

Tipo de artículo: Artículo original  
Temática: Matemática Computacional  
Recibido: 29/10/2015 | Aceptado: 18/05/2016

# **Análisis de vulnerabilidad en sistemas eléctricos de potencia usando la metaheurística GRASP**

## ***Vulnerability analysis in electric power systems using the GRASP metaheuristic***

**Juan J. Cortina<sup>1</sup>, Jesús M. López-Lezama<sup>2\*</sup> y Nicolás Muñoz-Galeano<sup>2</sup>**

<sup>1</sup> XM S.A. E.S.P. - Filial de ISA. Calle 12 Sur No. 18-168, Medellín – Colombia. [jcortina@xm.com.co](mailto:jcortina@xm.com.co).

<sup>2</sup> Grupo de Investigación GIMEL, Departamento de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de Antioquia. Calle 70 No. 52-21, Medellín – Colombia. [jmaria.lopez@udea.edu.co](mailto:jmaria.lopez@udea.edu.co), [nicolas.munoz@udea.edu.co](mailto:nicolas.munoz@udea.edu.co).

\* Autor para correspondencia: [jmaria.lopez@udea.edu.co](mailto:jmaria.lopez@udea.edu.co)

---

### **Resumen**

Este artículo presenta un modelo para análisis de vulnerabilidad en sistemas de potencia usando una técnica de optimización metaheurística. En su versión tradicional, el problema de vulnerabilidad es abordado usando un modelo lineal de la red y considerando solamente el ataque a líneas o transformadores. El modelo propuesto en este artículo no solo considera el ataque a líneas y transformadores, sino también a generadores. Adicionalmente, utiliza un modelo no lineal de la red, lo que permite obtener soluciones más aproximadas a la realidad. El modelo es resuelto mediante la metaheurística GRASP (Procedimiento de Búsqueda Aleatoria Adaptativa Golosa). La solución del modelo permite identificar un conjunto de contingencias que hacen el sistema de potencia más vulnerable. Esta información ayuda al operador de la red a tomar acciones para proteger su sistema y disminuir el riesgo.

**Palabras clave:** programación binivel, interdicción, vulnerabilidad y metaheurísticas.

### **Abstract**

*This paper presents a power system vulnerability analysis model using a metaheuristic optimization approach. In its traditional version, the vulnerability problem is approached using a lineal model of the network and considering only the attack of lines or transformers. The proposed model in this paper considers not only the attack of lines or transformers but also the one of generators. Furthermore, a nonlinear model of the network is considered, allowing more approximate solutions to reality. The proposed model is solved by the GRASP (Greedy Randomized Adaptive Search Procedures) metaheuristic technique. The solution of the model allows identifying a set of contingencies that*

*make the power system more vulnerable. This information helps the power system operator to take protective actions on the system and reduce risk.*

**Keywords:** *bi-level programming, interdiction, vulnerability, metaheuristics.*

---

## Introducción

Con la creciente amenaza del terrorismo en el mundo, se está prestando cada vez más atención a la seguridad de la infraestructura eléctrica (Corredor y Ruiz, 2011). Actualmente, la salida de operación de elementos en los sistemas de potencia no se debe únicamente a fenómenos naturales aleatorios, sino también a actos mal intencionados (Arroyo, 2010). En el contexto de los sistemas eléctricos de potencia existe el modelo de ataque-defensa conocido como “el problema del terrorista” o problema de interdicción introducido en (Salmeron et al., 2004). Este problema consta de un agente atacante (terrorista) que pretende hacer el máximo daño al sistema, y un agente defensor (operador de la red) que procura minimizar este daño. El objetivo del operador de la red es analizar el impacto de un conjunto de contingencias que pueden presentarse de manera simultánea e identificar aquellas a las que el sistema es más vulnerable. Esto a fin de tomar acciones correctivas para minimizar la demanda no suministrada. El objetivo del agente atacante consiste en maximizar la demanda no suministrada, sujeto a sus límites de recursos y a la reacción del agente defensor. Esta interacción ataque-defensa, da lugar a un problema de optimización binivel. En un problema de optimización binivel existen dos problemas de optimización que interactúan de forma jerárquica. En el nivel superior de optimización se ubica el líder del problema el cual decide sobre sus variables sujeto a la reacción del agente del nivel inferior o seguidor. Desde el punto de vista de programación matemática, un modelo binivel es un problema de optimización con restricciones de optimización, lo cual lo hace especialmente difícil de resolver, sobre todo cuando el problema del nivel inferior es no convexo (Brown et al., 2006).

El problema de interdicción propuesto inicialmente en (Salmerón et al., 2004) como un problema Max-Min es generalizado en (Arroyo y Galiana, 2005). En este caso, el objetivo del agente atacante es minimizar el número de elementos atacados para que la demanda no suministrada sea igual o mayor a un valor predefinido. En (Arroyo y Fernández, 2009) se propone un modelo de programación no lineal entera mixta para abordar el problema de interdicción. En el nivel superior se maximiza el deslastre de carga; mientras que en el nivel inferior el operador de la red reacciona al ataque ejecutando un despacho óptimo considerando como parte de su estrategia la posible apertura de líneas. Este nuevo abordaje del problema implica adicionar una variable binaria de decisión en el nivel inferior y es resuelto usando una metaheurística. En (Arroyo, 2010) se presentan dos modelos: de mínima y máxima

vulnerabilidad. En el modelo de mínima vulnerabilidad, el objetivo del atacante en el nivel superior es minimizar el número de líneas a atacar para lograr un nivel de deslastre de carga deseado; mientras que en el modelo de máxima vulnerabilidad, el objetivo del atacante es maximizar la carga deslastrada dado un número determinado de líneas a atacar. Ambos planteamientos se abordan mediante programación lineal entera mixta usando las condiciones de optimalidad de Karush Kuhn Tucker - KKT y la Teoría de la Dualidad para convertir el problema binivel en un problema equivalente de un solo nivel.

Tradicionalmente el modelo de interdicción ha sido resuelto usando modelos aproximados de la red de transmisión (Romero et al., 2012). Sin embargo, en (Agudelo et al., 2014) se plantea por primera vez el problema de interdicción considerando un modelo no lineal (AC) de la red de transmisión. Este modelo es más aproximado a la realidad y permite valorar mejor el impacto de las contingencias en la red. El objetivo del presente trabajo es proponer un nuevo modelo y método de solución para el problema de interdicción. El presente artículo amplía la contribución de (Agudelo et al., 2014), considerando también el modelo AC de la red de transmisión e incorporando en el análisis, no solo la salida de circuitos (líneas o transformadores), sino también la salida de generadores como elementos susceptibles de ser atacados. Con la inclusión de generadores como elementos potencialmente atacables es posible suministrar información al operador de la red sobre sus zonas vulnerables cuando el total de la generación no está disponible. Lo anterior puede cubrir situaciones, tanto de salidas fortuitas, como intencionales. El modelo es resuelto a través de la técnica metaheurística GRASP (Procedimiento de Búsqueda Aleatoria Adaptativa Golosa), la cual no ha sido utilizada para abordar el problema de interdicción. El modelo propuesto es probado en el sistema IEEE de 24 barras mostrando resultados satisfactorios.

## Modelo matemático del problema de vulnerabilidad

La formulación matemática del problema de interdicción AC está dada por las ecuaciones (1) a (20).

$$\max_{\delta_g^{Gen}, \delta_l^{Lin}} \sum_n P_{DSn}; \quad \forall n \in N \quad (1)$$

Sujeto a:

$$\sum_l M_l(1 - \delta_l^{Lin}) + \sum_g M_g(1 - \delta_g^{Gen}) \leq M; \quad \forall l \in Lin, \forall g \in Gen \quad (2)$$

$$\delta_g^{Gen} \in \{0,1\}; \quad \forall g \in Gen \quad (3)$$

$$\delta_l^{Lin} \in \{0,1\}; \quad \forall l \in Lin \quad (4)$$

$$\min_x \sum_g c_g P_g^{Gen} + \sum_n c_{DS_n} P_{DS_n}; \quad x = \begin{bmatrix} \theta_n, V_n, P_g^{Gen}, Q_g^{Gen}, P_l^{Lin}, Q_l^{Lin}, \\ P_{DS_n}, Q_{DS_n}, P_{DR_{i,n}} \end{bmatrix} \quad (5)$$

Sujeto a:

$$\theta_n^{min} \leq \theta_n \leq \theta_n^{max}; \quad \forall n \in N \quad (6)$$

$$V_n^{min} \leq V_n \leq V_n^{max}; \quad \forall n \in N \quad (7)$$

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

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

$$S_l^{min} \leq S_l^{Lin} \leq S_l^{max}; \quad \forall l \in Lin \quad (10)$$

$$0 \leq P_{DS_n} \leq P_{D_n}; \quad \forall n \in N \quad (11)$$

$$0 \leq Q_{DS_n} \leq Q_{D_n}; \quad \forall n \in N \quad (12)$$

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

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

$$(S_l^{Lin})^2 = (P_l^{Lin})^2 + (Q_l^{Lin})^2; \quad \forall l \in Lin \quad (15)$$

$$P_l^{Lin} = \delta_l^{Lin} \cdot [g_{mn} V_n^2 + g_{mn} V_m V_n \cos(\theta_{mn}) - b_{mn} V_m V_n \sin(\theta_{mn})]; \quad \forall l \in Lin \quad (16)$$

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

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

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

$$\theta_{ref} = 0 \quad (20)$$

Donde:

Índices y conjuntos

$m, n$  Índices que denotan barras del sistema.

$l, g$  Índice de líneas (o transformadores) y generadores, respectivamente.

$Lin, Gen$  Conjunto de líneas y generadores, respectivamente.

N Conjunto de barras del sistema de potencia.

Parámetros

$M$	Recursos disponibles totales para realizar un ataque, expresado en unidades monetarias.
$M_l$	Costo de atacar una línea o un transformador, expresado en unidades monetarias por elemento.
$M_g$	Costo de atacar un generador, expresado en unidades monetarias por elemento.
$c_g$	Precios de oferta de la generación, expresado en unidades monetarias por megavatio.
$c_{DSn}$	Costo de racionamiento de carga activa en la barra $n$ , expresado en unidades monetarias por megavatio.
$P_{Dn}, Q_{Dn}$	Demanda de potencia activa y reactiva en la barra $n$ , respectivamente.
$p_g^{max}, p_g^{min}$	Límites máximo y mínimo de generación de potencia activa en la barra $n$ , respectivamente.
$Q_g^{max}, Q_g^{min}$	Límites máximo y mínimo de generación de potencia reactiva en la barra $n$ , respectivamente.
$p_l^{max}, p_l^{min}$	Límites máximo y mínimo de potencia activa por la línea $l$ , respectivamente.
$Q_l^{max}, Q_l^{min}$	Límites máximo y mínimo de potencia reactiva por la línea $l$ , respectivamente.
$S_l^{max}, S_l^{min}$	Límites máximo y mínimo de potencia aparente por la línea $l$ , respectivamente.
$\theta_n^{max}, \theta_n^{min}$	Límites máximo y mínimo de ángulo de fase en la barra $n$ , respectivamente.
$V_n^{max}, V_n^{min}$	Límites máximo y mínimo de magnitud de tensión en la barra $n$ , respectivamente.
$g_{mn}$	Conductancia de la línea $l$ que interconecta las barras $m$ y $n$ .
$b_{mn}$	Susceptancia de la línea $l$ que interconecta las barras $m$ y $n$ .
$\theta_{mn}$	Diferencia angular de las barras $m$ y $n$ .

Variables

$\delta_g^{Gen}, \delta_l^{Lin}$	Vectores de interdicción de generadores y líneas (o transformadores), respectivamente.
$P_{DSn}, Q_{DSn}$	Deslastre de potencia activa y reactiva en la barra $n$ , respectivamente.
$P_l^{Lin}, Q_l^{Lin}$	Flujo de potencia activa y reactiva por la línea $l$ , respectivamente.
$P_g^{Gen}, Q_g^{Gen}$	Generación de potencia activa del generador $g$ , respectivamente.
$P_n, Q_n$	Inyecciones de potencia activa y reactiva en la barra $n$ , respectivamente.
$S_l^{Lin}$	Flujo de potencia aparente por la línea $l$ .
$\theta_n, V_n$	Ángulo de fase y magnitud de tensión en la barra $n$ , respectivamente

La ecuación (1) es la función objetivo del nivel superior, la cual representa las intenciones del agente atacante que consiste en maximizar la potencia deslastrada  $P_{DS}$ . La ecuación (2) indica las restricciones de recursos del agente atacante. Se supone que el agente atacante cuenta con un máximo de recursos igual a  $M$  y atacar un circuito (línea o transformador) cuesta  $M_l$ , mientras atacar un generador cuesta  $M_g$ . Las restricciones (3) y (4) indican la naturaleza binaria de los vectores de interdicción de generadores y circuitos, respectivamente. Si una posición de estos vectores es uno (1) indica que el elemento correspondiente está en funcionamiento; por otro lado, si la posición es (0) indica que el elemento correspondiente ha sido atacado. Note que las variables de decisión del nivel superior son únicamente el conjunto de elementos a ser atacados. El problema del agente atacante está sujeto a las limitaciones en sus recursos

destructivos (M) y a la reacción del operador de la red. Esta reacción corresponde al nivel inferior de optimización y está dada por las ecuaciones (5) a (20). Dado un plan de ataque el operador de la red reacciona modificando el esquema de generación de modo que se minimice la demanda no atendida; sin embargo, debe tener en cuenta las limitaciones físicas de la red. La función objetivo del operador de la red está dada por la ecuación (5), la cual minimiza los costos de atender la demanda, ya sea mediante el cambio en el esquema de generación o, como último recurso, mediante el deslastre de carga. Las ecuaciones (6) a (10) indican los límites en ángulos y tensiones de los nodos del sistema; a los límites en potencia activa y reactiva de los generadores; y a los límites de flujo de potencia aparente en las líneas y transformadores. Las ecuaciones (11) y (12) modelan los límites de deslastre de potencia activa y reactiva en cada barra del sistema. Las ecuaciones (13) y (14) representan las inyecciones nodales de potencia activa y reactiva, respectivamente. Las ecuaciones (15)-(17) representan para cada rama del sistema los flujos de potencia aparente, potencia activa y potencia reactiva, respectivamente. Las ecuaciones (18) y (19) modelan, para cada nodo, el balance de potencias activa y reactiva. Finalmente, la ecuación (20) define la referencia angular. Las ecuaciones (13) a (17) distinguen el modelo propuesto del abordaje tradicional del problema de interdicción, pues introducen la representación en corriente alterna (AC) de la red de transmisión. Adicionalmente, el efecto de posibles ataques en generadores no se ha reportado en este tipo de problema.

## **Metodología computacional**

El problema de interdicción, abordado mediante programación binivel, puede ser resuelto a través métodos exactos o métodos aproximados. Cuando el problema del nivel inferior es convexo, el problema original de dos niveles puede ser transformado en un problema equivalente de un solo nivel usando el Teorema de la Dualidad (Motto et al., 2005; Arroyo, 2010) o usando las condiciones de optimalidad de KKT (Arroyo y Galiana, 2005). El problema de un solo nivel equivalente puede ser resuelto usando técnicas de programación lineal entera mixta como Branch and Bound (Salmerón et al., 2009) o Descomposición de Benders (Delgadillo et al., 2010). Por otro lado, si el problema del nivel inferior no es convexo, el modelo no puede ser llevado a un equivalente de un solo nivel. En este caso se pueden encontrar soluciones usando métodos de optimización metaheurística (Salmerón et al., 2004; Arroyo y Fernández, 2009; Romero, et al., 2012; Agudelo, et al., 2014). El modelo descrito en las ecuaciones (1) - (20) representa un ejemplo de este último caso. Para encontrar soluciones al problema se optó por una técnica de optimización metaheurística para su solución. En particular, se utilizó el método GRASP debido su facilidad de implementación y a su capacidad para encontrar soluciones de alta calidad con bajos tiempos de cómputo (Resende y González, 2003).

## Representación de la Solución

En este caso se define el Vector de Interdicción (VI) como un candidato de solución o plan de ataque del agente atacante. Este vector es un arreglo lineal que resulta de la combinación de los vectores  $\delta_l^{Lin}$  y  $\delta_g^{Gen}$  (ecuación (2)). Pevio a su construcción, el total de elementos del sistema susceptibles de ser atacados debe ser enumerado. Se puede tener una representación binaria de VI o una representación entera. La representación binaria de VI es un arreglo de tamaño NL+NG; donde NL es el total de líneas y transformadores que existe en el sistema de potencia y NG es el total de generadores. Las primeras componentes de VI, desde la posición 1 hasta la posición NL representan el estado de líneas y transformadores en el sistema de potencia. El resto de las componentes representan el estado de los generadores. Cuando una componente de VI es cero (0) significa que el respectivo elemento del sistema de potencia ha sido atacado, de lo contrario, si la componente es uno (1) significa que el elemento está en servicio.

La representación entera de VI es un equivalente que se hace de la representación binaria y consiste en un vector cuyas componentes corresponden exactamente a las posiciones de los elementos del sistema que han sido atacados. Este vector es de tamaño K, siendo K el número de elementos que puede atacar el agente atacante, según se lo permitan sus recursos económicos [ecuación (2)]. En esta representación también se considera la misma numeración de elementos considerada en la representación binaria; de tal forma que si el valor de una componente de VI, en representación entera, es menor o igual a NL, significa que el elemento atacado fue una línea o un transformador y la posición atacada es la que indica la componente. Si el valor de la componente es mayor a NL, significa que el elemento atacado fue un generador. En este sentido, la representación binaria de VI es función del tamaño del sistema de potencia, mientras que la representación entera es independiente del tamaño del sistema. La codificación utilizada en el modelo propuesto fue la entera, la cual disminuye el esfuerzo computacional. A manera de ejemplo, en la Figura 1 se ilustra la representación binaria (Figura 1a) y la representación entera (Figura 1b) de un VI. En este caso, se considera un sistema de potencia con 3 generadores y 7 líneas donde el agente del nivel superior solo cuenta con recursos que le permitieron atacar las líneas de las posiciones 1, 4 y 6 y el generador de la posición 9.

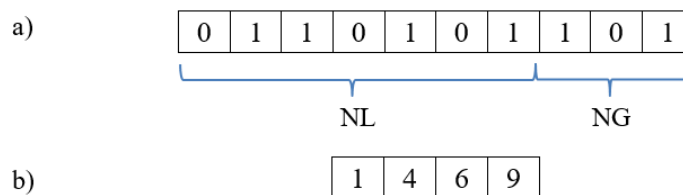


Figura 1. VI con K = 4. Sistema de potencia: 7 líneas y 3 generadores.  
 Representación: a) Binaria. b) Entera.

El agente atacante cuenta con recursos limitados que le permiten atacar  $K$  elementos del sistema de potencia.  $K$  puede cambiar de un VI a otro de acuerdo con los costos que representa atacar cada tipo de elemento (líneas, transformadores y generadores). Por lo anterior, el problema de interdicción se reduce a decidir la combinación de elementos que deben ser atacados para maximizar el deslastre de carga, considerando el límite  $M$  en los recursos destructivos, los costos de atacar cada elemento y la reacción del operador de la red. Para tener en cuenta esto último, dado un plan de ataque VI la reacción del operador de la red se calcula solucionando un problema de flujo de potencia óptimo mediante el software de optimización Matpower (Zimmerman et al., 2011). El flujo óptimo recibe como parámetros el nuevo estado de la red en función de VI y entrega como resultado la demanda desatendida.

### **Solución usando GRASP**

Para implementar la metaheurística GRASP se genera una solución inicial en la que se ataca aleatoriamente un elemento de la red eléctrica a la vez hasta completar un VI-semilla con  $K$  elementos atacados. El costo total de ataque, o función de costo (FC), se mantiene menor o igual al límite  $M$  de recursos económicos del agente atacante. La FC se actualiza cada vez que se ataca un elemento de la red de acuerdo a su tipo y costo. Este procedimiento constructivo se repite hasta lograr un número deseado de VI-semillas distintos entre sí que garanticen diversidad. Para cada VI-semilla que resulta del constructivo, se calcula el valor de la función objetivo (FO) del agente atacante (maximizar el deslastre de carga en función de los MW racionados) y este valor se mejora aplicando búsqueda local mediante dos movimientos. El primer movimiento está definido por la variación aleatoria y simultánea de dos (2) componentes de VI. La variación es aceptada si la FC del VI resultante es menor o igual a  $M$  y el deslastre de carga obtenido es mayor que el obtenido con los valores sustituidos. Este procedimiento se finaliza aplicando uno de los siguientes criterios: 1) Criterio de máxima mejora, que consiste en encontrar una mejor solución dentro de un número dado de iteraciones. 2) Criterio de primera mejora, que consiste en encontrar la primera mejor solución.

Para cada VI de las soluciones iniciales se aplican los dos movimientos descritos un número dado de iteraciones y al finalizar se obtiene un VI mejorado. Del conjunto de las soluciones finales mejoradas se seleccionan las que tienen mejor función objetivo que sean diferentes entre sí. Estas soluciones se toman como los resultados del modelo. La Figura 2 muestra el flujograma resumido de la técnica GRASP desarrollada.



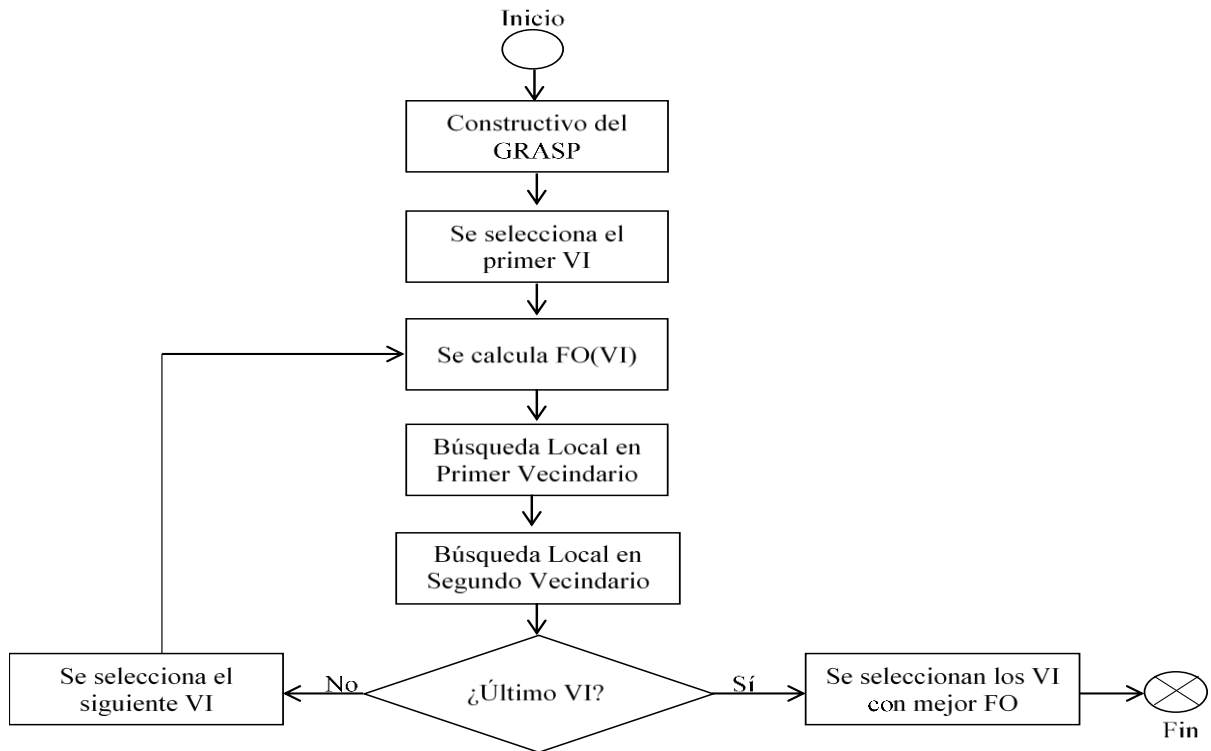


Figura 2. Esquemático del GRASP

## Resultados y discusión

Para probar el modelo propuesto se utilizó el sistema de prueba IEEE RTS-24 cuyos datos pueden ser consultados en (Wong, P. et al., 1999). Este sistema cuenta con 24 barras, 38 circuitos (líneas y transformadores), 11 generadores y 17 cargas. Se realizaron pruebas para un perfil de carga de un día de invierno a las 18 horas y demanda total de 2850 MW. Se asumió que todos los generadores tienen potencia mínima de generación de 0 MW. Así mismo, que el agente atacante cuenta con una cierta cantidad de recursos económicos  $M$  que, por simplicidad, se considerarán como valores enteros expresados en unidades monetarias.

Inicialmente, para calibrar los parámetros del algoritmo se consideraron diferentes variaciones del GRASP. Para tener un comparativo con una solución de referencia se ajustó el algoritmo para considerar únicamente ataques en líneas. Las soluciones fueron contrastadas con las reportadas en (Arroyo, 2010) para un ataque de 6 elementos ( $M = 6$ ). La Tabla 1 muestra las variantes consideradas.

Tabla 1. Variantes del GRASP bajo consideración

Variante		A	B	C	D
Número de iteraciones en la Búsqueda Local	Bajo	X	X		
	Alto			X	X
Criterio de parada de la Búsqueda Local	Primera Mejora	X		X	
	Max Mejora		X		X

En la Tabla 2 se muestra una comparación cualitativa del desempeño de las distintas variantes del método GRASP. Para cada variante se realizaron 3 ejecuciones. En cuanto al número de iteraciones de la búsqueda local se definieron las variantes “Bajo” y “Alto” para representar ejecuciones con 15 y 30 iteraciones, respectivamente. Con respecto al tiempo de cómputo se hizo un promedio de las ejecuciones y se definieron las etiquetas “Alto”, “Medio” y “Bajo” como aquellas soluciones que tomaron más de 2000 segundos, entre 1000 y 2000 segundos y menos de 1000 segundos, respectivamente. Para calificar la calidad de soluciones, estas se compararon con la solución óptima del problema linealizado reportada en (Arroyo, 2010), la cual es 1017 MW. Se definieron etiquetas de calidad “Alta”, “Media” y “Baja” como aquellas que diferían menos del 5, 20 y 30% de la solución de referencia, respectivamente. Se definieron etiquetas de estabilidad del algoritmo como “Alta”, “Media” y “Baja” para referirse a la capacidad de este de encontrar soluciones similares para cada corrida. Finalmente, se definieron etiquetas de variedad de soluciones de alta calidad como “Alta”, “Media” y “Baja” para referirse a la capacidad del algoritmo de encontrar soluciones alternativas a la reportada en (Arroyo, 2010) con función objetivo similar. Al margen de las variantes planteadas, se obtuvo mayor variedad de soluciones de alta calidad cuando el número de candidatos iniciales era mayor a 100.

Tabla 2. Comparación de desempeño para diferentes variantes del GRASP

	A	B	C	D
Tiempo de cómputo	Bajo	Bajo	Medio	Alto
Calidad de soluciones	Baja	Media	Alta	Alta
Estabilidad	Baja	Media	Alta	Alta
Variedad de soluciones de alta calidad	Baja	Baja	Media	Alta

A pesar de que el tiempo de cómputo es “Alto” se puede observar en la Tabla 2 que la variante del GRASP más conveniente, en función de los atributos estudiados, es la D. En particular, con esta variante fue posible encontrar 4 ataques diferentes con calidad similar a la reportada en (Arroyo, 2010). Esta es una fortaleza que no tienen los

algoritmos basados en programación matemática clásica, pues solo encuentran una solución al problema. Note que el resultado de racionamiento es ligeramente mayor a 1017 MW dado que se ha utilizado el modelo AC de la red. En la Tabla 3 se ilustran las mejores soluciones encontradas con la variante D. Las pruebas posteriores con la variante D se realizaron incrementando el número de candidatos de solución inicial a 500. A pesar de que el tiempo de cómputo aumenta, esto garantiza obtener variedad de soluciones de alta calidad.

Tabla 3. Mejores soluciones encontradas con la variante D del GRASP

$VI$	$\sum_n P_{DS_n} [MW]$
3-24, 7-8, 9-12, 10-12, 11-13, 14-16	1020.6
7-8, 9-12, 10-12, 11-13, 14-16, 15-24	1020.6
3-24, 7-8, 11-13, 12-13, 12-23, 14-16	1020.3
7-8, 11-13, 12-13, 12-23, 14-16, 15-24	1020.3

Con el fin de mostrar la versatilidad del modelo propuesto y analizar la criticidad de distintos elementos del sistema de potencia, se realizaron ensayos en los que se asumió que atacar cualquier circuito (línea o transformador) tenía el mismo costo  $M_l = 1$ . Posteriormente se modificó el costo de atacar las unidades de generación, asignando  $M_g = 3$ ,  $M_g = 2$  y  $M_g = 1$ . Se asumió un máximo de  $M_g = 3$ , dado que en promedio a cada barra de generación llegan tres líneas, por lo cual, atacar un generador, es equivalente a atacar tres líneas. Para efectos de validación los ensayos se consideraron variando los recursos  $M$ , de forma similar a como se presenta en (Arroyo, 2010). Para todas las simulaciones se asumió que el costo de racionamiento es igual al doble del costo de oferta de energía del generador más caro. Las Tablas 4 a 6 resumen los resultados de los mejores planes de ataque obtenidos en el modelo de interdicción. Para identificar un circuito (línea o transformador) se etiquetan las dos barras del sistema en las que se ubica el respectivo elemento, separado por un guion (-); mientras que para los generadores, se antepone la letra G a la barra en la que se ubica el mismo. El tiempo de cómputo se muestra en segundos. Las pruebas se realizaron con un computador de procesador Intel Core-i5 y 4GW de memoria RAM.

Tabla 4. Mejores planes de ataque con  $M_g = 3$  y  $M_l = 1$

$M$	$VI$	$\sum_n P_{DS_n} [MW]$	% Demanda Total	Tiempo de cómputo
3	16-19, 20-23, 20-23	309	10.8	2510.51
4	12-23, 13-23, 14-16, 15-24	724.47	25.4	4188.09
5	11-13, 12-13, 12-23, 14-16, 15-24	848.97	29.8	5248.65
6	3-24, 7-8, 11-13, 12-13, 12-23, 14-16	1020.6	35.8	7685.37
9	7-8, 11-13, 12-13, 12-23, 15-21, 15-21, 16-17, 20-23, 20-23	1375.57	48.3	8117.36

Tabla 5. Mejores planes de ataque con  $M_g = 2$  y  $M_l = 1$

$M$	$VI$	$\sum_n P_{DS_n} [MW]$	% Demanda Total	Tiempo de cómputo
3	16-19, 20-23, 20-23	309	10.8	3329.73
4	G13, G23	725.63	25.5	4095.98
5	7-8, G13, G23	896.16	31.4	5083.03
6	12-23, 13-23, 14-16, 15-24, G13	1113.97	39.1	7047.75
9	1-5, 7-8, 15-21, 15-21, 16-17, G13, G23	1642.29	57.6	8927.14

Tabla 6. Mejores planes de ataque con  $M_g = 1$  y  $M_l = 1$

$M$	$VI$	$\sum_n P_{DS_n} [MW]$	% Demanda Total	Tiempo de cómputo
3	G13, G18, G23	1112.7	39.0	2524.41
4	G13, G18, G21, G23	1507.9	52.9	5235.33
5	G7, G13, G18, G21, G23	1803.5	63.3	5936.47
6	G7, G13, G18, G21, G22, G23	2098.6	73.6	4470.48
9	G1, G2, G7, G13, G15, G18, G21, G22, G23	2695.1	94.6	8781.69

En la Tabla 4 se observa que si atacar un generador es tres veces más costoso que atacar un circuito, la mejor estrategia es atacar solamente líneas o transformadores. Estos resultados son consistentes con los reportados en (Agudelo et al., 2014) y (Arroyo y Galiana, 2005) que utilizan modelos donde solo se pueden atacar líneas o transformadores. Sin embargo, a medida que el costo de atacar un generador ( $M_g$ ) disminuye, es más atractivo atacar estos elementos (ver Tablas 5 y 6). Cuando  $M_g = 1$  se pueden evidenciar planes de ataques que incluyen solo generadores y que ocasionan mayor deslastre de carga. En la Tabla 4, cuando se considera  $M = 6$  no fue posible encontrar una combinación de ataque a dos generadores que produjeran un mayor deslastre de carga que el obtenido con el ataque de 6 circuitos. De igual forma, con  $M = 9$  no se encontró ninguna combinación de ataque de 3 generadores que pudieran causar más daño que atacar 9 circuitos.

Por otro lado, cuando el costo de atacar un generador es el doble del costo de atacar un circuito los mejores planes de ataques son, en su mayoría, aquellos que combinan circuitos y generadores. Este hecho queda manifiesto para el caso en que  $M = 9$ . Si atacar un generador cuesta  $M_g = 3$ , la mejor combinación obtenida de solo tres generadores produciría un deslastre de 1112.7 MW, 39% de la carga total del sistema (ver Tabla 6), y la mejor combinación de solo líneas atacadas alcanza los 1375.57 MW de deslastre de carga, 48.3% del total de carga (ver Tabla 4). Pero si atacar generadores cuesta  $M_g = 2$ , la mejor combinación de solo 4 generadores produce un deslastre 1507.9MW

52.9% del total de la carga (ver Tabla 6), mientras que la mejor combinación que incluye circuitos y generadores alcanza un deslastre superior de 1642.29MW, 57.6% del total de la demanda (ver Tabla 5).

De los diferentes planes de ataques encontrados se observa que los elementos más impactantes para este sistema de prueba resultan ser los circuitos 11-13, 12-23, 14-16 y 15-24 y los generadores de las barras 13 y 23, los cuales se repiten con más frecuencia en los resultados obtenidos. Si se detalla la topología del sistema de prueba (ver Figura 6), se observa que el área superior contiene en su mayor proporción la generación de energía del sistema y el área inferior aloja en su mayor proporción la carga; por lo que es atractivo desconectar las dos áreas ejecutando ataques a las líneas, transformadores y generadores ubicados en las proximidades de las barras frontera entre estas áreas (barras 11, 12 y 24). Esto es lo que determina que los elementos mencionados resulten críticos para este sistema. En la Figura 3 se ilustra el plan de ataque con  $M = 6$  para los distintos ensayos en los que se modificó el costo de atacar los generadores.

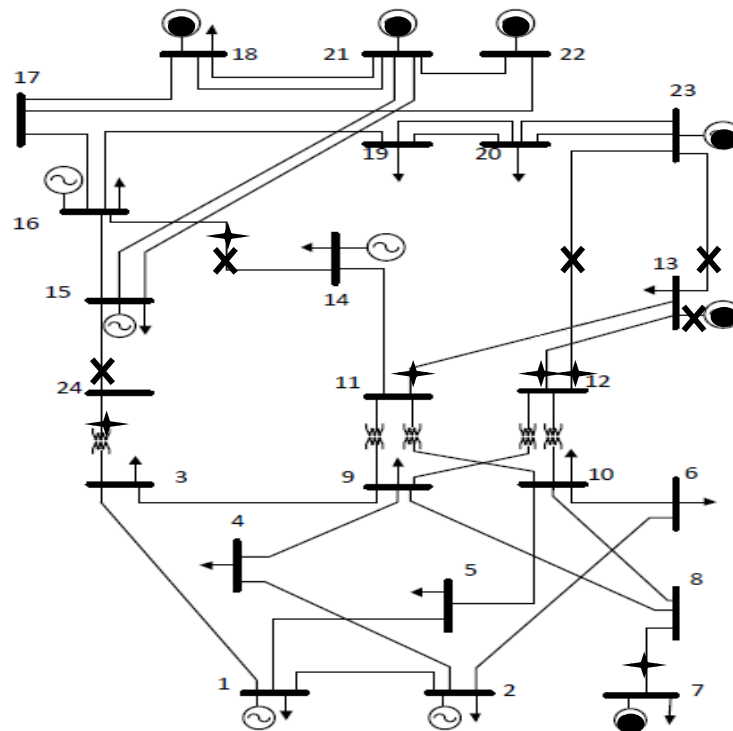


Figura 3. Resultados del problema de interdicción con  $M = 6$ .

+  $M_g = 3$ ,    X  $M_g = 2$ ,    •  $M_g = 1$

## Conclusiones

En este artículo se presentó un modelo de programación binivel que permite realizar un análisis de vulnerabilidad para encontrar los elementos más críticos de un sistema de potencia resolviendo el problema de interdicción. Como novedad de la propuesta, se resalta el hecho de que el análisis de vulnerabilidad se realiza considerando posibles ataques a las unidades de generación, en comparación con trabajos anteriores donde solo se consideran ataques a líneas y transformadores. Adicionalmente se ha modelado la red de transmisión en su versión no lineal (AC), lo cual permite encontrar soluciones más aproximadas a los valores reales de deslastre. Los ensayos y pruebas realizados en el sistema IEEE de 24 barras muestran la aplicabilidad del modelo y la efectividad de la técnica de solución implementada.

Se pudo observar que cuando atacar un generador cuesta el doble que atacar un circuito, se obtienen mayores deslastres de carga con planes de ataque mixtos (que combinan líneas y generadores) que con planes de ataque que consideran la salida de líneas o generadores solamente.

En un trabajo futuro se pueden considerar otras técnicas metaheurísticas para resolver el problema de interdicción e incluir la respuesta de la demanda como estrategia del operador de la red para reducir el deslastre de carga.

## Agradecimientos

Los autores agradecen a la Universidad de Antioquia (UdeA) por el apoyo del proyecto “Sostenibilidad 2016-2017” para el desarrollo de este trabajo.

## Referencias

- AGUDELO, L.; LOPEZ-LEZAMA J.M.; MUÑOZ, N. Análisis de Vulnerabilidad de Sistemas de Potencia mediante Programación Binivel, Revista Información Tecnológica, 2014, 25 (3): p. 103-114.
- ARROYO, J. Bilevel programming applied to power system vulnerability analysis under multiple contingencies. IET Generation, Transmission & Distribution. 2010, 4 (2): p. 178 – 190.
- ARROYO, J.; GALIANA F. On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem, IEEE Trans. Power Syst., 2005, 20 (2): p. 789 – 797.
- ARROYO, J.; FERNANDEZ, J. A Genetic Algorithm Approach for the Analysis of Electric Grid Interdiction with Line Switching, 15th International conference on Intelligent System Applications to Power Systems (ISAP), 2009, p.

1 – 6.

BROWN, G.; CARLYLE, M.; SALMERÓN J.; WOOD K. Defending Critical Infrastructure, Homeland Security: Operations Research Initiatives and Applications. Interfaces, 2006, 36 (6): p. 530 – 544.

CORREDOR, P.H.; RUIZ, M.E. Againts all Odds, IEEE Power & Energy Magazine, 2011, 9 (2): p. 59 – 66.

DELGADILLO, A.; ARROYO, J.; ALGUACIL, N. Analysis of electric grid interdiction with line switching, IEEE Transactions On Power Systems, 2010, 25 (2): p. 633 – 641.

MOTTO, A.L.; ARROYO, J.M.; GALIANA, F.D. A Mixed-Integer LP Procedure for the Analysis of Electric Grid Security Under Disruptive Threat, IEEE Transactions On Power Systems, 2005, 20 (3): p. 1357 – 1365.

RESENDE, M.G.C.; GONZÁLEZ, J. L. GRASP: Greedy Randomized Adaptive Search Procedures, Inteligencia Artificial, Revista Iberoamericana de Inteligencia Artificial, 2003, 19 (1): p. 61 – 76.

ROMERO, N.; XU, N.; NOZICK, L.; DOBSON, I. Investment Planning for Electric Power System Under Terrorist Threat, IEEE Transactions on Power Systems, 2012, 27(1): p. 108-116.

SALMERÓN, J.; WOOD, K.; BALDICK, R. Analysis of electric grid security under terrorist threat, IEEE Transactions on Power Systems, 2004, 19 (2): p. 905 – 912.

J., WOOD K., BALDICK R. Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids, IEEE Transactions on Power Systems, 2009, 24 (1): p. 96 – 104.

WONG, P.; ALBRECHT, P.; ALLAN, R.; BILLINTON, R.; CHEN, Q.; FONG, C.; HADDAD, S.; LI, W.; MUKERJI, R.; PATTON, D.; SCHNEIDER, A.; SHAHIDEHPOUR, M.; SINGH, C. The IEEE Reliability Test System – 1996, A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee, IEEE Transactions on Power Systems, 1999, 14 (3): p. 1010 – 1020.

ZIMMERMAN, R.; MURILLO, C.; THOMAS R. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education, Power System, IEEE Transactions on, 2011, 26 (1): p. 12-19.