{23}$$

where λ_{init} is the initial power demand value, while lost load λ^t is the value of demand loss occured during attack stage t. The residual load measures the demand in the giant component relatively to the initial load.

B. COMPARING VULNERABILITY CRITERIA: POWER LOSS VS. FLOW BOTTLENECK

The MDP attack in Fig. 4 is evaluated for two different immediate rewards: the power loss reward in (11) and the

TABLE 2. Targets for each attack scenario.

MPD_{λ^t}	$MDP_{\Delta q}$	$MDP^{rand}_{\lambda^t}$ con 50%+	$MDP^{electricB}_{\Delta q}$ con 50%	$MDP^{CS}_{\Delta q}$ con 50%+
(8,28)	(4,6)	(6-8)	(2,5)	(4,6)
(4,12)	(2,6)	(8-28)	(1,3)	(2,6)
(9,10)	(2,5)	(15-23)	(2,4)	(2,5)
(9,11)	(10,22)	(4-12)	(2,6)	(25,27)
(12,13)	(28,27)	(12-13)	(25,27)	(10,22)
(10,17)	(27,29)	(10-17)		
(10,22)	(25,27)	(28-27)		
(22,24)		(2-5)		

Algorithm 1 Cascading Failures Algorithm

Input: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, **c**, b, **p**, λ_{init}, δ^t.
Output: λ^t.

```
Trigger attack δ^t by Eq. (3).
Calculate flow routing f in (V-B).
if YES then
    recursively evaluate the cascading failure propagation
    and the network state by (1) - (3) until no risk exists or
    no flow path exists.
else
    Check for node islanding or connected component
    separation in the network.
    if YES then
        Identify giant component Ĝ. Check for supply nodes
        in the giant component.
        if YES then
            Re-dispatch generation proportionally according
            to its operation limits.
            Calculate flow routing f in (V-B).
            Recursively evaluate cascading failures and net-
            work state by (1) - (3) until no overload exists or
            no flow path exists.
        end if
    end if
    Find and save λ^t
end if
```

congestion increase in (12). The results of the attack can be evaluated and compared by observing the difference in the fraction of the edges attacked in (22) for a quantity of damage obtained by (23). Fig. 5 presents the results of the MDP attack application against the IEEE 30-bus. The green line represents the power loss by selecting the targets randomly. With a fraction of attacked edges $\rho^t = 0.2$, the network only lost 10% of its load. The black line presents the results of the MDP attack with the immediate reward of equivalent power loss λ^t. Close to 12% of the attacked edges, the power loss is higher than 50% of the initial power λ_{init}. The first attacks in the sequence do not represent losses for the system. The dotted orange line shows the attack results for the MPD attack with immediate reward congestion criteria i.e., $r(s, s', a) = \Delta q$. This attack strategy presents better results than the other two strategies. After the second attacker action of the sequence,

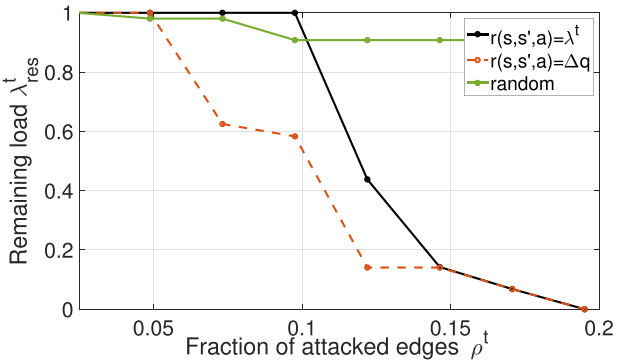

FIGURE 5. Results of the MDP attack application against the IEEE 30-bus without network reinforcement.

the system has lost 40% of the power. When 12% of the edges are attacked, the power lossess is twice higher than the power lossess in MDP with λ^t immediate reward. By the end of the attacks, both strategies behave the same. Therefore as can be observed, attacks based on the increased congestion produce more harmful results than attacks focused on the immediate loss of the load. Table 2 shows the targets selected for each attack. Attacks in the $MDP_{\Delta q}$ strategy is focused on the edges connecting nodes in the minimum cut set between generation and load, while attacks in the MPD_{λ^t} strategy target edges directly connected to centers of the load. The attack is not successful due to the redundancy of edges between load.

A fixed strategy to reinforce the transmission capacity of some edges as a measure to reduce the impact of cascading failure effects is also studied. The use of different criteria is implied to select the suitable candidates for the reinforcement of edge transmission capacity. The impact of this reinforcement is evaluated by the effect produced on the attack impact.

C. VULNERABILITY FOR DIFFERENT CAPACITY CONDITIONS

Considering the results of the previous section and the results in [21], the transmission capacity of edges, the network transmission capacity, and congestion play a central role in the vulnerability of the network to different events triggering cascading failures. In this way, it is interesting to evaluate how the attack impact can be affected by making the capacity value flexible for some edges. For this, consider a number k of edges selected under determined criteria in order to increase its transmission capacity. The increased capacity

will be selected for this example as a minimum required to produce changes in the network behavior. In this way, 10% of the edges are selected for a reinforcement of 50% increasing in transmission capacity.

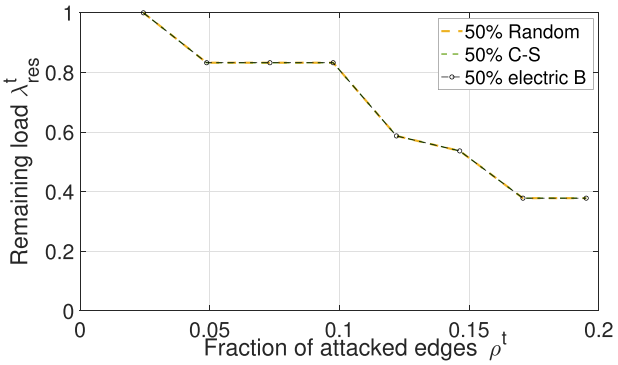

FIGURE 6. Results of the MDP attack with λ^t reward versus the reinforcement strategy.

Three different criteria are used to select suitable candidates for the reinforcement. The first strategy is a random selection of the candidates. The second strategy is the selection of the candidates according to electrical betweenness, [28], labeled as Δ_{e-b}. This measure is a result of the combination of betweenees centrality and power transfer distribution factors. Finally, the last strategy is the selection of candidates according to the cut-set metric for critical links identification described in [21]. The methodology to obtain attacks for the different target sets (i.e., MDP, random, rich, rich-poor, betweenness, electric betweenness, and flow betweenness) is described in general by simulation Algorithm 1. In terms of the Markov Decision Process, the reinforcement of the edges implies the inclusion of a defender who fixes a pure strategy against the attacker. Results of the MDP will be the best response from the attacker to the defender fixed strategy. The result will be different for both MDP attacks. Fig. 6 presents the results of the MDP attack with λ^t reward versus the reinforcement strategy. For any strategy to select candidates for the capacity increase, the network vulnerability to the attack is reduced by 50%. All the reinforcement gives the same results. By using a reward function λ^t, the vulnerability of the network is fixed and depends on load placement and its connectivity. Even if different edge sets are selected for a capacity reinforcement, the vulnerability of the network is fixed. Fig. 7 presents the results for the MDP attack with Δq reward versus the reinforcement strategy. A random reinforcement of the capacity does not affect the attack impact, as can be seen in the orange dotted line. On the other hand, an increase in the capacity of the elements of the CS presents a slight decrease in the vulnerability of the network as can be seen in the dotted black line. The most atypical case is the reinforcement of the edges selected by its electric betweenness. The edges with the highest electric betweenness are $(2, 5)$, $(2, 4)$, $(2, 6)$, $(1, 3)$. Those edges are also the edges with the higher capacity in all over the network (see Table 1). Increasing the capacity of

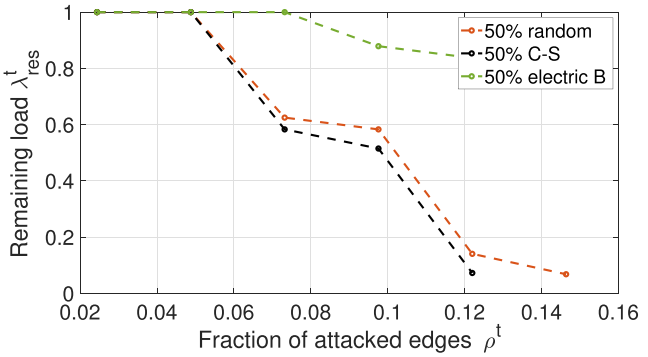

FIGURE 7. Lost of load for the MDP attack with Δq reward versus the reinforcement strategy.

these edges impacts the effectivity of the attack by 90%. For an increase of 50% in its capacity, the network transmission capacity increases in more than 20% of the initial transmission capacity, thereby reducing the congestion and increasing the resilience of the network in this particular operation point. Comparing results in Fig. 6 and Fig. 7, we observe that immediate reward based on network congestion can strongly affect the vulnerability of the network more than sequential attacks based on power loss. Reinforcement strategies do not present the same effect for vulnerability. Then it is necessary to propose future strategies to identify target reinforcement that reduce vulnerability depending on the kind of strategy that the attacker would select.

By observing these results, it is natural to note that a possible controlled rating of edges's capacities during contingencies could help reduce the impact that failures and threats against some of their elements can produce. Also, an appropriate strategy should be used to select the best candidates for reinforcement or controlled dynamic capacity rating in order to obtain the best response against attacks. As a consequence of these experiments, elements by themselves cannot be understood as vulnerables. There are specific arrangements of elements' interdiction that can be identified as vulnerable by estimating failure risk and evaluating its role in the evolution of the network.

VII. CONCLUSION

Vulnerability assessment of the power network is a useful tool for evaluating local and global network properties that favor failures propagation during possible events of sequential interdiction. Given the increasing complexity and fast growth of the power network, new methodologies and properties integrating the network, electrical properties, and uncertainty in the phenomena should be considered. This paper proposes a Markov-based methodology to evaluate the vulnerability to sequential attacks. The attack objective is to spread failures across the network until it achieves the total loss of service. Most vulnerable elements are identified as the most likely targets for the mechanism of attack. Network-based and electric-based metrics for long-term risk estimation are proposed. Congestion and network transmission capacity result in major issues that influence the vulnerability of the network.

The case study demonstrates that the mechanism of attack produces more significant damage when a network-based metric guides a target selection. Thus, the comparison of scenarios where random or specific reinforcements are applied to the network shows how the network is vulnerable to the proposed attack unless reinforcement is carefully selected as a response to the specific attack. Future work will address attack-defense models where the network reinforcement actions are considered strategically in response to the attack strategy.

REFERENCES

[1] J. Carlson, R. Haffenden, G. Bassett, W. Buehring, M. Collins, III, S. Folga, F. Petit, J. Phillips, D. Verner, and R. Whitfield, "Resilience: Theory and application," Argonne Nat. Lab., Argonne, IL, USA, Tech. Rep. ANL/DIS-12-1, 2012.

[2] H. Cetinay, F. A. Kuipers, and P. V. Mieghem, "A topological investigation of power flow," *IEEE Syst. J.*, vol. 12, no. 3, pp. 2524–2532, Sep. 2018.

[3] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2995–3000, May 2018.

[4] 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, Jun. 2017.

[5] 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, Sep. 2015.

[6] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem, "Comparing the effects of failures in power grids under the AC and DC power flow models," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 4, pp. 301–312, Oct./Dec. 2018.

[7] S. Soltan, D. Mazauric, and G. Zussman, "Analysis of failures in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 2, pp. 288–300, Jun. 2017.

[8] 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, Jul. 2016.

[9] W. Liao, S. Salinas, M. Li, P. Li, and K. A. Loparo, "Cascading failure attacks in the power system: A stochastic game perspective," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2247–2259, Dec. 2017.

[10] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1183–1195, May 2014.

[11] M. X. Cheng, M. Crow, and Q. Ye, "A game theory approach to vulnerability analysis: Integrating power flows with topological analysis," *Int. J. Electr. Power Energy Syst.*, vol. 82, pp. 29–36, Nov. 2016.

[12] B. Moussa, P. Akaber, M. Debbabi, and C. Assi, "Critical links identification for selective outages in interdependent power-communication networks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 472–483, Feb. 2018.

[13] D. Bienstock, *Electrical Transmission System Cascades and Vulnerability*. Philadelphia, PA, USA: SIAM, 2015.

[14] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid.*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[15] 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," *Phys. A, Statist. Mech. Appl.*, vol. 389, no. 3, pp. 595–603, 2010.

[16] 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, Mar. 2018.

[17] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[18] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2340–2354, Dec. 2014.

[19] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "The sequential attack against power grid networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 616–621.

[20] P. Cuffe, "A comparison of malicious interdiction strategies against electrical networks," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 7, no. 2, pp. 205–217, Jun. 2017.

[21] C. Caro-Ruiz, A. Pavas, E. Mojica-Nava, J. Ma, and D. J. Hill, "Qualifying transmission line significance on cascading failures using cut-sets," in *Proc. IEEE Milan PowerTech*, Jun. 2019, pp. 1–6.

[22] J. Yan, Y. Tang, Y. Zhu, H. He, and Y. Sun, "Smart grid vulnerability under cascade-based sequential line-switching attacks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–7.

[23] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[24] K. Savla, G. Como, and M. A. Dahleh, "Robust network routing under cascading failures," *IEEE Trans. Netw. Sci. Eng.*, vol. 1, no. 1, pp. 53–66, Jan. 2014.

[25] J. Filar and K. Vrieze, *Competitive Markov Decision Processes*. Berlin, Germany: Springer-Verlag, 1996.

[26] P. Grindrod and D. J. Higham, "Evolving graphs: Dynamical models, inverse problems and propagation," *Proc. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 466, no. 2115, pp. 753–770, 2010.

[27] J. Taylor and F. Hover, "Laplacians for flow networks," *SIAM J. Discrete Math.*, vol. 25, no. 3, pp. 1349–1364, 2011.

[28] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012.

CLAUDIA CARO-RUIZ received the B.S. degree in electronics engineering, the B.S. degree in electrical engineering, and the M.Sc. degree in electronics engineering from the Universidad de Los Andes (UAndes), Bogotá, Colombia, in 2008, 2009, and 2012, respectively. She is currently pursuing the Ph.D. degree in electrical engineering from the Universidad Nacional de Colombia, Bogotá, Colombia. She is also a full-time Faculty and a Researcher with Universidad Manuela Beltrán. Her current research interests include control of complex dynamical networks, multienergy systems, and power grids resilience.

AMEENA SAAD AL-SUMAITI received the B.Sc. degree in electrical engineering from United Arab Emirates University, United Arab Emirates, in 2008, and the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2010 and 2015, respectively. She was a Visiting Assistant Professor with MIT, Cambridge, MA, USA, in 2017. She is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, Khalifa University, United Arab Emirates. Her research interest includes intelligent systems.

SERGIO RIVERA received the Ph.D. degree from the Electric Energy Institute, National University of San Juan, San Juan, Argentina. He is currently an Associate Professor of electrical engineering with the Universidad Nacional de Colombia, Bogotá, Colombia, where he specializes in smart grids. He was a Postdoctoral Researcher with the Massachusetts Institute of Technology and LIINES, Masdar Institute of Science and Technology. Prior to his Postdoctoral Fellowship, he was with General Motors as a Senior Process Engineer in the manufacturing engineering area. He was a Professor of power systems with District University, where he taught courses in the reliability of power systems and electricity markets. There, he proposed a methodology for short-term investment decisions in electric distribution networks considering uncertainties in planning parameters. He received the Fulbright Fellowship as a Research Scholar with the University of Florida.

EDUARDO MOJICA-NAVA received the B.S. degree in electronics engineering from the Universidad Industrial de Santander, Bucaramanga, Colombia, in 2002, the M.Sc. degree in electronics engineering from the Universidad de Los Andes (UAndes), Bogotá, Colombia, in 2005, and the Ph.D. degree in automatique et informatique industrielle from the École des Mines de Nantes, Nantes, France, in cotutelle with UAndes, in 2010. He is currently an Associate Professor with the Department of Electrical and Electronics Engineering, Universidad Nacional de Colombia, Bogotá. His current research interests include optimization and control of complex networked systems, switched and hybrid systems, and control in smart grid applications.