J. Mod. Power Syst. Clean Energy (2018) 6(5):918–929
https://doi.org/10.1007/s40565-018-0436-y

A tri-level programming model for attack-resilient control of power grids

Hamzeh DAVARIKIA[1], **Masoud BARATI**[2]

Abstract The significance of modern power grids is acknowledged every time there is a major threat. This paper proposes the novel approaches to aid power system planner to improve power grid resilience by making appropriate hardening strategies against man-made attack or natural hazards. The vulnerability indices are introduced, which return the most vulnerable component in the system based on a tri-level defender-attacker-operator (DAO) interdiction problem which solves iteratively. The output of DAO is the set of hardening strategies that optimally allocated along the network to mitigate the impact of the worst-case damages. By repeating DAO problem based on the proposed algorithm, the various crafted attack is imposed on the system, and the defender's behavior demonstrates how an element is vulnerable to threats. The WSCC 9-bus, IEEE 24-bus, and IEEE 118-bus systems are employed to evaluate the model performance. The counter-intuitive results are proven by the proposed robust hardening strategy, which shows how the hardening strategy should be allocated to improve power network resilience against threats.

CrossCheck date: 5 June 2018

Received: 16 April 2018 / Accepted: 5 June 2018 / Published online: 24 August 2018

✉ Hamzeh DAVARIKIA
hdavar1@lsu.edu

Masoud BARATI
masoud.barati@pitt.edu

[1] Department of Electrical Engineering, Louisiana State University, Baton Rouge, LA 70808, USA

[2] Department of Electrical and Computer Engineering, University of Pittsburgh, Pittsburgh, PA 15261, USA

Keywords Cyber attack, Defender, Hardening, Protection, Resilience, Vulnerability

1 Introduction

Among the critical and extraordinarily complex infrastructure, the significance of the electric power grid is acknowledged every time there is a cyber/physical attack or a severe natural hazard. The ability of power networks to withstand man-made assault or Mother Nature's threats referred to the newly emerged discipline in infrastructure security community called power network resilience [1]. While the traditional reliability indices are not adequate by themselves to effectually plan for the emerging hazards, developing resilience indicators help network planner to allocate the maintenance budget and capital investment to elevate network functionality against low probability, high consequence risks.

The current resilience metrics can be classified into two broad categories, namely the attribute-based metrics and the performance-based metrics. The performance-based indices are ordinarily quantitative methods for answering the question "How resilient is my system?". However, the attribute-based metrics are usually process-based and attempt to response the question "What makes my system more/less resilient?" [1].

While the majority of the current techniques evaluate the resilience of power networks as a whole, we propose a novel quantitative approach to obtain vulnerability indices of power system components through a multi-level game-theoretic interedition problem. To this end, a game between attacker, defender, and system operator is established, where each party seeks to maximize its own interest. In one side is the aggressor, who tries to impose the maximum

damage by attacking to the minimal important components, while in the other side the defender makes the appropriate network's component hardening strategy to minimize system operating cost (SOC). Hardening refers to a protection status that makes an element invulnerable to damage [2, 3]. In the third level, the system operator returns the SOC which evaluates the defender's and attacker's tactic.

When the game is played with a certain number of recourses for attacker and defender, one can recognize the most important elements in the network from the defender behavior; the smart attacker always chooses to destroy the components that cause the worst possible SOC to the system, thereby the defender protects the most vulnerable component considering his limited available resources. Inspired by this fact, we propose the element's vulnerability indices by observing how frequent an element is defended when the game repeats with different resources for the defender. Remarkably, some elements in the system are rarely chosen for defending even if both defender and attacker have full resources to target all the network's components. While on the other hand, each system has some essential components that are the first choice for the defender to make the hardening strategy.

Despite continuing investments in power grid modernization, the electricity system remains vulnerable to a range of hazards [4]. The resilience concept in power networks has progressively been developed in the recent years [5] due to its capacity to lessen the risks associated with the inevitable disruption of systems. While there is no classical definition for resilience in power networks, [5] defines power networks resilience as the capability of electric power systems to resist against multiple possible outages, assimilate the initial damage, and restore to normal operation. As another accepted definition, a high resilience network should withstand immense and high-impact events that might have rarely been occurred before [6].

Although controlled islanding is generally considered as the last measure to rescue a blackout in power grids [7–9], a defensive intentional islanding scheme to improve grid resilience proposed by [6], where the corrective islanding approach utilized to mitigate severe weather effect on the power grids. In a more component-wise resiliency improvement approach, [10] proposes a methodology to model the fragility function for the transmission lines components, to observe how the whole power networks will react to the severe inclement weather. The output of this model finds the perilous network sections, whose solely depends on the weather intensity, and evaluates the benefits of alternative measures to augment resilience.

A resilient distribution system planning against natural hazards is proposed by [11], where a robust optimization approach utilized to design power networks to withstand against $N-k$ worst-case network interdiction problem. One can consider this approach as a resource allocation problem whose system planner allocate the hardening and distributed generator (DG) along the feeders to achieve a resilient network which tolerates worst-case interdictions.

One may summarize the reviewed and existing literature in the power network resilience to the different approaches taken for identifying the vulnerable component of the network. Among the various techniques, interdiction problem is well fitted with the resilience assessment necessities. Interdiction problem in the power network is a game-theoretic optimization approach between the defender and rational attacker, which attacker's and defender's strategies determine the most vulnerable elements in the power grid.

In bi-level network interdiction problems, a leader works against one or more followers who seek to operate the network with minimum cost. The leader may act to interdict (i.e., inflict damage upon) a limited number of network components. After interdiction actions have been made, each follower responds by developing an operational plan that maximizes performance on the surviving system. The modern field of network interdiction evolved from some works in the 1960s and 1970s that center around the resilience of a maximum-flow network subject to arc removal, a problem later proven by [12] to be NP-hard. Following these papers, some related studies consider both continuous [13–15] and discrete [15, 16] interdiction of shortest path networks.

While establishing a sequential game between the defender and the attacker was traditionally the typical approach in defining an interdiction problem, one can improve the model transparency by dividing the attacker, defender, and operator (defender) into different layers. Reference [17] applied tri-level programming to formulate the defender-attacker-defender (DAD) model in power networks. In this work, the solution attained by a decomposition-based technique to iterate between the outer problem and the inner bi-level problem.

For the bi-level problem itself, the Karush–Kuhn–Tucker (KKT) optimality conditions and duality theory are considered as the classical solution approach, which converts the bi-level optimization problem to the single level one [18].

Reference [19] proposed a tri-level mixed-integer nonlinear (MINLP) DAD model and used Tabu search with an embedded greedy algorithm to seek an optimum defense strategy. Although they formulate a more comprehensive interdiction model than the proposed approach in [17], their model is computationally expensive due to the high nonlinearity of formulation. This is also the reason why they used heuristic approaches to achieve the solution.

Reference [20] used the simple model proposed in [21] and applied a column and constraint generation (C&CG) decomposition technique to solve the tri-level problem, which results in a more efficient solution than heuristics or traditional Bender's decomposition approaches [22].

Reference [23] proposed a tri-level DAD model whose addresses the vulnerability of coupled gas-electric networks against crafted line interdictions. Due to the presence of binary variables in the inner problem, they used a nested C&CG method to solve the proposed model.

In this paper, we propose a tri-level interdiction problem, whose the players seek to optimize SOC based on their interests. Unlike most of the existing literature which considers the cost of the unserved load as the objective function, we formulate SOC as the cost of load shedding in addition to the generator operating cost. Moreover, the players can target all the three essential elements in power grids, namely generators, transmission lines, and substations (buses).

Considering Bender's decomposition framework and utilizing the duality theorem, the tri-level problem is decomposed into the so-called master problem and subproblem, and the efficient C&CG approach employed to reach the solution.

Once the game played with the specified number of resources for attacker and defender, the proposed approach returns the most critical elements in power systems. By repeating the game when a defender has the different amount of resources, we obtain the sensitivity of SOC to the number of defender's resources. When a diverse number of resources are available, the defender behavior investigation in defending network's component leads to the striking outcomes: ① protecting the specified number of elements in each system, results in a resilient system design, where the power system is robust against $N-k$ contingencies; ② there are some vulnerable elements which defended in each round of play, while on the other hand, some other components have a lower priority for the defender.

We are reporting this investigation in this paper as a novel approach to obtain vulnerability indices and ranking the power grids element vulnerability. This approach aids the network planner to make judicious planning strategy to enhance power network resilience.

The prominent contributions of this paper are: ① develop and solve a comprehensive tri-level MILP interdiction optimization model in power networks; ② perform a wide range of case studies in different test case systems; ③ find the robust defending strategy to design a resilient power network; ④ propose new vulnerability indices and ranking vulnerable elements in power grid.

The rest of the manuscript organized as follow: Sect. 2 discusses the problem formulation followed by the solution approach in Sect. 3. The proposed methodology applied to three different cases studies in Sect. 4. The conclusion is represented in Sect. 5.

2 Model formulation

2.1 Tri-level defender-attacker-operator (DAO) problem

The DAO interdiction problem is expressed as tri-level programming in this section. Figure 1 demonstrates the game pattern, where the defender's strategy is determined by allocating the limited defender's hardening resources to minimize SOC. Note that grid's elements are referred to as substations (buses), generators and transmission lines (power transformers also considered as the transmission lines) throughout this paper.

Defender, as the game leader, makes the first strategy by hardening the grid's elements considering the limited resources. The defender strategies then pass to both the attacker problem and the operator problem, where the operator evaluates the SOC associated with defender's plan. The follower in the game is the attacker, who receives the defender's decisions and seeks to maximize SOC by attacking to the undefended component within the network. This process can be formulated by three hierarchical dependent optimization problems, known as the sequential game, or so-called Stackelberg game.

2.2 Problem formulation

The problem (1)–(12) consists of three-level dependent optimization problem: ① upper-level defender problem (2);

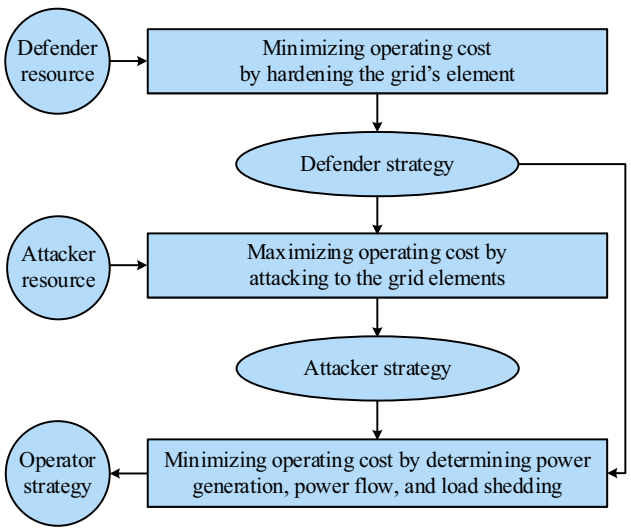

Fig. 1 Process of interaction between attacker, defender, and operator

② middle-level attacker problem (2)–(6); ③ lower-level operator problem (7)–(12). All the three optimization problems seek to optimize the objective function (1), although with different goals.

$$\min_{\Delta^D} \max_{\Delta^A} \min_{\Delta^O} \left(\sum_{i \in B} C_i^{Sh} P_i^{Sh} + \sum_{g \in G} C_g P_g^G \right) \tag{1}$$

s.t.

$$\begin{cases} \sum_{i \in B} x_i^D \le R^{DB} \\ \sum_{(i,j) \in L} y_{ij}^D \le R^{DL} \\ \sum_{g \in G} z_g^D \le R^{DG} \end{cases} \tag{2}$$

$$x_i^A \le 1 - x_i^D \qquad \forall i \tag{3}$$

$$y_{ij}^A \le 1 - y_{ij}^D \qquad \forall (i,j) \tag{4}$$

$$z_g^G \le 1 - z_g^D \qquad \forall g \tag{5}$$

$$\begin{cases} \sum_{i \in B} x_i^A \le R^{AB} \\ \sum_{(i,j) \in L} y_{ij}^A \le R^{AL} \\ \sum_{g \in G} z_g^A \le R^{AG} \end{cases} \tag{6}$$

$$F_{ij} = B_{ij}(\theta_i - \theta_j) U_{ij} \qquad \forall (i,j) : \left(\lambda_{ij}^F\right) \tag{7}$$

$$\sum_{g \in G_{b(i)}} P_g^G - \sum_{j|(i,j) \in L} F_{ij} + \sum_{j|(j,i) \in L} F_{ji} = P_i^D - P_i^{Sh} \qquad \forall i : (\lambda_i^B) \tag{8}$$

$$0 \le P_i^{Sh} \le P_i^D \qquad \forall i : \left(\mu_{i,\max}^D\right) \tag{9}$$

$$0 \le P_g^G \le P_{g,\max}^G (1 - z_g^A) \qquad \forall g : (\mu_{g,\max}^G) \tag{10}$$

$$|F_{ij}| \le F_{ij,\max} U_{ij} \qquad \forall (i,j) : \left(\mu_{ij,\min}^F, \mu_{ij,\max}^F\right) \tag{11}$$

$$U_{ij} = \left[1 - x_i^A (1 - x_i^D)\right] \left[1 - x_j^A \left(1 - x_j^D\right)\right] \cdot \left[1 - y_{ij}^A \left(1 - y_{ij}^D\right)\right] \qquad \forall (i,j) \tag{12}$$

where $P_{g,\max}^G$ is the max generation capacity of generator g; $F_{ij,\max}$ is the maximum capacity of transmission line (i, j); x_i^D is equal to 1 if bus i is hardened and 0 otherwise; x_i^A is equal to 1 if bus i is attacked and 0 otherwise; y_{ij}^D is equal to 1 if transmission line (i, j) is hardened and 0 otherwise; y_{ij}^A is equal to 1 if transmission line (i, j) is attacked and 0 otherwise; z_g^D is equal to to 1 if generator g is hardened and 0 otherwise; z_g^A is equal to 1 if generator g is attacked and 0 otherwise; F_{ij} is power flow through line (i,j); θ_i is the voltage angles at bus i; P_i^{Sh} is the load shedding at bus i; P_g^G is power output of generator g; P_i^D is the summation of loads connected to bus i; C_i^{Sh} is load-shedding cost at bus i; C_g is production cost of generator unit g; B_{ij} is the susceptance for transmission line (i,j); B is the set of indices of buses; G is the set of indices of generators; L is the set of indices of transmission lines; $G_{b(i)}$ is the set of indices of generators connected to bus i; $R^{DB}, R^{DG}$and R^{DL} are the number of defender's resource for hardening, respectively, buses, generators, and transmission lines; R^{AB}, R^{AG} and R^{AL} are the number of attacker's resource for attacking, respectively, buses, generators, and transmission lines.

Defender problem seeks to minimize (1) considering optimization variables in the set $\Delta^{\mathcal{D}} = \{x^D, y^D, z^D\}$, and constraints in (2) are the limits on defender resources for elements' hardening. In contrast to the defender problem, is the attacker problem which works toward maximizing (1) with the optimization variables in set $\Delta^{\mathcal{A}} = \{x^A, y^A, z^A\}$. Constraints (3) and (4) apply the rule that the only unprotected elements can be attacked. Constraints in (6) bound adversary's resources for attacking the grid elements. Both defender and attacker strategies are evaluated in the last level by the operator problem whose the optimization variables in set $\Delta^{\mathcal{O}} = \{P^G, P^{Sh}, \theta, F\}$. Constraint (7) formulates the active power flows on the transmission lines. Constraint (8) stands for the flow conservation at each bus. Constraint (9) is the upper-bound (UB)of load-shedding for each load. Constraint (10) sets the production limit of each generator. Constraint (11) bounds the maximum absolute values of the power flow in transmission lines. A transmission line can be functional at its full capacity when $U_{ij} = 0$, or non-functional due to the attack to its own, or its connected buses $(U_{ij} = 1)$ according to constraint (12). The dual variables λ_{ij}^F, λ_i^B, $\mu_{i,\max}^D$, $\mu_{g,\max}^G$, $\mu_{ij,\min}^F$, $\mu_{ij,\max}^F$ associated with each constraint of operator problem are shown following a colon.

2.3 Vulnerability indices

Perceiving the defender behavior in protecting network components during multiple runs of the model with a various number of resources, results in a significant observation: there are some elements in the system which are fortified almost in each round of the game, while there are some other elements that are less important for the defender. We use this observation and define vulnerability index for the component as the number of times that an element is defended during multiple runs of the DAO model with the different number of defender's resources. Algorithm 1 shows the procedure to obtain vulnerability indices.

Step 1: Initialization. Set $I^B_{V,i}$, $I^G_{V,g}$ and $I^L_{V,ij}$ to zero for all the network components, where $I^B_{V,i}$ is the vulnerability index for bus i, $I^G_{V,g}$ is the vulnerability index for generator g and $I^L_{V,ij}$ is the vulnerability index for transmission line (i,j).

Step 2: Set the R^{DB}, R^{DG} and R^{DL}.

Step 3: Solve the DAO interdiction problem.

Step 4: Update the vulnerability indices as follow: ① if $x^D_i = 1$, then $I^B_{V,i} = I^B_{V,i} + 1$, $\forall i$; ② if $z^A_g = 1$, then $I^G_{V,g} = I^G_{V,g} + 1, \forall g$; ③ if $y^A_{ij} = 1$, then $I^L_{V,ij} = I^L_{V,ij} + 1$, $\forall (i,j)$.

Step 5: Go to *Step 2* and set the new value for defender resources.

3 Solution approach

The proposed model in the previous section is complicated to solve due to the tri-level structure which renders an NP-hard problem [19, 24]. While no formal optimization method has been devised for solving this kind of problem so far [20, 25], several approaches are available in the literature based on various versions of Benders decomposition and C&CG methods [22, 26]. In Bender's based approaches, dual or sensitivity information from the so-called sub-problem is used to construct the objective function of the so-called master problem gradually. On the other hand, C&CG method generates a new set of constraints in each iteration utilizing cutting-plane strategies, based merely on primal cuts that involve only primal decision variables. Since differentiability of the problem is not required in the C&CG method, and it generally performs computationally better than its Benders' counterpart [22], it is used in this paper as the solution approach. Considering the C&CG framework, the first step to solve our tri-level problem is decomposing the problem into a master problem and a sub-problem. To this end, the master problem is formed as a combination of defender and operator (min-min) problems, and sub-problem constitutes of attacker and operator (max-min) problems.

The min-min structure of master problem renders a single-level minimization problem. However, sub-problem has a bi-level max-min structure which should be transformed to a single-level one, either with duality theorem or KKT optimality conditions. Note, this transformation is possible due to the linearity and convexity of the lower-level problem in its optimization variables. Figure 2 schematically demonstrates the interactions between the master problem and sub-problems.

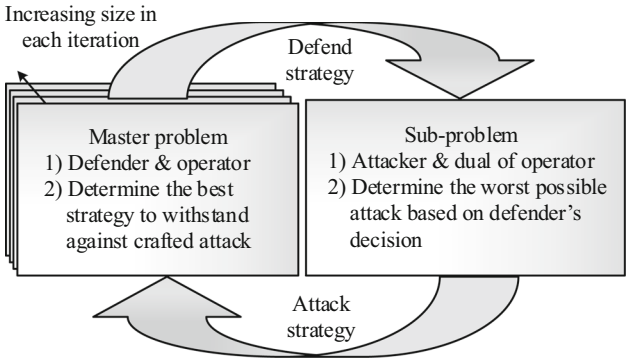

Fig. 2 Process of interaction between attacker, defender, and operator

3.1 Master problem

Considering C&CG framework, the master problem is formulated below:

$$\min_{\Delta^{\mathcal{M}}} \eta \tag{13}$$

s.t.

$$\eta \geq \sum_{i \in B} C^{Sh}_{i,v} P^{Sh}_{i,v} + \sum_{g \in G} C_{g,v} P^G_{g,v} \tag{14}$$

$$\begin{cases} \sum_{i \in B} x^D_{i,v} \leq R^{DB} \\ \sum_{(i,j) \in L} y^D_{ij,v} \leq R^{DL} \\ \sum_{g \in G} z^D_{g,v} \leq R^{DG} \end{cases} \tag{15}$$

$$\left| F_{ij,v} - B_{ij}\left(\theta_{i,v} - \theta_{j,v}\right) \right| \leq M U_{ij,v} \tag{16}$$

$$\sum_{g \in G_{b(i)}} P^G_{g,v} - \sum_{j|(i,j) \in L} F_{ij,v} + \sum_{j|(j,i) \in L} F_{ji,v} = P^D_{i,v} - P^{Sh}_{i,v} \qquad \forall i \tag{17}$$

$$0 \leq P^{Sh}_{i,v} \leq P^D_i \qquad \forall i \tag{18}$$

$$0 \leq P^G_{g,v} \leq P^G_{g,v,\max}\left(1 - \hat{z}^A_{g,v}\right) \qquad \forall g \tag{19}$$

$$\left| F_{ij,v} \right| \leq F_{ij,v,\max} U_{ij,v} \qquad \forall (i,j) \tag{20}$$

$$\begin{aligned} U_{ij,v} = &\left[1 - \hat{x}^A_{i,v}\left(1 - x^D_{i,v}\right)\right]\left[1 - \hat{x}^A_{j,v}\left(1 - x^D_{j,v}\right)\right] \\ &\cdot \left[1 - \hat{y}^A_{ij,v}\left(1 - y^D_{ij,v}\right)\right] \qquad \forall (i,j) \end{aligned} \tag{21}$$

where M is the sufficiently large number; subscript v is the iteration index, and $v = 1, 2, \ldots, v_{\max}$. The optimization variables of the master problem are in the set $\Delta^{\mathcal{M}}$ including the defender decision variables $x^D_{i,v}, y^D_{ij,v}, z^D_{g,v}$ and the operator decision variables $P^G_{g,v}, P^{Sh}_{i,v}, \theta_{i,v}, F_{ij,v}$ one per iteration of the algorithm, and auxiliary variable η, which is used to rebuild objective function (13) progressively. Attacker parameters $\hat{x}^A_{i,v}, \hat{y}^A_{ij,v}, \hat{z}^A_{g,v}$ are fixed to their optimal values

obtained from the solution of sub-problem at each iteration and used as input parameters of the master problem. Note that the variables denoted by the hat $(\hat{\cdot})$ are the fixed parameters gotten from the solution of the other problem, e.g., sub-problem. The size of master problem gradually increases with the iteration counter v since a new set of constraints (14)–(21) are integrated at each iteration of the algorithm.

3.2 Sub-problem

Sub-problem has a bi-level max-min structure. Since the lower-level operator problem is linear and thus convex in its optimization variables, due to the strong duality theorem, it can be replaced by its equivalent dual problem and then merge with attacker problem to form a max-max structure which is a single-level problem. Accordingly, the single-level sub-problem becomes:

$$\max_{\Delta^{\mathcal{S}}} \Bigg[\sum_{g\in G} \mu^{G}_{g,\max} P^{G}_{g,\max} \left(z^{A}_{g} - 1 \right) - \sum_{(i,j)\in L} B_{ij} \hat{U}_{ij} \left(\mu^{F}_{ij,\max} + \mu^{F}_{ij,\min} \right) + \sum_{i} P^{D}_{i} \left(\lambda^{B}_{i} - \mu^{D}_{i,\max} \right) \Bigg] \tag{22}$$

s.t.

$$x^{A}_{i} \le 1 - \hat{x}^{D}_{i} \qquad \forall i \tag{23}$$

$$z^{A}_{g} \le 1 - \hat{z}^{D}_{g} \qquad \forall g \tag{24}$$

$$y^{A}_{ij} \le 1 - \hat{y}^{D}_{ij} \qquad \forall (i,j) \tag{25}$$

$$\begin{cases} \sum_{i\in B} x^{A}_{i} \le R^{AB} \\ \sum_{(i,j)\in L} y^{A}_{ij} \le R^{AL} \\ \sum_{g\in G} z^{A}_{g} \le R^{AG} \end{cases} \tag{26}$$

$$C_{g} - \lambda^{B}_{i(g)} + \mu^{G}_{g,\max} = 0 \qquad \forall g \tag{27}$$

$$C^{\mathcal{S}_i}_{i} - \lambda^{B}_{i(d)} + \mu^{D}_{i,\max} \ge 0 \qquad \forall i \tag{28}$$

$$\lambda^{B}_{i} - \lambda^{B}_{j} - \lambda^{F}_{ij} + \mu^{F}_{ij,\max} - \mu^{F}_{ij,\min} = 0 \qquad \forall (i,j) \tag{29}$$

$$\mu^{D}_{i,\max} \ge 0 \qquad \forall i \tag{30}$$

$$\mu^{G}_{g,\max} \ge 0 \qquad \forall g \tag{31}$$

$$\sum_{j|(i,j)\in L} \lambda^{F}_{ij} B_{ij} \hat{U}_{ij} - \sum_{j|(j,i)\in L} \lambda^{F}_{ij} B_{ji} \hat{U}_{ji} \ge 0 \qquad \forall i \tag{32}$$

$$\begin{cases} \mu^{F}_{ij,\min} \ge 0 & \forall (i,j) \\ \mu^{F}_{ij,\max} \ge 0 & \forall (i,j) \end{cases} \tag{33}$$

where $\Delta^{\mathcal{S}} = \left\{ x^{A}_{i}, z^{A}_{g}, y^{A}_{ij}, \lambda^{B}_{i}, \lambda^{F}_{ij}, \mu^{G}_{g,\max}, \mu^{D}_{i,\max}, \mu^{F}_{ij,\min}, \mu^{F}_{ij,\max} \right\}$. The dual objective function (22) is equivalent to (1). Constraints (23)–(26) are identical to the attacker problem, where the defender's decisions are the input parameters. Constraints (27)–(33) are the associated dual constraints with operator problem. Note that dual variables λ^{B}_{i} in constraints (27) and (29) include different subscripts, namely $i(g)$ and $i(d)$, which respectively stand for the node in which generator unit g is located, and the node in which demand d is located.

3.3 Algorithm

The non-linear master problem and sub-problem presented in the previous sub-sections are linearized based on the linearization approaches described in [3, 24]. Considering C&CG framework, lower-bound (LB) and UB on the optimal value of objective function gradually construct with the master problem and the sub-problem respectively. The optimal solution of the master problem at each iteration is entered as a parameter into sub-problem and vice versa. The iterative procedure lasts until the gap between the LB and UB is less than the predefined threshold ϵ. The detailed steps of this iterative procedure are shown in the Algorithm 2 as follow.

Step 1: Initialization. Set LB and UB bounds to $-\infty$ and $+\infty$, respectively. Set the iteration counter to $v = 0$. Set attacker's variables $\hat{x}^{A}_{i,v} = 0$, $\hat{y}^{A}_{ij,v} = 0$, $\hat{z}^{A}_{g,v} = 0$.

Step 2: Update the iteration counter, $v \leftarrow v + 1$. Solve the master problem (13)–(21), using optimal values of attacker variables $\hat{x}^{A}_{i,v-1}$, $\hat{y}^{A}_{ij,v-1}$, $\hat{z}^{A}_{g,v-1}$ attained from *Step 3* (or initialization) to be given parameter. Obtain optimal solution value of variables $\Delta^{\mathcal{M}*}$. Update LB as $LB = \eta^{*}$ (the optimal solution denoted by $(\cdot)^{*}$ for the variables).

Step 3: Solve sub-problem (22)–(33) considering the optimal values of defender's variables $\hat{x}^{D}_{i,v}, \hat{y}^{D}_{ij,v}, \hat{z}^{D}_{g,v}$ to be given parameters. Obtain the optimal solution of sub-problem's variables $\Delta^{\mathcal{S}*}$. Update UB using

$$UB = \min \Bigg\{ UB, \Bigg[\sum_{i} P^{D}_{i} (\lambda^{B*}_{i} - \mu^{D*}_{i,\max}) + \sum_{g\in G} \mu^{G*}_{g,\max} P^{G}_{g,\max} (\hat{z}^{A}_{g} - 1) - \sum_{(i,j)\in L} B_{ij} U^{*}_{ij} (\mu^{F*}_{ij,\max} + \mu^{F*}_{ij,\min}) \Bigg] \Bigg\} \tag{34}$$

Step 4: If UB minus LB is lower than a predefined tolerance ϵ, terminate the algorithm and return the optimal solution in sets $\Delta^{\mathcal{S}*}$ and $\Delta^{\mathcal{M}*}$. Otherwise continue in *Step 2*.

4 Case study

The WSCC 9-bus, IEEE 24-bus and IEEE 118-bus systems are employed to demonstrate the performance of the proposed model. Note that the following considerations are made: $C_i^{Sh} = 1000$, $M = 1000$, C_g is equal to the quadratic coefficient of the quadratic generation cost, the maximum iteration for C&CG $\nu_{\max}$ is 50, and $\epsilon = 10^{-5}$. The algorithm is implemented and executed using PC with an Intel® Core™ i5 CPU running at 3.2 GHz and 8 GB RAM using GUROBI 7.0.2 under GAMS.

4.1 WSCC 9-bus system

The WSCC 9-bus system [27] with load level of 315 MW and optimum SOC equal to \$28.4 is employed in this section to perform the various analysis. Obtaining sensitivity of SOC to the number of defender's resources requires running the model multiple times with different resources. Note that in each sensitivity analysis, the attacker has full resources for the attack to all elements, and defender protects all the networks elements except one which study performs for those components.

Figure 3 demonstrates how the SOC varied when R^{DB} is changed. The network experiences full load-shed until defender hardens at least three buses. While SOC decreases gradually by increasing R^{DB}, the defender cannot decrease SOC by adding more than 7 resources for protecting buses. This protection status entails R^{DL} and R^{DG} to be at least 5 and 2 respectively.

We call this hardening status as the robust defending strategy, where the network has zero load shed for any number of attack, or in other words, the power system is robust against $N - k$ contingency. The sensitivity of SOC to the R^{DL} and R^{DG} are depicted in the Figs. 4 and 5 respectively. Figure 6 demonstrates the robust defending strategies for the WSCC 9-bus system, where the red elements stand for the protected one.

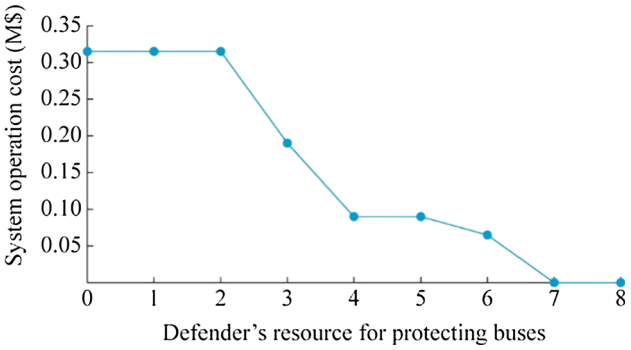

Fig. 3 Sensitivity of SOC to R^{DB} in WSCC 9-bus system

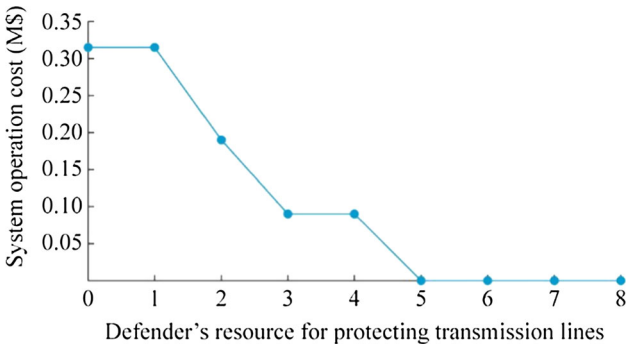

Fig. 4 Sensitivity of SOC to R^{DL} in WSCC 9-bus system

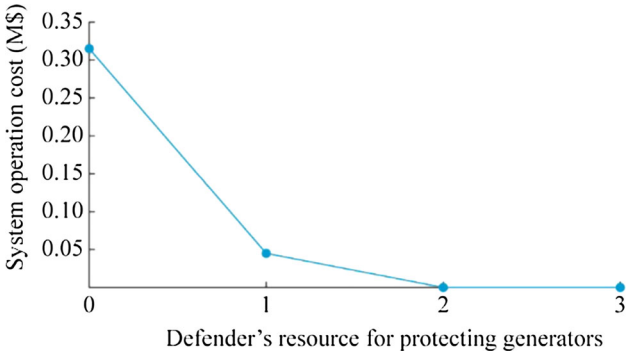

Fig. 5 Sensitivity of SOC to R^{DG} in WSCC 9-bus system

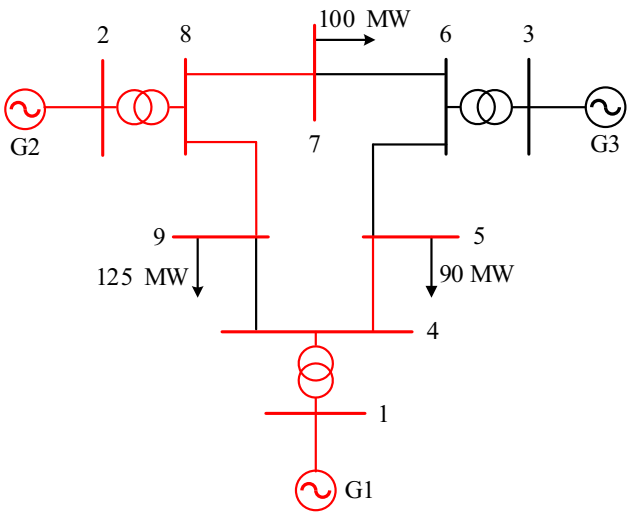

Fig. 6 Robust defending strategy for WSCC 9-bus system

Since the above sensitivity analyses are obtained by running the DAO problem with different defender resources, we can drive the vulnerability indices by feeding the Algorithm 1 according to the number of resources in the sensitivity analyses. After considering Algorithm 1 along with 21 runs of DAO, the vulnerability index in the WSCC 9-bus system for the buses, lines, and generators are shown in Figs. 7, 8, and 9 respectively. According to Fig. 7, the

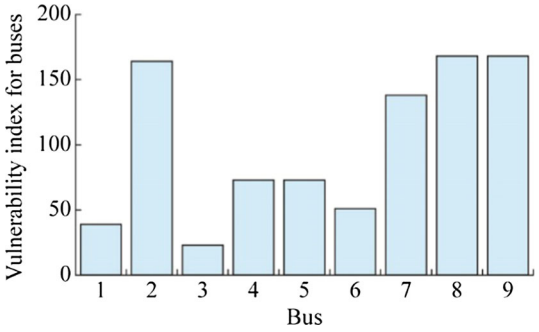

Fig. 7 Vulnerability index for buses in WSCC 9-bus system

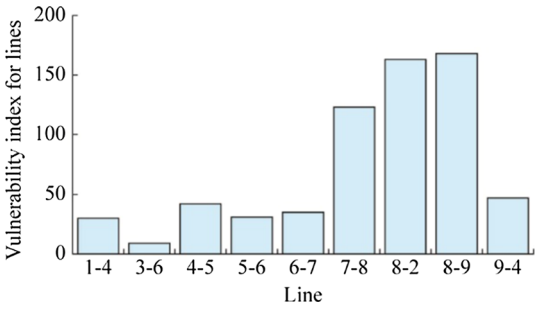

Fig. 8 Vulnerability index for lines in WSCC 9-bus system

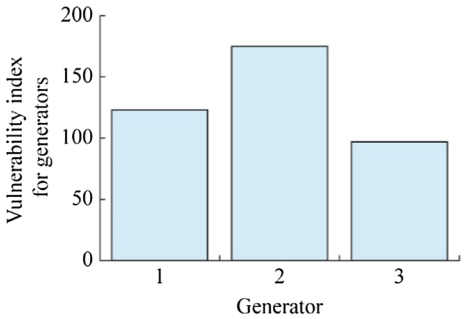

Fig. 9 Vulnerability index for generators in WSCC 9-bus system

ranking for the vulnerable buses in descending order is {9, 8, 2, 7, 5, 4, 1, 6, 3}. However, the buses {9, 8, 2} and {5, 4} have the same rank in the system. Figure 8 depicts the vulnerability indices for the lines. In this figure, line 8-2 and line 8-9 has the most I_V^L value, while line 3-6 is the last vulnerable line in the system. Needless to say that the defender protect vulnerable elements more frequently than others, like the generator 2 in Fig. 9.

4.2 IEEE 24-bus system

The IEEE 24-bus test system [28] consists of 12 generator units, 34 lines and 24 buses with the minimum SOC of $24702.73 employed to demonstrate the model's performance in this section. Figure 10 shows the robust defensive strategy for the current IEEE 24-bus, where the

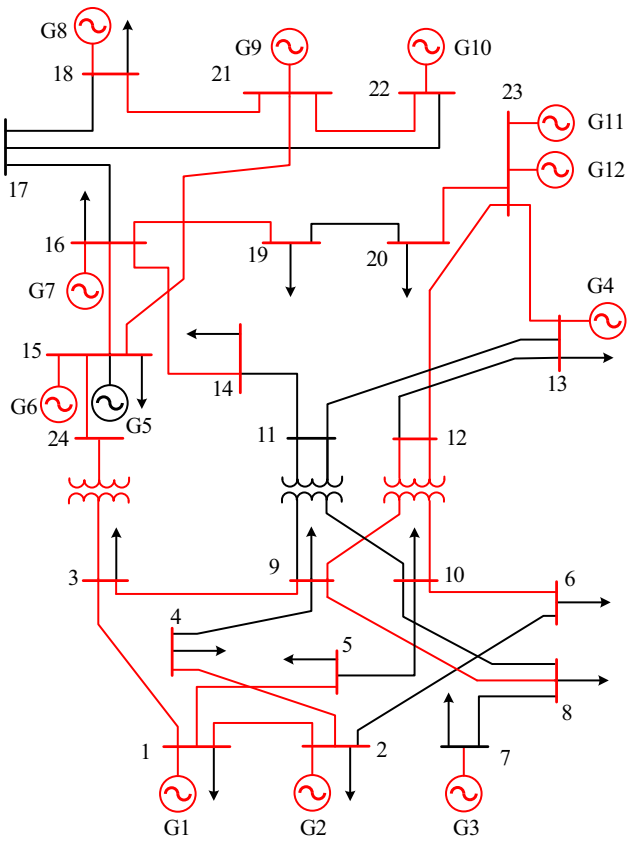

Fig. 10 Robust protecting strategy in IEEE 24-bus system

required resources are $R^{DB} = 21$, $R^{DL} = 22$, and $R^{DG} = 11$. One can decrease the number of necessary hardening resources by increasing the tight tolerable load shedding value to more than zero or applying reinforcement strategies for lines and generators.

Running the DAO model 11375 times on the IEEE 24-bus system results in more reliable vulnerability indices shown in Figs. 11, 12, and 13. According to these indices, bus 13, line 11 (between bus 7 and bus 8), and generator 4 are the most vulnerable components in the system.

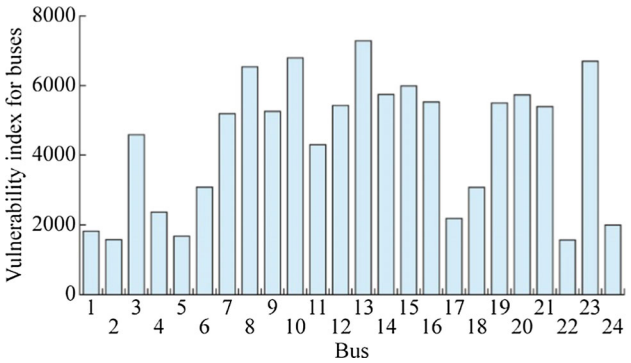

Fig. 11 Vulnerability index for buses in IEEE 24-bus system

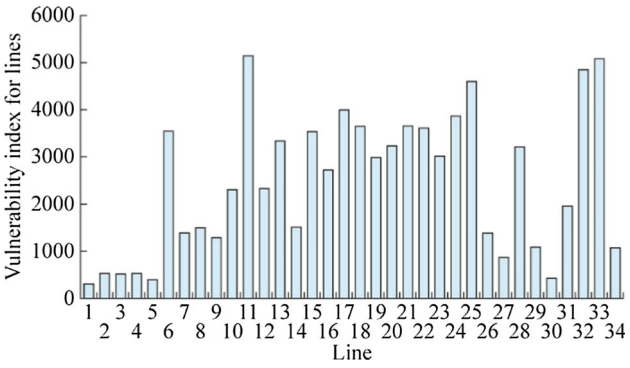

Fig. 12 Vulnerability index for lines in IEEE 24-bus system

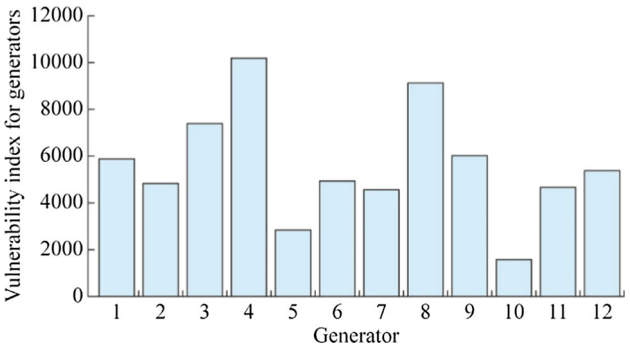

Fig. 13 Vulnerability index for generators in IEEE 24-bus system

A comprehensive sensitivity analyses of SOC to the defender's resources conducted in Fig. 14. As can be seen, different surfaces are created when the number of R^{DG} varied. It is shown that increasing R^{DG} to more than 7, has a slight effect on decreasing the SOC. Moreover, the system needs about 20 of each R^{DB} and R^{DL} to operate around the minimum operating cost.

4.3 IEEE 118-bus system

In this section, the proposed model is applied to the IEEE 118-bus system [27], with the load level of 4242 MW and optimum SOC of \$59.1. Note that $F_{ij,\max}, \forall(i,j)$ are considered as 150 MW. The studies are done to obtain robust defending strategies and the reliable vulnerability indices. To this end, Algorithm 1 was run 6700 times, with the different combination of the number of defender's resources for hardening.

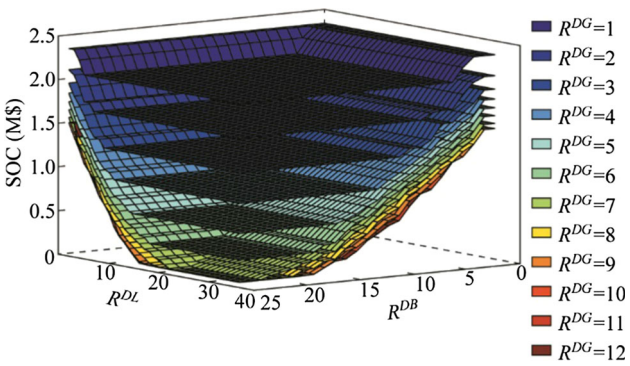

Fig. 14 Sensitivity of SOC to defender's resources in IEEE 24-bus system

Figure 15 shows the I_V^B, where the most vulnerable bus in the system, bus 77, was defended 6656 times, whereas bus 87 just defended 119 times. The robust defending strategies depicted in Fig. 16 can prove this attainment, in which bus 77 placed between two areas of the network, while bus 87 sited at an area with low connectivity.

The lines indices I_V^L are demonstrated in Fig. 17, where there are a few lines with a high level of vulnerability in the system. This phenomenon may due to the assumption made for $F_{ij,\max}$ in this study. However, there are still several lines with high I_V^L, that can be hardened to improve network resilience.

The last indices are represented in Fig. 18, where generators 29 and 30, connected to the buses 66 and 69 respectively, have the highest I_V^G, in contrast to the generator 51 (connected to bus 111) which has the lowest vulnerability within the system (Fig. 16).

5 Conclusion

This paper proposes novel approaches to assist network planner to improve power grid's resilience. While cyber and physical hazards are among the serious threats to the modern power networks, the effect of a man-made attack or Mother Nature's risk can be mitigated through preventive hardening strategies. To accomplish with an efficient hardening resources allocation for the power networks components, we propose the state-of-the-art vulnerability indices based on tri-level interdiction DAO problem.

The DAO problem is a leader-follower game-theoretic model, where a defender, attacker, and operator are the game players. To solve this complicated mathematical

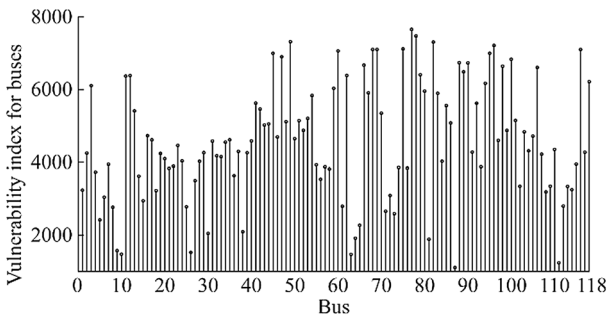

Fig. 15 Vulnerability index for buses in IEEE 118-bus system

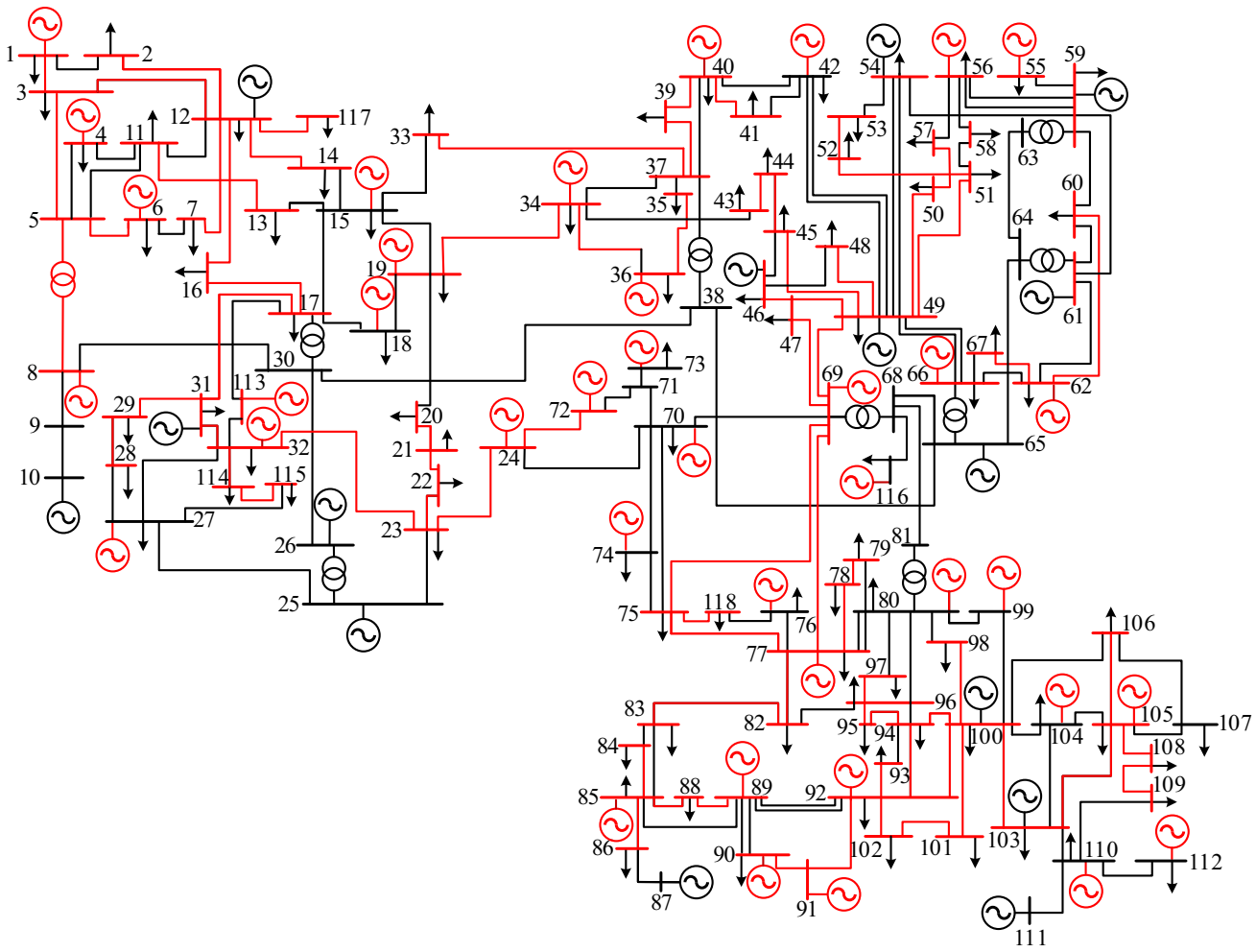

Fig. 16 Robust protecting strategy in IEEE 118-bus system

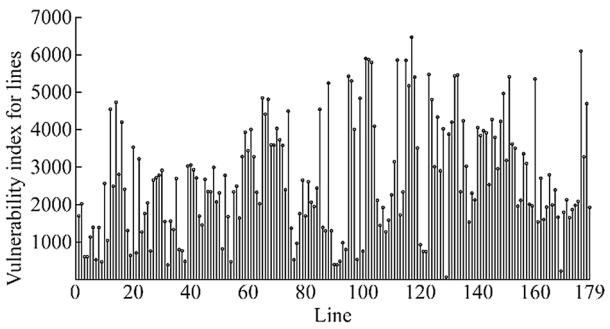

Fig. 17 Vulnerability index for lines in IEEE 118-bus system

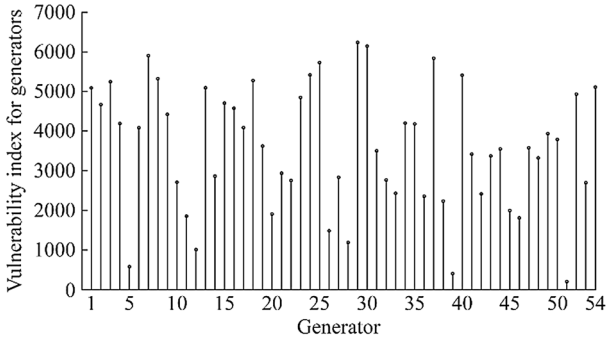

Fig. 18 Vulnerability index for generators in IEEE 118-bus system

programming, the whole problem decomposed to the so-called master problem and sub-problem and C&CG approach employed to obtain the solution iteratively.

Given the specified number of defender's resources for hardening, the DAO returns the best strategy for network protection. Iterating the game with different defender resources yields a various optimum strategy for network protection. Inspired by this fact, we propose vulnerability indices for the grid's elements which shows how a component is vulnerable to the threats, either natural hazard or crafted attack.

In addition to the vulnerability indices, we obtain a robust hardening strategy for the network, in which the system will be resilient against $N - k$ contingency.

The proposed methods are applied to the WSCC 9-bus, IEEE 24-bus, and IEEE 118-bus systems and the results show how vulnerable are the components against threats. These counter-intuitive outcomes are also proved by the robust hardening strategy, which suggests the set of protection tactics for the network components.

The extensive simulation studies on IEEE 24-bus and IEEE 118-bus systems validate that when the vulnerability indices obtained from more iteration of the proposed algorithm, the results are more reliable. Accordingly, one of the future extension of this paper is applying stochastic programming for the load, generation, and network topology beyond the different combination of resources for the defender.

References

[1] Vugrin E, Castillo A, Silva-Monroy C (2017) Resilience metrics for the electric power system: a performance-based approach. Report: SAND2017-1493

[2] Chan YP (2015) Network throughput and reliability: preventing hazards and attacks through gaming—part 1: modeling. In: Chan YP (ed) Game theoretic analysis of congestion, safety and security. Springer, Heidelberg, pp 113–139

[3] Davarikia H (2017) Investment plan against malicious attacks on power networks: multilevel game-theoretic models with shared cognition. Dissertation, University of Arkansas at Little Rock

[4] Preston BL, Backhaus SN, Ewers M et al (2016) Resilience of the US electricity system: a multi-hazard perspective. https://www.energy.gov/sites/prod/files/2017/01/f34/Resilience%20of%20the%20U.S.%20Electricity%20System%20A%20Multi-Hazard%20Perspective.pdf. Accessed 18 August 2016

[5] Ouyang M, Duenas-Osorio L (2014) Multi-dimensional hurricane resilience assessment of electric power systems. Struct Saf 48:15–24

[6] Panteli M, Trakas DN, Mancarella P et al (2016) Boosting the power grid resilience to extreme weather events using defensive islanding. IEEE Trans Smart Grid 7(6):2913–2922

[7] Davarikia H, Znidi F, Aghamohammadi MR et al (2016) Identification of coherent groups of generators based on synchronization coefficient. In: Proceedings of power and energy society general meeting (PESGM), Boston, USA, 17–21 July 2016, 5 pp

[8] Znidi F, Davarikia H, Iqbal K (2017) Modularity clustering based detection of coherent groups of generators with generator integrity indices. In: Proceedings of IEEE power and energy society general meeting, Chicago, USA, 16–20 July 2017, 5 pp

[9] Davarikia H, Barati M, Znidi F et al (2018) Real-time integrity indices in power grid: a synchronization coefficient based clustering approach. https://arxiv.org/abs/1804.02793. Accessed 9 April 2018

[10] Panteli M, Pickering C, Wilkinson S et al (2017) Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures. IEEE Trans Power Syst 32(5):3747–3757

[11] Yuan W, Wang J, Qiu F et al (2016) Robust optimization-based resilient distribution network planning against natural disasters. IEEE Trans Smart Grid 7(6):2817–2826

[12] Wood RK (1993) Deterministic network interdiction. Math Comput Model 17(2):1–18

[13] Fulkerson DR, Harding GC (1977) Maximizing the minimum source-sink path subject to a budget constraint. Math Program 13(1):116–118

[14] Golden B (1978) A problem in network interdiction. Naval Res Log Q 25(4):711–713

[15] Corley H, David YS (1982) Most vital links and nodes in weighted networks. Oper Res Lett 1(4):157–160

[16] Malik K, Mittal AK, Gupta SK (1989) The k most vital arcs in the shortest path problem. Oper Res Lett 8(4):223–227

[17] Yao Y, Edmunds T, Papageorgiou D et al (2007) Trilevel optimization in power network defense. IEEE Trans Syst Man Cybern Part C (Appl Rev) 37(4):712–718

[18] Arroyo JM (2010) Bilevel programming applied to power system vulnerability analysis under multiple contingencies. IET Generation, Transmission & Distribution 4(2):178–190

[19] Romero N, Xu N, Nozick LK et al (2012) Investment planning for electric power systems under terrorist threat. IEEE Trans Power Syst 27(1):108–116

[20] Wu X, Conejo AJ (2017) An efficient tri-level optimization model for electric grid defense planning. IEEE Trans Power Syst 32(4):2984–2994

[21] Alguacil CN, Arroyo SJM (2014) A trilevel programming approach for electric grid defense planning. Comput Oper Res 41:282–290

[22] Zeng B, Zhao L (2013) Solving two-stage robust optimization problems using a column-and-constraint generation method. Oper Res Lett 41(5):457–461

[23] Wang C, Wei W, Wang J et al (2017) Robust defense strategy for gas-electric systems against malicious attacks. IEEE Trans Power Syst 32(4):2953–2965

[24] Conejo AJ, Morales LB, Kazempour SJ et al (2016) Investment in electricity generation and transmission: decision making under uncertainty. Springer, Heidelberg

[25] Salmeron J, Wood K, Baldick R (2009) Worst-case interdiction analysis of large-scale electric power grids. IEEE Trans Power Syst 24(1):96–104

[26] Conejo AJ, Castillo E, Minguez R et al (2006) Decomposition techniques in mathematical programming: engineering and science applications. Springer, Heidelberg

[27] Zimmerman RD, Murillo-Sánchez CE, Thomas RJ (2011) MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans Power Syst 26(1):12–19

[28] Grigg C, Wong P, Albrecht P et al (1999) The IEEE reliability test system-1996: a report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee. IEEE Trans Power Syst 14(3):1010–1020

Hamzeh DAVARIKIA received the B.Sc. and M.Sc. degrees in electrical engineering from Power and Water University of Technology (Abbaspour School of Engineering, Shahid Beheshti University), and Shahed University, Tehran, Iran, in 2009 and 2011, respectively.

He received an M.Sc. degree in systems engineering from University of Arkansas at Little Rock in 2017. He is currently pursuing the Ph.D. degree in electrical engineering at the Louisiana State University. His research interests include operations research and optimization in power networks.

Masoud BARATI received the Ph.D. degree in electrical engineering from Illinois Institute of Technology, Chicago, in 2013. Presently, he is an assistant professor in the Electrical and Computer Engineering Department at University of Pittsburgh, Pittsburgh, USA. His research interests include optimization, microgrid operation and planning, microeconomics, mathematical modeling and multiple infrastructure assessment.