Analysis of Electric Grid Interdiction With Line Switching

Andrés Delgadillo, *Graduate Student Member, IEEE*, José Manuel Arroyo, *Senior Member, IEEE*, and Natalia Alguacil, *Senior Member, IEEE*

***Abstract*—This paper addresses the vulnerability analysis of the electric grid under terrorist threat. This problem is formulated as a mixed-integer nonlinear bilevel program. In the upper-level optimization, the terrorist agent maximizes the damage caused in the power system, which is measured in terms of the level of system load shed. On the other hand, in the lower-level optimization, the system operator minimizes the damage by means of an optimal operation of the power system. The distinctive modeling feature introduced in this paper is that, among the different corrective actions available, the system operator has the capability to modify the network topology.**

Due to its nonconvexity and nonlinearity, the resulting bilevel programming problem cannot be equivalently transformed into a standard one-level optimization problem. Therefore, this paper proposes a new approach based on Benders decomposition within a restart framework. Some numerical results obtained by the proposed algorithm are provided and compared with those published, based on the IEEE Reliability Test System.

***Index Terms*—Benders decomposition, bilevel programming, deliberate outages, line switching, load shedding, vulnerability.**

NOMENCLATURE

A. Indices and Counters

h	Global iteration index.
i	Benders iteration counter.
j	Generator index.
k	Global iteration counter.
l	Transmission line index.
m	Benders iteration index.
n	Bus index.

B. Sets

J	Set of indices of generators.
J_n	Set of indices of generators connected to bus n.
L	Set of indices of transmission lines.
N	Set of indices of buses.

C. Constants

A_{nl}	Element of the network incidence matrix that is equal to 1 if bus n is the sending bus of line l, -1 if bus n is the receiving bus of line l, and 0 otherwise.
$FR(l)$	Sending bus of line l.
I	Maximum number of iterations of the Benders loop.
K	Maximum number of iterations of the multi-start Benders algorithm.
M	Number of lines to be attacked.
P_n^d	Demand at bus n.
$\overline{P}_l^f$	Power flow capacity of line l.
$\overline{P}_j^g$	Capacity of generator j.
$TO(l)$	Receiving bus of line l.
x_l	Reactance of line l.
$\overline{\delta}$	Upper bound for the nodal phase angles.
$\underline{\delta}$	Lower bound for the nodal phase angles.
ϵ	Level of solution accuracy of the Benders loop.

D. Variables

P_l^f	Power flow of line l.
P_j^g	Power output of generator j.
q_l^{FR}	Variable equal to the product $v_l w_l \delta_{FR(l)}$.
q_l^{TO}	Variable equal to the product $v_l w_l \delta_{TO(l)}$.
s_l^{FR}	Auxiliary variable used in the linear expressions equivalent to the product $v_l w_l \delta_{FR(l)}$.

Manuscript received March 10, 2009; revised June 24, 2009. First published November 13, 2009; current version published April 21, 2010. This work was supported in part by the Ministry of Education and Science of Spain, under CICYT Project DPI2006-01501; and in part by the Junta de Comunidades de Castilla-La Mancha, under Project PAI08-0077-6243. Paper no. TPWRS-00184-2009.

The authors are with the Departamento de Ingeniería Eléctrica, Electrónica, Automática y Comunicaciones, E.T.S.I. Industriales, Universidad de Castilla-La Mancha, Ciudad Real E-13071, Spain (e-mail: AndresRamiro.Delgadillo@alu.uclm.es; JoseManuel.Arroyo@uclm.es; Natalia.Alguacil@uclm.es).

Digital Object Identifier 10.1109/TPWRS.2009.2032232

s_l^{TO}	Auxiliary variable used in the linear expressions equivalent to the product $v_l w_l \delta_{TO(l)}$.
v_l	Binary variable that is equal to 0 if line l is destroyed and 1 otherwise.
w_l	Binary variable that is equal to 0 if non-attacked line l is disconnected and 1 otherwise.
y_l	Variable equal to the product $v_l w_l$.
z^{best}	Best value of the system load shed.
z^{lo}	Lower bound for the system load shed.
z^{up}	Upper bound for the system load shed.
α	Objective function of the master problem.
δ_n	Phase angle at bus n.
ΔP_n^d	Load shed at bus n.
$\mu_l^{(k)}$	Dual variable associated with the Benders subproblem at iteration k.

E. Vectors

P^f	Line power flows.
P^g	Generator power outputs.
v	Attack plan.
v^{best}	Best attack plan.
w	Line switching scheme.
w^{best}	Best line switching scheme.
δ	Nodal phase angles.
ΔP^d	Nodal loads shed.

I. Introduction

THE introduction of deregulation, increased levels of consumption, and lack of investment are driving the operation of power systems close to their static and dynamic limits. The traditional assessment of power system vulnerability consists in examining a set of credible contingencies typically associated with random natural-occurring failures. The huge computational burden limits the simulations to a small subset of contingencies. The analyzed contingencies are ranked according to their severity and probability of occurrence, yielding the well-known $\mathrm{N}-1$ and $\mathrm{N}-2$ security criteria [1]. In addition to simulation-based vulnerability assessment, several topological studies have been conducted to analyze the structural vulnerability of power systems [2], [3]. Unfortunately, power systems are exposed not only to unintentional random failures but also to deliberate outages [4]–[6]. The distinctive aspects of intentional outages are: 1) they are nonrandom, i.e., probabilities of occurrence are unavailable [7]; 2) they may not be limited to a maximum of two simultaneous out-of-service components; and 3) they are intentionally malicious, i.e., their goal is to cause damage. The $\mathrm{N}-1$ and $\mathrm{N}-2$ criteria and topological studies do not consider these features, and therefore, they may not be sufficient to assess vulnerability in this new context. Consequently, new tools considering multiple contingencies are required [8].

Recent works have addressed power system vulnerability assessment under the framework of deliberate outages [9]–[16]. This problem, also known as vulnerability analysis, terrorist threat problem, or worst-case interdiction problem, consists in identifying the set of contingencies that makes the system most vulnerable so that effective defensive or protective measures can be determined [4], [17], [18]. In the vulnerability analysis, the destructive agents attack the system with the goal of maximizing the damage, whereas the system operator reacts to minimize such damage. Therefore, this problem can be modeled as a bilevel program [19], [20], where the terrorist is the upper-level agent, while the system operator is the lower-level agent.

Salmeron *et al.* [9] were the first to address this problem with mathematical programming by proposing a max-min model. In [10] and [11], the max-min terrorist threat problem was solved by first transforming the existing nonlinear expressions into linear constraints. Subsequently, by replacing the lower-level problem by its dual, the max-min problem became a max-max problem, i.e., a one-level problem, which was solved by Benders decomposition and mixed-integer linear programming. Arroyo *et al.* [12] provided a generalization of the terrorist threat problem, which was defined as a mixed-integer nonlinear bilevel program. This model was transformed into an equivalent one-level mixed-integer linear program by replacing the lower optimization problem with its Karush–Kuhn–Tucker optimality conditions. Motto *et al.* [13] presented an alternative solution procedure for the mixed-integer bilevel programming model of the terrorist threat problem. Based on duality theory, the authors recast the problem into a standard one-level mixed-integer linear program that was computationally more efficient than that described in [12]. Holmgren *et al.* [14] introduced a game theory model to study strategies for defending electric power systems against different types of antagonistic threats. Bier *et al.* [15] proposed a heuristic method to identify plausible strategies for interdiction in power systems. The solution algorithm consisted in iteratively attacking the most heavily loaded lines. Finally, a decomposition method has been recently presented in [16] to solve large-scale instances of the max-min model described in [9].

The determination of the most critical set of network components is performed by a deterministic worst-case analysis, i.e., the uncertainty associated with interdiction plans is not considered [9]–[16]. Notwithstanding, vulnerability analysis may be a useful tool to characterize such uncertainty through the generation of a set of scenarios, where each scenario represents a plausible interdiction plan. As an example, the worst-case interdiction method of [13] was used for this purpose in the vulnerability-constrained transmission expansion planning approach presented in [17] and [18].

This paper proposes a new model and a new solution procedure for vulnerability analysis under deliberate outages. The salient feature of the proposed model with respect to those proposed in [9]–[16] is the consideration of line switching [21], [22] as an additional corrective action available to the system operator following an attack. In other words, in addition to generation redispatch and load shedding, the system operator has the capability to modify the network topology by opening and closing lines. As mentioned in [21] and [22], line switching is already being implemented in practice by network operators in order to maintain reliability.

In our model, line switching decisions are characterized through lower-level binary variables; therefore, the resulting bilevel program cannot be addressed by means of previously reported techniques relying on the equivalent transformation to a one-level optimization problem [12], [13]. Bilevel programs with a nonconvex lower-level problem constitute a challenging field that is still unsolved by the operations research community [23]. Several attempts in this direction are available in the technical literature [24], [25]. The disadvantage of these methods is that they are limited to solving small problems.

Furthermore, this paper provides a solution methodology that combines Benders decomposition [26], [27] and a restart framework [28]. Benders decomposition is a technique for one-level optimization problems that is based on the reformulation of the original one-level problem into a bilevel program. Therefore, Benders decomposition is an attractive technique when the original problem is itself a bilevel programming problem. In order to guarantee convergence to the optimum, Benders decomposition has some requirements on convexity, which are not met in the case of the bilevel terrorist threat problem with line switching. This drawback is overcome here by restarting Benders decomposition so that most of the solution space is searched. The proposed multi-start Benders decomposition framework allows avoiding local optima, eventually reaching the global optimum. Thus, this technique is particularly appropriate for the terrorist threat problem with line switching since the alternative is a fully heuristic approach. It should be noted that the proposed algorithm is not the first attempt to solve a bilevel programming problem by Benders decomposition [4], [16], [29]. In [4], Benders decomposition was proposed to address general attacker-defender models. In [16], Benders decomposition was generalized for the terrorist threat problem of [9] based on empirically validated assumptions. However, these assumptions do not hold in general and binary lower-level decision variables, such as those associated with line switching, were not considered. In [29], a convex bilevel programming problem outside a power system framework was successfully solved.

The major contributions of this paper are as follows:

1) The bilevel model of the terrorist threat problem is extended by adding line switching to the set of corrective actions available to the system operator.
2) A novel Benders decomposition technique incorporating multiple restarts is used to solve the resulting bilevel program with binary lower-level decision variables.
3) The proposed decomposition algorithm is effective in attaining globally optimal or near-optimal solutions with moderate computational effort.

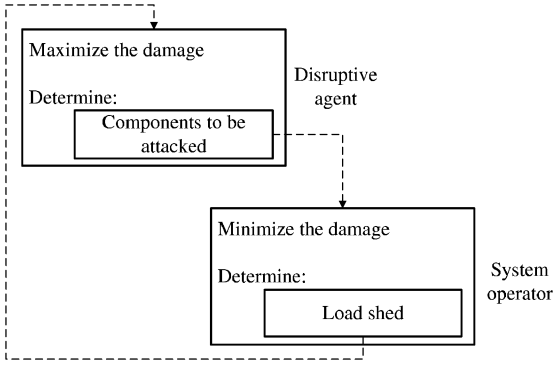

Fig. 1. Bilevel model for the terrorist threat problem.

4) The performance of the proposed approach is successfully validated with numerical simulations.

The remainder of this paper is organized as follows. Section II presents the bilevel formulation of the terrorist threat problem with line switching. Section III describes the proposed solution algorithm. Section IV provides and analyzes the numerical results. Section V draws relevant conclusions. Appendix A explains how to apply Benders decomposition to a general bilevel program. Finally, Appendix B shows the data of the test system.

II. Bilevel Approach

According to [12], the terrorist threat problem can be characterized as a bilevel program [19], [20], i.e., a decision-making problem involving two agents who try to optimize their respective objective functions over a jointly dependent set.

Fig. 1 shows a general bilevel model for the terrorist threat problem. The upper level is associated with the disruptive agent and determines the components of the power system to be attacked in order to maximize the damage caused to the electrical system. The damage is measured in terms of the level of system load shed. The maximization problem of the disruptive agent takes into account that destructive resources are limited, and that the system operator in the lower level optimally reacts to the attack. This reaction consists in determining the optimal power system operation that minimizes the effect caused by the terrorist. In previously reported works [9]–[16], the set of corrective actions was restricted to generation redispatch and load shedding. In contrast, in this paper, we extend the defensive reaction of the system operator by allowing line switching [21], [22].

It should be emphasized that the proposed approach can handle the destruction of any power system component. However, the power system components most commonly disrupted by destructive agents are transmission lines [30]. Based on this fact, and for the sake of clarity and simplicity, here we consider that the terrorist agent only attacks these assets.

The electric grid interdiction problem with line switching is formulated as the following bilevel programming problem:

$$\max_{v} \sum_{n\in N} \Delta P_n^d \tag{1}$$

subject to

$$\sum_{l\in L}(1-v_l) = M \tag{2}$$

$$v_l \in \{0,1\}, \quad \forall l \in L \tag{3}$$

$$\Delta P_n^d \in \arg\left\{ \min_{P^f,P^g,w,\delta,\Delta P^d} \sum_{n\in N} \Delta P_n^d \right. \quad (4)$$

subject to

$$P_l^f = v_l w_l \frac{1}{x_l}\left[\delta_{FR(l)} - \delta_{TO(l)}\right], \quad \forall l \in L \quad (5)$$

$$\sum_{j\in J_n} P_j^g - \sum_{l\in L} A_{nl} P_l^f + \Delta P_n^d = P_n^d, \quad \forall n \in N \quad (6)$$

$$0 \le P_j^g \le \overline{P}_j^g, \quad \forall j \in J \quad (7)$$

$$-\overline{P}_l^f \le P_l^f \le \overline{P}_l^f, \quad \forall l \in L \quad (8)$$

$$\underline{\delta} \le \delta_n \le \overline{\delta}, \quad \forall n \in N \quad (9)$$

$$0 \le \Delta P_n^d \le P_n^d, \quad \forall n \in N \quad (10)$$

$$w_l \in \{0,1\}, \quad \forall l \in L\}. \quad (11)$$

The disruptive agent is represented by the upper-level problem (1)–(3). The terrorist controls the vector of binary variables v, where v_l is equal to 0 if line l is destroyed, being 1 otherwise. The system operator is represented by the optimal power flow in the lower-level problem (4)–(11), which is parameterized in terms of the upper-level decision variables v_l. As is commonly assumed in the technical literature [9]–[13], [15], [16], a dc model of the transmission system is used. The system operator controls the vectors of continuous variables P^f, P^g, δ, ΔP^d, and the vector of binary variables w which models the capability to modify the network topology. Thus, w_l is equal to 0 if the system operator decides to disconnect non-attacked line l, being 1 otherwise.

The terrorist agent maximizes the system load shed (1) for a given number of simultaneously destroyed lines (2). Constraints (3) model the binary nature of variables v_l. The objective of the system operator (4) is to minimize the system load shed under the combination of destroyed lines v chosen by the terrorist. Constraints (5) express the line flows in terms of the nodal phase angles, the line switching variables w_l, and the upper-level variables v_l. Note that if line l is either attacked $(v_l = 0)$ or disconnected $(w_l = 0)$, the corresponding power flow is set to 0. Constraints (6) represent the power balance in each bus of the system. Upper and lower bounds on lower-level decision variables are imposed in constraints (7)–(10). Finally, constraints (11) model the integrality of variables w_l. It should be noted that weights could be assigned to nodal loads shed to reflect the relative importance of each load.

Constraints (5) constitute the main difference with respect to the bilevel models presented in [9]–[13], [15], and [16]. These constraints make the lower-level problem nonconvex due to the presence of lower-level binary variables w_l, and nonlinear due to the products of lower-level decision variables w_l and δ_n. Therefore, it is not possible to transform the bilevel problem (1)–(11) into an equivalent one-level optimization problem, as done in [12] and [13], and new tools are thus needed.

III. Solution Methodology

This section describes the solution methodology based on Benders decomposition. The relationship between Benders decomposition and bilevel programming is explained in detail in Appendix A. First, we present the mathematical formulation of the master problem and the subproblem resulting from the application of Benders decomposition to problem (1)–(11). Next, we provide the multi-start Benders decomposition approach. This methodology consists of two loops: 1) an inner loop where Benders decomposition is applied and 2) an outer loop used to restart Benders decomposition so that local optima are avoided. Benders decomposition is restarted by using the solution attained in the last iteration of the previous Benders loop. Alternative restart solutions can be straightforwardly used such as the random restart scheme applied in [28].

A. Formulation of the Master Problem and the Subproblem

Under the Benders decomposition framework described in Appendix A, problem (1)–(11) is transformed into a master problem and a subproblem that are iteratively solved. According to the notation in Appendix A, $f^u(x) = 0$, $g^u(y) = -\sum_{n\in N} \Delta P_n^d$, and $g^l(y) = \sum_{n\in N} \Delta P_n^d$. Thus, $\partial g^u(y)/\partial g^l(y) = -1$, and consequently $\lambda^{(\nu)} = -\mu^{(\nu)}$.

The master problem associated with problem (1)–(11) is

$$\min_{v,\alpha} \alpha \quad (12)$$

subject to

$$\sum_{l\in L}(1 - v_l) = M \quad (13)$$

$$\alpha \ge -\sum_{n\in N} \Delta P_n^{d(m)} - \sum_{l\in L} \mu_l^{(m)} \left(v_l - v_l^{(m)}\right), \quad m = k - i + 1, \ldots, k-1 \quad (14)$$

$$\sum_{l\in L} \left(1 - v_l^{(h)}\right)(1 - v_l) \le M - 1, \quad h = 1, \ldots, k-1 \quad (15)$$

$$v_l \in \{0,1\}, \quad \forall l \in L \quad (16)$$

where k and i are the global iteration counter and the Benders iteration counter, respectively.

The master problem (12)–(16) is an approximation of the upper-level problem (1)–(3). In each iteration, the search space is restricted by adding a Benders cut (14) corresponding to the current Benders loop, which is represented by index i. When the Benders decomposition is restarted, Benders cuts (14) of the previous Benders loop are discarded except for the last one. Constraints (15) guarantee that a new vector v is found at each iteration.

The subproblem at iteration k is formulated as

$$\min_{P^f,P^g,v,w,\delta,\Delta P^d} \sum_{n\in N} \Delta P_n^d \quad (17)$$

subject to

$$P_l^f = v_l w_l \frac{1}{x_l}\left[\delta_{FR(l)} - \delta_{TO(l)}\right], \quad \forall l \in L \quad (18)$$

$$\sum_{j\in J_n} P_j^g - \sum_{l\in L} A_{nl} P_l^f + \Delta P_n^d = P_n^d, \quad \forall n \in N \quad (19)$$

$$0 \le P_j^g \le \overline{P}_j^g, \quad \forall j \in J \quad (20)$$

$$-\overline{P}_l^f \le P_l^f \le \overline{P}_l^f, \quad \forall l \in L \quad (21)$$

$$\underline{\delta} \le \delta_n \le \overline{\delta}, \quad \forall n \in N \quad (22)$$

$$0 \le \Delta P_n^d \le P_n^d, \quad \forall n \in N \quad (23)$$

$$w_l \in \{0,1\}, \quad \forall l \in L \quad (24)$$

$$v_l = v_l^{(k)} : \mu_l^{(k)}, \quad \forall l \in L. \quad (25)$$

The subproblem (17)–(25) is the problem faced by the system operator for a given set of lines attacked by the destructive agent $v_l^{(k)}$, as imposed in (25). The solution of this problem provides the values of $P_l^{f\,(k)}$, $P_j^{g(k)}$, $w_l^{(k)}$, $\delta_n^{(k)}$, $\Delta P_n^{d(k)}$, and $\mu_l^{(k)}$, where $\mu_l^{(k)}$ is the dual variable associated with (25).

Note that constraints (18) are nonlinear due to the products of binary variables and continuous variables $v_l w_l \delta_{FR(l)}$ and $v_l w_l \delta_{TO(l)}$. According to [31], both nonlinearities can be replaced by equivalent linear expressions by introducing a new set of binary variables y_l, and four new sets of continuous variables q_l^{FR}, q_l^{TO}, s_l^{FR}, and s_l^{TO}, as follows:

$$P_l^f = \frac{1}{x_l}\left(q_l^{FR} - q_l^{TO}\right), \quad \forall l \in L \tag{26}$$

$$q_l^{FR} = \delta_{FR(l)} - s_l^{FR}, \quad \forall l \in L \tag{27}$$

$$q_l^{TO} = \delta_{TO(l)} - s_l^{TO}, \quad \forall l \in L \tag{28}$$

$$\underline{\delta} y_l \le q_l^{FR} \le \overline{\delta} y_l, \quad \forall l \in L \tag{29}$$

$$\underline{\delta} y_l \le q_l^{TO} \le \overline{\delta} y_l, \quad \forall l \in L \tag{30}$$

$$\underline{\delta}(1 - y_l) \le s_l^{FR} \le \overline{\delta}(1 - y_l), \quad \forall l \in L \tag{31}$$

$$\underline{\delta}(1 - y_l) \le s_l^{TO} \le \overline{\delta}(1 - y_l), \quad \forall l \in L \tag{32}$$

$$y_l \le v_l, \quad \forall l \in L \tag{33}$$

$$y_l \le w_l, \quad \forall l \in L \tag{34}$$

$$y_l + 1 \ge v_l + w_l, \quad \forall l \in L \tag{35}$$

where y_l represents the product $v_l w_l$; q_l^{FR} and q_l^{TO} represent the products $v_l w_l \delta_{FR(l)}$ and $v_l w_l \delta_{TO(l)}$, respectively; and s_l^{FR} and s_l^{TO} are auxiliary variables.

It should be noted that the master problem (12)–(16) and the subproblem (17), (19)–(35) are mixed-integer linear programs that can be efficiently solved by available off-the-shell branch-and-cut software.

B. Algorithm

The proposed methodology, hereinafter referred to as Benders decomposition line switching (BDLS), is shown in Fig. 2 and works as follows:

1) *Initialization*.
   - Set the global iteration counter k to 1.
   - Solve the terrorist threat problem assuming that the system operator does not have the capability to modify the network configuration. This step involves solving the same problem addressed in [13]. The optimal solution constitutes the best initial attack strategy, $v^{best} = v^{(1)}$, and provides an upper bound for the system load shed, $z^{up} = \sum_{n \in N} \Delta P_n^{d(1)}$.
   - Solve the subproblem (17), (19)–(35) for the attack strategy $v^{(1)}$. The optimal solution is the best initial line switching scheme, $w^{best} = w^{(1)}$, and provides $\mu^{(1)}$ and the best initial system load shed, $z^{best} = \sum_{n \in N} \Delta P_n^{d(1)}$.
2) *Initial optimality checking*. If z^{up} is equal to z^{best}, then the optimal solution is found and the algorithm stops; otherwise, go to step 3.
3) *Initialize the Benders loop*. Set the Benders iteration counter i to 1.
4) *Update the iteration counters*. Increase the iteration counters $k \leftarrow k + 1$ and $i \leftarrow i + 1$.

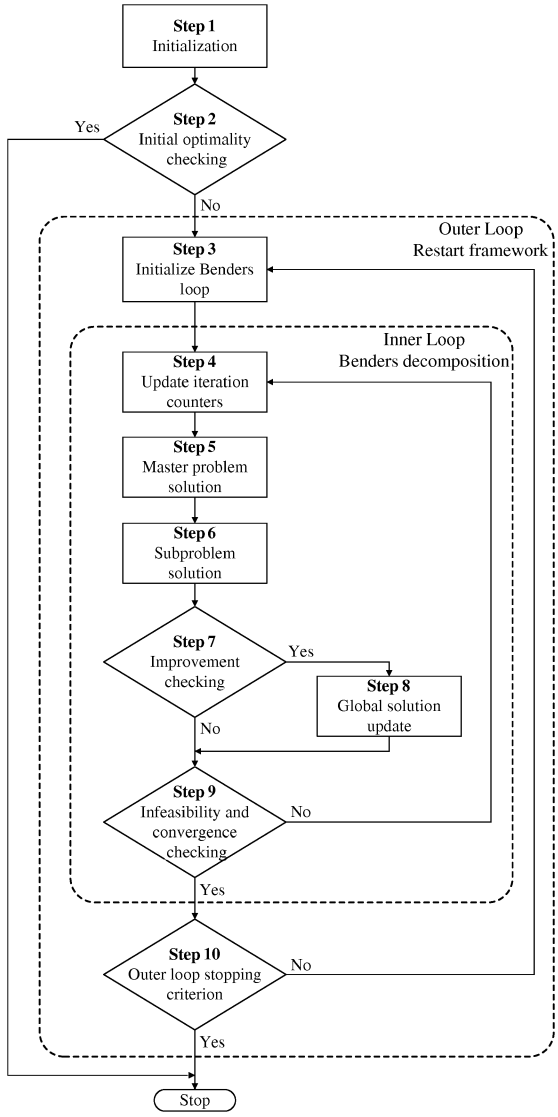

Fig. 2. Flowchart of the proposed methodology.

5) *Master problem solution*. Solve the master problem (12)–(16). This step provides $v^{(k)}$ and an upper bound for the system load shed, $z^{up} = -\alpha$.
6) *Subproblem solution*. Solve the subproblem (17), (19)–(35) for the given set of attacked lines $v^{(k)}$. This step provides $P_l^{f\,(k)}$, $P_j^{g(k)}$, $w_l^{(k)}$, $\delta_n^{(k)}$, $\Delta P_n^{d(k)}$, $\mu_l^{(k)}$, and a lower bound for the system load shed, $z^{lo} = \sum_{n \in N} \Delta P_n^{d(k)}$.
7) *Improvement checking*. If $z^{lo} > z^{best}$, then go to step 8; otherwise, go to step 9.
8) *Global solution update*. The best solutions found are updated: $v^{best} = v^{(k)}$, $w^{best} = w^{(k)}$, $z^{best} = z^{lo}$.
9) *Infeasibility and convergence checking*. If 1) a nonconvex region is reconstructed, i.e., $z^{up} < z^{lo}$; or 2) the Benders iteration counter reaches the maximum value, $i = I$; or 3) a solution with a level of accuracy ϵ has been found, i.e., $|z^{up} - z^{lo}|/|z^{lo}| \le \epsilon$, then go to step 10; otherwise, go to step 4.
10) *Outer loop stopping criterion*. If the global iteration counter reaches the maximum value, $k = K$, the al-

TABLE I
MAXIMUM SYSTEM LOAD SHED ATTAINED BY THE DESTRUCTIVE AGENT (MW)

M	BDLS	MO	BD
1	131	230	131
2	279	397	259
3	429	484	390
4	538	570	538
5	688	706	688
6	775	795	775
7	855	855	855
8	905	919	880
9	1002	1003	964
10	1017	1053	1014
11	1131	1131	1131
12	1194	1194	1194

gorithm stops; otherwise, the Benders decomposition is restarted by going to step 3.

IV. NUMERICAL RESULTS

This section presents a case study based on the IEEE One Area Reliability Test System-1996 (RTS-96) [32]. For illustration purposes, the data of RTS-96 are slightly modified as described in Appendix B. In addition, circuits sharing the same towers are treated as independent lines; e.g., line 20–23 has two circuits: 20–23A and 20–23B. For the sake of simplicity, line switching is restricted to the disconnection of lines. The algorithm was implemented under GAMS [33] on a Sun Fire X4600 M2 with four processors at 2.60 GHz and 32 GB of RAM. The optimization problems were solved using CPLEX 11.0.1 [34]. The stopping criteria used in the simulation are characterized by $I = 250$, $K = 2500$, and $\epsilon = 0.01$. In the absence of a measure of the distance to the global optimum, parameters I and K were selected by trial and error. These parameters achieved efficient solutions with moderate computational effort.

Table I presents the maximum system load shed obtained for a number of destroyed lines M up to 12. The quality of the solutions found by BDLS is assessed through the comparison with the optimal solutions achieved by the approach of Motto *et al.* [13], denoted by MO. The methodology MO does not consider line switching and thus provides an upper bound on the optimal system load shed.

As can be inferred from Table I, line switching is an effective corrective action since it reduces the maximum damage associated with deliberate outages, except for cases $M = 7$, 11, and 12. In those cases, step 2 of the proposed algorithm determines that the optimal solution to problem (1)–(11) is the same as that of MO (without line switching), and therefore, line switching is not required. For the remaining cases, line switching mitigates the impact of deliberate outages between 43.0% for $M = 1$ and 0.1% for $M = 9$. It is interesting to observe that for low values of M significant reductions of system load shed are achieved. This result supports the use of line switching as a corrective action also for random unintentional outages considered in traditional vulnerability assessment. Additionally, Table I provides the results obtained by a standard Benders procedure with no restarts (BD), i.e., the first iteration of the inner loop of BDLS. It should be noted that the proposed algorithm outperforms BD in cases $M = 2$, 3, 8, 9, and 10, thus showing the efficient performance of the restart framework.

TABLE II
BEST ATTACK PLAN AND ASSOCIATED LINE SWITCHING SCHEME

M	v	w
1	10-12	4-9, 6-10, 9-11, 12-13, 13-23, 15-16, 16-17, 16-19
2	9-12, 10-12	3-9, 6-10, 8-9, 15-16, 16-17
3	9-12, 10-12, 11-13	11-14
4	12-13, 12-23, 20-23A, 20-23B	3-9, 6-10, 15-16, 17-18
5	11-13, 12-13, 12-23, 20-23A, 20-23B	11-14
6	7-8, 11-13, 12-13, 12-23, 20-23A, 20-23B	9-11
7	7-8, 11-13, 12-13, 12-23, 15-24, 20-23A, 20-23B	-
8	7-8, 11-13, 12-13, 12-23, 14-16, 15-24, 20-23A, 20-23B	8-9, 10-12
9	7-8, 11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, 20-23B	10-11, 10-12
10	1-2, 2-4, 2-6, 7-8, 11-13, 12-13, 12-23, 16-19, 20-23A, 20-23B	15-16, 17-18
11	1-3, 1-5, 2-4, 2-6, 7-8, 11-13, 12-13, 12-23, 15-24, 20-23A, 20-23B	-
12	1-2, 2-4, 2-6, 7-8, 11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, 20-23B	-

Table II lists the set of lines attacked by the terrorist agent and the set of lines disconnected by the system operator, corresponding to the best solutions attained by BDLS (Table I). It is worth mentioning that the disconnection of a relatively low number of lines yields a significant reduction in the level of damage associated with deliberate outages. As an example, by just disconnecting line 9–11 in the case $M = 6$, a 2.5% reduction in load shedding can be achieved with respect to the solution found by MO.

Fig. 3 shows the results found by MO and BDLS for $M = 8$. Fig. 3(a) corresponds to MO and represents the optimal attack plan when the system operator is not allowed to modify the network topology. In this case, the optimal system load shed is 919 MW and the attacked lines are 1–5, 2–6, 7–8, 11–13, 12–13, 12–23, 20–23A, and 20–23B. If the system operator had the capability to modify the network topology, the system load shed associated with this attack plan would drop to 880 MW by opening lines 1–2, 15–16, and 17–18. However, this attack plan is not optimal, as shown in Tables I and II, and Fig. 3(b). Fig. 3(b) depicts the best solution found by BDLS. In this case, the system load shed is 905 MW, i.e., a 2.8% improvement from the perspective of the terrorist agent, and a 1.5% reduction in system load shed with respect to the optimal solution without line switching. The lines attacked by the destructive agent are 7–8, 11–13, 12–13, 12–23, 14–16, 15–24, 20–23A, and 20–23B, whereas the lines disconnected by the system operator are 8–9 and 10–12.

Finally, Table III shows the computational effort associated with the subproblems and the master problems, as well as the overall CPU time required by BDLS. As above mentioned, for $M = 7$, 11, 12, BDLS achieves the optimal solution at the initialization stage, and thus, no master problem is solved. For the remaining cases, it should be noted that high-quality solutions are obtained within moderate computational times, bearing in mind that a planning problem is solved.

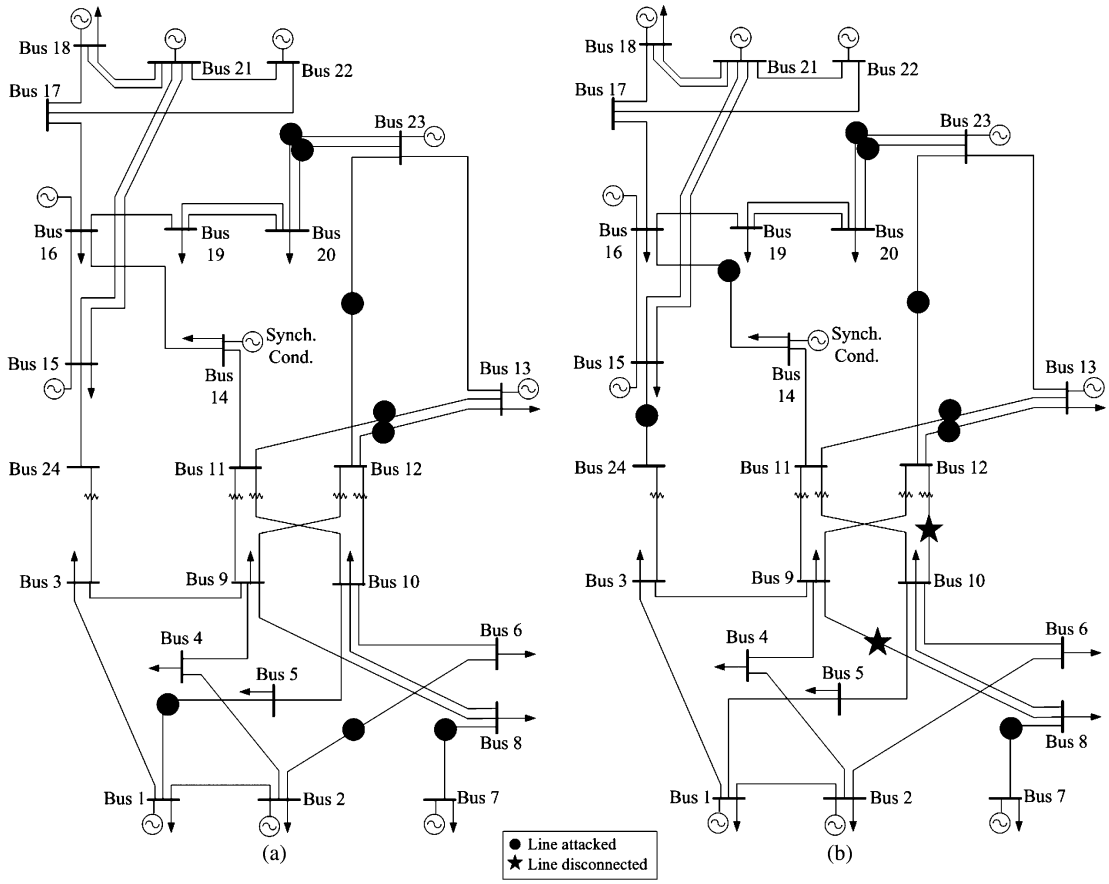

Fig. 3. Solutions for $M = 8$. (a) Best solution with MO. (b) Best solution with BDLS.

TABLE III
CPU TIME (s)

M	Subproblems	Master problems	Total
1	18.47	0.01	18.48
2	275.35	17.96	293.31
3	937.36	1324.23	2261.59
4	838.03	1342.64	2180.67
5	666.13	944.22	1610.35
6	596.75	923.72	1520.47
7	0.89	-	0.89
8	355.38	957.04	1312.42
9	322.79	832.85	1155.64
10	243.08	785.93	1029.01
11	0.85	-	0.85
12	0.88	-	0.88

V. CONCLUSIONS

This paper presents a new bilevel programming model and a novel solution procedure for the terrorist threat problem in an electrical network. The distinctive modeling feature is the consideration of line switching as a corrective action by the system operator. In order to solve the resulting mixed-integer nonlinear bilevel program, a multi-start Benders decomposition technique is applied. The proposed methodology comprises the iterative resolution of a master problem and a subproblem. Both problems are formulated as mixed-integer linear programming problems suitable for efficient off-the-shell branch-and-cut software. The master problem is an approximation of the optimization problem of the terrorist agent, while the subproblem represents the optimization problem associated with the system operator.

Numerical results show that line switching is a helpful instrument for the system operator to mitigate the impact of deliberate outages. In addition, simulations show the effective performance of the proposed approach. Research is currently underway to develop alternative heuristic-based solution procedures. Further work will also analyze the connection or disconnection of fast-acting generating units to reduce the impact of deliberate outages on power system vulnerability.

APPENDIX A
BENDERS DECOMPOSITION AND BILEVEL PROGRAMMING

Consider the general one-level optimization problem:

$$\min_{x,y} f(x) + g(y) \tag{36}$$

subject to

$$h(x) \leq 0 \tag{37}$$

$$d(x, y) \leq 0. \tag{38}$$

The solution of problem (36)–(38) can be obtained by parameterizing this problem in terms of variables x, yielding the following bilevel programming problem:

$$\min_{x} f(x) + \alpha(x) \tag{39}$$

subject to

$$h(x) \leq 0 \tag{40}$$

$$\alpha(x) = \min_{y} g(y) \tag{41}$$

$$\text{subject to}$$

$$d(x,y) \le 0. \tag{42}$$

Note that the lower-level objective function is equal to $\alpha(x)$, which is also minimized in the upper-level objective function.

The Benders decomposition solves this problem through the iterative solution of a master problem and a subproblem [26], [27].

The master problem at iteration ν is

$$\min_{x,\alpha} f(x) + \alpha \tag{43}$$

$$\text{subject to}$$

$$h(x) \le 0 \tag{44}$$

$$\alpha \ge g\left(y^{(m)}\right) + \lambda^{(m)^T}\left(x - x^{(m)}\right) \quad m = 1, \ldots, \nu - 1 \tag{45}$$

where $\lambda^{(m)} = \partial g(y^{(m)})/\partial x^{(m)}$.

The subproblem at iteration ν is

$$\min_{x,y} g(y) \tag{46}$$

$$\text{subject to}$$

$$d(x,y) \le 0 \tag{47}$$

$$x = x^{(\nu)} : \lambda^{(\nu)}. \tag{48}$$

Note that the solution of the subproblem provides $\lambda^{(\nu)} = \partial g(y^{(\nu)})/\partial x^{(\nu)}$, which is used in the master problem (45).

Since problem (39)–(42) is a bilevel program, it is straightforward to apply Benders decomposition to the following general bilevel optimization problem:

$$\min_{x} f(x) + g^u(y) \tag{49}$$

$$\text{subject to}$$

$$h(x) \le 0 \tag{50}$$

$$y \in \arg\left\{\min_{y'} g^l(y') \right. \tag{51}$$

$$\text{subject to}$$

$$\left. d(x,y') \le 0\right\} \tag{52}$$

where superscripts u and l denote upper level and lower level, respectively.

The only difference between problems (39)–(42) and (49)–(52) lies in the fact that the lower-level objective function in problem (49)–(52), $g^l(y')$, may be different from the term associated with variables y in the upper-level objective function, $g^u(y)$.

At each iteration ν, Benders decomposition transforms problem (49)–(52) into a master problem:

$$\min_{x,\alpha} f(x) + \alpha \tag{53}$$

$$\text{subject to}$$

$$h(x) \le 0 \tag{54}$$

$$\alpha \ge g^u\left(y^{(m)}\right) + \lambda^{(m)^T}\left(x - x^{(m)}\right), \quad m = 1, \ldots, \nu - 1 \tag{55}$$

where $\lambda^{(m)} = \partial g^u(y^{(m)})/\partial x^{(m)}$, and a subproblem:

$$\min_{x,y} g^l(y) \tag{56}$$

$$\text{subject to}$$

$$d(x,y) \le 0 \tag{57}$$

$$x = x^{(\nu)} : \mu^{(\nu)} \tag{58}$$

where $\mu^{(\nu)} = \partial g^l(y^{(\nu)})/\partial x^{(\nu)}$.

In general, $\mu^{(\nu)} \neq \lambda^{(\nu)}$. Hence, to obtain the value of $\lambda^{(\nu)}$, it is necessary to apply the chain rule as follows:

$$\begin{aligned}\lambda^{(\nu)} &= \frac{\partial g^u\left(y^{(\nu)}\right)}{\partial x^{(\nu)}} \\ &= \frac{\partial g^l\left(y^{(\nu)}\right)}{\partial x^{(\nu)}} \frac{\partial g^u\left(y^{(\nu)}\right)}{\partial g^l\left(y^{(\nu)}\right)} \\ &= \mu^{(\nu)} \frac{\partial g^u\left(y^{(\nu)}\right)}{\partial g^l\left(y^{(\nu)}\right)}.\end{aligned} \tag{59}$$

TABLE IV
POWER FLOW CAPACITY (MW)

Line	$\overline{P}_l^f$	Line	$\overline{P}_l^f$
1-2	87.5	12-13	250.0
1-3	87.5	12-23	250.0
1-5	87.5	13-23	50.0
2-4	87.5	14-16	50.0
2-6	87.5	15-16	50.0
3-9	87.5	15-21A	250.0
3-24	80.0	15-21B	250.0
4-9	100.0	15-24	80.0
5-10	100.0	16-17	250.0
6-10	87.5	16-19	50.0
7-8	87.5	17-18	250.0
8-9	50.0	17-22	250.0
8-10	87.5	18-21A	250.0
9-11	50.0	18-21B	250.0
9-12	200.0	19-20A	250.0
10-11	50.0	19-20B	250.0
10-12	200.0	20-23A	250.0
11-13	250.0	20-23B	250.0
11-14	50.0	21-22	250.0

TABLE V
NODAL POWER DEMAND (MW)

n	P_n^d	n	P_n^d
1	108	10	170
3	100	13	265
4	74	14	100
5	50	15	317
6	136	16	100
7	125	18	333
8	137	19	181
9	155	20	128

APPENDIX B
MODIFICATIONS TO RTS-96

The data of the test system that have been modified with respect to RTS-96 [32] are listed in Tables IV and V.

ACKNOWLEDGMENT

The authors would like to thank Dr. R. Mínguez for his valuable comments and suggestions.

REFERENCES

[1] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*, 2nd ed. New York: Wiley, 1996.

[2] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Phys. Rev. E*, vol. 69, no. 2, pp. 025103-1–025103-4, Feb. 2004.

[3] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabási-Albert network model," *Physica A*, vol. 355, no. 2–4, pp. 667–677, Sep. 2005.

[4] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, Nov. 2006.

[5] A. V. Gheorghe, M. Masera, M. Weijnen, and L. de Vries, *Critical Infrastructures at Risk. Securing the European Electric Power System*. Dordrecht, The Netherlands: Springer, 2006.

[6] Memorial Institute for the Prevention of Terrorism, MIPT, 2009. [Online]. Available: http://www.mipt.org.

[7] M. O. Buygi, G. Balzer, H. M. Shanechi, and M. Shahidehpour, "Market-based transmission expansion planning," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 2060–2067, Nov. 2004.

[8] V. Donde, V. López, B. Lesieutre, A. Pinar, C. Yang, and J. Meza, "Severe multiple contingency screening in electric power systems," *IEEE Trans. Power Syst.*, vol. 23, no. 2, pp. 406–417, May 2008.

[9] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.

[10] R. E. Alvarez, "Interdicting electrical power grids," M.Sc. thesis, Naval Postgraduate School, Monterey, CA, 2004.

[11] J. Salmeron, K. Wood, and R. Baldick, Optimizing Electric Grid Design Under Asymmetric Threat (II), Naval Postgraduate School, Monterey, CA, Tech. Rep. NPS-OR-04-001, 2004.

[12] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.

[13] 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 Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[14] Å. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 76–84, Feb. 2007.

[15] 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," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 9, pp. 1155–1161, Sep. 2007.

[16] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, Feb. 2009.

[17] M. Carrión, J. M. Arroyo, and N. Alguacil, "Vulnerability-constrained transmission expansion planning: A stochastic programming approach," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1436–1445, Nov. 2007.

[18] N. Alguacil, M. Carrión, and J. M. Arroyo, "Transmission network expansion planning under deliberate outages," presented at the 16th Power Systems Computation Conf., PSCC'08, Glasgow, U.K., Jul. 2008, Paper no. 23.

[19] J. F. Bard, *Practical Bilevel Optimization. Algorithms and Applications*. Dordrecht, The Netherlands: Kluwer, 1998.

[20] S. Dempe, *Foundations of Bilevel Programming*. Dordrecht, The Netherlands: Kluwer, 2002.

[21] E. B. Fisher, R. P. O'Neill, and M. C. Ferris, "Optimal transmission switching," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1346–1355, Aug. 2008.

[22] K. W. Hedman, R. P. O'Neill, E. B. Fisher, and S. S. Oren, "Optimal transmission switching—Sensitivity analysis and extensions," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1469–1479, Aug. 2008.

[23] S. Dempe, "Annotated bibliography on bilevel programming and mathematical programs with equilibrium constraints," *Optimization*, vol. 52, no. 3, pp. 333–359, Jun. 2003.

[24] Z. Gümüs and C. Floudas, "Global optimization of mixed-integer bilevel programming problems," *Comput. Manage. Sci.*, vol. 2, no. 3, pp. 181–212, Aug. 2005.

[25] A. Mitsos, P. Lemonidis, and P. I. Barton, "Global solution of bilevel programs with a nonconvex inner program," *J. Glob. Optim.*, vol. 42, no. 4, pp. 475–513, Dec. 2008.

[26] J. F. Benders, "Partitioning procedures for solving mixed-variables programming problems," *Numer. Math.*, vol. 4, no. 1, pp. 238–252, Dec. 1962.

[27] A. M. Geoffrion, "Generalized Benders decomposition," *J. Optim. Theory Appl.*, vol. 10, no. 4, pp. 237–260, Oct. 1972.

[28] R. Mínguez, F. Milano, R. Zárate-Miñano, and A. J. Conejo, "Optimal network placement of SVC devices," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1851–1860, Nov. 2007.

[29] R. Mínguez and E. Castillo, "Reliability-based optimization in engineering using decomposition techniques and FORMS," *Struct. Saf.*, vol. 31, no. 3, pp. 214–223, May 2009.

[30] J. S. Simonoff, C. E. Restrepo, and R. Zimmerman, "Risk-management and risk-analysis-based decision tools for attacks on electric power," *Risk Anal.*, vol. 27, no. 3, pp. 547–570, Jun. 2007.

[31] C. A. Floudas, *Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications*. New York: Oxford Univ. Press, 1995.

[32] Reliability Test System Task Force, "The IEEE Reliability Test System—1996," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

[33] The GAMS Development Corporation Website, 2009. [Online]. Available: http://www.gams.com.

[34] The ILOG CPLEX Website, 2009. [Online]. Available: http://www.ilog.com/products/cplex.

Andrés Delgadillo (S'05–GS'08) received the Ingeniería Eléctrica degree and the M.Sc. degree in economy from the Universidad Nacional de Colombia, Bogotá, Colombia, in 2004 and 2008, respectively. He is currently pursuing the Ph.D. degree in technical and economic management of electric energy generation, transmission, and distribution systems at the Universidad de Castilla-La Mancha, Ciudad Real, Spain.

He has participated in the Research Program of Acquisition and Analysis of Electromagnetic Signals at Universidad Nacional de Colombia Group (PAAS-UN) since 2004. His research interests are electricity markets, soft computing techniques, and power quality analysis, as well as optimization techniques.

José Manuel Arroyo (S'96–M'01–SM'06) received the Ingeniero Industrial degree from the Universidad de Málaga, Málaga, Spain, in 1995 and the Ph.D. degree in power systems operations planning from the Universidad de Castilla-La Mancha, Ciudad Real, Spain, in 2000.

From June 2003 through July 2004, he held a Richard H. Tomlinson Postdoctoral Fellowship at the Department of Electrical and Computer Engineering of McGill University, Montreal, QC, Canada. He is currently an Associate Professor of electrical engineering at the Universidad de Castilla-La Mancha. His research interests include operations, planning, and economics of power systems, as well as optimization and parallel computation.

Natalia Alguacil (S'97–M'01–SM'07) received the Ingeniero en Informática degree from the Universidad de Málaga, Málaga, Spain, in 1995 and the Ph.D. degree in power systems operations and planning from the Universidad de Castilla-La Mancha, Ciudad Real, Spain, in 2001.

She is currently an Associate Professor of electrical engineering at the Universidad de Castilla-La Mancha. Her research interests include operations, planning, and economics of power systems, as well as optimization.