

Analysis of Electric Grid Security Under Terrorist Threat

Javier Salmeron, Kevin Wood, and Ross Baldick, *Member, IEEE*

Abstract—We describe new analytical techniques to help mitigate the disruptions to electric power grids caused by terrorist attacks. New bilevel mathematical models and algorithms identify critical system components (e.g., transmission lines, generators, transformers) by creating maximally disruptive attack plans for terrorists assumed to have limited offensive resources. We report results for standard reliability test networks to show that the techniques identify critical components with modest computational effort.

Index Terms—Homeland security, interdiction, power flow.

I. INTRODUCTION

ELECTRIC power systems are critical to any country's economy and security. In the United States, the system's vulnerability to physical disruptions from natural disasters and other causes has long been recognized [1]. This vulnerability has increased in recent years because infrastructure has not expanded as quickly as demand has, thereby reducing the system's "cushion" against failed, destroyed, or otherwise unavailable system components [2]. The threat of human attacks on the system has become more serious, too. The Committee on Science and Technology for Countering Terrorism [3] states the problem succinctly: "The nation's electric power systems must clearly be made more resilient to terrorist attack." To help reach this goal, this paper describes new bilevel optimization models and solution techniques for analyzing the security and resilience of electrical power grids against disruptions caused by terrorist attacks. (These techniques could also help analyze a system's susceptibility to natural disasters, but we do not study this issue explicitly.)

We propose techniques to identify critical sets of a power grid's components, e.g., generators, transmission lines, and transformers, by identifying maximally disruptive, coordinated (nearly simultaneous) attacks on a grid, which a terrorist group might undertake. By studying how to attack power grids, we will ultimately understand how to make them less vulnerable. We report results for our techniques applied to reliability-benchmark networks.

We search for optimal attacks, i.e., a set of attacks that causes the largest possible disruption given posited offensive resources.

Manuscript received September 28, 2003. This work was supported by the U.S. Department of Justice, Office of Justice Programs and Office of Domestic Preparedness (2002-GT-R-057), by the Office of Naval Research, and by the Air Force Office of Scientific Research.

J. Salmeron and K. Wood are with the Operations Research Department, Naval Postgraduate School, Monterey, CA 93943-5001 USA.

R. Baldick is with the Department of Electrical Engineering, University of Texas at Austin, Austin, TX, 78712-1084 USA.

Digital Object Identifier 10.1109/TPWRS.2004.825888

By considering the largest possible disruptions, our proposed protection plans will be appropriately conservative. Actual terrorist "resources" will always be uncertain, so our techniques must be fast enough to quickly analyze a wide range of probable scenarios. We concern ourselves only with physical attacks on the power grid and neglect the issue of "cyber-attacks" on the controlling Supervisory Control and Data Acquisition (SCADA) infrastructure. The implicit assumption is that the SCADA infrastructure has been hardened. A discussion of the issues for reliable communication in this context is presented in [4].

The rest of this paper is organized as follows: Section II describes the mathematical formulation of our models and describes procedures to solve them. Section III reports results of those models and algorithms applied to two IEEE reliability test systems. Section IV provides conclusions and points out directions for future research.

II. APPROACH

A. Overview

Our approach to identifying critical system components first develops a network-interdiction model [5] to represent the optimal-attack problem that a terrorist group might face. This model is a max-min (Mm) problem

$$\begin{aligned} (\text{Mm}) \quad & \max_{\delta \in \Delta} \min_{\mathbf{p}} \mathbf{c}^T \mathbf{p} \\ & \text{s.t. } \mathbf{g}(\mathbf{p}, \delta) \leq \mathbf{b} \\ & \mathbf{p} \geq \mathbf{0}. \end{aligned}$$

An interdiction plan is represented by the binary vector δ , whose k th entry δ_k is 1 if component k of the system is attacked and is 0 otherwise. For a given plan, the inner problem is an optimal power-flow model [6, p. 514] that minimizes generation costs plus the penalty associated with unmet demand, together denoted by $\mathbf{c}^T \mathbf{p}$. Here, \mathbf{p} represents power flows, generation outputs, phase angles and "unmet demand," i.e., the amount of load shed; \mathbf{c} represents linearized generation costs, and the costs of unmet demand. The outer maximization chooses the most disruptive, resource-constrained interdiction plan $\delta \in \Delta$, where Δ is a discrete set representing attacks that a terrorist group might be able to carry out. In this model, \mathbf{g} corresponds to a set of functions that are nonlinear in (\mathbf{p}, δ) . The inner problem involves a simplified optimal power-flow model, with constraint functions $\mathbf{g}(\mathbf{p}, \delta)$ that are, however, linear in \mathbf{p} for a fixed $\delta = \hat{\delta}$. The model extends easily to handle the cost of repairs.

For simplicity, we first describe a power-flow model that minimizes the instantaneous cost of system operation, including unmet demand, measured in \$/h. Power disruptions resulting from cascading outages immediately after attack are ignored, so we are actually measuring cost after initial restoration of outaged but undamaged equipment. Later in the paper we consider the cost of unmet demand after the initial restoration, recognizing that this cost will be changing over time as damaged equipment is repaired following an attack.

The remainder of this section explains the basic mathematical models and algorithms our research has developed. We first summarize our DC approximation of the AC power-flow model, and then show how to incorporate that approximation as part of an interdiction model. Finally, we introduce a heuristic algorithm for solving the combined power-flow and interdiction model.

B. Power-Flow Model

We approximate active power flows with a DC model, denoted DC-OPF (DC-Optimal Power Flow), which neglects reactive power effects and nonlinear losses. This approximation is normally acceptable in the context of long-term, “coarse-grained” security analysis [6, p. 419]. In the eventual min-max interdiction model, DC-OPF will be modified through a set of interdiction variables.

Indices and Index Sets:

$i \in \mathbf{I}$	buses;
$g \in \mathbf{G}$	generating units;
$l \in \mathbf{L}$	transmission lines;
$c \in \mathbf{C}$	consumer sectors;
$s \in \mathbf{S}$	substations;
$i \in \mathbf{I}_s$	buses at substation s ;
$g \in \mathbf{G}_i$	generating units connected to bus i ;
$l \in \mathbf{L}_i^{Bus}$	lines connected to bus i ;
$l \in \mathbf{L}_s^{Sub}$	lines connected to substation s (including transformers, which are represented by lines);
$l' \in \mathbf{L}_l^{Par}$	lines $l' \neq l$ running in parallel to line l .

Parameters (units):

$o(l), d(l)$	origin and destination buses of line l ; more than one line with the same $o(l), d(l)$ may exist;
$i(g)$	bus for generator g , i.e., $g \in \mathbf{G}_{i(g)}$;
d_{ic}	load of consumer sector c at bus i (MW);
\bar{P}_l^{Line}	transmission capacity for line l (MW);
\bar{P}_g^{Gen}	maximum output from generator g (MW);
r_l, x_l	resistance, reactance of line l (Ω). (We assume $x_l \gg r_l$); series susceptance is $B_l = x_l / (r_l^2 + x_l^2)$;
h_g	generation cost for unit g (\$/MWh);
f_{ic}	load-shedding cost for customer sector c at bus i (\$/MWh).

Decision Variables (Units):

P_g^{Gen}	generation from unit g (MW);
P_l^{Line}	power flow on line l (MW);
S_{ic}	load shed by customer sector c at bus i (MW);
θ_i	phase angle at bus i (radians).

Formulation of DC-OPF: (Remark: All units above are converted into per-unit values for a base load of 100 MW.)

$$\min_{P^{Gen}, P^{Line}, S, \theta} \sum_g h_g P_g^{Gen} + \sum_i \sum_c f_{ic} S_{ic} \quad (\text{DC.0})$$

subject to:

$$P_l^{Line} = B_l(\theta_{o(l)} - \theta_{d(l)}) \quad \forall l \quad (\text{DC.1})$$

$$\sum_g P_g^{Gen} - \sum_{l|o(l)=i} P_l^{Line} + \sum_{l|d(l)=i} P_l^{Line} = \sum_c (d_{ic} - S_{ic}) \quad \forall i \quad (\text{DC.2})$$

$$-\bar{P}_l^{Line} \leq P_l^{Line} \leq \bar{P}_l^{Line} \quad \forall l \quad (\text{DC.3})$$

$$0 \leq P_g^{Gen} \leq \bar{P}_g^{Gen} \quad \forall g \quad (\text{DC.4})$$

$$0 \leq S_{ic} \leq d_{ic} \quad \forall i, c. \quad (\text{DC.5})$$

The objective of DC-OPF (DC.0) is to minimize generating plus shedding costs measured in \$/h. Constraints (DC.1) approximate active power flows on the lines. Constraints (DC.2) maintain power balance at the buses. Constraints (DC.3) and (DC.4) set maximum line power flows and generating-unit outputs. Minimum power outputs are set to zero for all generating units for simplicity here, but extensions to nonzero minima are straight-forward. Constraints (DC.5) state that load shedding cannot exceed demand. A version of DC-OPF will be a subproblem of the interdiction model described next.

C. Interdiction Model

“The interdictor” in our model, a group of terrorists, will make a coordinated set of resource-constrained interdictions (attacks) on the power grid. We make the following assumptions on the effect of each interdiction.

- Line interdiction: All lines running physically in parallel at the point of an attack are opened. (Typically, these lines are mounted on the same towers, and an attack on one is an attack on all.)
- Transformer interdiction: The line representing the transformer is opened.
- Generator interdiction: The generator is disconnected from the grid.
- Bus interdiction: All lines, generation, and load connected to the bus are disconnected.
- Substation interdiction: All buses at the substation are disconnected; this triggers the corresponding bus-interdiction effects just described.

Terrorist resource constraints can accommodate information from intelligence sources, whether it is specific as we shall assume, or generic, such as “any three attacks might happen.” For demonstration purposes, we model this feature through a simple knapsack constraint.

Additional Sets and Parameters Required:

$\mathbf{G}^* \subseteq \mathbf{G}$, $\mathbf{L}^* \subseteq \mathbf{L}$, $\mathbf{I}^* \subseteq \mathbf{I}$, $\mathbf{S}^* \subseteq \mathbf{S}$ interdictable generators, lines, buses, and substations, respectively. These are “interdictable components.”

$M_g^{Gen}, M_l^{Line}, M_i^{Bus}, M_s^{Sub}$

resource required to interdict generator g , line l , bus i , and substation s , respectively.

 M

total interdiction resource available to terrorists.

Interdiction Variables:

 $\delta_g^{Gen}, \delta_l^{Line}, \delta_i^{Bus}, \delta_s^{Sub}$

binary variables that take the value 1 if generator g , line l , bus i or substation s , respectively, are interdicted, and are 0 otherwise.

Formulation of I-DC-OPF:

$$\max_{\delta^{Gen}, \delta^{Line}, \delta^{Bus}, \delta^{Sub}} \gamma(\delta^{Gen}, \delta^{Line}, \delta^{Bus}, \delta^{Sub}) \quad (I.0)$$

subject to:

$$\sum_{g \in G^*} M_g^{Gen} + \sum_{l \in L^*} M_l^{Line} \delta_l^{Line} + \sum_{i \in I^*} M_i^{Bus} \delta_i^{Bus} + \sum_{s \in S^*} M_s^{Sub} \delta_s^{Sub} \leq M. \quad (I.1)$$

All variables δ are binary, but are fixed to 0 if not associated with G^* , L^* , I^* , or S^* . (I.2)

And where

$$\gamma(\delta^{Gen}, \delta^{Line}, \delta^{Bus}, \delta^{Sub}) = \min_{P^{Gen}, P^{Line}, S, \theta} \sum_g h_g P_g^{Gen} + \sum_i \sum_c f_{ic} S_{ic} \quad (IDC.0)$$

subject to:

(Note: Nonlinear constraints in δ are used for conciseness below; linear replacements are straightforward.)

$$P_l^{Line} = B_l(\theta_{o(l)} - \theta_{d(l)}) (1 - \delta_l^{Line}) (1 - \delta_{o(l)}^{Bus}) (1 - \delta_{d(l)}^{Bus}) \prod_{s|l \in L_s^{Sub}} (1 - \delta_s^{Sub}) \prod_{l'|l \in L_l^{Par}} (1 - \delta_{l'}^{Line}) \quad \forall l \quad (IDC.1)$$

$$\sum_g P_g^{Gen} - \sum_{l|o(l)=i} P_l^{Line} + \sum_{l|d(l)=i} P_l^{Line} = \sum_c (d_{ic} - S_{ic}) \quad \forall i \quad (IDC.2)$$

$$\begin{aligned} & - \bar{P}_l^{Line} (1 - \delta_l^{Line}) (1 - \delta_{o(l)}^{Bus}) (1 - \delta_{d(l)}^{Bus}) \\ & \prod_{s|l \in L_s^{Sub}} (1 - \delta_s^{Sub}) \prod_{l'|l \in L_l^{Par}} (1 - \delta_{l'}^{Line}) \\ & \leq P_l^{Line} \leq \bar{P}_l^{Line} (1 - \delta_l^{Line}) (1 - \delta_{o(l)}^{Bus}) (1 - \delta_{d(l)}^{Bus}) \\ & \prod_{s|l \in L_s^{Sub}} (1 - \delta_s^{Sub}) \prod_{l'|l \in L_l^{Par}} (1 - \delta_{l'}^{Line}) \quad \forall l \quad (IDC.3) \end{aligned}$$

$$0 \leq P_g^{Gen} \leq (1 - \delta_{i(g)}^{Bus}) (1 - \delta_g^{Gen}) \bar{P}_g^{Gen} \quad \forall g \quad (IDC.4)$$

$$0 \leq S_{ic} \leq d_{ic} \quad \forall i, c. \quad (IDC.5)$$

I-DC-OPF maximizes generation costs plus load-shedding costs, which we refer to as “disruption.” (A more intuitive

definition would also subtract nominal generation cost, but this is a constant factor we shall ignore.) Disruption is evaluated through the inner minimization problem that consists of the power-flow model DC-OPF with interdicted components removed. At the outer level, (I.1) reflects the terrorists’ options to interdict different combinations of components in the grid without exceeding their resources. Restrictions (I.2) define terrorist actions as binary variables and ensure noninterdiction of certain grid components (e.g., hardened components).

Equations (IDC.1)–(IDC.5) are analogs of (DC.1)–(DC.5). Here, however, the components that have been interdicted, directly or indirectly, are removed from the equations through the binary interdiction variables. For example, if some line l is connected to an interdicted substation s , i.e., $\delta_s^{Sub} = 1$, then constraints (IDC.1) and (IDC.3) for line l yield $P_l^{Line} = 0$.

The computational challenge of I-DC-OPF stems from the max-min structure of the problem. The optimal objective value of the linearized version of the inner minimization, as a function of continuous δ , is convex. Hence, I-DC-OPF involves the maximization of a convex function, which is usually a difficult task.

D. Interdiction Algorithm

Future research will investigate the conversion of I-DC-OPF to a linear mixed-integer program which could be solved directly or through decomposition [7]. At this juncture, we have devised a decomposition-based heuristic to obtain acceptable interdiction plans (for the terrorists), although not necessarily optimal ones.

The algorithm begins by solving DC-OPF, “the subproblem,” assuming no attacks. The result is an optimal power flow for normal operations, a flow that should minimize generation costs without shedding any load. The power-flow pattern is used to assign relative values (see below) to all the components of the power grid. Next, the algorithm solves a “master problem” to identify an interdiction plan that maximizes the estimated value of interdicted assets while not exceeding available interdiction resources. With this plan, the constraints of DC-OPF are modified and the new subproblem solved. The result is a power flow that minimizes generation costs plus the penalty associated with load shedding, given the new interdictions. Typically, some load will be shed in the new solution since valuable assets have been removed from the grid.

The process continues by finding alternative interdiction plans and by evaluating load shedding for each of them. This algorithm may be viewed as a heuristic version of Benders decomposition [7] to solve the bilevel program, I-DC-OPF. The master problem incorporates super-valid inequalities (constraints that eliminate some solutions, but not all optimal ones, unless an optimal solution has already been identified [5]) to avoid repeating solutions. We next provide details of the two models required in the decomposition algorithm.

Subproblem: DC-OPF for a Specific Interdiction Plan. Assume that at iteration t of our algorithm, a specific interdiction plan $\hat{\delta}^t = (\hat{\delta}^{Gen,t}, \hat{\delta}^{Line,t}, \hat{\delta}^{Bus,t}, \hat{\delta}^{Sub,t})$ is given. The power-flow model DC-OPF($\hat{\delta}^t$), (IDC.0)–(IDC.5), forms the

subproblem and its solution yields objective value $\gamma(\hat{\delta}^t) = \gamma(\hat{\delta}^{Gen,t}, \hat{\delta}^{Line,t}, \hat{\delta}^{Bus,t}, \hat{\delta}^{Sub,t})$ along with power flows, generation and unmet demand, which are represented by $\hat{\mathbf{P}}^t = (\hat{\mathbf{P}}^{Line,t}, \hat{\mathbf{P}}^{Gen,t}, \hat{\mathbf{S}}^t, \hat{\boldsymbol{\theta}}^t)$.

Value estimates:

The solution $\hat{\mathbf{P}}^t = (\hat{\mathbf{P}}^{Line,t}, \hat{\mathbf{P}}^{Gen,t}, \hat{\mathbf{S}}^t, \hat{\boldsymbol{\theta}}^t)$, provided by DC-OPF $(\hat{\delta}^t)$, serves to construct estimates of the attractiveness or “value” of components for further interdiction. To determine these estimates, we define a set of parameters which represent, essentially, estimated coefficients for a “Benders cut” that will be added to the master problem. (In this heuristic, a cut, or a set of aggregated cuts, is added to the master-problem objective function rather than being added as a constraint; the super-valid inequalities take the place of cuts that build up from iteration to iteration.) We first compute

$$F_i^{Out,t} = \sum_{\substack{l|o(l)=i \\ \wedge \hat{P}_l^{Line,t} > 0}} \hat{P}_l^{Line,t} + \sum_{\substack{l|d(l)=i \\ \wedge \hat{P}_l^{Line,t} < 0}} |\hat{P}_l^{Line,t}|, \text{ flow out of bus } i$$

$$F_i^{Met,t} = \sum_c (d_{ic} - \hat{S}_{ic}^t), \text{ load supplied to bus } i.$$

These totals are then used to compute:

$$V_g^{Gen,t} = w^{Gen} \hat{P}_g^{Gen,t} \quad \forall g$$

$$V_l^{Line,t} = w^{Line} \left(|\hat{P}_l^{Line,t}| + \sum_{v \in L_l^{Par}} |\hat{P}_v^{Line,t}| \right)$$

$$V_i^{Bus,t} = w^{Bus} (F_i^{Met,t} + F_i^{Out,t}) \quad \forall i$$

$$V_s^{Sub,t} = w^{Sub} \sum_{l|l \in L_s} |\hat{P}_l^{Line,t}| \quad \forall s.$$

The weights w^{Gen} , w^{Bus} , w^{Line} and w^{Sub} are specified by the user to reflect the relative importance of each type of component. Experience indicates that the algorithm is more efficient when using weights that provide higher incentives for attacks on buses and substations than on individual lines and generators, e.g., $w^{Gen} = 2$, $w^{Bus} = 5$, $w^{Line} = 1$, $w^{Sub} = 5$.

We have found that the following modifications to the definition of value are useful, too: (a) The value for a component defined above is divided by the amount of resource required to interdict that component, to reflect value per unit of effort, (b) a minimum value $\varepsilon > 0$ is always enforced, for reasons explained below, and (c) a running average of component values is used rather than just the current iteration’s values. Without the running average, if the power flow through a currently interdicted component is null, the asset will be unattractive in the immediately following iteration. This is counter-intuitive. (The running average could be computed in a variety of ways, but we use a simple arithmetic average over all iterations.)

Master Problem: Finding a Valuable Interdiction Plan:

Assume that a set of estimated values for each component of the grid, $\mathbf{V}^t = (\mathbf{V}^{Gen,t}, \mathbf{V}^{Line,t}, \mathbf{V}^{Bus,t}, \mathbf{V}^{Sub,t})$, has been calculated at iteration t ; and, define the vector of previously generated interdiction plans $\hat{\Delta}^t = (\hat{\delta}^1, \dots, \hat{\delta}^t)$. The interdiction master problem is then:

$$\text{MP}(\mathbf{V}^t, \hat{\Delta}^t): \max_{\substack{\delta^{Gen}, \delta^{Line}, \\ \delta^{Bus}, \delta^{Sub}}} \sum_{g \in \Gamma^*} V_g^{Gen,t} \delta_g^{Gen} + \sum_{l \in L^*} V_l^{Line,t} \delta_l^{Line} + \sum_{i \in I^*} V_i^{Gen,t} \delta_i^{Gen} + \sum_{s \in S^*} V_s^{Sub,t} \delta_s^{Sub}$$

subject to:

$$\text{Eqs. (I.1)–(I.2) replacing } \boldsymbol{\delta} \text{ with } \boldsymbol{\delta}' \quad (\text{MP.1)–(MP.2)}$$

$$\delta_g^{Gen} + \delta_i^{Bus} \leq 1 \quad \forall g \in \mathbf{G}_i^*, i \in \mathbf{I}^* \quad (\text{MP.3})$$

$$\delta_l^{Line} + \delta_i^{Bus} \leq 1 \quad \forall l \in \mathbf{L}_i \cap \mathbf{L}^*, i \in \mathbf{I}^* \quad (\text{MP.4})$$

$$\delta_l^{Line} + \delta_{l'}^{Line} \leq 1 \quad \forall l' \in \mathbf{L}_l^{Par} \cap \mathbf{L}^*, l \in \mathbf{L}^* \quad (\text{MP.5})$$

$$\delta_i^{Bus} + \delta_s^{Sub} \leq 1 \quad \forall i \in \mathbf{I}_s \cap \mathbf{I}^*, s \in \mathbf{S}^* \quad (\text{MP.6})$$

$$\delta_l^{Line} + \delta_s^{Sub} \leq 1 \quad \forall l \in \mathbf{L}_s \cap \mathbf{L}^*, s \in \mathbf{S}^* \quad (\text{MP.7})$$

$$\sum_{\substack{g \in \mathbf{G}^* | \\ \hat{\delta}_g^{Gen,t'} = 1}} (\hat{\delta}_g^{Gen,t'} - \delta_g^{Gen}) + \sum_{\substack{l \in \mathbf{L}^* | \\ \hat{\delta}_l^{Line,t'} = 1}} (\hat{\delta}_l^{Line,t'} - \delta_l^{Line}) + \sum_{\substack{i \in \mathbf{I}^* | \\ \hat{\delta}_i^{Bus,t'} = 1}} (\hat{\delta}_i^{Bus,t'} - \delta_i^{Bus}) + \sum_{\substack{s \in \mathbf{S}^* | \\ \hat{\delta}_s^{Sub,t'} = 1}} (\hat{\delta}_s^{Sub,t'} - \delta_s^{Sub}) \geq 1, \quad \forall t' \leq t. \quad (\text{MP.8})$$

The solution to $\text{MP}(\mathbf{V}^t, \hat{\Delta}^t)$ maximizes the estimated value of interdicted grid components. Constraints (MP.3)–(MP.7) serve the following purposes, respectively: Interdict a generator or the bus it is connected to, but not both; interdict a line or the bus it is connected to, but not both; if two lines run in parallel, interdict one line or the other, but not both (in the latter case, the interdiction of both lines simultaneously is actually represented by a single variable); interdict a bus or the substation it belongs to, but not both; and, interdict a line or the substation it is connected to, but not both. These constraints incorporate structural information about the system that the linear objective function cannot. Specifically, the constraints ensure that no system components are interdicted that are indirectly interdicted by attacks on other components. Finally, constraints (MP.8) ensure that the interdiction plan chosen at the incumbent iteration is different from all plans from previous iterations. These constraints assume that the optimal objective of the master problem always consumes a maximal amount of resource (i.e., insufficient resource remains to interdict any additional components). This is ensured by requiring every component maintain a minimum allowable value, $\varepsilon > 0$.

Let $\hat{\delta}^{t+1} = (\hat{\delta}^{Gen,t+1}, \hat{\delta}^{Line,t+1}, \hat{\delta}^{Bus,t+1}, \hat{\delta}^{Sub,t+1})$ de-

note the solution to $MP(\mathbf{V}^t, \hat{\Delta}^t)$. The vector $\hat{\delta}^{t+1}$ is used in the subproblem to start a new iteration of the algorithm described next.

I-ALG: Interdiction Algorithm:

Input: Grid data; Interdiction data; T (iteration limit).

Output: $\hat{\delta}^*$ is a feasible interdiction plan causing a disruption with cost γ^* . If the algorithm exits because $MP(\mathbf{V}^t, \hat{\Delta}^t)$ is infeasible, then all feasible solutions have been enumerated, and $\hat{\delta}^*$ is therefore optimal.

Initialization:

- Set $\hat{\delta}^1 \equiv (\hat{\delta}^{Gen,1}, \hat{\delta}^{Line,1}, \hat{\delta}^{Bus,1}, \hat{\delta}^{Sub,1}) \leftarrow (0, 0, 0, 0)$ (initial attack plan).
- Set $\hat{\delta}^* \leftarrow \hat{\delta}^1$ (best plan so far) and $\hat{\Delta}^1 \leftarrow \{\hat{\delta}^1\}$.
- Set $\gamma^* \leftarrow 0$ (cost of the best plan so far).
- Set $t \leftarrow 1$.

Subproblem:

- Solve DC-OPF($\hat{\delta}^t$) for objective value $\gamma(\hat{\delta}^t)$ and solution $\hat{\mathbf{P}}^t \equiv (\hat{\mathbf{P}}^{Line,t}, \hat{\mathbf{P}}^{Gen,t}, \hat{\mathbf{S}}^t, \hat{\boldsymbol{\theta}}^t)$.
- If $\gamma(\hat{\delta}^t) > \gamma^*$ then $\gamma^* \leftarrow \gamma(\hat{\delta}^t)$, and $\hat{\delta}^* \leftarrow \hat{\delta}^t$.
- If $t = T$, then Print ($\hat{\delta}^*, \gamma^*$) and halt.

Master problem:

- Compute “value estimates” using $\hat{\mathbf{P}}^{t'}, t' = 1 \dots, t$
- $$\mathbf{V}^t \equiv (\mathbf{V}^{Gen,t}, \mathbf{V}^{Line,t}, \mathbf{V}^{Bus,t}, \mathbf{V}^{Sub,t})$$
- $$= \frac{1}{t} \sum_{t'=1}^t (\mathbf{V}^{Gen,t'}, \mathbf{V}^{Line,t'}, \mathbf{V}^{Bus,t'}, \mathbf{V}^{Sub,t'}).$$
- Solve $MP(\mathbf{V}^t, \hat{\Delta}^t)$ for $\hat{\delta}^{t+1}$.
 - If $MP(\mathbf{V}^t, \hat{\Delta}^t)$ is infeasible, then Print ($\hat{\delta}^*, \gamma^*$) and halt.
 - Update $\hat{\Delta}^{t+1} \leftarrow \hat{\Delta}^t \cup \{\hat{\delta}^{t+1}\}$.
 - Set $t \leftarrow t + 1$.
 - Return to Subproblem.

III. RESULTS

A. Implementation

We have applied algorithm I-ALG to two test networks drawn from the 1996 IEEE Reliability Test System (RTS) [8] and [9]. Tests are carried out on a 1 GHz personal computer with 1 GB of RAM. The model and algorithm are implemented in GAMS, which is an algebraic modeling language for numerical optimization problems. GAMS enables easy generation and manipulation of the subproblems and master problems, which are actually solved with CPLEX, a highly efficient linear- and integer-programming code [10].

We restrict the number of iterations to $T = 500$ for all problems to limit computation time. For fixed M , the most difficult problems require about 200 seconds, excluding model-generation overhead. About 90% of the time is spent solving the master problem.

Our model is driven by generation and shedding costs. In the examples, we assume a fixed per-unit penalty for unmet load so only a single customer class is represented. Shedding costs are much higher than generation costs, so we present results only in terms of load shed.

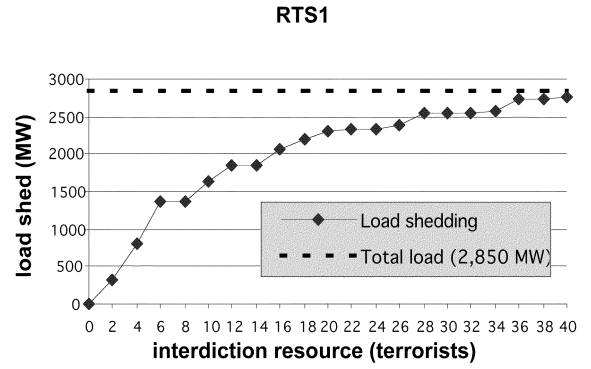


Fig. 1. Load shedding for RTS1 as a function of interdiction resource M (number of terrorists). Total load is 2850 MW.

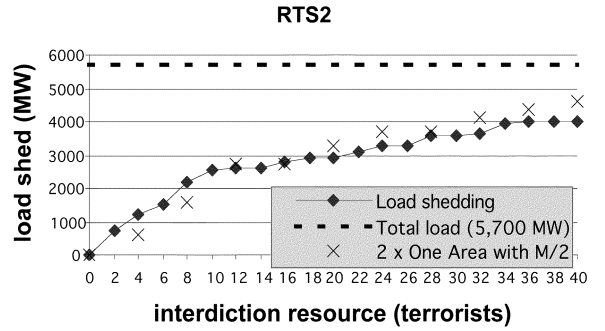


Fig. 2. Load shedding for RTS2 as a function of interdiction resource M . Total load is 5700 MW. Results are compared to twice the load shed in RTS1 with interdiction resource at $(1/2)M$.

B. Test-Case Description

The RTS examples are not intended to represent particular systems but, rather, general reference grids that contain most of the technologies and configurations found in typical power grids [8]. The cases we study, One Area RTS-96 (“RTS1”) and Two Area RTS-96 (“RTS2”), are described in detail in [8]. RTS2 duplicates RTS1 and adds three interconnections between the duplicated areas.

Interdiction data must be defined in addition to grid data. For these examples, we suppose that the terrorists’ resources are quantified as a given number of people: One person is required to interdict any overhead single line or physically parallel overhead lines, although underground cables cannot be interdicted; transformers (which are represented by lines) require two people; three people are required to interdict any bus or substation; but generators are well-protected and cannot be attacked directly (although they can be disconnected from the grid by attacking the associated bus).

C. Interdiction Plans

Figs. 1 and 2 display the amount of load shed in each grid when total interdiction resource M varies from zero to forty. The amount of load shed is a monotonically nondecreasing function of M , with a tendency to concavity as M increases; this is to be expected.

In RTS1, any case with $M \geq 28$ results in at least 90% of the total load being shed. For the most part, RTS2 is more difficult to interdict when compared to the RTS1 for twice the amount of interdiction resource. For example, 2311 MW are shed in

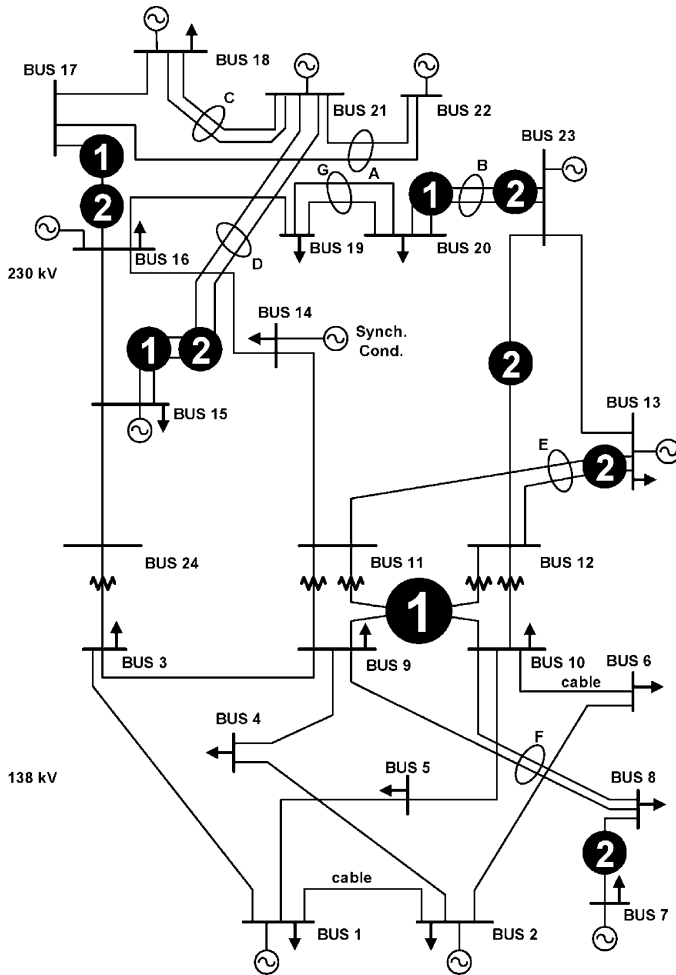


Fig. 3. Two interdiction plans (depicted as ① and ②) for RTS1 using $M = 6$. Total load is 2850 MW. Plan 1 sheds 1258 MW and plan 2 sheds 1373 MW. The large “①” indicates that the four transformers and buses in the substation are interdicted.

RTS1 when $M = 20$, whereas only 4000 MW are shed in RTS2 when $M = 40$. The interconnecting lines may be playing an important role in decreasing the impact of the attacks. However, we observe the opposite effect when M is small. For instance, there is little disruption that two terrorists can cause in RTS1 but four terrorists cause proportionately more disruption in RTS2 because they can, apparently, focus on the “weak links” of a single area. (We caution that these observations apply to this particular system and do not necessarily generalize.)

Determining likelihoods for each of these scenarios and incorporating them into a more elaborate stochastic program (e.g., [11] and [12]) is possible, but is beyond the scope of this paper. It is instructive to compare two specific scenarios, however, and we do this next for RTS1.

Two near-best plans for RTS1, for $M = 6$, are depicted in Fig. 3. “Plan 1” attacks the substation and three selected lines, shedding 1258 MW (44.1% of the total load), and “Plan 2” attacks six selected transmission lines, shedding 1373 MW (48.2%). Plan 2 sheds more instantaneous load, but we must ultimately consider the total amount of unsupplied energy while the effects of the attack last. The 115 MW of additional short-term load shedding in Plan 2 may be negligible compared to the long-term disruption caused by destroying the four transformers

in Plan 1, since it is unlikely those transformers could be replaced or repaired quickly. We investigate this issue more formally in Section III-D.

We now consider RTS2. Fig. 4 depicts the most disruptive attack plan found to affect instantaneous load shedding for $M = 12$. Here, 2,516 MW (44.1% of total load) is shed. Thus, doubling interdiction resource from $M = 6$ in RTS1 to $M = 12$ here yields not quite twice the disruption ($2,516 < 2 \times 1,373$); compare Fig. 2. The RTS2 plan partially duplicates Plan 1 for RTS1, which seems sensible since the RTS2 duplicates RTS1’s structure. Note, however, that one line connecting the duplicated areas is also interdicted.

D. Results Including Restoration Over Time

A time-phased version of I-DC-OPF is created by using interdiction constructs to couple instances of DC-OPF, one for each system state that represents a stage or “time period” of system repair. In outline, the model is

$$\begin{aligned}
 (\text{Mm}') \quad & \max_{\delta \in \Delta} \min_{\mathbf{p}_t, \tau=1, \dots, T} \sum_{\tau=1}^T \alpha_\tau \mathbf{c}^T \mathbf{p}_\tau \\
 \text{s.t.} \quad & \mathbf{g}_\tau(\mathbf{p}_\tau, \delta) \leq \mathbf{b}, \tau = 1, \dots, T \\
 & \mathbf{p}_\tau \geq \mathbf{0}, \tau = 1, \dots, T.
 \end{aligned}$$

Model (Mm') extends (Mm) to incorporate the hourly cost of power flow, $\mathbf{c}^T \mathbf{p}_\tau$, in each time period τ , multiplied by the period’s duration in hours, α_τ . The model could be extended to incorporate “sub-time periods” through load duration curves, but we have not yet explored this possibility; all loads are held constant over time. The conversion of I-ALG to solve (Mm') is straightforward.

Data for outage durations (i.e., repair or replacement times) are based loosely on [8]. Outage duration for transformers is 768 hours. For overhead lines, instead of the 10 or 11 hours used in [8], we are more conservative and assume 72 hours. This is justified because (a) we expect more damage to result from the intentional destruction of a line—this would probably involve the destruction of one or more towers [13]—than the average time needed to repair damage from common natural causes such as lightning, and (b) if n lines and other grid elements are attacked, total repair time may be longer if fewer than n repair teams are available. We also assume that a large substation requires 768 hours for repair, but buses, for which [8] provides no data, require 360 hours. These data are summarized in Table I.

Table II presents results for each time period for attack Plans 1 and 2 in RTS1 ($M = 6$). Immediately after the attack, Plan 2 sheds more power (1373 MW) than Plan 1 (1258 MW). But, with power restoration over time factored in, Plan 1 causes more disruption because repairs take longer and more total energy is shed.

As expected, the revised model incorporating outage durations identifies a more disruptive plan, Plan 3 (see Table II and Fig. 5) in terms of total energy shed, compared to Plans 1 and 2. Plan 3 interdicts the large substation, a transformer in the other substation (but without disconnecting the load associated with the substation on the left) and one line.

E. Identifying Candidate Components for Hardening

Our ultimate goal is to identify grid components which, when “hardened,” yield the best improvement in system security. A

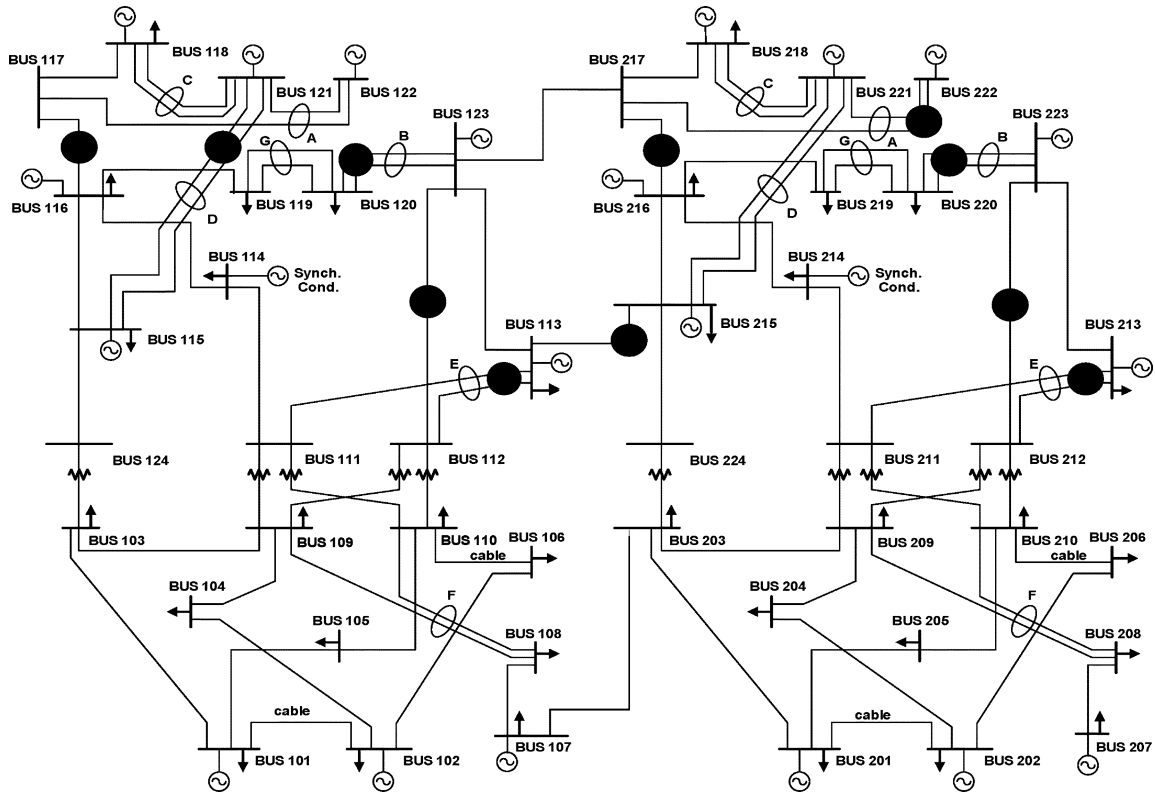


Fig. 4. An interdiction plan (●) for RTS2 using $M = 12$. Total load is 5700 MW. This plan sheds 2516 MW.

TABLE I
REPAIR AND INTERDICTION DATA FOR GRID COMPONENTS

Grid Component	Inter-dictable	Resources M (# of terrorists)	Outage Duration (h)
Lines (overhead)	YES	1	72
Lines (undergnd)	NO	N/A	N/A
Transformers	YES	2	768
Buses	YES	3	360
Generators	NO	N/A	N/A
Substations	YES	3	768

TABLE II
ENERGY SHED UNTIL SYSTEM REPAIR IS COMPLETE, FOR THREE ATTACK PLANS FOR RTS1. PLAN 3 IS SUPERIOR BECAUSE IT WAS GENERATED THROUGH (Mm') WHICH EXPLICITLY MODELS POWER RESTORATION OVER TIME

Plan	Time Period	Power Shed (MW)	Energy Shed (MWh)
1	0-72 h	1,258	90,576
	72-768 h	426	296,496
			Total: 387,072
2	0-72 h	1,373	98,856
3	0-72 h	902	64,944
	72-768 h	708	492,768
			Total: 557,712

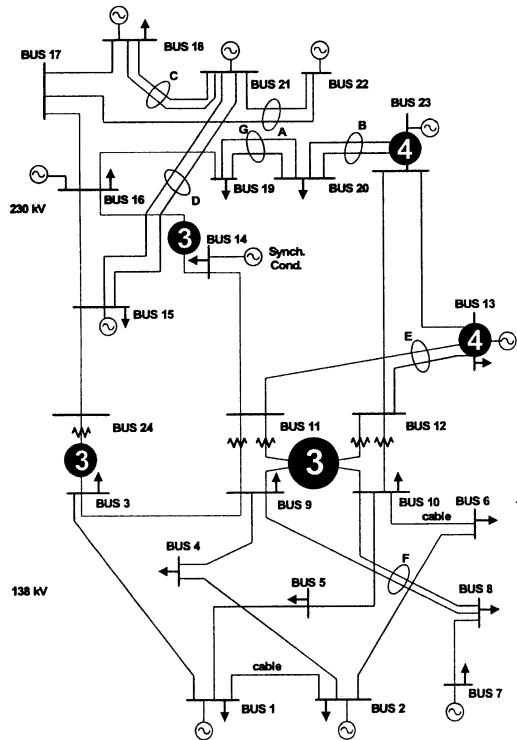


Fig. 5. Interdiction plans 3 (⊙) and 4 (⊙) for RTS1 with $M = 6$ and explicit modeling of system restoration over time. Total energy shed is 557 712 MWh for plan 3. Plan 4 (attack to two buses) is created assuming the two substations attacked in plan 3 have been rendered invulnerable. Total energy shed drops to 272 160 MWh.

transmission line like the one attacked in Plan 3 would be difficult or impossible to harden, although a similar effect might be achieved by adding redundant capacity in a new, separate, parallel corridor. However, opening up new corridors for power lines is a slow, difficult and expensive process and a more practical alternative might be to harden the two substations that Plan 3 indicates are important. Indeed, when those two substations

are treated as invulnerable, the best attack plan found, Plan 4 in Fig. 5, sheds only 272 160 MWh of electricity compared to

557 712 MWh for Plan 3. Hardening a substation could be accomplished in a number of ways, for example, by strengthening building walls or by enclosing outdoor facilities.

The components that are identified as candidates for hardening will naturally depend on the assumptions regarding M , i.e., the terrorists' assumed resources. If certain components appear to be critical over a wide range of values for M , then it would be reasonable to focus on those components for hardening. However, more research will be required to formalize an approach to this problem.

IV. CONCLUSIONS AND FUTURE WORK

In this paper we have formulated the problem of optimal interdiction of an electric power network and have developed a heuristic algorithm to solve the problem. We have demonstrated the algorithm using two RTS systems and have indicated how the results can be used by planners to identify critical components whose hardening will substantially improve system security. Critical components are identified with modest computational effort.

Numerous issues remain for future work, and they include:

- creating linear approximations of the model (Mm) having the form

$$\begin{aligned} (\text{LMm}) \quad & \max_{\delta \in \Delta} \min_{\mathbf{p}} \mathbf{c}^T \mathbf{p} \\ \text{s.t.} \quad & A\mathbf{p} \leq B\delta \\ & \mathbf{p} \geq \mathbf{0} \end{aligned}$$

which are amenable to exact solution methods;

- extending (Mm) and (LMm) to represent more detail about system restoration and unmet load over time;
- extending (Mm) and (LMm) to

$$\begin{aligned} (\text{PLMm}) \quad & \min_{\psi \in \Psi} \mathbf{d}^T \psi + \max_{\delta \in \Delta(\psi)} \min_{\mathbf{p}} \mathbf{c}^T \mathbf{p} \\ \text{s.t.} \quad & A(\psi)\mathbf{p} \leq B(\psi)\delta \\ & \mathbf{p} \geq \mathbf{0} \end{aligned}$$

where the new level of optimization over $\psi \in \Psi$ represents protective measures to be taken in advance, such as hardening particular grid components as discussed in Section III-E. These measures will reduce the ability of terrorists to attack the grid through the constraints represented by $\delta \in \Delta(\psi)$, and thereby improve post-attack power flows;

- incorporating uncertainty about terrorists' capabilities into our analysis;
- evaluating different spare-equipment policies, including the use of "generic" transformer spares that could provide

adequate, if imperfect, replacements for several types of transformers;

- representing the immediate aftermath of an attack, including cascading outages and the dynamics of voltage collapse and angular instability.

REFERENCES

- [1] "Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage," OTA-E-453, 1990.
- [2] "Report of the National Energy Policy Development Group," Vice President's Task Force, 2001.
- [3] "Making the Nation Safer. The Role of Science and Technology in Countering Terrorism," National Research Council, National Academy Press, Washington, D.C., 2002.
- [4] B. Qiu, Y. Liu, and A. G. Phadke, "Communication infrastructure design for strategic power infrastructure defense (SPID) system," in *Proc. IEEE Power Eng. Soc. Winter Meeting*, Jan. 27–31, 2002.
- [5] E. Israeli and K. Wood, "Shortest-Path network interdiction," *Networks*, vol. 40, pp. 97–111, 2002.
- [6] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation and Control*, 2nd ed. New York: Wiley, 1996.
- [7] A. M. Geoffrion, "Generalized benders decomposition," *J. Optim. Theory Applicat.*, vol. 10, pp. 237–260, 1972.
- [8] "The IEEE reliability test system—1996," *IEEE Trans. Power Syst.*, vol. 14, pp. 1010–1020, Aug. 1999.
- [9] (1999-II) IEEE Reliability Test Data. [Online]www.ee.washington.edu/research/pstca/
- [10] (2003) GAMS-CPLEX. [Online]www.gams.com
- [11] K. Cormican, D. Morton, and K. Wood, "Stochastic network interdiction," *Oper. Res.*, vol. 46, pp. 184–197, 1998.
- [12] J. Birge and F. Louveaux, *Introduction to Stochastic Programming*. New York: Springer-Verlag, 1997.
- [13] M. Herald, "Rebel Tactics Cause Concern," DTIC, 2002.

Javier Salmeron received the M.S. degree in mathematics from Complutense University, Madrid, Spain, and the Ph.D. degree in mathematics from Polytechnic University of Madrid, Spain.

Currently, he is a Research Assistant Professor in the Operations Research Department at the Naval Postgraduate School, Monterey, CA.

Kevin Wood received the B.S. degree in electrical engineering and mathematics from the University of Portland, Portland, OR, the M.S. degree in operations research from Columbia University, New York, and the Ph.D. degree in operations research from the University of California at Berkeley.

Currently, he is Professor in the Operations Research Department at the Naval Postgraduate School, Monterey, CA.

Ross Baldick (M'91) received the B.Sc. and B.E. degrees from the University of Sydney, Australia, and the M.S. and Ph.D. degrees from the University of California, Berkeley.

From 1991 to 1992, he was a Post-Doctoral Fellow at the Lawrence Berkeley Laboratory, Berkeley, CA. In 1992 and 1993, he was an Assistant Professor at Worcester Polytechnic Institute, Worcester, MA. He is currently a Professor with the Department of Electrical and Computer Engineering at the University of Texas at Austin.