Optimal Power Grid Protection through A Defender-Attacker-Defender Model

Wei Yuan, Long Zhao, and Bo Zeng

Department of Industrial and Management Systems Engineering, University of South Florida, Tampa, FL 33620
E-mail: {weiyuan,longzhao}@mail.usf.edu, bzeng@usf.edu

Abstract

Power grid vulnerability is a major concern of our society, and its protection problem is often formulated as a tri-level defender-attacker-defender model. However, this tri-level problem is computationally challenging. In this paper, we design and implement a Column-and-Constraint Generation algorithm to derive its optimal solutions. Numerical results on an IEEE system show that: (*i*) the developed algorithm identifies optimal solutions in a reasonable time, which significantly outperforms the existing exact algorithm; (*ii*) the attack solution obtained through solving the attacker-defender model does not lead to the optimal protection plan in general; and (*iii*) protection using the optimal solution from the defender-attacker-defender model always improves the grid survivability under contingencies. The proposed model and algorithm can be easily modified to accommodate for other critical infrastructure network protection problems.

Keywords:
Power grid protection, defender-attacker-defender model, Column-and-Constraint Generation method

1. Introduction

Critical infrastructure reliability and security problems have drawn tremendous attentions from the public. Defensive protection plans are derived to address the issue of possible terrorist attacks on reliability systems [4, 11, 15, 26]. Particularly, power grid vulnerability is a critical issue in modern society. According to a recent study by the National Research Council, a terrorist attack on the U.S. power grid could be much more destructive than natural disasters such as Hurricane Sandy, by blacking out large segments of the country for weeks or even months, costing hundreds of billions of economic damage, and leading to thousands of deaths due to heat stress or exposure to cold during the blackout [5]. Roughly, 200 terrorist attacks on power grids have been reported outside of the U.S. over the past few decades. In fact, from 1999 to 2002, there were over 150 attacks on electric power systems across the world [24]. A study report initiated by The National Academy of Engineering of the United States [14] extensively discussed critical infrastructure protection including electric power grid against terrorism. Zio [25] lists power transmission and distribution systems as one of the old problems with new challenges for reliability engineering due to its complexity of modeling and its critical role for the social welfare. Zio [25] also mentions that new approaches need to be formulated and computation times need to be restricted for application feasibility. N-1 and N-2 security criteria [9] are employed by North American Electric Reliability Corporation (NERC) to ensure the normal operations of power grids under one or two disruptions. Unfortunately, power grids are exposed to both unintentional random failures and terrorist attacks [6]. Hence, simultaneous out-of-service components in a system are not limited to 2. Con-

sequently, N-1 and N-2 criteria are not sufficient to deal with multiple contingencies on power grids [9, 20].

Screening and ranking infrastructure vulnerability across multiple infrastructures due to terrorism are highly studied in reliability engineering [1, 17]. Meanwhile, power grid interdiction problem, which is more focused on modeling the real operations of a power system,is introduced to identify the set of contingencies that make a power grid most vulnerable. Salmeron et al. [18] formulate a power grid interdiction problem as a max-min bi-level program, or an *attacker-defender* (AD) model, and later solve the problem by global Benders decomposition algorithm [19]. Similar min-max modeling approach is studied in power substation defense strategies [12]. It is noted that the system performance under the worst N-1 or N-2 scenarios can be computed through limiting the number of transmission lines under attack to be one or two. Hence, this attacker-defender model provides a framework to perform analysis with the general N-k criterion. . Motto et al. [16] transform the bi-level program to an equivalent single-level mixed integer program through dualizing the lower level liner programming problem, and solve the mixed integer program using available solvers. Zhao and Zeng [23] exactly solve an attacker-defender model with transmission line switching as a mitigation operation. In these models, two different agents, an attacker and a defender optimize their respective objective functions. The attacker, which could be a group of terrorists or a natural disaster, seeks to maximize the power grid disruption penalty (in terms of unmet demand or load shed [4]) given limited attacking resources. The defender, or the power grid operator, reacts after the attack with the goal of minimizing the disruption by re-dispatch. However, even though attacker-defender models are useful to find a set of most critical components for a system, protecting those components does not necessarily provide the best protection plan against system disruptions [4], [21] .

In order to determine an optimal solution of protection plan, Brown et al. [3] propose to extend the bi-level attacker-defender model to a tri-level defender-attacker-defender (DAD) model. As presented in [2, 3, 7, 21], a defender-attacker-defender model involves three agents acting sequentially: (i) the defender's protection: the system planner or defender identifies the system components to be protected or hardened; (ii) the attacker's disruption: a disruptive agent disrupts the power grid by forcing the critical system components out of service; and (iii) the system operator's mitigation: the operator reacts to the disruptive actions to minimize the overall damage by manipulating the power gird components. Both Brown et al. [4] and Yao et al. [21] argue that a tri-level defender-attacker-defender model produces a superior protection plan because it considers an additional level of interaction between the defender and the attacker, and selects the best strategy overall. In fact, the cost of protection plan from an attacker-defender model is 28 percent higher than that of the optimal protection plan from an defender-attacker-defender model for a particular power grid instance in [4]. The other reason that a defender-attacker-defender model is more appropriate for power grid protection is that the data required to support the defender-attacker-defender model are not much harder to obtain than those of an attacker-defender model. According to [21], 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. By introducing an extra level of defender to the model, a defender-attacker-defender model allows the defender to evaluate the impact of varying the defensive resources budget by doing sensitivity analysis that could not be completed by an attacker-defender model alone [21].

Brown et al. [4] initially formulate the optimal allocation of defensive resources problem in a power grid as an defender-attacker-defender model to determine the most critical network components to be protected against terrorist attacks. Results on some particular instances show that adopting a protection plan based on the optimal interdiction solution from an attacker-

defender model would result in a substantial misuse of defensive resources [4]. Yao et al. [21] study a similar tri-level optimization model and describe a decomposition approach that solves smaller bi-level problems iteratively. This approach is actually an extension of set covering decomposition discussed by Israreli and Wood [13]. It is observed from a set of numerical studies that the method in [21] is time-consuming. Delgadillo et al. [7] develop an improved algorithm, the *implicit enumeration algorithm*, which is within a branch and bound framework, to solve this tri-level programming problem. Their implicit enumeration algorithm is computationally more efficient than the method developed in [21]. However, it may not be efficient to deal with instances with multiple attacks and protection decisions. To reduce the computational burden for this type of problems, Bier et al. [2] propose a simple and inexpensive algorithm that iteratively applies *Max Line interdiction algorithm* to sequentially identify a promising hardening or interdiction operation. Although this approach determines sub-optimal solutions, the computational difficulty is reduced remarkably.

To analytically solve this challenging power grid defender-attacker-defender model, it is necessary to develop an efficient and exact computing method that can handle real systems. We adopt a recent solution strategy for two-stage robust optimization, the *Column-and-Constraint Generation* (*C&CG*) method, to develop an efficient algorithm to compute optimal defensive resources allocation plans. Our study has the following major contributions:

(*i*) The developed algorithm identifies optimal solutions in a reasonable time, which significantly outperforms the existing exact algorithm. Indeed, our algorithm is, to the best of our knowledge, the first algorithm that can efficiently solve a power grid defender-attacker-defender problem on practical instances.

(*ii*) We verify that the attack solution obtained through solving an attacker-defender model does not lead to the optimal protection plan in general.

(*iii*) Numerical results indicate that protection using the optimal solution from a defender-attacker-defender model always improves the grid survivability with less load shed.

Notations used in our model are described in Section 2. In Section 3, we present the tri-level formulation of a defender-attacker-defender model for power grid defensive resources allocation problem. Section 4 describes the proposed solution algorithm. Section 5 summarizes the relevant numerical results. Finally, a conclusion is provided in Section 7 with a discussion of future research.

2. Nomenclature

Indices and Sets

N	Set of indices of buses, indexed by n
J	Set of indices of generators, indexed by j
Jn	Set of indices of generators connected to bus n
L	Set of indices of transmission assets, indexed by l
$o(l)$	Origin bus of transmission asset l
$d(l)$	Destination bus of transmission asset l

Parameters

S	Budget of attacker on out-of-service transmission assets
R	Budget of defender's protection decision
D_n	Demand at bus n (in megawatts)
G_j	Generation capacity of generator j (in megawatts)
P_l	Power flow capacity of transmission line l (in megawatts)
x_l	Reactance at line l (Ω)
$\bar{\delta}$	Phase angle capacity of connecting bus (rad)

Decision variables

z_l	Binary protection decision, 1 if l is protected, and 0 otherwise
v_l	Binary attack decision, 0 if line l is attacked, and 1 otherwise
d_n	Load shed at node n (in megawatts)
δ_n	Phase angle at node n (rad)
g_j	Generation level of generator j (in megawatts)
p_l	Power flow on line l (in megawatts)

3. The model

In this section, we present a tri-level min-max-min formulation for a defender-attacker-defender model for power grid protection. Following the convention in [2, 7] etc., we assume that transmission lines are the only components that can be protected or disrupted in a power grid. Note that our approach can be extended to account for other components easily. Also, the defender-attacker-defender model can be also modified to accommodate for other critical infrastructure protection problems such as supply chain, water systems [4].

As described in Section 1, a tri-level defender-attacker-defender model involves three agents acting sequentially. The top level corresponds to the defender's decision on allocating defensive resources to protect transmission lines throughout a power grid before any attack is realized. The middle-lower level is a typical bi-level power grid interdiction problem. The middle level decisions are made by the attacker, who seeks to maximize the load shed of the power system by disconnecting a set of transmission lines. Then, after the disruption by the attacker is observed, the system operator reacts to that disruption by solving an optimal power flow problem to minimize the load shed. Similar to [2, 4, 7, 21], the optimal power flow problem in the lower level is modeled as a linear programming problem, where linear DC power flow model is used to compute power flows throughout the network. In the remainder of this paper, the boldface of a variable represents a vector of corresponding variables, and $\hat{\cdot}$ denotes a fixed decision variable. The formulation of the power grid defender-attacker-defender model is:

$$\min_{\mathbf{z}\in\mathbb{Z}} \max_{\mathbf{v}\in\mathbb{V}} \min_{\{p_l,g_j,d_n,\delta_n\}} \sum_{n\in\mathbf{N}} d_n \tag{1}$$

$$st. \sum_{l\in\mathbf{L}} z_l \le R \tag{2}$$

$$\sum_{l\in\mathbf{L}} (1-v_l) \le S \tag{3}$$

$$p_l x_l = (z_l + v_l - z_l v_l)[\delta_{o(l)} - \delta_{d(l)}],\ \forall l \in \mathbf{L} \tag{4}$$

$$\sum_{j\in\mathbf{Jn}} g_j - \sum_{l|o(l)=n} p_l + \sum_{l|d(l)=n} p_l + d_n = D_n,$$
$$\forall n \in \mathbf{N} \tag{5}$$

$$-P_l \le p_l \le P_l,\ \forall l \in \mathbf{L} \tag{6}$$

$$-\overline{\delta} \le \delta_n \le \overline{\delta},\ \forall n \in \mathbf{N} \tag{7}$$

$$0 \le g_j \le G_j,\ \forall j \in \mathbf{J} \tag{8}$$

$$0 \le d_n \le D_n,\ \forall n \in \mathbf{N} \tag{9}$$

$$v_l, z_l \in \{0,1\},\ \forall l \in \mathbf{L} \tag{10}$$

where $\mathbb{Z} = \{\sum_{l\in\mathbf{L}} z_l \le R, z_l \in \{0,1\}, \forall l \in \mathbf{L}\}$ is defender's protection decision set, and $\mathbb{V} = \{\sum_{l\in\mathbf{L}}(1-v_l) \le S, v_l \in \{0,1\}, \forall l \in \mathbf{L}\}$ is attacker's attack decision set. R is the cardinality budget for the defender, which means that the defender could protect up to R transmission lines in a power grid. Similarly, S is the cardinality budget for the attacker so that the attacker can remove up to S transmission lines.

Constraints (4) capture the active DC power flows on a power grid following the Kirchhoff's Laws with additional protection and attack decision variables. If line l is protected by the defender, z_l will be set to 1, and then $z_l+v_l-z_lv_l = 1$. Hence, this line will be invulnerable from any attack. If line l is not protected in advance, z_l will be set to 0, which means $z_l + v_l - z_l v_l = v_l$. Then, this line will be subject to attacker's decision during interdiction. Constraints (5) preserve power balance at bus n such that the inflow and outflow are equal. Constraints (6) simply state that the power flow on line l will be restricted within $[-P_l, P_l]$. Similarly, constraints (7) restrict the phase angle of bus n to be within $[-\overline{\delta}, \overline{\delta}]$. Constraints (8) bound the power generation of each generator by zero and its capacity. Constraints

(10) guarantee that the load shed at load bus n do not exceed its nominal demand and is always nonnegative.

4. Algorithm

In this section, we describe in details of our customization of the Column-and-Constraint Generation algorithm (*C&CG*) [22] to solve the power grid defender-attacker-defender problem defined in Section 3. We refer readers to [22] for the proof that the *C&CG* algorithm converges to an optimal solution in finite steps.

The *C&CG* algorithm is implemented at two levels, i.e., a *master problem* (MP) and a *subproblem* (SP). On the one hand, the master problem, which includes a subset of possible attacks, yields a lower bound and a protection plan to the defender-attacker-defender problem. On the other hand, the subproblem, which generates the worst attack plan for a given protection decision, leads to an upper bound. Clearly, when these two bounds merge, we obtain an optimal solution.

4.1. Master Problem

Given a set of attack plans $\hat{\mathbf{V}} = \{\hat{\mathbf{v}}^1, \ldots, \hat{\mathbf{v}}^k\} \subseteq \mathbb{V}$, we construct and solve MP to obtain a protection plan. Note that, for a particular attack $\hat{\mathbf{v}}^i$ ($\hat{\mathbf{v}}^i = \{\hat{v}_l^i, \forall l \in \mathbf{L}\}$), we define a set of dispatch variables $(\mathbf{p}^i, \mathbf{g}^i, \mathbf{d}^i, \boldsymbol{\delta}^k)$. Then, MP can be constructed as follows:

$$\min \ \alpha \tag{11}$$

$$st. \ \alpha \geq \sum_{n \in \mathbf{N}} d_n^i, \ \forall i = 1, ..., k \tag{12}$$

$$\sum_{l \in \mathbf{L}} z_l \leq R \tag{13}$$

$$p_l^i x_l = (z_l + \hat{v_l}^i - z_l \hat{v_l}^i)[\delta_{o(l)}^i - \delta_{d(l)}^i], \quad \forall l \in \mathbf{L}, i = 1, ..., k \tag{14}$$

$$\sum_{j \in \mathbf{Jn}} g_j^i - \sum_{l|o(l)=n} p_l^i + \sum_{l|d(l)=n} p_l^i + d_n^i = D_n, \quad \forall n \in \mathbf{N}, \forall i = 1, ..., k \tag{15}$$

$$-P_l \leq p_l^i \leq P_l, \ \forall l \in \mathbf{L}, \forall i = 1, ..., k \tag{16}$$

$$0 \leq g_j^i \leq G_j, \ \forall j \in \mathbf{J}, \forall i = 1, ..., k \tag{17}$$

$$0 \leq d_n^i \leq D_n, \ \forall n \in \mathbf{N}, \forall i = 1, ..., k \tag{18}$$

$$-\overline{\delta} \leq \delta_n^i \leq \overline{\delta}, \ \forall n \in \mathbf{N}, \forall i = 1, ..., k \tag{19}$$

$$z_l \in \{0, 1\}, \ \forall l \in \mathbf{L}. \tag{20}$$

Note that the constraints (14) are nonlinear. By adopting big-M method, we can easily linearize them. Specifically, let M be a sufficiently large real number. For any attack scenario $\hat{\mathbf{v}}^i$, we partition the set of transmission lines into two subsets: attacked lines $\mathbf{L}_\alpha^i$ and lines without attack $\mathbf{L}_\beta^i$, where $\mathbf{L}_\alpha^i = \{l|\hat{v}_l^i = 0, l \in \mathbf{L}\}$ and $\mathbf{L}_\beta^i = \{l|\hat{v}_l^i = 1, l \in \mathbf{L}\}$. For the attacked transmission lines ($l \in \mathbf{L}_\alpha^i$), (14) are replaced by a set of following constraints:

$$p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \leq M(1 - z_l), \ \forall l \in \mathbf{L}_\alpha^i$$
$$p_l^i x_l - [\delta_{o(l)}^i - \delta_{d(l)}^i] \geq M(z_l - 1), \ \forall l \in \mathbf{L}_\alpha^i$$
$$-P_l z_l \leq p_l^i \leq P_l z_l, \ \forall l \in \mathbf{L}_\alpha^i.$$

For the lines without attacks ($l \in \mathbf{L}_\beta^i$), (14) are replaced by $p_l^i x_l = \delta_{o(l)}^i - \delta_{d(l)}^i, \ \forall l \in \mathbf{L}_\beta^i$. As a result, MP, which is a single level mixed integer programming problem, can be readily solved by a professional mixed integer programming (MIP) solver. We point it out that because $\hat{\mathbf{V}}$ is a subset of $\mathbb{V}$, compared to the complete defender-attacker-defender model formation in (1)-(10), MP is a relaxation and therefore provides a lower bound value [22].

4.2. Subproblem

SP serves the function to identify the worst attack plan for a given protection decision. Hence, given protection plan $\hat{\mathbf{z}}$, where $\hat{\mathbf{z}} = \{\hat{z}_l, \forall l \in \mathbf{L}\}$, the corresponding SP is the following bi-level max-min problem:

$$\max_{\mathbf{v}\in\mathbb{V}} \min_{\{p_l,g_j,d_n,\delta_n\}} \sum_{n\in\mathbf{N}} d_n \tag{21}$$

$$st. \sum_{l\in\mathbf{L}} (1-v_l) \le S \tag{22}$$

$$p_l x_l - (\hat{z}_l + v_l - \hat{z}_l v_l)[\delta_{o(l)} - \delta_{d(l)}] = 0, \ \forall l \in \mathbf{L} \tag{23}$$

$$-P_l \le p_l \le P_l, \ \forall l \in \mathbf{L} \tag{24}$$

$$\sum_{j\in\mathbf{Jn}} g_j - \sum_{l|o(l)=n} p_l + \sum_{l|d(l)=n} p_l + d_n = D_n, \quad \forall n \in \mathbf{N} \tag{25}$$

$$0 \le g_j \le G_j, \ \forall j \in \mathbf{J} \tag{26}$$

$$0 \le d_n \le D_n, \ \forall n \in \mathbf{N} \tag{27}$$

$$-\overline{\delta} \le \delta_n \le \overline{\delta}, \ \forall n \in \mathbf{N} \tag{28}$$

$$v_l \in \{0,1\}, \ \forall l \in \mathbf{L}. \tag{29}$$

Based on a given protection plan $\hat{\mathbf{z}}$, the transmission lines can be divided into two subsets: unprotected lines $\mathbf{L}_a$ and protected lines $\mathbf{L}_b$, where $\mathbf{L}_a = \{l|\hat{z}_l = 0, l \in \mathbf{L}\}$ and $\mathbf{L}_b = \{l|\hat{z}_l = 1, l \in \mathbf{L}\}$. For the unprotected lines in $\mathbf{L}_a$, (23) and (24) are replaced by a set of following constraints:

$$p_l x_l - [\delta_{o(l)} - \delta_{d(l)}] \le M(1-v_l), \ \forall l \in \mathbf{L}_a \tag{30}$$

$$p_l x_l - [\delta_{o(l)} - \delta_{d(l)}] \ge M(v_l - 1), \ \forall l \in \mathbf{L}_a \tag{31}$$

$$-P_l v_l \le p_l \le P_l v_l, \ \forall l \in \mathbf{L}_a. \tag{32}$$

For the protected lines in $\mathbf{L}_b$, (23) and (24) are replaced by:

$$p_l x_l = \delta_{o(l)} - \delta_{d(l)}, \ \forall l \in \mathbf{L}_b \tag{33}$$

$$-P_l \le p_l \le P_l, \ \forall l \in \mathbf{L}_b. \tag{34}$$

Since the lower level problem of SP is a single level minimization linear program and always feasible for any attack, through strong duality, we obtain a single level maximization problem (35)-(46). In the following formulation (35)-(46), λ_n is the dual variable for (25), γ_j is the dual variable for (26), α_n is the dual variable for (27), ξ_n and χ_n are the dual variables for (28), β_l and τ_l are the dual variables for (30) and (31), θ_l and ρ_l are dual variables for (32), μ_l is the dual variable for (33), ϕ_l and φ_l are the dual variables for (34).

$$\max \sum_{l\in\mathbf{L}_b} P_l(\phi_l - \varphi_l) + \sum_{l\in\mathbf{L}_a} M(1-v_l)(\beta_l - \tau_l) + \sum_{j\in\mathbf{J}} G_j\gamma_j + \sum_{n\in\mathbf{N}} \overline{\delta}(\xi_n - \chi_n) + \sum_{n\in\mathbf{N}} D_n\alpha_n + \sum_{l\in\mathbf{L}_a} P_l(\theta_l - \rho_l)v_l \tag{35}$$

$$st. \sum_{l\in\mathbf{L}} (1-v_l) \le S \tag{36}$$

$$\mu_l + \phi_l + \varphi_l - \lambda_{n|o(l)=n} + \lambda_{n|d(l)=n} = 0, \quad \forall l \in \mathbf{L}_b \tag{37}$$

$$\beta_l + \tau_l + \theta_l + \rho_l - \lambda_{n|o(l)=n} + \lambda_{n|d(l)=n} = 0, \quad \forall l \in \mathbf{L}_a \tag{38}$$

$$\gamma_j + \lambda_{n|j\in\mathbf{Jn}} \le 0, \ \forall j \in \mathbf{J} \tag{39}$$

$$\sum_{l\in\mathbf{L}_b,d(l)=n} \mu_l - \sum_{l\in\mathbf{L}_b,o(l)=n} \mu_l - \sum_{l\in\mathbf{L}_a,o(l)=n} (\beta_l + \tau_l) + \sum_{l\in\mathbf{L}_a,d(l)=n} (\beta_l + \tau_l) + (\chi_n + \xi_n)x_l = 0, \ \forall n \in \mathbf{N}$$

$$\lambda_n + \alpha_n \le 1, \ \forall n \in \mathbf{N} \tag{40}$$

$$v_l \in \{0,1\}, \quad \forall l \in \mathbf{L} \tag{41}$$

$$\gamma_j \le 0, \ \forall j \in \mathbf{J} \tag{42}$$

$$\xi_n \le 0, \alpha_n \le 0, \ \forall n \in \mathbf{N} \tag{43}$$

$$\chi_n \ge 0, \lambda_n \ free, \ \forall n \in \mathbf{N} \tag{44}$$

$$\beta_l \le 0, \theta_l \le 0, \tau_l \ge 0, \rho_l \ge 0, \ \forall l \in \mathbf{L}_a \tag{45}$$

$$\mu_l \ free, \phi_l \le 0, \varphi_l \ge 0, \ \forall l \in \mathbf{L}_b \tag{46}$$

Again, since v_l is a binary variable, linearization of the nonlinear terms in (35) can be obtained by using big-M method. Thus, we obtain the linearized formulation of SP. Hence, SP can also be solved by a professional MIP solver.

4.3. Algorithm Implementation

Next, we present the implementation steps of our $C\&CG$ algorithm. The optimality tolerance gap of our algorithm is ϵ.

Step 1 Initialization: set the lower bound $LB = -\infty$, the upper bound $UB = \infty$, and the set of attack plan $\hat{\mathbf{V}}$ to be empty with iteration index $k = 1$.

Step 2 Solve MP (11)-(20), obtain its optimal value $objMP$ and a protection decision $\hat{\mathbf{z}}$, and update LB with $objMP$.

Step 3 Solve SP (35)-(46), obtain its optimal value $objSP$ and an optimal attack $\hat{\mathbf{v}}^k$. Then, update $UB = min\{UB, objSP\}$, add $\hat{\mathbf{v}}^k$ to $\hat{\mathbf{V}}$, create dispatch variables $(\mathbf{p}^k, \mathbf{g}^k, \mathbf{d}^k, \boldsymbol{\delta}^k)$, and add the following constraints to MP:

$$\alpha \geq \sum_{n \in \mathbf{N}} d_n^k$$

$$p_l^k x_l - [\delta_{o(l)}^k - \delta_{d(l)}^k] \leq M(1 - z_l), \forall l \in \mathbf{L}_\alpha^k \quad (47)$$

$$p_l^k x_l - [\delta_{o(l)}^k - \delta_{d(l)}^k] \geq M(z_l - 1), \forall l \in \mathbf{L}_\alpha^k \quad (48)$$

$$-P_l z_l \leq p_l^k \leq P_l z_l, \ \forall l \in \mathbf{L}_\alpha^k \quad (49)$$

$$p_l^k x_l = \delta_{o(l)}^k - \delta_{d(l)}^k, \ \forall l \in \mathbf{L}_\beta^k \quad (50)$$

$$-P_l \leq p_l^k \leq P_l, \ \forall l \in \mathbf{L}_\beta^k \quad (51)$$

$$\sum_{j \in \mathbf{Jn}} g_j^k - \sum_{l|o(l)=n} p_l^k + \sum_{l|d(l)=n} p_l^k + d_n^k = D_n, \forall n \in \mathbf{N} \quad (52)$$

$$0 \leq g_j^k \leq G_j, \ \forall j \in \mathbf{J} \quad (53)$$

$$0 \leq d_n^k \leq D_n, \ \forall n \in \mathbf{N} \quad (54)$$

$$-\overline{\delta} \leq \delta_n^k \leq \overline{\delta}, \ \forall n \in \mathbf{N}. \quad (55)$$

Step 4 If $(UB - LB)/LB \leq \epsilon$, stop; otherwise, $k \leftarrow k + 1$ and go to Step 2. ■

5. Computational results

We apply our method to IEEE one-area RTS-1996 system [10]. This system consists of 24 buses, 38 lines, 32 generators, and 17 loads, as illustrated in Figure 1. Circuits sharing the same towers are treated as independent lines. The algorithm is implemented with CPLEX 12.4 in C++ on top of an Intel dual core 3.00GHz, 4GB memory PC. The optimality tolerance gap ϵ is set at 0.1%.

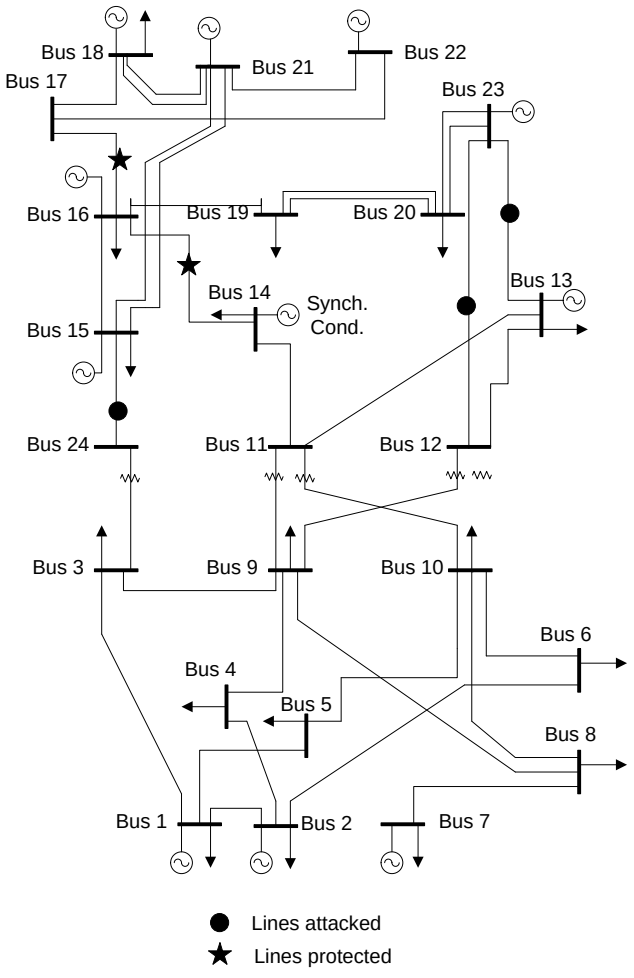

Figure 1: Reliability test system and the optimal solution of DAD for R=2, S=3

As an example, an optimal solution for the defender-attacker-defender model with protection budget two and attack budget three is illustrated in Figure 1. The best protection plan in this case is to protect line 14-16 and 16-17. We present the optimal load shed and computational time for all instances with attack budget $S = 1$ to 12 and protection budget $R = 0$ to 4 in Table 1 and Table 2, respectively. As can be seen, for each column of Table 1, the load shed is non-decreasing with the increase of attack budget S. This observation reveals that, generally, the attacker could cause more damage to a power gird with more attacking resources available. For each row, the load shed is non-increasing with an increasing protection budget R except for the cases with anticipated attack

Table 1: Load shed (MW) for IEEE One-Area RTS-96 System

S	$R=0$	$R=1$	$R=2$	$R=3$	$R=4$
1	0	0	0	0	0
2	194	151	136	118	118
3	618	571	422	377	266
4	922	733	618	571	492
5	1037	843	733	673	571
6	1057	969	788	731	676
7	1278	1057	898	808	761
8	1393	1265	1013	885	770
9	1413	1285	1013	885	825
10	1448	1320	1068	940	849
11	1468	1340	1103	975	927
12	1532	1404	1218	1052	927

Table 2: Computation time (s) for IEEE One-Area RTS-96 System

S	$R=0$	$R=1$	$R=2$	$R=3$	$R=4$
1	0.15	0.12	0.14	0.17	0.25
2	0.45	0.75	1.13	1.54	2.36
3	0.75	1.40	2.67	3.30	5.45
4	1.61	2.52	5.47	10.19	7.29
5	5.50	8.76	17.98	21.40	40.83
6	11.25	20.52	28.69	65.50	88.25
7	16.69	28.32	75.07	113.97	246.82
8	10.09	36.19	74.30	191.33	108.11
9	32.73	84.33	154.69	196.03	632.63
10	10.99	44.34	69.01	199.20	517.46
11	24.79	53.11	157.64	243.46	423.58
12	12.65	16.60	59.99	144.23	323.68

budget to be 1, i.e., $S = 1$. This observation reveals that adding defensive resources will always improve the power grid survivability considering multiple attacks on the grid.

Our algorithm demonstrates a superior computational performance over the other exact algorithm in [7], especially for complicated cases. Figure 2 presents the computational time (averaged over R from 0 to 4) of our algorithm compared with those made by the implicit enumeration method in [7], which are generated on a Sun Fire X4140 X64 with 2 processors at 2.3 GHz and 8GB RAM using MATLAB/CPLEX 11.0 under GAMS. Note that the computation time of the implicit enumeration method increases almost exponentially to over 2000 seconds with the number of interdicted lines (S) from 1 to 12. On the contrary, the computation time of Column-and-Constraint Generation algorithm increases at much a slower rate and is much less sensitive to S.

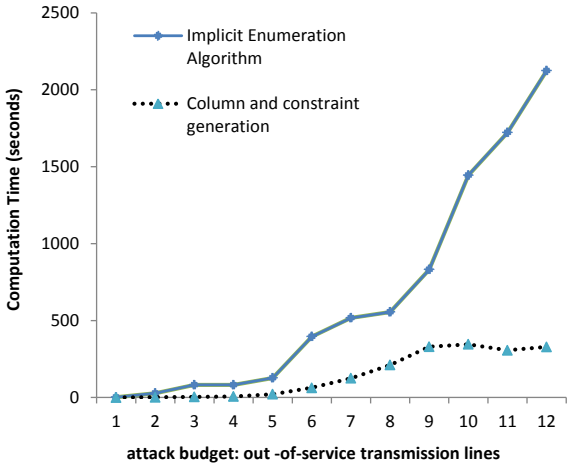

Figure 2: Comparison of computational time between the implicit enumeration [7] and the Column-and-Constraint Generation methods

6. The importance of optimal protection

To verify the conclusion that a protection plan based on a defender-attacker-defender model is better than that of an attacker-defender model with the same protection budget, we conduct a study to compare the protection plans from the attacker-defender model and the defender-attacker-defender model. The attacker-defender model is obtained by setting protection budget to zero and fixing all protection variables to zero in formulation (1)-(10). Load sheds of no protection and of different protection plans are computed under worst-case interdiction with attack budget S from 1 to 4. Specifically, load shed of no protection is obtained from the attacker-defender model directly. The protection plan from the attacker-defender model is the set of transmission lines in the most destructive interdiction

Table 3: Comparison between AD and DAD

S	No protection load shed (MW)	AD		DAD (R=S)	
		protected lines	load shed (MW)	protected lines	load shed (MW)
1	0	None	0	None	0
2	194	11-14, 14-16	151	14-16, 17-22	136
3	618	15-21A, 15-21B,16-17	571	13-23, 14-16,16-17	377
4	922	3-24,12-23, 13-23,14-16	733	12-23,14-16, 16-17,17-22	492

plan, which is the optimal solution of the attacker-defender model. After forcing those critical components to be protected, we solve the attacker-defender model again to obtain load sheds. Load sheds of optimal protection plans are simply obtained by solving the defender-attacker-defender model with $R = S$. Table 3 presents the protection plans and load sheds. As can be seen, even though both the attacker-defender model and the defender-attacker-defender model improve power grid survivability by reducing system load shed under contingency, the attacker-defender model fails to derive the optimal protection plan and leads to more load shed than that of the defender-attacker-defender model. Actually, the protection plans from the attacker-defender model could cause 50% more load shed, compared to the optimal protection plans from the defender-attacker-defender model. This result not only confirms the observations made by Brown et al. [4] and Yao et al. [21], but also further highlights the drastic difference between the attacker-defender model and the defender-attacker-defender model.

To investigate the effectiveness of allocating defensive resources on power grids based on the defender-attacker-defender model, we conduct experiments with different protection and attack budgets. Figure 3 presents the load shed of the power grid under different protection and attack budgets. Note that, as a general rule, the benefit of protecting transmission assets is always positive. When the attack budget S is small, e.g. less than 2 lines will be attacked, such a benefit is marginal, which concurs an observation made in Bier et al. [2] that protection may not be cost-effective. However, when S becomes larger, e.g. $S \geq 3$, the benefit of protection becomes more significant. In deed, typically more than $\frac{1}{3}$ load shed can be reduced with up to 4 lines protected. Given that, practitioners can select an appropriate protection plan to achieve their desired trade-off between cost and benefit.

In the empirical study of their computationally-friendly hardening (i.e. protection) method, Bier et al. [2] observe that hardening could have a negative impact on the system. They believe it is possibly due to the greedy nature of the *Max Line interdiction algorithm* for attack computation. To identify the true reason behind and to better understand the connection between attack and protection, we study their hardening method [2] and compare it with the defender-attacker-defender model.

We first implement the Max Line interdiction algorithm and investigate its effectiveness, compared with that of the attacker-defender model. We compute power grid load sheds for out-of-service transmission lines, i.e., the budget of attack, from 1 to 12. As a fast heuristic procedure, the Max Line interdiction algorithm performs well when the attack budget S is small. Nevertheless, it is not sensitive to S and could not generate optimal, i.e., most destructive, attack plans.

We then investigate the protection impact using the defender-attacker-defender model and the hardening method in [2]. Results are presented in

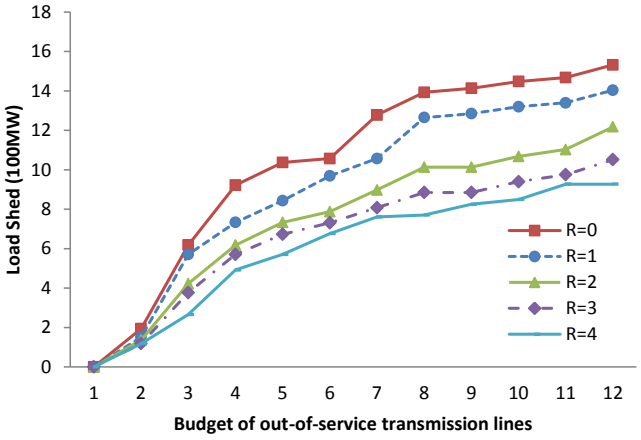

Figure 3: Load shed with different protection budgets (R)

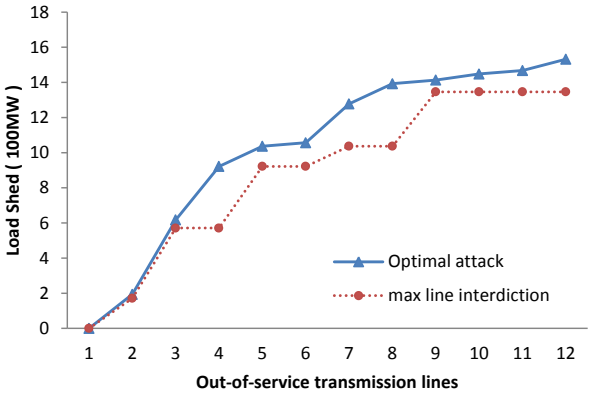

Figure 4: Performance of the Max Line interdiction algorithm in [2]

Figure 5 where protection budget is set as 2 and 4, respectively. H1 and H2 stand for the results with 2 lines and 4 lines hardened respectively, obtained by setting the Max Line interdiction iteration limit to 15, the hardening iteration to 1 and 2, respectively, and the hardening batch size to 2 [2]. As observed in Figure 5, for attacks with budget 5, 6, and 7, load sheds of H2 are more than those of H1, whereas H2 has 4 lines protected and H1 only has 2 lines protected. This observation may lead us to draw the same conclusion as in [2] that hardening could have a negative impact by incurring slight increase in load shed. If optimal protection plans are adopted, as shown in the dashed lines obtained by the defender-attacker-defender model with $R = 2$ and $R = 4$ in Figure 5 (also in Figure 3), protection does not make negative impact on the system performance.

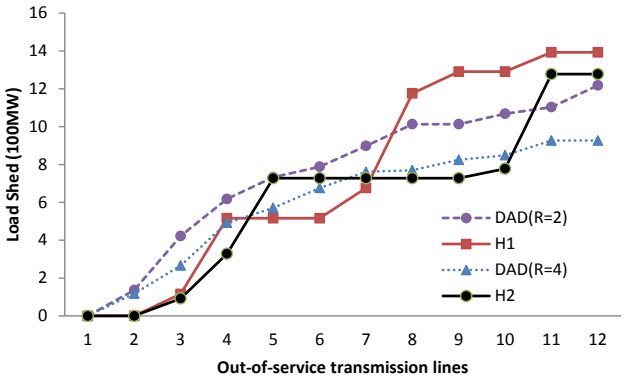

Figure 5: Performance of the hardening method in [2]

One explanation is that the hardening method may not precisely evaluate protection plans. Given that the Max Line interdiction algorithm can not identify optimal attack plans, load shed computed by the hardening method will underestimate the exact load shed. For example, load sheds represented by H1 could be less than optimal results represented by DAD($R = 2$). Similar observations can be seen comparing H2 and DAD($R = 4$). Therefore, together with the results in Table 3, we believe that: if we can not identify optimal targets of an attacker, we can not properly evaluate or derive effective protection plans.

7. Conclusion

This paper presents a new approach to solve a defender-attacker-defender model on power grids. The proposed Column-and-Constraint Generation algorithm finds the optimal protection plan within acceptable computational time, which significantly outperforms existing exact solution method. Case studies on IEEE one-area RTS-1996 system have been done to verify the effectiveness of optimally allocating defensive resources to hedge against terrorist attacks.

Transmission line switching, including the consequently islanding effect, is studied recently as an effective method to improve power grid operations [6, 8, 23] under various contingencies. Because the defender has the capability to disconnect transmission lines after attacks, the attacker-defender problem will a mixed integer lower-level problem,

which cannot be simply approximated by a linear program. Indeed, the optimal (i.e. the most destructive) attacks could be very different from those if line switching is ignored [6, 23]. So, as a future direction, it would be interesting to extend our study to investigate the impact of building line switching capability and how it affects the defensive resource allocation within the defender-attacker-defender framework.

8. Acknowledgement

The authors would like to acknowledge Dr. Jose M. Arroyo and Dr. Natalia Alguacil from School of Industrial Engineering at University of Castilla-La Mancha for their open discussions on power grid protection. We also thank Dr. Javier Salmeron from Department of Operations Research at the Naval Postgraduate School for discussing with us and sharing his opinions.

References

[1] G.E. Apostolakis, D.M. Lemon, A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism, Risk Analysis 25 (2005) 361–376.

[2] V. Bier, E. Gratz, N. Haphuriwat, W. Magua, K. Wierzbicki, Methodology for identifying near-optimal interdiction strategies for a power transmission system, Reliability Engineering & System Safety 92 (2007) 1155–1161.

[3] G. Brown, M. Carlyle, J. Salmeron, K. Wood, Analyzing the vulnerability of critical infrastructure to attack and planning defenses, in: Tutorials in Operations Research, INFORMS, 2005, pp. 102–123.

[4] G. Brown, M. Carlyle, J. Salmeron, K. Wood, Defending critical infrastructure, Interfaces 36 (2006) 530–544.

[5] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; National Research Council, Terrorism and the Electric Power Delivery System, The National Academies Press, 2012.

[6] A. Delgadillo, J. Arroyo, N. Alguacil, Analysis of electric grid interdiction with line switching, Power Systems, IEEE Transactions on 25 (2010) 633–641.

[7] A. Delgadillo, J. Arroyo, N. Alguacil, Power system defense planning against multiple contingencies, in: 17th Power Systems Computation Conference (PSCC11), Stockholm.

[8] N. Fan, D. Izraelevitz, F. Pan, P. Pardalos, J. Wang, A mixed integer programming approach for optimal power grid intentional islanding, Energy Systems 3 (2012) 1–17.

[9] J. Glover, M. Sarma, T. Overbye, Power System Analysis and Design: Fifth Edition, Thomson Engineering, 2011.

[10] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, C. Singh, The IEEE reliability test system–1996, Power Systems, IEEE Transactions on 14 (1999) 1010–1020.

[11] K. Hausken, Strategic defense and attack for reliability systems, Reliability Engineering & System Safety 93 (2008) 1740–1750.

[12] K. Hausken, G. Levitin, Minmax defense strategy for complex multi-state systems, Reliability Engineering & System Safety 94 (2009) 577–587.

[13] E. Israeli, System interdiction and defense, Ph.D. thesis, Monterey, California: Naval Postgraduate School; Springfield, Va.: Available from National Technical Information Service, 1999.

[14] B. John Garrick, J.E. Hall, M. Kilger, J.C. McDonald, T. O'Toole, P.S. Probst, E. Rindskopf Parker, R. Rosenthal, A.W. Trivelpiece, L.A. Van Arsdale, et al., Confronting the risks of terrorism: making the right decisions, Reliability Engineering & System Safety 86 (2004) 129–176.

[15] G. Levitin, H. Ben-Haim, Importance of protections against intentional attacks, Reliability Engineering & System Safety 93 (2008) 639–646.

[16] A. Motto, J. Arroyo, F. Galiana, A mixed-integer lp procedure for the analysis of electric grid security under disruptive threat, Power Systems, IEEE Transactions on 20 (2005) 1357–1365.

[17] S.A. Patterson, G.E. Apostolakis, Identification of critical locations across multiple infrastructures for terrorist actions, Reliability Engineering & System Safety 92 (2007) 1183–1203.

[18] J. Salmeron, K. Wood, R. Baldick, Analysis of electric grid security under terrorist threat, Power Systems, IEEE Transactions on 19 (2004) 905–912.

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

[20] A. Wood, B. Wollenberg, Power generation, operation, and control, Wiley New York, 1996.

[21] Y. Yao, T. Edmunds, D. Papageorgiou, R. Alvarez, Trilevel optimization in power network defense, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on 37 (2007) 712–718.

[22] B. Zeng, L. Zhao, Solving two-stage robust optimiza-

tion problems using a column-and-constraint generation method, to appear in *Operations Research Letters*, University of South Florida, 2011.

[23] L. Zhao, B. Zeng, An Exact Algorithm for Power Grid Interdiction Problem with Line Switching, Submitted, available in *optimization-online*, University of South Florida, 2011.

[24] R. Zimmerman, C. Restrepo, J. Simonoff, L. Lave, 14. risk and economic costs of a terrorist attack on the electric system, The Economic Costs and Consequences of Terrorism (2008) 273.

[25] E. Zio, Reliability engineering: Old problems and new challenges, Reliability Engineering & System Safety 94 (2009) 125–141.

[26] E. Zio, L.R. Golea, G. Sansavini, Optimizing protections against cascades in network systems: A modified binary differential evolution algorithm, Reliability Engineering & System Safety 103 (2012) 72–83.