POWER SYSTEM DEFENSE PLANNING AGAINST MULTIPLE CONTINGENCIES

Andrés Delgadillo
Universidad Pontificia Comillas
Madrid, Spain
Andres.Delgadillo@iit.upcomillas.es

José M. Arroyo
Universidad de Castilla-La Mancha
Ciudad Real, Spain
JoseManuel.Arroyo@uclm.es

Natalia Alguacil
Universidad de Castilla-La Mancha
Ciudad Real, Spain
Natalia.Alguacil@uclm.es

Abstract - This paper addresses the allocation of defensive resources in a power system under multiple contingencies. This problem is characterized by a defender-attacker-defender model which is formulated as a trilevel programming problem. In the first level, the system planner identifies the components to be hardened in order to reduce the damage associated with plausible outages. In the second level, the disruptive agent determines the set of out-of-service components so that the damage in the system is maximized. Finally, in the third level, the system operator minimizes the damage caused by the outages selected by the disruptive agent by means of an optimal operation of the power system. We propose a novel two-stage solution approach that attains optimality with moderate computational effort. The original trilevel program is first transformed into an equivalent bilevel program, which is subsequently solved by an efficient implicit enumeration algorithm. The effectiveness of the proposed methodology is validated on the IEEE Reliability Test System.

Keywords - Load shedding, multiple contingencies, power system defense, trilevel programming, vulnerability.

1 INTRODUCTION

POWER systems have become fundamental for the development of national economies worldwide [1], [2]. As any other critical infrastructure, power systems are subject to disruptions, either unintentional or deliberate, that may have a significant impact on their performance. The vulnerability of power systems has been uncovered by recent blackouts in industrialized countries [3]. Moreover, these catastrophic events have revealed that traditional security assessment tools such as the N-1 and N-2 criteria [1] are insufficient to cope with multiple contingencies. Therefore, it is of utmost importance to devise new tools and procedures to guarantee the correct operation of power systems even under the most adverse situations. As a consequence, research effort is required with two main goals: (i) to study the vulnerability of power systems, and (ii) to determine strategies to mitigate such vulnerability.

The first goal has been extensively addressed with the development of attacker-defender models for both intentional and unintentional outages [4]-[6]. Attacker-defender models allow identifying the critical components in a power system, i.e., those assets whose outage would yield the maximum damage to the system. These models are instances of bilevel programming [7] that have been solved by equivalent transformations to mixed-integer programs [4], [6] and decomposition-based approaches inspired by Benders decomposition [5].

In contrast to vulnerability analysis, little attention has been paid to the vulnerability mitigation of power systems. According to [2], several strategies for vulnerability reduction can be implemented such as adding new assets for purposes of redundancy, and hardening the infrastructure or improving its active defenses so that the hardened or defended assets become invulnerable. With respect to adding redundancy in a power system, transmission network expansion planning was proposed in [8] as an effective tool to mitigate the impact of deliberate outages on the performance of the transmission network. As for power system defense planning, this problem was addressed in [2], [9], [5].

Brown *et al.* [2] proposed a general defender-attacker-defender model to allocate budget-limited defensive resources in any critical infrastructure including power systems. In addition, Benders decomposition was suggested as a potential solution technique. Although this work provided some theoretical insight into the problem, no computational procedure was described for its solution.

In [9], Yao *et al.* first formulated the defense problem of a power system as a trilevel program [7] based on the general defender-attacker-defender model proposed in [2]. The solution method consisted in a decomposition-based approach that iteratively solved smaller nested bilevel programming problems. However, these bilevel problems were selected in a non-systematic sequence and solved by an iterative time-consuming procedure.

Bier *et al.* [5] presented a heuristic iterative approach to determine the optimal hardening of power system components. The methodology comprised three nested algorithms respectively corresponding to the agents of a defender-attacker-defender model. The main drawback of this approach was its reliance on a suboptimal strategy that identified the most heavily loaded lines as critical.

This paper presents a new optimization-based approach for the optimal allocation of defensive resources in a power system so that its vulnerability against multiple contingencies is mitigated. Vulnerability is measured in terms of the system load shed. Similar to [2], [5], [9], this problem is characterized by a defender-attacker-defender model wherein the defense plan takes into account the worst-case contingency set. Furthermore, optimal operation of the system under contingency is modeled. The resulting problem is formulated as a mixed-integer nonlinear trilevel program. The distinctive feature of the proposed approach with respect to [2], [5], [9] is the application of a two-stage solution methodology based on mathematical programming. First, the original trilevel program is transformed into an equivalent mixed-integer bilevel programming problem by replacing the two lowermost problems with a single-level equivalent. This stage uses an effective transformation previously reported in [4], [6]. In the second stage an efficient implicit enumeration algorithm is applied to the bilevel program derived in the first stage. The implicit enumeration algorithm was developed by Scaparra and Church [10] to solve a similar bilevel program for the protection of a logistic network. The proposed two-stage method presents the following main advantages over the approaches described in [2], [5], [9]: (i) the conversion to a bilevel programming problem is exact and computationally efficient, (ii) the implicit enumeration algorithm implements a systematic and sound solution search analogous to the branch-and-bound algorithm used in mixed-integer linear programming, and (iii) optimality is guaranteed in a finite number of steps.

The major contributions of this paper are:

1. The system planner is provided with a tool to optimally allocate defensive or hardening resources in order to mitigate power system vulnerability against multiple contingencies.
2. The resulting trilevel programming problem is solved by a two-stage approach based on the novel application of a previously reported implicit enumeration algorithm.
3. The performance of the proposed technique is successfully validated with numerical results. The methodology is effective in attaining globally optimal solutions with moderate computational effort.

The remainder of this paper is organized as follows. Section 2 highlights the differences between an attacker-defender model and a defender-attacker-defender model. Section 3 presents the trilevel formulation of the power system defense planning problem. Section 4 describes the proposed solution methodology. Section 5 provides and discusses some numerical results. Finally, Section 6 draws relevant conclusions.

2 ATTACKER-DEFENDER VERSUS DEFENDER-ATTACKER-DEFENDER MODELS

Worst-case analysis is crucial for vulnerability assessment and mitigation of critical infrastructures. Attacker-defender models and defender-attacker-defender models are examples of such worst-case analysis [2] considering both natural-occurring events and malicious attacks.

Attacker-defender models have been recently used to analyze the vulnerability of power systems under multiple contingencies [4]-[6]. These models characterize a decision-making problem involving two different agents, namely an attacker and a defender, who optimize their respective objective functions over a jointly dependent set. Under a worst-case analysis, the attacker or disruptive agent, which may represent either nature or a group of terrorists, determines the set of out-of-service system components with the goal of maximizing the system damage and subject to limited disruptive resources. The defender, which is identified with the system operator, reacts against the outages determined by the attacker to minimize the damage inflicted on the system.

Attacker-defender models are useful in finding critical components, but they do not explicitly determine which components have to be defended. As explained in [2], defending those components that are identified as critical by an attacker-defender model does not necessarily provide the best protection against a system disruption. Thus, new models are needed to determine the optimal defense plan for a power system exposed to multiple contingencies.

As shown in [2], [5], [9], a defender-attacker-defender model is suitable for the defense planning of critical infrastructures such as power systems. This model involves three agents acting in sequence: (i) a system planner who identifies the system components to be defended or hardened in order to minimize the damage caused by out-of-service components, (ii) a disruptive agent who determines the most-damaging set of out-of-service components, and (iii) the system operator who responds to any disruptive action by means of some corrective measures to minimize the overall damage.

Each agent optimizes its own objective function subject to the reaction of the agent of the subsequent level. Thus, the system planner considers the response of the disruptive agent whereas the reaction of the system operator is included in the constraint set of the disruptive agent. Moreover, it is assumed that defensive and disruptive resources are both limited.

3 PROBLEM FORMULATION

This section presents the mathematical formulation of the defender-attacker-defender model used for the power system defense planning problem. For the sake of clarity and simplicity, we consider that transmission lines and transformers (which are both characterized by their series reactance) are the only assets that can be respectively defended and disrupted by the system planner and the disruptive agent. Notwithstanding, the proposed approach can be straightforwardly extended to account for the defense and disruption of other power system components.

The optimal allocation of defensive resources is formulated as the following trilevel program:

$$\min_{w} \sum_{n \in N} \Delta P_n^{d^*} \tag{1}$$

subject to:

$$\sum_{l \in L} w_l = Z \tag{2}$$

$$w_l \in \{0,1\}; \qquad \forall l \in L, \tag{3}$$

where

$$\sum_{n \in N} \Delta P_n^{d^*} = \max_{v} \sum_{n \in N} \Delta P_n^{d'} \tag{4}$$

subject to:

$$v_l \geq w_l; \qquad \forall l \in L \tag{5}$$

$$\sum_{l \in L} (1 - v_l) \leq M \tag{6}$$

$$v_l \in \{0, 1\}; \qquad \forall l \in L, \tag{7}$$

and where

$$\Delta P_n^{d'} \in \arg\left\{ \min_{P^f, P^g, \delta, \Delta P^d} \sum_{n \in N} \Delta P_n^d \right. \tag{8}$$

subject to:

$$P_l^f = v_l \frac{1}{x_l} \left[\delta_{O(l)} - \delta_{D(l)} \right] : (\mu_l); \qquad \forall l \in L \tag{9}$$

$$\sum_{j \in J_n} P_j^g - \sum_{l|O(l)=n} P_l^f + \sum_{l|D(l)=n} P_l^f + \Delta P_n^d = P_n^d : (\lambda_n); \quad \forall n \in N \tag{10}$$

$$0 \leq P_j^g \leq \overline{P}_j^g : (\gamma_j); \qquad \forall j \in J \tag{11}$$

$$-\overline{P}_l^f \leq P_l^f \leq \overline{P}_l^f : (\phi_l, \varphi_l); \qquad \forall l \in L \tag{12}$$

$$-\overline{\delta} \leq \delta_n \leq \overline{\delta} : (\chi_n, \xi_n); \qquad \forall n \in N \tag{13}$$

$$\left. 0 \leq \Delta P_n^d \leq P_n^d : (\alpha_n); \qquad \forall n \in N \right\}. \tag{14}$$

Note that w is the vector of defended components, N is the set of indices of buses, ΔP_n^d is the load shed at bus n, L is the set of indices of transmission assets, w_l is a binary variable that is equal to 1 if transmission asset l is defended and 0 otherwise, Z is the number of transmission assets to be defended, v is the vector of out-of-service components, v_l is a binary variable that is equal to 0 if transmission asset l is out of service and 1 otherwise, M is the maximum number of out-of-service transmission assets, P^f is the vector of power flows, P^g is the vector of generator power outputs, δ is the vector of nodal phase angles, ΔP^d is the vector of nodal loads shed, P_l^f is the power flow of transmission asset l, x_l is the reactance of transmission asset l, δ_n is the phase angle at bus n, $O(l)$ is the origin or sending bus of transmission asset l, $D(l)$ is the destination or receiving bus of transmission asset l, J_n is the set of indices of generators connected to bus n, P_j^g is the power output of generator j, P_n^d is the demand at bus n, $\overline{P}_j^g$ is the capacity of generator j, J is the set of indices of generators, $\overline{P}_l^f$ is the power flow capacity of transmission asset l, and $\overline{\delta}$ is the upper bound for the nodal phase angles.

Problem (1)-(14) comprises three optimization levels: the upper level (1)-(3), which is associated with the system planner; the middle level (4)-(7), characterizing the behavior of the disruptive agent; and the lower level (8)-(14), corresponding to the system operator. The system planner controls the vector of binary variables w, which models the defense of transmission components. The disruptive agent controls the vector of binary variables v characterizing the operative state of transmission assets. Finally, the system operator controls the vectors of continuous variables P^f, P^g, δ, and ΔP^d. Dual variables associated with the lower-level problem (8)-(14) are in parentheses.

It should be noted that the middle-level problem is parameterized in terms of the upper-level variables w_l. Similarly, the lower-level problem is parameterized in terms of the middle-level variables v_l. It is also worth mentioning that lower-level decision variables ΔP_n^d are present in the objective functions of the upper- and middle-level optimizations. The asterisk and the apostrophe in (1), (4), and (8) are used to indicate that ΔP_n^d are decision variables of the lower-level problem.

The objective of the system planner is to minimize the damage, which is expressed as the system load shed (1). This vulnerability measure is widely used in the technical literature [4]-[6]. The number of simultaneously defended transmission assets is set in (2). Constraints (3) model the binary nature of variables w_l.

In contrast, the disruptive agent maximizes the system load shed (4) by disrupting undefended assets (5). Note that constraints (5) relate upper-level decision variables w_l with middle-level decision variables v_l. We assume that if transmission asset l is defended, i.e., $w_l = 1$, the disruptive agent cannot disable this component. Hence, the corresponding variable v_l is set to 1. In other words, if a line or transformer is defended it becomes invulnerable. Constraint (6) models the limitation on the number of transmission assets that can be simultaneously out of service. Constraints (7) impose the integrality of variables v_l.

The system operator is modeled by the optimal power flow (8)-(14). The objective of the system operator (8) is to minimize the system load shed under the combination of out-of-service transmission assets v chosen by the disruptive agent. Constraints (9) express the network power flows in terms of the nodal phase angles and the middle-level decision variables v_l. As is commonly assumed in the technical literature related to power system vulnerability [4]-[6], [8], [9], a dc model of the transmission system is used. Note that if transmission asset l is disrupted, i.e., $v_l = 0$, the corresponding power flow is set to 0. Constraints (10) represent the power balance at each bus of the system. Upper and lower bounds on lower-level decision variables are imposed in constraints (11)-(14).

Problem (1)-(14) is a mixed-integer nonlinear trilevel programming problem. The presence of binary decision variables in the middle level does not allow obtaining an equivalent single-level problem [2]. Moreover, the decomposition-based approaches proposed in the technical literature [2], [5], [9] might present difficulties in attaining optimality within moderate computing times. Thus, exact and efficient solution procedures are yet to be explored.

4 SOLUTION METHODOLOGY

The proposed solution approach consists of two stages. In the first stage, the original trilevel programming problem (1)-(14) is equivalently transformed into a bilevel programming problem. In the second stage, an effective implicit enumeration algorithm is applied to the bilevel program resulting from the first stage.

4.1 Stage 1: Transformation to an Equivalent Bilevel Program

Using the methodology described in [4], [6], the bilevel problem comprising the middle- and lower-level optimizations (4)-(14) can be equivalently recast as a single-level problem. Therefore, the original trilevel problem (1)-(14) is transformed into the following equivalent bilevel programming problem:

$$\min_{w} \sum_{n \in N} \Delta P_n^{d^*} \qquad (15)$$

subject to:

$$\sum_{l \in L} w_l = Z \qquad (16)$$

$$w_l \in \{0,1\}; \qquad \forall l \in L, \qquad (17)$$

where

$$\Delta P_n^{d^*} \in \arg\left\{ \max_{\substack{P^f, P^g, v, \alpha, \gamma, \delta, \\ \Delta P^d, \lambda, \mu, \xi, \phi, \varphi, \chi}} \sum_{n \in N} \Delta P_n^d \right. \qquad (18)$$

subject to:

$$v_l \geq w_l; \qquad \forall l \in L \qquad (19)$$

$$\sum_{l \in L} (1 - v_l) \leq M \qquad (20)$$

$$v_l \in \{0,1\}; \qquad \forall l \in L \qquad (21)$$

$$P_l^f = v_l \frac{1}{x_l} \left[\delta_{O(l)} - \delta_{D(l)} \right]; \qquad \forall l \in L \qquad (22)$$

$$\sum_{j \in J_n} P_j^g - \sum_{l|O(l)=n} P_l^f + \sum_{l|D(l)=n} P_l^f + \Delta P_n^d = P_n^d; \qquad \forall n \in N \qquad (23)$$

$$0 \leq P_j^g \leq \overline{P}_j^g; \qquad \forall j \in J \qquad (24)$$

$$-\overline{P}_l^f \leq P_l^f \leq \overline{P}_l^f; \qquad \forall l \in L \qquad (25)$$

$$-\overline{\delta} \leq \delta_n \leq \overline{\delta}; \qquad \forall n \in N \qquad (26)$$

$$0 \leq \Delta P_n^d \leq P_n^d; \qquad \forall n \in N \qquad (27)$$

$$-\lambda_{O(l)} + \lambda_{D(l)} + \mu_l + \phi_l + \varphi_l = 0; \qquad \forall l \in L \qquad (28)$$

$$\lambda_n|_{j \in J_n} + \gamma_j \leq 0; \qquad \forall j \in J \qquad (29)$$

$$-\sum_{l|O(l)=n} \frac{1}{x_l} v_l \mu_l + \sum_{l|D(l)=n} \frac{1}{x_l} v_l \mu_l + \chi_n + \xi_n = 0; \qquad \forall n \in N \qquad (30)$$

$$\lambda_n + \alpha_n \leq 1; \qquad \forall n \in N \qquad (31)$$

$$\gamma_j \leq 0; \qquad \forall j \in J \qquad (32)$$

$$\phi_l \geq 0; \qquad \forall l \in L \qquad (33)$$

$$\varphi_l \leq 0; \qquad \forall l \in L \qquad (34)$$

$$\chi_n \geq 0; \qquad \forall n \in N \qquad (35)$$

$$\xi_n \leq 0; \qquad \forall n \in N \qquad (36)$$

$$\alpha_n \leq 0; \qquad \forall n \in N \qquad (37)$$

$$\left. \sum_{n \in N} \Delta P_n^d = \sum_{l \in L} (\varphi_l - \phi_l) \overline{P}_l^f + \sum_{n \in N} (\alpha_n + \lambda_n) P_n^d + \sum_{j \in J} \gamma_j \overline{P}_j^g + \sum_{n \in N} (\xi_n - \chi_n) \overline{\delta} \right\}. \qquad (38)$$

The upper-level problem (15)-(17) is identical to the upper-level problem (1)-(3) of the original trilevel program.

The lower-level problem (18)-(38) of the bilevel equivalent is associated with the two lowermost levels (4)-(14) of the original trilevel program. The objective function (18) and constraints (19)-(21) are identical to (4)-(7), respectively. The remaining constraints comprise the primal constraints (22)-(27) and the dual feasibility constraints (28)-(37) of the original lower-level problem (8)-(14), as well as the equality associated with the strong duality theorem (38), where the primal and dual lower-level objective functions are equated. Nonlinear expressions (22) and (30) involving the product of binary variables and continuous variables are subsequently transformed into linear expressions using some well-known integer algebra results. Further details on this equivalent transformation can be found in [4], [6].

4.2 Stage 2: Implicit Enumeration Algorithm

Similar to problem (1)-(14), the binary nature of lower-level decision variables v in the bilevel problem (15)-(38) resulting from the first stage requires the use of alternative solution approaches. Scaparra and Church [10] derived an implicit enumeration algorithm for a bilevel programming problem associated with the defense planning of a logistic network, whose structure is essentially identical to that of problem (15)-(38). Therefore, the findings by Scaparra and Church are straightforwardly applicable here.

The implicit enumeration algorithm explores a search tree based on the following premise: the optimal set of defended components selected by the system planner must include at least one of the critical assets identified by the disruptive agent when no component is defended. It should be noted that if none of the critical assets is defended then the disruptive agent would disable this critical set and the worst-case interdiction would not be prevented by the defense plan selected by the system planner.

Due to their analogies, the implicit enumeration algorithm borrows the terminology from the branch-and-bound algorithm for mixed-integer linear programming. The algorithm starts at the root node of the search tree by solving the lower-level problem (18)-(38) with no defended transmission assets. The optimal disruption plan represents the set of candidate components to be defended associated with the root node. Based on the aforementioned premise, the system planner must then harden at least one of these assets. This is implemented by a process referred to as branching where new nodes are created according to the new defense plans resulting from the solution to problem (18)-(38) at the parent nodes. Branching is implemented until either the number of simultaneously defended assets is reached or no more candidate components are available for defense, being the corresponding node denoted as a leaf. The implicit enumeration algorithm is stopped when branching can no longer be performed. The optimal solution is the feasible defense plan with the lowest value of the upper-level objective function (15).

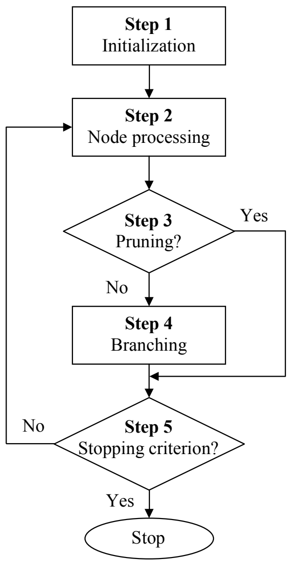

Figure 1: Flowchart of the implicit enumeration algorithm

The proposed methodology is illustrated in Fig. 1 and works as follows:

1. *Initialization.* Initialize the node set K with the root node associated with the undefended network, i.e., $w_l^{(0)} = 0, \forall l \in L$, and set the optimal system load shed $z^{best} = \infty$.

2. *Node processing.* Select and remove a node m from K. If node m is the root node or it was created from setting any w_l to 1 then solve its associated lower-level problem (18)-(38) for the corresponding vector $w^{(m)}$, thus yielding $v^{(m)}$ and $\sum_{n \in N} \Delta P_n^{d(m)}$. Those assets l with $v_l^{(m)} = 0$ constitute the set of candidate components for defense $C^{(m)}$. If $\sum_{n \in N} \Delta P_n^{d(m)} < z^{best}$ then the solution is stored as the optimal solution and $z^{best} = \sum_{n \in N} \Delta P_n^{d(m)}$.

   If node m was created from setting any w_l to 0 then candidate components for defense at the parent node except transmission asset l constitute $C^{(m)}$.

3. *Pruning.* If the number of defended assets is reached or $C^{(m)}$ is empty then go to step 5 since node m becomes a leaf.

4. *Branching.* Choose an element l from the the set of candidate components for defense $C^{(m)}$ and create two new nodes. At one node transmission asset l is hardened, i.e., the vector of defended assets w is updated by setting $w_l = 1$. At the other node asset l is not hardened, i.e., $w_l = 0$. Add the newly created nodes to the node set K.

5. *Stopping criterion.* If the node set K is empty, then exit the algorithm with the optimal solution; otherwise go to step 2.

Similar to the branch-and-bound algorithm, the implicit enumeration provides a systematic search that guarantees optimality in a finite number of node evaluations. As shown in [10], the upper bound for the number of node evaluations is $\frac{M^{Z+1}-1}{M-1}$, which does not depend on the system size and is significantly lower than the total number of feasible solutions $\binom{card(L)}{Z}\binom{card(L)-Z}{M}$.

It is worth mentioning that the most time-consuming aspect of the above procedure is the solution of the lower-level problem (18)-(38) in step 2. This step is suitable for parallel implementation, thereby leading to significant computational savings. In addition, the optimal solution to problem (18)-(38) at the parent node might be used as a starting solution for the evaluation at the next branching level. Note, however, that these implementation details are beyond the scope of this paper.

5 NUMERICAL RESULTS

The proposed approach has been tested on the IEEE Reliability Test System [6]. This system comprises 24 buses, 38 transmission assets, 32 generators, and 17 loads. The load profile corresponds to a winter weekday at 18:00. Circuits sharing the same towers are treated as independent lines; e.g., line 20-23 has two circuits: 20-23A and 20-23B. Defense schemes of up to five components and disruption plans comprising up to twelve transmission assets have been considered. In all of the simulations $\overline{\delta}$ has been set to $\pi/2$ rad.

The proposed two-stage algorithm was implemented on a Sun Fire X4140 X64 with 2 processors at 2.30 GHz and 8 GB of RAM using MATLAB. The optimization problems were solved with CPLEX 11.0 under GAMS.

Table 1 lists the sets of critical components when the system is not defended. Due to space limitations, critical sets are shown for a maximum of six simultaneous out-of-service transmission assets. For $M = 1$ there are no critical components since this test system requires at least two out-of-service assets to cause load shedding. Note that for $M = 4$ there are two different sets of out-of-service components that yield the same maximum level of system load shed. Analogously, for $M = 5$ and $M = 6$ there are four different critical sets.

M	Critical components
1	–
2	11-14, 14-16
3	16-19, 20-23A, 20-23B
4	3-24, 12-23, 13-23, 14-16
	12-23, 13-23, 14-16, 15-24
5	3-24, 9-12, 10-12, 11-13, 14-16
	3-24, 11-13, 12-13, 12-23, 14-16
	9-12, 10-12, 11-13, 14-16, 15-24
	11-13, 12-13, 12-23, 14-16, 15-24
6	3-24, 7-8, 9-12, 10-12, 11-13, 14-16
	3-24, 7-8, 11-13, 12-13, 12-23, 14-16
	7-8, 9-12, 10-12, 11-13, 14-16, 15-24
	7-8, 11-13, 12-13, 12-23, 14-16, 15-24

Table 1: Sets of out-of-service components without defense

Tables 2 and 3 present the optimal results attained by the proposed two-stage algorithm. Table 2 shows the optimal levels of system load shed. As can be seen, the defense of transmission assets is an effective action for vulnerability mitigation since it significantly reduces the maximum damage associated with multiple contingencies. For example, when five components are defended, i.e., $Z = 5$, vulnerability drops between 97.4% for $M = 2$ and 45.4% for $M = 12$.

Table 3 provides the optimal defense plans. Note that at least one of the critical components identified in Table 1 for each value of M is included in the corresponding defense plans. However, it is worth emphasizing that most optimal defense plans include components that do not belong to the associated critical sets of Table 1. Both observations also hold for values of M exceeding 6. As an example, for $M = 4$ and $Z = 4$, the defense of any of the critical sets listed in Table 1 (transmission assets 3-24, 12-23, 13-23, and 14-16, or assets 12-23, 13-23, 14-16, and 15-24) yields a level of system load shed equal to 387 MW. In contrast, the optimal solution is the defense of assets 7-8, 10-12, 12-23, and 14-16, resulting in 309 MW of system load shed, i.e., a 20.2% of vulnerability reduction with respect to the intuitive solutions.

	Z					
M	0	1	2	3	4	5
1	0	0	0	0	0	0
2	194	136	74	71	5	5
3	309	212	194	180	171	136
4	516	387	342	322	309	248
5	842	648	617	448	423	320
6	1017	823	617	503	457	442
7	1017	872	798	639	617	511
8	1198	1047	957	732	651	602
9	1373	1132	957	822	725	612
10	1373	1198	1028	893	765	727
11	1428	1293	1068	940	877	749
12	1468	1340	1178	1020	892	801

Table 2: Optimal levels of system load shed (MW)

Fig. 2 shows the percentage marginal improvements in vulnerability mitigation derived from increasing the number of defended components. This figure is useful to analyze the effect of adding defensive resources on the overall vulnerability mitigation. Moreover, this figure provides the system planner with relevant information on the trade-off between defense cost and the gain in vulnerability mitigation. Most of the defense benefit is achieved with a maximum of one or two defended assets, since they contribute more than 50% of the overall improvement. In contrast, larger defense investments produce progressively lower vulnerability reductions.

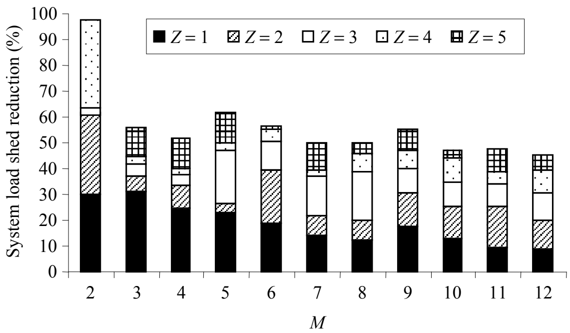

Figure 2: Marginal system load shed reduction

	Z														
M	1	2		3			4				5				
2	11-14	2-6	11-14	2-4	2-6	11-14	1-5	2-4	6-10	11-14	1-5	2-6	3-9	4-9	14-16
3	16-19	15-21A	16-19	11-14	15-21A	16-19	1-3	11-14	15-21A	16-19	3-9	7-8	11-14	15-21A	16-19
4	14-16	14-16	15-21B	7-8	11-13	14-16	7-8	10-12	12-23	14-16	9-12	12-23	14-16	16-17	20-23B
5	14-16	9-12	12-23	9-12	12-23	14-16	3-24	11-13	15-24	20-23A	7-8	10-12	12-23	14-16	20-23B
6	11-13	9-12	12-23	10-12	11-13	12-23	10-12	11-13	12-23	20-23B	9-12	10-11	11-13	12-23	20-23A
7	11-13	9-12	12-23	10-12	11-13	12-23	6-10	10-12	11-13	12-23	9-12	10-12	12-13	12-23	20-23A
8	11-13	7-8	11-13	10-12	11-13	12-23	10-12	11-13	12-23	20-23A	9-11	10-12	11-13	12-23	20-23B
9	11-13	7-8	11-13	10-12	11-13	12-23	7-8	9-12	12-23	20-23B	9-12	10-12	12-13	12-23	20-23A
10	11-13	9-12	12-23	7-8	10-12	12-23	7-8	10-12	12-23	20-23B	9-11	10-12	11-13	11-14	12-23
11	7-8	10-12	12-23	10-12	12-23	20-23A	7-8	9-12	10-12	12-23	7-8	9-12	10-12	12-23	20-23A
12	20-23A	10-12	12-23	7-8	10-12	12-23	7-8	10-12	12-23	20-23A	9-12	10-11	11-13	11-14	12-23

Table 3: Optimal defense plans

Finally, Table 4 shows the computational effort required by the proposed approach. It should be noted that optimality is obtained within moderate computational times, bearing in mind that a planning problem is solved and that no parallel evaluation of the search tree nodes has been implemented.

	Z					
M	0	1	2	3	4	5
1	0.45	0.87	1.36	1.85	2.52	2.73
2	0.39	1.82	7.35	18.51	44.35	94.18
3	0.65	4.32	12.95	41.04	111.13	322.81
4	0.36	2.19	10.31	37.23	108.85	333.21
5	0.29	1.69	7.66	37.45	136.77	575.86
6	0.20	1.80	13.80	80.90	436.16	1839.57
7	0.38	3.38	23.43	133.83	595.45	2347.00
8	0.34	3.23	21.80	116.55	564.90	2625.03
9	0.17	2.07	18.36	126.19	747.50	4092.05
10	0.35	4.02	32.12	236.81	1346.06	7048.65
11	0.34	4.27	41.93	279.68	1596.34	8405.74
12	0.31	4.45	38.15	287.99	1852.33	10564.00

Table 4: Computing times (s)

In order to assess the performance of the proposed approach we have implemented the method reported in [9] for the same values of Z and M. For $M = 1$ and $M = 2$, the approach proposed by Yao *et al.* attained optimality with computing times below 0.3 s and 300 s, respectively. However, for values of M exceeding 2 the algorithm was stopped after 20000 s without reaching the optimal solution. These results substantiate the computational superiority of the proposed two-stage algorithm.

6 CONCLUSIONS

This paper presents a new approach for the optimal allocation of defensive resources in a power system under multiple contingencies. This problem is formulated as a mixed-integer nonlinear trilevel program for which no efficient solution procedures are available in the technical literature. We have developed a novel two-stage methodology that attains global optimality in finite time. The first stage transforms the original trilevel program into an equivalent bilevel programming problem. The second stage subsequently solves the resulting bilevel program through the application of an implicit enumeration algorithm similar to the branch-and-bound algorithm used in mixed-integer linear programming.

The new procedure was successfully tested on the IEEE Reliability Test System. Numerical results reveal the effective performance of the proposed approach. Simulations also show that the proposed tool is a useful instrument for the system planner to identify defense schemes that mitigate the vulnerability against multiple outages.

Further work will be devoted to the parallel implementation of the implicit enumeration algorithm in order to gain significant computational savings.

7 ACKNOWLEDGMENT

The authors acknowledge the support from the Ministry of Science of Spain under CICYT project ENE2009-07836, and from the Junta de Comunidades de Castilla-La Mancha under project PAI08-0077-6243.

REFERENCES

[1] A. V. Gheorghe, M. Masera, M. Weijnen and L. de Vries, "Critical Infrastructures at Risk. Securing the European Electric Power System", Dordrecht, Springer, 2006, ISBN 1-4020-4306-6

[2] G. Brown, M. Carlyle, J. Salmerón and K. Wood, "Defending Critical Infrastructure", Interfaces, vol. 36, no. 6, pp 530-544, November-December 2006

[3] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", April 2004

[4] A. L. Motto, J. M. Arroyo and F. D. Galiana, "A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security under Disruptive Threat", IEEE Transactions on Power Systems, vol. 20, no. 3, pp 1357-1365, August 2005

[5] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua and K. R. Wierzbicki, "Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System", Reliability Engineering & System Safety, vol. 92, no. 9, pp 1155-1161, September 2007

[6] J. M. Arroyo, "Bilevel Programming Applied to Power System Vulnerability Analysis under Multiple Contingencies", IET Generation, Transmission & Distribution, vol. 4, no. 2, pp 178-190, February 2010

[7] L. N. Vicente and P. H. Calamai, "Bilevel and Multilevel Programming: A Bibliography Review", Journal of Global Optimization, vol. 5, no. 3, pp 291-306, October 1994

[8] J. M. Arroyo, N. Alguacil and M. Carrión, "A Risk-Based Approach for Transmission Network Expansion Planning under Deliberate Outages", IEEE Transactions on Power Systems, vol. 25, no. 3, pp 1759-1766, August 2010

[9] Y. Yao, T. Edmunds, D. Papageorgiou and R. Alvarez, "Trilevel Optimization in Power Network Defense", IEEE Transactions on Systems, Man, and Cybernetics–Part C: Applications and Reviews, vol. 37, no. 4, pp 712-718, July 2007

[10] M. P. Scaparra and R. L. Church, "A Bilevel Mixed-Integer Program for Critical Infrastructure Protection Planning", Computers & Operations Research, vol. 35, no. 6, pp 1905-1923, June 2008