Contemporary Engineering Sciences, Vol. 11, 2018, no. 24, 1165 - 1184
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ces.2018.8399

Assessment of Power System Vulnerability Using Metaheuristic Techniques

Jesús M. López-Lezama[1], Juan J. Cortina[2] and Nicolás Muñoz Galeano[1]

[1] Departamento de Ingeniería Eléctrica, Facultad de Ingeniería
Universidad de Antioquia, Calle 67 No 53-108, Medellín, Colombia

[2] XM S.A E.S.P, -Filial de ISA, Calle 12 Sur No 18-168, Medellín, Colombia

Abstract

This paper presents a comparison of different metaheuristic techniques applied to the assessment of power systems vulnerability to intentional attacks, also kwon as the electric grid interdiction problem. This problem is described through a bilevel formulation and comprises the interaction between a disruptive agent (attacker) and the power system operator (defender). The attacker is positioned in the upper level optimization problem and aims at finding the set of devices (lines, transformers and generators) that, once simultaneously attacked, would maximize the system load shedding. This problem is constrained by a limit on destructive resources and the response of the power system operator, located in the lower level optimization problem that reacts to the attack by modifying the generation dispatch aiming at minimizing the load shedding. The interdiction problem described in this paper is nonlinear and nonconvex; therefore, four different metaheuristic techniques are implemented and compared for its solution: Genetic Algorithm, GRASP, Iterated Local Search and Tabu Search. Results show that the Iterated Local Search adapts better to this problem obtaining the best rate between quality of solutions and computation time.

Keywords: Genetic Algorithm, GRASP, Iterated Local Search and Tabu Search

1 Nomenclature

The nomenclature used throughout the document is provided here for quick reference.

Variables:

δ^{Gen}	Binary vector that indicates the state of a generator (0 off service, 1 on service).
δ^{Br}	Binary vector that indicates the state of a branch (0 off service, 1 on service).
P_{LS_n}	Active load shedding in bus n.
Q_{LS_n}	Reactive load shedding in bus n.
P_l^{Br}	Active power flow in branch l.
Q_l^{Br}	Reactive power flow in branch l.
S_l^{Br}	Apparent power flow in branch l.
θ_n	Voltage angle in bus n.
V_n	Voltage magnitude in bus n.
P_g^{Gen}	Active power generation provided by generator g.
Q_g^{Gen}	Reactive power generation provided by generator g.
P_n	Active power injection in bus n.
Q_n	Reactive power injection in bus n.

Parameters:

M	Limit on destructive resources.
M_l	Cost of attacking a branch.
M_g	Cost of attacking a generator.
P_{D_n}	Active power demand in bus n.
Q_{D_n}	Reactive power demand in bus n.
P_g^{min}	Minimum active generation of generator g.
P_g^{max}	Maximum active generation of generator g.
Q_g^{min}	Minimum reactive generation of generator g.
Q_g^{max}	Maximum reactive generation of generator g.
P_l^{min}	Minimum active power flow limit in line l.
P_l^{max}	Maximum active power flow limit in line l.
Q_l^{min}	Minimum reactive power flow limit in line l.

Q_l^{max}	Maximum reactive power flow limit in line l.
S_l^{min}	Minimum apparent power flow limit in line l.
S_l^{max}	Maximum apparent power flow limit in line l.
θ_n^{min}	Minimum voltage angle limit in bus n.
θ_n^{max}	Maximum voltage angle limit in bus n.
V_n^{min}	Minimum voltage magnitude limit in bus n.
V_n^{max}	Maximum voltage magnitude limit in bus n.
g_{mn}	Conductance of the branch connecting nodes m and n.
b_{mn}	Susceptance of the branch connecting nodes m and n.

Sets:

N	Set of buses.
G	Set of generators.
L	Set of branches.

2. Introduction

Electric power systems are vulnerable not only to random natural phenomena but also to deliberate attacks. Physical damage that results in the electric infrastructure from a malicious attack is similar to that caused by an extreme natural event; therefore, any analysis conducted with respect to intentional attacks can also help in taking preventions and corrective actions when random natural phenomena take place [1]. In this paper, the electric grid interdiction problem, also known as the terrorist threat problem, is approached. This problem is analyzed from the standpoint of physical attacks to the power system infrastructure rather than cyberattacks, which is a different topic and can be consulted in [2] and [3]. The electric grid interdiction problem was first formulated in [4] in a bilevel programming scheme involving the interaction of two agents: an attacker and a defender. The attacker is positioned in the upper level optimization problem and its objective is to cause de maximum damage to the network measured as load shedding. On the other hand, the defender (in this case the system operator) is located in the lower level optimization problem and reacts to the attack by modifying the generation dispatch in order to minimize the load shedding.

Since its introduction in [4], the electric grid interdiction problem has been the focus of several studies. In [5], the authors proposed a generalization of the interdiction problem in which the bilevel model allows the definition of different objective functions for the attacker and system operator. In this case, the goal of the upper level optimization problem consists on minimizing the number of branches to attack in order to obtain a specific goal on loss of load. In [6], two different interdiction models of minimum and maximum vulnerability are proposed. The minimum vulnerability model is based on the ones presented in [4] and [5], while the maximum vulnerability model consists on identifying the maximum level of system load shedding that can be obtained with a fixed number of simultaneous outages. In [7], the authors present a worst-case interdiction analysis of the electric grid interdiction problem. The model identifies a set of power system components (lines and transformers) which destruction maximizes economic losses to customers. In [8] and [9], line switching is introduced as an alternative strategy of the system operator to respond to deliberate attacks. In this case, the system operator is able to modify the system topology in order to minimize the loss of load. In [10], the authors present a power grid interdiction model that combines cascading effects and medium-term impacts. These last are evaluated by means of a DC optimal power flow model, while short-term impacts are addressed by a cascading outage analysis. In [11], the authors introduce an interdiction model that indicates where and when, over a specific time horizon, a power system is most vulnerable to intentional attacks. In [12], the investment planning of electric power systems is conducted taking into account a vulnerability assessment that considers intentional attacks. In this case, the authors use a Tabu Search (TS) metaheuristic to solve the proposed model.

Bilevel programming models are intrinsically nonlinear and nonconvex, which makes their solution a challenging task. A common way to approach such models is by recasting the original bilevel problem into an equivalent single-level equivalent model. This is usually done by replacing the lower level optimization problem by its Karush Kuhn Tucker (KKT) optimality conditions as done in [4]-[9]. The main drawback of this approach is that the lower level optimization problem must be linear. In this sense, a common feature of most interdiction models proposed in the specialized literature is that they use a linear modeling of the network (DC power flow model), which makes the problem easier to solve but neglects the effect of reactive power. However, some recent studies have been conducted approaching a nonlinear modelling of the network (AC power flow model). The first of them was introduced in [13] in which a genetic algorithm is proposed to solve the electric grid interdiction problem. In [14], the same problem is solved considering demand response. In both studies, the interdiction problem is solved in its original bilevel form since, due to its nonlinearity; it is not possible to replace the lower level optimization problem by its KKT optimality conditions. Therefore, the problem is approach by using metaheuristic techniques. This paper focuses on this last type of models. Also, it introduces as a new feature the consideration of generators as susceptible elements to be attacked. The proposed approach also considers an AC model of the network, which is more accurate than traditional DC power flow models. A comparison of different metaheuristic techniques used to solve the proposed model is presented. The solution of the electric grid interdiction problem provides a list of elements which simultaneous outages would maximize load shedding. This information is of paramount importance to system operators which can develop preventive or corrective actions aiming to minimize the impact of such outages.

The remaining of this document is organized as follows: in Section 3, the mathematical formulation of the AC interdiction problem is presented. In Section 4, the metaheuristics applied to solve the proposed model are described. In Section 5, several tests are performed using the IEEE 24 bus power system to study the performance of the proposed techniques. Finally, in Section 6, the conclusions are presented.

3 Mathematical Formulation

The electric grid interdiction problem approached in this paper is given by (1)-(20). Equations (1)-(4) represent the upper level optimization problem, while (5)-(20) represent lower level optimization problem or reaction of the system operator. In this case, all attacks are considered to be 100% effective and transient effects as well as cascading outages are not considered.

3.1 Upper level optimization problem

As previously mentioned, the objective function of the upper level optimization problem consists on maximizing the total load shedding given by (1). This problem is restricted by the limit on total destructive resources given by (2). In this case, the cost of attacking a branch (line or transformer) and a generator are different and are represented by M_l and M_g, respectively. Equations (3) and (4) account for the binary nature of δ_g^{Gen} and δ_l^{Br} that are binary decision variables representing the state of generator g and branch l, respectively. The upper level optimization problem is also constrained by the reaction of the system operator (lower level optimization problem) described below.

$$\max_{\delta_g^{Gen},\delta_l^{Br}} \sum_n P_{LS_n}; \qquad \forall n \in N \tag{1}$$

Subject to:

$$\sum_l \left(1-\delta_l^{Br}\right)M_l + \sum_g \left(1-\delta_g^{Gen}\right)M_g \leq M; \qquad \begin{array}{l}\forall l \in L\\ \forall g \in G\end{array} \tag{2}$$

$$\delta_g^{Gen} \in \{0,1\}; \qquad \forall g \in G \tag{3}$$

$$\delta_l^{Br} \in \{0,1\}; \qquad \forall l \in L \tag{4}$$

3.2 Lower level optimization problem

The objective function of the Lower level optimization problem is given by (5) and it is made of two terms. The first term is the cost of redispatching generation and the second one is the cost of load shedding (which is used as a last resource). This problem is subject to power system limits given by (6)-(12). In this case, (6) and (7) represent limits on voltage magnitudes and angles, respectively. Equations (8) and (9) stand for limits on active and reactive power generation, respectively. Equation (10) represents the apparent power limits on branches; while (11) and (12) indicate limits on active and reactive load shedding, respectively. In this case the load shedding must be lower than the total demand on the bus. Equations (13) and (14) represent the active and reactive power injections in bus *n*, respectively. Equation (15) indicates the components of the apparent power flow. Equations (16) and (17) represent the active and reactive power flow in braches, respectively. These expressions are multiplied by δ_l^{Br} that indicates whether the branch is on or off service. Equations (18) and (19) represent the active and reactive power balance constraints in all nodes. Note that generators are multiplied by their respective binary variable δ_g^{Gen} that indicates if they are on or off service. Finally, the reference angle constraint if given by (20).

$$\begin{gathered}\min_{\boldsymbol{x}} \sum_g c_g P_g^{Gen} + \sum_n c_{DS_n} P_{DS_n}; \\ \boldsymbol{x} = \begin{bmatrix} \theta_n, V_n, P_g^{Gen}, Q_g^{Gen}, P_l^{Br}, Q_l^{Br}, \\ P_{DS_n}, Q_{DS_n} \end{bmatrix}\end{gathered} \tag{5}$$

Subject to:

$$\theta_n^{min} \leq \theta_n \leq \theta_n^{max}; \qquad \forall n \in N \tag{6}$$

$$V_n^{min} \leq V_n \leq V_n^{max}; \qquad \forall n \in N \tag{7}$$

$$P_g^{min} \leq P_g^{Gen} \leq P_g^{max}; \quad \forall g \in G \tag{8}$$

$$Q_g^{min} \leq Q_g^{Gen} \leq Q_g^{max}; \quad \forall g \in G \tag{9}$$

$$S_l^{min} \leq S_l^{Br} \leq S_l^{max}; \quad \forall l \in L \tag{10}$$

$$0 \leq P_{LS_n} \leq P_{D_n}; \quad \forall n \in N \tag{11}$$

$$0 \leq Q_{LS_n} \leq Q_{D_n}; \quad \forall n \in N \tag{12}$$

$$P_n = V_n \sum_n V_m[g_{mn}\cos(\theta_{mn}) + b_{mn}\sin(\theta_{mn})]; \forall n \in N \tag{13}$$

$$Q_n = V_n \sum_n V_m[g_{mn}\sin(\theta_{mn}) + b_{mn}\cos(\theta_{mn})]; \forall n \in N \tag{14}$$

$$(S_l^{Br})^2 = (P_l^{Br})^2 + (Q_l^{Br})^2; \ \ \forall l \in L \tag{15}$$

$$P_l^{Br} = \delta_l^{Br} \cdot \begin{bmatrix} g_{mn}V_n^2 + g_{mn}V_mV_n\cos(\theta_{mn}) \\ -b_{mn}V_mV_n\sin(\theta_{mn}) \end{bmatrix}; \ \ \forall l \in L \tag{16}$$

$$Q_l^{Br} = \delta_l^{Br} \cdot [-b_{mn}V_n^2 + b_{mn}V_mV_n\cos(\theta_{mn}) - b_{mn}V_mV_n\sin(\theta_{mn})]; \quad \forall l \in L \tag{17}$$

$$\delta_g^{Gen} \cdot P_g^{Gen} - P_{D_n} + P_{DS_n} = P_n; \qquad \forall n \in N \tag{18}$$

$$\delta_g^{Gen} \cdot Q_g^{Gen} - Q_{D_n} + Q_{DS_n} = Q_n; \qquad \forall n \in N \tag{19}$$

$$\theta_{ref} = 0 \tag{20}$$

The model given by (1)-(20) is nonlinear and nonconvex. Note that decision variables on the upper level problem are parameters to the lower level problem. Once the attacker has decided which elements to render out of service, the system operator reacts to such attack plan by redispatching generation, minimizing the load shedding. This must be done considering the power system limits.

3.3 Problem codification

Taking into account the binary nature of the upper level optimization variables and the integer nature of a given list of power system elements, a candidate solution to the interdiction problem can be represented either by a binary or integer interdiction vector (IV). Fig. 1 illustrates an attack plan on a power system composed by 13 branches and 4 generators. In this case, there are 17 elements susceptible to be attacked. These elements are arranged in a list in which the first 13 positions are branches and the last 4 (element 14 to element 17) are generators. Note that the representation of an attack plan can be done either by a binary vector representing the list of the 17 elements and their respective state (1 means that the element is operative, while 0 represents that the element has been attacked), or by an integer vector that indicates in each entry the number of the element that was attacked. In this case, branches L1, L10, L12 and generator G3 were attacked. These correspond to elements 1, 10 12 and 16 of the list as can be seen in Fig. 1.

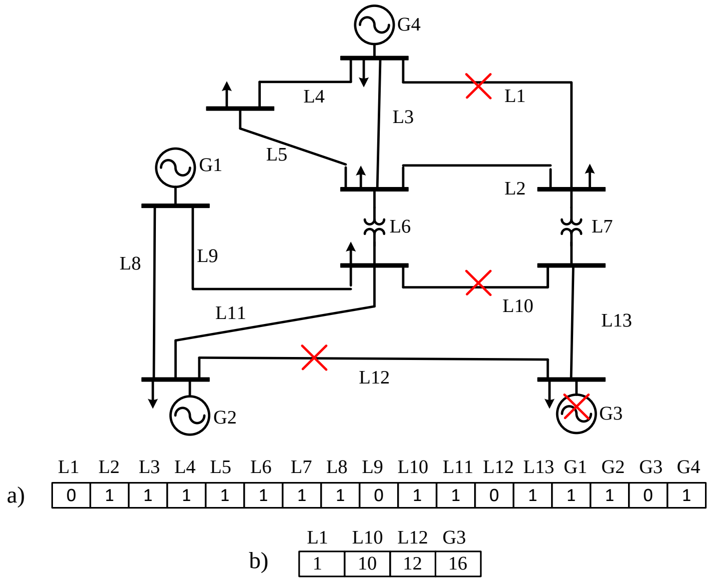

Fig.1 Representation of an attack plan through binary and integer interdiction vectors.

4. Implemented Metaheuristics

Metaheuristics are methodologies that can solve combinatorial optimization problems of high mathematical complexity with low computational effort. They are especially well suited to solve nonlinear, nonconvex and multimodal optimization problems such as the one described in this paper. There are a bunch of metaheuristic techniques that can be applied to solve the electric grid interdiction problem. In this paper four of them have been selected in order to compare their performance. The selection of these metaheuristics was based basically on the familiarity that the authors have with them, their ease of implementation and their proved effectiveness to tackle complex mathematical problems. A brief description of each metaheuristic is provided in this section. A detail description of each of them is out of the scope of the present paper. However, the interested reader can consult [15] and [16] for a more in depth discussion and details of these techniques.

4.1 Genetic Algorithm (GA)

Genetic Algorithms are based on an adaptive search based on the Darwinian principle of reproduction and survival of individuals that best adapt to a given environment. GAs have been successfully applied for solving highly complex problems related with the planning and operation of power systems as shown in [17] and [18]. Given an initial population, it is successively subjected to the stages of selection, recombination and mutation in order to find better individuals until a stopping criterion is met (see Fig.2) [19].

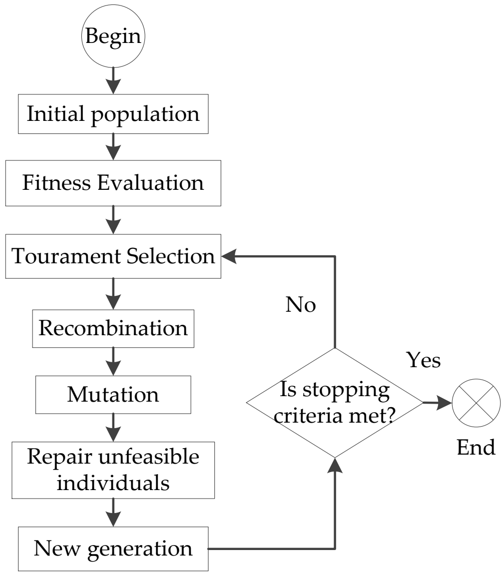

Fig. 2. Flowchart of the implemented GA.

In the implemented GA, the solution candidates or interdiction vectors represent the individuals of a population (see Fig. 1). The GA starts with a set of N different individuals (N being the size of the population which remains constant). Given certain limits of destructive resources, the creation of the initial population in done in such a way that they do not excess such limit (constrain given by (2)). The objective function of the initial population is evaluated as indicated by (1). This step is known as fitness evaluation; for this, an optimal power dispatch is computed to account for the reaction of the system operator using the software Matpower [20].

The individuals of the next generation are obtained by tournament selection. Such individuals are called parents and must go through the stage of recombination and mutation to generate new individuals (offspring). Mutation is done by selecting a position of the interdiction vector and changing its status.
In the recombination and mutation processes some individuals might turn out to violate constraint (2). In this case, they must be repaired; that is done by reducing the number of elements under attack until constraint (2) is enforced. A new generation is composed of the best N individuals obtained from the combined population of parents and offspring. The GA stops when a maximum number of iterations is reached.

4.2 Greedy Randomized Adaptive Search Procedure (GRASP)

This method consists on iterations made up from successive constructions of a greedy randomized solution and improvements of it through a local search. The GRASP metaheuristic has basically two phases: a greedy randomized constructive phase which is in charge of generating an initial solution and a local search that finds a local minimum of such solution.

The constructive phase of the GRASP is illustrated in Fig. 3. This phase initiates with an empty IV. A binary representation with zeros in all entries is suitable in this case (see Fig. 3). Then random attacks are added to the IV. In this case, it must be taken into account the fact that the Required Destructive Resources (RDR) do not exceed a predefined limit denoted as *M*. In this way, constraint (2) is enforced. Then, if the RDR exceeds *M*, the last element added to the IV is discarded. The procedure is done until a predefined number of different IVs is created.

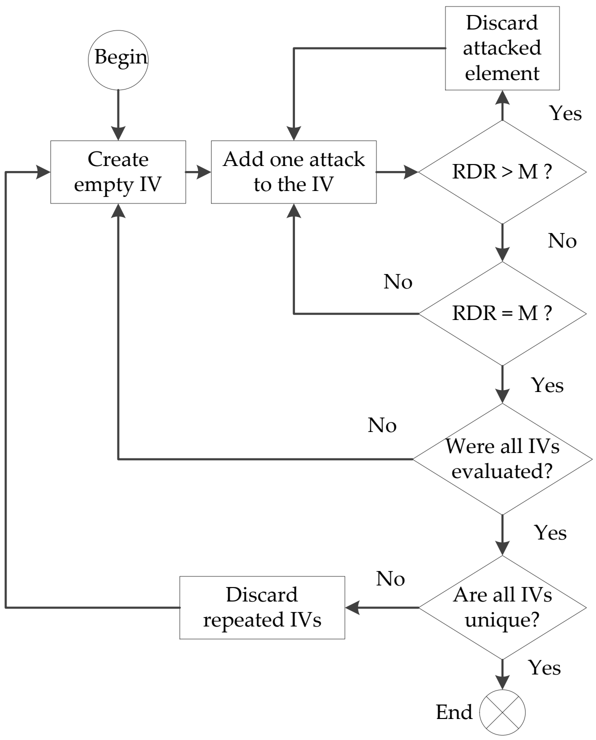

Fig. 3. Constructive phase of the GRASP metaheuristic.

Fig. 4 illustrates the flowchart of the implemented GRASP metaheuristic. Initially a set of IVs is built using the constructive phase illustrated in Fig.3. Then, one of the IVs is selected and its objective function is obtained. For this, the lower level optimization problem (reaction of the system operator) must be computed. This is done by solving the optimization problem given by (5)-(20) using as parameters the information of the attack plan indicated by the IV (operative states of branches and generators). Once this is done, a local search is performed to look for better solutions. The procedure is repeated until all IVs created in the constructive phase are evaluated. The best IV is selected as the solution.

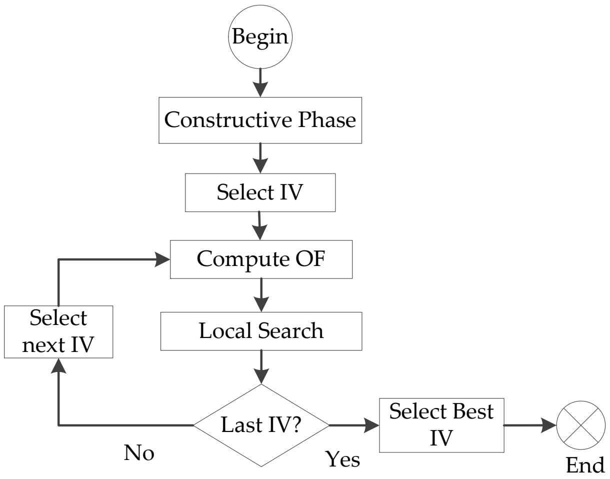

Fig. 4. Flowchart of the implemented GRASP metaheuristic.

4.3 Iterated Local Search (ILS)

This technique belongs to the category of neighborhood-search metaheuristics. It is based on finding a locally optimal solution by perturbing a current solution and applying local search [20]. Fig. 5 illustrates this procedure. Starting from a given initial solution (that can be obtained with a constructive algorithm), the ILS finds a local optimal solution. Then, a perturbation is applied and the algorithm starts from a different location in the search space to look again for a locally optimal solution.

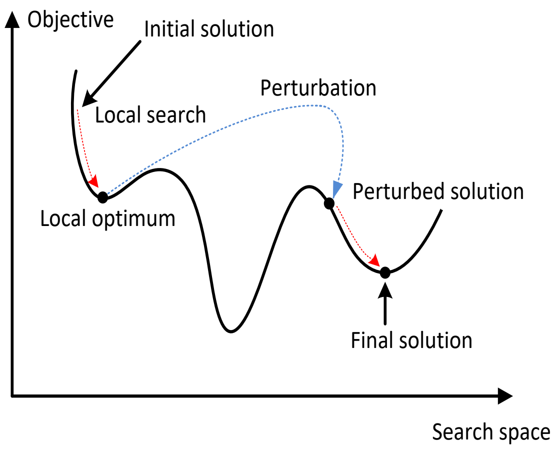

Fig. 5. Iterated local search representation.

ILS algorithms can be combined or hybridized with other metaheuristics as shown in [21] and [22]. The ILS implemented in this paper begins with an initial solution provided by a constructive heuristic algorithm. The local search is performed over a variable neighborhood in a two-step procedure, which guarantees both diversification and intensification. The initial solution for the ILS is found applying the constructive heuristic depicted in Fig. 3. Once an initial solution is given, a local search is performed.

The local search implemented within the ILS metaheuristic is performed in two steps. In the first step, a random and simultaneous variation of two IV components is performed. Such variation is accepted if the new IV does not violate constraint (2) and its new objective function is better than the current solution. The procedure stops after a given number of variations is executed, or after the first improvement of the objective function is reached. The second step of the local search is given by the random variation of each component of the IV; the stopping criterion is the same as the one described for the first step. Fig. 6 illustrates the implemented ILS. In this case, the stopping criterion is the maximum number of iterations.

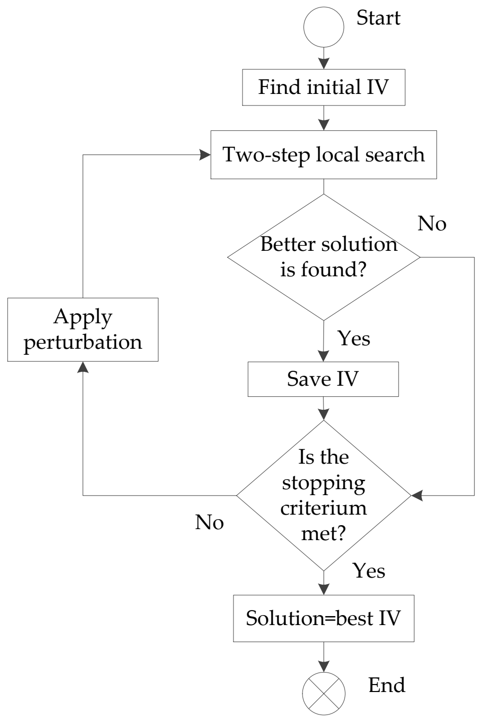

Fig. 6. Flowchart of the implemented ILS.

4.4 Tabu Search (TS)

This method belongs to the category of local search metaheuristics. The TS uses a neighborhood search procedure to move iteratively between solution candidates until a stopping criterion is satisfied. This technique modifies the structure of the neighborhood as the search progresses and uses a short-term memory (called tabu list) to avoid visiting regions that were explored in the recent past [16].

The implemented TS uses an integer representation of the interdiction vectors (see Fig. 1). It starts with an initial solution that is feasible in destructive resources (it complies with constraint (2)). This first solution is designed in such a way that only considers attacks on generators. The objective function of this first solution is saved as the best current solution. Subsequently, a neighborhood search is performed that consists on changing the types of elements to be attacked. It starts with the change of the first two components of the IV by two new components, continuing with the next two and so on. As the amount of resources diploid to attack a generator are supposed to be greater than those necessary to attack a branch; an attack on a generator can be replaced in the IV by its equivalent in number of branches. This requires a mechanism to stablish the ratio M_g/M_l. Fig 7a illustrates an example of the local search with an IV = [1 10 12 16] where the last element corresponds to the attack on a generator. If the ratio M_g/M_l is 2, the attack to generator G3 can be replaced by the attack of two branches maintaining the same cost of the solution to the attacker. If the ratio is not an integer value it is approximated to the lower integer value. In Fig. 7b the attack on two lines (L1 and L10) is replaced by the attack on two other lines (L3 and L4). In this case, the same destructive resources are required.

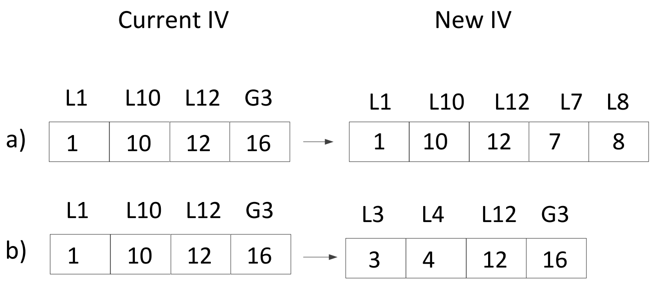

Fig. 7. Illustration of the local search used in the TS algorithm.

The elements that are initially exchanged in the IV are saved in the tabu list; indicating that they cannot be part of new candidate solutions at least for a given number of iterations. The aspiration criterion allows invalidating this assumption if these elements, when integrated to the IV result in better solutions (greater values of load shedding) than those currently found by the algorithm. Fig. 8 depicts the flow chart of the implemented TS. In this case, the initial solution can be obtained with a constructive heuristic, such as the one illustrated in Fig. 3 or it can be randomly generated. The algorithm stops when a maximum number of iterations is reached. More details on TS applications can be consulted in [16].

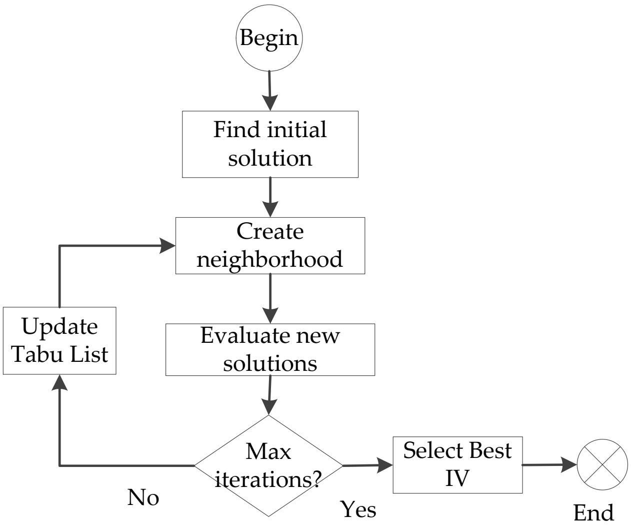

Fig. 8. Flowchart of the TS algorithm.

5 Tests and Results

In order to compare the performance of the proposed techniques several tests were performed on the IEEE 24 bus reliability test system [23]. This system comprises 24 buses, 38 branches, 11 generators and 17 loads. All tests were performed for a winter day at 18:00 with a total demand of 2850MW. Minimum generation limits, for all generators, were considered to be 0 MW. On the other hand, minimum and maximum voltage magnitude limits in all buses were considered to be 0.95 and 1.05 p.u, respectively.

For the sake of simplicity destructive resources (M) are given in integer numbers expressed as monetary units. It was assumed that the cost of attacking a branch is M_l=1 while the cost of attacking a generator is M_g=2. All simulations were performed on a laptop with 4.0GB of RAM and a core-i5 processor. Each of the parameters of the proposed metaheuristics was calibrated by trial and error. After several executions to calibrate the parameters of the metaheuristics, the best results were obtained with the following values:
ILS: 30 perturbations starting form an initial solution and 30 iterations in each local search.
GRASP: 500 initial candidates obtained from the constructive heuristic (Fig. 2) and 30 iterations in each local search.
AG: 100 initial individuals, 50 generations, mutation rate of 5% and single point crossover.
TS: 50 iterations. The elements in the tabu list were kept 5 iterations before being considered as components of new solutions.

Table 1, Table 2 and Table 3 present the best results obtained with the metaheuristics for M=4, M=5 and M=6, respectively. In this case, a branch is represented by the nodes it links, separated by a hyphen (-); while a generator is represented prefixing the letter G to the node where it is located. LS in the third column stands for load shedding.

Since attacking a branch costs 1 monetary unit and attacking a generator costs 2 monetary units; with M=4 the disruptive agent would be able to simultaneously attack 4 branches, 2 generators, or 1 generator and two branches. The results with M=4 are presented in Table 1. In this case ILS, GRASP and AG techniques obtained the same solution which consists on attacking generators on buses 13 and 23. This attack plan aims at reducing the generation capacity of the system and would result in a load shedding of 725.63 MW (25.46% of the total demand). On the other hand, the solution obtained with the TS was very similar in load shedding but with a completely different strategy: in this case, the interdiction plan consists on attacking branches 12-23, 13-23, 14-16 and 15-24, which would result in a load shedding of 724.47 MW (25.42% of the total demand). Note that both solutions reported in Table 1 are quite similar, however the TS was able to find the interdiction plan much faster than any other metaheuristic (see fourth column of Table 1).

Table 1. Best interdiction plans with different techniques for $M = 4$.

Technique	Interdiction plan	LS (MW)	Time (s)
ILS	G13, G23	725.63	813.06
GRASP	G13, G23	725.63	4095.98
GA	G13, G23	725.63	954.74
TS	12-23, 13-23, 14-16, 15-24	724.47	411.17

Table 2 presents the best results obtained with M=5 for the four techniques under study. The attack plans are also illustrated in Fig. 9. In this case, the ILS and GRASP obtained the same solution that consists on attacking the generators in buses 13 and 23 plus the branch connecting nodes 7-8. This attack plan would result in 896.17 MW of load shedding (31.44% of the total demand). Note that this solution contains the one already found by both techniques with M=4 (see Table 1) and incorporates a new attack on a branch. In this case, attacking branch 7-8 isolates the generator in bus 7 (see Fig. 9a); so that the total effect is as if three generators were under attack. In this case the GA and TS techniques found different attack plans with similar load shedding: 881.86 MW and 848.97 MW, respectively. The solution found by the GA consists on attacking 3 branches and 1 generator, while the solution found by the TS consist on attacking 5 branches. Both solutions are similar in quality as those found by the ILS and GRASP; however, the TS found the solution faster than the other techniques (see column 4 on Table 2).

The best attack plans obtained with the four metaheuristics with M= 6 are presented in Table 3 and illustrated in Fig 10. The ILS and GRASP found the best results considering an attack on four branches and one generator (see Fig 10a) which would result in 1115.4 MW of load shedding (39,13% of the total demand).

Table 2. Best interdiction plans with different techniques for *M* = 5.

Technique	Interdiction plan	LS (MW)	Time (s)
ILS	7-8, G13, G23	896.17	804.05
GRASP	7-8, G13, G23	896.17	5083.03
GA	15-21, 15-21, 16-17, G23	881.86	1208.39
TS	9-12, 10-12, 11-13, 14-16, 15-24	848.97	712.70

Table 3. Best interdiction plans with different techniques for *M* = 6.

Technique	Interdiction plan	LS (MW)	Time (s)
ILS	12-23, 13-23, 14-16, 15-24, G13	1115.40	1216.22
GRASP	12-23, 13-23, 14-16, 15-24, G13	1115.40	7047.75
GA	3-24, 7-8, 9-12, 10-12, 11-13, 14-16	1019.50	1608.33
TS	1-5, 3-24, 11-13, 12-13, 12-23, 14-16	850.76	1025.89

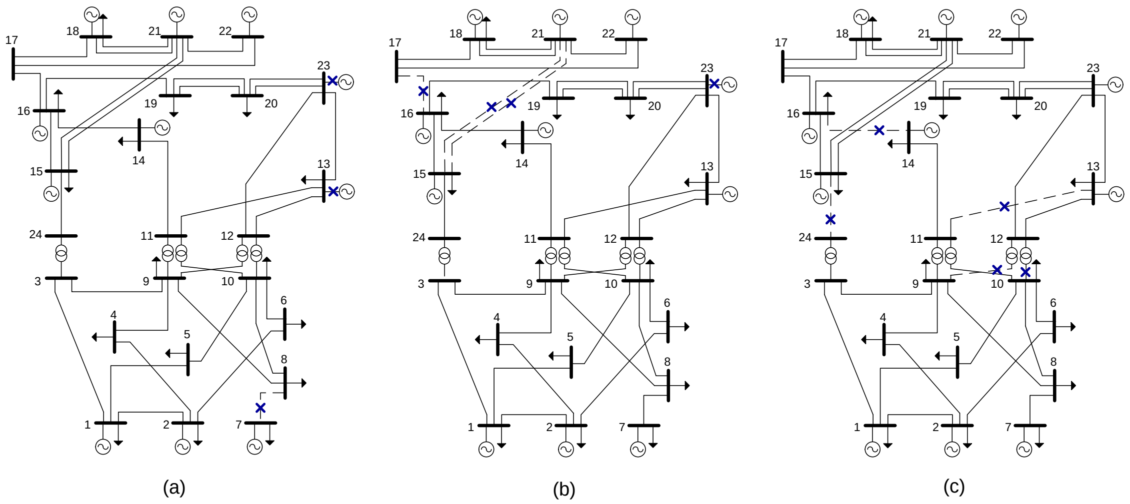

Fig. 9. Best attack plans with M=5 found by: a) ILS and GRASP, b) AG and c) TS.

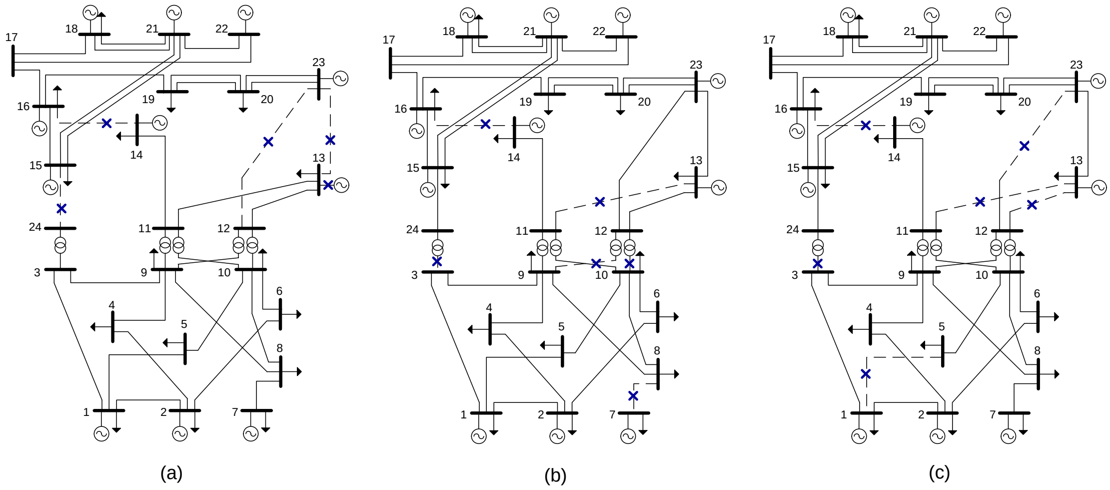

Fig. 10. Best attack plans with M=5 found by: a) ILS and GRASP, b) AG and c) TS.

The best solution found with the GA for M=6 is completely different from the one found by the ILS and GRASP. However it is very similar in terms of quality. In this case, the resulting load shedding would be 1019.50 MW (35.77% of the total demand) only 1.36% lower than the one obtained with ILS and GRASP techniques with respect to the total demand. Finally the TS found a solution of less quality resulting in 850.76 MW of load shedding (29.85% of the total demand).
As regards computational time, the GRASP technique always took more time that the other metaheuristics. The second most time consuming technique was the GA followed by ILS and finally TS that was the fastest technique.

6. Conclusions

This paper presented a comparison of four metaheuristic techniques applied to the electric grid interdiction problem. The implemented methods were: ILS, GRASP. GA and TS. The techniques under study allows to identify the most critical elements in terms of the load shedding that they might cause if they are simultaneously attacked. Identifying this set of elements is of paramount importance to the system operator and system planner in order to take preventive and corrective actions aiming at minimizing the damage cause by natural phenomena or deliberate attacks.

The tests carried out with the IEEE 24 bus reliability test system showed the applicability of all the techniques as well as their strengths and weaknesses. In particular, it was found that the ILS and GRASP techniques were able to find solutions of better quality than those obtained by the AG and TS methods. However, it was observed that the TS is able to find high quality solutions in less computational time than the other techniques. Nevertheless; when the number of attack elements is incremented, the quality of the solutions found by the TS were deteriorated. A future work will include more details in the modeling of the network such as the effect of distributed generation and demand response as well as other metaheuristic techniques.

Acknowledgments. The authors would like to acknowledge the University of Antioquia for the support provided by the "proyecto de sostenibilidad".

References

[1] P. H. Corredor, M. E. Ruiz, Against All Odds, *IEEE Power Energy Mag.*, **9** (2011), 59-66. https://doi.org/10.1109/mpe.2011.940266

[2] Y. Zhang, Y. Xiang, L. Wang, Power System Reliability Assessment Incorporating Cyber Attacks Against Wind Farm Energy Management Systems, *IEEE Trans. Smart Grid*, **8** (2017), 2343-2357. https://doi.org/10.1109/tsg.2016.2523515

[3] Y. Zhang, L. Wang, Y. Xiang, C. W. Ten, Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation, *IEEE Trans. Power Syst.*, **6** (2016), 4379-4394. https://doi.org/10.1109/tpwrs.2015.2510626

[4] J. Salmeron, K. Wood, R. Baldick, Analysis of electric grid security under terrorist threat, *IEEE Trans. Power Syst.*, **19** (2004), 905-912. https://doi.org/10.1109/tpwrs.2004.825888

[5] J. M. Arroyo F. D. Galiana, On the solution of the bilevel programming formulation of the terrorist threat problem, *IEEE Trans. Power Syst.*, **20** (2005), 789-797. https://doi.org/10.1109/tpwrs.2005.846198

[6] J. M. Arroyo, Bilevel programming applied to power system vulnerability analysis under multiple contingencies, *IET Generation, Transmission & Distribution*, **4** (2010), 178-190. https://doi.org/10.1049/iet-gtd.2009.0098

[7] J. Salmeron, K. Wood, R. Baldick, Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids, *IEEE Trans. Power Syst.*, **24** (2009), 96-104. https://doi.org/10.1109/tpwrs.2008.2004825

[8] A. Delgadillo, J. Arroyo, N. Alguacil, Analysis of electric grid interdiction with line switching, *IEEE PES General Meeting*, (2010). https://doi.org/10.1109/pes.2010.5588117

[9] L. Zhao B. Zeng, Vulnerability Analysis of Power Grids with Line Switching, *IEEE Trans. Power Syst.*, **28** (2013), 2727-2736.

https://doi.org/10.1109/tpwrs.2013.2256374

[10] Y. Wang and R. Baldick, Interdiction Analysis of Electric Grids Combining Cascading Outage and Medium-Term Impacts, *IEEE Trans. Power Syst.*, **29** (2014), 2160-2168. https://doi.org/10.1109/tpwrs.2014.2300695

[11] S. Sayyadipour, G. R. Yousefi, M. A. Latify, Mid-term vulnerability analysis of power systems under intentional attacks, *Transm. Distrib. IET Gener.*, **10** (2016), 3745-3755. https://doi.org/10.1049/iet-gtd.2016.0052

[12] N. Romero, N. Xu, L. K. Nozick, I. Dobson, D. Jones, Investment Planning for Electric Power Systems Under Terrorist Threat, *IEEE Trans. Power Syst.*, **27** (2012), 108-116. https://doi.org/10.1109/tpwrs.2011.2159138

[13] L. Agudelo, J. M. López-Lezama, N. Muñoz, Análisis de Vulnerabilidad de Sistemas de Potencia Mediante Programación Binivel, *Inf. Tecnológica*, **25** (2014), 103-114. https://doi.org/10.4067/s0718-07642014000300013

[14] J. J. Cortina, J. M. López-Lezama, N. Muñoz-Galeano, Modelo de Interdicción de Sistemas de Potencia considerando el Efecto de la Respuesta a la Demanda, *Inf. Tecnológica*, **28** (2017), 197-208. https://doi.org/10.4067/s0718-07642017000300020

[15] M. Eremia, C.-C. Liu, A.-A. Edris, *Advanced Solutions in Power Systems:HVDC, FACTS, and Artificial Intelligence*, Wiley-IEEE Press, 2016.

[16] C. Lagos, B. Crawford, R. Soto, E. Cabrera, J. Vega, F. Johnson, F. Paredes, Improving Tabu Search Performance by Means of Automatic Parameter Tuning, *Can. J. Electr. Comput. Eng.*, **39** (2016), 51-58. https://doi.org/10.1109/cjece.2015.2496338

[17] A. Ghadiri, M. R. Haghifam, S. M. M. Larimi, Comprehensive approach for hybrid AC/DC distribution network planning using genetic algorithm, *Transm. Distrib. IET Gener.*, **11** (2017), 3892-3902. https://doi.org/10.1049/iet-gtd.2016.1293

[18] C. Zhang, H. Chen, H. Ngan, Z. Liang, M. Guo, D. Hua, Solution of reactive power optimization including interval uncertainty using genetic algorithm, *Transm. Distrib. IET Gener.*, **11** (2017), 3657-3664. https://doi.org/10.1049/iet-gtd.2016.1195

[19] Fitriyani, E. S. Quartian, Y. Sibaroni, F. Nhita, Parallel genetic algorithm for traveling salesman problem on graphic processing unit, *J. Innov. Technol. Educ.*, **3** (2016), 139-146. https://doi.org/10.12988/jite.2016.6829

[20] R. D. Zimmerman, C. E. Murillo-Sanchez, R. J. Thomas, MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education, *IEEE Trans. Power Syst.*, **26** (2011), 12-19. https://doi.org/10.1109/tpwrs.2010.2051168

[21] E. A. Lemamou, P. Galinier, S. Chamberland, A Hybrid Iterated Local Search Algorithm for the Global Planning Problem of Survivable 4G Wireless Networks, *IEEEACM Trans. Netw.*, **24** (2016), 137-148. https://doi.org/10.1109/tnet.2014.2362356

[22] L. Thurner, A. Scheidler, A. Probst, M. Braun, Heuristic optimization for network restoration and expansion in compliance with the single-contingency policy, *Transm. Distrib. IET Gener.*, **11** (2017), 4264-4273. https://doi.org/10.1049/iet-gtd.2017.0729

[23] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, C. Singh, The IEEE Reliability Test System-1996. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee, *IEEE Trans. Power Syst.*, **14** (1999), 1010-1020. https://doi.org/10.1109/59.780914

Received: March 29, 2018; Published: April 25, 2018