Correspondence

Trilevel Optimization in Power Network Defense

Yiming Yao, *Member, IEEE*, Thomas Edmunds, Dimitri Papageorgiou, and Rogelio Alvarez

***Abstract*—We present a trilevel optimization model of resource allocation in electric power network defense. This model identifies the most critical network components to defend against possible terrorist attacks. The goal of defense is to minimize the economic cost that the attacks may cause, subject to resource constraints. We describe a decomposition approach for finding an optimal solution to the trilevel model, which is based on iteratively solving smaller nested bilevel problems. Our testing results demonstrate the advantages of trilevel optimization over bilevel optimization in network defense.**

***Index Terms*—Homeland security, interdiction, multilevel optimization, network defense.**

I. Introduction

Infrastructure networks supplying electricity, natural gas, water, and other commodities are at risk of disruption due to well-engineered and coordinated terrorist attacks. Countermeasures such as hardening targets, acquisition of spare critical components, and surveillance can be undertaken to detect and deter these attacks. Stockpiling spares of critical energy infrastructure components has been identified as a key element of a grid infrastructure defense strategy in a recent National Academy of Sciences report [1]. Allocation of available countermeasure resources to sites in a manner that maximize their effectiveness is a challenging problem. This allocation must take into account the adversary's response after the countermeasure assets are in place and subsequent mitigation measures the infrastructure operator can undertake after the attack. The adversary may simply switch strategies to avoid countermeasures while executing the attack.

Consider a scenario where an attacker attempts to interrupt the service of an electric power network by disabling some of its facilities while a defender wants to prevent or minimize the effectiveness of any attack. The interaction between the attacker and the defender can be described in three stages.

1) The defender deploys countermeasures.
2) The attacker disrupts the network.
3) The defender responds to the attack by rerouting power to maintain service while trying to repair damage.

In the first stage, the defender considers all possible attack scenarios, and deploys countermeasures to defend against an optimizing attacker. Countermeasures can include hardening targets, acquiring spare critical components, and installing surveillance devices. In the second stage, the attacker, with full knowledge of the deployed countermeasures, attempts to disable some nodes or links in the network to inflict the greatest loss on the defender. In the third stage, the defender redispatches power and restores disabled nodes or links to minimize the loss. The loss can be measured in economic terms, including the cost of using more expensive generators and the monetary losses that can be attributed to loss of load. The defender's goal is to minimize the loss while the attacker wants to maximize it.

The infrastructure network defense problem can be formulated as a trilevel optimization model, which is an extension of the bilevel program or Stackelberg game [2], [3]. In the two-stage game, a leader acts first to deploy countermeasures; then, a follower in the game observes the countermeasure deployment, and chooses a strategy with maximal system impact. Researchers in systems science, cybernetics, and operations research have developed algorithms to address instances of the bilevel programming problem [4]–[8]. Bard, Moore, and Edmunds replace the bilevel program by an equivalent single-level nonlinear program using Karush–Kuhn–Tucker optimality conditions [4]–[6]. The equivalent nonlinear optimization problem is then solved with a branch and bound scheme, where each branch corresponds to a complementary slackness condition.

The aforementioned general-purpose algorithms do not exploit the particular structure in the infrastructure network defense problem. In this problem, the defender and attacker play a zero sum game, i.e., the defender tries to minimize the same objective function that the attacker tries to maximize. Most algorithms that exploit this structure have been developed for problems in the system interdiction literature [9]–[12]. Israeli and Wood [9]–[10] use Benders' decomposition, and set covering methods to solve bilevel mixed integer (binary) linear programs in which only the upper bounds of the defender's decision variables are affected by the attacker's decisions. Israeli and Wood [9] have extended their methodology to solve trilevel mixed integer (binary) linear programs under the same restriction.

Salmeron, Wood, and Baldick [11]–[12] formulate the attacker's problem as a network interdiction problem. Their formulation differs from that of Israeli and Wood [9]–[10] in that the attacker's decision can effectively remove certain constraints in the defender's response model, in addition to affecting the upper bounds of the defender's decision variables. They also attempt to model the temporal element of system restoration, where the attacker's interdiction plan will disable some network components (e.g., a substation) for a longer period of time than other components (e.g., a power line). They develop heuristics to generate good solutions to the interdiction model by approximating the attacker's objective with a penalty function generated from the solution to the defender's response model.

In this correspondence, we extend the bilevel model of Salmeron *et al.* [11] by formulating the infrastructure network defense problem as a trilevel optimization model. Unlike the bilevel model, which only seeks to determine the single most damaging attack plan, our trilevel model provides a robust defense strategy against the n most damaging attack plans. One could argue that the solution to the bilevel model may also heuristically guide the defender to prevent more than just the single most damaging attack plan; however, it is our experience that the presence of multiple optima and ε-optimal solutions [13] render heuristic determination of high-quality defense plans difficult and/or time consuming. Furthermore, while the bilevel model represents passive defense in the sense that the defender responds to an attack only after it happens, the trilevel model can be considered active defense, since the defender deploys countermeasure resources in anticipation of an attack. The trilevel model is more complex than the bilevel model, and

Manuscript received January 13, 2005; revised August 10, 2006. This work was supported by Lawrence Livermore National Laboratory operated by the University of California for the U.S. Department of Energy under Contract W-7405-Eng-48. This paper was recommended by Editor V. Marik.

Y. Yao and T. Edmunds are with Lawrence Livermore National Laboratory, Livermore, CA 94550 USA (e-mail: yao3@llnl.gov; edmunds2@llnl.gov).

D. Papageorgiou is with the University of Texas, Austin, TX 78712 USA (e-mail: djpapag@mail.utexas.edu).

R. Alvarez is with the Naval Postgraduate School, Monterey, CA 93943 USA (e-mail: realvare@nps.navy.mil).

Digital Object Identifier 10.1109/TSMCC.2007.897487

therefore, its solution requires more computational effort. We present an exact algorithm based on a decomposition approach that finds an optimal solution to the trilevel model.

In this correspondence, we first present our formulation of the infrastructure network defense problem, followed by a description of the solution procedure. We, then, discuss testing results, and explore future research directions.

II. Problem Formulation

As described in Section I, the infrastructure network defense problem can be viewed as having three stages or levels: 1) the defender hardens the network; 2) the attacker attacks the network; and 3) the defender responds to the attack. Each level can be represented as an optimization model. The top level proposes a defense plan, the middle level then produces a most damaging attack plan under the defense, and the bottom level computes an optimal power distribution scheme in response to the attack. This section presents the problem formulation at each level, starting at the bottom with level 3, in which the defender responds to an attack.

A. Defender's Response Model

After an attack, the defender tries to produce and distribute power with undamaged generators and transmission facilities at minimum cost to meet customer demand on the power network. Technical details regarding power network operations can be found in [14]. A power network includes generators, buses, power lines, and substations. Power generated at a particular bus is used to satisfy demand at that bus and flows along power lines to satisfy demands at other buses. Power lines connecting buses can either be unitary or in parallel. A substation is a group of buses, and a bus is connected to one or more generators and power lines. The defender's objective is to minimize the generation cost and the cost incurred from unmet demand by solving a nonlinear AC optimal power flow (OPF) problem. We follow a common practice in electric utility management [14], and use a linear approximation of the nonlinear OPF problem. We model the linearized OPF problem as a linear program.

The objective function, which reflects the costs of power generation and unmet demands, can be expressed as

$$f(\mathbf{g}, \mathbf{h}) = \sum_{i\in G} c_i g_i + \sum_{i\in B} u_i h_i \tag{1}$$

where g_i is the power flow from generator i, c_i is the unit cost associated with g_i, G is the set of indices for all generators, h_i is the amount of unmet demand at bus i, u_i is the unit cost associated with h_i, and B is the set of indices for all buses.

There are several sets of constraints. The first one describes the power flow and phase angle relationship as

$$p_i - s_i\left(\theta_{o(i)} - \theta_{t(i)}\right) = 0 \qquad \forall i \in L \tag{2}$$

where p_i is the power flow on line i, s_i is the susceptance for line i, $\theta_{o(i)}$ is the originating bus's phase angle, $\theta_{t(i)}$ is the terminating bus's phase angle, and L is the set of indices for all power lines.

The second set of constraints provides lower and upper bounds for the variables as

$$\begin{array}{ll} 0 \le g_i \le \bar{g}_i & \forall i \in G \\ -\bar{p}_i \le p_i \le \bar{p}_i & \forall i \in L \\ h_i \ge 0 & \forall i \in B \end{array} \tag{3}$$

where $\bar{g}_i$ is the capacity of generator i, and $\bar{p}_i$ is the transmission capacity of line i.

Finally, there are constraints for conservation of flows. Normally, the power generated plus the power flowing into bus b equals the power flowing out plus the demand at bus b. When it is impossible to satisfy all demand, "unmet demand" is subtracted from the demand to balance the conservation of flows. Mathematically, this is represented as

$$\sum_{i\in G(b)} g_i + \sum_{i\in L_{t(b)}} p_i - \sum_{i\in L_{o(b)}} p_i = d_b - h_b \qquad \forall b \in B \tag{4}$$

where $G(b)$ is the set of all generators at bus b, $L_{o(b)}$ is the set of all lines originating at bus b, $L_{t(b)}$ is the set of all lines terminating at bus b, and d_b is the power demand at bus b.

Note that for buses with no demand, both h_b and d_b are zero. In an optimal solution, the unmet demand h_b will be zero if generators at bus b and other buses can produce and route (via power lines) enough power to satisfy d_b; otherwise, h_b will be positive. We can guarantee that this condition holds at optimality by ensuring that there is a sufficiently large penalty associated with unmet demand. To this end, for the remainder of the correspondence, we make the assumption that the minimum unit cost for unmet demand is greater than the maximum unit generation cost, i.e., $\min(u)_{i\in B} > \max(c_i)_{i\in G}$.

In summary, the defender's response model is a linearized OPF problem

$$\text{OPF}: \min_{(\boldsymbol{p},\boldsymbol{g},\boldsymbol{h},\boldsymbol{\theta})} f(\mathbf{g}, \mathbf{h})$$
$$\text{subject to (2)–(4).}$$

B. Attacker's Problem

The attacker must decide which network elements to attack. Let $y_j = 1$ if element j is attacked, and $y_j = 0$ otherwise. We assume that a network element will be completely disabled if it is attacked. The attacker's decision will impact the OPF model by interfering with power generation and flow. As a result, two sets of constraints in the OPF problem must be modified. Constraints (2) become

$$p_i = s_i(\theta_{o(i)} - \theta_{t(i)}) \prod_{j\in J(i)} (1 - y_j) \qquad \forall i \in L \tag{5}$$

where $J(i)$ is the set of indices of y_j variables that can make $p_i = 0$. For example, if index i represents a power line, $J(i)$ will include indexes of three y_j variables–one for the line itself and two for the end buses. Constraints (5) imply that if a line is attacked, the phase angle constraint for that line need not be enforced. This feature is included in Salmeron *et al.* [11], [12] but not in Israeli and Wood [9], [10].

With the introduction of y_j variables, the first two sets of constraints in (3) of OPF will have parameterized bounds, and the last set will remain the same.

$$\begin{array}{ll} 0 \le g_i \le \prod_{j\in G(i)} (1 - y_j)\bar{g}_i, & \forall i \in G \\ -\prod_{j\in J(i)} (1 - y_j)\bar{p}_i \le p_i \le \prod_{j\in J(i)} (1 - y_j)\bar{p}_i, & \forall i \in L \\ h_i \ge 0 & \forall i \in B \end{array} \tag{6}$$

where $G(i)$ is the set of indices of y_j variables that can make $g_i = 0$.

The attacker is limited by a budget, which leads to the constraint

$$\sum_{j\in J} r_j y_j \le r \tag{7}$$

where J is the set of indices of all attackable elements, r_j is the number of resources needed to attack element j, and r is the total number of resources available to the attacker.

There are several logical relationships between the variables that we assume, which prevent the attacker from making redundant interdictions, and thus, from expending unnecessary resources [10]. Specifically, we make the following assumptions on the consequences of each potential attack type: 1) an attack on a power line disables all of its parallel lines, in addition to the line itself; 2) an attack on a bus disables all the generators and power lines connected to it; and 3) an attack on a substation disables all of its buses. The aforementioned assumptions lead to the following sets of constraints:

$$\sum_{j \in L^y \cap \text{parallel}} y_j \le 1, \qquad \text{for all groups of parallel lines} \tag{8}$$

$$y_g + y_b \le 1 \qquad \forall g \in G^y(b), \forall b \in B^y \tag{9}$$

$$y_l + y_b \le 1 \qquad \forall l \in L^y_{o(b)}, L^y_{t(b)}, \text{and} \, \forall b \in B^y \tag{10}$$

$$y_b + y_s \le 1 \qquad \forall b \in B^y, \forall s \in S^y. \tag{11}$$

The superscript y denotes the subset of attackable elements from a corresponding set in the OPF model. As an example, a constraint in (9) prevents the attacker from using resources to interdict generators connected to a bus that has already been disabled, since we assume that all lines and generators connected to a disabled bus are disabled as well.

Since the attacker's objective is to maximize the defender's cost, we can formulate the attacker's problem as the following bilevel optimization model:

$$\begin{aligned}
\text{AP:} \quad & \max_{\mathbf{y}} \text{OPF}(\mathbf{y}) \\
& \quad \text{subject to (7)–(11)} \\
& \qquad y_j \in \{0, 1\}, \ \forall j \in J \\
& \qquad \text{where } \text{OPF}(\mathbf{y}) = \min_{(\mathbf{p}, \mathbf{g}, \mathbf{h}, \theta)} f(\mathbf{g}, \mathbf{h}) \\
& \qquad\qquad \text{subject to (4)–(6)}
\end{aligned}$$

Note that the minimization problem OPF(**y**) is a linearized optimal power flow problem conditioned on the attacker's interdiction plan **y**.

C. Defender's Problem

The decision to defend network element k can be represented by a binary variable x_k, where $x_k = 1$ if element k is defended, and $x_k = 0$ otherwise. We assume that a network element is infallible if it is defended. The defender's decision impacts the attacker through the constraints given by

$$y_j \le \prod_{k \in K(j)} (1 - x_k) \qquad \forall j \in J \tag{12}$$

where $K(j)$ is the set of all elements that collectively can make element j infallible. For example, if j represents a power line, $K(j)$ will include three elements—the line itself and its two end buses.

Like the attacker, the defender also has a defense budget constraint given by

$$\sum_{k \in K} q_k x_k \le q \tag{13}$$

where K is the set of defendable elements, q_k is the number of resources needed to defend element k, and q is the total number of resources available to the defender.

We make two assumptions to prevent the defender from making redundant defenses: 1) defending one power line simultaneously defends all power lines running in parallel with it, if any exist; and 2) defending a substation defends all of its buses as well. These assumptions are modeled by the following sets of constraints:

$$\sum_{k \in L^x \cap \text{parallel}} x_k \le 1, \quad \text{for all groups of parallel lines} \tag{14}$$

$$x_b + x_s \le 1 \qquad \forall b \in B^x, \forall s \in S^x. \tag{15}$$

The superscript x denotes the subset of defendable elements from a corresponding set in the OPF model. As an example, a constraint in (15) prevents the defender from using resources to defend an individual bus if the substation containing it has already been defended.

Considering the defender's cost minimization objective, we can formulate the defender's problem as a trilevel optimization model.

$$\begin{aligned}
\text{DP:} \ & \min_{\mathbf{x}} \text{AP}(\mathbf{x}) \\
& \quad \text{subject to (12)–(15)} \\
& \qquad x_k \in \{0, 1\}, \forall k \in K \\
& \qquad \text{where } \text{AP}(\mathbf{x}) = \max_{\mathbf{y}} \text{OPF}(\mathbf{y}) \\
& \qquad\qquad \text{subject to (7)–(11)} \\
& \qquad\qquad\quad y_j \in \{0, 1\}, \forall j \in J \\
& \qquad\qquad\quad \text{where } \text{OPF}(\mathbf{y}) = \min_{(\mathbf{p}, \mathbf{g}, \mathbf{h}, \theta)} f(\mathbf{g}, \mathbf{h}) \\
& \qquad\qquad\qquad \text{subject to (4)–(6)}
\end{aligned}$$

AP(**x**) is the attacker's problem conditioned on the defense plan **x**.

III. Solution Methodology

The trilevel optimization model for infrastructure network defense problem has a "min-max-min" structure that can be viewed as a nested bilevel optimization model. There are at least two general approaches one might consider to obtain a tractable model—duality and decomposition. We begin by making observations about the duality approach for the bilevel problem, and then, extend these comments to the trilevel case.

A first approach to solving a bilevel optimization problem with a nested "max-min" structure, in which the leader and the follower are diametrically opposed, is to take the dual of the inner minimization problem. This converts the inner problem into a maximization problem, which allows us to formulate a single model in which we simultaneously optimize the leader's decision variables and the follower's (dual) decision variables [15]. The key obstacle to overcome when attempting such an approach is that the resultant "max-max" formulation may not yield a tractable structure that is amenable to solution through standard optimization algorithms. Indeed, for our problem, dualizing the inner minimization problem (OPF) leads to a highly nonlinear structure due to the presence of cross products between the attacker's interdiction variables and the defender's dual variables [see (5) and (6)]. Salmeron *et al.* [12] reformulate this "max-max" problem as a mixed integer linear program (MILP) by introducing additional decision variables and constraints in the model to replace these cross products, but this does little to reduce the work required to solve the trilevel problem. We are still left with the task of dualizing either the highly nonlinear problem or its MILP reformulation in order to obtain a nested "min-min-min" structure, which itself has multiple products between decision variables. Furthermore, with the inclusion of additional constraints and decision variables, the model may become quite large.

In light of the complicating factors associated with the duality approach, we have opted for a decomposition-based approach, in which we iteratively solve smaller bilevel programs. Our approach to solving each bilevel program can be viewed as an extension of a set covering decomposition discussed by Israeli and Wood [9], [10], and allows us to exploit the interaction between the attacker and the defender in each of these bilevel problems.

In Section III-A, we first describe the algorithm for the solution of the defense problem, and then, the algorithms for the embedded attack and response models. In Section III-B, we use a simple example to illustrate the solution procedure.

A. Solution of the Defense Problem

We present a solution procedure that follows the interaction between the defender and the attacker. Without knowledge of an attack plan, the defender's problem can be formulated as a feasibility problem given by

$$\begin{aligned}\text{RDP:}\quad & \text{find } \mathbf{x}\\ & \text{subject to (12)–(15)}\\ & \qquad x_k \in \{0, 1\},\ \forall k \in K.\end{aligned}$$

RDP is a relaxation of the original defender's problem. A trivial solution to RDP is $\mathbf{x}^0 = 0$, in which no network components are defended. Given the defense plan $\mathbf{x}^0$, the attacker's goal is to find an attack plan $\mathbf{y}^0$ $(\mathbf{x}^0)$ that maximizes the defender's cost of power generation and unmet demand. In response, the defender can attempt to avoid this maximum cost by defending, or "covering," at least one of the network components in the attacker's plan $\mathbf{y}^0$ $(\mathbf{x}^0)$, if enough resources are available. We model the defender's desire to cover at least one of the components that was attacked by adding the following constraint, or cut, to RDP:

$$\sum_{\forall k \in K1(y^0)} x_k \geq 1 \tag{16}$$

where $K1(\mathbf{y}^0)$ contains the indices of x variables that, when set to one, will set to zero at least one y variable that was nonzero in $\mathbf{y}^0$. Assume that a feasible solution to RDP exists after constraint (16) is appended to it, and denote this solution by $\mathbf{x}^1$. Note that at least one of the x variables in (16) must be one in $\mathbf{x}^1$. Still seeking to maximize the defender's total cost, the attacker will derive a new attack plan $\mathbf{y}^1$ $(\mathbf{x}^1)$, and a new cut will be added to RDP to cover $\mathbf{y}^1$ $(\mathbf{x}^1)$, given as

$$\sum_{\forall k \in K1(y^1)} x_k \geq 1. \tag{17}$$

The new RDP now consists of two cuts (16) and (17), in addition to the original constraints (12)–(15), and a new iteration of the algorithm follows. The algorithm will continue, eventhough, not all cuts in RDP can be satisfied along with the original constraints, i.e., the defender cannot cover all attack plans proposed due to the budgetary constraint. At this point, an optimal defense plan has been found. This solution procedure finds the optimal defense plan in a finite number of steps, since there are a finite number of possible attack plans. The algorithmic steps of the solution procedure are as follows.

Algorithm Defense

Purpose: to solve the defense problem for an optimal solution **x*** and objective value $\bar{v}$.

```
1) create initial RDP; $s \leftarrow 0,\ x^s \leftarrow \mathbf{0},\ and\ \bar{v} \leftarrow \infty$
2) while $\mathbf{x}^s \neq \emptyset$ do
3)     solve attack problem AP($\mathbf{x}^s$) for $\mathbf{y}^s$ and objective value $v^s$
       (see algorithm attack)
4)     if $v^s < \bar{v}$ then
5)         $\mathbf{x}^* \leftarrow \mathbf{x}^s$ and $\bar{v} \leftarrow v^s$
6)     add the following cut to RDP:
           $$\sum_{\forall k \in K1(y^s)} x_k \geq 1 \tag{18}$$
7)     $s \leftarrow s + 1$
8)     solve RDP for $\mathbf{x}^s$ (see Section III-D)
9) exit (an optimal defense plan $\mathbf{x}^*$ has been found with objective
       value $\bar{v}$).
```

In line 1), the algorithm creates the initial RDP that includes (12)–(15), sets $\mathbf{x}^0$ to $\mathbf{0}$ (no defense), and sets to infinity—the best objective value (OV) found so far. In line 3), it solves the attacker's problem, given the defense plan $\mathbf{x}^s$. If the OV is smaller than the best one found so far, it saves both the defense plan and the OV in line 5). The algorithm adds a cut in line 6), and solves the RDP for $\mathbf{x}^s$ in line 8). If $\mathbf{x}^s = \emptyset$ (the RDP is infeasible), it will break the while loop with an optimal solution (**x***) to the defense problem.

B. Solution of the Attack Problem

The attack problem can be solved in a similar manner as the defense problem. Initially, the relaxed attack problem is given by

$$\begin{aligned}\text{RAP}(\mathbf{x})\text{:}\quad & \text{find } \mathbf{y}\\ & \text{subject to (7)–(11)}\\ & \qquad y_j \in \{0, 1\},\ \forall j \in J.\end{aligned}$$

We start with attack plan $\mathbf{y}^0 = \mathbf{0}$ (or more precisely, $\mathbf{y}^0(\mathbf{x}) = \mathbf{0}$, but for ease of presentation, we suppress the dependency of the attack plan **y** on the defense plan **x**), and solve the OPF problem, i.e., OPF($\mathbf{y}^0$). Based on the solution to the OPF model, a cut is created and appended to RAP(**x**). This cut represents the attacker's aim to interdict at least one of the undefended components that took a nonzero value in the defender's response plan. Intuitively, the only way for the attacker to force a higher cost response plan from the defender is to disable one of these components. Then, we begin a new iteration by solving RAP(**x**) for $\mathbf{y}^1$. The procedure will continue until RAP(**x**) becomes infeasible, at which point, an optimal solution to the attack problem is found. Again, this solution procedure finds the optimal attack plan in a finite number of steps, since at worst, the attacker needs to cover all (but still a finite number of) solutions to the parameterized OPF problem.

Algorithm Attack

Purpose: to solve the attack problem for an optimal solution **y*** and objective value, given defense plan **x**.

```
1) create initial RAP($\mathbf{x}$); $s \leftarrow 0,\ \mathbf{x}^{S\leftarrow}\mathbf{0},\ \underline{v} \leftarrow -\infty$
2) while $\mathbf{y}^s \neq \emptyset$ do
3)     solve the optimal power flow problem OPF($\mathbf{y}^s$) for objective
       value $v^s$ [see Section III-C]
4)     if $v^s > \underline{v}$ then
5)         $\mathbf{y}^* \leftarrow \mathbf{y}^s$ and $\underline{v} \leftarrow v^s$
6)     add the following cut to RAP($\mathbf{x}$) based on the solution $\mathbf{z}^s =$
       $(\mathbf{p}^s, \mathbf{g}^s, \mathbf{h}^s, \theta^s)$ to OPF($\mathbf{y}^s$):
           $$\sum_{\forall j \in K2(p^s,\ g^s)} y_j \geq 1 \tag{19}$$
7)     $s \leftarrow s + 1$
8)     solve RAP($\mathbf{x}$) for $\mathbf{y}^s$ [see Section III-D]
9) return $\mathbf{y}^*$ and $\underline{v}$ (an optimal attack plan and its objective
       function value).
```

In line 6), $K2(\mathbf{p}^s, \mathbf{g}^s)$ contains the indices of y variables, which when set to one, will set to zero at least one p or g variable that was nonzero in ($\mathbf{p}^s$, $\mathbf{g}^s$). In line 9), the optimal attack plan is returned to algorithm defense. The rest of the algorithm attack is very similar to algorithm defense.

We can prove that algorithm attack correctly identifies an optimal attack plan, in a similar way as done by Israeli and Wood to prove the correctness of the set covering decomposition algorithms in [9] and [10]. First, note that algorithm attack always generates a cut of type (19) in step 6) that is distinct from all the other cuts generated previously. To see this fact, note that the feasible solution $\mathbf{y}^s$ to RAP($\mathbf{x}$) found at iteration $s (s > 0)$ satisfies all cuts generated from iteration 0 to iteration s-1, since these cuts are a part of RAP($\mathbf{x}$). However, $\mathbf{y}^s$ does not satisfy the cut generated at iteration s, since

$$y_j^s = 0 \qquad \forall j \in K2\left(\mathbf{p}^s, \mathbf{g}^s\right)$$

due to the way the subset $K2$ is constructed. Satisfying a cut of type (19) requires at least one element in $\mathbf{y}$ to be positive, and consumes at least one unit of the attacker's resources. Due to the attacker's resource constraint (7), only a limited number of distinct cuts can be satisfied; therefore, RAP($\mathbf{x}$) will become infeasible ($\mathbf{y}^s = \emptyset$ in step 2) in a finite number of iterations. Next, note that

$$\underline{v} \equiv \max_{j=0,\ldots,s-1} \text{OPF}(y^j)$$

is a valid lower bound to the optimal objective value v*, i.e., $v * \geq \underline{v}$, because it is the objective function value of a feasible attack plan. On the other hand, when RAP($\mathbf{x}$) becomes infeasible, this corresponds to the point at which the attacker cannot force the defender to generate a response with higher cost than any of the responses seen so far, i.e., $v* \leq \underline{v}$. Thus, $v* = \underline{v}$ when algorithm attack terminates. In the same fashion, we can prove that algorithm defense correctly identifies an optimal defense plan. For more complete and rigorous proofs the reader is referred to [16].

C. Solution of the Optimal Power Flow Model

Iteration s of algorithm attack produces a parameterized OPF problem, i.e., OPF($\mathbf{y}^s$), a linear program. If

$$\prod_{j \in J(i)} (1 - y_j) = 0$$

for some i in (5), the corresponding phase angle constraint can be removed; otherwise, the constraint will remain in the model. If

$$\prod_{j \in J(i)} (1 - y_j) = 0$$

for some i in (6), g_i or p_i is fixed at 0; otherwise, they can change within the lower and upper bounds. OPF($\mathbf{y}^s$) differs from OPF($\mathbf{y}^{s-1}$) only in the number of constraints of type (5) and in the bounds of the g_i and p_i variables; therefore, the solution to OPF($\mathbf{y}^{s-1}$) is still dual feasible to OPF($\mathbf{y}^s$). Instead of solving it from scratch every time, we use the dual simplex method starting from the optimal basis to OPF($\mathbf{y}^{s-1}$) to solve OPF($\mathbf{y}^s$), for $s > 0$.

D. Solution of the Relaxed Problems

Both the relaxed attacker's problem (RAP) and the relaxed defender's problem (RDP) in line 8) of algorithm attack and algorithm defense, respectively, are integer linear programs (ILP). These problems can be solved with a generic ILP solution method such as branch-and-bound. Further computational efficiency can be gained by developing a specialized solution method that exploits the set packing constraints (8)–(11) and (14), (15), and set covering constraints (18), (19) (see [16] for details).

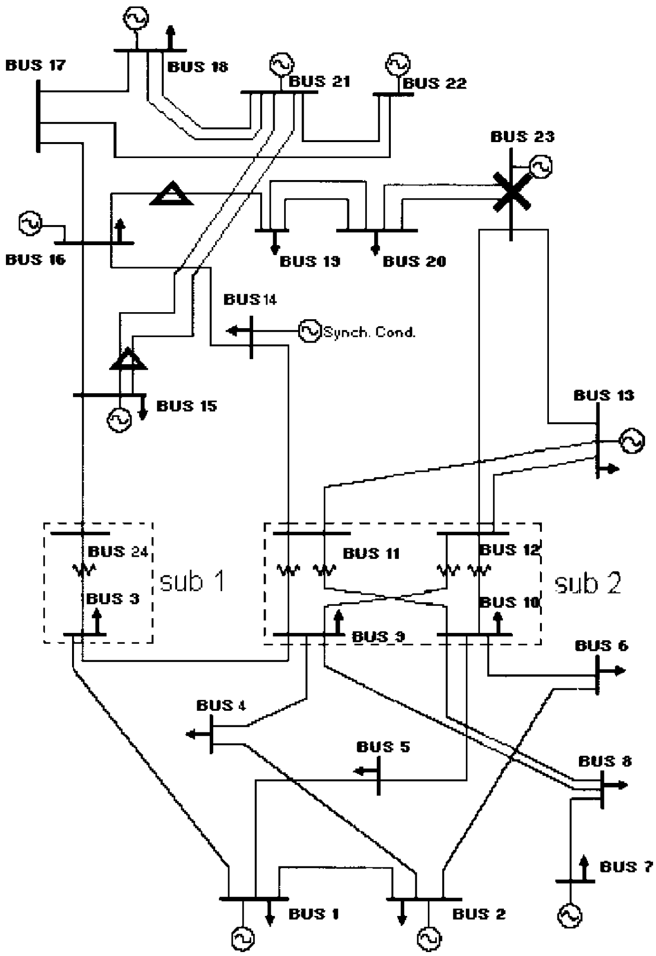

Fig. 1. IEEE reliability test system one area network with defense (delta) and attack (x) points.

E. Implementation and Testing

We implemented the algorithms described in this correspondence in Visual C++, while utilizing the open source code **co**mputational **in**frastructure for **o**perations **r**esearch (COIN-OR) [17]. We used COIN-OR's linear program solver, CLP, to solve the OPF problem repeatedly and incrementally. Test runs were conducted on a 2.4-GHz Windows 2000 machine with 1 GB memory.

All test runs were performed on the IEEE reliability test system (RTS) one area network as shown in Fig. 1 [18]. This hypothetical network is small compared to a national power grid where there are tens of thousands of substations, buses, transmission lines, and generators. Many researchers have reported their results by using this small hypothetical network, which is described in detail in [18]. The economic cost of unmet demand is \$1000/MWH. The resources required for the attacker to disable a line, bus, and substation, are 1, 2, and 3 units, respectively. One unit of resource may include a combination of manpower, equipment, and money. To defend a particular network element, the defender will need the same number of resources as the attacker, although the actual type of resources may differ from that of the attacker. Every network component is both attackable and defendable.

We assume that the resource budget for both the attacker and the defender is two units. The solution process is summarized in Table I. The second and third columns are defense and attack plans, respectively; the fourth column is the total cost of power generation and unmet demand

TABLE I
SOLUTION OF A NETWORK DEFENSE PROBLEM

Iteration	Defened Elements	Attacked Elements	Total Cost ($)
1		Lines 15-21, 16-17	346,678
2	Line 15-21	Lines 16-19, 20-23	341,075
3	Lines 15-21, 16-19	Bus 23	236,467

for the defender. There is no defense in the first iteration, and attack plan 1 is to disable lines 15–21 (between buses 15 and 21) and 16–17, inflicting a total cost of \$346,678 to the defender. In the second iteration, the defender covers lines 15–21 while attack plan 2 is to interdict lines 16–19 and 20–23. In the third iteration, the defender covers lines 16–19 in addition to lines 15–21, thus, interrupting both attack plans 1 and 2; attack plan 3 is to attack bus 23. With only two units of resource, the defender is unable to cover all three attack plans. Consequently, the defender's problem becomes infeasible, and an optimal solution to the trilevel model is found with a total cost of \$236,467. The optimal attack and defense plans are marked in Fig. 1.

We briefly contrast the final defense plans produced by the bilevel and trilevel models in the earlier example to illustrate the benefit of trilevel optimization in network defense. Recall that when bilevel optimization [11] is employed to construct a defense plan, the attacker finds the single most damaging attack plan without any defense (which in the earlier example is to interdict lines 15–21 and 16–17), and then, the defender attempts to harden these network components to thwart this attack plan. In the example, the defender has the resources to defend lines 15–21 and 16–17, and so, the defense plan is to harden these two lines. Under this defense plan, the optimal attack plan is to interdict lines 16–19 and 20–23, and the defender's cost is \$341,075, which is greater than the cost of \$236,467 obtained by using trilevel optimization. The key observation is that the trilevel optimization model produces a superior defense plan because it considers an additional level of interaction between the defender and the attacker, and selects an overall best strategy. The optimal defense plan calls for defending network elements from each of the two most damaging attack plans, not from the most damaging attack plan alone, in the example.

Furthermore, whereas it is difficult to estimate the number of resources required for the attacker to carry out an attack, it is easier to estimate the number of resources required for the defender. Consequently, we believe that the data required to support a trilevel model is not much harder to obtain than that of a bilevel model. More importantly, the trilevel model allows the defender to evaluate the impact of varying the defense resource budget by doing sensitivity analysis that cannot be formally done with a bilevel optimization alone.

To solve the defense problem on large networks, the algorithm as described earlier is prohibitively expensive in terms of computation time. However, with more efficient methods for solving the attacker's problem, including a heuristic algorithm such as the one proposed in [11], computation time could be reduced significantly. The exact solution method described in this correspondence can serve as a verification tool for more practical heuristic algorithms.

IV. CONCLUSION

To our knowledge, this correspondence is the first attempt in applying trilevel optimization to power network defense. The trilevel optimization model captures the interaction between the network defender and attacker in a more systematic way than bilevel optimization, and offers superior defense planning capabilities that ultimately improve system security. The modeling and solution approaches described in this correspondence can be readily applied to other types of infrastructure systems such as oil and gas pipelines, transportation, and telecommunication networks. While the defender's response model will differ for these types of networks, the defense and attack decision models will be very similar.

A number of issues are worthy of future exploration. First, reducing the solution time of the attacker's problem could significantly reduce the overall solution time needed to solve large-scale problems with our proposed algorithm. One possibility is to generate multiple cuts during each iteration of algorithm attack. With more cuts being appended to the attacker's problem, the algorithm should require fewer major iterations to terminate. However, Israeli and Wood found that such a modification is not always guaranteed to produce faster solution times because the attacker's problem takes longer to solve as more and more cuts are appended to it [9], [10].

A second and more promising possibility is to replace algorithm attack with a modified Benders' decomposition. Thanks to the MILP reformulation of the attacker's problem by Salmeron *et al.* [12], Alvarez [19] employed several variants of Benders' decomposition that have drastically reduced the computation time required to solve the attacker's problem to optimality. Incorporating these ideas should immediately translate into shorter solution times for the trilevel problem.

We could extend our model to incorporate the notion of restoration over time. Our current model for the attacker's problem assumes that a terrorist attack will affect all disabled network components in the power grid for roughly the same amount of time. Salmeron *et al.* [12] have relaxed this assumption and extended the model to capture the cost and timing of repairs so that the attacker's goal is to maximize total cost as the system is restored over time.

ACKNOWLEDGMENT

The authors would like to thank J. Salmeron and R. K. Wood (Naval Postgraduate School, Monterrey, CA) for sharing their research work. They are also grateful to three anonymous referees whose comments have helped improve the content of this correspondence.

REFERENCES

[1] National Research Council (NRC) *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington, DC: National Academy Press, 2002.

[2] K. Shimizu and M. Lu, "A global optimization method for the Stackelberg problem with convex functions via problem transformations and concave programming," *IEEE Trans. Syst. Man, Cybern.*, vol. 25, no. 12, pp. 1635–1640, Dec. 1995.

[3] J. F. Bard, *Practical Bilevel Optimization: Algorithms and Applications.* Norwell, MA: Kluwer, 1998.

[4] T. A. Edmunds and J. F. Bard, "Algorithms for nonlinear bilevel mathematical programs," *IEEE Trans. Syst. Man, Cybern.*, vol. 21, no. 1, pp. 83–89, Jan./Feb. 1991.

[5] T. A. Edmunds and J. F. Bard, "An algorithm for the mixed-integer nonlinear bilevel programming problem," *Ann. Oper. Res.*, vol. 32, pp. 149–162, 1992.

[6] J. F. Bard and J. Moore, "A branch and bound algorithm for the bilevel programming problem," *SIAM J. Sci. Statist. Comput.*, vol. 11, pp. 281–292, 1990.

[7] T. A. Edmunds and R. S. Strait, "Evaluating arms control treaty verification regimes: A risk analysis approach," in *Probabilistic Safety Assessment and Management*, G. Apostolakis, Ed. New York: Elsevier, 1991.

[8] Y. Wang, Y. Jiao, and H. Li, "An evolutionary algorithm for solving nonlinear bilevel programming based on a new constraint-handling scheme," *IEEE Trans. Syst. Man, Cybern. C*, vol. 35, no. 2, pp. 221–232, May 2005.

[9] E. Israeli and R. K. Wood, "System interdiction and defense," Oper. Res. Dept., Naval Postgrad. School. Monterey, CA, Draft Rep., Feb. 2002.

[10] E. Israeli and R. Kevin Wood, "Shortest-path network interdiction," *Networks*, vol. 40, pp. 97–111, 2002.

[11] J. Salmeron, R. K. Wood, and R. Baldick, "Optimizing electric grid design under asymmetric threat," Naval Postgrad. School. Monterey, CA, Tech. Rep. NPS-OR-03-002, Feb. 2003.

[12] J. Salmeron, R. K. Wood, and R. Baldick, "Optimizing electric grid design under asymmetric threat II," Naval Postgrad. School. Monterey, CA, Tech. Rep. NPS-OR-04-001, Mar. 2004.

[13] D. P. Bertsekas, *Network Optimization: Continuous and Discrete Models*. Belmont, MA: Athena Scientific, 1998.

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

[15] D. R. Fulkerson and G. C. Harding, "Maximizing the minimum source-sink path subject to a budget constraint," *Math. Program.*, vol. 13, pp. 116–118, 1977.

[16] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Tri-level optimization in power network defense," Lawrence Livermore Nat. Lab., Livermore, CA, Draft UCRL-JRNL-218910, Feb. 2006.

[17] Computational infrastructure for operations research (COIN-OR) [Online]. Available: http://www.coin-or.org/

[18] IEEE Committee Report, "IEEE reliability test system-1996," *IEEE Trans. Power Syst.*, vol. 14, pp. 1010–1020, 1999.

[19] R. E. Alvarez, "Interdicting electrical power grids," M.S. thesis, Naval Postgrad. School, Monterey, CA, 2004.