

# A Genetic Algorithm Approach for the Analysis of Electric Grid Interdiction with Line Switching

J. M. Arroyo, F. J. Fernández

Departamento de Ingeniería Eléctrica, Electrónica, Automática y Comunicaciones  
Universidad de Castilla – La Mancha  
Ciudad Real, Spain

JoseManuel.Arroyo@uclm.es, FcoJ.Fdez11@alu.uclm.es

**Abstract**—This paper addresses the vulnerability analysis of the electric grid under terrorist threat. This problem is formulated as a mixed-integer nonlinear bilevel program. In the upper-level optimization, the terrorist agent maximizes the damage caused in the power system, which is measured in terms of the level of system load shed. On the other hand, in the lower-level optimization, the system operator minimizes the damage by means of an optimal operation of the power system. The distinctive modeling feature introduced in this paper is that, among the different corrective actions available, the system operator has the capability to modify the network topology.

Due to its nonconvexity and nonlinearity, exact solution techniques are not currently available. This paper proposes a novel genetic algorithm approach to achieve near optimal solutions in moderate computing times. Some numerical results obtained by the proposed algorithm are provided and compared with those published, based on the IEEE Reliability Test System.

**Keywords**—*bilevel programming; deliberate outages; genetic algorithm; line switching; load shedding; vulnerability*

## I. INTRODUCTION

The introduction of deregulation, increased levels of consumption, and lack of investment are driving the operation of power systems close to their static and dynamic limits. Therefore, power systems are becoming increasingly vulnerable to both natural-occurring failures and intentional outages [1]. In this new context, currently used N-1 and N-2 criteria may not be sufficient to assess vulnerability. Consequently, new tools considering multiple contingencies are required.

Recent works have addressed power system vulnerability assessment under the framework of deliberate outages [2]-[7]. This problem, also known as vulnerability analysis, terrorist threat problem or interdiction problem, consists in identifying the set of contingencies that makes the system most vulnerable so that effective defensive or protective measures can be determined [8], [9]. In the vulnerability analysis, the destructive agents attack the system with the goal of maximizing the damage, whereas the system operator reacts to minimize such damage. Therefore, this problem can be modeled as a bilevel program [10], where the terrorist is the upper-level agent, while the system operator is the lower-level agent.

This paper proposes a new model and a new solution procedure for vulnerability analysis under deliberate outages. The salient feature of the proposed model with respect to those described in [2]-[7] is the consideration of line switching [11] as an additional corrective action available to the system operator following an attack. In other words, in addition to generation redispatch and load shedding, the system operator has the capability to modify the network topology by opening and closing lines.

In our model, line switching decisions are characterized through lower-level binary variables; therefore, the resulting bilevel program cannot be addressed by means of previously reported techniques relying on the equivalent transformation to a one-level optimization problem [3], [4]. Bilevel programs with a nonconvex lower-level problem constitute a challenging field that is still unsolved by the operations research community [12].

Furthermore, this paper presents a genetic algorithm approach as a solution methodology [13], [14]. A genetic algorithm is a search technique based on the evolution of biological systems. The search starts with a set (population) of solutions (individuals) randomly generated and large enough. This set of solutions is the first generation. Using crossover and mutation procedures, new generations are obtained. The characteristics of the initial set of solutions improve in terms of a fitness function from generation to generation. After a large enough number of generations, “good” solutions are obtained.

An example of successful application of genetic algorithms to solve a bilevel programming problem outside a power system framework can be found in [15]. The modeling framework provided by a genetic algorithm approach allows considering the nonlinearities and nonconvexities present in the resulting bilevel model. This is a major advantage of the proposed method.

For the terrorist threat problem with line switching, every generation is made up of a fixed number of solutions randomly obtained from the solutions of the previous generation. The first generation is randomly generated from scratch. A heuristic procedure is used to enforce feasibility, i.e., all solutions dealt with are feasible. Finally, evolution is implemented by genetic operators such as crossover, mutation,

and elitism. This repair genetic algorithm results in a well conditioned and efficient search.

The major contributions of this paper are:

1. The bilevel model of the terrorist threat problem is extended by adding line switching to the set of corrective actions available to the system operator.
2. A novel genetic algorithm approach is used to solve the resulting bilevel program with binary lower-level decision variables.
3. The proposed genetic algorithm is effective in attaining globally optimal or near-optimal solutions.
4. The performance of the proposed approach is successfully validated with numerical simulations.

The remaining sections are outlined as follows. Section II presents the bilevel formulation of the terrorist threat problem with line switching. Section III describes the proposed genetic algorithm. Section IV provides and analyzes the numerical results. Some relevant conclusions are drawn in Section V. Finally, the Appendix shows the data of the test system.

## II. BILEVEL APPROACH

According to [3], the terrorist threat problem can be characterized as a bilevel program [10], i.e., a decision-making problem involving two agents who try to optimize their respective objective functions over a jointly dependent set.

Fig. 1 shows a general bilevel model for the terrorist threat problem. The upper level is associated with the disruptive agent and determines the components of the power system to be attacked in order to maximize the damage caused to the electrical system. The damage is measured in terms of the level of system load shed. The maximization problem of the disruptive agent takes into account that destructive resources are limited, and that the system operator in the lower level optimally reacts to the attack. This reaction consists in determining the optimal power system operation that minimizes the effect caused by the terrorist. In previously reported works [2]-[7], the set of corrective actions was restricted to generation redispatch and load shedding. In contrast, in this paper we extend the defensive reaction of the system operator by allowing line switching [11].

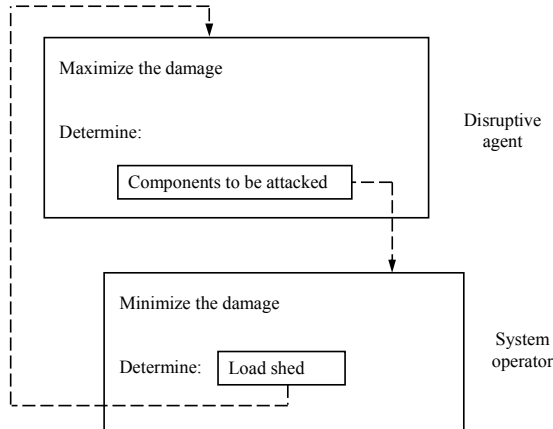


Figure 1. Bilevel model.

It should be emphasized that the proposed approach can handle the destruction of any power system component. However, the power system components most commonly disrupted by destructive agents are transmission lines [16]. Based on this fact, and for the sake of clarity and simplicity, here we consider that the terrorist agent only attacks these assets.

The electric grid interdiction problem with line switching is formulated as the following bilevel programming problem:

$$\max_{v_\ell} \sum_{n \in N} \Delta P_n^{d*} \quad (1)$$

subject to:

$$\sum_{\ell \in L} (1 - v_\ell) = M \quad (2)$$

$$v_\ell \in \{0,1\}; \forall \ell \in L \quad (3)$$

$$\Delta P_n^{d*} \in \arg \left\{ \min_{P_\ell^f, P_j^g, \delta_n, \Delta P_n^d} \sum_{n \in N} \Delta P_n^d \right\} \quad (4)$$

subject to:

$$P_\ell^f = v_\ell w_\ell \frac{1}{x_\ell} \sum_{n \in N} A_{n\ell} \delta_n; \forall \ell \in L \quad (5)$$

$$\sum_{j \in J_n} P_j^g - \sum_{\ell \in L} A_{n\ell} P_\ell^f + \Delta P_n^d = P_n^d; \forall n \in N \quad (6)$$

$$0 \leq P_j^g \leq \bar{P}_j^g; \forall j \in J \quad (7)$$

$$-\bar{P}_\ell^f \leq P_\ell^f \leq \bar{P}_\ell^f; \forall \ell \in L \quad (8)$$

$$\underline{\delta} \leq \delta_n \leq \bar{\delta}; \forall n \in N \quad (9)$$

$$0 \leq \Delta P_n^d \leq P_n^d; \forall n \in N \quad (10)$$

$$w_\ell \in \{0,1\}; \forall \ell \in L, \quad (11)$$

where  $v_\ell$  is a 0/1 variable which is equal to 0 if line  $\ell$  is out of

service and otherwise is equal to 1;  $N$  is the set of indices of buses,  $\Delta P_n^d$  is the load shed at bus  $n$ ;  $L$  is the set of indices of transmission lines;  $M$  is the number of simultaneous out-of-service lines;  $P_\ell^f$  is the power flow of line  $\ell$ ;  $P_j^g$  is the power output of generator  $j$ ;  $\delta_n$  is the phase angle at bus  $n$ ;  $w_\ell$  is a 0/1 variable which is equal to 0 if non-attacked line  $\ell$  is disconnected and 1 otherwise;  $x_\ell$  is the reactance of line  $\ell$ ;  $A_{n\ell}$  is the element of the network incidence matrix which is equal to 1 if bus  $n$  is the sending bus of line  $\ell$ , -1 if bus  $n$  is the receiving bus of line  $\ell$ , and 0 otherwise;  $J_n$  is the set of indices of generators connected to bus  $n$ ;  $P_n^d$  is the demand at bus  $n$ ;  $\bar{P}_j^g$  is the capacity of generator  $j$ ;  $J$  is the set of indices of generators;  $\bar{P}_\ell^f$  is the power flow capacity of line  $\ell$ ;  $\underline{\delta}$  is the lower bound for the nodal phase angles; and  $\bar{\delta}$  is the upper bound for the nodal phase angles.

The disruptive agent is represented by the upper-level problem (1)-(3). The terrorist controls binary variables  $v_\ell$ . The system operator is represented by the optimal power flow in the lower-level problem (4)-(11), which is parameterized in terms of the upper-level decision variables  $v_\ell$ . As is commonly assumed in the technical literature [2]-[7], a dc model of the transmission system is used. The system operator controls continuous variables  $P_\ell^f$ ,  $P_j^g$ ,  $\delta_n$ ,  $\Delta P_n^d$ , and binary variables  $w_\ell$  which model the capability to modify the network topology. The terrorist agent maximizes the system load shed (1) for a given number of simultaneously destroyed lines (2). Constraints (3) model the binary nature of variables  $v_\ell$ . The objective of the system operator (4) is to minimize the system load shed under the combination of destroyed lines chosen by the terrorist. Constraints (5) express the line flows in terms of the nodal phase angles, the line switching variables, and the upper-level variables. Note that if line  $\ell$  is either attacked ( $v_\ell = 0$ ) or disconnected ( $w_\ell = 0$ ), the corresponding power flow is set to 0. Constraints (6) represent the power balance in each bus of the system. Upper and lower bounds on lower-level decision variables are imposed in constraints (7)-(10). Finally, constraints (11) model the integrality of variables  $w_\ell$ . It should be noted that weights could be assigned to nodal loads shed to reflect the relative importance of each load.

Constraints (5) constitute the main difference with respect to the bilevel models presented in [2]-[7]. These constraints make the lower-level problem nonconvex due to the presence of lower-level binary variables  $w_\ell$ , and nonlinear due to the products of lower-level decision variables  $w_\ell$  and  $\delta_n$ . Therefore, it is not possible to transform the bilevel problem (1)-(11) into an equivalent one-level optimization problem, as done in [3], [4], and new tools are thus needed.

### III. GENETIC ALGORITHM

For the terrorist threat problem, every individual in the genetic algorithm is characterized through a vector  $v$  of 0s and 1s as follows:

$$v = \{v_1, \dots, v_{n_L}\}, \quad (12)$$

where  $n_L$  is the number of lines in the transmission network. In other words, the solution coding is straightforward since each individual represents an interdiction plan.

The proposed genetic algorithm starts by initializing the population of solutions, which comprises a set of randomly generated interdiction plans. Subsequently, four simple operators are iteratively applied: selection, crossover, mutation, and elitism. In addition, a heuristic is used to restore feasibility of the solutions.

The quality of each feasible individual  $v$  (upper-level decision vector) is assessed by a fitness function, which is the system load shed associated with the corresponding interdiction plan. Thus, the fitness value associated with each individual  $v$  is obtained from solving the dc mixed-integer nonlinear optimal power flow (4)-(11), i.e., the lower-level problem. This problem is nonlinear due to the products of binary variables and continuous variables  $w_\ell \delta_n$  in (5). By using algebra results [17], these nonlinearities can be replaced by equivalent linear expressions. Therefore, the resulting optimal power flow is a mixed-integer linear program that can be efficiently solved by available off-the-shell branch-and-cut software.

The operators applied by the genetic algorithm are explained next.

#### A. The Next Generation

Given a generation of feasible solutions the next generation is obtained as follows. Solutions of the current generation are randomly selected with probabilities proportional to their corresponding fitness value (system load shed), and arranged in couples. Using a single-point crossover procedure every couple of solutions of the current generation produces two solutions of the next generation. The solutions of the new generation will be in general infeasible and specifically tailored procedures are used to enforce feasibility.

#### B. Mutation

According to a pre-specified mutation probability, an individual in each generation is randomly selected. A random element from the 0/1 vector is flipped from 0 to 1 or vice versa. If the mutated individual is infeasible, feasibility procedures are run without undoing what the mutation procedure did.

#### C. Elitism

The elitist operator preserves the best solutions found by maintaining a group of them in the next generation. As is shown in [18], this operator is necessary to prove the convergence to the optimum through a Markov chain analysis.

#### D. Feasibility

In order to enforce feasibility of the upper-level constraint (2) the following feasibility procedure is implemented:

1. If the number of destroyed lines is less than  $M$ , a random element from the 0/1 vector  $v$  with value equal to 1 is flipped from 1 to 0. This process is repeated until the number of destroyed lines is equal to  $M$ .
2. If the number of destroyed lines is greater than  $M$ , a random element from the 0/1 vector  $v$  with value equal to 0 is flipped from 0 to 1. This process is repeated until the number of destroyed lines is equal to  $M$ .

It should be noted that once a feasible upper-level vector  $v$  is obtained, its associated optimal power flow is always feasible.

#### IV. NUMERICAL RESULTS

This section presents a case study based on the IEEE One Area Reliability Test System–1996 (RTS-96) [19]. For illustration purposes, the data of RTS-96 are slightly modified as described in the Appendix. In addition, circuits sharing the same towers are treated as independent lines; e.g., line 20-23 has two circuits: 20-23A and 20-23B. For the sake of simplicity, line switching is restricted to the disconnection of lines.

Some parameters of the genetic algorithm affect the quality of the solution and the computation time. These parameters are chosen by trial and error around conventional values used in the technical literature [13], [14]. Thus, the population size is 100 and the maximum number of generations is 100. In order to promote a higher exchange of genetic information among the individuals, the crossover rate is 1.0. It should be noted that in each generation a member of the population is randomly selected to be subject to mutation. Finally, the elitist operator maintains the best solution into the next generation.

In order to test the robustness of the method each algorithm was run 10 times with different initial populations created at random, and the results shown in this section are averages across those 10 runs. For most of these runs the best solutions attained were very similar in terms of objective function value, thus revealing a robust performance.

The simulations have been run on a Dell PowerEdge 6600 with 2 processors at 1.60 GHz and 2 GB of RAM using MATLAB [20]. The dc optimal power flows associated with each individual have been solved using GAMS [21] and CPLEX 10.2 [22], which were called from MATLAB using the interface developed by Ferris [23]. The average computing time required to run each simulation was 238 minutes, which is moderate bearing in mind that a planning problem is being solved. Moreover, it should be noted that no effort was made to achieve optimized implementation of this program. This implementation aspect is beyond the scope of this paper.

Table I presents the maximum system load shed obtained for a number of destroyed lines  $M$  up to 12. In the absence of a measure of the distance to the optimum, the quality of the solutions found by the proposed genetic algorithm is assessed through the comparison with the optimal solutions achieved by

TABLE I. MAXIMUM SYSTEM LOAD SHED ATTAINED BY THE DESTRUCTIVE AGENT (MW)

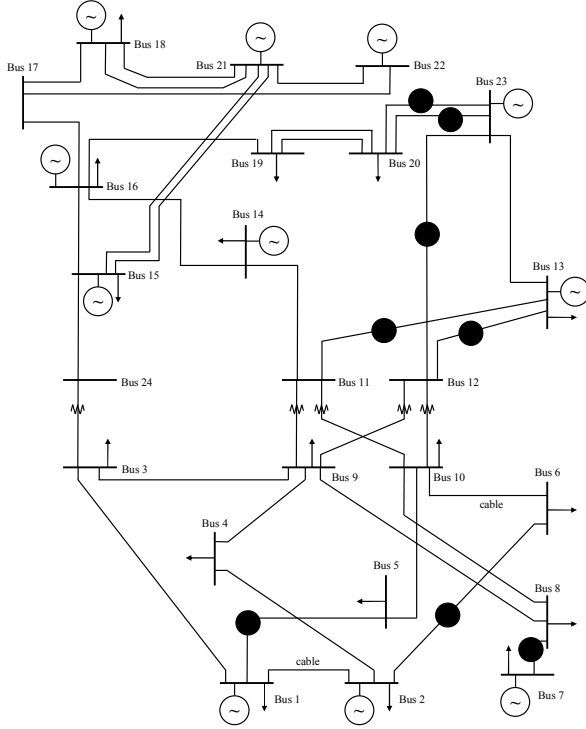
$M$	Genetic Algorithm	MO
1	131	230
2	279	397
3	429	484
4	538	570
5	688	706
6	775	795
7	855	855
8	915	919
9	1002	1003
10	1051	1053
11	1131	1131
12	1194	1194

the approach of Motto et al. [4], denoted by MO. The methodology MO does not consider line switching and thus provides an upper bound on the optimal system load shed.

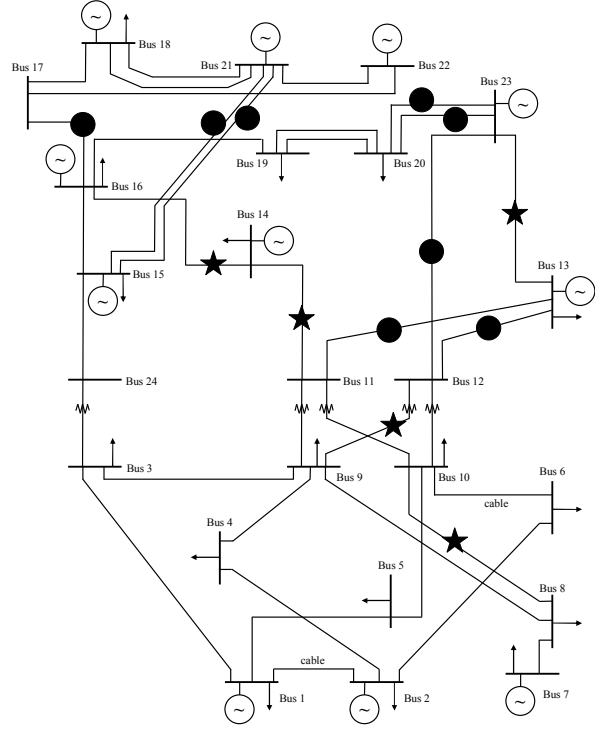
As can be inferred from Table I, line switching is an effective corrective action since it reduces the maximum damage associated with deliberate outages, except for cases  $M = 7, 11, 12$ . In those cases, the proposed genetic algorithm attains a solution to problem (1)-(11) with the same level of system load shed as that achieved by MO (without line switching). Therefore, these solutions are optimal and consequently line switching is not required. For the remaining cases, line switching mitigates the impact of deliberate outages between 43.0% for  $M = 1$  and 0.1% for  $M = 9$ . It is interesting to observe that for low values of  $M$  significant reductions of system load shed are achieved. This result supports the use of line switching as a corrective action also for random unintentional outages considered in traditional vulnerability assessment.

Table II shows the set of lines attacked by the terrorist agent and the set of lines disconnected by the system operator, corresponding to the best solutions attained by the genetic algorithm (Table I). It is worth mentioning that the disconnection of a relatively low number of lines yields a significant reduction in the level of damage associated with deliberate outages. As an example, by just disconnecting line 9-11 in the case  $M = 6$ , a 2.5% reduction in load shedding can be achieved with respect to the solution found by MO.

Fig. 2 shows the results found by MO and the proposed genetic algorithm for  $M = 8$ . Destroyed lines and switched lines are represented by blackened circles and blackened stars, respectively. Fig. 2a corresponds to MO and represents the optimal attack plan when the system operator is not allowed to modify the network topology. In this case, the optimal system load shed is 919 MW and the attacked lines are 1-5, 2-6, 7-8, 11-13, 12-13, 12-23, 20-23A, and 20-23B. If the system operator had the capability to modify the network topology, the system load shed associated with this attack plan would drop to 880 MW by opening lines 1-2, 15-16, and 17-18. However, this attack plan is not optimal, as shown in Tables I and II, and Fig. 2b. Fig. 2b depicts the best solution found by the proposed genetic algorithm. In this case, the system load shed is 915 MW, i.e., a 4.0% improvement from the perspective of the terrorist agent, and a 0.4% reduction in



(a) Best solution with MO



(b) Best solution with the genetic algorithm

Figure 2. Solutions for  $M=8$ .

TABLE II. BEST ATTACK PLAN AND ASSOCIATED LINE SWITCHING SCHEME

$M$	$v_{\ell}$	$w_{\ell}$
1	10-12	4-9, 6-10, 9-11, 12-13, 13-23, 15-16, 16-17, 16-19
2	9-12, 10-12	3-9, 6-10, 8-9, 15-16, 16-17
3	9-12, 10-12, 11-13	11-14
4	12-13, 12-23, 20-23A, 20-23B	3-9, 6-10, 15-16, 17-18
5	11-13, 12-13, 12-23, 20-23A, 20-23B	11-14
6	7-8, 11-13, 12-13, 12-23, 20-23A, 20-23B	9-11
7	7-8, 11-13, 12-13, 12-23, 15-24, 20-23A, 20-23B	–
8	11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, 20-23B	8-10, 9-12, 11-14, 13-23, 14-16
9	7-8, 11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, 20-23B	10-11, 10-12
10	1-3, 1-5, 2-4, 2-6, 7-8, 9-12, 10-12, 11-13, 20-23A, 20-23B	1-2, 4-9, 5-10, 9-11
11	1-3, 1-5, 2-4, 2-6, 7-8, 11-13, 12-13, 12-23, 15-24, 20-23A, 20-23B	–
12	1-2, 2-4, 2-6, 7-8, 11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, 20-23B	–

system load shed with respect to the optimal solution without line switching. The lines attacked by the destructive agent are 11-13, 12-13, 12-23, 15-21A, 15-21B, 16-17, 20-23A, and 20-23B, whereas the lines disconnected by the system operator are 8-10, 9-12, 11-14, 13-23, and 14-16.

Finally, Fig. 3 shows the evolution of the best system load shed found by the proposed genetic algorithm for  $M=8$ . It should be noted that the quality of the best solution found is rapidly improved in the first 20 generations. Moreover, it is worth emphasizing that the upper bound for the optimal solution is 919 MW (optimal solution found by MO in Table I) and the best solution found by the genetic algorithm is 915 MW. Therefore, it seems reasonable to state that the genetic algorithm is able to achieve optimality for this case.

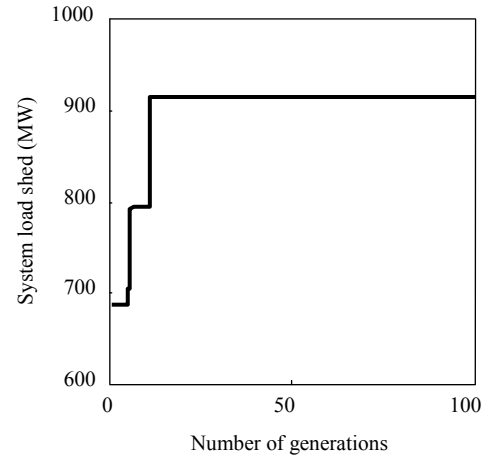


Figure 3. Evolution of the system load shed for  $M=8$ .

## V. CONCLUSIONS

This paper presents a new bilevel programming model and a novel solution procedure for the terrorist threat problem in an electrical network. The distinctive modeling feature is the consideration of line switching as a corrective action by the system operator. In order to solve the resulting mixed-integer nonlinear bilevel program, a genetic algorithm is applied.

Numerical results show that line switching is a helpful instrument for the system operator to mitigate the impact of deliberate outages. In addition, simulations show the effective performance of the proposed approach. Research is currently underway to develop alternative heuristic-based solution procedures. Further work will also analyze the connection or disconnection of fast-acting generating units to reduce the impact of deliberate outages on power system vulnerability.

## APPENDIX

The data of the test system that have been modified with respect to RTS-96 [19] are listed in Tables III and IV.

TABLE III. POWER FLOW CAPACITY (MW)

Line	$\bar{P}_l^f$	Line	$\bar{P}_l^f$
1-2	87.5	12-13	250.0
1-3	87.5	12-23	250.0
1-5	87.5	13-23	50.0
2-4	87.5	14-16	50.0
2-6	87.5	15-16	50.0
3-9	87.5	15-21A	250.0
3-24	80.0	15-21B	250.0
4-9	100.0	15-24	80.0
5-10	100.0	16-17	250.0
6-10	87.5	16-19	50.0
7-8	87.5	17-18	250.0
8-9	50.0	17-22	250.0
8-10	87.5	18-21A	250.0
9-11	50.0	18-21B	250.0
9-12	200.0	19-20A	250.0
10-11	50.0	19-20B	250.0
10-12	200.0	20-23A	250.0
11-13	250.0	20-23B	250.0
11-14	50.0	21-22	250.0

TABLE IV. NODAL POWER DEMAND (MW)

$n$	$P_n^d$	$n$	$P_n^d$
1	108	10	170
3	100	13	265
4	74	14	100
5	50	15	317
6	136	16	100
7	125	18	333
8	137	19	181
9	155	20	128

## REFERENCES

- [1] A. V. Gheorghe, M. Masera, M. Weijnen, and L. de Vries, *Critical Infrastructures at Risk. Securing the European Electric Power System*. Dordrecht: Springer, 2006.
- [2] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Trans. Power Syst.*, vol. 19, no. 2, pp. 905–912, May 2004.
- [3] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.
- [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 Trans. Power Syst.*, vol. 20, no. 3, pp. 1357–1365, August 2005.
- [5] Å. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," *IEEE Trans. Power Syst.*, vol. 22, no. 1, pp. 76–84, February 2007.
- [6] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, and K. R. Wierzbicki, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 9, pp. 1155–1161, September 2007.
- [7] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 96–104, February 2009.
- [8] G. Brown, M. Carlyle, J. Salmeron, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, November 2006.
- [9] M. Carrión, J. M. Arroyo, and N. Alguacil, "Vulnerability-constrained transmission expansion planning: A stochastic programming approach," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1436–1445, November 2007.
- [10] J. F. Bard, *Practical Bilevel Optimization. Algorithms and Applications*. Dordrecht: Kluwer Academic Publishers, 1998.
- [11] E. B. Fisher, R. P. O'Neill, and M. C. Ferris, "Optimal transmission switching," *IEEE Trans. Power Syst.*, vol. 23, no. 3, pp. 1346–1355, August 2008.
- [12] S. Dempe, "Annotated bibliography on bilevel programming and mathematical programs with equilibrium constraints," *Optimization*, vol. 52, no. 3, pp. 333–359, June 2003.
- [13] D. E. Goldberg, *Genetic Algorithms in Search, Optimization, and Machine Learning*. Reading: Addison-Wesley, 1989.
- [14] Z. Michalewicz, *Genetic Algorithms + Data Structures = Evolution Programs*. New York: Springer Verlag, 1996.
- [15] R. Mathieu, L. Pittard, and G. Anandalingam, "Genetic algorithm based approach to bi-level linear programming," *Recherche Op'erationnelle/Operations Research*, vol. 28, no. 1, pp. 1–21, 1994.
- [16] J. S. Simonoff, C. E. Restrepo, and R. Zimmerman, "Risk-management and risk-analysis-based decision tools for attacks on electric power," *Risk Anal.*, vol. 27, no. 3, pp. 547–570, June 2007.
- [17] C. A. Floudas, *Nonlinear and Mixed-Integer Optimization: Fundamentals and Applications*. New York: Oxford University Press, 1995.
- [18] D. B. Fogel, *Evolutionary Computation. Toward a New Philosophy of Machine Intelligence*, 2nd ed. New York: IEEE Press, 2000.
- [19] Reliability Test System Task Force, "The IEEE Reliability Test System–1996," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 1010–1020, August 1999.
- [20] The MathWorks, Inc., *Using MATLAB. Version 7.4.0.336 (R2007a)*. Natick: The MathWorks, Inc., 2007.
- [21] The GAMS Development Corporation Website, 2009. [Online]. Available: <http://www.gams.com>
- [22] The ILOG CPLEX Website, 2009. [Online]. Available: <http://www.ilog.com/products/cplex>
- [23] M. C. Ferris, "MATLAB and GAMS: Interfacing optimization and visualization software," Computer Sciences Department, University of Wisconsin – Madison, May 2005. [Online]. Available: <http://pages.cs.wisc.edu/~ferris/matlabgams.pdf>