Assessing the Vulnerability of Power Systems Using Multilevel Programming: A Literature Review*

*Juan Pablo Hernández Valencia***
*Jesús María López Lezama****
*Bonie Johana Restrepo Cuestas*****

Received: 9/3/2020 • Accepted: 7/7/2020
https://doi.org/10.22395/rium.v20n38a6

Abstract

Vulnerability studies can identify critical elements in electric power systems in order to take protective measures against possible scenarios that may result in load shedding, which can be caused by natural events or deliberate attacks. This article is a literature review on the latter kind, i.e., the interdiction problem, which assumes there is a disruptive agent whose objective is to maximize the damage to the system, while the network operator acts as a defensive agent. The non-simultaneous interaction of these two agents creates a multilevel optimization problem, and the literature has reported several interdiction models and solution methods to address it. The main contribution of this paper is presenting the considerations that should be taken into account to analyze, model, and solve the interdiction problem, including the most common solution techniques, applied methodologies, and future studies. This literature review found that most research in this area is focused on the analysis of transmission systems considering linear approximations of the network, and a few interdiction studies use an AC model of the network or directly treat distribution networks from a multilevel standpoint. Future challenges in this field include modeling and incorporating new defense options for the network operator, such as distributed generation, demand response, and the topological reconfiguration of the system.

Keywords: interdiction problem; multilevel optimization; power system vulnerability; power system resilience; power system optimization.

* This article is part of *Modelo de Interdicción Mediante Programación Multinivel para Evaluar la Vulnerabilidad de Sistemas de Potencia* (Interdiction Model using Multilevel Programming to Assess the Vulnerability of Power Systems), which is an ongoing research project carried out by Instituto Tecnológico Metropolitano in association with Universidad de Antioquia.

** Electric Power T&D Specialist, MSc Student in Industrial Energy Management, Instituto Tecnológico Metropolitano, Calle 54A N° 30-01, Medellín, Colombia. Orcid: 0000-0002-3278-0473 Email: juanhernadez282742@correo.itm.edu.co

*** Ph.D in Electrical Engineering, Professor of the Electrical Engineering Department, Universidad de Antioquia, Calle 67 N° 53-108, Medellín, Colombia. Orcid: 0000-0002-2369-6173 Email: jmaria.lopez@udea.edu.co.

**** MSc in Electrical Engineer, Electronics and Telecommunications Department Lecturer, Instituto Tecnológico Metropolitano, Calle 54A N° 30-01, Medellín, Colombia. Orcid: 0000-0001-5276-1651 Email: bonierestrepo@itm.edu.co

Evaluación de la vulnerabilidad de sistemas eléctricos por medio de programación multinivel: una revisión bibliográfica

Resumen

Los estudios de vulnerabilidad pueden identificar elementos críticos en los sistemas de distribución de potencia eléctrica con el fin de tomar medidas de protección contra posibles escenarios que pueden resultar en desconexión de carga (también llamado deslastre de carga), que puede ser ocasionada por eventos naturales o ataques deliberados. Este artículo es una reseña bibliográfica sobre el segundo tipo de casos, es decir, los del problema de interdicción, en el que se asume la existencia de un agente disruptivo cuyo objetivo es maximizar los daños ocasionados al sistema mientras el operador de red actúa como agente de defensa del mismo. La interacción no simultánea de estos dos agentes crea un problema de optimización multinivel y en la bibliografía se reportan varios modelos de interdicción y soluciones para abordar el problema. La contribución principal de este artículo es la presentación de consideraciones que deben tomarse en cuenta para analizar, modelar y resolver el problema de la interdicción, incluyendo las soluciones, métodos y técnicas más comunes para solucionarlo, así como futuros estudios al respecto. Esta revisión encontró que la mayoría de la investigación en el tema se enfoca en el análisis de los sistemas de transmisión, considerando las aproximaciones lineales de la red; algunos estudios en interdicción usan un modelo AC de la red o tratan las redes de distribución directamente desde un enfoque multinivel. Algunos retos en este campo son el modelado y la inclusión de nuevas opciones de defensa para el operador de la red, como la generación distribuida, la respuesta a la demanda y la reconfiguración topológica del sistema.

Palabras clave: problema de interdicción; optimización multinivel; vulnerabilidad de sistemas eléctricos; resiliencia de sistemas eléctricos; optimización de sistemas eléctricos.

INTRODUCTION

Electricity transmission and distribution systems are exposed to failures caused not only by nature but also by disruptive agents [1]. The effects of the latter kind of attacks have been historically evaluated using security analysis techniques, among which contingency analysis is a subset [2]. The traditional approach of security studies of power systems is based on N-1 or N-2 criteria and consists of ensuring that the system can continue operating normally, even if one or two elements are out of service [3].

Nevertheless, this approach cannot be applied to the modeling of simultaneous attacks of k elements because, in real systems, the number of combinations to be evaluated would be prohibitive [4]. Furthermore, current reliability policy and security standards for electric power systems around the world are limited to the analysis of a small set of events [5], and traditional reliability indices are not adequate to effectively plan for emerging dangers.

As a result, developing resilience indicators can help network planners to adequately budget the maintenance of the network and investments to improve its functionality in case of low-probability high-consequence risks [6].

In the technical literature, intentional attacks in which the disruptive agent deliberately tries to maximize its damage to the system have been analyzed using multilevel interdiction models. A model is defined here as a set of equations, functions, and mathematical formulas that represent a particular phenomenon, in this case, the interdiction problem. Interdiction models generally implement a simplified representation of transmission networks. Such simplification, known as the DC model, is achieved using linear equations that represent the relationship between power injections and flows in the network. However, a few interdiction multilevel studies have used a more realistic representation of the network, i.e., an AC model. This is because using a DC model of the network facilitates the use of exact methods to solve the interdiction problem, while the AC model limits the solution methods to heuristic or meta-heuristic strategies.

Network operators can adopt different strategies in the face of an attack. The most common of them is redispatch [1], [7], but other possibilities are modifying the topology of the network [8] or exploiting distributed generation (DG) to operate in isolation [9], which is the most widely used in distribution networks.

However, multiple reliability metrics that are generally accepted often exclude important interruptions caused by unexpected events; for instance, the Customer Average Interruption Frequency Index (Caifi) and Customer Average Interruption Duration Index (Caidi). As a consequence, according to the existing reliability metrics, a highly

reliable power system may not necessarily be resilient. The objective of resilience is not only to withstand all possible disaster scenarios but also to have quick and efficient recovery measures [10].

The number of studies regarding the vulnerability of electric power systems has presented an important upward trend in recent years. A bibliometric analysis using the keywords *power system vulnerability* and *power system security* in the databases Science Direct, Scopus, and Web of Science produced the results in figure 1 and figure 2.

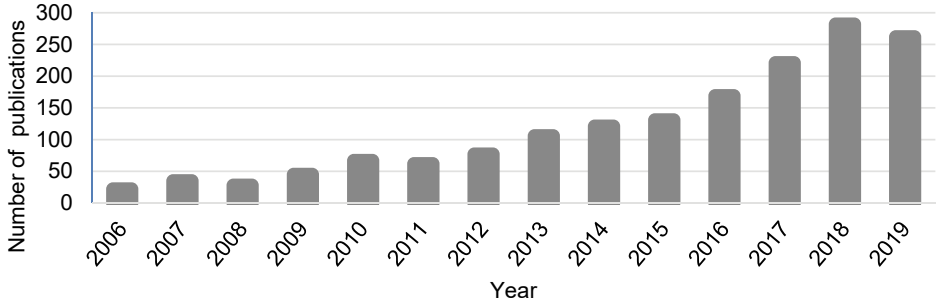

Figure 1. Number of publications that include the term *power system vulnerability* (2006–2019).

Source: own elaboration.

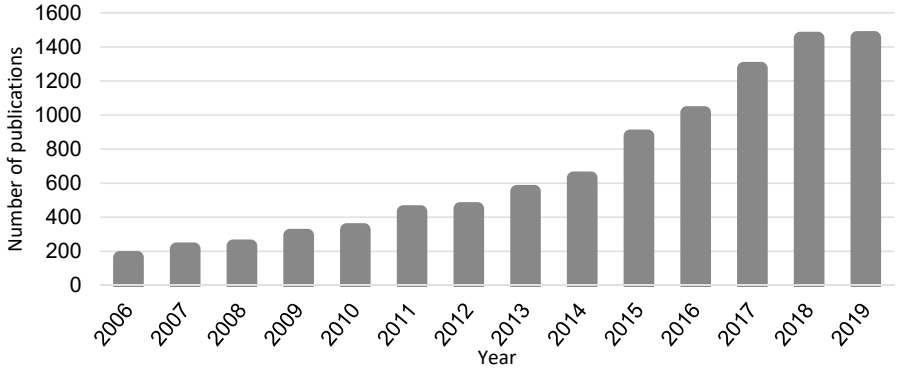

Figure 2. Number of publications that include the term *power system security* (2006–2019).

Source: own elaboration.

Although figure 1 and figure 2 present a similar trend of both keywords, the second case includes a much higher number of publications. For instance, in 2018, the number of vulnerability studies of power systems reached a total of 282 publications, while there were 1,451 security studies. It should be clarified that although there have been many vulnerability and security studies of power systems (as proven by our preliminary search in the databases above), only a small subset of them addresses the topic of

interest in this article. This literature review focuses on vulnerability studies of power systems, more specifically, those that include deliberate attacks and are modeled using multilevel programming.

This article is structured as follows. The first section introduces and defines concepts of vulnerability studies of power systems. The second section classifies these studies paying special attention to multilevel models. The third section describes future challenges, which consist of incorporating new defense options for network operators. Finally, the fourth section presents the conclusions.

1. THE VULNERABILITY PROBLEM

In [11], the authors define vulnerability as the decrease in the performance of an electrical network in the face of a disturbance and present a correlation analysis of different vulnerability metrics. In [12], the authors reviewed the literature on the resilience of power systems in order to face high-probability high-risk events. They associate the vulnerability problem of power systems with a specific triggering event. Therefore, defining the triggering event is the first step in a vulnerability analysis.

Vulnerability studies can be grouped by triggering events: random failures, natural threats, and malicious attacks [13].

Random failures are a series of triggering events that exhibit wide variations and uncertainty [14]. These failures can be modeled by (a) randomly eliminating a given part or number of components of a system; (b) assigning a failure probability to each component and then comparing that probability with a random number between zero and one uniformly distributed to assess the state of the component [15]; or (c) selecting, first, the number of defective components based on a given distribution and, then, randomly eliminating a set of components with the selected number [16].

The second type of vulnerability analysis considers natural threats such as earthquakes, hurricanes, floods, and thunderstorms [17]. These dangers can cause the components of a system distributed over an area of influence to fail simultaneously. The impact of these natural hazards on the components of a system is generally modeled using fragility curves. The latter show the probability of exceeding a certain threshold of damage, which is constrained by a selected danger intensity measurement, such as maximum acceleration of the terrain, maximum soil speed, permanent deformation of the ground for seismic dangers [18] or gust wind speed for hurricane dangers [19].

The third type is the analysis of vulnerability in the face of malicious attacks. In this case, on the one hand, a disruptive agent tries to maximize the damage to the system

by intentionally attacking some of its components [20]. On the other hand, the network operator minimizes the damage by redispatching or making topological changes to the network. Due to its action-reaction nature, the vulnerability to disruptive attacks is analyzed using multilevel optimization models [1].

Figure 3 presents a classification of events in electric power systems. Although the events due to internal failures were the most frequent (47.86 %), those caused by natural disasters, vandalism, and cyber attacks still resulted in 37.85 % of the total power cuts around the world from 1965 to 2012 [10]. This highlights the importance of studies into the vulnerability of electric power systems to intentional attacks.

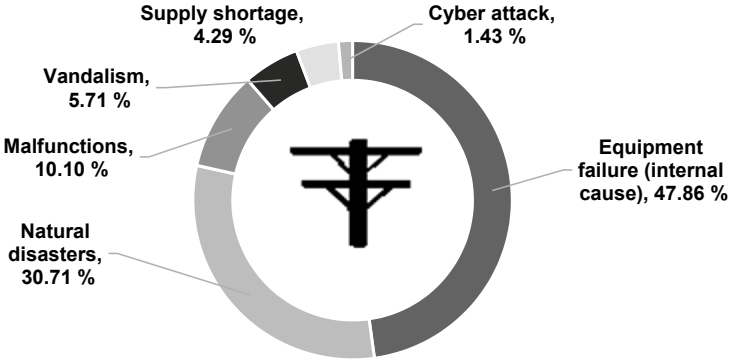

Figure 3. Occurrence of events in electric power systems (1965–2012).

Source: Adapted from [10].

2. CLASSIFICATION OF VULNERABILITY ASSESSMENT APPROACHES

The specialized literature presents different approaches to analyze vulnerability. This section describes the conventional vulnerability analysis models and those that involve multilevel programming.

2.1 Conventional vulnerability models

The conventional models of the vulnerability of electric power systems do not usually consider intentional attacks. Such models are focused on finding a set of critical elements that, if out of service, would cause the biggest problems to the system, whether in terms of load shedding, overloading of other elements, or technical aspects such as voltage stability issues [21]. In order to identify critical lines in a power system, the network can be modeled as a graph with links (transmission lines, transformers, etc.) and nodes (busbars, substations, etc.). This approach was proposed in [3] for a vulnerability analysis using what the authors call an *improved maximum power flow*. Similar studies [2], [22] rank critical lines in a context of safe and economical electricity dispatch.

In addition to power lines and transformers, substations and generators can also be critical elements in electric power systems. In [23] the authors considered substation failures that can occur sequentially and non-synchronously. In particular, they found that this kind of attacks generates many combinations, and these failures may cause large-size blackouts. Additionally, they proposed a metric called the *sequential attack graph* and a strategy based on such metric.

The vulnerability metrics in [24] are useful to implement guidelines to plan, design, invest in, and operate electricity networks. In countries such as China, studies have identified critical attack areas with three types of vulnerabilities, and a comparative analysis was conducted using vulnerability metrics under different tolerance parameters [25]. Likewise, a multidimensional vulnerability analysis was carried out based on given metrics and failure scenarios in order to identify critical areas from the topological and functional standpoints [26].

Another approach [4] combines traditional metrics based on the physical and operating characteristics of the network with two newly proposed metrics: entropic degree and network capacity. This approach can be used to evaluate the structural vulnerabilities of electric power systems.

The tolerance of electric power networks to contingencies has been analyzed in the context of complex network theory [27] by comparing the efficiency of the system with a newly defined parameter such as network capacity. The efficiency and capacity of the network are compared by estimating its vulnerability in terms of both metrics.

The effects of uncertain repair times and recovery resources after the interruption to the critical infrastructure are investigated in [28]. In that case, a restoration framework is applied to the British electric power system, and the results demonstrate the added value of using a stochastic model instead of a deterministic one.

Because electric power systems should reestablish their operation in the face of contingencies, the concept of resilience and their dimensions in distribution networks have also been studied. The methodology proposed in [29] is based on mixed-integer linear programming and an adequate evaluation of the resilience of smart distribution systems. Such model examines the formation of dynamic microgrids, their service areas, and the optimal management of different technologies, such as energy storage systems, demand management programs and distributed generation.

In [30], the authors proposed an improved model to study the reconfiguration of a distribution network based on a refined genetic algorithm. Their objective was to minimize the energy losses of the system.

Another defense strategy based on planning is assigning resources to strengthen the electric power network in order to maximize its immunity against malicious attacks [31], not only by increasing the protection of the power system components but also by building redundant schemes [32].

Other authors have proposed simple critical interdiction strategies for transmission systems [33], [34]. Their method is based on a greedy algorithm in which the transmission line with the highest load is interdicted at each iteration.

The effectiveness of protecting transmission lines identified as promising candidates for interdiction has also been investigated. In [35], two typical models to evaluate the vulnerability of an electric power network were used under intentional attacks: a purely topological model and an interrelation-based model. Afterwards, their results were compared with a DC power flow model.

The inclusion of renewable energy sources on a large scale in distribution networks and its impact on vulnerability was modeled in [36] using a complex network based on a bidirectional flow that considered the change in topology and the power flow pattern in the smart grid.

2.2 Bilevel models

Multilevel models are based on the hypothesis that, on the one hand, there is an aggressor whose objective is to cause maximum damage to the system; and, on the other hand, an agent reacts to the disruptive actions, modifying its operating scheme in order to minimize the damages caused by the attack. This attack-defense relationship can be modeled using a bilevel programming structure (see figure 4.).

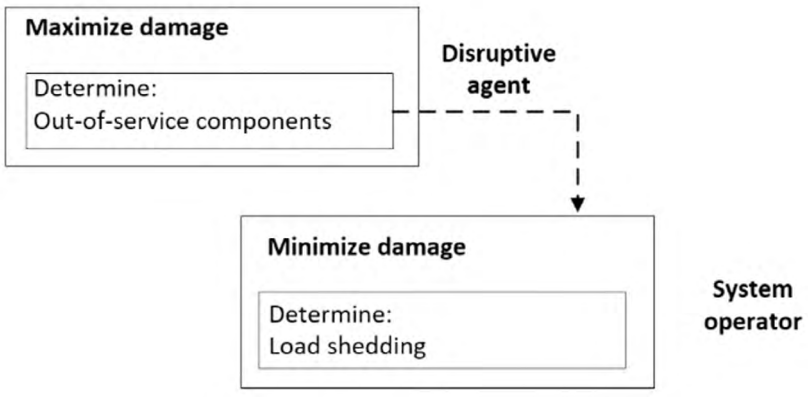

Figure 4. Bilevel model (attack-defense).

Source: Adapted from [37].

In figure 4., the aggressor should determine an attack scheme that maximizes the damage to the network (measured in load shedding). For that purpose, it should consider the fact it has limited resources and anticipate the system operator's response. From the viewpoint of game theory, this dynamic represents a Stackelberg competition [38]. In this type of games, there are a leader and a follower who have conflicting objectives. The leader should determine its game strategy by anticipating the possible reaction of the follower [39]. In addition, the objective function of the leader depends on the decision made by the follower. In the vulnerability problem, the leader is the aggressor and the value of its objective function (load shedding) depends on the network operator's strategy.

The vulnerability problem under a bilevel programming scheme, also known as the *terrorist threat problem*, was first proposed in [7]. Later, the model in [7] was generalized in [1], thus allowing users to define different objective functions for both agents. In [40], the authors proposed minimum and maximum vulnerability models. The former aims to find a minimum number of elements to attack in order to cause a previously defined load shedding, while the latter aims to cause as much shedding as possible with a predetermined number of elements to attack.

Given the non-convexity intrinsic in multilevel programming models, some authors have adopted metaheuristics to address the vulnerability problem. In [41], the authors proposed a genetic algorithm (GA) to solve the interdiction problem considering the topological modification of the system an additional strategy for the network operator to minimize load shedding.

A hybrid GA that involves a local search was used in [42] to address the vulnerability problem in different demand and generation scenarios. In [43], the authors implemented an iterated local search (ILS) to solve the vulnerability problem modeling attacks to lines and generators. In [44], other authors compared different metaheuristics (including GA, ILS, taboo search, and Grasp) applied to the vulnerability problem of electric power systems. Benders decomposition, another numerical tool, has also been employed to deal with interdiction problems, as described in [45].

The vulnerability of power systems can also be analyzed using a specific time horizon. In [46], the authors presented a vulnerability analysis model that can be used to determine where and when (over a given horizon) a power system will be more vulnerable to intentional attacks. In this case, at the upper level of the optimization, the disruptive agent should determine an attack plan that includes the elements to attack and the best time for such attack.

The interdiction model presented in [44] identifies the attacks that have the biggest impact on the power network. The contribution of this model lies in the fact that it incorporates the impacts of the possible attack in the short term (seconds to minutes) and the long term (minutes to days). The medium-term impacts are examined using a DC optimal power flow (DCOPF) model. The short-term impacts are addressed by means of an interruption cascade analysis model that uses a set of verifiers sequentially applied.

A common characteristic among most vulnerability studies is the representation of the transmission network using a DC model. This simplifies the modeling of the problem and, as a result, a bilevel model can be transformed into a single-level equivalent. However, DC models do not consider the effect of reactive power and network voltage limits.

In turn, the interdiction model in [43] and [47] uses an AC model of the transmission network. Such model can produce more realistic results because it considers voltage limits, the contribution of the reactive power, and the losses at the transmission network elements. Another vulnerability model [48] implemented an AC model of the network and quantified the impact of the attacks to said network in different ways, including the deviation of the voltages at the busbars and the minimum load that should be eliminated in order to restore the network to a stable operation.

The integration of information technologies into power systems makes the latter vulnerable to cyber attacks. This type of attacks can even affect the service provision or the information of the control and protection systems by injecting fake data [49]. Possible scenarios of coordinated attacks can be found in the specialized literature. The power grid is becoming more vulnerable to various kinds of cyber and physical attacks. Coordination between the attacks could bring higher impacts on the power system, as evidenced by the 2015 Ukrainian power system cyberattack. There is limited study in existing literature about possible coordinated attack scenarios and the detailed mathematical modeling of them. To prevent future coordinated attacks against power systems, in this paper the cyber-physical security of the power system is analyzed and probable coordinated attack scenarios are proposed. In [50], the authors studied in detail two typical examples of attack coordination: (1) between the load redistribution (LR) attack and the attackers; and (2) between the LR attack and the attacked lines. Operators could be misled to develop an uninformed energy dispatch strategy and, as a result, load reduction could be maximized.

2.3 Trilevel models

Trilevel vulnerability models contain the attack-defense bilevel scheme mentioned above and involve a third agent at the upper level of the optimization. The new agent is the network planner, who should make decisions about the construction of new reinforcements in order to minimize the impacts of eventual attacks. The attacker and system operator are on the second and third level, respectively. Figure 5. presents a scheme of the interaction between these agents. In this case, the system planner receives information about the lower-level problems based on which it makes decisions regarding network reinforcements.

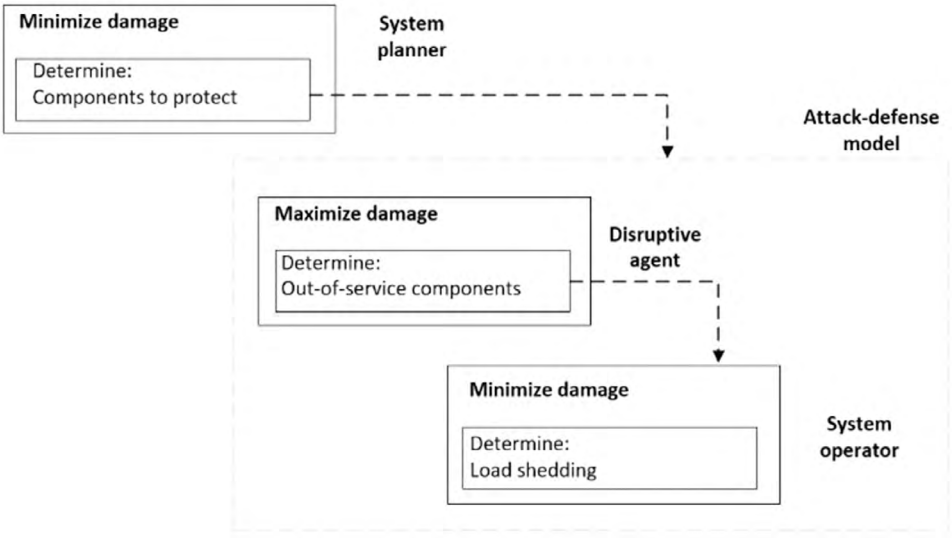

Figure 5. Trilevel vulnerability model.

Source: Adapted from [37].

In other studies [6], [9], trilevel vulnerability models have been applied to distribution systems. In [6], the objective function was formulated as the load shedding cost, in addition to the operation cost of the generator. Furthermore, the trilevel problem can be broken down into two stages: master and slave problem. Dual transformation has been proposed [51], [52] the authors numerically validate and analyse the tri-level transmission expansion planning (TTEP) to turn the trilevel model into a single-level one, which ensures a global optimum. In [53], the objective function was the load shedding cost, and the authors proposed the conversion to a bilevel problem using the duality principle. Finally, they utilized Benders decomposition to solve the problem.

In [54], the model was focused on protecting the network against cyber-physical attacks from the viewpoint of the allotment of defense resources. A coordinated

attack means a physical short circuit of the transmission lines after hijacking the communication network of the safety relays. A systematic review of interaction models and solution methods in studies of the interaction between cyber-networks and power systems was presented in [49]. In turn, unidentifiable attacks produced by cyber attacks (wrong readings of meters) were considered in the reliability evaluation of power systems in [55]. More cyber technologies are being deployed in the modern cyberphysical power systems. However, as a result higher cyberattack risks will be brought about. Unidentifiable attacks, which are a type of emerging false data injection attacks, could affect the outcomes of State Estimation (SE).

In [56], a trilevel vulnerability model was implemented using an algorithm that generates columns and restrictions. The results showed that the protection using the optimal solution of the defender-attacker-defender model always enabled the network to survive in case of contingencies. Some defense strategies studied in the literature include the formation of DG islands and the reconfiguration of the network [9]. The model in [57] introduced multiple sets of uncertainty to characterize possible interruptions caused by attackers, and the probabilities of the multiple sets of uncertainty were estimated by means of an analytic hierarchy process.

Another perspective on vulnerability evaluation [13] aims to mitigate the vulnerability of the power system to the worst attacks located in space. These attacks are defined as the failure of a group of system components distributed over an area due to natural dangers or malicious attacks, while other components outside that area do not fail directly.

Regarding the allotment of resources for the defense or reinforcement of an electric power network, other authors [37] have proposed a two-stage solution approach that achieves optimization with a moderate computational effort. The original trilevel program is transformed, first, into an equivalent bilevel program, which is later solved using an implicit enumeration algorithm.

Table 1 presents a classification of the literature reviewed in this paper specifying the type of network model, solution method and defense strategies modeled for the network operator.

Table 1. Multilevel programming studies applied to the vulnerability problem of electric power systems.

Ref.	Multilevel prob.		Type of system		Model		Solution method		Defense strategies
	Bilevel	Trilevel	Dist.	Transm.	AC	DC	Exact	Heuristic	
[1]	X			X		X	X		Redispatch
[5]	X			X		X		X	Redispatch
[6]		X		X		X	X		Planning
[7]	X			X		X		X	Planning
[8]	X			X		X	X		Redispatch
[9]		X	X		X		X		Reconfiguration/Islanding
[37]		X		X		X			Planning
[40]	X			X		X	X		Redispatch
[41]	X			X		X		X	Reconfiguration
[42]	X			X		X		X	Planning
[43]	X			X	X			X	Redispatch
[44]	X			X		X		X	Redispatch
[45]	X			X		X	X		Planning
[47]	X			X	X			X	Planning
[48]	X			X	X			X	Reconfiguration
[51]		X		X		X		X	Planning
[52]		X		X		X		X	Planning
[53]		X		X		X	X		Planning
[54]		X		X		X	X		Planning
[57]		X		X		X	X		Reconfiguration
[58]	X			X		X	X		Planning

Source: own elaboration.

2.4 Future research

Future studies to solve the interdiction problem are connected to multiple fields. They include new formulations of mixed-integer linear programming models that represent the interdiction problem and integrate primary control actions in a single level, as proposed in [1], or incorporate uncertainty into terrorist objectives [7]. Other proposals introduce alternative solution techniques based on heuristics [8], [41].

Nevertheless, multilevel models need greater detail in the modeling of power systems, which involves more complex solution methods that could be considered in future work; for instance, the use of genetic operators in the metaheuristic applications [5]; stochastic programming to model the load, generation, and topology of the network [6]; and linear approximations of the min-max model, as proposed in [7]. Other studies seek to optimize computational calculation times [5], [9]. Finally, some defense strategies are the connection or disconnection of fast-acting generating units [8], [41], the mitigation of consequences of attacks (cascading outages, temporary stability, etc.) [7], and network reinforcement based on planning and considering stochasticity and distributed generation [9].

3. CONCLUSIONS

This paper presented a review of the literature on the vulnerability problem in power systems. Such review was mainly focused on the description of bi- and trilevel programming models. Bilevel models represent attack-defense dynamics between a disruptive agent and the network operator, while their trilevel counterparts involve the network planner and represent defense-attack-defense dynamics.

The studies we retrieved were classified based on their solution method, network model, and type of system. This review found that most vulnerability or interdiction studies were focused on the analysis of transmission systems. That is because attacks to distribution systems have less serious consequences regarding the load level and number of affected users. Most authors adopted a simplified network model, i.e., a DC model, to represent the transmission network, which enabled them to solve the problem using exact techniques based on mixed-integer linear programming. In addition, the studies that implemented an AC model of the network adopted heuristic methods to solve the vulnerability problem. The defense strategies in bilevel problems were redispatch or network reconfiguration. In turn, trilevel models considered network reinforcements to be the core defense strategy against eventual attacks.

This literature review also revealed future research lines to analyze the vulnerability of power systems. They include new mathematical formulations to achieve more accurate representations of the network; the introduction of uncertainty to model the system load and generation; new (heuristic and exact) solution techniques and novel defense strategies for network operators and planners that incorporate the effects of demand response, distributed generation and energy storage programs.

REFERENCES

[1] 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, pp. 789–797, 2005. DOI: 10.1109/TPWRS.2005.846198

[2] C.M. Rocco, J.E. Ramirez-Marquez, D.E. Salazar, and C. Yajure, "Assessing the Vulnerability of a Power System Through a Multiple Objective Contingency Screening Approach," *IEEE Trans.Reliab.*, vol. 60, pp. 394–403, 2011. DOI: 10.1109/TR.2011.2135490

[3] J. Fang, C. Su, Z. Chen, H. Sun, and P. Lund, "Power System Structural Vulnerability Assessment Based on an Improved Maximum Flow Approach," *IEEE Trans.Smart Grid*, vol. 9, pp. 777–785, 2018. DOI: 10.1109/TSG.2016.2565619

[4] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *Int.J. Crit. Infrastruct. Prot.*, vol. 2, pp. 5–12, 2009. DOI: 10.1016/j.ijcip.2009.02.002.

[5] J.M. Arroyo, and F.J. Fernández, "A Genetic Algorithm for Power System Vulnerability Analysis under Multiple Contingencies," in: *Springer, Berlin, Heidelberg*, 2013, 41–68 p. DOI: 10.1007/978-3-642-37838-6_2

[6] H. Davarikia, and M. Barati, "A tri-level programming model for attack-resilient control of power grids," *J. Mod.Power Syst. Clean Energy*, vol. 6, pp. 918–929, 2018. DOI: 10.1007/s40565-018-0436-y

[7] J. Salmeron, K. Wood, and R. Baldick, "Analysis of Electric Grid Security Under Terrorist Threat," *IEEE Trans.Power Syst.*, vol. 19, pp. 905–912, 2004. DOI: 10.1109/TPWRS.2004.825888

[8] A. Delgadillo, J.M. Arroyo, and N. Alguacil, "Analysis of Electric Grid Interdiction With Line Switching," *IEEE Trans.Power Syst.*, vol. 25, pp. 633–641, 2010. DOI: 10.1109/TPWRS.2009.2032232

[9] 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, 2018. DOI: 10.1016/j.apenergy.2017.06.059

[10] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the Extreme: A Study on the Power System Resilience," *Proc. IEEE*, vol. 105, pp. 1253–1266, 2017. DOI: 10.1109/JPROC.2017.2679040

[11] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Phys.A Stat. Mech. Its Appl.*, vol. 396, pp. 204–211, 2014. DOI: 10.1016/J.PHYSA.2013.10.041

[12] Y. Lin, Z. Bie, and A. Qiu, "A review of key strategies in realizing power system resilience," *Glob.Energy Interconnect.*, vol. 1, pp. 70–78, 2018. DOI: 10.14171/j.2096-5117.gei.2018.01.009

[13] M. Ouyang, M. Xu, C. Zhang, and S. Huang, "Mitigating electric power system vulnerability to worst-case spatially localized attacks," *Reliab.Eng. Syst. Saf.*, vol. 165, pp. 144–154, 2017. DOI: 10.1016/J.RESS.2017.03.031

[14] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power system," *Reliab.Eng. Syst. Saf.*, vol. 183, pp. 153–172, 2019. DOI: 10.1016/j.ress.2018.11.019

[15] M. Ouyang, and L. Dueñas-Osorio, "Time-dependent resilience assessment and improvement of urban infrastructure systems," *Chaos*, vol. 22, pp. 033122, 2012. DOI: 10.1063/1.4737204

[16] M. Ouyang, L. Dueñas-Osorio, and X. Min, "A three-stage resilience analysis framework for urban infrastructure systems," *Struct.Saf.*, vol. 36–37, pp. 23–31, 2012. DOI: 10.1016/j.strusafe.2011.12.004

[17] A. Gholami, T. Shekari, M.H. Amirioun, F. Aminifar, M.H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018. DOI: 10.1109/ACCESS.2018.2845378

[18] K. Poljanšek, F. Bono, and E. Gutiérrez, "Seismic risk assessment of interdependent critical infrastructure systems: The case of European gas and electricity networks," *Earthq. Eng. Struct. Dyn.*, vol. 41, pp. 61–79, 2012. DOI: 10.1002/eqe.1118

[19] M. Ouyang, and L. Dueñas-Osorio, "Multi-dimensional hurricane resilience assessment of electric power systems," *Struct.Saf.*, vol. 48, pp. 15–24, 2014. DOI: 10.1016/j.strusafe.2014.01.001

[20] I.B. Sperstad, G.H. Kjølle, and O. Gjerde, "A comprehensive framework for vulnerability analysis of extraordinary events in power systems," *Reliab.Eng. Syst. Saf.*, vol. 196, pp. 106788, 2020. DOI: 10.1016/j.ress.2019.106788

[21] A. Wang, Y. Luo, G. Tu, and P. Liu, "Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory," *IEEE Trans.Power Syst.*, vol. 26, pp. 442–450, 2011. DOI: 10.1109/TPWRS.2010.2052291

[22] C.C. Marín-Cano, J.E. Sierra-Aguilar, J.M. López-Lezama, Á. Jaramillo-Duque, and W.M. Villa-Acevedo, "Implementation of User Cuts and Linear Sensitivity Factors to Improve the Computational Performance of the Security-Constrained Unit Commitment Problem," *Energies*, vol. 12, pp. 1399, 2019. DOI: 10.3390/en12071399

[23] Y. Zhu, J. Yan, Y. Tang, Y.L. Sun, and H. He, "Resilience Analysis of Power Grids Under the Sequential Attack," *IEEE Trans.Inf. Forensics Secur.*, vol. 9, pp. 2340–2354, 2014. DOI: 10.1109/TIFS.2014.2363786

[24] P.E. Roege, Z.A. Collier, J. Mancillas, J.A. McDonagh, and I. Linkov, "Metrics for energy resilience," *Energy Policy*, vol. 72, pp. 249–256, 2014. DOI: 10.1016/J.ENPOL.2014.04.012

[25] S. Wang, J. Zhang, M. Zhao, and X. Min, "Vulnerability analysis and critical areas identification of the power systems under terrorist attacks," *Phys.A Stat. Mech. Its Appl.*, vol. 473, pp. 156–165, 2017. DOI: 10.1016/j.physa.2017.01.003

[26] S. Wang, J. Zhang, and N. Duan, "Multiple perspective vulnerability analysis of the power network," *Phys.A Stat. Mech. Its Appl.*, vol. 492, pp. 1581–1590, 2018. DOI: 10.1016/J.PHYSA.2017.11.083

[27] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos An Interdiscip. J. Nonlinear Sci.*, vol. 19, pp. 013119, 2009. DOI: 10.1063/1.3077229

[28] Y.-P. Fang, and G. Sansavini, "Optimum post-disruption restoration under uncertainty for enhancing critical infrastructure resilience," *Reliab.Eng. Syst. Saf.*, vol. 185, pp. 1–11, 2019. DOI: 10.1016/j.ress.2018.12.002

[29] S. Mousavizadeh, M.-R. Haghifam, and M.-H. Shariatkhah, "A linear two-stage method for resiliency analysis in distribution systems considering renewable energy and demand response resources," *Appl.Energy*, vol. 211, pp. 443–460, 2018. DOI: 10.1016/J.APENERGY.2017.11.067

[30] J.Z. Zhu, "Optimal reconfiguration of electrical distribution network using the refined genetic algorithm," *Electr.Power Syst. Res.*, vol. 62, pp. 37–42, 2002. DOI: 10.1016/S0378-7796(02)00041-X

[31] A. Costa, D. Georgiadis, T.S. Ng, and M. Sim, "An optimization model for power grid fortification to maximize attack immunity," *Int.J. Electr. Power Energy Syst.*, vol. 99, pp. 594–602, 2018. DOI: 10.1016/j.ijepes.2018.01.020

[32] H. Mo, M. Xie, and G. Levitin, "Optimal resource distribution between protection and redundancy considering the time and uncertainties of attacks," *Eur.J. Oper. Res.*, vol. 243, pp. 200–210, 2015. DOI: 10.1016/J.EJOR.2014.12.006

[33] T. Kim, S.J. Wright, D. Bienstock, and S. Harnett, "Vulnerability Analysis of Power Systems," *ArXiv Prepr.*, 2015. Disponible: http://arxiv.org/abs/1503.02360

[34] V.M. Bier, E.R. Gratz, N.J. Haphuriwat, W. Magua, and K.R. Wierzbicki, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliab. Eng. Syst. Saf.*, vol. 92, pp. 1155–1161, 2007. DOI: 10.1016/J.RESS.2006.08.007

[35] M. Ouyang, L. Zhao, Z. Pan, and L. Hong, "Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks," *Phys.A Stat. Mech. Its Appl.*, vol. 403, pp. 45–53, 2014. DOI: 10.1016/J.PHYSA.2014.01.070

[36] A.B.M. Nasiruzzaman, H.R. Pota, and M.N. Akter, "Vulnerability of the large-scale future smart electric power grid," *Phys.A Stat. Mech. Its Appl.*, vol. 413, pp. 11–24, 2014. DOI: 10.1016/J.PHYSA.2014.06.024

[37] N. Alguacil, A. Delgadillo, and J.M. Arroyo, "A trilevel programming approach for electric grid defense planning," *Comput.Oper. Res.*, vol. 41, pp. 282–290, 2014. DOI: 10.1016/j.cor.2013.06.009

[38] T. Lu, Z. Wang, J. Wang, Q. Ai, and C. Wang, "A Data-Driven Stackelberg Market Strategy for Demand Response-Enabled Distribution Systems," *IEEE Trans.Smart Grid*, vol. 10, pp. 2345–2357, 2019. DOI: 10.1109/TSG.2018.2795007

[39] J. Zhang, and J. Zhuang, "Modeling a multi-target attacker-defender game with multiple attack types," *Reliab.Eng. Syst. Saf.*, vol. 185, pp. 465–475, 2019. DOI: 10.1016/j.ress.2019.01.015

[40] J.M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Gener.Transm. Distrib.*, vol. 4, pp. 178, 2010. DOI: 10.1049/iet-gtd.2009.0098

[41] J.M. Arroyo, and F.J. Fernandez, *A Genetic Algorithm Approach for the Analysis of Electric Grid Interdiction with Line Switching.* in: 2009 15th Int. Conf. Intell. Syst. Appl. to Power Syst. *IEEE*, 2009, 1–6 p. DOI: 10.1109/ISAP.2009.5352849

[42] L. Agudelo, J.M. López-Lezama, and N. Muñoz Galeano, "Vulnerability Assessment of Power Systems to Intentional Attacks using a Specialized Genetic Algorithm," *DYNA*, vol. 82, pp. 78–84, 2015. DOI: 10.15446/dyna.v82n192.48578

[43] 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, 2017. DOI: 10.1016/j.epsr.2016.12.017

[44] J.J. Cortina, J.M. López-Lezama, and N. Muñoz-Galeano, "Metaheurísticas Aplicadas al Problema de Interdicción en Sistemas de Potencia," *Inf.Tecnológica*, vol. 29, pp. 73–88, 2018. DOI: 10.4067/s0718-07642018000200073

[45] J. Salmeron, K. Wood, and R. Baldick, "Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids," *IEEE Trans.Power Syst.*, vol. 24, pp. 96–104, 2009. DOI: 10.1109/TPWRS.2008.2004825

[46] S. Sayyadipour, G.R. Yousefi, and M.A. Latify, "Mid-term vulnerability analysis of power systems under intentional attacks," *IET Gener.Transm. Distrib.*, vol. 10, pp. 3745–3755, 2016. DOI: 10.1049/iet-gtd.2016.0052

[47] L. Agudelo, J.M. López-lezama, and N. Muñoz, "Análisis de Vulnerabilidad de Sistemas de Potencia Mediante Programación Binivel Vulnerability Analysis of Power Systems using Bilevel Programing," *Inf.Tecnol.*, vol. 25, pp. 103–114, 2014. DOI: 10.4067/S0718-07642014000300013

[48] T. Kim, S.J. Wright, D. Bienstock, and S. Harnett, "Analyzing Vulnerability of Power Systems with Continuous Optimization Formulations," *IEEE Trans.Netw. Sci. Eng.*, vol. 3, pp. 132–146, 2016. DOI: 10.1109/TNSE.2016.2587484

[49] L. Shi, Q. Dai, and Y. Ni, "Cyber–physical interactions in power systems: A review of models, methods, and applications," *Electr. Power Syst. Res.*, vol. 163, pp. 396–412, 2018. DOI: 10.1016/j.epsr.2018.07.015

[50] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electr.Power Syst. Res*., vol. 149, pp. 156–168, 2017. DOI: 10.1016/j.epsr.2017.04.023

[51] H. Nemati, M.A. Latify, and G.R. Yousefi, "Tri-level transmission expansion planning under intentional attacks: virtual attacker approach – part I: formulation," *IET Gener.Transm. Distrib.*, vol. 13, pp. 390–398, 2019. DOI: 10.1049/iet-gtd.2018.6104

[52] H. Nemati, M.A. Latify, and G.R. Yousefi, "Tri-level transmission Expansion planning under intentional attacks: virtual attacker approach-part II: Case studies," *IET Gener. Transm. Distrib.*, vol. 13, pp. 399–408, 2019. DOI: 10.1049/iet-gtd.2018.6105

[53] X. Wu, and A.J. Conejo, "An Efficient Tri-Level Optimization Model for Electric Grid Defense Planning," *IEEE Trans.Power Syst.*, vol. 32, pp. 2984–2994, 2017. DOI: 10.1109/TPWRS.2016.2628887

[54] 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, 2019. DOI: 10.1016/J.APENERGY.2018.10.077

[55] Z. Ding, Y. Xiang, and L. Wang, *Incorporating Unidentifiable Cyberattacks into Power System Reliability Assessment*.in: IEEE Power Energy Soc. Gen. Meet. *IEEE*, 2018, 1–5 p. DOI: 10.1109/PESGM.2018.8585884

[56] W. Yuan, L. Zhao, and B. Zeng, "Optimal power grid protection through a defender–attacker–defender model," *Reliab.Eng. Syst. Saf.*, vol. 121, pp. 83–89, 2014. DOI: 10.1016/J.RESS.2013.08.003

[57] T. Ding, L. Yao, and F. Li, "A multi-uncertainty-set based two-stage robust optimization to defender–attacker–defender model for power system protection," *Reliab.Eng. Syst. Saf.*, vol. 169, pp. 179–186, 2018. DOI: 10.1016/j.ress.2017.08.020

[58] Y. Wang, and R. Baldick, "Interdiction Analysis of Electric Grids Combining Cascading Outage and Medium-Term Impacts," *IEEE Trans.Power Syst.*, vol. 29, pp. 2160–2168, 2014. DOI: 10.1109/TPWRS.2014.2300695