Computers & Operations Research 41 (2014) 282–290

Contents lists available at ScienceDirect

Computers & Operations Research

journal homepage: www.elsevier.com/locate/caor

A trilevel programming approach for electric grid defense planning☆

Natalia Alguacil [a], Andrés Delgadillo [b], José M. Arroyo [a,*]

[a] Departamento de Ingeniería Eléctrica, Electrónica, Automática y Comunicaciones, E.T.S.I. Industriales, Universidad de Castilla-La Mancha, Ciudad Real E-13071, Spain
[b] Instituto de Investigación Tecnológica, IIT, Escuela Técnica Superior de Ingeniería, ICAI, Universidad Pontificia Comillas, Madrid E-28015, Spain

ARTICLE INFO

Available online 29 June 2013

Keywords:
Electric grid defense planning
Multiple contingencies
Trilevel programming
Vulnerability mitigation

ABSTRACT

This paper addresses the allocation of defensive or hardening resources in an electric power grid to mitigate the vulnerability against multiple contingencies. This planning problem is characterized by a defender-attacker-defender model which is formulated as a trilevel programming problem. In the upper level, the system planner identifies the components to be defended or hardened in order to reduce the damage associated with plausible outages. In the middle level, the disruptive agent determines the set of out-of-service components so that the damage in the system is maximized. Finally, in the lower 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. Numerical results show the effectiveness of the proposed methodology.

1. Introduction

Power systems have become fundamental for the development of national economies worldwide [1–3]. 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 [4–7]. Moreover, these catastrophic events have revealed that traditional security assessment tools such as the N-1 and N-2 criteria [8] are insufficient to cope with multiple contingencies. Therefore, it is of utmost importance to devise new tools to guarantee the correct operation of power systems even under the most adverse, conceivable 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 through the development of attacker-defender models for both intentional [9–16] and unintentional outages [17–19]. 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 [20,21] that have been solved by decomposition-based approaches inspired by Benders decomposition [9,14–16], equivalent transformations to mixed-integer programs [10–12,17,18], and approximate methods [13,19].

In contrast to vulnerability analysis, little attention has been paid to the vulnerability mitigation of power systems. According to [2,3], several strategies for vulnerability reduction can be implemented such as (i) adding new assets for purposes of redundancy, and (ii) hardening the infrastructure or improving its active defenses so that the hardened or defended assets become invulnerable. Hardening and defense actions may include appropriate surveillance measures, patrolling localized assets, and undergrounding specific transmission components. For exposition purposes, terms related to defense and hardening are used interchangeably hereinafter.

The determination of optimal strategies for vulnerability mitigation is essentially a planning problem where investment decisions are made to either build new assets or reinforce existing ones. Moreover, these planning decisions take into account the occurrence of outages similarly to contingency-constrained planning models [22].

With respect to adding redundancy in a power system, transmission network expansion planning was proposed in [23–25] as an effective tool to mitigate the impact of deliberate outages on the performance of the transmission network. Regarding power system defense planning, which is the subject of this paper, relevant references are [3,13,26–29].

Brown et al. [3] proposed a general defender-attacker-defender model to allocate budget-limited defensive resources in any critical infrastructure including power systems. This model was

☆This work was supported in part by the Ministry of Science of Spain, under CICYT Project ENE2012-30679; and by the European Commission, under Grant Agreement Number 309048.

[*] Corresponding author. Tel.: +34 926 295496; fax: +34 926 295361.
E-mail addresses: Natalia.Alguacil@uclm.es (N. Alguacil), Andres.Delgadillo@iit.upcomillas.es (A. Delgadillo), JoseManuel.Arroyo@uclm.es (J.M. Arroyo).

0305-0548/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cor.2013.06.009

shown to be appropriate to consider all possible combinations of outages in an efficient manner. In addition, Benders decomposition was suggested as a potential solution technique.

Bier et al. [13] presented a heuristic iterative approach to determine the optimal defense of power system components. The methodology comprised three nested algorithms 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.

Holmgren et al. [26] introduced a game theoretical model to study strategies for defending and protecting electric power systems subject to different types of antagonistic threats. However, decisions by the defender and the attacker were both modeled in a simplified way through the use of continuous variables rather than binary variables.

Yao et al. [27] first formulated the defense planning problem of a power system as a trilevel program [30] based on the general defender-attacker-defender model proposed in [3]. 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.

Rose [28] addressed the trilevel programming formulation presented in [27] through a master-subproblem methodology inspired by the Benders decomposition approach described in [3]. The solution technique interestingly included a set of cuts in the master problem based on the underlying rationale of [31] by which defense schemes should include at least one of the components disrupted in previous iterations. Despite this relevant feature, this approach was characterized by several unresolved convergence issues.

The practical relevance and timeliness of power system defense planning for vulnerability mitigation are both backed by the recent contribution reported in [29], where the game theoretical work of [26] was extended by allowing a dynamic interaction among defenders and attackers.

This paper presents a new optimization-based approach for the optimal allocation of defensive resources in an electric power grid so that its vulnerability against multiple contingencies is mitigated. Similar to [3,13,27,28], this planning problem is characterized by a defender-attacker-defender model wherein optimal operation of the system under contingency is modeled. The resulting problem is formulated as a mixed-integer nonlinear trilevel program [30]. The distinctive feature of the proposed approach with respect to [3,13,27,28] 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 a duality-based transformation previously reported in [32], that was applied in [10] for an attacker-defender model similar to the two lowermost optimization levels of the original trilevel program. Two recent examples of successful application of this transformation in the context of power systems can be found in [33,34]. 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 [31] to solve a similar bilevel program for the protection of a logistic network.

Thus, the main motivation of this paper is to solve the trilevel model presented in [27] by using the implicit enumeration algorithm described in [31], for which the duality-based transformation of [10,32] is applied. It is worth mentioning that collecting the valuable features of [10,27,31,32] and combining them give rise to a novel, systematic, and effective solution approach.

The proposed two-stage method presents the following main advantages over the approaches described in [3,13,27,28]: (i) the conversion to a bilevel programming problem is exact and its computational burden is moderate, (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 [35], and (iii) optimality is guaranteed in a finite number of steps.

The major contributions of this paper are as follows:

1. A tool is developed for the system planner to optimally allocate defensive resources in order to mitigate the vulnerability of the electric power grid against multiple contingencies.
2. A two-stage approach is proposed to solve the resulting trilevel programming problem. The methodology is based on the novel application of a previously reported implicit enumeration algorithm which guarantees the attainment of globally optimal solutions.
3. Numerical experience is reported from solving case studies based on the IEEE Reliability Test System and the IEEE 300-bus system.

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 electric grid 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

Attacker-defender models have been recently used to analyze the vulnerability of power systems under multiple contingencies [9–19]. These models, also known as interdiction models, characterize a decision-making problem involving two different agents, namely an attacker and a defender (Fig. 1). The attacker or disruptive agent 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.

Although attacker-defender models are useful in finding critical components, they do not explicitly determine which components have to be defended. As explained in [3], defending those components that are identified as critical by an attacker-defender model does not necessarily provide the best protection against a system disruption. Therefore, new models are needed to determine the optimal defense plan for a power system exposed to multiple contingencies.

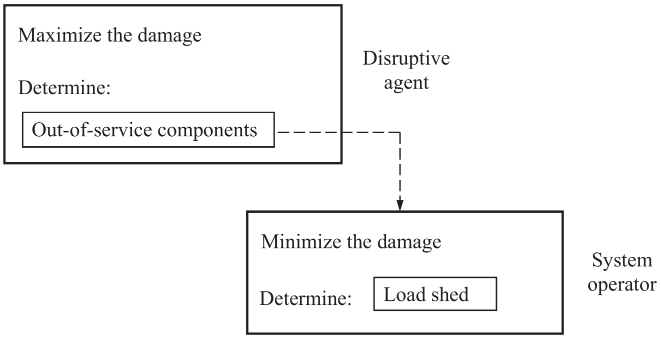

Fig. 1. Attacker-defender model.

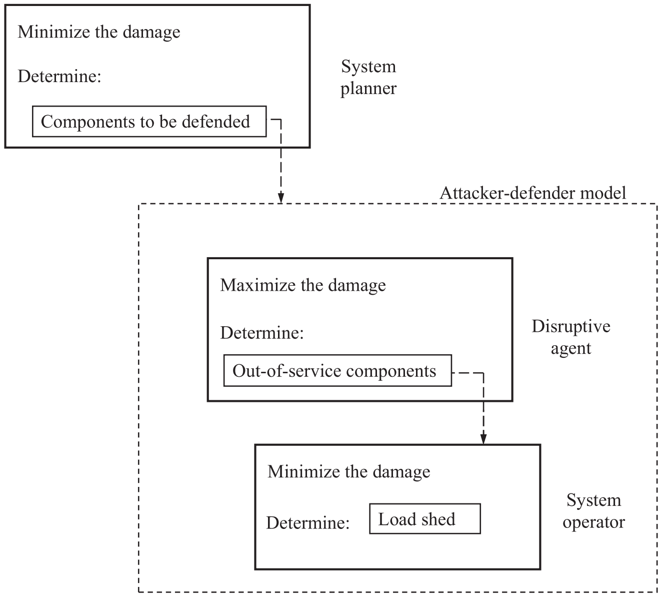

Fig. 2. Defender-attacker-defender model.

As shown in [3,13,27,28], a defender-attacker-defender model is suitable for the defense planning of critical infrastructures such as power systems. This model, also referred to as fortification model, involves three agents acting in sequence (Fig. 2): (i) a system planner who identifies the system components to be defended 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.

As can be seen in Fig. 2, the bilevel attacker-defender model of Fig. 1 is embedded in the defender-attacker-defender model as the two lowermost optimization levels. Thus, all feasible combinations of out-of-service components are implicitly considered.

3. Problem formulation

This section presents the mathematical formulation of the defender-attacker-defender model used for the electric grid defense planning problem. This formulation is based on the following modeling assumptions commonly adopted in state-of-the-art models for both vulnerability analysis and vulnerability mitigation [2,3,9,11–16,18,23–29]:

1. A steady-state security model is used where vulnerability and criticality are measured in terms of the system load shed, i.e., the total amount of involuntary decreases in consumption of real power.
2. A deterministic worst-case analysis is implemented. This is fundamental to deal with outages with low probability of occurrence but catastrophic impact on the system.
3. A static planning model comprising a single period is considered. During this target period generation sites are known and a single load scenario is modeled, typically corresponding to the highest load demand forecast for the considered planning horizon.
4. A dc load flow model is used to characterize the behavior of the transmission network. This linearized and static model is a standard and useful simplification in power system planning.

Admittedly, the use of such a simplified model leads to results that may be optimistic. A complete study of the defense planning problem would, however, render the problem essentially intractable through optimization and would have to be solved by repeated simulations. These modeling limitations notwithstanding, the solution of the proposed defense planning problem provides the system planner with a first estimate of the defense strategies required to mitigate the vulnerability of the system.

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. However, it should be noted that the proposed approach can be straightforwardly extended to account for the defense and disruption of other power system components. Using the notation presented in Tables 1–5, the optimal allocation of defensive resources is thus formulated as the following trilevel program:

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

subject to:

$$w_l \in \{0,1\}; \quad \forall l\in L \tag{2}$$

$$w \in W, \tag{3}$$

where

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

subject to:

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

$$\sum_{l\in L}(1-v_l) = K \tag{6}$$

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

and where

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

subject to:

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

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

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

$$-\overline{P}_l^f \leq P_l^f \leq \overline{P}_l^f : (\underline{\phi}_l, \overline{\phi}_l); \quad \forall l\in L \tag{12}$$

$$-\overline{\delta} \leq \delta_n \leq \overline{\delta} : (\underline{\chi}_n, \overline{\chi}_n); \quad \forall n\in N \tag{13}$$

Table 1
Indices.

j	Generator index
l	Transmission asset index
m	Search tree node index
n	Bus index

$$0\le\Delta P^d_n\le P^d_n : (\overline{\alpha}_n); \quad \forall n\in N. \tag{14}$$

Problem (1)–(14) comprises three optimization levels: (i) the upper level (1)–(3), which is associated with the system planner; (ii) the middle level (4)–(7), characterizing the behavior of the disruptive agent; and (iii) 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 the transmission components. Thus, w_l is equal to 1 if transmission asset l is defended, being 0 otherwise. The disruptive agent controls the vector of binary variables ν, where ν_l is equal to 0 if transmission asset l is out of service, being 1 otherwise. 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 ν_l. It is also worth mentioning that lower-level decision variables ΔP^d_n 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^d_n 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). Based on previously reported models on electric grid defense planning [3,13,27,28], upper-level decision variables w_l are binary (2) and are constrained by resource limitations, which are modeled in a compact way by (3). A possible form for expression (3) is [31]:

$$\sum_{l\in L} w_l = Z, \tag{15}$$

where constraint (15) is a cardinality expression setting the number of simultaneously defended transmission assets.

Table 2
Sets.

C	Set of candidate components for defense
J	Set of indices of generators
J_n	Set of indices of generators connected to bus n
L	Set of indices of transmission assets
M	Set of nodes of the search tree
N	Set of indices of buses
W	Feasibility set for vector w

Table 3
Constants.

$D(l)$	Destination or receiving bus of transmission asset l
K	Number of simultaneous out-of-service transmission assets
$O(l)$	Origin or sending bus of transmission asset l
p^d_n	Demand at bus n
$\overline{P}^f_l$	Power flow capacity of transmission asset l
$\overline{P}^g_j$	Capacity of generator j
x_l	Reactance of transmission asset l
Z	Number of transmission assets to be defended
$\overline{\delta}$	Upper bound for the nodal phase angles

Table 4
Variables and vectors.

P^f_l	Power flow of transmission asset l, lth component of vector P^f
p^g_j	Power output of generator j, jth component of vector P^g
ν_l	Binary variable that is equal to 0 if transmission asset l is out of service and 1 otherwise, lth component of vector ν
w_l	Binary variable that is equal to 1 if transmission asset l is defended and 0 otherwise, lth component of vector w
z^{best}	Optimal system load shed
δ_n	Phase angle at bus n, nth component of vector δ
ΔP^d_n	Load shed at bus n, nth component of vector ΔP^d

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 ν_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 ν_l is set to 1. In other words, if a line or a transformer is defended it becomes invulnerable. Constraint (6) sets the number of transmission assets that can be simultaneously out of service. Constraints (7) impose the integrality of variables ν_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 ν chosen by the disruptive agent. Using a dc network model [8], constraints (9) express the network power flows in terms of the nodal phase angles and the middle-level decision variables ν_l. Note that if transmission asset l is disrupted, i.e., $\nu_l=0$, 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 [3]. Moreover, the decomposition-based approaches proposed in the technical literature [3,27,28] might present difficulties in attaining optimality within moderate computing times. These difficulties are associated with (i) the need for solving the attacker-defender model corresponding to the two lowermost optimization levels, (ii) the reliance on a master problem of increasing dimension, and (iii) the lack of a systematic search process. 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.

Table 5
Dual variables and vectors.

$\overline{\alpha}_n$	Dual variable associated with the upper bound for the load shed at bus n, nth component of vector $\overline{\alpha}$
$\overline{\gamma}_j$	Dual variable associated with the upper bound for the power output of generator j, jth component of vector $\overline{\gamma}$
λ_n	Dual variable associated with the power balance equation at bus n, nth component of vector λ
μ_l	Dual variable associated with the equation relating power flow and phase angles for transmission asset l, lth component of vector μ
$\underline{\phi}_l$	Dual variable associated with the lower bound for the power flow of transmission asset l, lth component of vector $\underline{\phi}$
$\overline{\phi}_l$	Dual variable associated with the upper bound for the power flow of transmission asset l, lth component of vector $\overline{\phi}$
$\underline{\chi}_n$	Dual variable associated with the lower bound for the phase angle at bus n, nth component of vector $\underline{\chi}$
$\overline{\chi}_n$	Dual variable associated with the upper bound for the phase angle at bus n, nth component of vector $\overline{\chi}$

4.1. Stage 1: Transformation to an equivalent bilevel program

Using the methodology described in [10,32], the max-min problem comprising the middle- and lower-level optimizations (4)–(14) can be equivalently recast as a single-level problem. This transformation consists in replacing the lower-level problem by its dual thereby converting the max-min problem into a max-max problem, i.e., a single-level maximization. Therefore, the original trilevel problem (1)–(14) is transformed into the following equivalent bilevel programming problem:

$$\min_{w} \sum_{n \in N} \Delta P_n^{d^*} \tag{16}$$

subject to:

$$w_l \in \{0,1\}; \quad \forall l \in L \tag{17}$$

$$w \in W, \tag{18}$$

where

$$\sum_{n \in N} \Delta P_n^{d^*} = \max_{\substack{\nu,\overline{\alpha},\overline{\gamma},\lambda,\mu,\\ \underline{\phi},\overline{\phi},\underline{\chi},\overline{\chi}}} \sum_{l \in L} (\overline{\phi}_l - \underline{\phi}_l) \overline{P}_l^f + \sum_{n \in N} (\overline{\alpha}_n + \lambda_n) P_n^d$$
$$+ \sum_{j \in J} \overline{\gamma}_j \overline{P}_j^g + \sum_{n \in N} (\overline{\chi}_n - \underline{x}_n) \overline{\delta} \tag{19}$$

subject to:

$$\nu_l \geq w_l; \quad \forall l \in L \tag{20}$$

$$\sum_{l \in L} (1 - \nu_l) = K \tag{21}$$

$$\nu_l \in \{0,1\}; \quad \forall l \in L \tag{22}$$

$$-\lambda_{O(l)} + \lambda_{D(l)} + \mu_l + \underline{\phi}_l + \overline{\phi}_l = 0; \quad \forall l \in L \tag{23}$$

$$\lambda_{n|j \in J_n} + \overline{\gamma}_j \leq 0; \quad \forall j \in J \tag{24}$$

$$-\sum_{l|O(l)=n} \frac{1}{x_l} \nu_l \mu_l + \sum_{l|D(l)=n} \frac{1}{x_l} \nu_l \mu_l + \underline{\chi}_n + \overline{\chi}_n = 0; \quad \forall n \in N \tag{25}$$

$$\lambda_n + \overline{\alpha}_n \leq 1; \quad \forall n \in N \tag{26}$$

$$\overline{\gamma}_j \leq 0; \quad \forall j \in J \tag{27}$$

$$\underline{\phi}_l \geq 0; \quad \forall l \in L \tag{28}$$

$$\overline{\phi}_l \leq 0; \quad \forall l \in L \tag{29}$$

$$\underline{\chi}_n \geq 0; \quad \forall n \in N \tag{30}$$

$$\overline{\chi}_n \leq 0; \quad \forall n \in N \tag{31}$$

$$\overline{\alpha}_n \leq 0; \quad \forall n \in N. \tag{32}$$

The upper-level problem (16)–(18) is identical to the upper-level problem (1)–(3) of the original trilevel program.

The lower-level problem (19)–(32) of the bilevel equivalent is associated with the two lowermost levels (4)–(14) of the original trilevel program. According to the strong duality theorem [35], the objective function (19) is equal to the dual lower-level objective function. Constraints (20)–(22) are identical to (5)–(7), respectively. The remaining constraints comprise the dual feasibility constraints (23)–(32) of the original lower-level problem (8)–(14). Nonlinear expressions (25) involving the product of binary variables and continuous variables are subsequently transformed into linear expressions using some well-known integer algebra results [36]. Further details on this equivalent transformation can be found in [10,32].

4.2. Stage 2: Implicit enumeration algorithm

Similar to problem (1)–(14), the binary nature of lower-level decision variables ν_l in the bilevel problem (16)–(32) resulting from the first stage requires the use of alternative solution approaches. Scaparra and Church [31] 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 (16)–(32). 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 [35]. The algorithm starts at the root node of the search tree by solving the lower-level problem (19)–(32) 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 by which new nodes are created according to the new defense plans resulting from the solution to problem (19)–(32) in the parent nodes. Branching is implemented until either defensive resource limitations (18) can no longer be met or no more candidate components are available for defense, being the corresponding node denoted as a leaf. The implicit enumeration algorithm is stopped when all nodes are leaves. The optimal solution is the feasible defense plan with the lowest value of the upper-level objective function (16).

The proposed methodology is shown in Fig. 3 and works as follows:

1. *Initialization*: Initialize the node set M 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 M. 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 (19)–(32) for the corresponding vector $w^{(m)}$, thus yielding $\nu^{(m)}$ and $\sum_{n \in N} \Delta P_n^{d^{(m)}}$. Those assets l with $\nu_l^{(m)} = 0$ 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 set of defended assets cannot be further expanded without violating (18) or $C^{(m)}$ is empty then go to step 5 since node m becomes a leaf.
4. *Branching*: Choose an element l from the set of candidate components for defense $C^{(m)}$ and create two new nodes. In one node, transmission asset l is hardened, i.e., the vector of defended assets w is updated by setting w_l=1. In the other node, asset l is not hardened, i.e., w_l=0. Add the newly created nodes to the node set M.

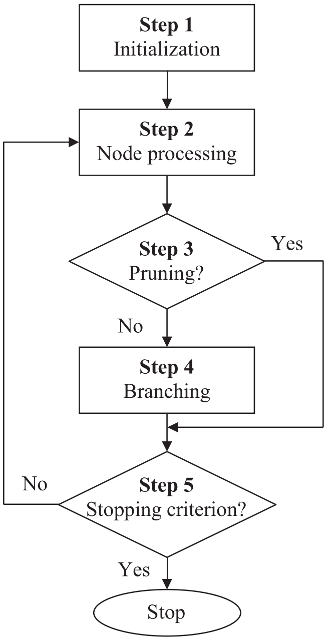

Fig. 3. Flowchart of the implicit enumeration algorithm.

5. *Stopping criterion*: If the node set M 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 [31] for the case of defensive resource limitations (18) adopting the cardinality form of (15), the upper bound for the number of node evaluations is $(K^{Z+1}-1)/(K-1)$, which does not depend on the system size and is significantly lower than the total number of feasible solutions $\binom{card(L)}{Z}\binom{card(L)-Z}{K}$.

It is worth mentioning that step 2 is suitable for parallel implementation, thereby leading to significant computational savings. This step also lends itself to depth-first and breadth-first search strategies analogous to those used in the branch-and-bound algorithm, which may yield additional computational improvement. Moreover, the optimal solution to problem (19)–(32) 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, although constituting distinctive features over [3,27,28], are beyond the scope of this paper.

5. Numerical results

This section presents results from three case studies. First, two test cases based on the IEEE Reliability Test System [37] are analyzed, namely, the One Area RTS-96 (RTS1) and the Two Area RTS-96 (RTS2). The IEEE Reliability Test System is widely adopted as a benchmark in the literature related to power system vulnerability [2,3,9,11–19,23–29] since it allows both reproducibility and a comprehensive analysis of the results. 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.

In order to assess the scalability of the proposed approach, a case study based on the IEEE 300-bus system [38] has also been analyzed. This system comprises 411 transmission assets, 69 generating units, and 191 demands.

For illustration purposes, expression (18) has been modeled as the cardinality constraint (15). Defense schemes of up to 5 components and disruption plans comprising up to 12 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 [39]. The optimization problems were solved with CPLEX 11.2 [40] under GAMS 23.0 [41].

5.1. Case RTS1

Table 6 provides information on optimal vulnerability levels attained by the two-stage algorithm for case RTS1. The second column lists the maximum levels of damage for the undefended system, i.e., for $Z=0$. Note that at least two out-of-service assets, i.e., $K=2$, are required to cause load shedding. Columns 3–7 list the percent vulnerability reduction over the undefended case when hardening is implemented.

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 $K=2$ and 45.4% for $K=12$.

Moreover, the proposed approach provides the system planner with valuable information on the compliance with a deterministic N-K security criterion, which is the standard in industry practice for values of K equal to 1 or 2 [8]. As shown in Table 6, the test system meets the N-1 criterion with no need for defense, whereas hardening four components practically ensures the N-2 security criterion. Note that higher values of K require the allocation of further defensive resources.

Table 6 is also useful to analyze the tradeoff between the defense cost incurred by adding defensive resources and the gain in vulnerability mitigation. Most of the defense benefit is achieved with a maximum of three defended assets, since they contribute more than 50% of the overall improvement. In contrast, larger defense investments produce progressively lower vulnerability reductions.

The case characterized by $K=4$ and $Z=4$ is relevant to motivate the need for a defender-attacker-defender model since it illustrates the suboptimality of defending critical transmission assets as determined by an attacker-defender model [3]. For $K=4$, the optimal solution provided by an attacker-defender model [12] identifies two sets of critical transmission assets whose disruption yields a maximum vulnerability level of 516 MW: (i) 3-24, 12-23, 13-23, and 14-16, and (ii) 12-23, 13-23, 14-16, and 15-24. The defense of either of those critical sets would yield a maximum

Table 6
Case RTS1. Impact of defense planning on vulnerability.

K	System load shed without defense (MW)	System load shed reduction (%)				
		Z				
		1	2	3	4	5
1	0	–	–	–	–	–
2	194	29.9	61.9	63.4	97.4	97.4
3	309	31.4	37.2	41.7	44.7	56.0
4	516	25.0	33.7	37.6	40.1	51.9
5	842	23.0	26.7	46.8	49.8	62.0
6	1017	19.1	39.3	50.5	55.1	56.5
7	1017	14.3	21.5	37.2	39.3	49.8
8	1198	12.6	20.1	38.9	45.7	49.7
9	1373	17.6	30.3	40.1	47.2	55.4
10	1373	12.7	25.1	35.0	44.3	47.1
11	1428	9.5	25.5	34.2	38.6	47.5
12	1468	8.7	19.8	30.5	39.2	45.4

level of system load shed equal to 387 MW, i.e., a 25.0% vulnerability reduction. Both suboptimal defense plans are shown in Fig. 4. In contrast, the optimal four-asset defense plan against any combination of four disrupted transmission components includes the hardening of assets 7-8, 10-12, 12-23, and 14-16, as depicted in Fig. 4. With this defense scheme, the maximum damage inflicted on the protected system is equal to 309 MW thereby leading to a 40.1% reduction in the vulnerability level (Table 6). In other words, the optimal solution to the defense planning problem significantly improves upon the intuitive solutions by 25.2%.

The average computing time required to achieve the optimal solutions to all simulations was 3.9 min. In order to assess the performance of the proposed approach we have implemented the method reported in [27]. For $K=1$ and $K=2$, the approach proposed by Yao et al. performed similar to the proposed two-stage method. However, for values of K exceeding 2 the algorithm of [27] was unable to find the optimal solution within 20 000 s. These results substantiate the superiority of the proposed two-stage approach.

5.2. Case RTS2

The optimal results for case RTS2 are listed in Table 7. As can be observed, the mitigation of vulnerability for a specific value of Z generally reaches a lower level than that for case RTS1 due to the larger size of the test system. Notwithstanding, it should be noted that significant vulnerability reductions are achieved by defending a relatively low number of transmission assets.

The average computing time for the simulations of this case was 19.6 min, which represents a moderate computational effort, bearing in mind that a planning problem is solved. Similar to case RTS1, the available tool described in [27] failed to efficiently address this medium-sized test system, thus corroborating that the proposed methodology is a superior approach.

5.3. Case based on the IEEE 300-bus system

The optimal results for the case based on the IEEE 300-bus system are listed in Table 8. Unlike cases RTS1 and RTS2, disrupting a single transmission asset yields load shedding due to the presence of radial areas within the system, which are highly vulnerable. Note also that, as expected, the larger size of this system leads to lower levels of vulnerability reduction for the same amount of defensive resources. As can be seen, for $Z=5$, vulnerability is reduced by factors ranging between 0.71% for $K=1$ and 8.38% for $K=12$.

The average computing time required to attain optimality for this larger case study was 35.3 min. Therefore, the associated computational effort is still moderate within the context of power system planning.

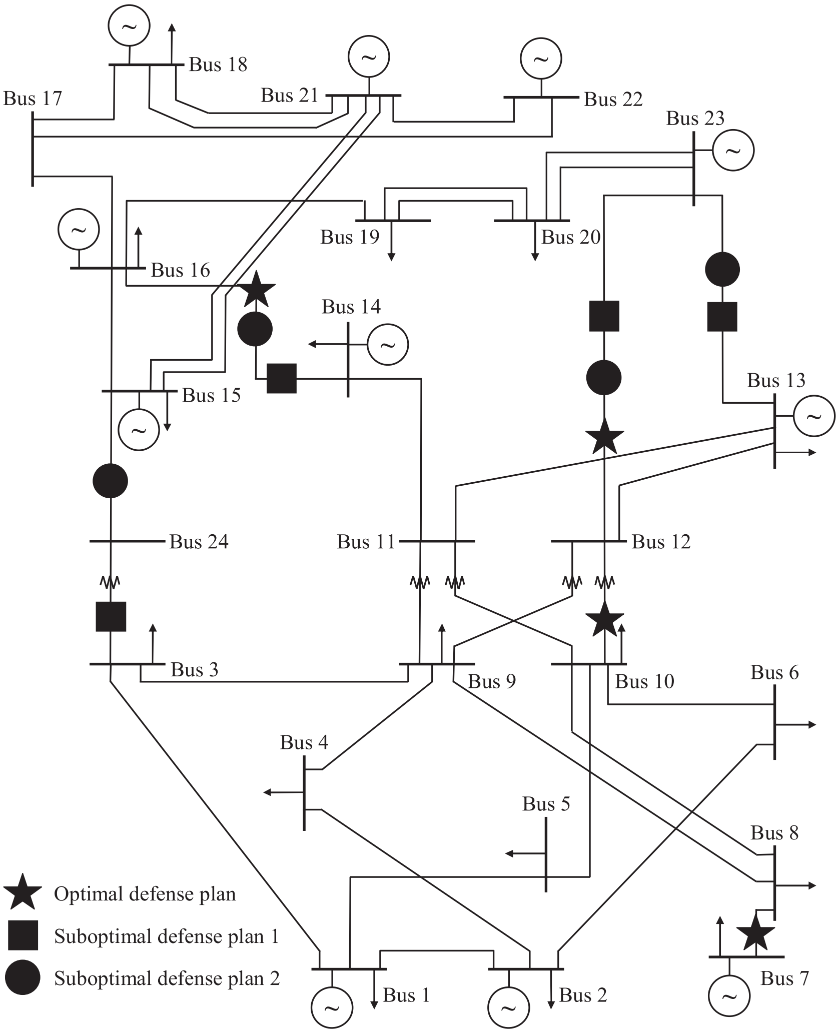

Fig. 4. Case RTS1. Defense plans for $Z=4$ and $K=4$.

Table 7
Case RTS2. Impact of defense planning on vulnerability.

K	System load shed without defense (MW)	System load shed reduction (%)				
		Z				
		1	2	3	4	5
1	0	–	–	–	–	–
2	194	0.0	29.9	29.9	61.9	61.9
3	309	0.0	37.2	37.2	41.7	44.7
4	442	8.1	22.6	30.1	30.1	38.5
5	842	20.8	23.0	38.6	43.8	43.8
6	1017	17.2	19.1	36.3	37.5	39.2
7	1036	1.8	18.7	20.6	29.7	35.6
8	1211	14.5	16.0	25.4	27.9	32.9
9	1373	11.8	17.6	23.7	25.9	32.6
10	1684	11.5	23.0	28.3	32.8	40.3
11	1859	10.4	21.5	29.3	34.9	39.8
12	1859	7.8	15.9	19.9	28.7	33.6

Table 8
Case based on the IEEE 300-bus system. Impact of defense planning on vulnerability.

K	System load shed without defense (MW)	System load shed reduction (%)				
		Z				
		1	2	3	4	5
1	8071.3	0.03	0.15	0.53	0.64	0.71
2	8368.9	0.35	0.63	1.15	1.34	1.64
3	8613.9	0.20	0.99	1.43	1.56	2.03
4	8883.1	0.46	1.05	1.85	2.29	2.72
5	9128.3	0.88	1.23	2.19	2.63	3.15
6	9396.6	0.79	1.91	2.60	3.09	3.79
7	9653.9	1.07	2.18	2.54	3.78	4.59
8	9889.1	0.85	1.68	2.91	4.18	5.21
9	10 146.1	1.05	2.13	3.56	4.64	6.08
10	10 439.5	1.13	2.81	4.38	5.45	7.12
11	10 721.1	1.71	3.49	5.04	6.36	8.03
12	10 937.8	1.83	3.58	5.17	6.73	8.38

6. Conclusions

This paper has presented a new approach for the optimal allocation of defensive resources in an electric power grid to mitigate the vulnerability against multiple contingencies. This planning 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 cases based on the IEEE Reliability Test System and the IEEE 300-bus system. Numerical results show that the proposed tool is a useful instrument for the system planner to identify optimal defense strategies to mitigate the vulnerability against multiple contingencies. Simulations also reveal the effective performance of the proposed approach and its superiority over previously reported methods.

Although computational issues are not a primary concern in this kind of planning problems, we recognize that the proposed approach may be computationally expensive for a large power system. Further work will examine the computational savings that may be gained from the parallel implementation of the implicit enumeration algorithm, the consideration of effective strategies for exploring the search tree, and the use of appropriate initialization schemes in the evaluation of the tree nodes.

Moreover, this method could be extended to address additional complexities of power systems such as reactive power, stability issues, and cascading power failures.

References

[1] Gheorghe AV, Masera M, Weijnen M, de Vries L. Critical infrastructures at risk. Securing the European electric power system. Dordrecht: Springer; 2006.

[2] Brown GG, Carlyle WM, Salmerón J, Wood K. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In: Greenberg HJ, Smith JC, editors. Tutorials in operations research. Emerging theory, methods, and applications Hanover: INFORMS; 2005. p. 102–23.

[3] Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces 2006;36:530–44.

[4] 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. ⟨http://www.nerc.com/filez/blackout.html⟩ [accessed December 19, 2012]; 2004.

[5] Larsson S, Ek E. The black-out in southern Sweden and eastern Denmark, September 23, 2003. In: Proceedings of the 2004 IEEE Power Engineering Society General Meeting, Denver, USA; 2004. p. 1668–72.

[6] Berizzi A. The Italian 2003 blackout. In: Proceedings of the 2004 IEEE Power Engineering Society General Meeting, Denver, USA; 2004. p. 1673–9.

[7] E.ON Netz GmbH. Report on the status of the investigations of the sequence of events and causes of the failure in the continental European electricity grid on Saturday, November 4, 2006, after 22:10 hours. 2006.

[8] Wood AJ, Wollenberg BF. Power generation, operation, and control. 2nd ed. New York: John Wiley & Sons, Inc.; 1996.

[9] Salmeron J, Wood K, Baldick R. Analysis of electric grid security under terrorist threat. IEEE Transactions on Power Systems 2004;19:905–12.

[10] Alvarez RE. Interdicting electrical power grids. M.Sc. thesis, Monterey: Naval Postgraduate School; 2004.

[11] Arroyo JM, Galiana FD. On the solution of the bilevel programming formulation of the terrorist threat problem. IEEE Transactions on Power Systems 2005;20:789–97.

[12] Motto AL, Arroyo JM, Galiana FD. A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat. IEEE Transactions on Power Systems 2005;20:1357–65.

[13] Bier VM, Gratz ER, Haphuriwat NJ, Magua W, Wierzbicki KR. Methodology for identifying near-optimal interdiction strategies for a power transmission system. Reliability Engineering and System Safety 2007;92:1155–61.

[14] Salmeron J, Wood K, Baldick R. Worst-case interdiction analysis of large-scale electric power grids. IEEE Transactions on Power Systems 2009;24:96–104.

[15] Delgadillo A, Arroyo JM, Alguacil N. Analysis of electric grid interdiction with line switching. IEEE Transactions on Power Systems 2010;25:633–41.

[16] Bienstock D, Verma A. The N-k problem in power grids: new models, formulations, and numerical experiments. SIAM Journal on Optimization 2010;20:2352–80.

[17] Donde V, López V, Lesieutre B, Pinar A, Yang C, Meza J. Severe multiple contingency screening in electric power systems. IEEE Transactions on Power Systems 2008;23:406–17.

[18] Arroyo JM. Bilevel programming applied to power system vulnerability analysis under multiple contingencies. IET Generation, Transmission & Distribution 2010;4:178–90.

[19] Pinar A, Meza J, Donde V, Lesieutre B. Optimization strategies for the vulnerability analysis of the electric power grid. SIAM Journal on Optimization 2010;20:1786–810.

[20] Bard JF. Practical bilevel optimization. Algorithms and applications. Dordrecht: Kluwer Academic Publishers; 1998.

[21] Dempe S. Foundations of bilevel programming. Dordrecht: Kluwer Academic Publishers; 2002.

[22] Seifu A, Salon S, List G. Optimization of transmission line planning including security constraints. IEEE Transactions on Power Systems 1989;4:1507–13.

[23] Carrión M, Arroyo JM, Alguacil N. Vulnerability-constrained transmission expansion planning: a stochastic programming approach. IEEE Transactions on Power Systems 2007;22:1436–45.

[24] Alguacil N, Carrión M, Arroyo JM. Transmission network expansion planning under deliberate outages. International Journal of Electrical Power & Energy Systems 2009;31:553–61.

[25] Arroyo JM, Alguacil N, Carrión M. A risk-based approach for transmission network expansion planning under deliberate outages. IEEE Transactions on Power Systems 2010;25:1759–66.

[26] Holmgren ÅJ, Jenelius E, Westin J. Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Transactions on Power Systems 2007;22:76–84.

[27] Yao Y, Edmunds T, Papageorgiou D, Alvarez R. Trilevel optimization in power network defense. IEEE Transactions on Systems, Man, and Cybernetics–Part C: Applications and Reviews 2007;37:712–8.

[28] Rose RW. Defending elecrical power grids. M.Sc. thesis, Monterey: Naval Postgraduate School; 2007.

[29] Chen G, Dong ZY, Hill DJ, Xue YS. Exploring reliable strategies for defending power systems against targeted attacks. IEEE Transactions on Power Systems 2011;26:1000–9.

[30] Vicente LN, Calamai PH. Bilevel and multilevel programming: a bibliography review. Journal of Global Optimization 1994;5:291–306.

[31] Scaparra MP, Church RL. A bilevel mixed-integer program for critical infrastructure protection planning. Computers & Operations Research 2008;35:1905–23.

[32] Bertsimas D, Sim M. Robust discrete optimization and network flows. Mathematical Programming 2003;98:49–71.

[33] Street A, Oliveira F, Arroyo JM. Contingency-constrained unit commitment with n-K security criterion: a robust optimization approach. IEEE Transactions on Power Systems 2011;26:1581–90.

[34] Jiang R, Wang J, Guan Y. Robust unit commitment with wind power and pumped storage hydro. IEEE Transactions on Power Systems 2012;27:800–10.

[35] Nemhauser GL, Wolsey LA. Integer and combinatorial optimization. New York: Wiley-Interscience; 1999.

[36] Floudas CA. Nonlinear and mixed-integer optimization: fundamentals and applications. New York: Oxford University Press; 1995.

[37] Reliability Test System Task Force. The IEEE Reliability Test System-1996. IEEE Transactions on Power Systems 1999;14:1010–20.

[38] The Power Systems Test Case Archive website. ⟨http://www.ee.washington.edu/research/pstca⟩ [accessed December 19, 2012]; 2012.

[39] The MathWorks website. ⟨http://www.mathworks.com⟩ [accessed December 19, 2012]; 2012.

[40] The IBM ILOG CPLEX website. ⟨http://www-01.ibm.com/software/integration/optimization/cplex-optimizer⟩ [accessed December 19, 2012]; 2012.

[41] The GAMS Development Corporation website. ⟨http://www.gams.com⟩ [accessed 19.12.2012]; 2012.