International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 9 (2020), pp. 2313-2317
 https://dx.doi.org/10.37624/IJERT/13.9.2020.2313-2317

An Approach to the Power System Interdiction Problem Considering Reconfiguration

Esteban López Arcila[1], Jesús María López-Lezama[2] and Nicolás Muñoz-Galeano[3]

[1]Departamento de Ingeniería Eléctrica, Universidad de Antioquia Calle 70 No 52-21, Medellín 050010, Colombia,

[2]Departamento de Ingeniería Eléctrica, Universidad de Antioquia Calle 70 No 52-21, Medellín 050010, Colombia,

[3]Departamento de Ingeniería Eléctrica, Universidad de Antioquia Calle 70 No 52-21, Medellín 050010, Colombia,

ORCIDs: 0000-0003-0039-8963 (Esteban), 0000-0002-2369-6173 (Jesús), 0000-0003-1407-5559 (Nicolás)

Abstract

This paper presents a metaheuristic approach to solve the power system interdiction problem considering reconfiguration. The problem consists on the interaction of two agents: an attacker that aims at causing the greatest damage to the network in terms of load shedding, and the system operator who reacts by re-dispatching available energy resources, and also by altering the topology of the system. The interaction of these two agents is modeled as a bilevel programing problem and solved by means of a genetic algorithm. Several tests were performed on a benchmark power system evidencing the applicability of the proposed approach. It was found that reconfiguration of the power system is a valuable strategy for reducing load shedding caused by intentional attacks.

Keywords: Power systems, Interdiction problem, Genetic Algorithm, Reconfiguration.

I. INTRODUCTION

Electric power systems are exposed not only to natural occurring phenomena but also to intentional attacks [1]. The classic approach to assess power system vulnerability consists on the so called N-1 and N-2 security criterion. This means that the system must be able to operate within specified limits when one or two elements are rendered out of service. Despite of the fact that this approach provides a useful insight regarding the security of a network, it does not take into account the fact that power lines are susceptible to malicious attacks.

The first approach to model the interdiction problem in power systems within an attacker-defender model was proposed in [2]. The attacker aims at maximizing the damage caused to the power system by destroying lines; while the defender is the system operator that must change the generation dispatch to minimize load shedding. The interaction of these agents is modeled as a bilevel programming problem. The attacker or disruptive agent is located in the upper-level optimization problem and the system operator is located in the lower-level optimization problem.

Since the seminal work reported in [2], several studies have been performed to approach the bilevel attacker-defender problem (also known as the terrorist threat problem or interdiction problem). In [3], the authors presented a generalization of the interdiction problem that allows to define different objective functions for the attacker and defender. The goal of the disruptive agent is to minimize the number of power system components that must be rendered out of service so that the load shedding is greater or equal to a specified level. Such goal is contrasted with the assumption that the system operator will deploy strategies to mitigate the impact of the attack. In [4] the authors introduced transmission line switching as a binary variable in the lower-level optimization problem to account for another strategy of the system operator to mitigate the impact of deliberate attacks. In [5], the authors introduced cascading outages in the interdiction problem to consider short-term and medium-term impacts on the system.

The attacker-defender model has also been introduced within the expansion problem of electric power systems as reported in [6] and [7]. In both papers, the bilevel programming framework is expanded into a tri-level optimization model which considers the system planner as the upper-level agent that must find the right set of reinforcements to minimize the damage caused by a disruptive agent (located in the middle-level optimization problem), which in turn must anticipate the reaction of the system operator (located in the lower-level optimization problem). Recent studies have also combined cyber and physical attacks within a similar attacker-defender structure as presented in [8].

Vulnerability assessment using a bilevel approach is a challenging nonconvex discrete optimization problem [9].

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 9 (2020), pp. 2313-2317
 https://dx.doi.org/10.37624/IJERT/13.9.2020.2313-2317

These types of problems are better handled by metaheuristic techniques than by classic mathematical optimization [10]. In this paper, the interdiction problem is solved through a genetic algorithm (GA) that considers reconfiguration. Several tests were performed on the IEEE 24 bus reliability test system showing the applicability of the proposed approach. It was found that reconfiguration is an attractive option to reduce the impact of malicious attacks in power systems. The rest of the document is organized as follows: Section II presents the mathematical formulation of the problem, Section III describes the methodology implemented to solve the proposed model, Section IV describes the tests and results; and finally, conclusions are presented in Section V.

II. PROBLEM FORMULATION

II.I Upper level optimization problem

The objective of the disruptive agent is to maximize the total load shedding as indicated in equation (1); where ΔP_n^d is the active load shedding at bus *n*. The lower index *n* indicates the number of the bus, while the upper index *d*, refers to the demand, IV is the binary interdiction vector and N is the set of buses. The size of the interdiction vector is equal to the number of lines. The entries of the interdiction vector take the value one if the corresponding line is on service and zero if it is under attack. Equation (2) indicates the limit of destructive resources, where M is the number of lines under attack and IV_l is the l^{th} entry of the interdiction vector. Equation (3) indicates the nature of the interdiction vector entries and Equation (4) represents the reaction of the system operator.

$$\underset{IV}{Max} \sum_{n \in N} \Delta P_n^d; \qquad \forall n \in N \tag{1}$$

Subject to:

$$\sum_{l \in L} (1 - IV_l) = M; \qquad \forall l \in L \tag{2}$$

$$IV_l \in \{0,1\} \tag{3}$$

$$Reaction\ of\ the\ System\ Operator \tag{4}$$

II.II Lower level optimization problem

The lower-level optimization problem corresponds to the reaction of the system operator. The details of this problem are presented below.

A) Lower-Level Objective Function

The objective function given by (5) is exactly the opposite of the disruptive agent, which corresponds to the minimization of the total load shedding.

$$Min \sum_{n \in N} \Delta P_n^d; \qquad \forall n \in N \tag{5}$$

B) Power Balance Equations

Net injections of active and reactive power must be zero as indicated by (6) and (7). In this case, P_n^G indicates the active power generation provided by a generator located at bus *n*; while P_n and P_n^d represent the active power injection and demand at bus *n*, respectively. Finally, N indicates the set of nodes. Note that the same components are considered for reactive power in (7).

$$P_n^G - P_n^d + \Delta P_n^d - P_n = 0; \qquad \forall n \in N \tag{6}$$

$$Q_n^G - Q_n^d + \Delta Q_n^d - Q_n = 0; \qquad \forall n \in N \tag{7}$$

C) Limits on Active and Reactive Power Generation

Constraints given by (8) and (9) indicate limits on active and reactive power respectively. In this case, upper scripts min and max indicate the type of limit; while J indicates the set of generators.

$$P_j^{G\_min} \le P_j^G \le P_j^{G\_max}; \qquad \forall j \in J \tag{8}$$

$$Q_j^{G\_min} \le Q_j^G \le Q_j^{G\_max}; \qquad \forall j \in J \tag{10}$$

D) Voltage limits

The AC representation of the network considers limits on magnitude and voltage angles as indicated in (11) and (12), respectively. In this case, V_n and θ_n indicate magnitude and angle of the voltage at bus n, respectively.

$$V_n^{min} \le V_n \le V_n^{max}; \qquad \forall n \in N \tag{11}$$

$$\theta_n^{min} \le \theta_n \le \theta_n^{max}; \qquad \forall n \in N \tag{12}$$

E) Power Flow Limits

Power flow limits must be enforced in normal operation and under any attack. Equations (13) and (14) indicate the active and reactive power flow in a given line. Note that the power flow expressions are multiplied by the corresponding entry of the interdiction vector. If a given position of the interdiction vector is zero (indicating that the element is under attack) the corresponding power flows must be zero. In this case, g_{mn} and b_{mn} are the conductance and susceptance of line l_{mn}, respectively. Equations (16) and (17) indicate the apparent power and its limits, respectively. P_{lmn} and Q_{lmn} are the active and reactive power flow in line l_{mn}, respectively, while S_{lmn}^f indicates the apparent power flow on the same line.

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 9 (2020), pp. 2313-2317
 https://dx.doi.org/10.37624/IJERT/13.9.2020.2313-2317

$$P_{lmn}^{f} = (IV_l) * [V_n^2 g_{mn} - V_n V_m g_{mn} \cos(\theta_{mn}) - V_n V_m b_{mn} \operatorname{sen}(\theta_{mn})]; \ \forall l \in L \quad (13)$$

$$Q_{lmn}^{f} = IV_l) * [-V_n^2 b_{mn} + V_n V_m b_{mn} \cos(\theta_{mn}) - V_n V_m g_{mn} \operatorname{sen}(\theta_{mn})]; \quad \forall l \in L \quad (14)$$

$$S_{lmn}^{2} = P_{lmn}^{2} + Q_{lmn}^{2}; \quad \forall l \in L \quad (16)$$

$$S_{lmn}^{fmin} \leq S_{lmn}^{f} \leq S_{lmn}^{fmax}; \quad \forall l \in L \quad (17)$$

F) Load Shedding Limits

Constraints (18) and (19) indicate that load shedding corresponding to active and reactive power, denoted as ΔP_n^d and ΔQ_n^d must be lower or equal than the total active and reactive demand of each bus denoted as P_n^d and Q_n^d, respectively.

$$0 \leq \Delta P_n^d \leq P_n^d; \quad \forall n \in N \quad (18)$$

$$0 \leq \Delta Q_n^d \leq Q_n^d; \quad \forall n \in N \quad (19)$$

III. PROPOSED METHODOLOGY

A GA was implemented for showing the effect of reconfiguration in the electric grid interdiction problem. The flowchart of the implemented GA is depicted in Fig 2.

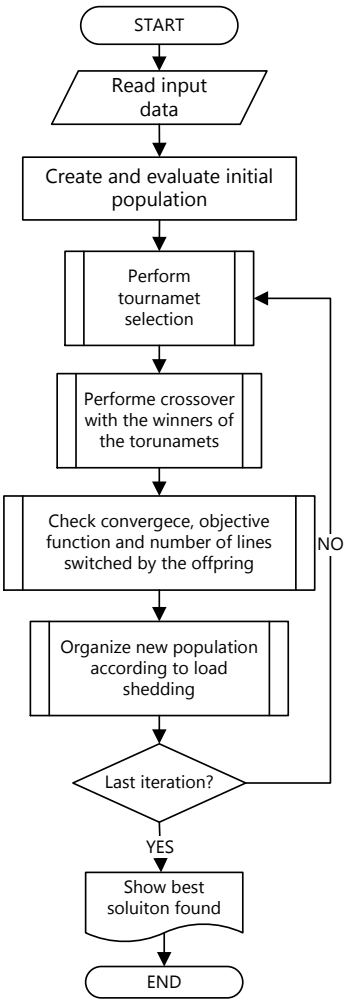

Fig 1. Flowchart of the proposed GA

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 9 (2020), pp. 2313-2317
 https://dx.doi.org/10.37624/IJERT/13.9.2020.2313-2317

Given an attack plan previously devised as indicated in the model given by (1)-(19), the proposed methodology aims at finding the best reconfiguration that would minimize the load shedding. The attack plans were selected from those reported in [13] for the IEEE RTS 24 bus test system.

The GA starts by creating a set of candidate solutions in which the attack plan is included along with possible line switching of the remaining lines. Then the initial population is ordered in terms of load shedding and number of lines switched. It is worth to mention that the lines that are selected in the attack plan are remained open and the GA tries to find a combination of line switching that would minimize the initial load shedding. Once the initial population is created and evaluated, tournament selection is performed. This consists on selecting two subsets of the given population and obtaining the best solution. The two winners of the tournament go to the stage of crossover in which they interchange information of their codification. After that, the GA checks for convergence to discard unfit individuals. The new candidate solutions are organized in the current population according to the number of lines switched and their corresponding load shedding. The process is repeated until a given number of iteration is reached. Finally, the best solution is shown.

IV. TESTS AND RESULTS

Several tests with the IEEE 24 bus test system were initially performed for the correct tuning of the AG parameters. Fig 2 depicts the process of calibration of parameters considering an attack of 4 lines (M=4). Note that from this figure it is possible to identify the best combination of population and generations in terms of minimizing the load shedding after an attack of four lines.

sed GA for M=4

Table 1 presents the results obtained with the GA for different sets of attack plans. Note that for M=2 there is not any improvement by the proposed line switching. The same occurs for M=3 although is not reported in Table 1. This happens because the attack plans in those two cases results in islanding of the power system (see Fig 3a). The best attack plan with M=2 indicated in Fig 3a with a black dot consists on isolating bus 14; while the best attack plan with M=3, indicated with a square in Fig 3a consist on isolating buses 19 and 20. In both cases, there is no way to reduce the load shedding by the switching of adjacent lines. In contrast, two alternatives were found for M=4 as indicated in Fig 3b. In this case, the attack is indicated by the red dashed lines while the reconfiguration actions are indicated in green dashed lines with squares and triangles. A reduction of load shedding of 5.43 MW is obtained in this case. Finally, for M=6 a reduction of 0.7MW in load shedding is obtained. No convergence was obtained with other values of M. This is due to the fact that multiple islands were formed in the process, rendering inadequate the tool used for power flow calculation.

Table 1. Effect of reconfiguration on the load shedding

# of lines under attack	Switched lines	Initial load shedding (MW)	Final load shedding (MW)
2	2-6, 8-10, 9-11, 12-13, 17-22, 18-21, 20-23	194	194
4	1-2, 5-10, 19-20	553.36	547.93
6	1-2, 8-10, 10-11, 15-16, 21-22	1021.2	1020.5

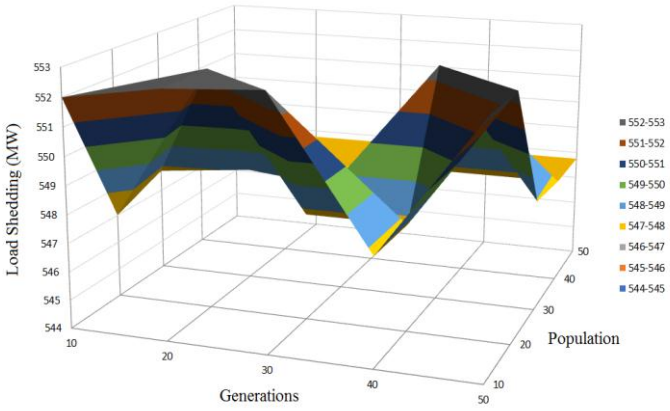

Fig 2. Tuning of the propo

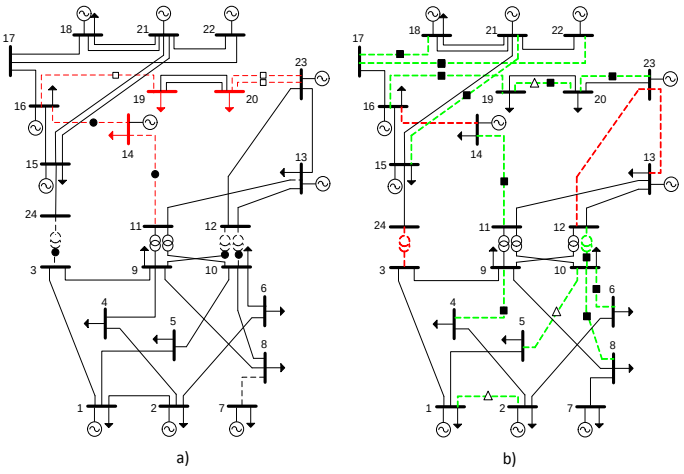

Fig 3. a) Island formations due to attacks with M= 2 and M= 3; b) proposed schemes of line switching found by the GA for M=4

V. CONCLUSIONS

This paper presented an attacker-defender model that considers the interaction of a malicious agent and the system operator. The two-agent interaction is modeled as a bilevel programming problem and solved considering topology changes as part of the defense strategies. A genetic algorithm

was used to solve the proposed model. Several tests performed on the IEEE 24 bus reliability test system showed the applicability and effectiveness of the proposed model and solution approach. Results show that line switching has an important impact on reducing load shedding after an attack. Although a small percentage of load shedding is reduced, the methodology presents encouraging results to search for new ways to approach the interdiction problem.

The information provided by the proposed algorithm regarding critical elements and attacks can be used by the system operator and system planer to device strategies in order to reduce the vulnerability of the power system and improve its relicense. These strategies might include the location of DG in strategic load buses, stricter surveillance of specific transmission assets and reinforcement of certain corridors.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the financial support provided by the Colombia Scientific Program within the framework of the call Ecosistema Científico (Contract No. FP44842- 218-2018). Likewise, Universidad de Antioquia (Colombia) is acknowledged for the financial support through the Sostenibilidad program.

REFERENCES

[1] P. H. Corredor and M. E. Ruiz, "Against All Odds," IEEE Power Energy Mag., vol. 9, no. 2, pp. 59–66, Mar. 2011. DOI: 10.1109/MPE.2011.940266.

[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. DOI: 10.1109/TPWRS.2004.825888.

[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. DOI: 10.1109/TPWRS.2005.846198.

[4] L. Zhao and B. Zeng, "Vulnerability Analysis of Power Grids With Line Switching," IEEE Trans. Power Syst., vol. 28, no. 3, pp. 2727–2736, Aug. 2013. DOI: 10.1109/TPWRS.2013.2256374.

[5] Y. Wang and R. Baldick, "Interdiction Analysis of Electric Grids Combining Cascading Outage and Medium-Term Impacts," IEEE Trans. Power Syst., vol. 29, no. 5, pp. 2160–2168, Sep. 2014. DOI: 10.1109/TPWRS.2014.2300695.

[6] N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment Planning for Electric Power Systems Under Terrorist Threat," IEEE Trans. Power Syst., vol. 27, no. 1, pp. 108–116, Feb. 2012. DOI: 10.1109/TPWRS.2011.2159138.

[7] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," Appl. Energy, vol. 235, pp. 204–218, Feb. 2019. DOI: 10.1016/j.apenergy.2018.10.077.

[8] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems," IEEE Trans. Smart Grid, vol. 7, no. 5, pp. 2260–2272, Sep. 2016. DOI: 10.1109/TSG.2015.2456107.

[9] L. Agudelo, J. M. López-Lezama, and N. M. Galeano, "Vulnerability Assessment of Power Systems to Intentional Attacks using a Specialized Genetic Algorithm," DYNA, vol. 82, no. 192, pp. 78–84, Jul. 2015. DOI: 10.15446/dyna.v82n192.48578.

[10] J. M. López-Lezama, J. Cortina-Gómez, and N. Muñoz-Galeano, "Assessment of the Electric Grid Interdiction Problem using a nonlinear modeling approach," Electr. Power Syst. Res., vol. 144, pp. 243–254, Mar. 2017. DOI: 10.1016/j.epsr.2016.12.017.

[11] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," IEEE Trans. Power Syst., vol. 26, no. 1, pp. 12–19, Feb. 2011. DOI: 10.1109/TPWRS.2010.2051168.

[12] C. Grigg et al., "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., vol. 14, no. 3, pp. 1010–1020, Aug. 1999. DOI: 10.1109/59.780914.

[13] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," Transm. Distrib. IET Gener., vol. 4, no. 2, pp. 178–190, Feb. 2010. DOI: 10.1049/iet-gtd.2009.0098.