

## **Análisis de Vulnerabilidad de Sistemas de Potencia Mediante Programación Binivel**

**Laura Agudelo<sup>(1)</sup>, Jesús M. López-Lezama<sup>(2)</sup> y Nicolás Muñoz<sup>(2)</sup>**

(1) Interconexión Eléctrica S.A. (ISA), Calle 12 Sur No. 18-168, Medellín - Colombia  
(e-mail: lyagudelo@isa.com).

(2) Grupo de Investigación GIMEL, Departamento de Ingeniería Eléctrica, Facultad de Ingeniería,  
Universidad de Antioquia, Calle 70 No. 52-21, Medellín - Colombia  
(e-mail: lezama@udea.edu.co; nicolasm@udea.edu.co).

*Recibido Dic. 16, 2013; Aceptado Ene. 13, 2014; Versión final recibida Feb. 11, 2014*

---

### **Resumen**

Este artículo presenta una nueva técnica de análisis de vulnerabilidad en sistemas de potencia bajo múltiples contingencias. El modelo bajo estudio es conocido como el "Problema del Terrorista". El principal aporte de este trabajo es la formulación y solución de la versión AC de este problema, lo que permite identificar los elementos más críticos del sistema de potencia y dar señales tempranas al operador, asociadas a la vulnerabilidad del sistema de potencia. Adicionalmente, la versión AC del modelo permite obtener resultados más realistas que la versión DC tradicional ya que considera el efecto de la potencia reactiva y los niveles de tensión en las barras del sistema. El modelo propuesto se solucionó mediante una técnica metaheurística híbrida que combina algoritmos genéticos y búsqueda local. Los resultados obtenidos utilizando el sistema de prueba IEEE RTS de 24 barras muestran la pertinencia y aplicabilidad de la metodología propuesta.

*Palabras clave: programación binivel, vulnerabilidad y seguridad de sistemas de potencia, técnicas de optimización metaheurística.*

## **Vulnerability Analysis of Power Systems using Bilevel Programming**

### **Abstract**

This paper presents a new technique for vulnerability analysis in power systems under multiple contingencies. The model under study is known as the "Terrorist Problem". The main contribution of this work is the formulation and solution of the AC version of this problem, which allows identifying the most critical elements of the power system and gives early signals to the system operator regarding the vulnerability of the system. Furthermore, the AC version of the model allows obtaining more realistic results than the traditional DC model, due to the fact that such version considers the effect of reactive power and voltage magnitudes in the system buses. The proposed model is solved by means of a hybrid metaheuristic technique that combines genetic algorithms with local search. The results obtained using the IEEE RTS – 24 bus test system show the relevance and applicability of the proposed methodology.

*Keywords: bilevel programming, power system security and vulnerability, metaheuristic optimization techniques.*

## INTRODUCCIÓN

El análisis de vulnerabilidad de sistemas de potencia está basado en el estudio de contingencias mediante el criterio N-1 ó N-2. Dicho criterio considera la salida aleatoria, de origen natural, de uno o dos elementos del sistema al mismo tiempo (Nguyen *et al.*, 2013). Sin embargo, los sistemas eléctricos de potencia pueden estar expuestos a ataques de origen intencional. El sistema eléctrico colombiano constituye un ejemplo de esta realidad. Dicho sistema ha sufrido más de 200 ataques terroristas desde el año 1999 (Corredor y Ruiz, 2011). En este sentido, en (Salmeron *et al.*, 2004) se plantea el problema de interdicción de sistemas de potencia, conocido como el “Problema del Terrorista”. Este problema consiste en un modelo matemático que considera la interacción de un agente atacante y un agente defensor. El agente atacante (en este caso el terrorista) realiza un ataque selectivo de los componentes del sistema. Sin embargo, los efectos sobre el sistema son controlados o mitigados mediante la rápida reacción y aplicación de estrategias por parte del agente defensor (en este caso el operador del sistema). Por su naturaleza, el problema de interdicción es abordado desde una perspectiva de programación binivel. En general, un modelo binivel es un problema de optimización en el que una de sus restricciones es otro problema de optimización. En este caso, el problema del agente atacante (maximizar el deslastre de carga) está sujeto a la reacción del agente defensor (minimizar el deslastre de carga). En Fig. 1 se ilustra la estructura del modelo de programación binivel aplicado al problema de interdicción en sistemas de potencia.

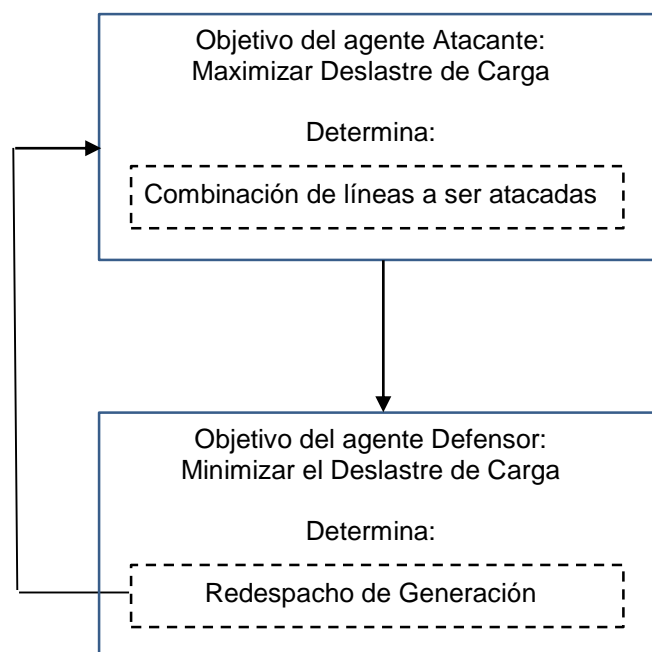


Fig. 1: Modelo Binivel de interdicción

El problema de interdicción fue formulado inicialmente en (Salmeron *et al.*, 2004) como un modelo Max-Min, en el cual el agente atacante busca maximizar los costos de generación y deslastre de carga, mientras que el agente defensor busca minimizar dichos costos. En (Arroyo y Galiana, 2005), se plantea un modelo Min-Min, en donde la función objetivo del agente atacante consiste en minimizar el número de elementos de la red a atacar, sujeto a que la demanda desatendida sea igual o mayor a un valor esperado. Este modelo de interdicción es resuelto mediante programación lineal entera mixta (PLEM), al convertir las no linealidades del nivel inferior en restricciones lineales, mediante las condiciones de optimalidad de Karush Kuhn Tucker (KKT). En (Arroyo, 2009), se plantea el problema de interdicción mediante un modelo de optimización Max-Max, donde la función objetivo del agente atacante es maximizar el deslastre de carga en el sistema. En este problema se linealizan las restricciones del nivel inferior mediante técnicas de dualidad y se plantea un problema equivalente de PLEM. En (Arroyo y Fernández, 2009), se propone un nuevo modelo de interdicción que permite definir diferentes funciones objetivo para el agente atacante y defensor. Además, dicho modelo permite incluir restricciones en el nivel superior que dependan de las variables del nivel inferior. En (Romero *et al.*, 2012), se plantea un modelo de interdicción con tres niveles de optimización, en el nivel superior se encuentra planeador del sistema, el cual determina la estrategia de inversión que debe ser adoptada para proteger el sistema, al mínimo costo de generación, deslastre de carga y reparación; en los niveles intermedio e inferior se encuentran los agentes atacante y defensor, respectivamente; este problema de optimización es solucionado usando Búsqueda Tabú para el nivel superior y búsqueda selectiva para los niveles intermedio e inferior. Otros modelos de vulnerabilidad en sistemas de potencia son

planteados en (Teng *et al.*, 2013) y (Cheng and Mili, 2013) considerando almacenamiento y fallas en cascada, respectivamente. Sin embargo, no modelan de forma explícita la interacción entre agente atacante y agente defensor.

Una característica común de los modelos de interdicción propuestos en la literatura especializada, es su desarrollo usando un modelo DC de la red de transmisión. En este trabajo se propone un nuevo planteamiento del problema, al considerar un modelo AC del sistema de potencia. La utilización de este modelo permite obtener resultados más realistas, ya que se consideran restricciones de tensión, aporte de la potencia reactiva en los nodos del sistema y las pérdidas en los elementos de la red de transmisión. El modelo de interdicción AC (MI-AC) es solucionado usando una técnica de optimización metaheurística híbrida que combina un algoritmo genético con búsqueda local.

## FORMULACIÓN MATEMÁTICA

La formulación matemática del MI-AC desarrollado en este trabajo se presenta en las ecuaciones (1)-(19). En este caso, el objetivo del agente atacante consiste en maximizar el deslastre de carga del sistema. Sin embargo, dicho agente cuenta con recursos limitados (solo puede atacar un número fijo de líneas o transformadores). Por otro lado, el agente defensor (operador de red) reacciona ejecutando un redespacho de generación que le permita minimizar el deslastre de carga, y al mismo tiempo cumplir con las restricciones de red. A continuación se explica en detalle cada uno de estos problemas.

### *Problema del agente atacante*

El problema del agente atacante está dado por las ecuaciones (1) a (3). La ecuación (1) es la función objetivo que consiste en maximizar el deslastre de carga total, expresado como la sumatoria de los racionamientos en cada uno de los nodos del sistema. Dado que el agente atacante cuenta con recursos limitados, solo puede seleccionar un número de elementos  $M$  a ser atacados. Esta limitante está dada por la ecuación (2). El estado de las líneas y transformadores del sistema se ha codificado en un vector de números binarios  $VI$  (vector de interdicción) cuya longitud es igual al número de circuitos ( $L$ ). Si un elemento del vector de interdicción tiene un valor igual a cero, significa que el circuito correspondiente (línea o transformador) está fuera de servicio (ha sido atacado), si su valor es uno, significa que el circuito correspondiente está en funcionamiento. Esta restricción está dada por la ecuación (3). Es importante resaltar que el problema del agente atacante también está sujeto a la reacción del agente defensor. Esta reacción se puede expresar mediante las ecuaciones (4) a (18) que se explican a continuación.

$$\text{Max}_{VI} \sum_{n \in N} \Delta P_n^d; \quad \forall n \in N \quad (1)$$

Sujeto a:

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

$$VI \in \{0,1\}, \quad \forall l \in L \quad (3)$$

### *Problema del agente defensor*

Dado un plan de ataque, representado por el vector de interdicción, el agente defensor del sistema debe reaccionar y minimizar el posible deslastre de carga. El objetivo del agente defensor está dado por la ecuación (4). Es importante resaltar que la ecuación (4) es exactamente contraria a la ecuación (1); sin embargo; las variables de decisión de ambos agentes son diferentes. El agente atacante tiene como variables de decisión las posiciones del vector de interdicción, es decir, decide atacar o no un elemento determinado, mientras que el agente defensor tiene como variables de decisión las relacionadas con el control del despacho de carga (decide modificar el despacho de forma óptima para minimizar el desastre de carga). La reacción del agente defensor se ha modelado como un flujo de potencia óptimo AC descrito por las ecuaciones (4) a (18).

$$\text{Min}_x \sum_{n \in N} \Delta P_n^d; \quad x = \left[ \theta, V, P^g, Q^g, P^f, \right. \\ \left. Q^f, \Delta P^d, \Delta Q^d \right] \quad (4)$$

Sujeto a:

$$P_n^g - P_n^d + \Delta P_n^d - P_n = 0; \quad \forall n \in N \quad (5)$$

$$Q_n^g - Q_n^d + \Delta Q_n^d - Q_n = 0; \quad \forall n \in N \quad (6)$$

$$P_j^{gmin} \leq P_j^g \leq P_j^{gmax}; \quad \forall j \in J \quad (7)$$

$$Q_j^{gmin} \leq Q_j^g \leq Q_j^{gmax}; \quad \forall j \in J \quad (8)$$

$$V_n^{min} \leq V_n \leq V_n^{max}; \quad \forall n \in N \quad (9)$$

$$\theta_n^{min} \leq \theta_n \leq \theta_n^{max}; \quad \forall n \in N \quad (10)$$

$$S_{lmn}^{fmin} \leq S_{lmn}^f \leq S_{lmn}^{fmax}; \quad \forall l \in L \quad (11)$$

$$S_{lmn}^2 = P_{lmn}^2 + Q_{lmn}^2; \quad \forall l \in L \quad (12)$$

$$P_n = V_n \sum_{m \in N} V_m [g_{mn} \cos(\theta_{mn}) + b_{mn} \text{sen}(\theta_{mn})]; \quad \forall n \in N \quad (13)$$

$$Q_n = V_n \sum_{m \in N} V_m [g_{mn} \text{sen}(\theta_{mn}) + b_{mn} \cos(\theta_{mn})]; \quad \forall n \in N \quad (14)$$

$$P_{lmn}^f = (VI_l) * [V_n^2 g_{mn} - V_n V_m g_{mn} \cos(\theta_{mn}) - V_n V_m b_{mn} \text{sen}(\theta_{mn})]; \quad \forall l \in L \quad (15)$$

$$Q_{lmn}^f = (VI_l) * [-V_n^2 b_{mn} + V_n V_m b_{mn} \cos(\theta_{mn}) - V_n V_m g_{mn} \text{sen}(\theta_{mn})]; \quad \forall l \in L \quad (16)$$

$$0 \leq \Delta P_n^d \leq P_n^d; \quad \forall n \in N \quad (17)$$

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

#### Variables

$VI$ : Vector de Interdicción.

$\Delta P_n^d$ : Deslastre de carga activa en el nodo  $n$ .

$\Delta Q_n^d$ : Deslastre de carga reactiva en el nodo  $n$ .

$P_{lmn}^f$ : Flujo de potencia activa por la línea  $l$  que interconecta los nodos  $m$  y  $n$ .

$Q_{lmn}^f$ : Flujo de potencia reactiva por la línea  $l$  que interconecta los nodos  $m$  y  $n$ .

$S_{lmn}^f$ : Flujo de potencia aparente por la línea  $l$  que interconecta los nodos  $m$  y  $n$ .

$\theta_n$ : Ángulo nodal de fase en el nodo  $n$ .

$V_n$ : Magnitud de la tensión en el nodo  $n$ .

$P_j^g$ : Generación de potencia activa por el generador  $j$ .

$Q_j^g$ : Generación de potencia reactiva por el generador  $j$ .

$P_n^d$ : Demanda de potencia activa en el nodo  $n$ .

$Q_n^d$ : Demanda de potencia reactiva en el nodo  $n$ .

$P_n^g$ : Generación de potencia activa en el nodo  $n$ .

$Q_n^g$ : Generación de potencia reactiva en el nodo  $n$ .

$P_n$ : Inyección de potencia activa en el nodo  $n$ .

$Q_n$ : Inyección de potencia reactiva en el nodo  $n$ .

#### Parámetros

$M$ : Número de elementos que pueden ser atacados.

$P_j^{gmin}$ : Generación mínima de potencia activa del generador  $j$ .

$P_j^{gmax}$ : Generación máxima de potencia activa del generador  $j$ .

$Q_j^{gmin}$ : Generación mínima de potencia reactiva del generador  $j$ .

$Q_j^{gmax}$ : Generación máxima de potencia reactiva del generador  $j$ .

$P_l^{fmin}$ : Flujo de Potencia activa mínima por la línea  $l$ .

$P_l^{fmax}$ : Flujo de Potencia activa máxima por la línea  $l$ .

$Q_l^{fmin}$ : Flujo de Potencia reactiva mínima por la línea  $l$ .

$Q_l^{fmax}$ : Flujo de Potencia reactiva máxima por la línea  $l$ .

$V_n^{min}$ : Magnitud de la tensión mínima en el nodo  $n$ .

$V_n^{max}$ : Magnitud de la tensión máxima en el nodo  $n$ .

$\theta_n^{min}$ : Ángulo mínimo en el nodo  $n$ .

$\theta_n^{max}$ : Ángulo máximo en el nodo  $n$ .

$S_{lmn}^{Lmin}$ : Flujo de potencia aparente mínimo por la línea  $l$  que interconecta los nodos  $m$  y  $n$

$S_{lmn}^{Lmax}$ : Flujo de potencia aparente máximo por la línea  $l$  que interconecta los nodos  $m$  y  $n$ .

$g_{mn}$ : Parte real del elemento  $mn$  de la matriz de admitancia nodal.

$b_{mn}$ : Parte imaginaria del elemento  $mn$  de la matriz de admitancia nodal.

Las restricciones (5) y (6) representan el balance de potencia activa y reactiva en cada nodo, respectivamente. Ambas expresiones tienen cuatro términos: la potencia generada, la potencia demandada, el deslastre de carga y la potencia neta calculada en el nodo. Se puede observar que la potencia generada y el deslastre de carga tienen el mismo signo. Por otro lado, también se ha tenido en cuenta en la formulación el deslastre de carga de potencia reactiva; sin embargo, por simplicidad, no se le ha asignado ningún costo. Las restricciones (7) y (8) especifican los límites mínimos y máximos de generación de potencia activa y reactiva para cada generador, respectivamente. En este caso se considera un conjunto de  $J$  generadores. La restricción (9) está asociada con los límites mínimos y máximos de la magnitud de la tensión. Para cada uno de los  $N$  nodos del sistema la solución del problema debe garantizar que las tensiones se encuentran dentro de los límites permitidos por la regulación (normalmente entre 0.95 y 1.05 p.u.). La restricción (10) especifica los límites mínimos y máximos de los ángulos en cada nodo. Estos límites especifican el grado de libertad de las diferencias angulares entre las barras del sistema. Las restricciones (11) y (12) corresponden a los límites técnicos de flujo de potencia aparente por los circuitos. Para que la solución del problema sea factible (y segura) se debe garantizar que no existan sobrecargas en los circuitos que todavía están funcionando después del ataque. Las restricciones (13) y (14) representan las expresiones matemáticas de las inyecciones de potencia activa y reactiva, respectivamente. Estas expresiones son función de las tensiones, los ángulos y los parámetros de la matriz de admitancia nodal. Note que estas expresiones corresponden al último término que se utiliza en las ecuaciones (1) y (2) para los balances de potencia activa y reactiva, respectivamente. Las restricciones (15) y (16) corresponden a las expresiones matemáticas que describen los flujos de potencia activa y reactiva en un circuito, respectivamente. Nótese que en este caso se han multiplicado dichas expresiones por el valor correspondiente del vector de interdicción, de esta forma solo habrá flujo de potencia en los circuitos que estén en funcionamiento (que no hayan sido atacados). Finalmente, las restricciones (17) y (18) limitan el deslastre de carga activa y reactiva en cada nodo, el cual no puede ser mayor a la carga total del sistema.

## ALGORITMO HÍBRIDO

El modelo propuesto en (1)-(18) corresponde a un problema de programación no lineal entero mixto. Para este tipo de problemas la aplicación de técnicas matemáticas convencionales no garantiza la obtención del óptimo global (Anaut et. al., 2009), (Catalao et. al., 2006). Por este motivo se ha optado por la aplicación de una técnica metaheurística híbrida. El algoritmo híbrido propuesto consiste en la combinación de un Algoritmo Genético con Búsqueda Local. En la Fig. 2 se ilustra el diagrama de flujo del algoritmo implementado.

### Población inicial

La población inicial se genera de forma aleatoria. Cada individuo corresponde a un vector de interdicción ( $V$ ) y representa una estrategia de ataque del terrorista. Como se mencionó anteriormente, la longitud del vector corresponde al número de elementos del sistema. Si el valor de una posición es cero significa que este elemento ha sido atacado. Si el valor de una posición es uno, significa que el elemento correspondiente se encuentra en funcionamiento.

### Evaluación del desempeño

En este caso se debe calcular el racionamiento para cada uno de los planes de ataque generados en el

paso anterior. Desde el punto de vista del agente atacante, el plan de ataque con mejor desempeño es aquel que resulte en mayor racionamiento. Para calcular el racionamiento que genera un plan de ataque en particular, es necesario considerar la reacción del agente defensor. En este caso se debe resolver el problema de optimización dado por las ecuaciones (4)-(18). Para resolver este problema se utilizó el software Matpower (Zimmerman, et al., 2011), el cual permite realizar el cálculo del flujo de potencia óptimo y determinar el racionamiento ocasionado por un plan de ataque en particular.

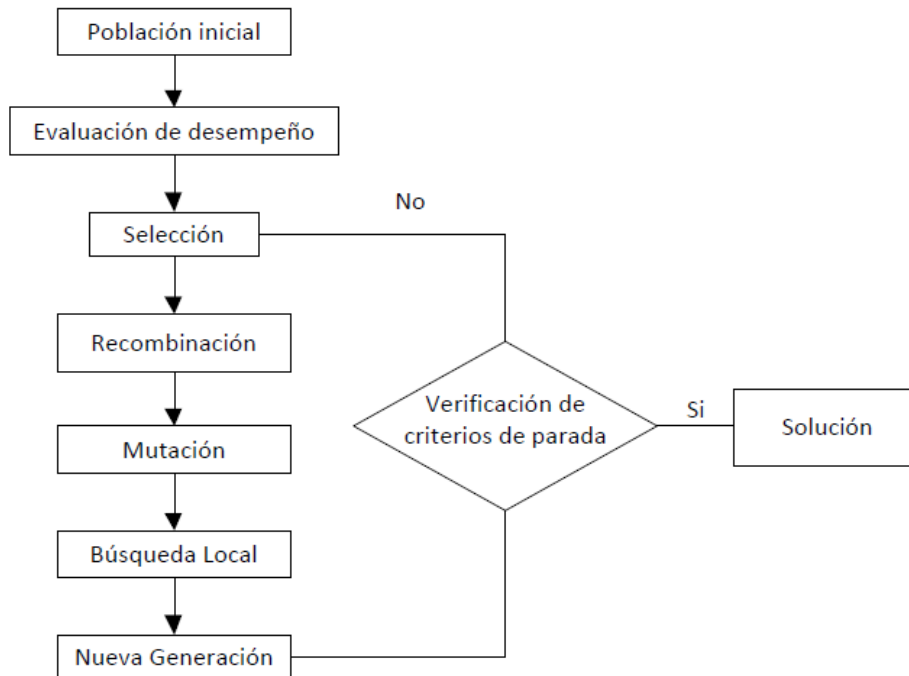


Fig. 2: Diagrama de flujo del Algoritmo Híbrido

### *Selección*

Una vez se conocen los racionamientos producidos por cada uno de los planes de ataque se debe escoger entre los mejores para generar nuevas posibles soluciones. Para la Selección se aplicó el torneo binario, el cual consiste en seleccionar aleatoriamente dos parejas y escoger el individuo de mejor desempeño. En este caso se realizan tantos torneos como número de individuos haya. Los mejores individuos (planes de ataque con mayor impacto), pasan a la fase de recombinación.

### *Recombinación*

La recombinación es la fase del algoritmo genético en el que los individuos intercambian su material genético para generar nuevos individuos. En este caso se selecciona aleatoriamente un punto del vector de interdicción y se intercambian las cadenas de bits de los planes de ataque obtenidos en la etapa anterior, generando dos nuevos individuos. Los nuevos individuos comparten el material genético de sus padres y probablemente representen planes de ataque con mejor desempeño.

### *Mutación*

La Mutación consiste en alterar, con una probabilidad dada, un elemento del vector de interdicción. Este paso permite, eventualmente, escapar de óptimos locales y le imprime al algoritmo más diversificación entre sus individuos. Una vez se lleve a cabo la mutación se debe evaluar nuevamente la función objetivo de los planes de ataque que hayan sido modificados en esta fase.

### *Búsqueda Local*

Para la Búsqueda Local se selecciona el mejor individuo de la población actual y se realiza una exploración del vecindario del vector de interdicción. El vecindario se define cambiando un elemento de estado a la vez. Si el individuo vecino tiene mejor desempeño, se incluye en la nueva población y se reemplaza por el individuo anterior.

*Criterio de parada*

Existen básicamente dos criterios de parada: el número total de iteraciones o un número máximo de iteraciones sin que se haya encontrado una mejora en los individuos. Si se cumple cualquiera de estos dos criterios, el algoritmo para y entrega la mejor solución encontrada.

**PRUEBAS Y RESULTADOS**

Para probar la validez del modelo propuesto se realizaron varias simulaciones usando el sistema de prueba IEEE RTS-24 (Grigg *at al.*, 1999). Este sistema cuenta con 24 barras, 38 líneas, 32 generadores y 17 cargas. Se realizaron pruebas para escenarios de demanda máxima, media y mínima. La demanda máxima corresponde al perfil de carga de un día de invierno a las 18 horas y demanda total de 2850 MW. Para el escenario de demanda media se tomó como referencia un día de invierno a las 21 horas con carga de 2365 MW y para el escenario de demanda mínima, se usó el perfil de carga de un día de verano a las 5 horas con 1653 MW. Las impedancias de línea se tomaron con una base de 100 MVA. Se asumió que todos los generadores tienen potencia mínima de generación de 0 MW.

En todos los nodos de carga del sistema se modeló generación ficticia activa y reactiva para cuantificar el deslastre de carga, a los generadores ficticios se les asignó un costo 10 veces el costo de los generadores reales, a fin de garantizar que fuera el último recurso despachado para suplir la demanda de su propio nodo. Para tener en cuenta las restricciones de magnitud de tensión se consideraron límites mínimos y máximos de 0.9 y 1.05 p.u, respectivamente en todas las barras.

*Racionamiento variando el número de circuitos atacados*

Para cada uno de los tres escenarios de carga (mínima media y máxima) se realizaron pruebas al modelo variando el número de circuitos atacados simultáneamente. Como era de esperarse, al aumentar el número de circuitos atacados de forma simultánea, se registran mayores racionamientos. Adicionalmente, la demanda no atendida es mayor cuando el ataque se realiza en el escenario de carga máxima, lo que significa que el sistema es más vulnerable en las horas pico. En la Tabla 1 se ilustran los resultados obtenidos. Se puede observar que para producir el máximo daño al sistema atacando dos elementos de forma simultánea, se deberían seleccionar los circuitos 11-14 y 14-16. Por otro lado, para causar máximo daño al sistema, atacando tres elementos al mismo tiempo, estos deberían ser: la línea 16-19 y el corredor de doble línea 20-23. De forma análoga, en la Tabla 1 se ilustran los resultados para 5 y 6 circuitos atacados simultáneamente. Se encontró que para los casos 2, 3, 5 y 6 hay una combinación única de circuitos que causa el máximo daño en cualquiera de los tres escenarios de carga. Por otro lado, para el caso de 4 elementos atacados simultáneamente los circuitos que causan el máximo daño son diferentes dependiendo del nivel de carga, como se ilustra en la Tabla 2. En este caso, en el escenario de mínima demanda, el máximo daño se presenta con la salida de los circuitos que llegan a los nodos 7 y 14, ocasionado pérdida total de la carga en tales nodos (194.7 MW), lo cual corresponde al 11.8% de la demanda total. En los escenarios de demanda media y máxima el mayor deslastre corresponde, respectivamente, al 10.98% y 18.47% del total de la carga del sistema.

Tabla 1: Resultados del MI-AC para diferentes escenarios de demanda

CASO	Circuitos	Deslastre en diferentes escenarios (MW)		
		Carga Mínima	Carga Media	Carga Máxima
2	11-14, 14-16	114.46	161	194
3	16-19, 20-23, 20-23	182.31	256.47	309
5	3-24, 9-12, 10-12, 11-13, 14-16	279.52	612.88	850.03
6	3-24, 7-8, 9-12, 10-12, 11-13, 14-16	449.38	783.34	1020.51

Tabla 2: Resultados del MI-AC en diferentes escenarios con cuatro circuitos atacados

CASO	Deslaste (MW)	Circuitos
Mínima	194.7	2-7, 7-10, 11-14, 16-14
Media	256.47	15-24, 16-19, 20-23, 20-23
Máxima	531.35	3-24, 12-23, 13-23, 14-16

En Fig 3 se ilustra las cuatro líneas atacadas simultáneamente para los tres escenarios de demanda (ver Tabla 2). La equis corresponde al escenario de demanda mínima, el círculo a demanda media y el triángulo a la demanda máxima. En general, el escenario más crítico en cuanto a pérdida de carga corresponde al perfil de carga máxima, al presentarse el mayor deslaste de carga para todos los casos.

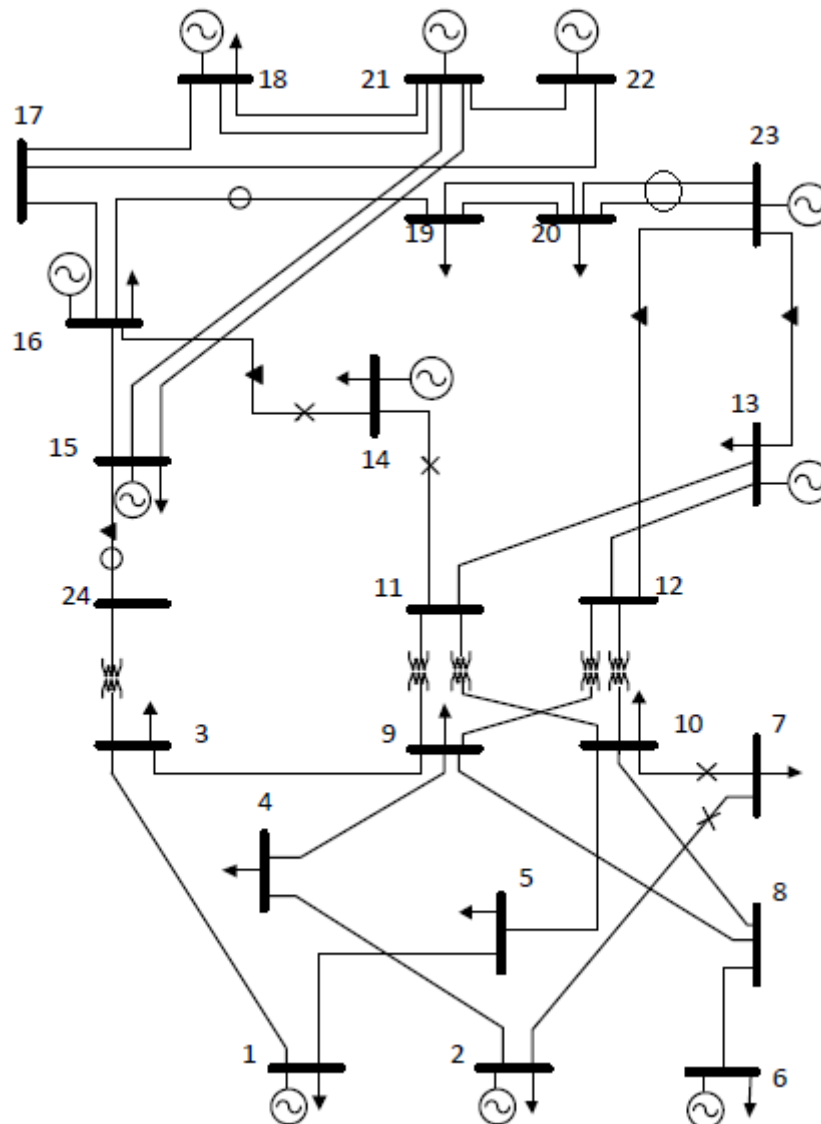


Fig 3: Resultados del MI-AC en diferentes escenarios con cuatro circuitos atacados

#### Comparación de resultados

En la Tabla 3 se comparan los resultados de este trabajo con los reportados en (Arroyo, 2009). Se puede observar que el modelo de interdicción DC (MI-DC) presentado en (Arroyo, 2009) arroja valores más conservadores respecto al deslaste de carga. Por otro lado, en ambos modelos se identifican los mismos



circuitos críticos. La diferencia en deslastre de carga de debe a que el modelo AC considera el aporte de potencia reactiva en los nodos y las pérdidas en los elementos de la red. En lo referente a tiempos de cálculo, el modelo DC es más rápido debido a la simplificación de las ecuaciones de flujo de carga. En (Arroyo, 2009) se reportan tiempos de cálculo que varían de algunos segundos a pocos minutos, dependiendo del número de circuitos a ser atacados simultáneamente y del tipo de método utilizado para abordar el problema de optimización del nivel inferior (condiciones de optimalidad o dualidad). El modelo AC reportado en este artículo requiere tiempos de cálculo que varían entre 1 y 2 horas (dependiendo del número de circuitos a ser atacados). Vale la pena mencionar que el principal aporte del modelo propuesto no radica en su rapidez. Las ventajas del modelo AC propuesto radican en obtener resultados más realistas y en la posibilidad de identificar diferentes planes de ataque. Mientras los modelos tradicionales identifican un único plan de ataque óptimo, la metodología utilizada para solucionar el modelo AC propuesto permite identificar múltiples planes de ataque (puede identificar óptimos locales), que pueden causar daño al sistema en menor magnitud, pero que podrían ser ignorados por el operador del sistema. En la Tabla 4 se presenta una lista de posibles planes de ataque que pueden causar daño al sistema, en orden de magnitud. Para este caso se han considerado 4 líneas bajo ataque y el escenario de carga máxima. En la primera fila se presenta el plan de ataque más crítico que causaría un racionamiento de 531.35 MW. A partir de este valor se presentan otros planes de ataque que pueden causar daño al sistema en menor medida, pero que involucran otros circuitos.

Tabla 3: Comparación de resultados del MI-DC y MI-AC para el caso IEEE RTS-24.

Circuitos	Deslastre (MW) Modelo DC	Deslastre (MW) Modelo AC
11-14, 14-16	194	194
3-24, 12-23, 13-23, 14-16	516	531.35
3-24, 7-8, 9-12, 10-12, 11-13, 14-16	1017	1023.41

Tabla 4: Resultados del MI-AC para el caso IEEE RTS-24 con cuatro líneas atacadas.

Deslastre (MW)	Circuitos
531.35	3-24, 13-23, 14-16, 15-16
372.36	11-13, 12-13, 12-23, 15-24
370.18	1-3, 9-11, 9-12, 15-24
233.18	11-14, 13-23, 14-16, 15-24
216.61	3-9, 7-8, 9-11, 15-24

Como se mencionó anteriormente, una de las ventajas del modelo AC es que considera restricciones de límites de magnitud de tensión. Esto puede hacer que en algunos casos los resultados con respecto al modelo DC sean significativamente diferentes. Para ilustrar este fenómeno en la Tabla 5 se presenta un análisis de sensibilidad de tensión en la barra 3 del MI-AC, con respecto a la demanda no atendida en ese nodo ante la salida simultánea de cinco circuitos: 11-13, 11-14, 12-13, 12-23, 3-24. Los resultados son comparados con el MI-DC presentado en (Arroyo, 2009), el cual no considera el efecto de la potencia reactiva y por lo tanto, presenta menor deslastre de carga. A medida que se incrementa el límite mínimo de tensión en el nodo 3, se aumenta considerablemente el deslastre de carga en este nodo. Observe que inclusive para el caso en que se considera una tensión mínima de 0.9 p.u las diferencias entre los resultados de ambos modelos son significativas. En este caso, el modelo DC indica que el racionamiento en el nodo 3 es de 87.2 MW, mientras en realidad el racionamiento sería de 156 MW debido a la restricción de tensión. Cuando se hace más fuerte esta restricción (1.0 p.u) el racionamiento calculado usando el modelo AC aumenta a 309 MW, por otro lado, el racionamiento calculado usando el modelo DC siempre será igual a 87.2 MW ya que considera un perfil de tensiones ideal.

Tabla 5: Análisis de sensibilidad de tensión en nodo 3 para 5 líneas atacadas.

Circuitos: 11-13,11-14,12-13,12-23,3-24	Modelo AC					Modelo DC
Tensión Nodo 3 (P.U.)	0.9	0.93	0.95	0.98	1.0	1.0
Deslastre en el Nodo 3 (MW)	156	198	238	282	309	87.2

En Fig. 4 se ilustra el diagrama IEEE RTS – 24 con el ataque de cinco líneas, marcadas con equis, considerando el escenario de demanda máxima (ver Tabla 5). Esta nueva topología implica un esfuerzo importante en los nodos 3 y 10 por mantener las tensiones luego de quedar separados los sistemas de 230 kV y 138 kV. Este esquema de ataque hace que los nodos 3 y 10 queden alejados de la generación (nodos 1, 2 y 6), obligándolos a operar cerca de 0.9 p.u. y causando racionamiento por tensiones.

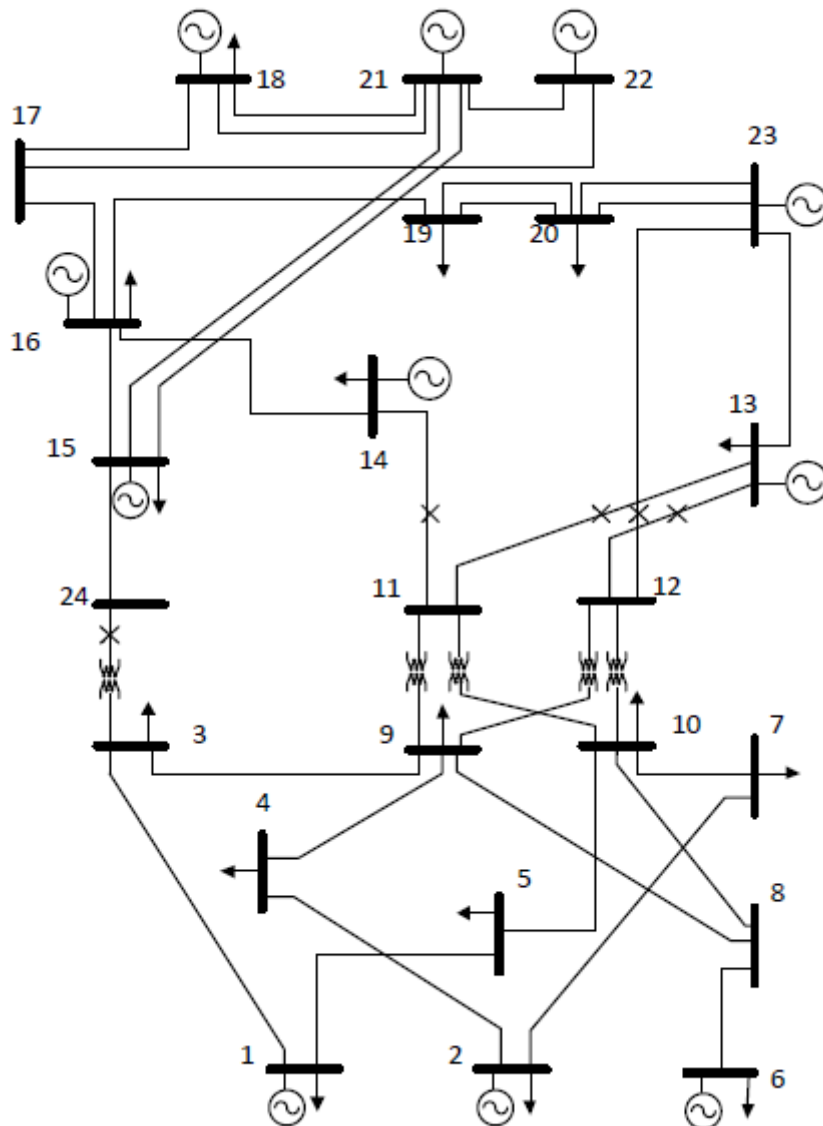


Fig. 4: Diagrama de prueba IEEE RTS-24 con 5 líneas atacadas

**CONCLUSIONES**

Este artículo presentó un nuevo modelo de análisis de confiabilidad bajo múltiples contingencias. El principal aporte consiste en la utilización de un modelo AC de la red de transmisión y el uso de un algoritmo híbrido para su solución. Para todos los casos simulados con el MI-AC fue posible encontrar una solución óptima y comparar los resultados con los reportados mediante un MI-DC. La utilización de un modelo AC permite

obtener resultados más cercanos a la realidad, ya que es posible modelar las restricciones de tensión en los nodos del sistema. Esto permite al operador realizar acciones preventivas, como traslados de carga y manejo de reactivos en la red, a fin de evitar un racionamiento por bajas tensiones en los nodos. El análisis de vulnerabilidad bajo múltiples contingencias presentado en este artículo, entrega al operador de red la combinación de líneas, que ante su salida, genera el mayor impacto sobre el sistema, cuantificado en deslastre de carga. Además, dado que se utiliza un método poblacional, es posible obtener no solo una solución sino un conjunto de soluciones con características similares (un conjunto de contingencias críticas para el sistema, pero con menor pérdida de carga).

La metodología propuesta en este artículo, puede ser usada como una herramienta preventiva que permita al operador de red identificar las líneas más críticas o áreas más vulnerables del sistema, evaluar el riesgo asociado a la operación y confrontar esta información con zonas en conflicto, equipos con baja confiabilidad, equipos en mantenimiento, equipos operando cerca a límites técnicos, cargas esenciales o estratégicas, condiciones climáticas desfavorables, entre otras, y tomar acciones tempranas para la operación.

## AGRADECIMIENTOS

Los autores agradecen a la Universidad de Antioquia (UdeA) por el apoyo del proyecto “Sostenibilidad 2013-2014”.

## REFERENCIAS

Anaut, D., Di Mauro, G., Meschino, G., y Suarez, J., *Optimización de Redes Eléctricas Mediante la Aplicación de Algoritmos Genéticos*, Revista Inf. Tecnol. Cit: 20(4), 137-148 (2009).

Arroyo J., y Galiana F., *On the Solution of the Bilevel Programming Formulation of the Terrorist Threat Problem*, IEEE Trans. Power Syst.: 20 (2), 789-797 (2005).

Arroyo J., *Bilevel programming applied to power system vulnerability analysis under multiple contingencies*, IET Generation, Transmission & Distribution: 4(2), 178-190 (2009).

Arroyo J., y 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), Curitiba, Brazil, Nov. (2009).

Catalao, J., Mariano, S., Mendes V., y Ferreira, L., *Planificación de la Operación de Corto Plazo de Sistemas de Energía Hidroeléctrica*, Revista Inf. Tecnol. Cit: 20(3), 149-155 (2006).

Cheng Q., and Mili L., *Composite power system vulnerability evaluation to cascading failures using importance sampling and antithetic variates*, IEEE Transactions on Power Systems: 28(3), 2321-2330 (2013).

Corredor P., y Ruiz M., *Against all Odds*, IEEE Power & Energy Magazine: 9(2), 59-66 (2011).

Grigg C., Wong P., Albrecht P., Allan R., Bhavaraju M., Billinton R., Chen Q., Fong C., Haddat S., Kuruganty S., Li W., Mukerji R., Patton D., Rau N., Reppen D., Schneider A., Shahidehpour M., and 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 Trans. Power Syst.: 14(3), 1010–1020 (1999).

Nguyen D.T., Shen Y., and Thai, M.T., *Detecting critical nodes in interdependent power networks for vulnerability assessment*, IEE Transactions on Smart Grids: 4(1), 151-159 (2013).

Romero N., Xu N., Nozick L., y Dobson I., *Investment planning for electric power system under terrorist threat*, IEEE Trans. Power Syst.: 27(1), 108-116 (2012).

Salmeron J., Wood K. y Baldick R., *Analysis of electric grid security under terrorist threat*, IEEE Trans. Power Syst.: 19(2), 905–912 (2004).

Teng J.H., Chen C.Y., y Martinez I.C., *Utilizing energy storage systems to mitigate power system vulnerability*, IET Generation Transmission and Distribution: 7(7), 790-798 (2013).

Zimmerman R., Murillo C., y Thomas R., *Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education*, IEEE Trans. Power Syst.: 26 (1), 12-19 (2011).

