A Bilevel Attacker-Defender Model for Enhancing Power Systems Resilience with Distributed Generation

Un modelo Binivel de Ataque-Defensa para Mejorar la Resiliencia de los Sistemas de Potencia con Generación Distribuida

J. P. Hernández-Valencia ; B.J. Restrepo-Cuestas ; J.M. López-Lezama

DOI: https://doi.org/10.22517/23447214.23721
Artículo de investigación científica y tecnológica

Abstract— **Electric transmission and distribution systems are subject not only to natural occurring outages but also to intentional attacks. These lasts performed by malicious agents that aim at maximizing the load shedding of the system. Intentional attacks are counteracted by the reaction of the system operator which deploys strategies to minimize the damage caused by such attacks. This paper presents a bilevel modeling approach for enhancing resilience of power systems with high participation of distributed generation (DG). The model describes the interaction of a disruptive agent that aims at maximizing damage to a power system and the system operator that resorts to different strategies to minimize system damage. The proposed mixed integer nonlinear programming model is solved with a hybrid genetic algorithm. Results are presented on a benchmark power system showing the optimal responses of the system operator for a set of deliberate attacks. It was observed that the higher the participation of DG the lower the impact of the attacks was. The presence of DG also influenced the optimal strategies of the attacker which in some cases deviated from optimal attack plans to suboptimal solutions. This allows concluding that the presence of DG benefits the power system in terms of less expected load shedding under intentional attacks.**

Index Terms— **Bilevel programming, distributed generation, interdiction problem, power systems, resilience.**

Resumen— **Los sistemas de transmisión y distribución están sujetos no solo a fallas naturales sino también a fallas causadas por ataques intencionales. Estos últimos llevados a cabo por agentes maliciosos que tienen como objetivo maximizar el deslastre de carga del sistema. Los ataques intencionales son contrarrestados por la reacción del operador del sistema que lleva a cabo estrategias para minimizar el daño causado por los ataques. Este artículo presenta un modelo de programación binivel para mejorar la resiliencia de los sistemas de potencia con alta participación de generación distribuida (GD). El modelo describe la interacción de un agente disruptivo que pretende maximizar el daño al sistema de potencia y el operador de red que recurre a diferentes estrategias para minimizar el daño. El modelo propuesto es no lineal entero mixto y se soluciona mediante un algoritmo genético híbrido. Se pudo observar que a mayor participación de la GD el impacto de los ataques era menor. La presencia de GD también tuvo influencia en las estrategias del atacante, el cual, en algunos casos, se desviaba de los ataques óptimos a soluciones sub-óptimas. Lo anterior permite concluir que la presencia de GD beneficia al sistema de potencia en términos de menor deslastre de carga esperado ante ataques intencionales.**

Palabras claves—**Programación binivel, generación distribuida, problema de interdicción, sistemas de potencia, resiliencia.**

I. Introduction

MODERN societies are highly dependent on the reliable operation of critical infrastructure. Electric transmission and distribution systems are examples of structures that need to be protected from both natural occurring phenomena and malicious attacks [1]. Due to their meshed topology, power outages due to failures of the transmission system are not as often as those in distribution systems; nevertheless, transmission failures affect a greater number of customers with higher costs involved [2]. The classical approach to power system vulnerability assessment consists on verifying that the system is able to operate within specified limits after the failure of one or two elements. This is the so called N-1 or N-2 security criterion. Although this approach provides a useful insight regarding the vulnerability of a network, it does not consider the fact that power lines are susceptible to deliberate attacks.

The first approach to model deliberate attacks in power systems considering deliberate attacks within a two-agent model was proposed in [3]. In this case, two agents are considered: an attacker and a defender. The former is a malicious agent that aims at maximizing damage to the power system by destroying lines; while the latter is the system operator that must redispatch the available generation to minimize load shedding. This interaction is modeled in a bilevel programming framework. The attacker or disruptive

This manuscript was sent on November 08, 2020 and accepted on November 26, 2020. This work was supported by Universidad de Antioquia and Instituto Tecnológico Metropolitano.

J. P. Hernández-Valencia is with Instituto Tecnológico Metropolitano, Calle 54A N° 30-01, Medellín, Colombia (e-mail: juanhernandez282742@correo.itm.edu.co).

B. J. Restrepo-Cuestas is with the Research Group MATyER, Department of Electronic and Telecommunications, Instituto Tecnológico Metropolitano, Calle 54A N° 30-01, Medellín, Colombia (e-mail: bonierestrepo@itm.edu.co).

J. M. López-Lezama is with the Research Group GIMEL, Department of Electrical Engineering, University of Antioquia, Calle 67 No 53-108, Medellín, Colombia (e-mail: jmaria.lopez@udea.edu.co).

agent is positioned in the upper-level optimization problem, while the system operator is positioned in the lower-level optimization problem. This scheme also corresponds to an action-reaction or leader-follower game.

Since the seminal work reported in [3], several studies have been performed to approach the bilevel attacker-defender problem (also known in the specialized literature as the interdiction problem or terrorist threat problem). In [4] the authors proposed a generalization of the interdiction problem that allows defining differentiated objective functions for the attacker and defender which was not possible within the min-max model proposed in [3]. In this case, the disruptive agent aims at minimizing the number of power system components that must be rendered out of service so that the load shedding is equal to or greater than a specified value. Such goal is contrasted with the assumption that the system operator would deploy strategies to alleviate the impact of the attack. In [5] the attacker-defender problem is solved thorough a generalization of the Benders decomposition method. The model is devised to identify the set of power system circuits that would maximize economic losses to customers if such elements are destroyed. In [6], transmission line switching is introduced as a binary variable in the optimization problem solved by the system operator to account for another strategy to mitigate the impact of deliberate attacks. In [7] the authors introduce 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 planning problem as presented in [8] and [9]. In both papers, the bilevel programming framework is expanded into a tri-level optimization model which considers the agent in charge of the system expansion planning as the one that must find the right set of reinforcements to minimize the damage caused by a disruptive agent, which in turn must anticipate the reaction of the system operator. A similar modeling applied to distribution networks is also presented in [10]. Recent studies have also combined cyber and physical attacks within a similar attacker-defender structure are reported in [11] and [12].

The attacker-defender bilevel programming model that describes the interaction of a malicious agent and the system operator is a challenging nonconvex discrete optimization problem [13]. A way to tackle this problem is turning the original bilevel formulation into an equivalent single-level problem. This can be performed by substituting the lower-level optimization problem by its KKT (Karush Kuhn Tucker) optimality conditions. Also, an equivalent alternative is the use of duality properties as presented in [4]. In both cases, linearization strategies must be performed to turn the original nonlinear bilevel formulation into a single-level linear equivalent. Nevertheless, this strategy is not applicable when the lower-level optimization problem is nonlinear (for example with an AC representation of the network), that is because the KKT conditions are in this case necessary but not sufficient to guarantee optimality. Therefore, when modeling the network with an AC approach the best way to deal with the attacker-defender problem is by means of metaheuristic techniques. Nevertheless, few studies have been conducted in this regard [14], [15].

An attacker-defender model is proposed in this paper to examine the effect of distributed generation (DG) in the resilience of power systems subjected to intentional attacks. The proposed model considers the interaction of two agents with conflicting interests. On the one hand, a disruptive agent, with limited destructive resources, aims at executing an attack plan that would maximize the damage of the system. On the other hand, the system operator aims at protecting the system by redispatching available generation resources. The model includes de effect of DG that can be used as back up generation to mitigate the impact of malicious attacks, and therefore reduce load shedding. For the sake of simplicity only dispatchable DG technologies are considered in the model. Given the fact that bilevel programming problems are nonlinear and nonconvex and that the network is represented by its AC model, a hybrid genetic algorithm (HGA) was implemented for the solution of the model. A number of tests were carried out on the IEEE 24 bus reliability test system and a comparison with other models reported in the specialized literature is provided. It was found that the participation of DG reduces the effect of disruptive attacks resulting in higher benefits for customers and the system operator. The model also provides a list of critical transmission assets that can be used by the system planer to consider reinforcements in strategic elements improving the resilience of the power system.

The rest of the document is organized as follows: the mathematical formulation of the problem is presented in Section II, Section III describes the methodology implemented to solve the proposed model, Section IV describes the tests and results; and finally, Section V presents the main conclusions of the research.

II. Problem Formulation

Fig. 1 depicts the scheme of the attacker-defender problem. Note that for every action of the upper-level agent there is a reaction of the lower-level agent; from the standpoint of game theory, the attacker-defender problem corresponds to a leader-follower game.

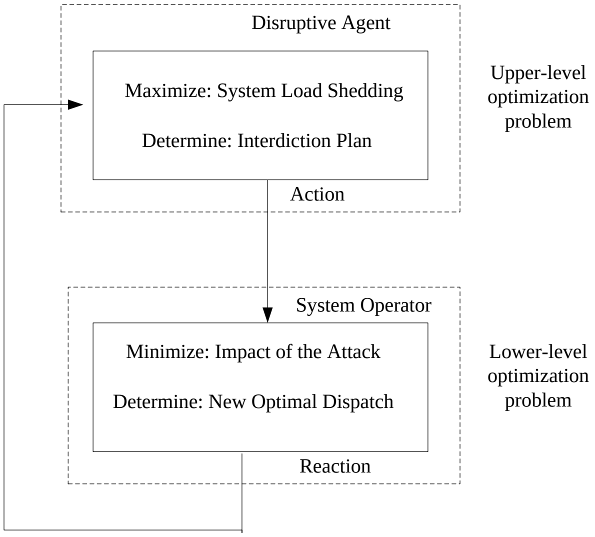

Disruptive Agent
Maximize: System Load Shedding
Determine: Interdiction Plan
Action
Upper-level optimization problem
System Operator
Minimize: Impact of the Attack
Determine: New Optimal Dispatch
Reaction
Lower-level optimization problem

Fig. 1. Bilevel attacker-defender problem.

A. Upper-level Optimization Problem

The purpose of the disruptive agent is to maximize the total load shedding as indicated in (1). In this case, the lower index n indicates the number of the bus; while the upper index d, refers to the demand. This is subject to the limits of destructive resources as given by (2). In this case, *IV* stands for Interdiction Vector, which is a binary array that indicates the states of every transmission asset. Fig. 2 illustrates an example of an interdiction vector in a power system. Note that lines identified as L1, L5, L10 and L12 are under attack and represented by entries equal to zero in the corresponding positions of the IV. The expression given by (3) indicates the nature of the interdiction vector entries while (4) represents the reaction of the system operator.

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

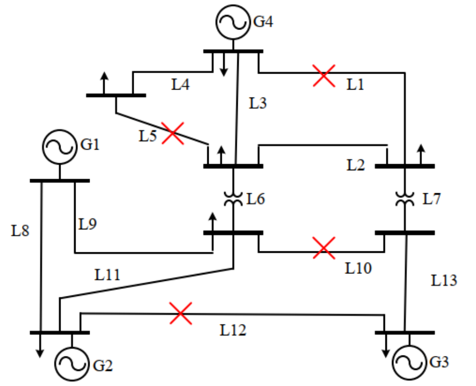
Subject to:

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

$$IV_l \in \{0,1\} \qquad (3)$$

$$Reaction\ of\ the\ System\ Operator \qquad (4)$$

Where:
ΔP_n^d: Active load shedding at bus *n*
IV: Interdiction vector
IV_l: Lth entry of the interdiction vector
N: Set of buses
L: Set of lines
M: Limit of destructive resources



	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13
IV =	0	1	1	1	0	1	1	1	1	0	1	0	1

Fig. 2. Example of an interdiction vector (IV): entries in 0 indicate that the corresponding element is under attack.

B. Lower-Level Optimization Problem

This problem corresponds to the reaction of the system operator. The details of this problem are presented below.

1) Lower-Level Objective Function

In this case, the objective function given by (5) is exactly the opposite of the disruptive agent, which relates to the minimization of the total load shedding.

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

2) Power Balance Equations

Net power injections of active and reactive power must be zero as indicated by (7) and (8). In this case, P_n^G and P_n^{DG} indicate the active power generation provided by centralized and DG, respectively. P_n and P_n^d represent the active power injection and demand at bus *n*, respectively. Note that the same components are considered for reactive power in (8).

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

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

3) Limits on Active and Reactive Power Generation

Constraints given by (8) and (9) indicate limits on active power provided by centralized and DG, respectively. Equations given by (10) and (11) account for reactive power limits of centralized and DG, respectively. In this case upper scripts min and max indicate the type of limit; finally, J indicates the set of centralized generator while K stands for the set of distributed generators.

$$P_j^{G\_min} \leq P_j^G \leq P_j^{G\_max}; \qquad \forall j \in J \qquad (8)$$

$$P_k^{DG\_min} \leq P_k^{DG} \leq P_k^{DG\_max}; \qquad \forall k \in K \qquad (9)$$

$$Q_j^{G\_min} \leq Q_j^G \leq Q_j^{G\_max}; \qquad \forall j \in J \qquad (10)$$

$$Q_k^{DG\_min} \leq Q_k^{DG} \leq Q_k^{GD\_max}; \qquad \forall k \in K \qquad (11)$$

4) *Voltage Limits*

The AC representation of the network considers limits on magnitude and voltage angles as indicated in (12) and (13), respectively. In this case, θ_n and V_n and indicate the angle and magnitude of the voltage at bus n, respectively.

$$V_n^{min} \leq V_n \leq V_n^{max}; \qquad \forall n \in N \qquad (12)$$
$$\theta_n^{min} \leq \theta_n \leq \theta_n^{max}; \qquad \forall n \in N \qquad (13)$$

5) *Power Flow Limits*

Power flow limits must be enforced in normal operation and under any attack. The expressions given by (14) and (15) indicate the active and reactive power flow in each 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

$$P_{lmn}^{f} = (IV_l) * [V_n^2 g_{mn} - V_n V_m g_{mn} \cos(\theta_{mn}) - V_n V_m b_{mn} se\, n(\theta_{mn})];\ \forall l \in L \qquad (14)$$
$$Q_{lmn}^{f} = IV_l) * [-V_n^2 b_{mn} + V_n V_m b_{mn} \cos(\theta_{mn}) - V_n V_m g_{mn} se\, n(\theta_{mn})]; \quad \forall l \in L \qquad (15)$$
$$S_{lmn}^2 = P_{lmn}^2 + Q_{lmn}^2; \qquad \forall l \in L \qquad (16)$$
$$S_{lmn}^{fmin} \leq S_{lmn}^{f} \leq S_{lmn}^{fmax}; \qquad \forall l \in L \qquad (17)$$

6) *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.

$$0 \leq \Delta P_n^d \leq P_n^d; \qquad \forall n \in N \qquad (18)$$
$$0 \leq \Delta Q_n^d \leq Q_n^d; \qquad \forall n \in N \qquad (19)$$

III. Methodology

The model given by equations (1)-(19) is nonlinear and nonconvex; therefore, a metaheuristic was developed to find high quality solutions of such model. This is a common practice to tackle bilevel programming problems, especially when the lower-level optimization problem is nonlinear [15]. In this case, HGA as depicted in Fig. 3 was implemented.

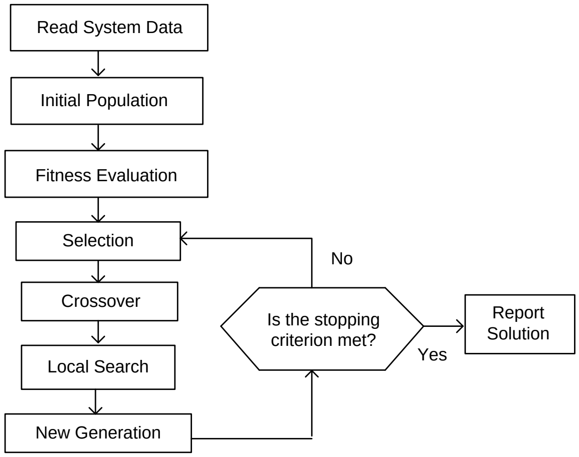


Fig. 3. Flowchart of the proposed HGA.

A. *Problem Codification*

Codification of the HGA is depicted in Fig.2. An alternative representation of the IV is illustrated in Fig.4. The entries of IV correspond to the number of the element under attack. The main advantage of the integer codification over the binary one is that the former avoids unfeasible solutions when performing the crossover stage.

a)

L1	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12	L13
0	1	1	1	0	1	1	1	1	0	1	0	1

b)

L1	L5	L10	L12
1	5	10	12

Fig. 4. Codification of the attacker-defender problem: a) binary and b) integer.

B. *Initial Population*

The initial population is a set of interdiction vectors that are randomly generated bearing in mind the limits on destructive resources of the attacker (M). In this case, it is considered that every line has the same attacking cost (equal to one) so that M indicates the number of lines to be attacked.

C. *Objective Function Evaluation*

Once an initial population is generated, the objective function is evaluated. This stage is the fitness function evaluation indicated in Fig. 3. The fitness function evaluation is performed by running an optimal power flow (OPF) for every IV considering the new states of the lines. The OPFs are computed using Matpower [16]. Fictitious generators are used to account for load shedding, to guarantee the feasibility of the OPF. Every IV of the initial population is evaluated and their corresponding load shedding (objective function) is stored.

D. *Selection by Tournament*

A two-round tournament is performed over the initial formulation for the selection stage. In this case, two subsets with k randomly selected elements are built; then, the best elements (interdiction vectors with the highest load shedding) of each subset are chosen as the parents. An illustration of the selection stage is depicted in Fig. 5.

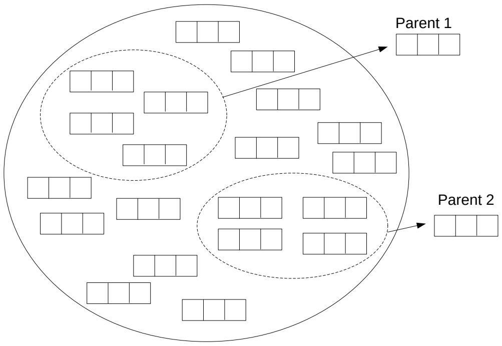


Fig. 5. Illustration of selection by tournament.

E. Crossover

Once the two parents are selected in the previous stage, the crossover is executed. A single point crossover is done for binary representations of the IV, while a crossover by alternating positions is performed for integer representations of IVs as indicated in Fig. 6. Once the crossover is performed the objective function of both offspring is evaluated.

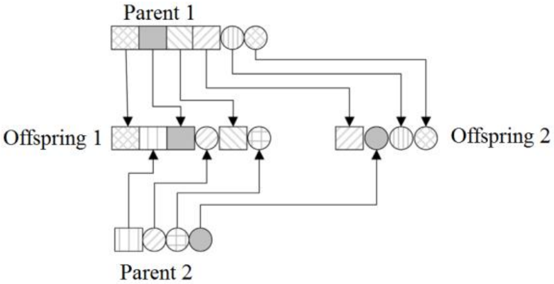


Fig. 6. Crossover by alternating positions.

F. Local Search and New Generation

The best solution is selected out of the two offspring generated in the crossover stage. Over this IV a local search is carried out to identify neighboring solutions with better objective function. The local search is performed by changing the states of the entries of the IV and, after verifying feasibility, computing the new objective function. If a new and better solution is found, this one is introduced in the new generation only if it is better and different than any of the solutions of the current population. The process continues until a given number of generations are evaluated.

IV. Tests and Results

To test the effectiveness of the described model and solution approach, a number of tests were carried out using the IEEE 24 bus reliability test system, which is composed of 38 branches, 11 generators, 17 loads and 24 buses. The interested reader can consult the data of this system in [17]. The tests were carried out for a day of winter season at 6:00 pm, considering a demand of 2850MW. For comparative purposes initial tests were performed without the effect of DG. The HGA was set with 50 initial solutions and 100 generators, and k=5 for tournament selection.

A. Results without DG

The best solutions found for diverse values of M are presented in Table I. A comparison is presented with previous works reported in the specialized literature. In this case, LS stands for load shedding. The results obtained with the proposed methodology (without DG) are in some cases better than those found in [13] and [18]. This is because a nonlinear model of the network has been taken into account. Furthermore, for M=4 a different solution from the one reported in [13] was found. These solutions are indicated in Fig. 7. The square represents the solution reported in [13] while the circle corresponds to the solution found in [18] and in this paper.

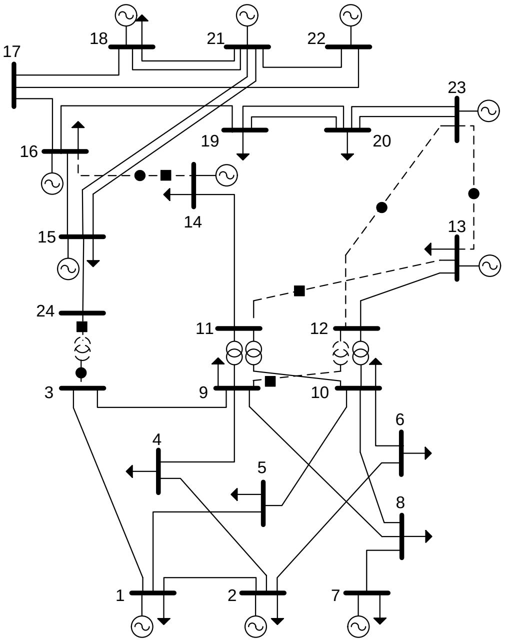


Fig. 6. Different solutions found for M =4 (without DG).

TABLE I
PRELIMINARY TESTS AND COMPARISON OF RESULTS (WITHOUT DG)

M	Destroyed lines	LS reported in [13]	LS reported in [18]	LS this paper
2	11-14, 14-16	194	194	194
3	16-19, 20-23, 20-23	309	-	309
4	3-24, 12-23,13-23, 14-16	442	516	526
5	11-13, 12-13, 12-23, 14-16, 15-24	842	-	842

B. Results with DG: Case 1

There are different generation technologies that can be used as DG. Some of these are based on intermittent resources such as wind and photovoltaic generation. Due to their nature, when an outage takes place it is not guaranteed that such DG units would be available for back-up generation. Therefore, for the sake of simplicity, only dispatchable DG units are considered in the model. Initially, a small participation (from 5 to 10%) of DG was considered uniformly for all load buses. In this case, the destroyed lines reported in Table I remained the same; however, the load shedding was reduced in the same rate as the participation of DG (see Table II). These results make sense since part of the expected load shedding is supplied by the DG units. Nevertheless, results are different when the participation of DG is strategically located in load buses. This is explained in the next subsection.

TABLE II
PRELIMINARY TESTS AND COMPARISON OF RESULTS (WITHOUT DG)

M	Destroyed lines	LS without DG	LS with 5% of DG	LS with 10% of DG
2	11-14, 14-16	194	184.3	174.6
3	16-19, 20-23, 20-23	309	293.5	278.1
4	3-24, 12-23,13-23, 14-16	526	499.7	473
5	11-13, 12-13, 12-23, 14-16, 15-24	842	799.9	757

C. *Results with DG: Case 2*

Table III shows three different attack plans for M=2 considering different participation of DG. The first attack plan is the one already reported in Table I in which no DG is considered. In this case, lines 11-14 and 14-16 are attacked leaving bus 14 isolated from the system. Although there is a generator in bus 14 this one is used as a synchronous capacitor and does not provide active power. Nevertheless, if DG is located in this bus to cover up to 30% of the local demand, then the strategy of the attacker changes and a new attack plan is found. The new optimal solution for the attacker consists on isolating bus 6 by destroying lines 6-10 and 6-2 resulting in a load shedding of 136MW; again, if part of this demand (at least 45%) along with the one already considered in bus 14, the attacker must find another strategy to cause damage. In this case, the new strategy consists on attacking lines 4-9 and 4-2 which results in a much less load shedding of 74MW. The attack plans presented in Table III are illustrated in Fig. 6. Black circles and squares represent attack plans 1 and 2, while the white triangle represents attack plan 3.

TABLE III
DIFFERENT ATTACK PLANS FOR M=2 (WITH DG)

Attack plan	Destroyed lines	Load Shedding	DG participation (% of local load)
1	11-14, 14-16	194	0
2	6-10, 6-2	136	Bus 14 (30%)
3	4-9, 4-2	74	Bus 14 (30%) and Bus 6 (45%)

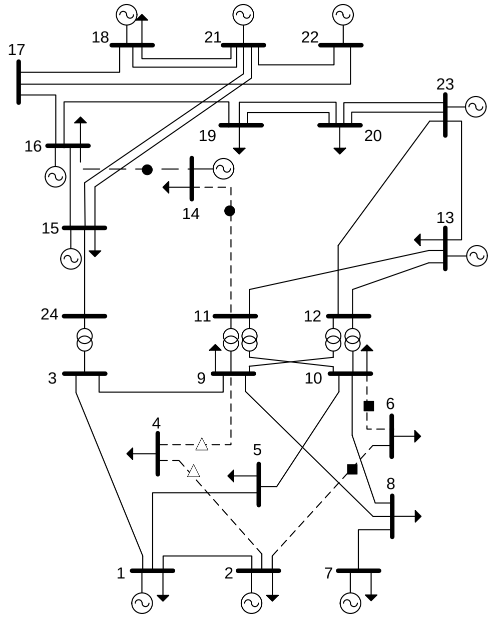


Fig. 6. Different solutions found for M =2 (with DG).

There are also alternative solutions with M=3 when considering DG located in strategic load buses. The default attack plan for M=3 (without DG) consists on destroying lines 16-19, 20-23, 20-23, isolating load buses 19 and 20 (see Fig. 7) and leading to 309MW of load shedding.

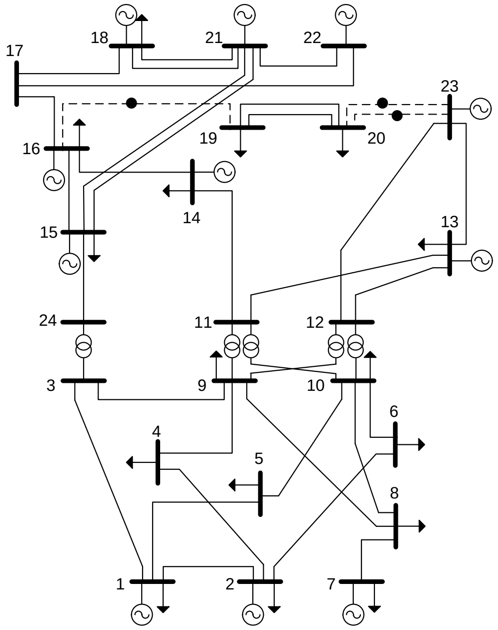


Fig. 7. Attack plan for M =3 (without DG).

The strategic location of DG at buses 19 and 20 leads to a reduction of the expected load shedding. If approximately 37.2% of this demand is locally supplied, then the initial attack plan would change and the new strategy would be to attack lines 16-14 and 14-11 plus any other line (multiple solutions are found with the same load shedding), which results in 194MW of load shedding.

For M=4 and M=5 the strategies of the disruptive agent found by the HGA do not change with the presence of DG (only the amount of load shedding). With this amount of resources, the strategy of the disruptive agent is not performed locally, but instead the attack is systemic, in the sense that it aims at detaching the upper and lower portions of the system, this is because most generation resources are located in the upper section of the system. DG in this case might mitigate the consequences of the attack by reducing the effective load shedding; however, it won't persuade the attacker to look for a different strategy. Fig. 8 illustrates the solution with M=5.

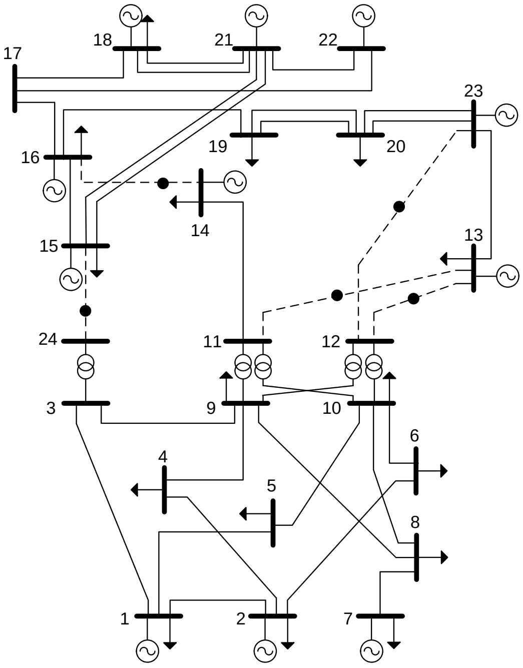


Fig. 8. Attack plan for M =5 (with and without DG).

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 conceived as a bilevel programming problem, which is then solved using a hybrid genetic algorithm that considers local search instead of mutation. The novelty of the proposed approach lies on considering the effect of dispatchable DG. Several tests performed on an IEEE benchmark system showed the applicability and effectiveness of the presented model and solution approach. Results show that DG does not have a significant impact on the strategies of the disruptive agent when this one is scattered in the system with a small percentage. Nevertheless, DG allocated in strategic load buses proved to be effective in both reducing load shedding and moving the strategies of the disruptive agent toward sub-optimal solutions.

The information provided by the proposed algorithm 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, minimizing the load shedding resulting from malicious attacks. These strategies might include the location of DG in strategic load buses as illustrated in the paper, stricter surveillance of specific transmission assets or their reinforcement.

Acknowledgments

The authors acknowledge the Sustainability Project of Universidad de Antioquia and Instituto Tecnológico Metropolitano for their support in the development of this project.

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] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 2, pp. 566–575, Mar. 2015. DOI: 10.1109/TSG.2014.2372315.

[3] 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.

[4] 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.

[5] 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, Feb. 2009. DOI: 10.1109/TPWRS.2008.2004825.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Y. Lin and Z. Bie, "Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding," *Appl. Energy*, vol. 210, pp. 1266–1279, Jan. 2018. DOI: 10.1016/j.apenergy.2017.06.059.

[11] 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.

[12] J. Fu, L. Wang, B. Hu, K. Xie, H. Chao, and P. Zhou, "A Sequential Coordinated Attack Model for Cyber-Physical System Considering Cascading Failure and Load Redistribution," in *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2018, pp. 1–6. DOI:10.1109/ei2.2018.8582135.

[13] 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.

[14] 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.

[15] L. Agudelo, J. M. López-Lezama, and N. Muñoz, "Análisis de Vulnerabilidad de Sistemas de Potencia Mediante Programación Binivel," *Inf. Tecnológica*, vol. 25, no. 3, pp. 103–114, 2014. DOI: 10.4067/S0718-07642014000300013.

[16] 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.

[17] 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.

[18] 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.

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 at University of Antioquia in Medellin, Colombia. His interests include power systems optimization and distributed generation.
ORCID: https://orcid.org/0000-0002-2369-6173

Bonie Johana Restrepo Cuestas received a BSc. in Electrical Engineering in 2005 and a MSc. in Electrical Engineering in 2009, both from Universidad Tecnológica de Pereira in Risaralda, Colombia. From 2005 to 2009, she worked as a teacher at Universidad Tecnológica de Pereira. From 2009 to 2010, also as a project management specialist at Siemens Colombia. Currently, she works at the Faculty of Engineering at Instituto Tecnológico Metropolitano in Medellín and is member of the research group Advanced Materials and Energy. Her research interests include renewable energies and efficient use of energy.
ORCID: https://orcid.org/0000-0001-5276-1651

Juan Pablo Hernández Valencia received a degree in Electrical Engineering from the University Pontificia Bolivariana in Colombia and in the Specialization in Transmission and Distribution Systems of Electric Energy at the University from the Andes in Colombia too. Currently he works at the Faculty of Mechanical, Electronic and Biomedical Engineering at University Antonio Nariño in Medellin, Colombia. His interests include power systems analysis and electric asset management.
ORCID: https://orcid.org/0000-0002-3278-0473