Specialized Genetic Algorithm Applied to the Electric Grid Interdiction Problem

L. Agudelo, J. M. Lopez-Lezama, *Member, IEEE* and N. Muñoz, *Member, IEEE*

Abstract-- A specialized genetic algorithm applied to the solution of the electric grid interdiction problem is presented in this paper. This problem consists in the interaction of a disruptive agent who aims at maximizing damage of the power system (measured as load shed), and the system operator, who implements corrective actions to minimize system load shed. This problem, also known as "the terrorist threat problem", is formulated in a bilevel programming structure and solved by means of a genetic algorithm. The solution identifies the most vulnerable links of the network in terms of a terrorist attack, providing signals for future reinforcement of the network or more strict surveillance of critical elements.

The proposed approach has been tested on two case studies: a didactic five-bus power system and a prototype of the Colombian power system. Results show the robustness and applicability of the proposed approach.

Index Terms-- Bilevel programming, power system security, genetic algorithms, terrorist threat.

I. INTRODUCTION

THE constant growth of power demand, along with stronger environmental regulation, that in most cases delay the building of new transmission lines, have forced most power systems in industrialized countries to operate near their static and dynamic limits. Under this scenario, electric power systems are more vulnerable to intentional attacks [1]-[2]. Some of the most important effects of such attacks include load shedding and higher operational costs associated to the repairment of towers and transmission lines [3].

The traditional approach for power system vulnerability is based on the study of credible contingencies (N-1 and N-2 criteria) [4]-[5]. However, such studies require exhaustive simulation and therefore, they are associated with high computational burden; on the other hand, only natural-occurring outages are taken into account. Currently, it is well known that electric power systems are exposed not only to natural random phenomena, but also to malicious attacks. That is the case of the Colombian interconnected power system which has undergone the effects of terrorist attacks for several decades. As a matter of fact, only between 1999 and 2010 the National Interconnected System (NIS) faced as many as 200 terrorist attacks per year [3].

The electric grid interdiction problem, also kwon as the "terrorist threat problem" has been the focus of several studies in the last decade. This problem was first formulated in [6] as a max-min attacker-defender model. In such model the terrorist maximizes load shedding, while the system operator minimizes it. In [7] and [8] this problem is solved by using linearization and applying duality properties. First, the nonlinear expressions were recasted as linear constraints; then, the inner optimization problem was replaced by its dual, turning the max-min bilevel optimization problem into a max-max bilevel optimization problem. Such model is equivalent to a single-level maximization problem solvable via branch and cut methods. In [9] Arroyo and Galiana generalized the terrorist threat problem proposed by Salmeron, Wood and Baldick in [6]. The modeling approach of the problem proposed in [9] allows defining different objective functions for the terrorist and system operator. Also, it permits the imposition of new constraints in the outer optimization problem that might depend on both, inner and outer variables. As regards the terrorist's interests, different objectives can be considered. For example: *i)* to minimize the number of system components to be attacked, in order to achieve a given load shed, or *ii)* to maximize the load shed for a given number of system components that can be attacked.

In [10] the authors present a Mixed Integer Linear Programming approach for the analysis of the electric grid interdiction problem. In this case the bilevel programming problem is first turned into a one-level mixed-integer nonlinear programming program by using the fundamental duality theorem of linear programming [11]; then, disjunctive constraints are used to eliminate the nonlinearities of the problem. The resulting problem can be solved by using commercially available software. In [12] a worst-case interdiction analysis of the terrorist threat problem is performed by a generalization of Benders decomposition. In [13] the electric grid interdiction problem is formulated including line switching, which means that, after a terrorist attack, the system operator has also the option of switching some lines in order to reduce load shedding.

In this paper the authors propose a novel Genetic Algorithm (GA) approach to address the electric grid interdiction problem. Instead of turning the model into a one-level mixed-integer linear programming problem, the problem is solved in

Laura Agudelo is with Interconexión Eléctrica S.A (ISA). (e-mail: laura.agudelo@gmail.com).

Jesús María Lopez Lezama and Nicolás Muñoz are with GIMEL (Efficient Energy Management Research Group) Department of Electrical Engineering, Faculty of Engineering, University of Antioquia, Street 70 No 52-21 Medellín, Colombia. (e-mail: lezama@udea.edu.com; nicolasm@udea.edu.co)

its original form as a mixed-integer non-linear programming problem. Results of the proposed algorithm are validated with studies reported in the specialized literature, showing its capability to attain globally optimal or near-optimal solutions.

II. MATHEMATICAL FORMULATION

The mathematical formulation of the electric grid interdiction problem is provided in equations (1) to (9) [9]. In this case the objective of the disruptive agent consists on maximizing the total load shedding that can be attain given a fixed number of elements (lines or transformers) under attack.

$$\underset{VI_l}{Max} \quad \sum_{n \in N} \Delta P_n^d \qquad (1)$$

Subject to:

$$VI \in \{0,1\} \qquad (2)$$

$$\sum_{l \in L}(1 - VI_l) = M \qquad (3)$$

$$\underset{x}{Min} \quad \sum_{n \in N} \Delta P_n^d \ ; \ x = [\theta, P^g, P^f, \Delta P^d] \qquad (4)$$

Subject to:

$$P_l^f = (VI_l) * \frac{1}{Z_l} \sum_{n \in N} A_{nl} \theta_n ; \quad \forall l \in L \qquad (5)$$

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

$$P_j^{gmin} \le P_j^g \le P_j^{gmax}; \quad \forall j \in J \qquad (7)$$

$$\theta_n^{min} \le \theta_n \le \theta_n^{max}; \quad \forall n \in N \qquad (8)$$

$$0 \le \Delta P_n^d \le P_n^d; \quad \forall n \in N \qquad (9)$$

Where:

VI: Interdiction vector
ΔP_n^d: Load shed in node n
P_l^f: Power Flow in line l
A_{nl}: Incidence Matrix in node n of line l
θ_n: Phase angles in node n
P_j^g: Power generation by generator j
P_n^d: Power demand in node n
M: Number of elements under attack
Z_l: Impedance of line l
P_j^{gmin}: Minimum power generation by generator j
P_j^{gmax}: Maximum power generation by generator j
θ_n^{min}: Minimum phase angle in node n
θ_n^{max}: Maximum phase angle in node n

The interdiction vector consists of a binary array in which every position indicates the state of the element. If the position is equal to one it indicates an element on service; conversely, if the position is zero it indicates an element out of service (under attack). Equations (1) to (3) represent the upper level optimization problem (disruptive agent problem). For a given number of system components that could be attacked (*M*), the disruptive agent must maximize

the load shedding of the system. Such problem is at the same time restricted by the reaction of the system operator (equations (4) to (9)). For a given interdiction vector, the system operator must perform a redispatch of generation in order to minimize load shedding. Note that equations (4) to (9) correspond to an optimal DC power flow; furthermore, for a given interdiction vector, the inner optimization problem is a linear programming problem.

III. SPECIALIZED GENETIC ALGORITHM

The strategy proposed in this paper to approach the electric grid interdiction problem consists of using a Genetic Algorithm (GA); however, any other metaheursistic technique could be applied. The methodology proposed in this paper takes advantage of the fact that, for a given interdiction vector, the equivalent problem is a DC optimal power flow. In this case, a number of interdiction vectors are randomly generated as initial candidate solutions and are modified in each generation according to the GA's rules. The objective of the GA is to find the maximum load shedding for a fixed number of elements are under attack. The flowchart of the proposed algorithm is presented in Figure 1.
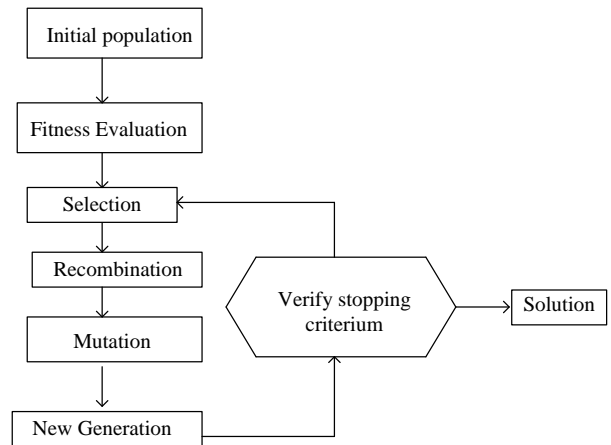

Fig. 1. Flowchart of the proposed GA

A. Problem Codification

As stated above, every solution candidate of the GA consists of a binary chain representing the interdiction vector. Figure 2 illustrates an interdiction vector for a power system of 10 elements over which the elements 3, 5 and 8 are under attack.

1	2	3	4	5	6	7	8	9	10
1	1	0	1	0	1	1	0	1	1

Fig. 2 GA Codification

B. Initial Population

The initial population is randomly generated and consists on a set of different interdiction vectors (every interdiction vector must have the same number of elements under attack). For each interdiction vector a DC optimal power flow is run in order to determine the load shedding (which is the fitness function of the GA). With such information the individuals are

ready to proceed for the next GA steps.

C. GA's Operators

The selection operator of the GA is performed by choosing the best solutions after applying a series of tournaments with a given number of elements. In this case, the number of candidates selected for the next step (recombination) is the same number of parents. The recombination is performed at a single point randomly selected. Every individual generates two new ones; in this stage two times the initial population is created. The mutation makes a minimal change in some of the individuals. The mutation is performed using a mutation factor (with a low probability) with every bit of the interdiction vector. If mutation or recombination leads to non feasible candidates, such candidates are penalized in the objective function. Finally, to keep the number of candidate solutions constant, only the best solutions are kept in each iteration.

IV. TESTS AND RESULTS

The proposed methodology was tested using two different systems: a didactic 5 bus power system which solution has already been provided in [9], and a prototype of the Colombian power system.

A. Case A. Five bus Power System

The first test is performed with the 5 bus power system illustrated in Figure 3. This system has been used only for comparison purposes, and to illustrate that the proposed GA is able to reach global optimal solutions. The data for this system are provided in Tables 1 and 2.
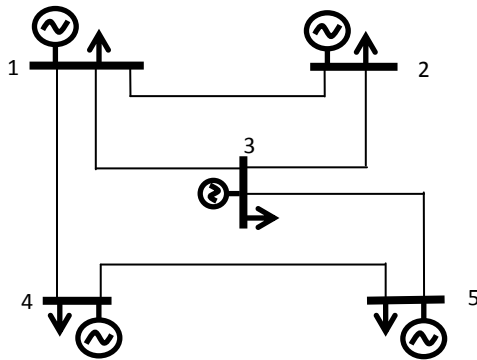

Fig. 3. Five bus power system.

TABLE I
LOAD AND GENERATION OF THE POWER SYSTEM PROVIDED IN FIG. 3

Bus	Load (MW)	Generation (MW)
1	50	150
2	170	150
3	90	150
4	30	150
5	300	150

TABLE II
LINE PARAMETERS OF THE POWER SYSTEM PROVIDED IN FIG. 3

Line	Impedance (p.u.)
1-2	0.336
1-3	0.126
1-4	0.180
2-3	0.215
3-5	0.215
4-5	0.130

After running several tests, for different numbers of lines under attack, the proposed algorithm was able to find the same results reported in [9]. These results correspond to globally optimal solutions. Table 3 summarizes the results obtained with the GA.

TABLE III
CRITICAL COMBINATION OF DESTROYED LINES FOR THE POWER SYSTEM PROVIDED IN FIG. 3

Number of Destroyed lines	Load Shedding (MW)	Worst combination of destroyed lines
1	50	3-5
		4-5
2	150	3-5, 4-5
3	150	1-2, 3-5, 4-5
		1-3, 3-5, 4-5
		1-4, 3-5, 4-5
		2-3, 3-5, 4-5
4	170	1-2, 2-3, 3-5, 4-5

It can be observed that for a single line under attack, the maximum load shedding obtained is 50 MW. In this case the line under attack must be either line 3-5 or line 4-5. Any other single attacked line would not result in load shedding. On the other hand, for two lines under attack there is only one strategy to obtain maximum load shedding (attacking lines 3-5 and 4-5 simultaneously). For a maximum of three lines under attack there are three possible interdiction vectors that would render a maximum load shedding of 150 MW. Finally, if only 4 lines could be taken down simultaneously, the maximum load shedding would be 170 MW.

B. Case B. Prototype of the Colombian Power System

To show the applicability of the proposed approach in real power systems, a prototype of the Colombian power system was considered. Due to security reasons, a real Colombian system with actual data can not be displayed. Figure 4 illustrates the system under study. This system has 20 nodes and 40 lines and is distributed in 5 sub-areas. The total demand of the system is 9010 MW and the installed capacity is 12850 MW. Specific line, load and generation data for this system can be consulted in [14]. Three different scneraios

were considered:

- *Scennario A*: Considering all generation units available.
- *Scenario B*: Limiting generation in sub-area 5. The generation availabe in node 18 was reduced to 42% (1500MW).
- *Scenario C*: Limiting generation in sub-area 3. The generation available in node 13 was reduced to 25% (500 MW).
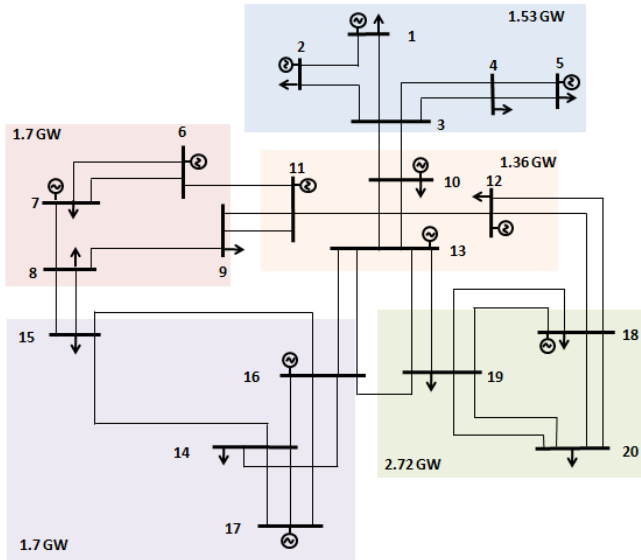

Fig. 4. Prototype of the Colombian power system.

Several tests were performed in each scenario, for different number of circuits under attack, to find the worst combination of destroyed lines. The GA was developed in Matlab and run in a computer with CORE I3 processor and 2Gb of RAM memory. The mutation rate was set to 5% and 100 parents were used in the initial population. The best results were found in only ten generations and around 300 seconds. Results are shown in Tables 4, 5 and 6.

As it can be seen in Figure 5, the more circuits under simultaneous attack, the higher the load shedding and cost of energy rationing.

TABLE IV
CRITICAL COMBINATION OF DESTROYED LINES FOR SCENARIO A.

Number of Destroyed lines	Load Shedding (MW)	Worst combination of destroyed lines
1	242.3	9-11
2	695.90	15-16, 17-14
3	1194.89	9-11, 15-16, 17-14
4	1694.89	7-8,9-11, 15-16, 17-14
5	2194.89	7-8,9-11,9-11, 15-16, 17-14
6	2428.20	7-8,9-11,9-11, 15-16, 17-14,20-18

TABLE V
CRITICAL COMBINATION OF DESTROYED LINES FOR SCENARIO B.

Number of Destroyed lines	Load Shedding (MW)	Worst combination of destroyed lines
1	291.70	9-11
2	772.35	16-19,20-23
3	1200.18	7-8,9-11,9-11
4	1892.40	7-8,9-11, 15-16, 17-14
5	2392.40	7-8,9-11,9-11, 15-16, 17-14
6	2490.04	7-8,9-11,9-11, 15-16, 17-14,20-18

TABLE VI
CRITICAL COMBINATION OF DESTROYED LINES FOR SCENARIO C.

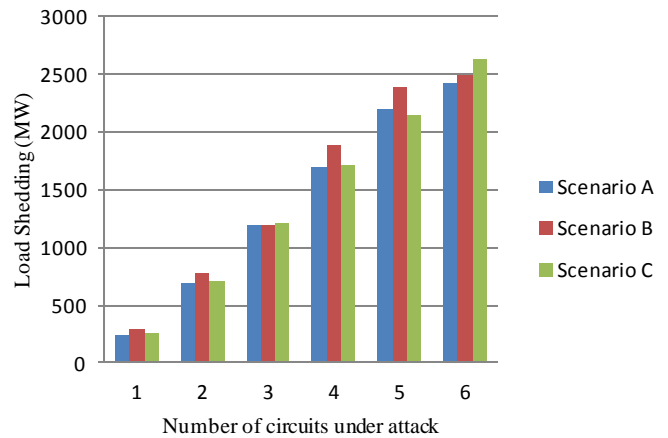| Number of Destroyed lines	Load Shedding (MW)	Worst combination of destroyed lines
1	264.90	20-18
2	718.17	15-16,17-14
3	1218.17	9-11,15-16,17-14
4	1718.17	7-8,9-11, 15-16, 17-14
5	2137.58	17-14,19-18,19-18,20-18,20-18
6	2637.58	9-11,17-14,19-18,19-18,20-18,20-18

Fig. 5 Load shedding for different scenarios and elements under attack.

Results show that Scenario C with 6 destroyed lines is the worst possible case in terms of load shedding. It causes 2637.58 MW of load shed, 29.27% of the total system demand. This attack would cause a bottled up of energy in bus 18 and load shedding in buses 4, 5, 8, 9, 10, 14, 19 and 20. Figure 6 illustrates the lines and buses affected.

The tests also revealed that sub-area 4 is the most sensitive to load shedding, especially buses 14 and 15. This is due to the fact that in this area the load is higher than the installed generation. Furthermore, such generation is mainly thermal which is the most expensive.
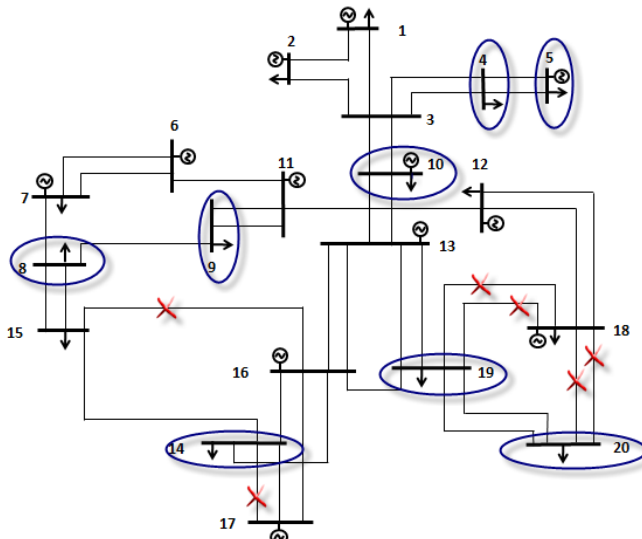

Fig. 6. Worst case Combination of DL

V. CONCLUSIONS

A specialized genetic algorithm for the electric grid interdiction problem was presented in this paper. The proposed approach is robust and efficient and can be applied to real power systems. The tests carried out with a prototype of the Colombian power system allowed to identify the most vulnerable lines in terms of terrorist attacks.

The main advantage of using a GA for solving the electric grid interdiction problem is the possibility of having a set of high quality solutions instead of a single one solution. This gives the system operator more information about its most vulnerable elements and provides signals for future reinforcements of the network or more strict surveillance on critical elements.

With the use of a GA instead of classical mathematical programming there is no need to bring into play duality theory or linearization schemes to transform the electric grid interdiction problem into a single-level optimization problem. This opens the possibility to approach the interdiction problem with a more accurate modeling of the network, such as an AC optimal power flow. This will be the focus of further work.

VI. ACKNOWLEDGMENT

VII. REFERENCES

[1] *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism,* Nat. Res. Council, Nat. Academy Press, Washington D.C., 2002.
[2] L. Leffler, "The NERC program for the electricity sector critical Infrastructure protection," in *Proc. Power Eng. Soc. Winter Meeting*, vol. 1, Columbus, OH, Jan.-Feb. 2001, pp. 95–97.
[3] Corredor P. and Ruiz M.: "Againts all Odds", IEEE Power & Energy Magazine, March – April 2011.
[4] Arragada G. "Evaluación de Confiabilidad en Sistemas Eléctricos de Distribución" Tesis de Maestría. Pontificia Universidad Católica de Chile. 1994.
[5] Kinney R., Crucitti P., Albert R., and Latora V. "Modeling cascading failures in the North American power grid". The European Physical Journal B 46, 2005, pp 101-107
[6] Salmeron J., Wood K. and Baldick R. 'Analysis of electric grid security under terrorist threat', IEEE Trans. Power Syst., 2004, 19, (2), pp. 905–912.
[7] R. E. Álvarez, "Interdicting electrical power grids," M.Sc. thesis, Naval Posgraduate School, Monterey, CA, 2004.
[8] J. Salmerón, K. Wood, and R. Baldick, "Optimizing electric grid design under asymmetric threat (II)," Naval Postgraduate School, Monterey, C.A., Tech. Rep. NPS-OR-04-001, 2004.
[9] Arroyo J. and Galiana F., "On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem", IEEE Trans. Power Syst., 2005, 20, (2), pp. 789-797.
[10] Motto L., Arroyo J., and Galiana F. "A mixed-integer LP procedure for the analysis of electric grid security under disruptive threat," IEEE Trans. Power Syst., 2005, 20, (3), pp. 1357-1365.
[11] D. Bertsimas and J. Tsitsiklis, *Introduction to Linear Optimization* Belmont, MA: Athena Scientific, 1997.
[12] Salmeron J., Wood K., and Baldick R. "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Trans. Power Syst.*, 2009, 24, (1), pp. 96-104.
[13] M. Arroyo and J.F. Fernandez, "A genetic algorithm approach for the analysis of electric grid interdiction with line switching", 15th *International conference on Intelligent System Applications to Power Systems (ISAP)*, Curitiba, Brazil, Nov. 2009.
[14] J.M López-Lezama, C.E Murillo-Sanchez, L.J. Zuluaga and J.F. Gutierrez-Gomez. "A contingency-based security-constraint optimal power flow model for revealing the marginal cost of a blackout risk equalizing policy in the Colombian energy market", *IEEE PES Transmission and Distribution Conference and Exposition*, Caracas, Venezuela, 2006.

VIII. BIOGRAPHIES

Laura Agudelo Zapata studied electrical engineering and currently She is studying a Master in Engineering at the University of Antioquia. She works at operation department in Interconexion Electrica S.A. Utility (ISA) in Medellin, Colombia. Her interests include power systems optimization and real time operation.

Jesús María Lopéz Lezama studied electrical engineering at Colombia's National University, where he also obtained a Master Degree. He obtained a Ph.D degree from the UNESP in Sao Paulo, Brazil. Currently he works at the department of electrical engineering in the University of Antioquia in Medellin, Colombia. His interests include power systems optimization and distributed generation.

Nicolás Muñoz Galeano studied electrical engineering at Universidad de Antioquia in Medellín, Colombia. He obtained a Ph.D degree from Universidad Politécnica de Valencia. Currently he works as an assistant professor at the department of electrical engineering in the University of Antioquia in Medellin, Colombia. His interests include power system electronics and electrical machines.