NUEVAS REALIDADES PARA LA EDUCACIÓN EN INGENIERÍA: CURRÍCULO, TECNOLOGÍA, MEDIO AMBIENTE Y DESARROLLO
13 - 16 DE SEPTIEMBRE 2022 CARTAGENA DE INDIAS, COLOMBIA
Encuentro Internacional de Educación en Ingeniería ACOFI

Analysis of vulnerability and resilience in electrical distribution systems in the event of a deliberate disruptive event

Darin J. Mosquera Palacios, Edwin Rivas Trujillo

Universidad Distrital Francisco José de Caldas
Bogotá, Colombia

Luis Alejandro Arias Barragán

Universidad ECCI
Bogotá, Colombia

Resumen

Este trabajo propone maximizar la resiliencia del sistema eléctrico ante ataques intencionales a través de la implementación de recursos energéticos distribuidos (DER) generación distribuida (GD) y respuesta a la demanda (RD). Se aborda en primera instancia el caso en el que un agente disruptor, tiene como objetivo maximizar el daño a la red (expresado a través del costo total de operación), mientras que el OS toma las medidas necesarias para mitigar los efectos de este ataque. La interacción entre estos dos agentes se modela mediante un problema de optimización de dos niveles. Por un lado, el agente disruptivo se posiciona en el problema de optimización de nivel superior y debe decidir qué elementos dejar fuera de servicio (líneas y generadores) dado un presupuesto limitado. Por otro lado, el OS, ubicado en un problema de optimización de nivel inferior, reacciona al ataque implementando medidas de mitigación para minimizar los sobrecostos en la operación del sistema. Se proponen tres métricas para evaluar la resiliencia mediante la asignación de DER en islas generadas por la destrucción de líneas y generadores., para ello se toman dos casos de estudio, un sistema de prueba de 5 buses y el sistema de prueba IEEE RTS-24 buses.

Palabras clave: agente disruptor; algoritmo genético; análisis de vulnerabilidad; Deslastre de carga; generación distribuida; gestión de recursos energéticos distribuidos; métricas; resiliencia; respuesta a la demanda

Abstract

This work proposes to maximize the resilience of the electricity system to intentional attacks through the implementation of distributed energy resources (DER), distributed generation (GD) and demand response (DR). It addresses in the first instance the case in which a disruptor agent aims to maximize the damage to the network (expressed through the total cost of operation), while the system operator takes the necessary measures to mitigate the effects of this attack. The interaction between these two agents is modeled using a two-level optimization problem. On the one hand, the disruptive agent is positioned in the problem of top-level optimization and must decide which elements to leave out of service (lines and generators) given a limited budget. On the other hand, the system operator, located in a lower-level optimization problem, reacts to the attack by implementing mitigation measures to minimize cost overruns in system operation. Three metrics are proposed to evaluate resilience by assigning DER on islands generated by the destruction of lines and generators, for these two case studies are taken, a 5-bus test system and the IEEE RTS-24 buses test system.

Keywords*: disruptor agent; genetic algorithm; vulnerability analysis; Load shedding; distributed generation; management of distributed energy resources; metrics; resilience; demand response*

1. Introducción

La infraestructura eléctrica en la sociedad moderna juega un papel primordial ya que su uso y funcionamiento de forma adecuada facilita la productividad en la industria y un bienestar a los usuarios. Los Operadores de Red de Distribución (ORD) y los planificadores de los sistemas de energía eléctrica deben realizar esfuerzos para garantizar la calidad y continuidad del suministro de energía. Desafortunadamente, los Sistemas de Energía Eléctrica (SEE) son vulnerables no solo a eventos naturales sino también a ataques deliberados (Zang et al., 2019). Estos eventos disruptivos traen consigo altos costos operativos por cambios no previstos en el plan de despacho inicial, costos de reparación de elementos como líneas, transformadores y torres, así como eventuales indemnizaciones a los consumidores por cortes de carga. Los ORD están a cargo de evaluar dichos costos y desarrollar estrategias para minimizar el impacto de eventuales apagones (Corredor & Ruiz, 2011). Dado que los costos de las interrupciones son altos tanto para los consumidores como para el operador de la red; es necesario establecer estrategias antes, durante y después de un ataque para mitigar el impacto y la duración de las interrupciones del servicio). Los problemas de optimización bi-nivel son particularmente difíciles de resolver, pues incluso si ambos niveles son lineales, el problema de optimización resultante es no lineal y no convexo (Wang et al., 2021). El problema de interdicción de sistemas de potencia fue inicialmente modelado como un problema de optimización bi-nivel en (Salmeron et al., 2004). En este caso, la función objetivo del agente disruptivo y del operador del sistema son la maximización y la minimización del deslastre de carga, respectivamente; lo que da lugar a un modelo de optimización max-min. (Arroyo et al.,2005) proponen una generalización de este problema introduciendo diferentes funciones objetivo para el agente disruptivo y el operador del sistema. Un modelo similar es propuesto por (Lai et al., 2019) considerando ataques cibernéticos. Este artículo se diferencia de los enfoques de la teoría de grafos como (Biswas et al., 2021) , (Yang et al., 2020) y (Pu et al., 2020) en el sentido de que no solo los buses, sino también las líneas y los generadores pueden identificarse como elementos críticos.

Además, a diferencia de (Salmeron et al., 2004), (Arroyo et al., 2005) y (Delgadillo et al., 2010), se implementa un modelado AC de la red, lo que permite un enfoque más realista del problema. También se diferencia de otros modelos EGIP en el sentido de que propone nuevas métricas de resiliencia y considera el uso de DERs dentro de las opciones del operador del sistema para reaccionar ante un ataque malicioso.

1.1. Escenarios para el caso de estudio

Las acciones de resiliencia son estrategias que se ejecutan en la etapa post-ataque e implican la optimización conjunta del uso de la infraestructura activa, los tipos de generadores disponibles y los arreglos de RD que se establecieron antes del desarrollo del evento disruptivo. Para evaluar la resiliencia que se puede lograr en los posibles escenarios derivados del uso de GD y el mecanismo de RD, se desarrolla un estudio de caso con cuatro escenarios.

- Escenario 1: no hay acuerdo para el deslastre voluntario de carga, bajo esta condición se ejecuta el plan de ataque más severo del análisis de vulnerabilidad sin tomar acciones de mitigación por parte del operador de red.
- Escenario 2: existe un acuerdo bilateral entre el operador de red y algunas cargas del sistema para desconectar voluntariamente un porcentaje de la carga total. A partir de esta condición, el agente disruptivo ejecuta el ataque más severo del análisis de vulnerabilidad. En la etapa posterior al ataque, el operador de red no realiza ninguna acción para disminuir la pérdida de carga.
- Escenario 3: no hay acuerdo para el deslastre voluntario de carga; bajo esta condición se ejecuta el plan de ataque más severo del análisis de vulnerabilidades. En la etapa posterior al ataque, el operador de red optimiza la ubicación y el tamaño de los generadores distribuidos para reducir la pérdida de carga.
- Escenario 4: existe un acuerdo bilateral entre el operador de la red y algunas cargas del sistema para desconectar voluntariamente un porcentaje de la carga total. A partir de la condición el agente disruptivo ejecuta el ataque más severo del análisis de vulnerabilidad. En la etapa posterior al ataque, el operador de red optimiza la ubicación de los generadores distribuidos y reasigna la respuesta de la demanda para reducir la pérdida de carga.

2. Modelado del enfoque matemático

2.1. Algoritmo Genético

Los AG son técnicas metaheurísticas inspiradas en la teoría darwiniana de la evolución. Este tipo de técnicas se han aplicado con éxito para resolver problemas de programación bi-nivel (Calvete et al., 2008)(Li et al., 2010)(G M Wang et al., 2007). La Figura 2 muestra el diagrama de flujo de la metodología implementada que incluye el AG. En este caso, una solución o individuo candidato se representa mediante un vector binario que representa las líneas y generadores fuera de servicio. La población inicial consiste en la generación aleatoria de vectores de interdicción. Cada vector de interdicción representa un ataque al sistema y una solución individual o candidata dentro del AG. A partir de la población inicial se obtienen nuevas soluciones candidatas mediante

operadores de selección, recombinación y mutación (Arroyo et al., 2013)(López-Lezama, 2020)(G. Wang et al., 2008). El mecanismo de selección garantiza que los mejores individuos sean elegidos para generar nuevas soluciones candidatas. Tales soluciones se obtienen mediante el operador de recombinación en el que los padres seleccionados intercambian su información genética. La etapa de mutación se encarga de agregar diversidad al algoritmo y eventualmente evitar quedar atrapado en soluciones óptimas locales. En cada generación, se conservan las mejores soluciones candidatas (aquellas que maximizan el deslastre de carga). El proceso se detiene después de que haya transcurrido un número determinado de generaciones (Smith, 2008).

2.2. Problema de optimización nivel superior

El problema de optimización de nivel superior viene dado por las ecuaciones (1)-(4). La función objetivo ilustrada en (1) es maximizar el costo operativo de la red después de un ataque. En este caso, C_g es el costo de la potencia entregada por el generador g; P_g es la potencia entregada por g; C_{RD_n} es el costo de la carga despachable en el nodo *n*; P_{RD_n} es la respuesta de la demanda en el nodo *n*; P_{D_m} es el deslastre de carga en el nodo *m*; C_{D_m} es el costo de deslastre de carga en el nodo *m*. La estrategia del agente disruptivo se modela a través de un vector de interdicción para líneas y generadores. En (2) y (3) el vector de interdicción para líneas y generadores, respectivamente, se define como un vector de variables binarias, donde 1 representa los elementos atacados. En este caso, $\delta_L(l)$ y $\delta_G(g)$ son los vectores de interdicción para el conjunto de líneas y generadores, respectivamente. La restricción (4) describe los recursos destructivos del agente atacante, donde M_l es el costo de atacar una línea mientras que M_g es el costo de atacar un generador. L es el conjunto de líneas; G es el conjunto de generadores; M representa los recursos totales del atacante; N es el conjunto de buses y NRD es el conjunto de buses con respuesta a la demanda.

$$Max \quad Z = \sum_g C_g P_g + \sum_n C_{RD_n} P_{RD_n} + \sum_m P_{D_m} C_{D_m} \quad \forall\, g \in G, \forall\, n \in NRD, m \in N \tag{1}$$

$$\delta_L(l) \in \{0,1\}; \quad \forall\, l \in L \tag{2}$$

$$\delta_G(g) \in \{0,1\}; \quad \forall\, g \in G \tag{3}$$

$$\sum_l M_l \delta_L(l) + \sum_g M_g \delta_G(g) \leq M; \quad \forall\, l \in L, \forall\, g \in G \tag{4}$$

2.3. Problema de optimización nivel inferior

El problema de optimización de nivel inferior define la respuesta del operador del sistema a través del cálculo de un despacho de potencia óptima AC. La ecuación (5) presenta la función objetivo del operador de la red. Considera el costo de operación de los generadores disponibles, el costo de desconexión voluntaria de carga a través del mecanismo DR y el costo de desconexión obligatoria de carga. Tenga en cuenta que, en este caso, el problema es de minimización. Las restricciones (6) a (10) definen las características físicas de la red relacionadas con los límites de potencia activa, reactiva y aparente en generadores, cargas y líneas, respectivamente. En este caso, Q_g es la potencia reactiva entregada por el generador g; P_d y Q_d son la demanda de potencia activa y reactiva, respectivamente; S_l^{Br} es el flujo de potencia aparente en la línea l. Las ecuaciones (11) y

(12) describen el equilibrio del flujo de potencia activa en cada nodo incorporando el límite de potencia activa desconectada (voluntaria y obligatoria) en las cargas, así como el vector de interdicción descrito en (2) y (3). En este caso, P_{RD_n} es la respuesta de la demanda en el nodo n; P_{D_m} es el deslastre de carga en el nodo m; Wn es la potencia programada para el generador n. En (13) y (14) se representan las potencias activas y reactivas transmitidas por las líneas. Las ecuaciones (15) y (16) indican el balance de potencia activa y reactiva, respectivamente; ${\Psi_G}^n$ es el conjunto de generadores conectados al nodo n; ${\Psi_D}^n$ es el conjunto de demandas conectadas al nodo y ${\Psi_L}^n$ es el conjunto de líneas conectadas al nodo n. El modelo de optimización de nivel inferior establece el flujo de potencia óptimo en la red después del ataque y el costo de operación del sistema representado por la variable Z.

$$Min \quad Z = \sum_g C_g P_g + \sum_n C_{RD_n} P_{RD_n} + \sum_m P_{D_m} C_{D_m} \qquad (5)$$

$$\forall\, g \in G\,, \forall\, n \in NRD, m \in N$$

$$P_g^{min} < P_g < P_g^{max} \qquad (6)$$

$$Q_g^{min} < Q_g < Q_g^{max} \qquad (7)$$

$$0 < P_d < P_d^{max} \qquad (8)$$

$$0 < Q_d < Q_d^{max} \qquad (9)$$

$${S_l}^{Br\,min} < {S_l}^{Br} < {S_l}^{Br\,max} \qquad (10)$$

$$P_d + P_{RD_n} + P_{D_m} = P_d^{max} \qquad (11)$$

$$0 < P_{RD_n} \leq P_d^{max} W_n RD_n \qquad (12)$$

$$P_{sr} = |V_s|^2 g_{sr} - |V_s||V_r|\, cos\, g_{sr} cos\,(\delta_s - \delta_r) - |V_s||V_r| b_{sr} sen(\delta_s - \delta_r) \qquad (13)$$

$$Q_{sr} = |V_s|^2 b_{sr} + cos\, b_{sr} |V_s||V_r| cos\,(\delta_s - \delta_r) - |V_s||V_r| b_{sr}\, g_{sr} sen(\delta_s - \delta_r) \qquad (14)$$

$$\sum_{\forall g \in {\Psi_G}^n} (1 - \delta_G(g)) P_g - \sum_{\forall d \in {\Psi_D}^n} P_d - \sum_{\forall s \in {\Psi_L}^n} {\delta_l}^{Br} P_{sr} = 0 \qquad (15)$$

$$\sum_{\forall g \in {\Psi_G}^n} (1 - \delta_G(g)) Q_g - \sum_{\forall d \in {\Psi_D}^n} Q_d - \sum_{\forall s \in {\Psi_L}^n} {\delta_l}^{Br} Q_{sr} = 0 \qquad (16)$$

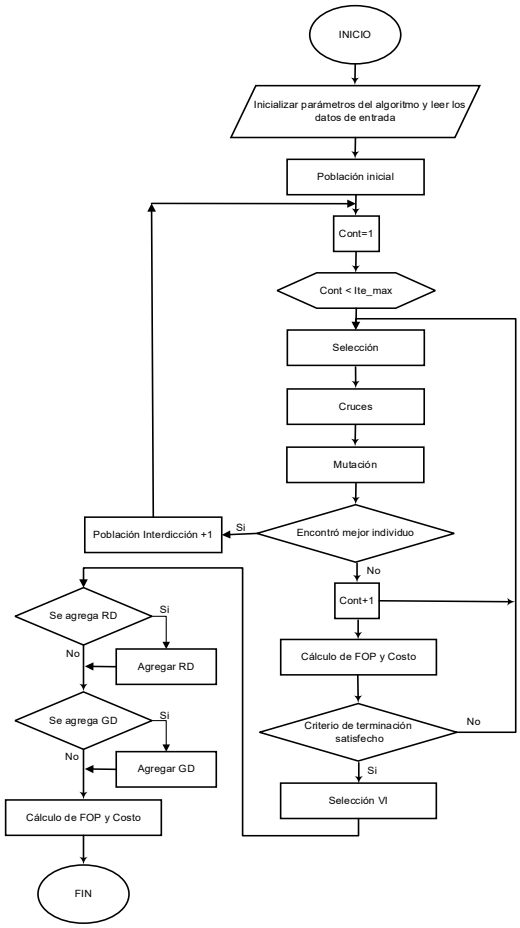

Figura 2. Diagrama de flujo de la metodología propuesta

2.4. Resiliencia de un sistema eléctrico

La resiliencia de un sistema de energía eléctrica implica prepararse, responder y mitigar los ataques que afectan una red eléctrica. Una evaluación cualitativa de la resiliencia de una red eléctrica requiere evaluar la efectividad de las medidas tomadas y la comparación de diferentes estrategias de respuesta por parte del operador de la red. En este documento, se proponen tres métricas para evaluar la resiliencia de las redes eléctricas, que se basan en la carga total servida y el costo operativo de la red, respectivamente. La ecuación (20) presenta la métrica de resiliencia en base a la carga total servida, lo que permite medir la efectividad de las acciones de mitigación para reducir el efecto del ataque disruptivo.

$$\mu 1 = \frac{Carga\ Servida}{Garga\ Total} \tag{20}$$

En la métrica $\mu 1$, un valor cercano a 1 representa la capacidad del sistema para gestionar adecuadamente el flujo de potencia óptimo para satisfacer la demanda. Por otro lado, un valor cercano a 0 define el peor escenario para la red en la que el suministro de energía es mínimo. La ecuación (21) presenta la métrica $\mu 2$, que mide la eficiencia de las acciones de mitigación del operador de

red para minimizar el costo de operación de la red después de un ataque mediante la evaluación de la porción del costo total de operación de la red que corresponde al deslastre de carga.

$$\mu 2 = 1 - \frac{Costo\ de\ Deslastre\ de\ Carga}{Costo\ de\ Operation} \tag{21}$$

En la métrica $\mu 2$, un valor cercano a 1 muestra que la red eléctrica tiene mecanismos para minimizar la desconexión de carga obligatoria como el peor de los casos para el operador de la red y las cargas. Mientras que un valor cercano a 0 coincide con un escenario en el que el costo del deslastre de carga es considerablemente mayor que los costos de operación de los generadores y el costo del deslastre voluntario de carga. En la ecuación (22) se propone la métrica μ como la medida de resiliencia de la topología y características de la red eléctrica ante el evento disruptivo más severo que puede desarrollar un atacante. En esta métrica, se evalúa conjuntamente la capacidad de las acciones de mitigación para disminuir el deslastre de carga y el costo de operación de la red luego de un ataque.

$$\mu = \frac{\mu 1 + \mu 2}{2} \tag{22}$$

Los valores de μ iguales a 1 y 0 cuantifican, respectivamente, una red completamente resiliente y una resiliente cero. Si bien la desconexión obligatoria implica mayores costos, la discriminación de los costos de deslastre de carga introduce una relación que no es necesariamente directamente proporcional. La Tabla 1 permite al operador de la red generar una evaluación cuantitativa y cualitativa de la resiliencia de una red eléctrica.

Tabla 1. Cuantificación de Resiliencia

μ	Grado de Resiliencia
$\mu = 0$	Ninguna
$0 < \mu \leq 0.25$	Deficiente
$0.25 < \mu \leq 0.5$	Pobre
$0.5 < \mu \leq 0.75$	Regular
$0.75 < \mu < 1$	Bueno
$\mu = 1$	Excelente

2.5. Estrategias para maximizar la resiliencia de la Red Eléctrica después de un Evento Disruptivo

En esta sección se describe el modelo que optimiza en conjunto la ubicación de la GD y el mecanismo DR como acciones de mitigación frente a eventos disruptivos. En función del ataque que el agente disruptivo seleccionó del análisis de vulnerabilidad, se evalúan la ubicación y el tamaño óptimos de DG, así como DR. La función objetivo del modelo de optimización para la ubicación de GD se describe en (23), en comparación con la ecuación (5) la función objetivo para este modelo incorpora el costo de GD. Las restricciones asociadas con los límites de potencia activa y reactiva en generadores, cargas y líneas se toman de (6)-(12). Las ecuaciones (24) y (25) son el balance de potencia activa y reactiva en cada nodo, mientras que las ecuaciones (26) y (27) definen la potencia máxima generada por el GD. En este caso, C_g y P_g son el costo y la potencia entregada por el generador g, respectivamente. C_{gd} y $P_g d$ son el costo

de la demanda y la potencia demandada, respectivamente. C_{RD_n} y $\mathrm{P_{RD_n}}$ son el costo y la cantidad de DR, respectivamente. P_{D_m} y C_{D_m} son la demanda en el nodo m y sus costos, respectivamente. P_g es la potencia activa suministrada por el generador g, $\mathrm{P_{gd}}$ es la potencia activa suministrada por DG, P_d es la potencia activa demandada. Finalmente (28) establece el número máximo de unidades de GD que se pueden utilizar dentro del proceso de optimización. En este caso, Q_g y Q_d son la generación y demanda de potencia reactiva, V_n es la magnitud del voltaje en la barra n.

$$Min \;\; Z = \sum_{g} C_g \, P_g + \sum_{gd} C_{gd} \, P_{gd} + \sum_{n} C_{RD_n} P_{RD_n} + \sum_{m} P_{D_m} C_{D_m} \tag{23}$$

$$\forall \, g \in G \, , \forall \, n \in NRD, m \in N$$

$$\sum_{\forall g \in \Psi_G{}^n} P_g + \sum_{\forall gd \in \Psi_{GD}{}^n} P_g d - \sum_{\forall d \in \Psi_D{}^n} P_d = V_n \sum_{j \in \Omega N} V_j Y_{ij} \, cos \, (\delta j - \delta i + \theta ij) \tag{24}$$

$$\sum_{\forall g \in \Psi_G{}^n} Q_g - \sum_{\forall d \in \Psi_D{}^n} Q_d = V_n \sum_{j \in \Omega N} V_j Y_{ij} \, sin \, (-\delta j + \delta i - \theta ij) \tag{25}$$

$$0 \leq P_{gd} \leq x_{gd} P_{gd}^{max} \tag{26}$$

$$x_{GD}(gd) \in \{0, 1\}; \;\; \forall \, gd \;\in\; GD \tag{27}$$

$$\sum\nolimits_{gd} x_{gd} \leq N_{gd}^{max} \tag{28}$$

3. Resultados y pruebas

Para mostrar la aplicabilidad y eficacia del enfoque propuesto, se llevaron a cabo varias pruebas con un sistema de alimentación didáctico de 5 buses y el sistema de alimentación IEEE RTS de 24 buses.

Para el sistema de 5 buses, el análisis de vulnerabilidad propuesto se aplicó inicialmente a un sistema de potencia compuesto por 5 buses y 5 generadores, cuyos datos se pueden consultar en [36]. Este sistema de potencia se ilustra en la Figura 3.

La efectividad de los ataques realizados para maximizar el deslastre de carga y aumentar el costo de operación de la red depende de la cantidad de recursos del agente perturbador, el costo asociado con atacar un conjunto de líneas o generadores y la resiliencia de la red después del ataque. La resiliencia de la red se cuantifica por la capacidad de cumplir con la carga programada y minimizar el aumento en el costo de operación de la red con la infraestructura en funcionamiento después del ataque. Los costos relacionados con el operador de red y el agente disruptivo se presentan en la Tabla 2. En este caso, el mecanismo de cobro por desconexión obligatoria de carga (deslastre de carga) permite al usuario recibir una compensación por el costo de cada MWh que no se está entregando y establece una jerarquía de cargas en función del coste del deslastre de cargas.

Tabla 2. Recursos del sistema

Recursos	Costos de elementos de ataque, DR, y deslastre de carga
Costo de atacar una línea ($/Línea)	50
Costo de atacar un generador ($/generador)	100
Recursos totals del atacante($)	300
Costo de deslastre de carga en los buses 2, 3, 4 ($/MWh)	100, 100, 400
Costo de DR a los buses 2, 3, 4 (%)	0, 50, 25
Costo de DR a los buses 2, 3, 4 ($/MWh)	0, 50, 50

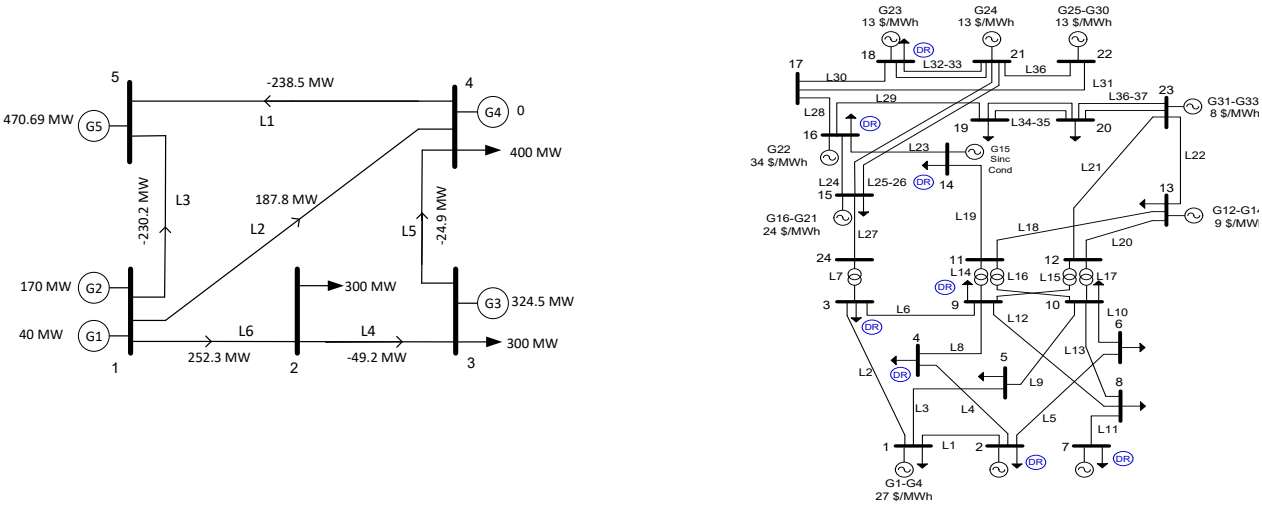

Figura 3., a.) Sistemas de pruebas de 5 buses, b.) Sistema IEEE RTS-24 buses

La Tabla 3a cuantifica la resiliencia en términos de costo operativo y porcentaje de la carga total servida, la Tabla 3b describe cuantitativa y cualitativamente el nivel de resiliencia alcanzado con cada escenario propuesto, que se muestra en la Figura 4. Esta figura muestra el nivel de carga servida en el desarrollo del evento disruptivo (t0-t1) y en la etapa posterior al evento (t1-t2) con respecto a las condiciones normales de operación.

	Served Load (MW)	Operation Cost ($)	Load Shedding Cost ($)
Escenario 1	520	183650	168000
Escenario 2	700	144645	120000
Escenario 3	920	41648	8000
Escenario 4	1000	37645	0

	$\mu 1$	$\mu 2$	μ	Resilience
Escenario 1	0.52	0.0852	0.3026	Pobre
Escenario 2	0.70	0.1703	0.4351	Pobre
Escenario 3	0.92	0.8079	0.8639	Bueno
Escenario 4	1	1	1	Excelente

Tabla 3**.,** a.) costos de carga servida, b.) Métricas de Resiliencia

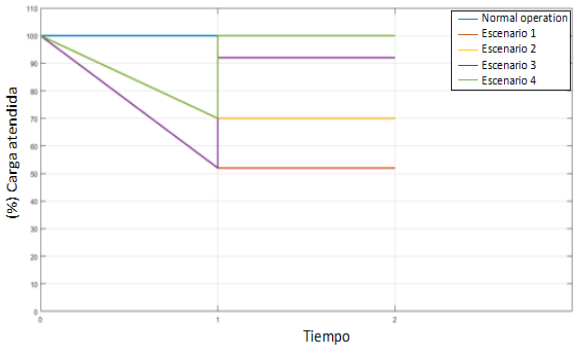

Figura 4. Porcentaje de carga servida

IEEE RTS 24, En condiciones normales de operación, la carga total servida es de 2850 MW y el costo total de operación es de $38284. Los recursos asignados al agente disruptivo le permiten ejecutar planes de ataques que resultan en diferentes niveles de deslastre de carga. Se consideran

cuatro casos como se indica en la Tabla 4a. En el Escenario 1, el porcentaje de carga servida es solo del 38% y el costo operativo es de $336464 por deslastre de carga. Para el Escenario 2, el operador del sistema establece acuerdos bilaterales de desconexión voluntaria de carga (DR) y alcanza un porcentaje de carga servida del 54%. En este caso DR permite atender el 15% de la demanda total y tiene un costo de $13325. En el Escenario 3, la DG se usa para mitigar el efecto del evento disruptivo en la red. Ubicar las 6 unidades GD en los buses más afectados permite atender un porcentaje del 8% de la carga total abastecida. En el Escenario 4, usando tanto DG como DR juntos, se logra el mayor nivel de resiliencia, reduciendo el costo total del sistema y la cantidad de deslastre de carga en relación a los anteriores; Se atiende el 61% de la carga total de la red y en conjunto estos mecanismos representan el 23% de la carga atendida. Las tablas 4a y 4b resumen los resultados de vulnerabilidad y resiliencia para los cuatro casos. La Tabla 4b presenta las métricas de resiliencia en cada uno de los casos ante un ataque disruptivo.

Tabla 4., a.) Resumen de costos, b.) Métricas de Resiliencia

	Carga servida (MW)	Carga servida (%)	Costo de carga deslastrada ($)
Escenario 1	1094.5	38.40	336464
Escenario 2	1527.2	53.58	218736
Escenario 3	1318.0	46.24	255394
Escenario 4	1750.7	61.42	184442

	μ1	μ2	μ	Resiliencia
Escenario 1	0.3840	0.052211	0.21812	Deficiente
Escenario 2	0.5359	0.131355	0.33360	Pobre
Escenario 3	0.4625	0.078019	0.27023	Pobre
Escenario 4	0.6142	0.147741	0.38095	Pobre

4. Agradecimientos

Los autores agradecen al C.I.D.C. Centro de Investigación y Desarrollo Científico de la Universidad Distrital Francisco José de Caldas, por el apoyo en el desarrollo de este trabajo, bajo el código 2-5-604-19 asociado al proyecto "Gestión de Recursos Energéticos Distribuidos (DER) y monitoreo de señales sísmicas en situaciones de desastre".

5. Conclusiones

Este artículo aborda el problema de la interdicción de la red eléctrica, en el que un agente malicioso tiene como objetivo causar el máximo daño a la red sujeto a un presupuesto limitado y la reacción del operador del sistema que puede recurrir a los DER para mitigar los impactos en la red. Las métricas propuestas por los autores permiten medir las acciones realizadas por el operador del sistema en cuanto a deslastre de carga y recursos energéticos distribuidos como respuesta a la demanda y generación distribuida a ser utilizados para la resiliencia del sistema y los costos que esto representa para la red y el usuario. Los resultados presentados muestran que el operador del sistema minimiza los daños causados a la red, así como los costos de operación cuando existe un acuerdo para desconectar voluntariamente un porcentaje de la carga y se ubican generadores distribuidos en ciertos nodos para atender la demanda.

6. Referencias

- Amirioun, M. H., Aminifar, F., Lesani, H., & Shahidehpour, M. (2019). Metrics and quantitative framework for assessing microgrid resilience against windstorms. *International Journal of Electrical Power and Energy Systems*, *104*(January 2018), 716–723. https://doi.org/10.1016/j.ijepes.2018.07.025
- Arroyo, J. M., & Fernández, F. J. (2013). A genetic algorithm for power system vulnerability analysis under multiple contingencies. *Studies in Computational Intelligence*, *482*, 41–68. https://doi.org/10.1007/978-3-642-37838-6_2
- Arroyo, J. M., & Galiana, F. D. (2005). On the solution of the bilevel programming formulation of the terrorist threat problem. *IEEE Transactions on Power Systems*, *20*(2), 789–797. https://doi.org/10.1109/TPWRS.2005.846198
- Bie, Z., Lin, Y., Li, G., & Li, F. (2017). Battling the Extreme: A Study on the Power System Resilience. *Proceedings of the IEEE*, *105*(7), 1253–1266. https://doi.org/10.1109/JPROC.2017.2679040
- Biswas, R. Sen, Pal, A., Werho, T., & Vittal, V. (2021). A Graph Theoretic Approach to Power System Vulnerability Identification. *IEEE Transactions on Power Systems*, *36*(2), 923–935. https://doi.org/10.1109/TPWRS.2020.3010476
- Calvete, H. I., Galé, C., & Mateo, P. M. (2008). A new approach for solving linear bilevel problems using genetic algorithms. *European Journal of Operational Research*, *188*(1), 14–28. https://doi.org/10.1016/j.ejor.2007.03.034
- Chalishazar, V., Poudel, S., Hanif, S., & Mana, P. T. (2021). Power System Resilience Metrics Augmentation for Critical Load Prioritization, 23. Retrieved from https://www.ntis.gov
- Corredor, P. H., & Ruiz, M. E. (2011). Mitigating the Impact of Terrorist Activity on Colombia's Power System. *IEEE Power and Energy Magazine*, *9*(2), 59–66.
- Costa, A., Georgiadis, D., Ng, T. S., & Sim, M. (2018). An optimization model for power grid fortification to maximize attack immunity. *International Journal of Electrical Power and Energy Systems*, *99*(January), 594–602. https://doi.org/10.1016/j.ijepes.2018.01.020
- Delgadillo, A., Arroyo, J. M., & Alguacil, N. (2010). Analysis of electric grid interdiction with line switching. *IEEE Transactions on Power Systems*, *25*(2), 633–641. https://doi.org/10.1109/TPWRS.2009.2032232
- Henry, D., & Emmanuel Ramirez-Marquez, J. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering and System Safety*, *99*, 114–122. https://doi.org/10.1016/j.ress.2011.09.002
- Lai, K., Illindala, M., & Subramaniam, K. (2019). A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Applied Energy*, *235*(August 2018), 204–218. https://doi.org/10.1016/j.apenergy.2018.10.077
- Li, H., Jiao, Y., & Zhang, L. (2010). Orthogonal genetic algorithm for solving quadratic bilevel programming problems. *Journal of Systems Engineering and Electronics*, *21*(5), 763–770. https://doi.org/10.3969/j.issn.1004-4132.2010.05.008
- Liu, B., Li, Z., Chen, X., Huang, Y., & Liu, X. (2018). Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *65*(3), 346–350. https://doi.org/10.1109/TCSII.2017.2705482
- López-Lezama, J. P. H.-V. B. J. R.-C. J. M. (2020). A Bilevel Attacker-Defender Model for Enhancing Power Systems Resilience with Distributed Generation. *Scientia et Technica*, *25*(4), 540–547. https://doi.org/10.22517/23447214.23721

Sobre los autores

- **Darin J. Mosquera Palacios**: Ingeniero de Sistemas, Máster en Teleinformática, Docente Universidad Distrital Francisco José de Caldas. Profesor Asociado djmosquerap@correo.udistrital.edu.co
- **Edwin Rivas Trujillo**: ingeniero electricista universidad del Valle Colombia, doctor en ingeniería eléctrica universidad Carlos III de Madrid, docente Universidad Distrital Francisco José de Caldas. Profesor titular. erivas@udistrital.udu.co
- **Luis Alejandro Arias Barragán**. Ingeniero Electromecánico, Doctor en ingeniería con énfasis en Ingeniería eléctrica universidad Distrital Francisco José de Caldas, Docente Universidad ECCI. lariasb@ecci.edu.co

---