IEEE TRANSACTIONS ON
POWER SYSTEMS
IEEE POWER & ENERGY SOCIETY

An Efficient Tri-level Optimization Model for Electric Grid Defense Planning

Xuan Wu, *Member, IEEE*, and Antonio J. Conejo, *Fellow, IEEE*

***Abstract*—The work reported in this paper aims at developing a practical and efficient tool for utility transmission planners to protect critical transmission assets from potential physical attacks. A trilevel min-max-min optimization model is proposed to represent actions of a planner, an attacker and an operator. These three agents share a common objective function, which is the system load shedding. The strong duality theorem is used to merge the middle- and lower-level problems into a single-level one. The resulting mixed-integer bilevel model is solved by a Benders decomposition technique using primal cuts. Two case studies are presented as applications of this novel technique. Additionally, the proposed technique is compared with an implicit enumeration algorithm.**

***Index Terms* -- Trilevel optimization, physical attack, transmission protection, Benders decomposition**

I. Introduction

THE electric grid is a critical infrastructure that enables the supply of electricity to customers including hospitals, government facilities, industries and others. As a result, the electric grid is attracting increasing interests from potential physical attackers that intend to greatly disrupt power supply to damage the economy or create chaos. In the context of this paper a "physical attack" is the disabling of one or several transmission lines or power transformers. Most parts of the high-voltage electric grid in the US are located in rural areas with low or no security to withstand. In 2013, an attack called "Meltcalf Incident" occurred at the Meltcalf substation in California, which damaged 17 transformers and caused a loss of at least 15 million dollars [1]. This indicates that the electric grid around Meltcalf substation was not well-prepared to withstand physical attacks. However, it is not that difficult to protect some transmission facilities including substations and lines. For example, it is possible to increase the substation fence/wall perimeters and the heights of transmission lines to protect substation equipment, and transmission lines from, for instance, gunshots attack. However, it would be very costly to protect every single facility. As a result, this paper provides a methodology for utilities to select the most critical facilities to protect so that the worst-case load shedding after attack can be minimized. As a result, utilities may use the proposed model and algorithm to find efficiently their best transmission assets protection plans considering their available budget.

Related to the work in this paper, two models are reported in the literature, the attacker-defender model (AD) and the defender-attacker-defender model (DAD).

Reference [2] developed a pioneering AD model. This AD model includes an upper-level problem whose objective is maximizing the attacker's disruptions and a lower-level problem whose objective is minimizing the resulting disruptions (Fig. 1). These authors proposed a decomposition-based heuristic method to solve the resulting mixed-integer bilevel optimization problem. Then, the same authors developed a new approach called Global Benders Decomposition (GLBD) method [3] to replace the heuristic method. The GLBD method is based on adding cuts to the master problem using sensitivities that reflect the impact of changing the corresponding master problem binary variable in the subproblem. However, these sensitivities are difficult to compute if the subproblem is discontinuous and may lead to inaccurate solutions. This is why we propose a new approach. In addition, references [4] and [5] utilized the strong duality theorem and Karush-Kuhn-Tucker (KKT) optimality conditions, respectively, to convert the AD bilevel problem into a single-level problem, which can then be solved using mixed-integer linear programming solvers.

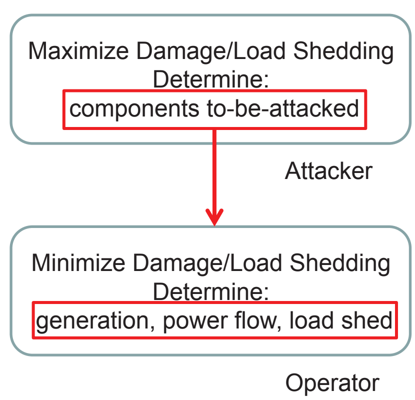

Fig. 1. Attacker-operator model in the interdiction analysis

The DAD model is built based on the AD model, and was originally proposed in [6]. Reference [7] used a heuristic approach to solve this model, which could be biased due to the limitations of the proposed heuristic. Reference [8] used game

This work is partially supported by NSF grant 1548015.

X. Wu is with the ECE Department, The Ohio State University, Columbus, OH 43210 USA (e-mail: wu.3018@osu.edu), and with the Station Engineering Department, American Electric Power, Columbus, OH.

A. J. Conejo is with the ISE and ECE Departments, The Ohio State University, Columbus, OH 43210 USA (e-mail: conejonavarro.1@osu.edu).

Digital Object Identifier 10.1109/TPWRS.2016.2628887

theory as the solution technique, which was novel and simple, but unsuitable for complex real-world applications. Reference [9] applied trilevel optimization theory to formulate the DAD model mathematically and proposed a decomposition-based method to iterate between the outer problem and the bilevel inner problem. Recently, reference [10] used the algorithm developed in [11] to solve this trilevel optimization problem. However, this algorithm might not be applicable for large-scale electric grids due to long computational times or stringent hardware requirement.

Within the framework of these previous works, this paper considers a DAD model, illustrated as a planner-attacker-operator model in Fig. 2.

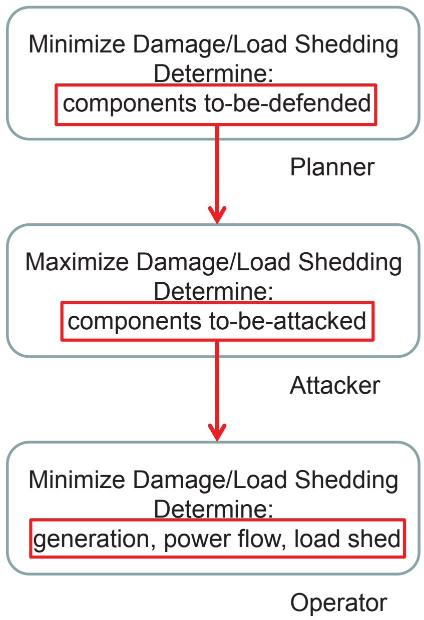

Fig. 2. Planner-attacker-operator model in the electric grid defense planning problem

The planner represents the transmission operator that wishes to create effective defense plans to protect the electric grids from possible physical attacks without exceeding budget limits or defense resource limits. In other words, the planner wishes to minimize load shedding by determining the components to be defended. Oppositely, the attacker knows which components are protected and then determines which components to attack in order to maximize load shedding. In this paper, a rational attacker is considered. If the attacker does not act rationally, the damage will not be maximized. From the planner/defender's perspective, the worst-case attack plan is the only target, which needs to be mitigated by choosing an appropriate protection plan. Once the appropriate protection plan has been determined by the proposed algorithm, no larger damage than that pertaining to the situation of the attacker acting rationally (using the worst-case attack plan) is possible. Once the attacked components are out of service, the system operator modifies the system operating variables to minimize load shedding. This way the system damage is reduced to a minimum. Thus, the earliest decision is made by the planner at the upper-level, the next one by the attacker at the middle-level, and the last one by the operator at the lower-level. As a result, it is not possible to consider that the attacker has only partial information of the planner's defense action. Nevertheless, note that the worst condition corresponds to the case of an attacker with full information.

Mathematically, the proposed model (Fig. 2) can be recast as a min-max-min trilevel problem. Note that both upper-level and middle-level problems include sets of binary variables that represent defense and attack plans. Trilevel problems are hard to solve. However, using duality theory, the two inner level problems (max-min) can be merged into a single level (max) problem. This results in a final min-max problem with two sets of binary variables, one per level. A Benders primal decomposition method is proposed in this paper to solve this min-max problem, which results in an efficient solution algorithm.

Note that the lower-level problem must include both upper-level and middle-level variables information, otherwise the proposed algorithm cannot be applied. Therefore, we propose a revisited formulation as compared to previous formulations [10].

The major contributions of this paper are listed below:

1. A new efficient algorithm is proposed to solve the planner-attacker-operator model based on Benders decomposition with primal cuts.
2. Comprehensive numerical studies are carried out to show the computational efficiency of the proposed algorithm.

II. Problem Formulation

A. Assumptions

In this paper we assume that the attacker is rational enough to attack the most significant assets of the electric grid, which can be easily identified as higher-voltage transmission assets (≥69 kV). They can be categorized as transmission line assets, which are outside of the substation fences and visible/reachable by potential attackers, and transmission substation assets which are inside the fences and visible/reachable with difficulty by potential attackers. Even though destroying one entire substation or one substation bus can cause all the incoming transmission lines that are connected to that attacked substation or bus to be tripped out together, it is not easy to make this happen and complex for the attackers due to the substation fences and multiple components to be attacked. Conversely, damaging the transmission line suspension insulators or the transformer bushings is easier and may drive the corresponding line or transformer into fault condition and out of service. As a result, this paper focuses on attacks to transmission lines or transformers. In addition, we assume that the attacker can attack multiple elements (transmission lines or power transformers) simultaneously. For instance, there are more and more 345 kV double-circuit tower corridors in the PJM network, which provide easier opportunities for an attacker to simultaneously disable two parallel circuits on the same tower due to their proximity. Note that this is a conservative assumption from the planner point of view. In turn, the system operator re-dispatches the system to minimize load shedding.

We consider the ramping limits of the generating units in the proposed model and case studies. Specifically, we set the ramping-up limit as the unit capacity (default setting) and as a certain percentage of each unit capacity. Additionally, the ramping-down limit is implicitly set to the capacity of each unit by allowing the possibility of attacking one or several lines to isolate the unit.

On the other hand, we consider the worst-case situation in which the attacker disables the transmission lines/transformers permanently until the linemen's repair. In other words, the network topology is changed after the attack and remains so for at least several hours. As a result, the power flow of other lines should be restricted by their steady-state capacity constraints as in optimal power flow problems.

Note that N-1 security is equivalent to single-element attack security in the defense planning problem. Thus, if the system operator enforces N-1 security, the attacker needs at least to attack two elements to achieve any load shedding. N-1 security is not enforced in the pre-attack state, but can be easily incorporated at the cost of higher computational burden.

B. Notation

Indices and sets:

j	generator index
l	transmission line index
n	bus index
J	set of indices of generators
J_n	set of indices of generators connected to bus n
L	set of indices of transmission lines
N	set of indices of buses

Variables:

a_l	binary variable representing the attack to line l: 0 if attacked and 1 otherwise
d_l	binary variable representing the defense to line l: 0 if undefended and 1 otherwise
P_l^F	power flow through line l
P_j^G	power output of generator j
ΔP_n^D	load shedding at bus n
δ_n	voltage angle at bus n
η	master problem objective

Dual variables:

μ_l	dual variable associated with the lth line power flow equation
λ_n	dual variable associated with the nth bus power balance equation
γ_j	dual variable associated with the jth generator capacity
$\overline{\phi_l}$	dual variable associated with the upper bound of the lth line power flow
$\underline{\phi_l}$	dual variable associated with the lower bound of the lth line power flow
$\overline{\alpha_n}$	dual variable associated with the upper bound of the nth bus load shedding

Constants:

Z	attack resource limit in terms of maximum number of simultaneously attacked components
K	defense resource limit in terms of maximum number of protected components
$O(l)$	origin bus of line l
$D(l)$	destination bus of line l
$\overline{P}_j^G$	capacity of generator j
$\overline{P}_l^F$	load flow capacity of line l
P_n^D	load at bus n
RD_j	ramping-down capacity of generator j
RU_j	ramping-up capacity of generator j
$P_{j,0}^G$	power output in pre-attack state of generator j
X_l	reactance of line l
I	maximum number of iterations
ε	convergence parameter

C. Formulation

$$\min_{d\in\Theta}\left\{\max_{a\in\Lambda}\ \min_{p\in P(d,a)}\sum_{n\in N}\Delta P_n^D\right\} \tag{1}$$

where

$$\Theta=\{\,d\mid d_l\in\{0,1\};\ \forall l\in L, \tag{2}$$

$$\sum_{l\in L} d_l\le K\,\} \tag{3}$$

$$\Lambda=\{\,a\mid a_l\in\{0,1\};\ \forall l\in L, \tag{4}$$

$$\sum_{l\in L}(1-a_l)\le Z\,\} \tag{5}$$

$$P(d,a)=\{p: P_l^F=[1-(1-d_l)(1-a_l)]\frac{1}{X_l}\left[\delta_{O(l)}-\delta_{D(l)}\right];\quad \forall l\in L\quad(\mu_l) \tag{6}$$

$$\sum_{j\in J_n}P_j^G-\sum_{l|O(l)=n}P_l^F+\sum_{l|D(l)=n}P_l^F+\Delta P_n^D=P_n^D;\quad \forall n\in N\quad(\lambda_n) \tag{7}$$

$$0\le P_j^G\le\overline{P}_j^G;\quad \forall j\in J\quad\left(\overline{\gamma_j}\right) \tag{8}$$

$$-RD_j\le P_j^G-P_{j,0}^G\le RU_j;\quad \forall j\in J\quad\left(\underline{\chi_j},\overline{\chi_j}\right) \tag{9}$$

$$-\overline{P}_l^F\le P_l^F\le\overline{P}_l^F;\quad \forall l\in L\quad\left(\underline{\phi_l},\overline{\phi_l}\right) \tag{10}$$

$$0\le\Delta P_n^D\le\overline{P}_n^D;\quad \forall n\in N\quad\left(\overline{\alpha_n}\right)\} \tag{11}$$

Problem (1)-(11) includes three optimization levels, which are: 1) planner's upper-level; 2) attacker's middle-level; and 3) operator's lower-level. The three levels have the same objective function (1), which is total load shedding. The planner tries to minimize load shedding through binary variables d_l as shown in constraint (2). If d_l equals to 1, line l is protected and the attacker cannot disable it. Oppositely, line l is vulnerable to a potential attack if d_l equals 0. Constraint (3) states that the planner has a defense resource limit. On the other hand, the attacker uses binary variables a_l to maximize load shedding after the planner has made the protection decisions. If a_l equals 0, line l is under attack. Otherwise, line l is safe. Similarly as in the upper-level problem, the attacker resources are limited by (5). Then, the operator will respond to the loss of lines after the attack by changing the operating control variables P_j^G and ΔP_n^D to minimize load shedding (variables P_l^F and δ_n change as a result). The power flow equation that we propose is (6), which incorporates the impacts of protection (d_l) and attack (a_l) variables. If $d_l = 1$ and $a_l = 1$ or $d_l = 0$ and $a_l = 1$, (6) becomes the standard power flow equation since line l is not attacked. If $d_l = 1$ and $a_l = 0$, (6) also becomes the standard power flow equation since line l is protected and is not attack-able. If $d_l = 0$ and $a_l = 0$, the right-hand side of (6) is zero since line l is not protected and attacked. The node balance equation at bus n is (7) and incorporates load shedding variable ΔP_n^d. Constraint (8) limits the production of each generator. Constraint (9) enforces ramping limits between the pre-attack and the post-attack states. Note that constants $P_{j,0}^G$ are obtained by solving model (6)-(11) with all a_l equal to 1, that is, the pre-attack condition. Similarly, constraint (10) enforces the power flow of line l to be within its capacity limits. Constraint (11) makes the load shedding at each bus smaller than or equal to that bus's demand.

Model (1)-(11) consists of three decision-making levels. In the first level the planner decides which components to protect to create the best protection plan by assuming the attacker's most destructive attack plan; whereas the attack plan is made assuming that the operator responds to the attack by minimizing damage. For instance, consider an example in which there are three lines whose unavailability entail load shedding of 100 MW (line 1), 90 MW (line 2) and 80 MW (line 3). In this example, both the protection and attack resource limits are selected as 1 line. These load shedding values are calculated assuming that the operator operates the system to minimize load shedding once a specific line has been attacked and made unavailable. Therefore, the planner assumes that the second-level attacker's decision would be attacking line 1 since the attacker intends to maximize load shedding. As a result, the planner would protect line 1 and then the worst-case situation is line 2 attacked and the corresponding load shedding is 90 MW instead of 100 MW. The tutorial reference [12] provides additional background information.

III. Solution Technique

The first step for solving this trilevel problem is merging the lower-level and middle-level problems into one single-level problem using either the strong duality theorem [13] or KKT optimality conditions [14]. This is possible because the lower-level problem is linear and thus convex in its optimization variables. As a result, this trilevel problem is transformed into a bilevel problem with binary variables and nonlinear constraints that can be linearized [15]-[17]. Since both the master problem and the subproblem have binary optimization variable vectors (a and d), which prevent directly deriving dual variables (sensitivities) to formulate dual cuts, a Benders primal decomposition method (also called C&CG decomposition method [18]) is used to solve this bilevel problem. Outcomes are compared with those from an implicit enumeration method [19]. Note that in addition to the implicit enumeration method, to the best of authors' knowledge, there is no other existing methods for solving this trilevel planner-attacker-operator model. Since a decomposition-based method is used, a subproblem and a master problem have to be formulated.

A. Subproblem

Duality theory is used below to transform the lower-level problem including its set of constraints (6)-(11) into its equivalent dual problem. Since the lower-level problem becomes linear and convex once the upper-level vector d and the middle-level vector a are fixed, the strong duality theorem indicates that the primal and dual objective function values are equal at the optimum. Thus, the max-min subproblem is transformed into a max-max problem which is a single-level maximization problem. As a result, the subproblem becomes:

$$\begin{aligned}\max_{a,\overline{\phi},\underline{\phi},\overline{\chi},\underline{\chi},\overline{\gamma},\overline{\alpha},\mu,t,h}\; & \sum_{l\in L}\left(\overline{\phi}_l-\underline{\phi}_l\right)\overline{P}_l^F+\sum_{n\in N}\left(\overline{\alpha}_n+\lambda_n\right)P_n^D\\ &+\sum_{j\in J}\left[\overline{\gamma}_j\overline{P}_j^G+\overline{\chi}_jRU_j-\underline{\chi}_jRD_j+\left(\overline{\chi}_j-\underline{\chi}_j\right)P_{j,0}^G\right]\end{aligned}\tag{12}$$

subject to:

$$a_l\in\{0,1\};\quad \forall l\in L\tag{13}$$

$$\sum_{l\in L}\left(1-a_l\right)\le Z\tag{14}$$

$$\begin{aligned}-\sum_{l|O(l)=n}\frac{\left(1-d_l^*\right)}{X_l}t_l+\sum_{l|D(l)=n}\frac{\left(1-d_l^*\right)}{X_l}t_l-\sum_{l|O(l)=n}\frac{d_l^*}{X_l}\mu_l\\ +\sum_{l|D(l)=n}\frac{d_l^*}{X_l}\mu_l=0;\quad \forall l\in L\end{aligned}\tag{15}$$

$$t_l=\mu_l-h_l;\quad \forall l\in L\tag{16}$$

$$\underline{\mu}_l a_l\le t_l\le \overline{\mu}_l a_l;\quad \forall l\in L\tag{17}$$

$$\underline{\mu}_l\left(1-a_l\right)\le h_l\le \overline{\mu}_l\left(1-a_l\right);\quad \forall l\in L\tag{18}$$

$$-\lambda_{O(l)}+\lambda_{D(l)}+\mu_l+\overline{\phi}_l+\underline{\phi}_l=0;\quad \forall l\in L\tag{19}$$

$$\lambda_{n|j\in J_n}+\overline{\gamma}_j+\overline{\chi}_j+\underline{\chi}_j\le 0;\quad \forall j\in J\tag{20}$$

$$\lambda_n+\overline{\alpha}_n\le 1;\quad \forall n\in N\tag{21}$$

$$\overline{\gamma}_j\le 0;\quad \overline{\chi}_j\le 0;\quad \underline{\chi}_j\ge 0;\quad \forall j\in J\tag{22}$$

$$\overline{\phi}_l\le 0;\quad \underline{\phi}_l\ge 0;\quad \forall l\in L\tag{23}$$

$$\overline{\alpha}_n\le 0;\quad \forall n\in N\tag{24}$$

The objective function (12) is equivalent to the original objective function (1) due to the strong duality equality. Constraints (13) and (14) are identical to constraints (4) and (5), respectively. Constraints (15)-(18) are nonlinear dual constraints. Their non-linearities originate from the product of binary and continuous variables. However, these products are easily linearized using two additional sets of continuous variables t_l and h_l. Take the lth line as an example. Based on the dual transform of (6), the following equation is obtained:

$$-\sum_{l|O(l)=n}\frac{\left(1-d_l^*\right)}{X_l}a_l\mu_l+\sum_{l|D(l)=n}\frac{\left(1-d_l^*\right)}{X_l}a_l\mu_l-\sum_{l|O(l)=n}\frac{d_l^*}{X_l}\mu_l+\sum_{l|D(l)=n}\frac{d_l^*}{X_l}\mu_l=0$$

Since a_l is a binary variable and μ_l is a continuous dual variable, their product is non-linear, but can be linearized using the following method: 1) Let t_l be a new continuous variable that represents the product of a_l and μ_l, 2) let h_l be a new continuous variable satisfying (16), and 3) introduce new inequalities (17) and (18). Thus, if a_l is equal to 0, t_l is also equal to 0 (as desired), and h_l is equal to μ_l. Oppositely, if a_l is equal to 1, h_l is equal to 0, and then, t_l is equal to μ_l (as desired). Additionally, since dual variable μ_l is free, its upper and lower bounds which are used in (17) and (18) can be set equal to large enough constants. Constraints (19)-(21) are additional dual constraints. The limits of dual variables (22)-(24) are set based on primal constraints (8)-(11).

B. Master Problem

Considering a Bender's framework, the master problem is then formulated based on (3) and (6)-(11) as follows:

$$\min_{d, P_l^F, P_i^G, \Delta P_i^D, \delta_i, \eta} \quad \eta \tag{25}$$

subject to:

$$\eta \geq \sum_{n \in N} \Delta P_{n,i}{}^D; \forall i \leq I \tag{26}$$

$$\sum_{l \in L} d_{l,i} \leq K; \forall i \leq I \tag{27}$$

$$\begin{aligned} -\left(1-a_{l,i}{}^*\right)\left(1-d_{l,i}\right)M \leq P_{l,i}{}^F - \frac{1}{X_l}\left[\delta_{O(l),i} - \delta_{D(l),i}\right] \\ \leq \left(1-a_{l,i}{}^*\right)\left(1-d_{l,i}\right)M \;; \forall l \in L, \forall i \leq I \end{aligned} \tag{28}$$

$$\sum_{j \in J_n} P_{j,i}{}^G - \sum_{l|O(l)=n} P_{l,i}{}^F + \sum_{l|D(l)=n} P_{l,i}{}^F + \Delta P_{n,i}{}^D = P_{n,i}{}^D; \forall n \in N, \forall i \leq I \tag{29}$$

$$0 \leq P_{j,i}{}^G \leq \overline{P}_j^G; \quad \forall j \in J, \forall i \leq I \tag{30}$$

$$-RD_j \leq P_{j,i}{}^G - P_{j,0}{}^G \leq RU_j; \quad \forall j \in J, \forall i \in I \tag{31}$$

$$\begin{aligned} -\left[a_{l,i}{}^*\overline{P}_l^F + \left(1-a_{l,i}{}^*\right)d_{l,i}\overline{P}_l^F\right] \leq P_{l,i}{}^F \leq a_{l,i}{}^*\overline{P}_l^F + \left(1-a_{l,i}{}^*\right)d_{l,i}\overline{P}_l^F; \\ \forall l \in L, \forall i \leq I \end{aligned} \tag{32}$$

$$0 \leq \Delta P_{n,i}{}^D \leq P_n{}^D; \quad \forall n \in N, \forall i \leq I \tag{33}$$

The optimization variables of master problem (25)-(33) are the auxiliary variable η, the operating variables P_l^F, P_j^G, δ_n and ΔP_n^D, and the defense decisions d. Variables a are fixed ($a = a^*$) in the master problem. In addition, note that all parameters in constraints (26)-(33) incorporate subscript i, which is the iteration counter.

C. Master-Sub Problem Interaction

Fig. 3 clarifies the flow of communication between the master problem and the subproblem.

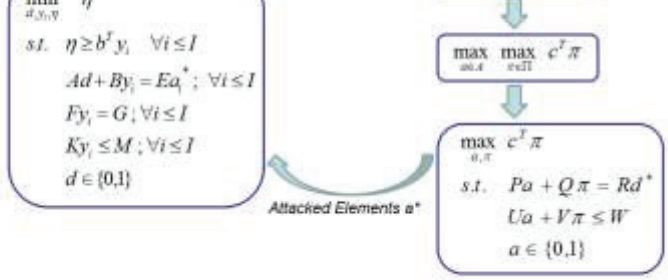

Fig. 3. Illustration of master-sub problem interaction

In Fig. 3, vector y and π generically refer to the operating variables and the dual variables of the lower-level problem, respectively, which are continuous. The constant scalars, matrices and vectors A, B, E, F, G, K, M, P, Q, R, U, V and W correspond to the parameter information of the master problem and the subproblem. The right-hand side of the figure represents the subproblem, given a fixed defense decision vector d^* determined at the master problem. On the other hand, the attack decision vector a^* is obtained after solving the subproblem and transferred to the master problem at each iteration. The subscript i is the iteration counter. All parameter information of iterations prior to the current iteration is kept for future iterations. It should be noted that primal (not dual) information a^* is transferred to the master problem from the subproblem. Another observation is that both the master problem and the subproblem are mixed integer linear programming problems, which can be solved efficiently using standard branch-and-cut solvers.

Therefore, both the master problem and the subproblem should incorporate primal operation information. Additionally, the master problem includes upper-level variables (d_l) while the subproblem includes middle-level variables (a_l). Benders primal decomposition method requires that the lower-level problem includes both upper-level and middle-level variables. And this is the reason why constraint (6) needs to incorporate the upper-level decisions d.

The master problem and the subproblem provide a lower and upper bound, respectively, of the objective function optimal value. The master problem is obtained by partially defining its feasible region, while the subproblem is obtained by fixing the master problem variable vector d. As a result, the master problem and the subproblem are relaxed and further constrained versions, respectively, of the original problem. Therefore, the master problem and the subproblem generate lower and upper bounds, respectively. Both master problem and subproblem interact until the gap between the lower and upper bounds is small enough.

Therefore, the algorithm is described in the following:

Step 0: Set the lower bound (LB) and upper bound (UB) to negative infinity and positive infinity, and set the iteration counter to i=0. Solve the subproblem protecting 0 lines and using the defense resource limit (K) as the attack resource limit (Z). As a result, the model provides the K most vulnerable lines. Then, use the selected lines as current defense decisions d^*_0. Note that the subscription "i" of d means the corresponding defense decisions in iteration i.

Step 1: If i=0, solve the subproblem using d^*_0 obtained in *Step 0*, and update the iteration counter, $i \leftarrow i+1$. Otherwise, solve the subproblem using $d^*_{(i-1)}$ obtained in *Step 2* of iteration *i-1*. Obtain the optimal solution a^* and π^*, and update the upper bound as UB = min{UB, $c^T\pi^*$ }.

Step 2: Solve the master problem using a^* obtained in *Step 1*. Obtain the optimal solution {d^*_i, η}. Update the lower bound as LB = η.

Step 3: If (UB - LB) / UB ≤ ε, return either d^*_{i-1} or d^*_i, whichever leads to the smaller objective function value (the load shedding), and stop, an optimal solution has been found. Otherwise, update the iteration counter, $i \leftarrow i+1$. The algorithm continues in *Step 1*.

D. Computational Considerations

To illustrate the efficiency of the proposed algorithm, we compare it with an implicit enumeration one [11]. The implicit enumeration algorithm explores a tree with nodes and branches. Each node corresponds to an attack decision vector (a) and requires solving the subproblem. Each branch represents one defense decision variable (d_l) obtained based on its up-connected node (a). The criterion of branch development is that the selected defense decision variable (d_l) must be contained in the attack decision vector (a), otherwise the next node will always correspond to the same attack decision vector (a) as the previous node (to maximize load shedding). In order to minimize load shedding, the planner must counteract the attacker's previous choice by protecting at least one of the components to be attacked.

An illustrative example of this algorithm is provided in Fig. 4. If there is no defense, the attacker will attack line 2 and 4. Then, the planner has to choose lines 2 or 4 to protect so as to counteract the attacker's action. The algorithm always chooses the first element, which is line 2, to be protected. After protecting line 2, the subproblem is rerun and the attacker optimally chooses to attack lines 3 and 5 with line 2 being protected. The algorithm continues until the stopping criterion is reached, i.e., the defense resources are used up. More details of this implicit enumeration algorithm can be found in [11].

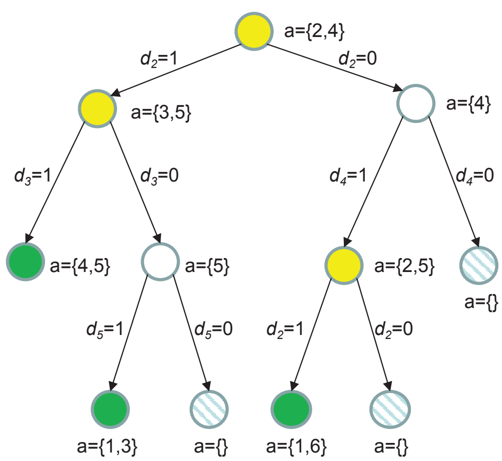

Fig. 4. Illustrative example of using implicit enumeration algorithm

Even though this implicit enumeration algorithm can obtain the globally optimal solution(s) [19], it is too time-consuming. As mentioned in [11], the subproblem could possibly be run as many times as $(Z^{K+1} - 1) / (Z - 1)$. If the attacker is capable of attacking 2 lines simultaneously, and the planner can protect 10 lines, the subproblem needs to be run $(2^{10+1} - 1) / (2 - 1) =$ 2,047 times. Assuming that solving a subproblem for a large system needs 30 seconds on average, the total computational time is 2,047 × 30 = 61,410 seconds ≈ 17 hours. As a result, a more efficient methodology, i.e. Benders primal decomposition method, is needed for larger systems and combinations of defense and attack resource limits.

IV. Numerical Results

In this section, two case studies are presented including a 9-bus system and a 118-bus system. The constants I and ε are defined as 100 and 0.1, respectively, in both case studies. In addition, a comparison between the Benders primal decomposition method and the implicit enumeration method is reported for the 118-bus system case study.

Both methods are implemented on a laptop with an Intel Core i7 CPU running at 2.60 GHz and 8GB of RAM using MATLAB [20]. The optimization solver Gurobi 6.5 [21] is used within MATLAB.

A. WSCC 9-bus System

This WSCC 9-bus test system [22] is a simple equivalent of the Western System Coordinating Council (WSCC). It includes 9 buses, 3 generators and 3 loads, which are connected through 6 lines and 3 transformers as shown in Fig. 5. Generators and lines data are provided in Table I.

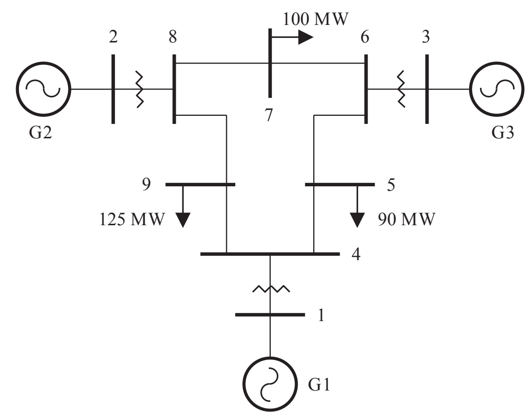

Fig. 5. Single-line diagram of the WSCC 9-bus System

TABLE I
Data for Generators and Lines

Generator	Generator capacity (MW)	Line	Line capacity (MW)
G1	250	1-4	250
G2	300	4-5	250
G3	270	5-6	150
		3-6	300
		6-7	150
		7-8	250
		8-2	250
		8-9	250
		9-4	250

Table II provides outcomes for the worst-case load shedding corresponding to different combinations of attack and defense resource limits. The attacker's capability is represented by the maximum number of attacked lines as shown in the first column of Table II. If the attacker can only attack one line, there is no need to protect any line. However, if the attacker can attack two lines, WSCC has to protect at least five lines to avoid any load shedding. It is clear that the worst-case load shedding decreases and increases with the defense resource limit and attack resource limit, respectively. Note that the protection resource limit (K) plus the attack resource limit (Z) can be larger than the total number of lines according to constraints (3) and (5). For instance, if there are two lines and both are protected (K=2) and the attacker is capable of attacking two lines (Z=2), then the attacker will be unable to attack any line and the load shedding should be zero (or whatever it is in the pre-attack state).

TABLE II
Worst-Case Load Sheddings with Different Combinations of Defense & Attack Resource Limits in the WSCC 9-Bus System

Z	Load shedding (MW)					
	K=0	K=1	K=2	K=3	K=4	K=5
1	0	0	0	0	0	0
2	125	100	90	65	65	0
3	315	215	190	90	90	0
4	315	315	190	90	90	0
5	315	315	190	90	90	0
6	315	315	190	90	90	0
7	315	315	190	90	90	0
8	315	315	190	90	90	0
9	315	315	190	90	90	0

Considering that WSCC assumes that the attacker is capable of attacking two lines, the outcomes of different defense plans are shown in Table III. If no line is protected, the attacker would attack lines 8-9 and 9-4 to cause a maximum load shedding of 125 MW. As expected, the largest load at bus 9 is isolated. If WSCC can only protect 1 line, line 9-4 could be protected and the attacker would move targets to lines 6-7 and 7-8 to isolate the secondly largest load of 100 MW. If WCSS can protect 3 lines, lines 5-6, 7-8, and 9-4 would be protected and the attacker will disable lines 3-6 and 8-2 to cut off the two largest generators resulting in a load shedding of 65 MW. Note that the protected lines could be different from those in Table III. As a result, WSCC can protect three particular lines to reduce the worst-case load shedding from 125 MW to 65 MW, which might be good enough.

TABLE III
Outcomes of Defense Plans when the Attack Resource Limit (Z) Equals 2

K	Protected lines	Attacked lines	Load shedding (MW)
0	n/a	8-9, 9-4	125
1	9-4	6-7, 7-8	100
2	7-8, 8-9	4-5, 5-6	90
3	5-6, 7-8, 9-4	3-6, 8-2	65
4	4-5, 5-6, 7-8, 9-4	3-6, 8-2	65
5	1-4, 4-5, 6-7, 8-2, 9-4	n/a	0

Note that the planner may wish intuitively to protect lines 8-9 and 9-4 if K=2, because disabling these two lines results in maximum load shedding (isolating the largest load of 125 MW). If so, the attacker would disable lines 7-8 and 7-6 to isolate the second largest load of 100 MW. However, protecting lines 7-8 and 8-9 can reduce the worst-case load shedding to 90 MW. In other words, protecting lines 8-9 and 9-4 is only a sub-optimal solution.

B. IEEE 118-bus System

The IEEE 118-bus system [23] represents a portion of the American Electric Power footprint in the Midwest of United States as of December, 1962. The system consists of 118 buses, 19 generators, 35 synchronous condensers, 177 lines, 9 transformers, and 91 loads. In other words, it has 186 candidate components to be defended and to be attacked. This system is shown in Fig. 6.

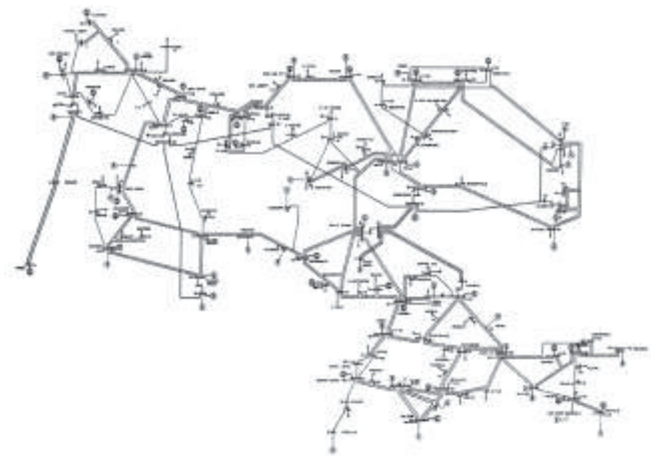

Fig. 6. Single-line diagram of IEEE 118-bus System

For large systems, computational time is critical. To illustrate this, both the implicit enumeration method and the proposed method are considered with this 118-bus system.

The attack resource limit (Z) is considered equal to 2. The planner will decide which lines to protect so that the corresponding worst-case load shedding is acceptable by either the operator or the regulator. After simulating several defense resource limits (K), the results are shown in Table IV.

TABLE IV
Realistic Computational Results with Average Run Time Comparisons

K	Z	Load shedding (MW)	Implicit enumeration method (s)	Proposed method (s)
0	2	110	30	28
1	2	104	112	105
2	2	48	300	178
3	2	42	627	198
4	2	42	975	340
5	2	41	1620	365
6	2	41	2740	378
7	2	39	5438	414
8	2	37*	10777	440
9	2	34	21400	522
10	2	34	30507	582
11	2	34	n/a	690
12	2	33	n/a	757

* The load shedding calculated by the implicit enumeration method is 34 MW, which is the globally optimal solution. It also means the proposed method gives a sub-optimal solution.

The total load of the IEEE 118-bus system is 4,242 MW. If no line is protected, the worst-case load shedding is 110 MW. There is a significant difference between defending 1 line and defending 2 lines. From the simulation results, it is advisable to assign a protection resource limit (K) equal to the considered attack resource limit (Z) for this case study. As the defense resource limit (K) increases, the worst-case load shedding decreases smoothly after defending 2 lines. However, it still makes a difference in terms of load shedding, as defending 2 lines results in 48 MW of load shedding, while defending 12 lines results in 33 MW of load shedding. Comparing the last two columns, we conclude that the proposed method needs much shorter run time than the implicit enumeration method, while additional time savings as the defense resource limit (K) increases. If K equals 10, the implicit enumeration method needs on average 8.5 hrs whereas the proposed method only needs about 10 minutes. If K is greater than or equal to 11, the implicit enumeration method would need more than 14 hrs. However, the proposed method will require 11.5 min and 12.6 min on average for defending 11 and 12 lines, respectively.

Generally speaking, the proposed method is a decomposition-based algorithm, which has been widely used and proven efficient. The implicit enumeration method is a searching method, whose solving speed is highly impacted by the problem size. In addition to the 118-bus system case study, using other systems and case studies we have computationally verified that the efficiency of the proposed algorithm is clearly better than that of the implicit enumeration method, which exhibit an exponential relationship between number of iterations and K.

If the ramping-up limit (RU) is tightened to 40% of each unit capacity, the optimal solution changes. Table V and VI provide the optimal results. Table V provides load shedding values for the cases without and with ramping limits, whereas Table VI provides defense plans for both cases. Note that ramping-down limits are not explicitly enforced since the attacker could possibly isolate generating units.

TABLE V
Outcomes of Load Shedding with Two Ramping Limits

K	Z	Load shedding (MW)	
		$RU_j = \overline{P}_j^G$	$RU_j = 0.4\overline{P}_j^G$
0	2	110	172
1	2	104	110
2	2	48	61
3	2	42	48
4	2	42	48
5	2	41	42
6	2	41	42
7	2	39	42
8	2	37	41
9	2	34	39
10	2	34	37
11	2	34	34
12	2	33	34

TABLE VI
Outcomes of Defense Plans with Two Ramping Limits

K	$RU_j = \overline{P}_j^G$	$RU_j = 0.4\overline{P}_j^G$
4	77-78 88-89 68-116 12-117	77-78 85-88 68-116 75-118
5	22-23 77-78 88-89 95-96 68-116	22-23 77-78 85-88 68-116 75-118
6	19-20 29-31 77-78 85-88 95-96 68-116	19-20 77-78 88-89 110-112 68-116 75-118
7	19-20 29-31 51-52 77-78 88-89 95-96 68-116	76-77 77-78 79-80 85-88 94-95 110-112 68-116
8	22-23 27-28 51-52 77-78 79-80 85-88 95-96 68-116	22-23 76-77 77-78 79-80 85-88 95-96 110-112 68-116

Considering Tables V and VI, we conclude that the case with tighter ramping limits results in a different optimal solution (in terms of lines to be protected) and higher load shedding.

As mentioned in the note below Table IV, the proposed method may just achieve a sub-optimal solution, such as in the case with 8 protected lines. This is due to the non-convexity of this trilevel problem. However, we have computationally verified that the chance of having this situation is low, and it can be avoided by adjusting the starting solution. Note that there is no general method to initialize the algorithm. However, physical insight can be used to obtain a number of appropriate starting solutions. For instance, if K=2 in the 9-bus system case study, the algorithm will initially solve the subproblem with K=0, Z=2, and the result is a = $[1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0]^T$, which means the attacker would attack line 8 and 9 (please refer to Table III) to maximize load shedding. Then, the initial protection plan is assigned using d = $[0\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$ to protect these two most critical lines. In addition to the algorithm's initial solution obtained by initialization method above, some other initial solutions should be considered in order to avoid reaching sub-optimal solutions, such as that pertaining to protecting the lines that supply the largest loads.

The general properties of C&CG method is provided in [18]. However, the implementation of the C&CG method in the proposed formulation is different from that in the case study of [18], where convergence and optimality can be proven.

Constraint (6) involves the product of an upper-level binary variable (d), a middle-level binary variable (a) and a lower-level continuous variable (δ). As a result, the proposed optimization model has a non-convex feasible region and it is therefore non-convex. Note that in the master problem or in the subproblem, a given binary variable is fixed. Therefore, the product of the remaining binary variable (d or a) and the continuous variable (δ) can be linearized [15]-[17]. However, this does not change the non-convex nature of the initial problem. Nevertheless, we have computationally verified that has good convergence and optimality properties. A stronger theoretical result needs further research and is outside the scope of this paper. In order to further analyze the convergence behaviors of the proposed method, two cases out of those in Table IV are illustrated in Fig. 7, where the solution of the upper and lower bounds are represented.

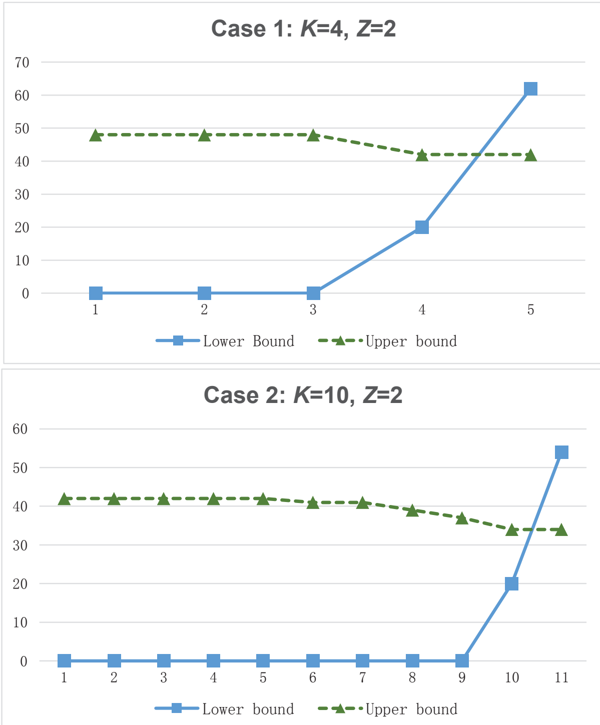

Fig. 7. Convergence analysis plots

The first case with K = 4, Z = 2 converges at iteration 5, while the second case with K = 10, Z = 2 converges at iteration 11. The trends of both cases are similar with upper and lower bound monotonically decreasing and increasing, respectively, until they cross.

Since the proposed algorithm is an instance of Benders' decomposition and the considered problem is non-convex (as the example in Fig. 9 of the Appendix), the subproblem may generate an invalid inequality, such as the second-iteration inequality in Fig. 9. In a non-convex problem, a Benders' cut that originates bound crossing is denominated invalid inequality, since such cut (or inequality) prevents a cut reconstruction of the original objective function. If, on the other hand, the problem is convex, all cuts help reconstructing the original objective function, and thus invalid inequalities are not possible. Therefore, while solving (1)-(11), which is non-convex, a given starting solution could result in the subproblem generating an invalid inequality to be added to the master problem, which may result in bound crossing. The bounds generated by the Benders' algorithm are true upper and lower bounds if the problem is convex. If it is not, these bounds may not be true upper or lower bounds and they may cross. Please refer to the Appendix for additional details. Note that the non-convexity might cause the proposed algorithm to find sub-optimal solutions, but this does not mean that all obtained solutions must be sub-optimal [24][25]. The needed number of iterations increases as the problem size increases.

In order to verify the stability and convergence of the proposed algorithm, we also tried several other case studies in different systems with multiple combinations of Z and K. All of them resulted in low occurrence ($\leqslant$3%) of sub-optimal solutions. Due to space limitation, they are not presented in this paper.

V. Conclusion

A planner-attacker-operator model is presented for electric grid defense planning. The mathematical formulation results in a trilevel problem. A Benders primal decomposition method is used to decompose the trilevel problem into a master problem and a subproblem, which results in an efficient solution algorithm.

Two case studies are presented to prove the effectiveness and efficiency of this proposed technique. One is a small case with 9 buses representing a simplified WSCC system and another one is the IEEE 118-bus system. The proposed technique is much more efficient than a branch-and-bound method and it is applicable to complex real-world problems.

Future work could include involving defense cost into the planner's objective function or constraints, or considering substation attacks.

VI. Acknowledgment

The authors would like to acknowledge support from both "Station Engineering" and "East Transmission Planning" departments at American Electric Power. In addition, Dr. Hui Zhang provided useful suggestions on algorithm development and solver selection.

Appendix

Benders' Decomposition in Convex & Non-Convex Problems

We use two simple examples below (Fig. 8 and 9) to illustrate how Benders' decomposition works in convex and non-convex problems. Fig. 8 illustrates the use of Benders' decomposition to find the minimum of the convex function $y = f(x)$ subject to $x \geq 0$. The algorithm starts at x_1 being its corresponding function value $f(x_1) = UB_1$ (note that evaluating the function corresponds to solving the subproblem). Therefore, the initial upper bound is $UB = UB_1$. The slope at this point (x_1, UB_1) and the corresponding intersection point with the x-axis x_2 provides the initial lower bound $LB = LB_1$ (note that minimizing the ordinate subject to being above the slope corresponds to solving the master problem). Then, we consider x_2, obtain the subproblem solution as $UB_2 = f(x_2)$ and update the upper bound as $UB = \min(UB, UB_2) = UB_2$. The slope at ($x_2$, UB_2) and the previous slope intersect at (x_3, LB_2), being LB_2 the master problem solution, as it is the minimum above the two previous slopes. Therefore, the lower bound is updated as $LB = LB_2$. Then, we obtain the subproblem solution as $UB_3 = f(x_3)$ and update the upper bound as $UB = \min(UB, UB_3) = UB_3$. The slope at ($x_3$, UB_3) and the previous two slopes intersect at two points, being LB_3 the master problem solution, as it is the minimum above the three previous slopes. Therefore, the lower bound is updated as $LB = LB_3$. After a number of iterations, the bound difference between UB and LB is small enough and the minimum of this convex function is obtained. As a result, in a convex case bounds do not cross.

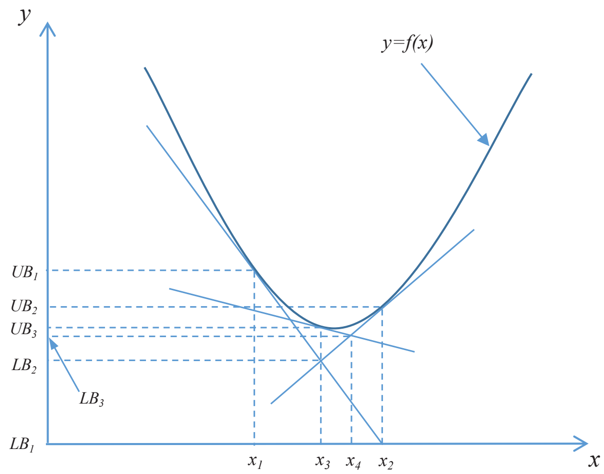

Fig. 8 Convex function Benders decomposition illustration

On the other hand, Fig. 9 illustrates the use of Benders' decomposition to find the minimum of the non-convex function $y = f(x)$ subject to $x \geq 0$. The algorithm starts at x_1 being its corresponding function value $f(x_1) = UB_1$ (note that evaluating the function corresponds to solving the subproblem). Therefore, the initial upper bound is $UB = UB_1$. The slope at this point (x_1, UB_1) and the corresponding intersection point with the x-axis x_2 provides the initial lower bound $LB = LB_1$ (note that minimizing the ordinate subject to being above the slope corresponds to solving the master problem). Then, we consider x_2, obtain the subproblem solution as $UB_2 = f(x_2)$ and update the upper bound as $UB = \min(UB, UB_2) = UB = UB_1$. The slope at ($x_2$, UB_2) and the previous slope intersect at (x_3, LB_2), being LB_2 the master problem solution as it is the minimum above the two previous slopes. Therefore, the lower bound is updated as $LB = LB_2$. Since LB_2 is larger than UB_1, the lower bound (LB) is larger than the upper bound (UB). As a result, non-convexity could cause bound crossing.

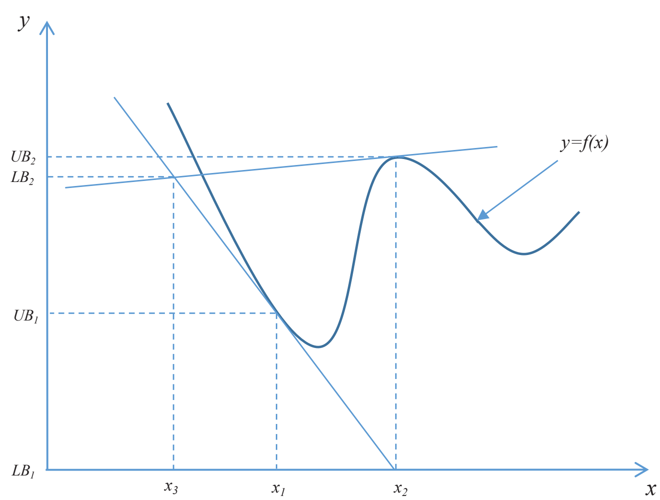

Fig. 9 Non-convex function Benders decomposition illustration

VII. References

[1] P. W. Parfomak, "Physical security of the U.S. power grid: high-voltage transformer substations," *Congressional Research Service*. June 17, 2014.

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

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

[4] 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 Transactions on Power Systems*, vol. 20, no. 3, pp. 1357-1365, Aug. 2005.

[5] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 789-797, May 2005.

[6] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530-544, Nov.-Dec. 2006.

[7] 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," *Reliability Engineering and System Safety*, vol. 92, pp. 1155-1161, 2007.

[8] A. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," *IEEE Transactions on Power Systems*, vol. 22, no. 1, pp. 76-84, Feb. 2007.

[9] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews*, vol. 37, no. 4, pp. 712-718, July 2007.

[10] N. Alguacil, A. Delgadillo, and J. M. Arroyo, "A trilevel programming approach for electric grid defense planning," *Computers & Operations Research*, vol. 41, pp. 282-290, 2014.

[11] M. P. Scaparra and R. L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Computers & Operations Research*, vol. 35, pp. 1905-1923, 2008.

[12] Wood, R.K., 2011, "Bilevel Network Interdiction Models: Formulations and Solutions," in Wiley Encyclopedia of Operations Research and Management Science. DOI: 10.1002/9780470400531.eorms0932

[13] D. Bertsimas and M. Sim, "Robust discrete optimization and network flows," *Mathematical Programming*, vol. 98, pp. 49-71, 2003.

[14] C. Ruiz and A. J. Conejo, "Robust transmission expansion planning," *European Journal of Operational Research*, vol. 242, pp. 390-401, 2014.

[15] L. Bahiense, G. C. Oliveira, M. Pereira, and S. Granville, "A mixed integer disjunctive model for transmission network expansion," *IEEE Transactions on Power Systems*, vol. 16, no. 3, pp. 560–565, Aug. 2001.

[16] H. Zhang, V. Vital, G. T. Heydt, and J. Quintero, "A mixed-integer linear programming approach for multi-Stage security-constrained transmission expansion planning," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 1125–1133, May 2012.

[17] C. A. Floudas, Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications. New York: Oxford Univ. Press, 1995, pp. 245–247.

[18] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Operation Research Letters*, vol. 41, no. 5, pp. 457-461, Sept. 2013.

[19] R. L. Church and M. P. Scaparra, "Protecting critical assets: the r-interdiction median problem with fortification," *Geographical Analysis*, vol. 39, pp. 129-146, 2007.

[20] MathWorks. [Online]. Available: http://www.mathworks.com.

[21] Gurobi Optimization, Gurobi Optimizer Reference Manual. [Online]. http://www.gurobi.com.

[22] The Illinois Center for a Smarter Electric Grid (ICSEG), "WSCC 9-bus system," [Online]. http://publish.illinois.edu/smartergrid/wscc-9-bus-system/.

[23] R. Christie, "Power systems test case archive," Aug. 1993, [Online]. http://www.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm.

[24] A. J. Conejo, E. Castillo, R. Minguez, and R. Garcia-Bertrand, Decomposition Techniques in Mathematical Programming, Engineering and Science Applications. Springer, Heidelberg. 2006.

[25] R. Minguez, F. Milano, R. Zarate-Minano and A. J. Conejo, “Optimal network placement of SVC devices,” *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1851-1860, Nov. 2007.

VIII. Biographies

Xuan Wu (M’14) is from Nanjing, China. He received the B.S. degree in EE from Nanjing University of Aeronautics and Astronautics, Nanjing, China in 2011 and the M.S. degree in EE from Arizona State University, Tempe, in 2013. Currently, he is working as a station design standards engineer at American Electric Power and a part-time Ph.D. student at The Ohio State University. His research interests include transmission planning, electromagnetic & electrostatic coupling effects, substation fault analysis and grounding design.

Antonio J. Conejo (F’04) received the M.S. Degree from MIT, Cambridge, Massachusetts, US, in 1987, and the Ph.D. degree from the Royal Institute of Technology, Stockholm, Sweden, in 1990. He is currently a full professor at the Integrated System Engineering and the Electrical & Computer Engineering Departments, The Ohio State University, Columbus, Ohio, US. His research interests include control, operations, planning, economics and regulation of electric energy systems, as well as statistics and optimization theory and its applications.