Investment Planning for Electric Power Systems Under Terrorist Threat

Natalia Romero, Ningxiong Xu, Linda K. Nozick, Ian Dobson, *Fellow, IEEE*, and Dean Jones

***Abstract*—Access to electric power is critical to societal welfare. In this paper, we analyze the interaction between a defender and a terrorist who threatens the operation of an electric power system. The defender wants to find a strategic defense to minimize the consequences of an attack. Both parties have limited budgets and behave in their own self-interest. The problem is formulated as a multi-level mixed-integer programming problem. A Tabu Search with an embedded greedy algorithm for the attack problem is implemented to find the optimum defense strategy. We apply the algorithm to a 24-bus network for a combination of four different defense budgets, three attack budgets, and three assumptions as to how the terrorists craft their attacks.**

***Index Terms*—Decision support system, game theory, load flow analysis, power system security, systems engineering.**

NOMENCLATURE

A. Model Parameters

T	Set of transmission lines and transformers (assumed to be directed to facilitate formulation).
B	Set of buses.
L	Set of transformers.
S	Set of substations.
E	Set of generators.
a_{ij}^D	Cost of adding c_{ij} units to transmission line (i,j).
b_g^D	Cost of adding q_g units to generator g.
M^A	Terrorist's budget.
M^D	Defender's budget.
c_g^E	Per-unit cost for generation using generator g.
c_{ij}	Size of capacity increments that can be added to transmission line (i,j).
c_l^L	Cost to replace interdicted transformer l.
D_i	Demand at bus i.
e_{ij}^A	Cost of attacking transmission line (i,j).
f_s^A	Cost of attacking substation s.
f_s^D	Cost of protecting substation s.
G_g^m	Capacity of generator g.
h_g^D	Cost of protecting generator g.
h_g^A	Cost of attacking generator g.
h_l^L	Unit purchasing cost of transformer l.
k	Stage of recovery, $k \in \{1,2,3,4\}$.
m_{ij}	Reactance for transmission line (i,j).
P_{ij}^m	Capacity of line (i,j).
q_g	Increments of capacity that can be added to generator g.
r_s^S	Cost of repairing substation s.
r_{ij}^T	Cost of repairing transmission line (i,j).
r_g^E	Cost of repairing generator g.
S_i	Substation where bus i is located.
μ_i	Unit load-shedding cost at bus i.
t_k	Time to complete stage k.
T_{ijl}	Binary parameter, 1 indicates a transformer; otherwise indicates a transmission line.
$\delta^+(i)$	Set of lines that start in bus i.
$\delta^-(i)$	Set of lines that end in bus i.
I_i	Set of generators that are connected to bus i.
O_s	Set of buses in substation s.
$(k,l)\|\|(i,j)$	Transmission line (k,l) is the line sharing right of way with (i,j).

B. Defender's Decision Variables

$x^D = (x_s^D)$	Vector of binary decision variables, $x_s^D = 1$ if substation s is protected and 0 otherwise.
$z^D = (z_g^D)$	Vector of binary decision variables, $z_g^D = 1$ if generator g is protected and 0 otherwise.
$w^D = (w_g^D)$	Vector of integer decision variables, w_g^D indicates that q_g units of capacity are added to generator g.
$v^D = (v_{ij}^D)$	Vector of integer decision variables, v_{ij}^D indicates that c_{ij} units of capacity are added to transmission line (i,j).
$H^D = (H_i^D)$	Vector of integer decision variables, H_i^D indicates the number of transformers of type l purchased.

Manuscript received July 22, 2010; revised December 01, 2010, March 17, 2011, and May 17, 2011; accepted May 25, 2011. This work was supported in part by DOE grant DESC0002283. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Paper no. TPWRS-00592-2010.

N. Romero, N. Xu, and L. K. Nozick are with the School of Civil and Environmental Engineering, Cornell University, Ithaca, NY 14853 USA (e-mail: nr229@cornell.edu; lkn3@cornell.edu).

I. Dobson is with the Department of Electrical and Computer Engineering, University of Wisconsin, Madison, WI 53706 USA.

D. Jones is with the Sandia National Laboratories, Albuquerque, NM 87185-1138 USA.

Digital Object Identifier 10.1109/TPWRS.2011.2159138

C. Terrorist's Decision Variables

$x^A = \left(x_s^A\right)$	Vector of binary decision variables, $x_s^A = 1$ if substation s is attacked and 0 otherwise.
$y^A = \left(y_{ij}^A\right)$	Vector of binary decision variables, $y_{ij}^A = 1$ if transmission line (i,j) is attacked and 0 otherwise.
$z^A = \left(z_g^A\right)$	Vector of binary decision variables, $z_g^A = 1$ if generator g is attacked and 0 otherwise.

D. Power-Link Network Decision Variables

$G = \left(G_g^k\right)$	Vector of nonnegative continuous decision variables, G_g^k indicates the power generated by generator g in period k.
$P = \left(P_{ij}^k\right)$	Vector of continuous decision variables, P_{ij}^k, indicates the electric power flows in line (i,j) in period k.
$U = \left(U_i^k\right)$	Vector of nonnegative continuous decision variables, U_i^k, indicates the load shed at bus i in stage k.
$\theta = \left(\theta_i^k\right)$	Vector of continuous decision variables, θ_i^k, indicates the phase angle at bus i in period k.
$R = (R_{ijl})$	Vector of binary decision variables, $R_{ijl} = 1$ if spare transformers l is used in line (i,j) and 0 otherwise.

I. Introduction

DELIBERATE attacks do not occur frequently, but when they do, they can be disastrous. From 1999 to 2002, there were over 150 attacks on electric power systems across the world [1]. In the United States, there is awareness that it is important to make these systems more resilient to terrorist attacks. For example, the National Academies suggests that it is important to consider protection of key equipment and whether there should be additional reserve capacity for generation, transmission, and distribution to promote resiliency to address these threats [2].

This paper presents a formulation for the problem of a strategic defender to a carefully crafted attack. We develop a leader-follower model representation of this strategic interaction. The leader determines the protection measures to be adopted including specific investments to increase operating margin and the acquisition of spare transformers. The follower is the terrorist that selects an attack with full knowledge of the defender investments and the understanding that the operator will optimize the use of the system after the attack in order to minimize the consequences of the attack.

Reference [3] describes a range of related models across a variety of infrastructures focused on a bioterrorist threat. Reference [4] develops an investment planning model using a linear dc power flow representation of an electric power transmission network. They include a range of scenarios for the disruption and solve for investments in line capacities that minimize the investment needed to honor all demands under all scenarios. Reference [5] analyzes the fortification problem for networks. They assume different profiles for attacker behavior: destruction based on capacity of arcs, destruction based on flow, or optimal behavior to minimize or maximize the flow in the system. Reference [6] uses a bilevel mixed-integer program to identify the critical components in a network under terrorist threats. They use an implicit enumeration algorithm to solve the fortification problem or upper level. The lower level is formulated as an r-interdiction median problem. Reference [7] studies different models and algorithms to solve network interdiction games.

References [8] and [9] develop an interdiction model for electric power systems, using a set of linear dc power flow models, with the goal of identifying the attack that would result in the maximum disruption. Reference [8] develops an iterative heuristic scheme to identify prices which represent the value of each component in an attack. They then select those components which result in the largest estimated damage, given the prices developed and that are consistent with the terrorist's budget. Reference [9] focuses on the same formulation but uses generalized Benders decomposition to create a heuristic solution procedure. References [10] and [11] develop a bilevel formulation of the interdiction problem. In [11], the terrorist's objective is to cause a maximal amount of load-shed with the removal of as few lines as possible and the defender wants to minimize load-shed. References [10] and [11] use the Karush-Kuhn-Tucker conditions to convert the bilevel formulation into a single level optimization problem. Reference [12] employs a simple procedure to identify "near-optimal" interdiction strategies for power transmission systems. They consider attacks only to lines and implement a greedy algorithm. At each iteration of that algorithm, the line with maximum flow is identified. This process continues until the budget of the terrorist is exhausted. Additionally, it explores the benefits from hardening (protecting) a number of lines that the terrorist would most likely choose.

Reference [13] uses a stochastic programming formulation to reinforce and expand a power system with the objective of reducing the impact of a deliberate attack. The attacks are generated using results from [10] and [11]. Reference [14] analyzes the expansion plans proposed in [13] in relation to economic and vulnerability issues. Reference [15] evaluates the benefit of line switching as a mitigation strategy. They use a genetic algorithm to solve the interdiction problem. Reference [16] analyzes the vulnerability of a power grid to unintentional and deliberate outages. The interdiction bilevel mixed-integer problem is transformed into a single level problem using two different methods: its Karush-Kuhn-Tucker conditions and duality theory. Reference [17] expands on the defender-attacker problem by focusing on the amount of information available to attackers when they form the attack as a mechanism to determine the defenders optimal strategy.

We formulate a multi-level mixed-integer programming problem. The defender's optimization is solved using a Tabu Search similar to that presented by [18]. The attack is found with a greedy algorithm. It has three different variations that correspond to three assumptions as to how the terrorist will craft the attack. These assumptions are identified as: capacity based attack (CBA), maximum flow based attack (MFA), and greedy attack (GA).

The defender can allocate a limited budget to protect generators and substations, to increase generation and line capacity, or to purchase spare transformers. Terrorists can attack any combination of lines, substations, and/or generation units subject to their budget constraint. This paper compares the results for three different assumptions of how terrorists will craft the attack and four budgets each for the defender and the terrorists using the one-area IEEE Reliability Test System (RTS)—1996 [19].

This paper can be viewed as an extension of [12] in that it extends their interdiction problem to consider the performance of the systems during the entire repair process, not just in the period right after the attack. It also explores the limitations of a CBA attack in comparison to GA and MFA crafted attacks. Finally, we significantly broaden the approach to the investment aspect of the problems to include opportunities to add operating margin to the systems as well as to stockpile spares. This paper can also be viewed as an extension of [8] and [9] in that their focus is on interdiction under the assumption that it is known how spare transformers will be used. This is a key element of this analysis; however, we also focus on the investment elements of the problem in addition to how to optimally use spares after an attack.

II. Approach

A. Formulation

We formulate the defender-attacker-operator problem as a three-level optimization problem.

The upper level corresponds to the defender's decision to minimize the costs after an attack to the power grid through investments (pre-attack). The intermediate and lower levels are the interdiction problem. In the interdiction problem, the attacker damages a set of components in the system in order to optimize her/his interest. However, we assumed that the attacker knows what the operating strategy would be to minimize the costs after the attack. The third level corresponds to operator's minimization of operating costs after the attack.

The repair process consists of four stages. During the first stage, all attacked components and those in proximity to attacked components cannot have any flow. During the second stage, the only lines that are not repaired are those connected to attacked substations. During the third stage, all substations components have been repaired except damaged transformers. In the fourth and final stage, spare transformers are assumed to be in place.

The linear dc power flow network model is used to estimate the power flows in the network at each stage during the repair process and the demands not satisfied. The defender's objective is to minimize the sum of the power generation costs, load-shed costs, and the repair costs by implementing an effective pre-attack investment strategy. The objective of the terrorist is to maximize the sum of the power generating costs, load-shed costs, and repair costs. Both players have limited resources. The objective of the operator is to minimize the sum of the generation costs, the load shed costs, and the repair costs for transformers which are attacked and for which there is not a spare.

B. Power-Flow Optimization Model

The linear dc power flow model formulated below represents the optimal response of the operator during the recovery period. In this model, the investment strategy of the defender is assumed known to the terrorist. We assume that the operator observes the defender's and attacker's decisions and makes his decision during these four time periods by minimizing operating costs during the repair process. Mathematically, for $(x^A, y^A, z^A, v^D, w^D, H^D)$, this network optimization problem is to choose (θ, G, P, U, R) that minimizes

$$\sum_{k=1,2,3,4}\left(\sum_{i\in B}\mu_i U_i^k+\sum_{g\in E}c_g^E G_g^k\right)(t_k-t_{k-1}) +\sum_{s\in S}\sum_{i\in O_s}\sum_{(i,j)\in T}\sum_{l\in L}c_i^L(1-R_{ijl})T_{ijl}x_s^A \quad (1)$$

subject to

$$\left(\theta_i^1-\theta_j^1\right)\left(1-x_{s_i}^A\right)\left(1-x_{s_j}^A\right)\left(1-y_{ij}^A\right)\prod_{(k,l)||(i,j)}\left(1-y_{kl}^A\right) = \frac{m_{ij}P_{ij}^1}{\left(1+\frac{c_{ij}v_{ij}^D}{P_{ij}^m}\right)},\ (i,j)\in T, \quad (2)$$

$$\left(\theta_i^2-\theta_j^2\right)\left(1-x_{s_i}^A\right)\left(1-x_{s_j}^A\right)=\frac{m_{ij}P_{ij}^2}{\left(1+\frac{c_{ij}v_{ij}^D}{P_{ij}^m}\right)},\ (i,j)\in T \quad (3)$$

$$\left(\theta_i^3-\theta_j^3\right)\left(1-x_{s_i}^A\sum_{l\in L}T_{ijl}\right)=\frac{m_{ij}P_{ij}^3}{\left(1+\frac{c_{ij}v_{ij}^D}{P_{ij}^m}\right)},\ (i,j)\in T \quad (4)$$

$$\left(\theta_i^4-\theta_j^4\right)\left(1-x_{s_i}^A\sum_{l\in L}(1-R_{ijl})T_{ijl}\right)=\frac{m_{ij}P_{ij}^4}{\left(1+\frac{c_{ij}v_{ij}^D}{P_{ij}^m}\right)},\ (i,j)\in T \quad (5)$$

$$\sum_{g\in l(i)}G_g^k-\sum_{(i,j)\in\delta^+(i)}P_{ij}^k+\sum_{(i,j)\in\delta^-(i)}P_{ij}^k=D_i-U_i^k,\ i\in B,\ k=1,2,3,4 \quad (6)$$

$$0\le U_i^k\le D_i,\ i\in B,\ k=1,2,3,4 \quad (7)$$

$$0\le G_g^k\le\left(G_g^m+q_g w_g^D\right)\left(1-z_g^A\right),\ g\in E,\ k=1,2,3,4 \quad (8)$$

$$\left|P_{ij}^1\right|\le\left(P_{ij}^m+c_{ij}v_{ij}^D\right)\left(1-x_{s_i}^A\right)\left(1-x_{s_j}^A\right)\left(1-y_{ij}^A\right)\prod_{(k,j)||(i,j)}\left(1-y_{kl}^A\right),\ (i,j)\in T \quad (9)$$

$$\left|P_{ij}^2\right|\le\left(P_{ij}^m+c_{ij}v_{ij}^D\right)\left(1-x_{s_i}^A\right)\left(1-x_{s_j}^A\right),\ (i,j)\in T \quad (10)$$

$$\left|P_{ij}^3\right|\le\left(P_{ij}^m+c_{ij}v_{ij}^D\right)\left(1-x_{s_i}^A\sum_{l\in L}T_{ijl}\right),\ (i,j)\in T \quad (11)$$

$$\left|P_{ij}^4\right|\le\left(P_{ij}^m+c_{ij}v_{ij}^D\right)\left(1-x_{s_i}^A\sum_{l\in L}(1-R_{ijl})T_{ijl}\right),\ (i,j)\in T \quad (12)$$

$$\sum_{(i,j)\in T}R_{ijl}\le H_l,\ l\in L \quad (13)$$

$$R_{ijl}=0,1,\ (i,j)\in T,\ l\in L. \quad (14)$$

The objective function given in (1) is the sum of the power generation, load-shed, and replacement costs (for spare transformers for which there are no spares). Constraints (2)–(5) approximate the active power flows on the transmission lines in the four stages of the repair process. It is important to notice that some forms of line capacity upgrades, such as reconductoring or adding parallel lines, may reduce line reactance. We model this by reducing the line's reactance in proportion to the capacity increase due to the enhancement. Constraints (6) preserve the power balance at the buses in the four-stage repair process. Constraints (7) state that the load-shedding at a bus cannot exceed the demand at the bus. Constraints (8) bound the power produced at each generator. If a generator is not attacked, the generator has the full capacity, which is its original capacity plus any capacity added by the defender. Otherwise, the generator does not function during the four time periods. Note that the power flow in each transmission line can go in either direction; therefore, the flow load on each transmission line can take either a negative or positive value. Constraints (9)–(12) set the maximum absolute values of the flows for transmission lines in each stage. A line is not available in the first stage if it is attacked, if a substation to which is connected is attacked, and/or if a line in close proximity is attacked. Otherwise, the line has full transmission capacity. For the second stage, lines that are connected to attacked substations are the only ones with no transmission capacity. Substations without transformers can be repaired by the third stage; thus, during the third stage, only lines that represent transformers damaged during a substation attacked are not available. In the final stage, the interdicted transformers, for which there is a spare, are back in operation. Constraints (13) state that the number of transformers of each type used to replace the interdicted transformers of that same type cannot exceed the number available. Constraints (14) impose binary restrictions. It is important to notice that this formulation includes the length of time each component attacked will be out of service. It is these durations that drive the definition of the stages, indexed by k, in the model. We assume, as in [8], that lines, transformers for which there are available spares, and substations are repaired within 72 h, 360 h, and 768 h, respectively.

Recall that mathematical program (1)–(14) depends on the defender and terrorist's decisions $(x^A, y^A, z^A, v^D, w^D, H^D)$. Let $F_L(x^A, y^A, z^A, v^D, w^D, H^D)$ be the minimum value in (1).

C. Terrorist's Optimization Problem

The terrorist is assumed to have perfect information on network protection, network capacity, and number of stored spare transformers. The terrorist also understands that the operator will strive to mitigate the impact of the attack to the extent possible including identifying how to use the spare transformers effectively. Based on all information, the terrorist chooses his/her attack strategy under a budget constraint. Mathematically, for the given $(x^D, z^D, v^D, w^D, H^D)$, the terrorist's optimization problem is to choose (x^A, y^A, z^A) that maximizes.

$$F_L(x^A, y^A, z^A, w^D, v^D, H^D) + \sum_{(i,j)\in T} r^T_{ij} y^A_{ij} + \sum_{g\in E} r^E_g z^A_{ig} + \sum_{s\in S} r^S_s x^A_s \quad (15)$$

subject to

$$x^A_s \le 1 - x^D_s,\ s \in S \quad (16)$$

$$z^A_g \le 1 - z^D_g,\ g \in E \quad (17)$$

$$y^A_{ij} \le 1 - \sum_{l\in L} T_{ijl},\ (i,j) \in T \quad (18)$$

$$\sum_{s\in S} f^A_s x^A_s + \sum_{(i,j)\in A} e^A_{ij} y^A_{ij} + \sum_{g\in E} h^A_g z^A_g \le M^A \quad (19)$$

$$x^A_s,\ z^A_g,\ y^A_{ij} = 0, 1,\ s \in S,\ g \in E,\ (i,j) \in T. \quad (20)$$

The objective function (15) is the sum of the power generation costs and load-shed costs during the four stages, and the repair costs. Constraints (16) and (17) enforce the rule that only the unprotected generators and substations can be attacked. Constraints (18) prohibit attacks on single transformers; these can only be damaged through attacks to substations. Constraint (19) states that the total cost of attacking the generators, lines, and substations cannot exceed the available budget. Constraints (20) require the decision variables to be binary.

Recall that mathematical program (15)–(20) depends on the defender's decisions $(x^D, z^D, v^D, w^D, H^D)$. Then let $F_A(x^D, z^D, v^D, w^D, H^D)$ be the maximum value.

D. Defender's Optimization Problem

The defender understands that the terrorist has perfect information and will optimize his attack to further his objectives. Therefore, the defender chooses a protection strategy to minimize their objective function subject to a limited budget. Mathematically, we formulate this optimization problem as a static transmission and generation planning problem [20] to choose $(x^D, z^D, v^D, w^D, H^D)$ that minimizes

$$F_A(x^D, z^D, v^D, w^D, H^D) \quad (21)$$

subject to

$$\sum_{s\in S} f^D_s x^D_s + \sum_{g\in E} h^D_g z^D_g + \sum_{(i,j)\in A} a^D_{ij} v^D_{ij} + \sum_{g\in E} b^D_g w^D_g + \sum_{l\in L} h^L_l H^D_l \le M^D \quad (22)$$

$$x^D_s, z^D_g, v^D_{ij}, w^D_g = 0, 1,\ s \in S,\ g \in E,\ (i,j) \in T,\ H^D_l \text{ non-negative integer } l \in L. \quad (23)$$

The treatment of investment costs is parallel to [21] and [4].

E. Solution Procedure

It is known that this three-level optimization problem is NP-hard [22]. We used a Tabu Search to solve the defender's problem and greedy algorithms to address the attacker's problem. For the Tabu Search, the first neighbors are generated based on attacks generated from past neighborhoods. All the substations and generators attacked on these previous iterations are likely critical components; thus, in these first iterations, we explore the benefit from protecting them. However, if these protection strategies are infeasible, the neighbors are generated randomly. The other neighbors are randomly generated. The

attack is estimated using a greedy algorithm, which represents specific assumptions about how the terrorist will craft their attack. Those algorithms are: CBA, MFA, or GA. CBA is an algorithm which iteratively removes the component with the largest capacity until the attacker's budget is exhausted [5]. MFA iteratively removes components with the largest weighted flow across the four repair periods as computed by the dc power flow model. This algorithm is an extension to that given in [12]. In each iteration, the GA algorithm removes the component which causes the greatest increase in the terrorist's objective function until the terrorist's budget is exhausted.

For the case study developed based on the One-Area IEEE RTS-96 [19] system described in Section IV, the algorithm was implemented and executed using IBM ILOG OPL 6.3 in a Dell Optiplex 755, Intel® Core™ 2 Quad, with 2.83 GHz and 3.25 GB of RAM memory (though the code was not parallelized). For 20 iterations, 10 neighbors per iteration, keeping solutions as tabu for 5 iterations, an attack budget of 6 units, and a defense budget of US$ 25 million, the execution times was approximately: 3. 5 min for CBA, 22 mi for MFA, and about 12 h for GA. For a dc model of the Eastern Interconnect which has about 23 000 links and 15 000 nodes for a defense budget of US$ 100 million, an attack budget of 10, and an attack strategy of CBA, about 14 h was required. In this case, CPLEX 12.1 C++ concert technology was used. Computation time can be reduced if the problem is parallelized using CPLEX 12.2.

III. Case Study

We applied our method to the IEEE One-Area RTS—1996. It has 24 nodes and 38 links that correspond to 24 buses and 38 transmission lines. We included generation units and substations as independent sets of components that can be related to the buses. Substations were defined as combinations of one or more buses. With the exception of buses 3, 9, 10, 11, 12, 13, and 24, each bus represents a substation. Buses 3 and 24 are connected by a transmission line identified as a transformer; thus, these two buses are part of the same substation. Likewise, buses 9, 10, 11, and 12 are part of a single substation. With these considerations, the model has 20 substations. The IEEE RTS document has a comprehensive description of the location of generation units among the buses [19]. The 5 transformers on the one-area RTS-96 were modeled as links for the load-flow model.

Reference [8] identifies the average outage time when certain components of a power system are disrupted. Overhead lines, transformers for which there are available spares, single buses, and substations are assumed to take 72 h, 360 h, and 768 h, respectively. In addition to this data, we assume that replacing transformers and generation units can take on the order of 4320 h (6 months). These outage lengths are the basis for the four time periods considered in this model.

The costs to attack a component can vary based on a variety of factors including the type of attack and the location of the component. Therefore, we assigned a relative cost to attack each type of element: attacking a line costs one unit, attacking a substation, three units, and attacking a generator four units. An attack to a line damages the line and any line with common right of way (see ovals identified with letters from A to G in One-Area IEEE RTS-96 [19]). An attack to a substation damages the buses and transformers within the substation and all the lines coming connected to the substation. The attack to a generation unit exclusively damages the generation plant; it does not affect the bus where it is located. The costs to protect substations and generators, increase capacity of lines and generation units, and replace components were obtained from a variety of sources. Reference [23] provides the generation unit costs for hydro and coal plants; they include capital costs and operational costs. Reference [24] classifies costs for several power system capacity enhancement projects; it was a source for repair costs and lines capacity enhancement strategies. Reference [25] presents data for line upgrades and new transformers costs. New generation unit capital costs and generating cost were obtained from [26], the Energy Information Administration [27], and Secretary-General of the OECD [28]. All the costs were converted to 2002 U.S. dollars and adjusted to make them consistent among sources.

TABLE I
Defender's Resources Allocation

Attack Type	Budget	*Defender's Budget [Millions of U.S. dollars]* 25.0		50.0		75.0	
		Defense resource allocation					
		Pro.	*Enh.*	*Pro.*	*Enh.*	*Pro.*	*Enh.*
GA	2	0.0	23.7	0.0	47.4	0.0	74.8
	3	21.6	0.0	43.2	4.8	64.7	9.6
	6	21.6	0.0	21.6	27.2	21.6	52.5
	7	21.6	0.0	43.2	4.8	64.7	8.3
MFA	2	0.0	23.7	0.0	47.0	0.0	74.8
	3	0.0	25.0	3.8	28.5	2.4	71.1
	6	0.0	23.7	0.0	45.8	0.0	74.8
	7	21.6	0.0	21.6	25.0	21.6	52.7
CBA	2	0.0	25.0	0.0	49.9	0.0	71.3
	3	21.6	0.0	21.6	0.0	28.9	43.7
	6	10.8	13.1	10.8	38.0	10.8	61.8
	7	10.8	11.7	21.6	21.6	21.6	47.0

Table I shows how the defender's budget is allocated under each scenario. Protection (*Pro.*) corresponds to protecting substations and generators. Protecting the nuclear generators and the coal/steam generator (U350) is very expensive but these generators are the most attractive for the terrorist. Since it is not possible for the defender to protect these components with any of the explored budgets, protection of generators is not considered. Therefore, protection, in these experiments, is focused on substation security. Enhancement (*Enh.*) refers to investments in operating capacity for transmission lines and generators. In this analysis, the largest benefits are the result of investments in generation capacity. It is useful to notice that the model tends to recommend a relatively equal investment in protection and enhancement and, because of the cost of transformers, no investment in spares.

Table II shows the components that the defender decides to protect or enhance. As in Table I, this table has an entry for each attack rule and defender and attacker budgets. Substations are identified with an S and with the number of the bus (B) within them. Enhancements to generators, G, are referenced using the corresponding bus and the total generating MW added to generators at the bus. Notice how protecting substations 3 and 9 is a key element of many defense strategies. In addition, notice the recurrence of enhancements to the capacity of generators in bus 1, 2, and 15. Increasing generation capacity in these three buses

TABLE II
DEFENSE STRATEGY CRITICAL COMPONENTS

Attack		*Defender's Budget [Millions of U.S. dollars]*					
		25.0		*50.0*		*75.0*	
Type	**Budget**	***Defense resource allocation***					
		Protection	*Enhancement*	*Protection*	*Enhancement*	*Protection*	*Enhancement*
GA	2		G:(B:1(4MW), B:2(12MW), B:15(4.8MW))		L:(3),G:(B:1(4MW), B:2(15.2MW), B:15(2.4MW))		L:(11)G:(B:1(4MW), B:2(8MW), B:22(10MW))
	3	S:**3**,9***		S:**3**,9*, (B:13), (B:23)	G:(B:15(2.4MW))	S:**3**,9*,(B:13), (B:15),(B:16), (B:23)	G:(B:15(4.8MW))
	6	S:**3**,9***		S:**3**,9***	G(B:1(8MW),B:2(12MW), B:15(4.8MW))	S:**3**,9***	L:(7),G:(B:1(8MW), B:2(8MW),B:15(9.6MW))
	7	S:**3**,9***		S:**3**,9*, (B:23)	G:(B:15(2.4MW))	S:**3**,9*,(B:13), (B:17),(B:21), (B:23)	G:(B:1(4MW),B:15(2.4MW))
MFA	2		G:(B:1(8MW),B:2(8MW),B:15(4.8MW))		G:(B:1(4MW),B:2(19.2MW), B:15(4.8MW))		L:(10),G:(B:1(8MW), B:2(4MW),B:22(10MW))
	3		L:(28),G:(B:1(4MW), B:2(4MW))	(B:2)	L:(28),G:(B:1(4MW), B:2(8MW))	G(B:15(2.4MW))	L:(3,28),G:(B:1(12MW), B:2(19.2MW))
	6		G:(B:1(8MW),B:2(8MW),B:15(4.8MW))		G:(B:1(8MW),B:2(19.2MW), B:15(2.4MW))		L:(11),G:(B:1(4MW), B:2(8MW),B:22(10MW))
	7	S:**3**,9***		S:**3**,9***	G:(B:1(8MW),B:2(4MW), B:15(7.2MW))	S:**3**,9***	L:(10),G:(B:1(8MW),B:2(12MW),B:15(14.4MW))
CBA	2		L:(28),G:(B:1(4MW), B:2(4MW))		L:(1,25-1), G:(B:1(4MW),B:2(8MW))		L:(1,25-1),G:(B:1(12MW), B:2(8MW),B:15(7.2MW))
	3	S:**3**,9***		S:**3**,9***		S:**3**,9*,(B:8), G:(B:1(4MW), B:2(4MW))	L:(10),G:(B:1(4MW), B:2(19.2MW))
	6	S:**9***	G:(B:2(4MW), B:15(4.8MW))	S:**9***	L:(1,27),G:(B:1(4MW), B:2(4MW),B:15(4.8MW))	S:**9***	L:(29,31-2),G:(B:2(15.2MW))
	7	S:**3**,9***	L:(1),G:(B:1(4MW), B:2(8MW))	S:**3**,9***	L:(33-2), G:(B:15(2.4MW))	S:**3**,9*,(B:8), G:(B:1(4MW), B:2(4MW))	G:(B:1(4MW), B:2(19.2MW))

* *S:9 Corresponds to bus 9, 10, 11, and 12*

** *S:3 corresponds to bus 3, and 24*

is cheaper than in most of the other buses. In addition, buses 1 and 2 are located in an area of the system with less generating capacity, and there is a risk of isolation from other sources of generation depending on the character of the attack.

For the different attack budgets and strategies and different defense budgets, the attack decision follows a simple behavior. When the terrorist's budget is low, lines are the target of attacks. As their budget grows, substations become attractive and finally, when there are sufficient funds, generators. The nuclear power plant is frequently targeted when the terrorist has sufficient resources, regardless of the rule the terrorist uses in crafting the attack.

Table III shows the incurred costs after an attack. Each row corresponds to a unique combination of attack rule and budget. There are three types of costs: repair, generation (*Gen.*), and load-shed (*L.shed*). Note that the after-attack generation costs vary based on costs of available generation units, and connectivity between power sources and demand. When there is no defense budget and the terrorist has 2 units, each decision rule for the terrorist selects different lines to attack. All the selected lines are among lines with greater transmission capacity. For 3 units, the terrorist can attack substations and lines; the best attack will include damaging substation 9. Substation 9 has 4 transformers and corresponds to 80% of the connectivity between high voltage transmission and low voltage transmission areas. The low voltage area does not have enough generation capacity to cope with the local demand. The logic behind MFA leads the attacker to target substation 3. This situation highlights a weakness in the MFA rule. MFA depends on the solution to the dc power flow model which is often not unique. Therefore, it may be possible for the operator to effectively compensate for the loss as understood through this model.

When the attacker has 6 units, there are sufficient funds to attack two substations. It is important to remember that attacks to substations with transformers and to any generator last for all four periods. It is also important to notice that example network has a total of 3405 MW of generation capacity and 2850 MW of demand. Therefore, capacity exceeds demand by about 20%. The three larger generators are the two nuclear plants, that can produce 400 MW, and one coal/steam plant that can produce 350 MW. If one of these generators were attacked, the system would still have 5% excess capacity. On the other hand, attacking substations 3 and 9 would split the system into two areas. The lower voltage area includes the first 10 buses of the RTS; it has a total demand of 1332 MW and a local generation capacity of 684 MW. In addition to the limitations in local generation capacity

TABLE III
COSTS AFTER ATTACK

Attack		*Defender's Budget [Millions of U.S. dollars]*											
		0.0			*25.0*			*50.0*			*75.0*		
Type	**Budget**	***Cost after attack [Billions of U.S. dollars]***											
		Repairs	*Gen.*	*L.shed*	*Repairs*	*Gen.*	*L.shed*	*Repairs*	*Gen.*	*L.shed*	*Repairs*	*Gen.*	*L.shed*
GA	2	0.00	0.23	0.05	0.29	0.00	0.23	0.29	0.00	0.23	0.29	0.00	0.23
	3	0.37	0.19	2.81	0.59	0.11	0.23	0.54	0.11	0.23	0.45	0.11	0.23
	6	0.55	0.17	4.02	1.58	1.22	0.24	1.57	1.22	0.24	1.55	1.22	0.24
	7	1.59	0.18	3.86	1.90	1.30	0.23	1.82	1.32	0.24	1.76	1.32	0.24
MFA	2	0.00	0.23	0.07	0.31	0.00	0.23	0.31	0.00	0.23	0.31	0.00	0.23
	3	0.37	0.19	2.81	1.72	0.17	0.23	1.71	0.17	0.23	1.61	0.17	0.23
	6	1.22	0.24	0.07	1.52	1.22	0.24	1.52	1.22	0.24	1.52	1.22	0.24
	7	1.59	0.18	3.86	1.67	1.32	0.24	1.66	1.32	0.24	1.66	1.32	0.24
CBA	2	0.00	0.23	0.06	0.26	0.00	0.24	0.26	0.01	0.24	0.26	0.01	0.24
	3	0.37	0.19	2.81	0.34	0.11	0.24	0.34	0.11	0.24	0.34	0.11	0.24
	6	0.55	0.17	4.02	1.52	1.22	0.24	1.48	1.22	0.24	1.46	1.22	0.24
	7	1.59	0.18	3.86	1.56	1.32	0.24	1.56	1.32	0.24	1.56	1.32	0.24

in this area, it is important to highlight that 370 MW of the demand are located in buses 9 and 10 which are part of substation 9. If attacked, the lines connected to this substation would remain disrupted for the first two time periods cutting off any energy supply to these two buses. The second area has enough local generation capacity; it only has load-shed problems due to connectivity. Consequently, the system would have a total load-shed of 35% during the first two time periods and 25% in the third and fourth periods. The costs of the load-shed are more significant than the difference between the repair costs of the nuclear plant versus the 5 transformers. Therefore, the optimal attack with a budget of 6 units corresponds to damaging substations 3 and 9. The system has enough redundancy to cope with losing 400 MW and with part of the new limitations of connectivity. CBA and GA decision rules choose to attack substations 9 and 3; but the MFA rule results in an attack on one of the nuclear plants and two lines and therefore a much lower post-event consequence for the operator.

When the terrorist has 7 units and the defender zero budget, effective attacks include a high capacity generator and substation 9. All three rules identify the same generator and substation. Investing in protection reduces losses in connectivity, and investing in generation capacity provides redundancy. This explains the slight increment in generation costs with larger defense budgets. Notice the reductions in load-shed costs, for GA and CBA, when the attacker has 3 or more units and the defense budget increases to US$25 million. In the later case, the defender protects substations 3 and 9. With only 3 units, a secondary substation is attacked. With 6 units, the attack focuses on a nuclear plant and two lines. With 7 units, the nuclear plant and a secondary substation are targeted.

It is useful to understand what the impacts might be if a defensive strategy is crafted based on an incorrect estimate of how the terrorist will craft his/her strategy. We explored this question when the investment budget is US$25 million and the terrorist's budget is 6 units. If the defender assumes that the terrorist will use an MFA-based strategy but they use GA or CBA instead, the post-event costs would be about US$4.7 billion in contrast with the US$1.5 billion the defender might have anticipated. In this example, planning for a GA attack is the most conservative. However, examples can be constructed for which GA does not lead to favorable post-event consequences when the original defense was based on a different attack strategy.

IV. CONCLUSIONS

This paper presents a formulation for the problem of a strategic defender of an electric power system to a carefully crafted attack. We develop a leader-follower model representation of this strategic interaction. We then apply this model to the One-Area RTS-96 [19] with several different budgets for the terrorist and defender and three different rules for how the terrorist might craft the attack. Based on those experiments, we identify four important ideas for investment in these types of networks. First, MFA as a decision rule for the attacker is often inferior to GA and CBA. A key reason for this is that there are often alternative optimums to the network flow problem. This makes the connection between high flow and criticality fragile. Second, when protecting electric power systems against these types of attacks, investments in operating margin are important to consider in addition to more traditional protection measures. Operating margin can make the systems more resilient to attacks and alleviate the need for some types of traditional protection measures. Third, as the defender's budget increases, many of the investments recommended by smaller budgets remain useful. This is important because these types of investments are often done incrementally. Fourth, if the defensive strategy is developed assuming a different strategy will be used to craft the attack than that which is actually used, the post-event costs may be significantly higher than anticipated. This implies that it is important to look for investment strategies that are robust against different methods which might be used to craft the attack.

This research points to several different avenues for future research. First, the probability of an attack is not considered as part of this analysis; hence, extensions which would include this element are important. This analysis assumes that the user of the model's results subjectively incorporates what "soft" information

about the likelihood of an attack might be available to support decision making. In some countries, terrorism has been a long-term problem that persists on a time scale of decades. A country that has already suffered from persistent attacks would have data to construct an analysis estimating the probability of attack and could weigh the costs of an attack accordingly. A country with rare attacks or no previous attacks might need to develop a more subjective approach and integrate this approach with the estimation of a trade-off frontier of the reduction in attack consequences versus costs. This trade-off frontier might be somewhat similar to the results given in Tables I–III in the case study.

Second, we formulate a static defender-attacker-operator model. There is significant value in the creation of a dynamic representation of this strategic interaction over a longer time scale. For example, we consider the initial investment costs for capacity expansion and protection as well as the costs incurred during a 6-month recovery period. A dynamic representation would allow explicit treatment of operating and maintenance costs, return on investment constraints, environmental constraints, etc. It would also allow for the simultaneous consideration of traditional issues like changes in demand over time. Further, improvements in generation and transmission capacity would provide economic and reliability benefits (in addition to benefits of protection from attack) and quantifying these is useful. Third, the attack strategy actually used is difficult to determine *a priori*; therefore, developing a method which identifies robust investments against a range of rules is important. Fourth, infrastructure networks are interdependent; therefore, it is possible that investments in other networks on which the electric power system relies could be as important as investments in the electric power systems itself. Therefore, research to extend the modeling to consider interdependencies is important. Fifth, there are a range of targets available, should an entity be interested in engaging in terrorist activities. In order to defend infrastructures, it is useful to consider the broad range of actions that can be taken to reduce the attractiveness of targets or to increase the difficulty of mounting a successful attack. It is also important that the costs and benefits of these measures be fully assessed. For example, [29] focuses on the costs of pre-event and post-event security measures in transportation systems. Reference [30] focuses on estimating tangible and intangible benefits of security measures. Therefore, research to look across the range of targets available and the range of mitigation measures, including costs incurred and benefits accrued, is critical. Sixth, and finally, electric power systems are subject to a range of hazards; therefore, it is important to think about investment strategies in a multi-hazard context. Some investments, which could be made, improve post-event performance after multiple types of events (e.g., earthquakes, hurricanes, cascading from a small initial failure, etc.) while others are only helpful for one type of event. A multi-hazard approach is likely to create the most effective investment strategy for the total funds expended.

REFERENCES

[1] R. Zimmerman, C. E. Restrepo, J. S. Simonoff, and L. Lave, Risk and Economic Costs of a Terrorist Attack on the Electric System, Presentation for the CREATE Economics of Terrorism Symp., 2005. [Online]. Available: http://create.usc.edu/assets/pdf/51818.pdf.

[2] Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, DC: National Academy Press, 2002.

[3] National Research Council, *Department of Homeland Security Bioterrorist Risk Assessment: A Call for Change*. Washington, DC: National Academies Press, 2008.

[4] D. Bienstock and S. Mattia, "Using mixed-integer programming to solve power grid blackout problems," *Discrete Optim.*, vol. 4, no. 1, pp. 115–141, Mar. 2007.

[5] J. C. Smith, C. Lim, and F. Sudargho, "Survivable network design under optimal and heuristic interdiction scenarios," *J. Glob. Optim.*, vol. 38, no. 2, pp. 181–199, Jun. 2007.

[6] M. P. Scaparra and R. L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Comput. Oper. Res.*, vol. 35, no. 6, pp. 1905–1923, Jun. 2008.

[7] J. C. Smith and C. Lim, "Algorithms for network interdiction and fortification games," in *Optimization and its Applications*, A. Chinchuluun, Ed. *et al.* New York: Springer, 2008, vol. 17, pp. 609–644.

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

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

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

[11] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat," *IEEE Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.

[12] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, and K. R. Wierzbicki, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliab. Eng. Syst. Safety*, vol. 92, no. 9, pp. 1155–1161, Sep. 2007.

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

[14] N. Alguacil, M. Carrion, and J. M. Arroyo, "Transmission network expansion planning under deliberate outages," *Int. J. Elect. Power Energy Syst.*, vol. 31, no. 9, pp. 553–561, Oct. 2009.

[15] J. M. Arroyo and F. J. Fernandez, "A genetic algorithm approach for the analysis of electric grid interdiction with line switching," in *Proc. Intelligent System Applications to Power Systems*, Nov. 2009, pp. 1–6.

[16] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Gen., Transm., Distrib.*, vol. 4, no. 2, pp. 178–190, Feb. 2010.

[17] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," *IEEE Trans. Power Syst*, to be published.

[18] U. P. Wen and A. D. Huang, "A simple tabu search method to solve the mixed-integer linear bilevel programming problem," *Eur. J. Oper. Res.*, vol. 88, no. 3, pp. 563–571, Feb. 1996.

[19] C. Grigg, "The IEEE reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

[20] G. Latorre, R. D. Cruz, J. M. Areiza, and A. Villegas, "Classification of publications and models on transmission expansion planning," *IEEE Trans. Power Syst.*, vol. 18, no. 2, pp. 938–946, May 2003.

[21] N. Alguacil, A. L. Motto, and A. J. Conejo, "Transmission expansion planning: A mixed-integer LP approach," *IEEE Trans. Power Syst.*, vol. 18, no. 3, pp. 1070–1077, Aug. 2003.

[22] J. F. Bard, "Convex two-level optimization," *Math. Program.*, vol. 40, no. 1–3, pp. 15–27, Jan. 1988.

[23] R. Billington, S. Kumar, N. Chowdhury, K. Chu, and K. Debnath, "A reliability test system for educational purposes-basic data," *IEEE Trans. Power Syst.*, vol. 4, no. 3, pp. 1238–1244, Aug. 1989.

[24] P. J. Balducci, L. A. Schienbein, T. B. Nguyen, D. R. Brown, and E. M. Fathelrahman, "An examination of the costs and critical characteristics of electric utility distribution system capacity enhancement projects," in *Proc. Transmission and Distribution Conf. Exhib.*, 2006, pp. 78–86.

[25] M. Vaziri, K. Tomsovic, and A. Bose, "A directed graph formulation of the multistage distribution expansion problem," *IEEE Trans. Power Del.*, vol. 19, no. 3, pp. 1335–1341, Jul. 2004.

[26] M. L. Wald, Costs Surge for Building Power Plant, The New York Times, 2007. [Online]. Available: http://www.nytimes.com/2007/07/10/business/worldbusiness/10energy.html.
[27] Energy Information Administration. (2009, January). Electric Power Annual, U.S. Department of Energy, Washington, DC, 2007. [Online]. Available: http://www.eia.doe.gov/cneaf/electricity/epa/epa_sum.html.
[28] Secretary-General of the OECD (2005). Projected Costs of Generating Electricity NEA, IEA & OECD, Paris, France, 2005 update. [Online]. Available: http://www.iea.org/textbase/nppdf/free/2005/ElecCost.PDF.
[29] P. M. Murray-Tuite, "A framework for evaluating risk to the transportation network from terrorism and security policies," *Int. J. Critic. Infrastruct.*, vol. 3, no. 3/4, pp. 389–407, 2007.
[30] B. E. Prentice, "Tangible and intangible benefits of transportation security measures," *J. Transp. Security*, vol. 1, no. 1, pp. 3–14, Mar. 2008.

Natalia Romero received the B.S. degree in civil engineering from the University of Los Andes, Bogotá, Colombia, and the M.S. degree in civil and environmental engineering from Cornell University, Ithaca, NY. She is currently pursuing the Ph.D. degree in the School of Civil and Environmental Engineering at Cornell University.

Her research interests are in the modeling of civil infrastructure systems under natural and man-made extreme events.

Ningxiong Xu received the B.S. and M.S. degrees in control theory from Xiamen University, Xiamen, China, and the Ph.D. degree in management science and engineering from Stanford University, Stanford, CA.

He is a Research Associate in the School of Civil and Environmental Engineering at Cornell University, Ithaca, NY. His research interests are in large-scale optimization under uncertainty and the application of those tools to transportation systems.

Linda K. Nozick received the B.S. degree in systems analysis and engineering from The George Washington University, Washington, DC, and the M.S. and Ph.D. degrees in systems engineering from University of Pennsylvania, Philadelphia.

She is currently a Professor in the School of Civil and Environmental Engineering at Cornell University, Ithaca, NY. Her research interests are in the modeling of complex systems with a particular focus on infrastructure systems and resiliency to natural and man-made hazards.

Ian Dobson (F'06) received the B.A. degree in mathematics from Cambridge University, Cambridge, U.K., and the Ph.D. degree in electrical engineering from Cornell University, Ithaca, NY.

He is currently a Professor in the Electrical and Computer Engineering Department at the University of Wisconsin-Madison. His research interests are cascading failure risk and complex systems approaches to blackouts.

Dean Jones received the B.S. degree in applied mathematics, and the M.S. degree in applied mathematics from the University of New Mexico, Albuquerque, NM.

He is a Distinguished Member at Sandia National Laboratories. He is the principal technical and programmatic lead of the Operations Research & Computational Analysis Group (ORCA). His emphasis is on the research, design, and application of mathematical models for use in the analysis of complex systems with particular emphasis on systems that can be represented mathematically as graph-based networks.