1-1-2006

Estudio y aplicación de nuevas metodologías para el análisis de la vulnerabilidad de los sistemas de potencia

Andrés Felipe Leal Quintero
Universidad de La Salle, Bogotá

Diana Lorena Sandoval Nino
Universidad de La Salle, Bogotá

ESTUDIO Y APLICACIÓN DE NUEVAS METODOLOGÍAS PARA EL ANÁLISIS DE LA VULNERABILIDAD DE LOS SISTEMAS DE POTENCIA

ANDRÉS FELIPE LEAL QUINTERO
DIANA LORENA SANDOVAL NIÑO

UNIVERSIDAD DE LA SALLE
FACULTAD DE INGENIERÍA ELÉCTRICA
BOGOTÁ
2006

ESTUDIO Y APLICACIÓN DE NUEVAS METODOLOGÍAS PARA EL ANÁLISIS DE LA VULNERABILIDAD DE LOS SISTEMAS DE POTENCIA

ANDRÉS FELIPE LEAL QUINTERO
DIANA LORENA SANDOVAL NIÑO

Proyecto de grado para optar por el título de Ingeniero Electricista

Director, Dr.-Ing. Camilo Andrés Cortés
Profesor Asociado Universidad de La Salle

UNIVERSIDAD DE LA SALLE
FACULTAD DE INGENIERÍA ELÉCTRICA
BOGOTÁ
2006

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá (30 de octubre de 2006)

AGRADECIMIENTOS

Primeramente queremos darle gracias a nuestros padres, profesores, compañeros y a todas las personas que nos facilitaron el poder concluir nuestros estudios profesionales.

También queremos expresar nuestro agradecimiento a nuestro director, que más que un profesor ha sido un amigo, que ha tenido la paciencia para guiar esta investigación. Gracias porque siempre tuvo palabras de aliento cuando teníamos vacilaciones.

Gracias a dos maravillosas personas Patricia Leal y Juan Urrego, por ayudarnos a concluir este proyecto, por tomarse el tiempo para revisarlo a pesar de todo el trabajo que tenían y por sus valiosos comentarios.

CONTENIDO

pág

LISTA DE TABLAS

pág

LISTA DE FIGURAS

pág

LISTA DE ANEXOS

pág

INTRODUCCIÓN

En el mundo se le había dado poca importancia al tema de la vulnerabilidad de los sistemas de potencia frente a un posible ataque por parte de un grupo terrorista; pero tras los atentados del 11 de septiembre de 2001 los estadounidenses vieron la necesidad de proteger los sistemas eléctricos ante cualquier eventualidad ya sea natural o intencional, razón por la cual, actualmente se están estudiando e investigando nuevos métodos en diferentes países para el análisis de la vulnerabilidad de los sistemas de potencia frente a los ataques terroristas. Una de estas metodologías se comenzó a desarrollar en la escuela naval de postgrados de Monterrey California (USA), con el nombre de proyecto VEGA 1.0 (Vulnerability of Electric Power Grids Analysis Project) a cargo de Javier Salmerón, Kevin Wood y Ross Baldick.

VEGA 1.0 es un proyecto que propone una serie de algoritmos y modelos matemáticos para hallar los puntos más vulnerables en el sistema eléctrico ante un ataque dirigido hacia cualquiera de sus componentes (centrales de generación, líneas de transmisión, transformadores, redes de distribución, etc.) y busca identificar las falencias en el diseño de los sistemas eléctricos para hacerlos más robustos. Esta metodología hace un análisis de **estado estacionario** del sistema y no analiza la vulnerabilidad del sistema desde punto de vista de la estabilidad.

Por otra parte, para nadie es un secreto que en Colombia se están viviendo tiempos muy difíciles en materia de orden público y que los ataques contra la infraestructura eléctrica son cada vez más frecuentes. Cabe anotar que en Colombia también se están desarrollando metodologías para el análisis de la vulnerabilidad de los sistemas de potencia ante cualquier ataque terrorista, sin embargo, este trabajo toma como punto de partida el proyecto VEGA 1.0 ya que esta metodología no se ha analizado en la Facultad de Ingeniería Eléctrica de Universidad de La Salle y tampoco en Colombia.

El objetivo general de esta investigación es hacer un estudio riguroso de la metodología propuesta en el proyecto Vega 1.0 con la finalidad de determinar su posible aplicabilidad en el sistema eléctrico colombiano y hacer aportes que fortalezcan esta metodología.

Para facilitar el análisis de la metodología del proyecto VEGA 1.0 se hicieron tablas comparativas de sus dos niveles, así como un diagrama de flujo del algoritmo de interdicción[1].

Se hace una serie de simulaciones aplicando esta metodología a un sistema de prueba de confiabilidad de la IEEE denominado RTS-96 [8] utilizando la herramienta computacional que de simulación MATLAB[2], en la cual se creó un modesto toolbox para hacer el análisis de vulnerabilidad llamado AVSP. Posteriormente se realizó el análisis de la vulnerabilidad del sistema para comparar los resultados obtenidos con los resultados expuestos en el artículo: *"Analysis of Electric Grid Security Under Terrorist Threat"* [2].

Tras verificar el buen funcionamiento de la herramienta desarrollada se realiza una simulación en un sistema pequeño propuesto llamado *Salle-06*, diseñado para poder analizar las implicaciones de considerar la desconexión de generadores conectados directamente a subestaciones atacadas. Esta es una **modificación** propuesta al modelo original de VEGA 1.0, mostrada en la sección 2.1.2 de esta monografía.

Finalmente se propone una extensión de la metodología con el fin de considerar la necesidad de protección del sistema frente a ataques terroristas, mediante un recurso destinado para ello, utilizándolo de forma óptima.

Esta investigación propone también unos lineamientos para orientar la forma en que se puede seguir desarrollando el tema del análisis de vulnerabilidad para trabajos futuros en esta Facultad, así como las consideraciones pertinentes para la implementación de la metodología en el sistema eléctrico colombiano.

[1] Interdicción es un ataque o conjuntos de ataques coordinados contra la infraestructura de un sistema eléctrico, esta palabra también toma forma de verbo y de adjetivo. Por ejemplo: el componente *x* fue interdicto, es decir, salió de operación por causa de un ataque.
[2] Optimization ToolBox 3.1 of Matlab [3].

1. METODOLOGÍAS PARA EL ANÁLISIS DE LA VULNERABILIDAD DE LOS SISTEMAS DE POTENCIA ANTE UN EVENTUAL ATAQUE

Los sistemas de potencia siempre poseen cierta vulnerabilidad frente a diferentes factores, ya sean internos o externos; por esta razón se busca protegerlos cada vez más ante cualquier eventualidad. Desde hace unos 10 años aproximadamente, el terrorismo ha afectado directamente los sistemas eléctricos de varios países alrededor del mundo afectando la economía, la política, el desarrollo y la calidad de vida de muchas personas.

Actualmente se están desarrollando nuevas metodologías para mitigar los efectos que trae un ataque en el funcionamiento de un sistema eléctrico, pero además de esto se está analizando qué tan vulnerable es un sistema frente a diferentes panoramas de ataque, y de esta manera definir qué componentes son más críticas.

En Colombia el sistema eléctrico se ve afectado por la intervención de ataques en las torres de transmisión, aunque existe un recurso de protección por medio de las fuerzas militares. Los efectos de estas acciones siguen siendo una gran preocupación para el funcionamiento satisfactorio del sistema.

El análisis de diferentes panoramas de ataques de un sistema eléctrico en cualquier parte del mundo, es un paso para estudiar nuevos diseños de componentes e infraestructuras que hagan más resistente el sistema, ya sea ante un ataque directo o indirecto.

En este capítulo se hace un breve resumen de algunas metodologías que se están desarrollando en el mundo para el análisis de la vulnerabilidad de los sistemas de potencia ante un eventual ataque.

1.1. CLASIFICACIÓN JERÁRQUICA DE CONTINGENCIAS RESULTADAS DEL TERRORISMO UTILIZANDO REDES BAYESIANAS

Esta metodología es desarrollada en la Universidad de los Andes (Colombia) y el Instituto Politécnico Nacional de Grenoble (Francia), por los autores Carolina Tranchita, Nouredine Hadjsaid y Álvaro Torres [10]-[13].

Ellos introducen una técnica para determinar el ataque más disruptivo por medio de la modelación de los ataques a través de redes Bayesianas[3]; una vez obtenido el ataque más grave se hace un estudio de la seguridad estática por medio de lógica difusa.

El método propuesto está dividido en dos partes, donde la primera es el desarrollo de la red Bayesiana y la segunda es alinear las contingencias del ataque por medio del cálculo del riesgo y los rasgos del panorama debidos al ataque, teniendo en cuenta la ubicación geográfica de cada una de las componentes del sistema y de todo el sistema en general.

Aunque está basada bajo el marco sociopolítico colombiano, también es propuesta para ser aplicada en los sistemas eléctricos europeos; pues una ventaja que tiene esta metodología es que calcula el riesgo para cada contingencia y de esta manera se pueda disminuir el número de panoramas posibles para elegir el más disruptivo, con el fin de estudiarlo más a fondo. Igualmente obtiene la probabilidad de ocurrencia de una contingencia para poder hacer un análisis probabilístico de la seguridad del sistema, es decir, hacer un ranking de contingencias para tomar la más disruptiva.

Para la construcción de la red Bayesiana se tienen en cuenta diferentes aspectos del sistema:

- Súper componentes del sistema. Se llaman así a los generadores, las subestaciones y las líneas de transmisión, gracias a su dimensión y trascendencia en el sistema.

- Evento. Es el fenómeno de incertidumbre de ocurrencia de un ataque, ya que los ataques dependen de la voluntad humana.

- Probabilidad de Ataque. Se refiere a qué tan factible sea un ataque en cierta componente del sistema.

- Eventos que no se toman en cuenta, es decir, sólo una súper componente puede ser atacada en un momento.

- Eventos colectivos, es decir, pueden ocurrir varios eventos a la vez.

[3] Es un modelo probabilístico multivariado que relaciona un conjunto de variables aleatorias mediante un grafo dirigido, el cual indica explícitamente influencia causal. Gracias a su motor de actualización de probabilidades, el Teorema de Bayes, las redes bayesianas son una herramienta extremadamente útil en la estimación de probabilidades ante nuevas evidencias [19].

Las variables que considera la red Bayesiana, son las siguientes:

- Situación política en la que se encuentra el país.
- Posición del grupo atacante. Es la posición del grupo terrorista en un país dado. Se califica teniendo en cuenta el grado social y territorial de control del atacante.
- Qué tan crítico es el sistema. Esta variable se refiere a qué tan crítico es el sistema de energía para la indisponibilidad forzada de una súper componente dada.
- Localización geográfica de las componentes del sistema.
- Protección física de las componentes del sistema.
- Intensidad del ataque en una súper componente del sistema. Las variables para deducir la intensidad del ataque en una súper componente son la motivación del ataque, el fácil acceso y el tipo de súper componente.
- Severidad del ataque. La consecuencia del ataque se deduce de la intensidad del ataque y de qué tan crítico es el sistema ante la ausencia de una de sus componentes. Un acercamiento para cuantificar la severidad es el número de los componentes afectados por el ataque. Algunas variables a considerar que se pueden agregar a la red Bayesiana para determinar la severidad del ataque son: que el ataque afecte la estabilidad nacional del sistema, los costos económicos de los daños del sistema, los costos económicos de indisponibilidad de la fuente, la seguridad física y las consecuencias para el medio ambiente. Para simplificar la red, se utiliza solamente el acercamiento del número de componentes afectados.

Como se pudo ver anteriormente, la metodología tiene en cuenta tanto las condiciones del sistema como las condiciones del atacante y sus recursos.

La evaluación de la seguridad de la infraestructura eléctrica bajo un ataque terrorista permite determinar la seguridad del sistema con respecto a la posibilidad de actos terroristas y a las incertidumbres asociadas con la carga y la generación.

La incertidumbre en los actos terroristas se considera por la teoría de la probabilidad subjetiva y el grupo de contingencias bajo estudio se obtiene a través de una red Bayesiana. El método se valida en un sistema de prueba, tomando

como ejemplo las condiciones del terrorismo sobre la infraestructura eléctrica colombiana.

El modelo propuesto define la seguridad frente a un acontecimiento terrorista, ya sea directo o indirecto, el modelo consiste en una serie de pasos para evaluación de la seguridad del sistema.

Esta metodología propone una clasificación de acontecimientos y estados de operación para determinar la incertidumbre que genera cada acontecimiento en la seguridad del sistema.

1.1.1. Clasificación de acontecimientos y estados de operación del sistema considerando el terrorismo en el análisis de seguridad [11].

En este trabajo (Tranchita et al) se analizó que la seguridad de un sistema eléctrico es la capacidad que tiene el mismo para soportar pérdidas o la falta de alguna de sus componentes. La metodología hace un estudio de las posibles causas y consecuencias de las contingencias a las cuales está expuesto el sistema.

El tratamiento apropiado de la incertidumbre para las causas y las consecuencias de perturbaciones ayuda a encontrar un límite óptimo entre los recursos del atacante y la confiabilidad de operación del sistema. Por lo tanto es necesario saber los acontecimientos a los cuales se expone el sistema, teniendo en cuenta que cualquier amenaza, ya sea verbal, es considerada como un hecho o fenómeno de la ocurrencia incierta que afecta el funcionamiento normal del sistema.

En la tabla 1.1 se reproduce la clasificación de las causas que hacen que falle el sistema y una clasificación de las consecuencias de las fallas sobre el sistema. Esta clasificación es uno de los puntos clave de la metodología de [10] porque ayuda a centralizar el estudio de la protección del sistema dependiendo de su procedencia: si es natural o no natural, externa o interna, intencional o no intencional, etc.

1.2. USO DE MÉTODOS DE GRAFOS PARA EL ANÁLISIS DE LA VULNERABILIDAD DE LAS REDES DE ENERGÍA ELÉCTRICA

En esta metodología se modelan las redes de energía eléctrica como grafos, y se conduce al estudio de dos redes de transmisión de energía de los estados nórdicos y occidentales de Estados Unidos [14] y [15].

Utilizando como herramienta matemática la teoría de grafos se calculan los valores de cada una de las características topológicas de las redes (estructurales) y se compara su error. Luego se hace un ataque en la tolerancia de las redes (vulnerabilidad estructural), es decir, su funcionamiento cuando se remueve una componente.

Además, realiza un análisis estructural de la vulnerabilidad de una red eléctrica ficticia con una estructura simple. En este análisis, el contraste de las diversas estrategias para disminuir la vulnerabilidad del sistema se evalúa; finalmente, presenta un planteamiento sobre la aplicabilidad práctica de modelamiento con grafos.

Aunque esta metodología no tiene en cuenta el flujo de potencia de las redes cuando ocurre el ataque, es una forma más sencilla de analizar la vulnerabilidad de un sistema eléctrico. Sin embargo es necesario estudiarla a fondo para establecer que tan adecuado es el hacer esta simplificación.

1.3. PROYECTO VEGA 1.0 (VULNERABILITY OF ELECTRICAL POWER GRIDS ANALYSIS)

Bajo el patrocinio del Ministerio de Energía de Estados Unidos, los investigadores del departamento de investigación de operaciones de la Escuela Naval Graduada y el Departamento de Ingeniería Eléctrica y Sistemas de la Universidad de Texas realizaron una investigación para el uso de técnicas de optimización y análisis de la seguridad y la resistencia de los sistemas de potencia contra las interrupciones causadas por ataques terroristas [1].

VEGA 1.0 es un proyecto que propone una serie de algoritmos y modelos matemáticos para hallar los puntos que son más vulnerables en el sistema eléctrico ante un ataque terrorista dirigido hacia cualquiera de sus componentes (centrales de generación, líneas de transmisión, transformadores, redes de distribución, etc.) y de esta manera poder determinar los puntos más débiles del sistema.

La solución matemática es un problema de optimización de dos niveles (min - max), lineal y lineal entero binario; a lo largo de la solución se hace la minimización y la maximización por separado para obviar la complejidad de solucionar el problema de dualidad por medio de *cortes de Bender* [4], es decir,

hacer el min-max simultáneo y también evitar la complejidad de la solución de sistemas no lineales.

La metodología consta de tres partes:

1) Solución del flujo de potencia. Se hace una aproximación del sistema en AC a DC, es decir se formula un DC – OPF (flujo de potencia óptimo en DC) para llevar el problema a una forma lineal (se supone que es una aproximación válida) que minimiza los costos de generación por cada unidad generadora y los costos de demanda insatisfecha.

2) Modelo de interdicción que minimiza los costos de generación más la carga no satisfecha, a la cual se define como la "interrupción." En este segundo nivel se toman en cuenta las posibles opciones de ataque de los terroristas a las diferentes componentes del sistema de potencia sin exceder los recursos con los que se cuenta. Las acciones de los terroristas son variables binarias.

3) Algoritmo de interdicción. Comienza solucionando el IDC – OPF (flujo de potencia óptimo en DC considerando las componentes atacadas) que es el "subproblema" del problema matemático. Asumiendo que no es atacado el sistema, el resultado es un flujo de potencia óptimo para operaciones normales.

   Luego el algoritmo resuelve un "problema maestro" e identifica un plan de interdicción que maximiza el valor estimado de los recursos de ataque sin exceder los recursos disponibles del atacante. Con este plan, las restricciones del DC-OPF se modifican y se resuelve el nuevo subproblema. Este proceso continúa encontrando planes alternativos de interdicción y evaluando la carga no satisfecha para cada uno de ellos.

El algoritmo fue aplicado en dos sistemas de prueba de confiabilidad de la IEEE llamados RTS-96 [8]. Las pruebas se realizaron en un computador personal de 1 GHz con 1 GB de RAM. El modelo y el algoritmo se introdujeron en la herramienta computacional GAMS, que es un lenguaje de programación para modelar algebraicamente los problemas numéricos de optimización.

GAMS permite fácilmente la generación y la manipulación de los subproblemas y de los problemas principales, que se solucionan realmente con la herramienta CPLEX, un código de programación lineal y entero altamente eficiente [1].

Finalmente esta metodología busca identificar los errores y falencias en el diseño del sistema para que sean reparadas de una manera eficiente; siendo el diseño de los sistemas eléctricos cada día más seguros y resistentes ante cualquier ataque.

Después de estudiar las metodologías nombradas anteriormente se determinó:

- Que la metodología del proyecto VEGA 1.0 no se ha analizado en Colombia.
- No se ha realizado un estudio riguroso de esta metodología para encontrar las ventajas y desventajas de su aplicación.
- Es una metodología desarrollada recientemente (2003).
- Esta metodología permite ser expandida de tal manera que se pueda considerar el recurso de protección.

A lo largo de la presente investigación se hará un estudio y análisis más riguroso de la metodología propuesta en el proyecto VEGA 1.0 para ser aplicada en una área del sistema de prueba de confiabilidad IEEE RTS-96 utilizando una herramienta computacional diferente y accesible en la Universidad de La Salle. Se observará su funcionamiento, se determinará su aplicabilidad para concluir qué beneficios tanto sociales como económicos se pueden obtener con la posible aplicación de esta metodología en el sistema eléctrico colombiano.

Tabla 1.1. Clasificación de contingencias en los sistemas de potencia

Clasificación de causas			Descripcion de las causas	Clasificacion de contingencias	Algunos casos
NATURAL Eventos que suceden sin intervención humana. Ellos, incluyen el fenómeno asociado con el envejecimiento de las componentes el sistema y las fallas en la operación, exposición y localización del sistema entre otros. También ellos incluyen los fenómenos naturales.	**INTERNO** Eventos asociados en condiciones anormales sólo por la operación del sistema. En general ellos involucran los elementos que fallan en el sistema de potencia, protecciones,etc.		Originados por daños de la constitución de los equipos del sistema de potencia. Por ejemplo fallas en transformadores, lineas, protecciones, etc.	**ADMISIBLE**	Fallas técnicas en los equipos del sistema. Errores en la producción de los equipos.
				NO ADMISIBLE	Fallas técnicas en los equipos críticos del sistema. Fallas técnicas en los equipos primarios y en las protecciones. Fallas en los estados de operación del sistema. Errores en la producción de los equipos críticos y las protecciones.
	EXTERNO Eventos asociados con condiciones anormales no debidos a la operación del sistema. Estos eventos a los que el sistema de potencia está expuesto pueden ser por su localización geográfica o por su entorno.		Estos son eventos a los que el sistema de potencia está expuesto dependiendo de su ubicación geográfica y de la exposición al ambiente. Estos ocurren por fenomenos naturales como descargas atmosféricas, vientos, etc.	**ADMISIBLE**	Descargas atmosféricas. Animales en las líneas de transmisión. Vientos y movimientos telúricos menores a los determinados por los criterios de diseño. Polución.
				NO ADMISIBLE	Descargas atmosféricas que superen las especificaciones de diseño. Vientos y movimientos telúricos no comunes que superen las especificaciones de diseño. Avalanchas e inundaciones; Polución exagerada.
NO NATURAL Eventos que suceden con la intervención humana. Estos eventos pueden ser intencionales o no intencionales.	**INTERNO** Eventos asocioados con condiciones anormales por la operación del sistema. En general incluyen los elementos fallados del sistema, protecciones, etc., debido a las acciones de operadores del sistema.	**INTENCIONAL** Eventos donde el responsable de estos tiene como objetivo el daño del sistema de potencia.	Estos ocurren por actos humanos intencionales en la operción y el mantenimiento del sistema con el propósito de dañar la integridad y la operación del sistema. Ellos pueden causar fallas ocultas.	**ADMISIBLE**	Sabotaje interno (huelgas, sindicatos).
				NO ADMISIBLE	Sabotaje interno.
		NO INTENCIONAL Eventos donde el responsable de estos no tiene como objetivo el daño del sistema de potencia.	Estos pueden ocurrir por errores y accidentes humanos durante la planeacion, operación y mantenimiento del sistema.	**ADMISIBLE**	Errores en el diseño del sistema. Decisiones de operación erroneas, errores de ejecución. Accidentes en el mantenimiento.
				NO ADMISIBLE	Decisión equivocada del operador o errores en la ejecución durante una alerta o emergencia cuando el sistema está operando. Accidentes catastróficos en el mantenimiento.
	EXTERNO Eventos asociados con condiciones anormales no debidos a la operación del sistema. Estos eventos son debidos a que el sistema está expuesto según su ubicación geográfica o su entorno, el impacto económico en la sociedad y la interdependencia de los sistemas eléctricos con otros sistemas.	**INTENCIONAL** Eventos donde el responsable de estos tienen como obgetivo el daño del sistema de potencia.	Estos son eventos a los que el sistema de potencia está expuesto por su impacto en la economía y por su interdependencia con otros sistemas. El objetivo es el daño del sistema de potencia.	**ADMISIBLE**	Ataques terroristas ,generalmente pequeños. Actos de guerra. Ataques en otros sistemas que tienen dependencia con el sistema de potencia.
				NO ADMISIBLE	Ataques terroristas. Cyberataques en los controles del sistema. Actos de guerra.
		NO INTENCIONAL Eventos donde el responsable de estos no tiene como objetivo el daño del sistema de potencia.	Estos son eventos no naturales a que el sistema está expuesto por su localización geográfica y por su exposición al ambiente. Pueden ocurrir como consecuencia de otras acciones sucedidas cerca del sistema.	**ADMISIBLE**	Errores Humanos: tala de árboles, líneas, construcciones vecinas.
				NO ADMISIBLE	Errores Humanos: aeronaves y helicópteros volando sobre las líneas de transmisión, construcciones vecinas.

Extraído y traducido del artículo: *"Events classification and operation status considering terrorism in security analysis"* de la referencia [11, pág. 3, Tabla 1].

2. PLANTEAMIENTO DEL PROBLEMA

Al abordar la posibilidad de determinar la vulnerabilidad de un sistema de potencia sometido ante una o un conjunto de fallas provocadas intencionalmente (ataques terroristas), es indispensable determinar en primera instancia un gran número de variables a tener en cuenta con el fin de llevar este escenario a una situación factible y ajustada a la realidad, es decir, a las condiciones reales que pudieran llegar a ocurrir en determinado caso.

Una manera didáctica de abordar este problema sería definir concretamente qué es la vulnerabilidad de un sistema de potencia ante un atentado terrorista, lo cual resulta bastante fácil de definir ya que la vulnerabilidad del sistema está estrechamente ligada con su funcionamiento y ésta no es más que la necesidad de entregar una potencia eléctrica en un sitio específico para su uso y la disponibilidad de una infraestructura para transportarla desde el lugar de su generación hasta el sitio de consumo.

No sería difícil entonces pensar en un sabotaje total del sistema (ser inhabilitado por completo), lo cual sería el peor de los escenarios, pero no necesariamente el más nocivo de todos. Este sería un escenario demasiado pesimista e ilógico, y es precisamente esta última apreciación el punto de partida para abordar el problema del análisis de la vulnerabilidad de un sistema eléctrico, y la razón por la cual se hace indispensable determinar las variables que entran a jugar un papel importante en este análisis. Ya que se hace obvio que un sistema no es totalmente vulnerable (susceptible de ser destruido por completo) entonces se debe determinar qué partes de él si lo son y bajo qué condiciones (variables del problema).

A continuación se enumeran las que serían probablemente las más importantes variables:

- ✓ No todas las componentes de un sistema son vulnerables:
  Si bien pudiera llegar a ocurrir un ataque directo a la infraestructura de un sistema eléctrico existen lugares inaccesibles para un grupo de individuos que estén interesados en perpetrar este tipo de acción.

- ✓ Los recursos de un grupo terrorista son limitados:
  La capacidad de ataque contra la infraestructura está limitada y restringida también por la disponibilidad de recursos con que cuente un grupo terrorista, pero este no es el propósito de esta investigación, pues esto requeriría de otras disciplinas más idóneas para su análisis.

- ✓ Un sistema eléctrico debe ser óptimo:
  Al satisfacer la demanda de energía debe hacerse de una manera óptima, es decir, de una manera eficiente tanto desde el punto de vista económico como energético y sin dejar de lado las especificaciones técnicas que determinan la calidad de la potencia entregada.

- ✓ La magnitud de la vulnerabilidad del sistema se mide en la necesidad de aprovechar el recurso eléctrico:
  El objetivo fundamental de un sistema de potencia es satisfacer una demanda de energía en un lugar determinado, es decir, el ataque contra un sistema es en el fondo un ataque contra una comunidad que depende de la energía eléctrica que éste le suministra.

- ✓ El objetivo de un grupo terrorista es llevar a cabo el mejor ataque posible con los recursos que dispone:
  Se parte de la suposición, cuando se lleva a cabo un ataque coordinado contra la infraestructura de un sistema, que la parte responsable de ejecutarlo espera hacer la mayor cantidad de daño que sea posible con los recursos de que dispone.

Dadas las anteriores condiciones se inicia una descripción del planteamiento del problema para determinar la vulnerabilidad de un sistema de potencia, que abarque la influencia de todos los tópicos contemplados anteriormente; que sería plantear un modelo que encuentre el ataque o conjunto de ataques coordinados contra algunas de las componentes de un sistema eléctrico que ocasione mayor disrupción en este, sujeto a las restricciones determinadas por el recurso del terrorista y la posible accesibilidad que el atacante tenga a las diferentes componentes, en un momento dado y con las condiciones actuales de operación del mismo.

2.1. PLANTEAMIENTO DE UN MODELO MATEMÁTICO DEL PROBLEMA

Teniendo en cuenta que el ataque ocurre cuando el sistema está operando en condiciones normales, y el hecho que una de sus componentes sea atacada implica que esta salga de funcionamiento totalmente, el proyecto VEGA 1.0 [2] plantea un modelo de flujo de potencia óptimo en función de las diferentes componentes y sujeto a la capacidad de las mismas, que brinde la posibilidad de suprimir la acción de cada una de las componentes susceptibles de ser atacadas.

Para simplificar el problema matemático, el flujo óptimo es una aproximación en DC del flujo en AC, siendo esto válido porque refleja el comportamiento del sistema. El flujo de potencia óptimo en DC es una minimización de los costos de

operación y no satisfacción de la demanda, sujeto a las condiciones de funcionalidad y eficiencia del sistema.

2.1.1. Flujo óptimo de potencia.

$$\min_{P^{Gen},P^{Line},S,\theta} \sum_g h_g P_g^{Gen} + \sum_i \sum_c f_{ic} S_{ic} \tag{2-1}$$

La función objetivo minimiza los costos de generación y de no satisfacción de la demanda donde h_g representa el costo de generar la potencia P_g en el generador g, f_{ic} representa los costos de la penalidad asociada con la no satisfacción de S_{ic}, que es la demanda no satisfecha en el nodo i del sector c.

Sujeto a las siguientes restricciones:

$$P_l^{Line} = B_l\left(\theta_{o(l)} - \theta_{d(l)}\right) \qquad \forall l \tag{2-2}$$

Estas restricciones aproximan los flujos de potencia activa en las líneas P_l^{Line}, en función de la susceptancia B_l, de cada línea l, y de los ángulos de la tensión ($\theta_{o(l)}$, $\theta_{d(l)}$) tanto en el nodo de origen de la línea $o(l)$, como el nodo de destino de la línea $d(l)$, esto para todas las líneas del sistema.

$$\sum_g P_g^{Gen} - \sum_{l|o(l)=i} P_l^{Line} + \sum_{l|d(l)=i} P_l^{Line} = \sum_c \left(d_{ic} - S_{ic}\right) \qquad \forall i \tag{2-3}$$

Estas restricciones mantienen el equilibrio de las potencias en los nodos, es decir la suma de las potencias generadas en el nodo P_g^{Gen}, más la suma de las potencias de las líneas P_l^{Line} que llegan al nodo $l|d(l)$, menos la suma de las potencias de las líneas P_l^{Line} que salen del nodo $l|o(l)$, son iguales a la suma de las demandas d_{ic}, menos las demandas no satisfechas S_{ic}, en el nodo i del sector c para todos los nodos (la suma de las potencias que entran a un nodo es igual a la suma de las potencias que salen de este).

$$-\overline{P}_l^{Line} \le P_l^{Line} \le \overline{P}_l^{Line} \qquad \forall l \tag{2-4}$$

Manifiestan que la potencia P_l^{Line}, que corre por la línea l, no puede exceder la potencia máxima $\overline{P}_l^{Line}$ de transmisión para la que fue diseñada, esto es para todas las líneas.

$$0 \le P_g^{Gen} \le \overline{P}_g^{Gen} \qquad \forall g \tag{2-5}$$

Que es lo mismo que la potencia P_g^{Gen} que puede generar una unidad generadora ***g***, no puede sobrepasar la potencia máxima nominal $\overline{P}_g^{Gen}$ de ésta, lo cual es válido para las unidades generadoras.

$$0 \le S_{ic} \le d_{ic} \qquad \forall i,c \qquad (2\text{-}6)$$

Finalmente estas restricciones indican que la demanda insatisfecha S_{ic}, no puede ser mayor que la demanda d_{ic}, en el nodo ***i*** del sector ***c***, esto es para todos los nodos y sectores del sistema.

Después, determina cuál de las posibles combinaciones de ataques contra la infraestructura del sistema sería la más perjudicial, es decir, la que ocasione mayor disrupción en éste, y que no exceda la capacidad de ataque con que cuenta el grupo atacante. Lo cual se hace suprimiendo del modelo de flujo de potencia, las componentes susceptibles de ser atacadas en las diferentes combinaciones que permita la cantidad de recurso terrorista, y evaluando la disrupción que cada combinación ocasionaría para entonces determinar cuál es el ataque más disruptivo, que se pueda llevar a cabo con un determinado recurso. Es decir, maximizar las disrupciones sujetas al acceso que el atacante tenga a las diferentes componentes y a la cantidad de recursos con que éste cuente.

2.1.2. Flujo de potencia óptimo incluyendo las variables de ataque (componentes susceptibles de ser atacadas). Este es un modelo de flujo óptimo de potencia, el cual permite remover del sistema las componentes atacadas directa o indirectamente[4], mediante el uso de un problema de optimización binario, donde las variables binarias son: $\delta_g^{Gen}, \delta_l^{Line}, \delta_i^{Bus}, \delta_s^{Sub}$, las cuales toman el valor de 1 si la componente del sistema fue atacada y cero 0 si por el contrario no lo fue.

Esto funciona de una manera muy sencilla multiplicando la componente del sistema por el grupo de ecuaciones $(1-\delta)$ que correspondan según sea o no afectadas, ya sea directa o indirectamente por un ataque contra una de ellas.

Como se puede ver, al ser atacada una componente del sistema su variable binaria toma el valor de **1** lo que resultaría en un valor de cero **0** en la ecuación

[4] Un componente es afectado directamente sí hay un ataque realizado sobre él y es afectado indirectamente cuando el ataque es realizado sobre otro componente del cual éste depende, por ejemplo un ataque contra un nodo afecta indirectamente las líneas que estén conectadas al mismo.

$(1-\delta)\,|_{\delta=1}=0$, suprimiendo el componente afectado directa o indirectamente del sistema para calcular posteriormente el flujo de potencia teniendo en cuenta la falta de dicho componente. El flujo de potencia incluyendo las variables de ataque es el siguiente:

$$\gamma\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}\right)=\min_{P^{Gen},P^{Line},S,\theta}\ \sum_g h_g P_g^{Gen}+\sum_i\sum_c f_{ic}S_{ic} \tag{2-7}$$

Sujeto a:

$$P_l^{Line}=B_l\left(\theta_0(l)-\theta_d(l)\right)\left(1-\delta_l^{Line}\right)\left(1-\delta_{0(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'|l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\quad\forall l \tag{2-8}$$

$$\sum_g P_g^{Gen}-\sum_{l|o(l)=i}P_l^{Line}+\sum_{l|d(l)=i}P_l^{Line}=\sum_c\left(d_{ic}-S_{ic}\right)\qquad\forall i \tag{2-9}$$

$$\begin{aligned}&-\overline{P}_l^{Line}\left(1-\delta_l^{Line}\right)\left(1-\delta_{0(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'|l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\le P_l^{Line}\le\\ &\overline{P}_l^{Line}\left(1-\delta_l^{Line}\right)\left(1-\delta_{0(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s|l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'|l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\qquad\forall l\end{aligned} \tag{2-10}$$

$$0\le P_g^{Gen}\le\left(1-\partial_{i(g)}^{Bus}\right)\left(1-\partial_g^{Gen}\right)\overline{P}_g^{Gen}\qquad\forall g \tag{2-11}$$

Se propone una modificación a esta última restricción (2-11) considerando que no tiene en cuenta las consecuencias de analizar la vulnerabilidad de un sistema de potencia con una configuración en la que existan generadores conectados directamente a uno de los nodos de una subestación. Porque en el momento de ser atacada la subestación, los generadores que estén entregando su potencia a los nodos de ella deberían ser desconectados como consecuencia del ataque.

La ecuación (2-11) con la modificación propuesta queda de la siguiente manera:

$$0\le P_g^{Gen}\le\left(1-\partial_{i(g)}^{Bus}\right)\left(1-\partial_g^{Gen}\right)\left(1-\partial_s^{Sub}\right)\overline{P}_g^{Gen}\qquad\forall g \tag{2-11'}$$

En el capítulo 5 se hace un análisis de la diferencia en los resultados al realizar esta modificación.

$$0\le S_{ic}\le d_{ic}\qquad\forall i,c \tag{2-12}$$

En esta minimización las variables binarias permanecen constantes en sus respectivos, valores ya sean uno (**1**) o cero (**0**) (para modelar si una componente del sistema fue o no atacada). Estas sólo varían dependiendo del estado de cada componente y serán determinadas en el problema principal, es decir, se evalúa el flujo óptimo de potencia (2-7 a 2-12) del sistema en el estado actual de ataques.

Para hallar cuál es el ataque disruptivo con su respectiva combinación o conjunto de componentes afectadas, se hace una maximización en función de las componentes binarias que determinan el estado del sistema, donde los valores obtenidos en el flujo óptimo $\left(P^{Line}, P^{Gen}, S\right)$ son utilizados para determinar las constantes de esta maximización.

2.1.3. Plan de ataque más disruptivo. Considerando que el sistema se encuentra operando bajo unas condiciones de ataque específicas, lo que la metodología [2] plantea para determinar cuál combinación de ataques simultáneos sería la más nociva, es darle una valoración al comportamiento de las componentes del sistema en función de las variables obtenidas del flujo de potencia $\left(P^{Line}, P^{Gen}, S\right)$ para estas condiciones.

Los resultados obtenidos del flujo de potencia $\left(P^{Line}, P^{Gen}, S\right)$ se utilizan para determinar el valor del aporte[5] de cada componente al sistema y finalmente maximizar la suma de estos aportes, según sean o no atacados para así obtener la mayor pérdida que cualquier grupo de ataques pueda ocasionar, claro está, restringido por el recurso de ataque y el acceso que se tenga a las componentes del sistema.

Esto se consigue haciendo una optimización que determine el valor máximo de pérdidas de capacidad del sistema de potencia, sujeto a las restricciones ya mencionadas, y otras dadas por la disposición física de la infraestructura.

Valores estimados del aporte de capacidad de cada componente al sistema. Los valores estimados para unas condiciones de ataque específicas son fáciles de calcular a partir de los resultados obtenidos en el flujo de potencia dado para estas condiciones $\left(P^{Line}, P^{Gen}, S\right)$. Los valores se determinan de la siguiente manera:

[5] Cada componente le aporta al sistema una capacidad específica, por ejemplo, un generador le aporta al sistema capacidad de generación, una línea capacidad de transmisión, etc.

- Valor de potencia generada en el generador ***g***

$$V_g^{Gen} = w^{Gen} P_g^{Gen} \qquad \forall g \tag{2-13}$$

Donde: $\boldsymbol{V_g^{Gen}}$ es el valor estimado, y $\boldsymbol{P_g^{Gen}}$ es la potencia generada por la unidad generadora ***g***, obtenida en el flujo de potencia; esto para todos los generadores.

- Valor de potencia transmitida por la línea ***l***

$$V_l^{Line} = w^{LIne}\left(\left|P_l^{Line}\right| + \sum_{l' \in L_l^{Par}} \left|P_{l'}^{Line}\right|\right) \tag{2-14}$$

Donde: $\boldsymbol{V_l^{Line}}$ es el valor estimado, que es igual a la potencia $\boldsymbol{P_l^{Line}}$ transmitida por la línea ***l,*** más la suma de las potencias transmitidas por las líneas en paralelo ***l'***, a esta; esto para todas las líneas.

- Valor de potencia en la subestación ***S***

$$V_s^{Sub} = w^{Sub}\left(\sum_{l | l \in L_s} \left|P_l^{Line}\right|\right) \qquad \forall s \tag{2-15}$$

Donde: $\boldsymbol{V_s^{Sub}}$ es el valor estimado, que es igual a la suma de las potencias $\boldsymbol{P_l^{Line}}$ transmitidas por las líneas ***l,*** que pertenecen a la subestación ***S***; esto para todas las subestaciones del sistema.

- Valor de potencias en el nodo ***i***

$$V_i^{Bus} = w^{Bus}\left(F_i^{Met} + F_i^{Out}\right) \qquad \forall i \tag{2-16}$$

Donde: $\boldsymbol{V_i^{Bus}}$ es el valor estimado, $\boldsymbol{F_i^{Mte}}$ es la carga suministrada para el nodo ***i***, y está dado por:

$$F_i^{Met} = \sum_c \left(d_{ic} - S_{ic}\right) \tag{2-17}$$

Que es igual a la suma de las demandas $\boldsymbol{d_{ic}}$ menos las demandas no satisfecha $\boldsymbol{S_{ic}}$ en el nodo ***i*** del sector ***c*** para todos los nodos. $\boldsymbol{F_i^{Out}}$ es el flujo de potencia fuera del nodo ***i***, y está dado por:

$$F_i^{Out} = \sum_{\substack{l|o(l) \\ \wedge \hat{P}_l Line>0}} P_l^{Line} + \sum_{\substack{l|d(l) \\ \wedge \hat{P}_l Line<0}} \left| P_l^{Line} \right| \quad (2\text{-}18)$$

Es igual a la suma de las potencias $P_l^{Line}>0$ de las líneas que salen del nodo, que sean mayores de cero $l|o(l)$, más la suma de los valores absolutos de las potencias de las líneas $P_l^{Line}<0$, que lleguen al nodo $l|d(l)$, que sean menores que cero.

Nota: Los valores de $w^{Gen}, w^{Bus}, w^{Line}$ y w^{Sub} son los valores del peso, especificados para reflejar la importancia relativa de cada tipo de componente, estos pueden usarse para hacer más o menos atractivos los componentes del sistema y podrían modificarse de acuerdo a la geografía, zona de influencia de los grupos atacantes y la protección física del componente (ver recomendaciones y trabajo futuros).

Modelo del problema para determinar el plan de ataque más disruptivo. Como se había mencionado anteriormente, este modelo consiste en una maximización de la suma de los valores estimados para cada componente por la variable binaria que representa el estado de éste, sujeto a las restricciones debidas al recurso terrorista, la accesibilidad al sistema y las restricciones de la disposición física del sistema.

El modelo de maximización es de tipo binario, es decir, las variables que intervienen son de tipo binario (pueden tomar únicamente valores de uno ***1,*** o cero ***0***).

La función objetivo es:

$$\max_{\substack{\delta Gen, \delta Line, \\ \delta Bus, \delta Sub}} \sum_{g \in \Gamma^*} V_g^{Gen} \delta_g^{Gen} + \sum_{l \in L^*} V_l^{Line} \delta_l^{Line} + \sum_{i \in I^*} V_i^{Gen} \delta_i^{Gen} + \sum_{s \in S^*} V_s^{Sub} \delta_s^{Sub} \quad (2\text{-}19)$$

Esta consiste en determinar el máximo de la suma de los productos entre los valores estimados y su respectiva variable binaria $\left(\delta^{Gen}, \delta^{Line}, \delta^{Bus}, \delta^{Sub}\right)$, que corresponden a cada una de las componentes del sistema que son susceptibles de ser atacadas.

Como se puede apreciar, si una componente del sistema es atacada, el valor que toma la variable que le corresponde es uno ***1***, pero si por lo contrario no es

atacada, el valor que su variable tomaría sería cero ***0***, de lo que resulta la sumatoria de los valores estimados de las componentes atacadas únicamente.

Esta función estará sujeta a las siguientes restricciones:

$$\sum_{g\in G^*} M_g^{Gen} + \sum_{l\in L^*} M_l^{Line}\delta_l^{Line} + \sum_{i\in I^*} M_i^{Bus}\delta_i^{Bus} + \sum_{s\in S^*} M_s^{Sub}\delta_s^{Sub} \le M \qquad (2\text{-}20)$$

La anterior restricción hace referencia al recurso que dispone un grupo terrorista para perpetrar el ataque, significa que la suma de los recursos requeridos para atacar el generador ***g***, la línea ***l***, el nodo ***i*** o la subestación ***s*** ($M_g^{Gen}, M_l^{Line}, M_i^{Bus}, M_s^{Sub}$), no puede exceder el recurso total de ataque ***M*** que dispone el terrorista.

Todas las variables δ son binarias, pero se fijan a 0 si no están asociadas con G^*, L^*, I^*, o S^*, que son los conjuntos de unidades generadoras, líneas, nodos, o subestaciones, respectivamente que son susceptibles de ser atacados.

$$\delta_k^{componente} = 0 \quad \forall \quad k \notin G^*, L^*, I^*, S^* \qquad (2\text{-}21)$$

Las siguientes restricciones indican la información de la disposición física de la infraestructura del sistema y que ninguna componente que halla sido afectada indirectamente por un ataque contra otra, sea atacada.

$$\delta_g^{Gen} + \delta_i^{Bus} \le 1 \quad \forall g \in G_i^*, i \in I^* \qquad (2\text{-}22)$$

Se puede atacar un generador o el nodo al que se conecta pero no los dos al tiempo.

$$\delta_l^{Line} + \delta_i^{Bus} \le 1 \quad \forall l \in L_i \cap L^*, i \in I^* \qquad (2\text{-}23)$$

Se puede atacar una línea o el nodo al que se conecta pero no ambos.

$$\delta_l^{Line} + \delta_{l'}^{Line} \le 1 \quad \forall l' \in L_l^{Par} \cap L^*, l \in L^* \qquad (2\text{-}24)$$

Se puede atacar una de dos líneas que estén en paralelo pero no ambas, aunque en la realidad dos líneas que se encuentran en paralelo normalmente comparten la misma estructura y un ataque contra una de ellas es un ataque contra ambas

$$\delta_i^{Bus} + \delta_s^{Sub} \le 1 \quad \forall i \in I_S \cap I^*, s \in S^* \qquad (2\text{-}25)$$

Un ataque contra un nodo o contra la subestación a la que está conectado, pero no contra las dos componentes.

$$\delta_l^{Line} + \delta_s^{Sub} \leq 1 \qquad \forall l \in L_S \cap L^*, s \in S^* \tag{2-26}$$

Se asegura que sólo sea atacada una línea o la subestación a la cual está conectada.

2.2. MODELO COMPLETO DEL PROBLEMA PARA DETERMINAR EL ATAQUE MÁS DISRUPTIVO

El modelo completo que representa este problema es una optimización (Máximo-mínimo) no lineal (mixta) de tipo entero binario[6]:

$$\begin{aligned} (Mm) \quad & \max_{\delta \in \Delta} \min_{p} \; c^T p \\ s.t. \quad & g(p,\delta) \leq b \\ & p \geq 0 \end{aligned} \tag{2-27}$$

Un plan de ataque es representado por el vector binario δ, cuya entrada *k*ésima δ_k es ***1*** si la componente ***k*** del sistema es atacada y por otra parte es ***0*** si no hay ataque. Para un planteamiento dado, el problema interno es un modelo de flujo de potencia óptimo que minimiza los costos de la generación más la penalidad asociada con la demanda insatisfecha, juntos denotados por la expresión $\boldsymbol{c^T p}$.

Aquí, ***p*** representa los flujos de potencia, rendimientos de la generación, ángulos de la fase y la demanda insatisfecha; ***c*** representa los costos de generación linealizados, y los costos de demanda insatisfecha. El problema externo es una maximización que escoge el plan de ataque más perjudicial, $\delta \in \Delta$, restringido por recursos, dónde Δ es un conjunto discreto que representa los ataques que un grupo terrorista pude llevar a cabo.

En este modelo, ***g*** corresponde a un conjunto de funciones de ***(p,δ)*** que no son lineales. El problema interno involucra un modelo de flujo de potencia óptimo simplificado, con funciones de restricción ***g(p,δ)*** que son, sin embargo, lineales en ***p*** para un valor fijo de $\delta = \hat{\delta}$ [2].

[6] Para información sobre este tipo de problemas de optimización se recomienda consultar las referencias [4] y [5].

La parte interna es el flujo de potencia óptimo incluyendo las variables de ataque y el problema externo es el modelo para determinar el plan de ataque más valioso (descritos en las secciones 2.1.2 y 2.1.3 respectivamente), en esta sección se hará una explicación más profunda sobre cómo se relacionan estos dos problemas en uno sólo.

Primero se determina el flujo de potencia óptimo para un δ constante, que representa un grupo de ataques coordinados.

Posteriormente haciendo uso de los resultados obtenidos del flujo de potencia $\left(P^{Line}.P^{Gen},S\right)$, se calculan los valores estimados (2-13 a 2-16) para éste y con ellos se determina la función objetivo (2-19) del *modelo del problema para determinar el plan de ataque más valioso*. Se halla el nuevo vector δ, que pasa a ser el nuevo plan de ataque constante para iniciar nuevamente el proceso.

Es importante aclarar que se determina un flujo de potencia para cada plan de ataque en cada iteración, pero los valores estimados son promediados de una iteración a otra, lo que obedece a un corte de Bender [4], y se debe agregar otra restricción a la maximización que condiciona que el ataque δ, no sea igual a un ataque δ', de una iteración anterior. El anterior ciclo debe cumplirse hasta encontrar el ataque más perjudicial; en el capítulo 3 se hará una explicación más detallada de este algoritmo.

2.3. SÍNTESIS DEL PROBLEMA PARA DETERMINAR EL ATAQUE MÁS DISRUPTIVO

La siguiente tabla 2.1 ilustra el problema completo, discriminando las variables y las constantes. En el primer nivel del modelo se puede observar que las variables del segundo nivel son sus constantes y en el segundo nivel sus constantes son las variables del primer nivel.

Tabla 2.1. Descripción de variables y constantes dependiendo del modelo.

Modelo	Descripción	Variables	Constantes
Flujo de potencia óptimo con variables binarias constantes	$$\gamma\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}\right)=\min_{P^{Gen},P^{Line},S,\theta}\sum_g h_g P_g^{Gen}+\sum_i\sum_c f_{ic}S_{ic}$$ sujeto a: $$P_l^{Line}=B_l\left(\theta_{o(l)}-\theta_{d(l)}\right)\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s\mid l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'\mid l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\quad\forall l$$ $$\sum_g P_g^{Gen}-\sum_{l\mid o(l)=i}P_l^{Line}+\sum_{l\mid d(l)=i}P_l^{Line}=\sum_c\left(d_{ic}-S_{ic}\right)\quad\forall i$$ $$-\overline{P}_l^{Line}\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s\mid l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'\mid l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\le P_l^{Line}\le$$ $$\overline{P}_l^{Line}\left(1-\delta_l^{Line}\right)\left(1-\delta_{o(l)}^{Bus}\right)\left(1-\delta_{d(l)}^{Bus}\right)\prod_{s\mid l\in L_s^{Sub}}\left(1-\delta_s^{Sub}\right)\prod_{l'\mid l'\in L_l^{Par}}\left(1-\delta_{l'}^{Line}\right)\quad\forall l$$ $$0\le P_g^{Gen}\le\left(1-\partial_{i(g)}^{Bus}\right)\left(1-\partial_g^{Gen}\right)\overline{P}_g^{Gen}\quad\forall g$$ $$0\le S_{ic}\le d_{ic}\quad\forall i,c$$	P_g^{Gen} Generación de la unidad ***g*** (MW); P_l^{Line} Flujo de potencia en la línea ***l*** (MW); S_{ic} Carga no satisfecha por el sector ***c*** al nodo ***i*** (MW); θ_i Ángulo de fase del nodo ***i*** (radianes).	$o(l),d(l)$ Origen y destino del nodo de línea ***l***; d_{ic} Carga de consumo del sector ***c*** al nodo ***i*** (MW); $\overline{P}_l^{Line}$ Capacidad de la transmisión para la línea ***l*** (MW); $\overline{P}_g^{Gen}$ Máxima potencia generada del generador ***g*** (MW); $B_l=xl/(r_l^2+x_l^2)$ susceptacia en serie h_g Costo de generación de la unidad ***g*** ($/MWh); f_{ic} Costo de carga no satisfecha del sector ***c*** en el nodo ***i*** ($/MWh). $\delta=\left(\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}\right)$ Constantes binarias de ataque (son constantes para cada iteración)

Modelo del problema para determinar el plan de ataque más disruptivo

$$\max_{\delta^{Gen},\delta^{Line},\delta^{Bus},\delta^{Sub}} \sum_{g\in I^*} V_g^{Gen,t}\delta_g^{Gen} + \sum_{l\in L^*} V_l^{Line,t}\delta_l^{Line} + \sum_{i\in I^*} V_i^{Gen,t}\delta_i^{Gen} + \sum_{s\in S^*} V_s^{Sub,t}\delta_s^{Sub}$$

Sujeto a:

$$\sum_{g\in G^*} M_g^{Gen} + \sum_{l\in L^*} M_l^{Line}\delta_l^{Line} + \sum_{i\in I^*} M_i^{Bus}\delta_i^{Bus} + \sum_{s\in S^*} M_s^{Sub}\delta_s^{Sub} \le M$$

Todas las variables δ son binarias, pero se fijan a 0 si no están asociadas Con G^*, L^*, I^*, o S^*.

$$\delta_g^{Gen} + \delta_i^{Bus} \le 1 \qquad \forall g \in G_i^*, i \in I^*$$

$$\delta_l^{Line} + \delta_i^{Bus} \le 1 \qquad \forall l \in L_i \cap L^*, i \in I^*$$

$$\delta_l^{Line} + \delta_{l'}^{Line} \le 1 \qquad \forall l' \in L_l^{Par} \cap L^*, l \in L^*$$

$$\delta_i^{Bus} + \delta_s^{Sub} \le 1 \qquad \forall i \in I_S \cap I^*, s \in S^*$$

$$\delta_l^{Line} + \delta_s^{Sub} \le 1 \qquad \forall l \in L_S \cap L^*, s \in S^*$$

$$\sum_{\substack{g\in G^* \mid \\ \hat{\delta}_g^{Gen,t'}=1}} \left(\hat{\delta}_g^{Gen,t'} + \delta_g^{Gen}\right) + \sum_{\substack{l\in L^* \mid \\ \hat{\delta}_l^{Line,t'}=1}} \left(\hat{\delta}_l^{Line,t'} + \delta_l^{Line}\right) + \sum_{\substack{i\in I^* \mid \\ \hat{\delta}_i^{Bus,t'}=1}} \left(\hat{\delta}_i^{Bus,t'} + \delta_i^{Bus}\right) + \sum_{\substack{s\in S^* \mid \\ \hat{\delta}_s^{Sub,t'}=1}} \left(\hat{\delta}_s^{Sub,t'} + \delta_s^{Sub}\right) \ge 1, \quad \forall t' \le t.$$

$\delta = \left(\delta^{Gen}, \delta^{Line}, \delta^{Bus}, \delta^{Sub}\right)$

Variables binarias que corresponden a cada una de las componentes del sistema que son susceptibles de ser atacadas, estas toman el valor de uno ***1***, sí la componente fue atacada, y son por otra parte cero ***0***, sí esta no fue atacada

P_g^{Gen} Generación de la unidad ***g*** (MW);

P_l^{Line} Flujo de potencia en la línea ***l*** (MW);

S_{ic} Carga no satisfecha por el sector ***c*** al nodo ***i*** (MW);

Para determinar:

V_g^{Gen}, Valor de potencia generada en el generador ***g***

V_l^{Line}, Valor de potencia transmitida por la línea ***l***

V_s^{Sub} , Valor de potencia en la subestación ***S***

V_i^{Bus}, Valor de potencias en el nodo ***i***

$M_g^{Gen}, M_l^{Line}, M_i^{Bus}, M_s^{Sub}$

Recurso necesario para atacar cada tipo de componente

M, Recurso total con el que cuenta el grupo terrorista

$\hat{\delta} \in \hat{\Delta}$ Vector de grupos de ataques ya considerados

3. METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

Basado en el algoritmo aplicado en el proyecto VEGA 1.0 (algoritmo de interdicción[7]), este algoritmo resuelve en forma iterativa el flujo de potencia óptimo incluyendo las variables de ataque y el plan de ataque más disruptivo.

Inicialmente soluciona el "subproblema" que es el flujo de potencia óptimo incluyendo las variables de ataque asumiendo que no se ha presentado ningún ataque, es decir, todas las variables binarias δ igual a cero (0).

Posteriormente, utilizando los valores obtenidos del flujo óptimo $\left(P^{Line}, P^{Gen}, S\right)$, calcula los valores estimados del aporte que cada componente le brinda al sistema y los guarda para ser utilizados durante la solución del problema principal, creando la función objetivo (2-18) del *problema del plan de ataque más disruptivo*.

Continúa resolviendo el problema principal (el plan de ataque más disruptivo) donde se obtienen los valores de las variables binarias δ, es decir, cuáles componentes deberán ser atacadas para conseguir la máxima pérdida del sistema hasta el momento. Los resultados de δ también son guardados para ser comparados con los futuros conjuntos de ataques obtenidos en las siguientes iteraciones y agregar una nueva restricción en cada iteración para asegurar que no existan valores repetidos de δ, con este paso se concluye cada iteración.

Finalmente retorna al subproblema, y lo resuelve con las condiciones de ataque δ halladas en el paso anterior y continúa repitiendo el ciclo hasta determinar la mayor pérdida de capacidad del sistema con el mínimo costo de generación y de no satisfacción de la demanda, teniendo en cuenta que los valores estimados del aporte de cada componente obtenidos en cada iteración son promediados con los de iteraciones anteriores guardas durante el algoritmo.

3.1. ALGORITMO DE INTERDICCIÓN

Este algoritmo empieza solucionando el flujo de potencia óptimo incluyendo variables binarias, denominado "subproblema", sin ser atacado el sistema (δ=0).

[7] Una descomposición basada en métodos heurísticos para obtener los planes de interdicción aceptables (para los terroristas), aunque no necesariamente óptimos [2].

El resultado es el flujo de potencia óptimo para operaciones normales del sistema, es decir, se minimizan los costos de generación sin ninguna carga insatisfecha, el modelo de flujo de potencia se usa para asignar los valores relativos a todas las componentes del sistema.

Después, el algoritmo resuelve el "problema principal" para identificar un grupo de ataques coordinados (plan de ataque), que maximiza el valor estimado de los recursos atacados sin exceder los recursos disponibles para realizar el ataque (*M*). Con este plan de ataque, las restricciones del flujo óptimo de potencia se modifican suprimiendo las variables de las componentes afectadas (se suprimen las componentes atacadas) y se resuelve el nuevo subproblema.

El resultado es un flujo de potencia que minimiza los costos de la generación más la penalidad asociada con la demanda insatisfecha, dadas las nuevas condiciones de ataque en el sistema. En este proceso, alguna cantidad de carga será interrumpida en la nueva solución porque algunas componentes importantes se habrán removido del sistema y este proceso continúa iterando hasta obtener el ataque más disruptivo.

En el problema principal se incorporan restricciones que no permiten que se repitan soluciones de iteraciones anteriores, y continúa iterando hasta que haya identificado una solución óptima, esto se hace de la siguiente forma:

$$\sum_{\substack{g\in G^* | \\ \hat{\delta}_g^{Gen,t'}=1}}\left(\hat{\delta}_g^{Gen,t'}+\delta_g^{Gen}\right)+\sum_{\substack{l\in L^* | \\ \hat{\delta}_l^{Line,t'}=1}}\left(\hat{\delta}_l^{Line,t'}+\delta_l^{Line}\right) + \sum_{\substack{i\in I^* | \\ \hat{\delta}_i^{Bus,t'}=1}}\left(\hat{\delta}_i^{Bus,t'}+\delta_i^{Bus}\right)+\sum_{\substack{s\in S^* | \\ \hat{\delta}_i^{Sub,t'}=1}}\left(\hat{\delta}_s^{Sub,t'}+\delta_s^{Sub}\right) \geq 1, \quad \forall t' \leq t. \tag{3-1}$$

Donde: el valor de δ representa la variable binaria y los $\hat{\delta}^{t'}$ son constantes y representan los resultados de soluciones de iteraciones anteriores siendo t' la iteración correspondiente a dicho resultado, esto para todos los resultados de iteraciones anteriores.

El subproblema es el flujo de potencia óptimo para un plan de ataque dado, en la iteración ***t*** del algoritmo $\hat{\delta}^t = \left(\hat{\delta}^{Gen,t}, \hat{\delta}^{Line,t}, \hat{\delta}^{Bus,t}, \hat{\delta}^{Sub,t}\right)$.

El modelo de flujo de potencia incluyendo las variables de ataque en función de $\left(\hat{\delta}^t\right)$, forma el subproblema y su solución proporciona el valor objetivo $\gamma(\hat{\delta}^t) = \gamma\left(\hat{\delta}^{Gen,t}, \hat{\delta}^{Line,t}, \hat{\delta}^{Bus,t}, \hat{\delta}^{Sub,t}\right)$ junto con los flujos de potencia, la generación y la demanda no satisfecha, los cuales se representan por $\hat{P}^t = \left(\hat{P}^{Line,t}, \hat{P}^{Gen,t}, \hat{S}^t, \hat{\theta}^t\right)$.

Los valores estimados del aporte de capacidad de cada componente al sistema: la solución $\hat{P}^t = \left(\hat{P}^{Line,t}, \hat{P}^{Gen,t}, \hat{S}^t, \hat{\theta}^t\right)$, dada por $\gamma(\hat{\delta}^t) = \gamma\left(\hat{\delta}^{Gen,t}, \hat{\delta}^{Line,t}, \hat{\delta}^{Bus,t}, \hat{\delta}^{Sub,t}\right)$, sirve para construir los valores estimados de las componentes para futuros ataques.

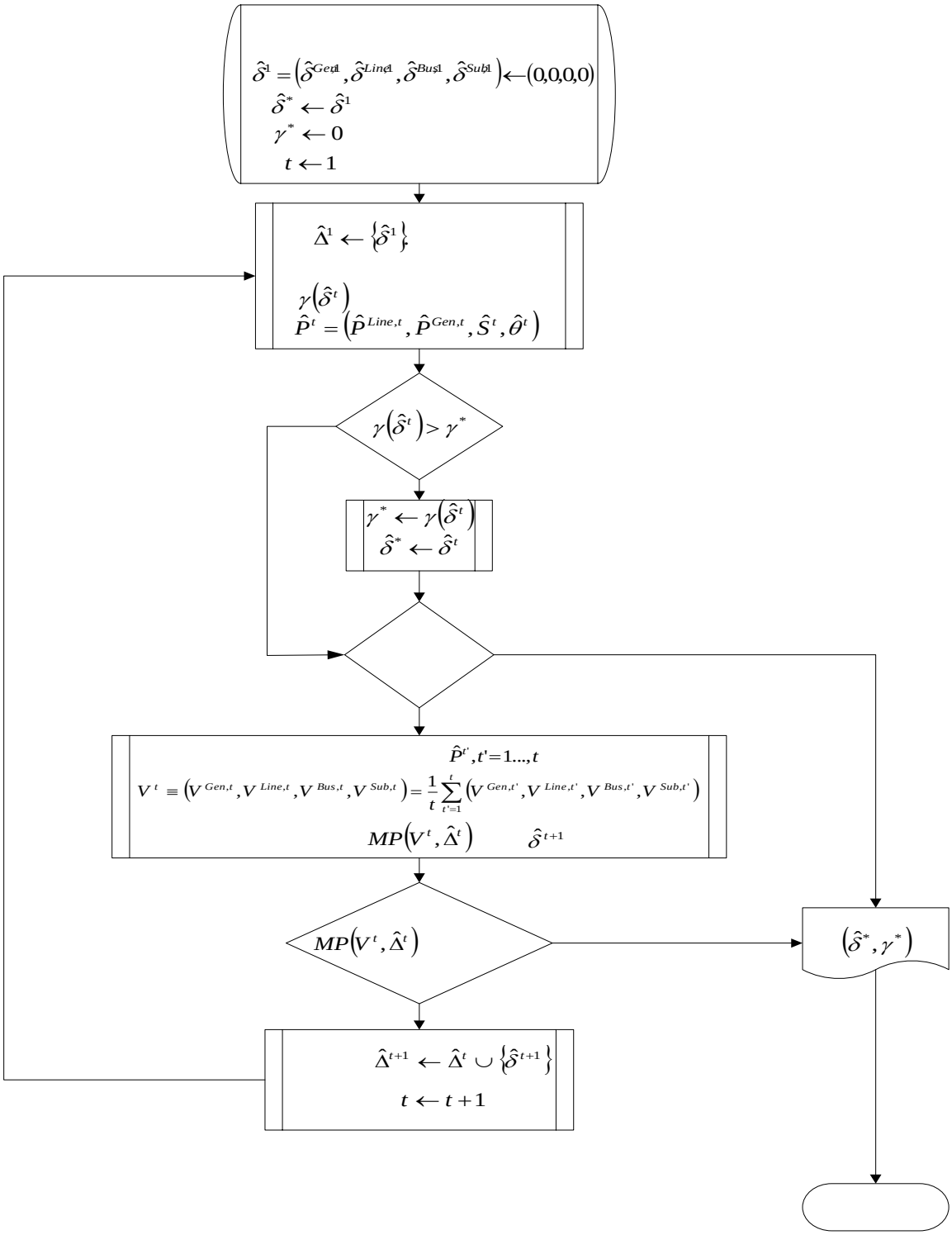
Para determinar estas estimaciones, se define un juego de parámetros con las ecuaciones (2-13) a (2-18).

El problema principal sirve para encontrar un plan de ataque poderoso: asumiendo que un conjunto de los valores estimados para cada componente del sistema $V^t = \left(V^{Gen,t}, V^{Line,t}, V^{Bus,t}, V^{Sub,t}\right)$, se calculó en la iteración ***t***; y se define el vector de los planes de ataque previamente generados $\hat{\Delta}^t = \left(\hat{\delta}^1, ..., \hat{\delta}^t\right)$. El problema principal de interdicción es entonces el modelo del problema para determinar el plan de ataque más disruptivo definido en el capítulo 2 (sección 2.1.3) agregándole la restricción (3-1) para evitar repetir soluciones de iteraciones anteriores.

La solución del modelo del problema para determinar el plan de ataque más disruptivo maximiza el valor estimado de las componentes atacadas del sistema; el plan de ataque obtenido en la iteración $\hat{\delta}^{t+1} = \left(\hat{\delta}^{Gen,t+1}, \hat{\delta}^{Line,t+1}, \hat{\delta}^{Bus,t+1}, \hat{\delta}^{Sub,t+1}\right)$ es usado en el subproblema para comenzar una nueva iteración del algoritmo.

3.1.1. Diagrama de flujo del algoritmo de interdicción. Con el fin de aclarar al lector la metodología planteada en [1], [2]. Aquí se muestra la interacción de los niveles del algoritmo y el proceso de obtención de resultados usando un diagrama de flujo.

Figura 3.1. Algoritmo de Interdicción



4. IMPLEMENTACIÓN DE LA METODOLOGÍA

4.1. SELECCIÓN DE LA HERRAMIENTA COMPUTACIONAL PARA LA SOLUCIÓN DEL PROBLEMA MATEMÁTICO

Debido a la complejidad del problema matemático para hallar la vulnerabilidad de los sistemas de potencia, se buscó una herramienta computacional que pueda suplir estas necesidades y hacer el proceso iterativo de la forma más rápida y precisa. Por esta razón se hizo un análisis[8] de las posibles herramientas computacionales, teniendo en cuenta lo que se necesita a nivel matemático y operacional, y el acceso que se tiene a ellas.

Las principales características que deben tener los programas para la solución del problema matemático y operacional son las siguientes:

- ***Condición 1:*** solucione problemas de minimización.
- ***Condición 2***: solucione problemas de maximización.
- ***Condición 3:*** solución de sistemas lineales.
- ***Condición 4:*** solucione problemas de optimización de tipo lineal entero binario.
- ***Condición 5:*** haga ciclos iterativos rápidos y confiables.
- ***Condición 6:*** admita crear un código abierto que permita la modificación de las funciones objetivo y las restricciones del problema principal y el subproblema, y se puedan guardar los resultados de cada iteración para luego ser comparados y escoger el posible plan de ataque más disruptivo.
- ***Condición 7:*** el programa sea de fácil aprendizaje y de rápida implementación.
- ***Condición 8:*** licencia gratuita o acceso directo para ser utilizado el programa en la Universidad de La Salle.

[8] Esta metodología de comparación y selección del programa que se va implementar es adoptada del artículo “Estudio de flujos de potencia al instalar un facts en la línea de transmisión circo - Guavio perteneciente al sistema de transmisión colombiano” por Fredy Murcia, Guillermo Díaz, y Camilo Cortés [20].

Tabla 4.1. Comparación y selección de programas para la solución del problema matemático.

	Software	Cond 1	Cond 2	Cond 3	Cond 4	Cond 5	Cond 6	Cond 7	Cond 8
Asociados con MATLAB	Optimization Toolbox 3.1	x	x	x	x	x	x	x	x
	LSQR	x	_	x	_	x	x	x	x
	LUMOD	_	x	x	_	x	x	x	x
	MOSEK	x	x	x	_	x	x	x	_
Software Comerciales	MINOS	x	x	x	x	x	x	_	_
	LSSOL	x	x	x	x	x	x	_	_
	NPSOL	x	x	_	x	x	x	_	_
	SNOPT	x	x	x	x	x	x	_	_
	GAMS	x	x	x	x	x	x	x	_

En la tabla 4.1 se mencionan algunas de las herramientas que se consideraron más relevantes, es decir, estas no son las únicas herramientas. Existen un gran número de herramientas especializadas[9] que pueden cumplir con las condiciones necesarias para la solución del problema.

4.2. POSIBLES HERRAMIENTAS DE SOLUCIÓN

Teniendo las especificaciones dadas anteriormente, se analizan más a fondo tres posibles herramientas computaciones que pueden ayudar a la solución del modelo que se describe en este documento.

4.2.1. GAMS [17]. El nombre de este programa se deriva de las iniciales de *General Algebraic Modelling System,* un programa inicialmente desarrollado por el Banco Mundial para evaluar los modelos de crecimiento en los países en vía de desarrollo. Como su nombre lo indica, es un lenguaje de modelamiento, más que un programa para re*solver* problemas de optimización. Una de las principales ventajas de este programa, es que junto al módulo de modelización (base)

[9] Para una consulta más amplia sobre estas herramientas especializadas se recomienda visitar referencia electrónica [6].

incorpora diferentes *solvers*[10] (algoritmos de resolución de problemas) tanto de programación no lineal, como lineal y entera, como por ejemplo:

Tabla 4.2. Solvers de GAMS para diferentes modelos de optimización.

Modelos matemáticos de optimización	***Solver***
NLP (programación no lineal)	CONOPT, MINOS, etc.
LP (programación lineal)	OSL, CPLEX,MINOS, BDMLP, etc
MIP (programación lineal entera mixta)	OSL, ZOOM, XA, CPLEX, etc.
MINLP (programación no lineal entera mixta)	DICOPT

GAMS utiliza un *"input file"*, es decir, un archivo donde va toda información del problema (función objetivo, restricciones, punto partida de la iteración, cómo se desea resolver el problema, etc.), esta ficha se puede hacer en cualquier programa de editor de líneas o en procesadores de texto, como por ejemplo Word y Wordperfect, entre otros. De esta manera, se llama la ficha desde GAMS y se comienza buscar la solución óptima dependiendo de las especificaciones dadas en la ficha.

Para hacer cambios en las funciones objetivo, las restricciones, los resultados, etc., se debe crear otro archivo con los nuevos datos que se desean ingresar; se vuelve a correr el programa y de esta manera se puede interactuar con diferentes archivos.

La metodología de solución del problema que se describe en este proyecto fue desarrollada con este software, por los autores Javier Salmerón, Kevin Wood y Ross Baldick en el proyecto VEGA 1.0. Esta investigación busca implementar un software diferente al ya utilizado para solucionar esta metodología, del cual se disponga en la Universidad de La Salle y que sea de uso común entre los integrantes de la Facultad de Ingeniería Eléctrica. Además de esta razón, GAMS es una herramienta computacional muy potente y precisa especializada en problemas de optimización, pero es un programa que requiere de una licencia con la que no se cuenta. Se pueden obtener versiones estudiantiles gratuitas pero limitan el tiempo de su uso y la cantidad de variables que puede tener el problema, así como el número de restricciones, es decir, las características de este software no se acomodan, por ahora, al alcance de esta investigación.

[10] Solver (s), es una herramienta con la que cuenta un software que soluciona un problema específico, se aclara que no es conveniente reemplazar este término por un vocablo en castellano.

4.2.2. MOSEK [18]. Este es un toolbox[11] de optimización gratuito para ser utilizado en MATLAB, está diseñado para solucionar problemas matemáticos de gran escala (problemas de optimización demasiado extensos) y complejidad. MOSEK proporciona una variedad de *solvers* especializados para programación lineal, programación lineal entera mixta y otros tipos de problemas convexos no lineales de optimización, además soluciona los siguientes problemas:

- Problemas lineales
- Problemas cónicos cuadráticos
- Problemas convexos no lineales en general

MOSEK tiene dos interfases, una es el lenguaje base de su programación (C/C++, .NET y Java.) y la segunda es el toolbox de optimización para ser utilizado en la plataforma MATLAB.

El toolbox de Optimización 3.1 MATLAB es lento para la solución de problemas de optimización de gran escala. MOSEK es un toolbox de optimización que permite la solución rápida y eficiente de problemas robustos y dispendiosos.

En general el toolbox MOSEK puede solucionar problemas de optimización solamente convexos mientras que el toolbox de Optimización 3.1 de MATLAB puede solucionar problemas no convexos también. MOSEK utiliza algoritmos de programación para problemas extensos o breves dependiendo de la necesidad del usuario, el motor principal de cómputo dentro del toolbox de optimización es un *primal-dual* con un algoritmo de tipo *punto-interior* que está demostrado que puede resolver problemas a gran escala [18].

Por ejemplo, una de las funciones que usa MOSEK y el toolbox de optimización 3.1 de MATLAB para la optimización de problemas lineales es el "*linprog"*, con la gran diferencia que en MOSEK si acepta límites arbitrarios y no utiliza todas las opciones del toolbox de optimización 3.1 de MATLAB para llegar a un posible resultado.

MOSEK ofrece una licencia estudiantil gratuita durante un semestre, pero aún cuando este programa brinda la ventaja de trabajar en MATLAB, tiene la gran desventaja que no soluciona problemas de optimización de tipo lineal binario, por esta razón se decidió no usarlo en esta investigación.

[11] Este término traduce "Caja de Herramientas", toolbox es el término tradicional de dichas cajas en el software MATLAB.

4.2.3. Toolbox de Optimización 3.1. MATLAB. Este toolbox contiene un conjunto de funciones que incluyen diferentes rutinas de solución para varios tipos de optimización, las cuales incluyen:

- Minimización no lineal sin restricciones
- Minimización no lineal con restricciones
- Incluye problemas de dualidad min-max
- Programación cuadrática y lineal
- Resuelve problemas estructurados y de gran escala
- Soluciona ecuaciones de sistemas no lineales

El Toolbox de Optimización 3.1 soluciona los problemas de optimización según su tipo y tamaño:

- Larga escala
- Media escala
- Larga y media escala

Entre las herramientas investigadas el Toolbox de Optimización 3.1. de MATLAB es la herramienta que más se acomoda a las necesidades requeridas para la solución del problema de determinar la vulnerabilidad de sistemas eléctricos ante atentados. A continuación se enumeran las características más relevantes por las que se resolvió utilizarlo:

- Acceso directo: La Universidad de La Salle cuenta con la licencia del MATLAB.
- Permite la solución de optimización lineal y lineal entera binaria.
- No está limitado por la cantidad de variables ni restricciones del problema operacional.
- Admite la interacción con las variables: Al ser un toolbox que hace parte de MATLAB, permite realizar un código de programación en donde se pueden modificar los datos de entrada y las constantes de los problemas de optimización (funciones objetivo y restricciones), así como guardar los resultados obtenidos.
- Aunque al momento de iterar es lento, permite variar el tiempo disponible para la solución del problema de optimización de tipo binario (en la sección 4.3.1 se profundizará este tema) pero no es un problema de gran relevancia.

4.3. DESCRIPCIÓN DE LA PROGRAMACIÓN Y EL USO DE LA HERRAMIENTA SELECCIONADA

Se desarrolló una programación que pudiera ser implementada en cualquier sistema de potencia para el análisis de la vulnerabilidad ante un ataque terrorista, es decir, no se realizó una programación para cada sistema de prueba específico sino que se desarrollo un programa, que a partir de unos datos necesarios del sistema, modela el problema de análisis de vulnerabilidad.

4.3.1. Uso de funciones del Optimization Toolbox 3.1 necesarias para la solución de la metodología. La metodología plantea el uso de dos tipos de optimización, minimización lineal (en el subproblema) y una maximización de tipo lineal binario (en el problema principal). A continuación se hace una breve descripción del uso de las funciones que se implementaron [7]:

- ***linprog:*** soluciona problemas de minimización lineal del siguiente tipo:

$$\min_x f^T x \quad \text{Sujeto a} \quad \begin{aligned} A \cdot x &\le b \\ Aeq \cdot x &= beq \\ lb \le x &\le ub \end{aligned} \tag{4-1}$$

  Donde f, x, b, lb, ub, y beq son vectores y A y Aeq son matrices.

- ***bintprog:*** soluciona problemas de tipo lineal binario de la siguiente forma:

$$\min_x f^T x \quad \text{Sujeto a} \quad \begin{aligned} A \cdot x &\le b \\ Aeq \cdot x &= beq \end{aligned} \tag{4-2}$$

  Donde *f, x, b,* y *beq* son vectores, *A* y *Aeq* son matrices y *x* es un vector que puede tomar el valor de 1 ó 0 solamente.

Tabla 4.3. Datos de entrada para las funciones *linprog* y *bintprog*

Argumento de Entrada	Descripción
X0	Es el vector de los valores iniciales que toman las variables.
f	Es el vector de coeficientes que conforman la función objetivo (ecuación lineal): $f^T * x$
A, b	*A* es la matriz de coeficientes de las restricciones de "*desigualdad*" y *b* corresponde al lado derecho del vector: $A * x \leq b$
Aeq , beq	*Aeq* es la matriz de coeficientes de las restricciones de "*igualdad*" y *beq* corresponde al lado derecho del vector: $Aeq * x = beq$
lb, ub (solo aplica para la función linprog)	*ub* es el vector de los valores más altos que pueden tomar el vector de variables *x* y el vector *lb* representa los valores más bajos que pueden tomar los valores del vector de variables *x*
options	Opciones de la estructura del algoritmo utilizado en la solución.

Optimization Toolbox 3.1 for Use with MATLAB, User's Guide Version 3 [7].

Tabla 4.4. Datos de salida para las funciones *linprog* y *bintprog*

Argumentos de Salida	Descripción
x	El vector de los valores que deben tomar las variables para conseguir el valor óptimo de $f^T * x$, el valor mínimo. Para hacer una maximización se debe multiplicar $f^T * -1$, lo que daría como resultados de *x* para conseguir el valor óptimo máximo.
fval	Es el resultado de evaluar la función objetivo *f* en el vector *x,* de variables obtenido, es decir, el valor óptimo mínimo o el negativo del valor máximo.
exitflag	Muestra la razón por la cual el algoritmo de optimización terminó. Por ejemplo la función convergió con el valor de *x*, el problema no es factible, excede el tiempo asignado para solución, etc.
output	Muestra la información acerca de la optimización como número de iteraciones realizadas, el algoritmo usado para la solución y otras opciones que dependen si se usa linprog o bintprog.

Optimization Toolbox 3.1 for Use with MATLAB, User's Guide Version 3 [7].

- ***optimset:*** se utiliza para habilitar o darle un valor a las opciones disponibles para solucionar el problema de optimización según la escala del problema y el tipo de función utilizada, estas opciones se programan por parejas conformadas por el nombre de la opción y su estado o valor. Por ejemplo máximo número de iteraciones ('*Maxiter*',50), tolerancias ('*TolFun*',1e-6), algoritmo a utilizar ('*Simplex*','*on*'), etc.

Tabla 4.5. Opciones de optimización utilizadas para las funciones *linprog* y *bintprog*

Nombre de opción	Descripción	Funciones
Simplex	Si su estado es '*on*' el algoritmo utilizado para la solución del problema es el método simplex.	*linprog*
LargeScale	Su estado debe ser '*on*' si el problema es de larga escala.	*linprog* y *bintprog*
Display	Muestra los resultados de iteración a iteración con el estado '*iter*'.	*linprog* y *bintprog*
BranchStrategy	Estrategia de ramas utilizada para la solución del problema de tipo binario.	*bintprog*
NodeStrategy	Estrategia de nodos utilizada para la solución del problema de tipo binario.	*bintprog*
Maxtime	El máximo tiempo en segundos admisible para la solución del problema.	*bintprog*
TolFun	Tolerancia o margen de error permitido para el valor final de la función objetivo, es decir, el *fval*.	*linprog* y *bintprog*

Optimization Toolbox 3.1 for Use with MATLAB, User's Guide Version 3 [7].

Estas funciones[12] fueron utilizadas de la siguiente manera para la programación de los diferentes algoritmos:

- ✓ options = optimset('Simplex','on','LargeScale','on','Display','iter');
  [x,fval,exitflag,output] = linprog(f,[ ],[ ],Aeq,Beq,lb,ub)

- ✓ options=optimset('Display','iter','BranchStrategy','mininfeas',
  'MaxTime',15,'TolFun',1e-5);
  [x1,fval1,exitflag,output] = bintprog(Vt,A,b,Aeq1,Beq1,xb0,options);

[12] Para ampliar más la información sobre las herramientas implementadas en la solución de problemas de optimización se puede consultar la ayuda del toolbox de optimización 3.1 que ofrece MATLAB [7].

4.3.2. Programación Realizada. Teniendo en cuenta tanto el tipo de variables formuladas en la metodología, como la forma de entrada de datos para las herramientas del toolbox de optimización, lo primero que se hizo fue armar los vectores y las matrices de la función objetivo del subproblema, así como las restricciones del subproblema y problema principal a partir de los datos necesarios de entrada requeridos del sistema, que son las constantes[13] del subproblema, asumiendo todos los valores iniciales de variables binarias como cero.

Con este grupo de restricciones y la función objetivo se resuelve el problema de minimización lineal con la ayuda de la función "*linprog*" y se reservan los resultados tanto del valor de la minimización al que se le asigna el nombre de gama "γ", y que dará la pauta para seleccionar el resultado óptimo del modelo completo, como los valores de las variables "*x*" correspondientes a las variables del subproblema, que son las potencias generadas, las pérdidas, las potencias por las líneas y ángulos en los nodos.

Con estos valores se construyen los valores de atracción[14] de cada componente binaria "*Vl, Vi, Vs, Vg*", los cuales se guardan para posteriormente formar el vector de coeficientes de la función objetivo del problema principal, que es una maximización de tipo lineal binario. Utilizando esta última función objetivo y las restricciones ya construidas para el problema principal, se resuelve la maximización de tipo lineal binario con la ayuda de la función "*bintprog*".

Finalmente se utilizan los resultados obtenidos de las variables "x1" para crear una nueva restricción del problema principal que garantice la no repetición de esta solución en futuras iteraciones, y se modifican las restricciones del subproblema para empezar nuevamente el proceso ya descrito. Esto se logra fácilmente con la ayuda de un ciclo "*while*", que está condicionado por dos posibles eventualidades que son: que se cumpla el número máximo de iteraciones "*T*" o que la solución del problema principal no sea factible.

4.3.3. Toolbox de Análisis de Vulnerabilidad de Sistemas de Potencia (AVSP). En esta investigación se desarrolló un toolbox en MATLAB con el objetivo de facilitar tanto el ingreso de los datos del sistema de potencia que se desea estudiar, como el análisis de los resultados obtenidos de las simulaciones,

[13] Estas constantes se nombran el la "Tabla 2.1. Descripción de variables y constantes dependiendo del modelo".
[14] Valores que hacen a una componente más atractiva que a otra dependiendo de la cantidad de potencia que maneje.

ya que éste muestra de una manera ordenada y sencilla los resultados; también muestra en un cuadro de Excel un reporte completo de la simulación.
Además permite seccionar la metodología que se quiere usar para analizar la vulnerabilidad del sistema, las metodologías con las cuales se puede hacer este análisis son las siguientes:

- *Algoritmo VEGA 1.0*. Realiza el análisis de la vulnerabilidad utilizando la metodología original propuesta en el proyecto VEGA 1.0.

- *Algoritmo VEGA 1.0 modificado*. Realiza el análisis de la vulnerabilidad utilizando la metodología del proyecto VEGA 1.0 incluyendo la modificación propuesta en la sección 2.1.2, ecuación (2-11').

- *Algoritmo AVSP*. Realiza el análisis de la vulnerabilidad considerando el recurso de protección, esta metodología se muestra más detalladamente en capítulo 6.

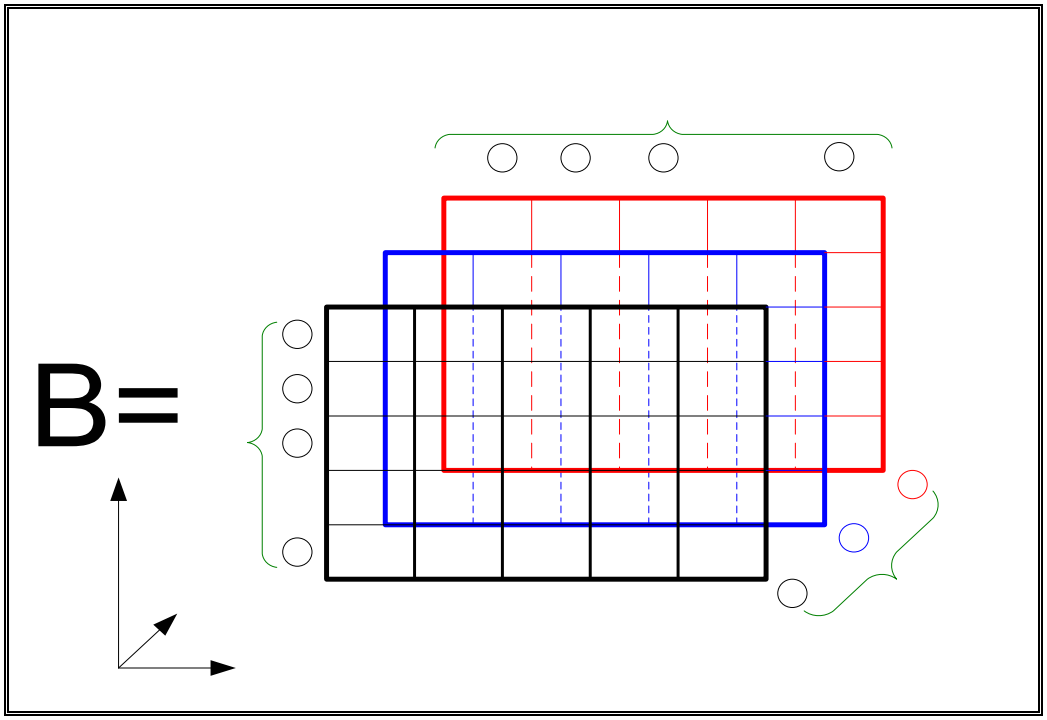
Una copia de este toolbox está anexada en el CD ROM del proyecto.

4.3.4. Ingreso de datos necesarios del sistema. Los datos que se necesitan para la modelación son los que en este documento se denominaron "constantes del subproblema". Además de que estos valores son necesarios para la formulación de la metodología, también se requiere información adicional de estos, como su ubicación dentro del sistema. Por esta razón se plantea una forma de entrada de estos valores a la programación realizada con la finalidad de poder realizar la formulación de la metodología. A continuación se ilustra la forma como se deben ingresar estos datos:

- **Susceptancias de las líneas (B_l).** La forma en que se deben ingresar al programa los valores de susceptancia de las líneas debe permitir asociar cada valor con una línea específica así como su ubicación dentro del sistema, o si existe una línea que se encuentre en paralelo a ésta. Puesto que los transformadores en esta modelación se asumen como líneas y también se debe tener en cuenta a qué subestación están conectados estos, se planteó una matriz tridimensional en la cual se contienen los valores de las susceptancias y al mismo tiempo sirve para extraer la información adicional que se requiere de las líneas.

  Para aclarar la forma como se debe construir la matriz de susceptancias, se ilustra en la figura 4.1:

Figura 4.1. Construcción de la matriz de susceptancias



Esta matriz tiene tres niveles a lo largo de la dimensión *Z* marcados con los números 1, 2 y 3 de color negro, azul y rojo respectivamente, es decir, una matriz tridimensional formada por tres matrices cuadradas de dos dimensiones ***nxn*** en cada uno de los niveles, donde ***n*** es el número de nodos. En el primer nivel se sitúan los valores de las susceptancias de las líneas o transformadores en la posición que corresponda al nodo de origen (columna) y nodo de destino (fila), por ejemplo, el valor de la susceptancia que tendría una línea que va del nodo 1 al nodo 2 se ubica en el primer nivel en la intersección de la columna 1 con la fila 2 y viceversa.

De igual forma se ubican los valores de las susceptancias de las líneas o transformadores que estén en paralelo, que vayan desde el mismo nodo de origen hasta mismo nodo de destino. Finalmente en tercer nivel se pone el número de la subestación a la que pertenece cada transformador representado por una línea.

- **Potencias máximas generadas ($\overline{P}_g^{Gen}$).** Estos valores son necesarios para restringir el máximo valor de potencia que puede generar una unidad generadora. Al ingresar estos datos al programa es importante también

darle una ubicación dentro del sistema a cada unidad generadora, es decir, al nodo al cual se conecta. Para esto se crea una matriz de dos columnas por *m* filas, donde *m* es el número total de unidades generadoras con que cuenta el sistema; en cada una de las filas se pone el valor máximo de potencia que puede generar la unidad generadora y el nodo al cual esta conectada.

- **Costos de generación (h_g).** Estos valores hacen parte de los coeficientes del vector de la función objetivo, debe existir un costo para cada unidad generadora, es decir, se ingresa al programa un vector de *1xm* donde *m* es el número total de unidades generadoras. La ubicación de cada uno de los costos dentro del vector corresponde a la ubicación de cada variable del subproblema asociada a la potencia generada.

- **Demandas del sistema (d_{ic}).** Estos valores determinan la carga total del sistema. Como en el caso de las potencias máximas generadas, también es necesario relacionar el consumo de cada nodo con su ubicación; para esto se crea una matriz de dos columnas por *p* filas, donde *p* es el número total de nodos con carga, en cada una de las filas se pone el valor de la demanda del nodo y el número del nodo.

- **Costo de carga no satisfecha (f_{ic}).** Estos valores también hacen parte de los coeficientes del vector de la función objetivo, debe existir un costo para cada demanda en cada nodo, entonces, se ingresa al programa un vector de *1xq* donde *q* es el número total de demandas asociadas con un nodo determinado. La ubicación de cada uno de los costos dentro del vector corresponde a la ubicación de cada variable del subproblema asociada a la demanda insatisfecha.

- **Capacidad de potencia máxima en las líneas ($\overline{P}_l^{Line}$).** Se crea un vector en el cual se ubica cada una de las potencias máximas de las líneas en orden ascendente dependiendo de su configuración, de tal forma que en cada posición debe estar el valor de la potencia máxima que le corresponde a cada línea.

En el capítulo 5 se muestran ejemplos que incluyen el ingreso de los datos necesarios del sistema.

5. RESULTADOS OBTENIDOS

En este capítulo, primero se muestran los resultados obtenidos en el sistema de prueba mencionado, *sistema Salle-06* que se planteó para efectos netamente académicos.

Este sistema es muy sencillo y permite analizar fácilmente su comportamiento ante diferentes ataques, también permite visualizar el comportamiento de la modelación con la modificación de la restricción (2-11) planteada en esta investigación, con el fin de poder comparar los efectos que ésta tendría con respecto a la modelación original del proyecto *VEGA 1.0*.

Además, se presentan los resultados arrojados en las simulaciones realizadas al caso de prueba IEEE RST-96 [8] con la programación que se hizo en esta investigación, así mismo se compararán los resultados obtenidos por los autores del proyecto *VEGA 1.0* para el mismo caso de prueba. Estos resultados fueron consultados en la referencia [2].

5.1. SISTEMA DE POTENCIA *SALLE-06*

Las características del sistema de prueba planteado que se presenta en la figura 5.1 están orientadas a permitir un fácil análisis de los resultados obtenidos del modelo "*análisis de vulnerabilidad ante atentados terroristas*", e ilustrar el comportamiento del modelo modificado que se plantea en esta monografía; para esto se necesita tener generadores acoplados directamente a una subestación.

Otras características del sistema propuesto son: que sea un sistema pequeño y susceptible al más mínimo sabotaje.

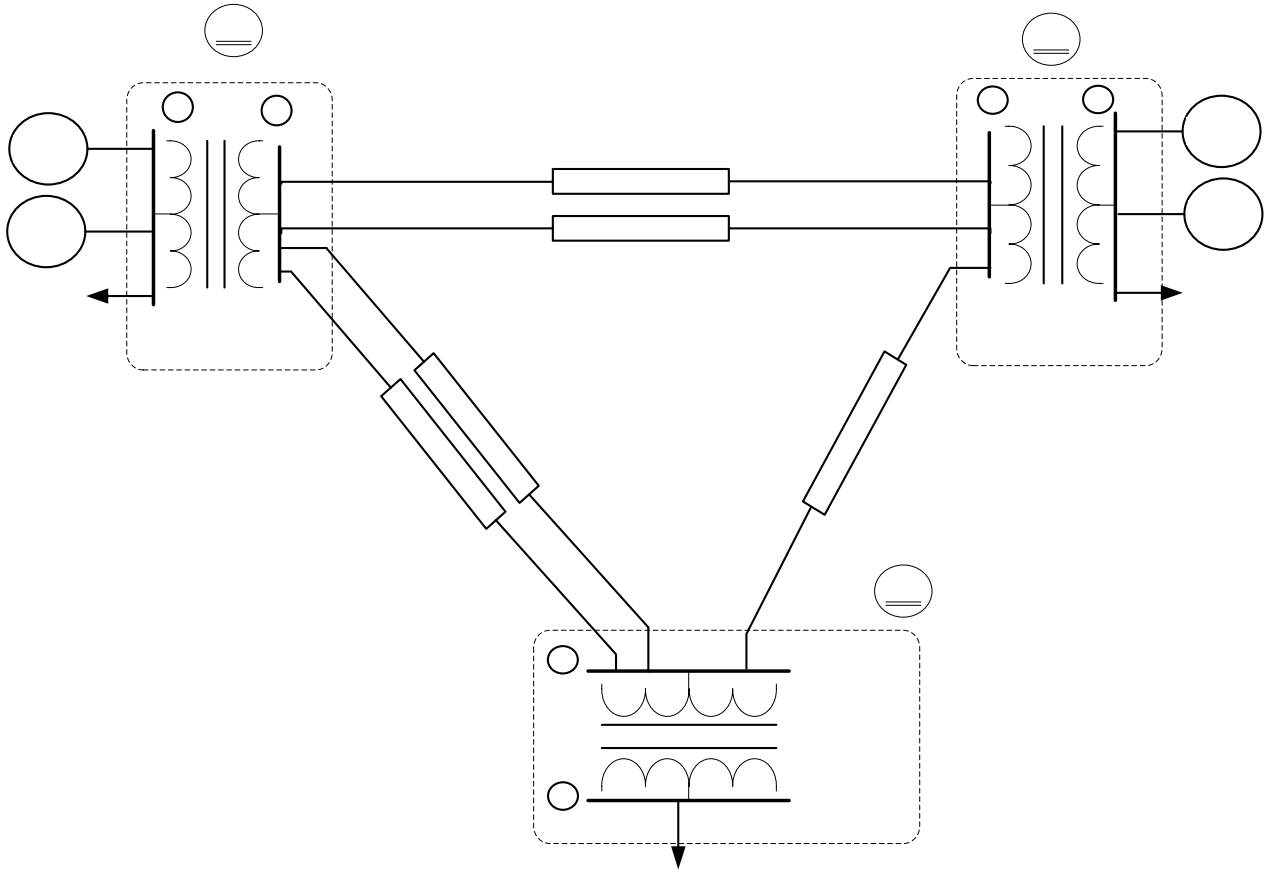
La figura 5.1 muestra la configuración del sistema con los respectivos valores de los datos a tener en cuenta en la programación. Un reporte completo de estos datos se muestra en la tabla 5.1.

Tabla 5.1. Datos del sistema de prueba *Salle-06*

Componente			Pot. Máxima	Costo	Susceptancia
Líneas	L 2-3		2 p.u	N/A	19,96 p.u
	L' 2-3		2 p.u	N/A	19,96 p.u
	L 2-5		2 p.u	N/A	19,96 p.u
	L' 2-5		2 p.u	N/A	19,96 p.u
	L 3-5		2 p.u	N/A	19,96 p.u
Subestaciones	S. 1	Tr. 1-2	2 p.u	N/A	6,67 p.u
		Dem. Bus 1	1 p.u	100 [$/kWh]	N/A
	S. 2	Tr. 3-4	2 p.u	N/A	6,67 p.u
		Dem. Bus 4	1,3 p.u	100 [$/kWh]	N/A
	S. 3	Tr. 5-6	3 p.u	N/A	6,67 p.u
		Dem. Bus 6	2,5 p.u	100 [$/kWh]	N/A
Generadores	Bus1	G 1-1	2,5 p.u	5 [$/kWh]	N/A
		G 1-2	2 p.u	6 [$/kWh]	N/A
	Bus4	G 2-1	3 p.u	7 [$/kWh]	N/A
		G 2-2	1,5 p.u	8 [$/kWh]	N/A

Tr. Transformadores
Dem. Demanda
L. Línea
L'. Línea en paralelo
N/A. No Aplica

Figura 5.1. Esquema sistema de potencia *Salle-06*



Se debe crear un archivo "**.mat* "que contenga la información del sistema, es decir, las matrices y vectores (consultar sección 4.3.4), para posteriormente cargar el sistema al toolbox. A continuación se muestra la forma como se introducen los datos del sistema de prueba al programa. Cabe anotar que los nombres de las matrices y vectores deben ser iguales a los que se muestran en la figura 5.2 para cualquier sistema, y no se deben incluir comentarios, aunque en la figura 5.2 se muestran comentarios, estos tienen la finalidad de ilustrar cada una de las matrices y vectores que conforman los datos de entrada del sistema *Salle-06*.

Figura 5.2. Forma de Introducir los datos del sistema al programa

```
% Matriz de Susceptancias
B(:,:,1)=[ 0          6.67       0          0          0          0
           0          0          19.96      0          19.96      0
           0          0          0          6.67       19.96      0
           0          0          0          0          0          0
           0          0          0          0          0          6.67
           0          0          0          0          0          0];

B(:,:,2)=[ 0          0          0          0          0          0
           0          0          19.96      0          19.96      0
           0          0          0          0          0          0
           0          0          0          0          0          0
           0          0          0          0          0          0
           0          0          0          0          0          0];

 B(:,:,3)=[ 0          1          0          0          0          0
            0          0          0          0          0          0
            0          0          0          2          0          0
            0          0          0          0          0          0
            0          0          0          0          0          3
            0          0          0          0          0          0];
% Matriz de Potencias máximas generadas
Pg=[2.5,1;2,1;3,4;1.5,4];   % CONSTANTE
% Matriz de Demandas en los nodos
dic=[1,1;1.3,4;2.5,6]; % CONSTANTE
Plmax=[2;2;2;2;2;3;2;2]; %CONSTANTE
%vector de costos de Generación
hg=[5,5,5,5]; % CONSTANTE
%Vector de costos de carga no satisfecha
fic=ones(size(dic(:,1)'))*20; %CONSTANTE
```

5.1.1. Análisis de los resultados obtenidos en el sistema de prueba *Salle-06*. A continuación se muestran los resultados obtenidos y se hace una comparación de estos, utilizando primero la modelación original desarrollada en el proyecto *VEGA 1.0* y posteriormente la modelación con la modificación planteada.

Tabla 5.2. Resultados para recursos de ataque *M=2* y *M=3*

Recurso de ataque (*M*)	Algoritmo	Nodos			Líneas				Subestaciones	
		Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
2	VEGA 1,0	1	0	0	1	2	0,0571 p.u	0	1	0
		2	0	0	2	3	0,0286 p.u	0	2	0
		3	0	0	2	5	0	1	3	0
		4	0	0	3	4	0,0571 p.u	0		
		5	0	0	3	5	0	1		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0,0286 p.u	0		
					2	5	0	0		
	VEGA 1,0 Modificado	1	0	0	1	2	0,0571 p.u	0	1	0
		2	0	0	2	3	0,0286 p.u	0	2	0
		3	0	0	2	5	0	1	3	0
		4	0	0	3	4	0,0571 p.u	0		
		5	0	0	3	5	0	1		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0,0286 p.u	0		
					2	5	0	0		
3	VEGA 1,0	1	0	0	1	2	0,0578 p.u	0	1	0
		2	0	0	2	3	0,0289 p.u	0	2	0
		3	0	0	2	5	0	0	3	1
		4	0	0	3	4	0,0578 p.u	0		
		5	0	0	3	5	0	0		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0,0289	0		
					2	5	0	0		
	VEGA 1,0 Modificado	1	0	0	1	2	0,0578 p.u	0	1	0
		2	0	0	2	3	0,0289 p.u	0	2	0
		3	0	0	2	5	0	0	3	1
		4	0	0	3	4	0,0578 p.u	0		
		5	0	0	3	5	0	0		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0,0289 p.u	0		
					2	5	0	0		

Tabla 5.3. Resultados para recursos de ataque *M=4* y *M=6*

Recurso de ataque (*M*)	Algoritmo	Nodos			Líneas				Subestaciones	
		Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
4	VEGA 1,0	1	0	0	1	2	0	0	1	0
		2	0	0	2	3	0	1	2	0
		3	0	0	2	5	0	1	3	0
		4	0	0	3	4	0	0		
		5	0	0	3	5	0	1		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0	0		
					2	5	0	0		
	VEGA 1,0 Modificado	1	0	0	1	2	0	0	1	0
		2	0	0	2	3	0	0	2	1
		3	0	0	2	5	0	1	3	0
		4	1,3	0	3	4	0	0		
		5	0	0	3	5	0	0		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	3,8 p.u.		2	3	0	0		
					2	5	0	0		
6	VEGA 1,0	1	0	0	1	2	0	0	1	1
		2	0	0	2	3	0	0	2	1
		3	0	0	2	5	0	0	3	0
		4	0	0	3	4	0	0		
		5	0	0	3	5	0	0		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	2,5 p.u.		2	3	0	0		
					2	5	0	0		
	VEGA 1,0 Modificado	1	1 p.u.	0	1	2	0	0	1	1
		2	0	0	2	3	0	0	2	1
		3	0	0	2	5	0	0	3	0
		4	1,3 p.u.	0	3	4	0	0		
		5	0	0	3	5	0	0		
		6	2,5 p.u.	0	5	6	0	0		
		Total Pérdidas	4,8 p.u.		2	3	0	0		
					2	5	0	0		

Cuando hay un recurso de ataque *M=2* los resultados obtenidos utilizando el algoritmo *VEGA 1.0* son totalmente iguales a los resultados obtenidos con el algoritmo *VEGA 1.0 modificado*. Esto se debe a que el recurso de ataque (*M*) no

es suficiente para atacar nodos ($M_i=5$) o subestaciones ($M_s=3$) y sólo alcanza para realizar un ataque en dos líneas ($M_l=2$). Como la diferencia entre el algoritmo modificado y el original se fundamenta en el efecto que tendría un ataque contra una subestación que tenga un generador conectado, en este caso no se puede distinguir la diferencia entre los dos algoritmos.

Pero cuando el recurso es *M=3*, es suficiente para atacar una subestación. La razón por la que se obtuvieron resultados iguales en los dos algoritmos es, que el plan de ataque más nocivo para este recurso afecta una subestación sin un generador conectado.

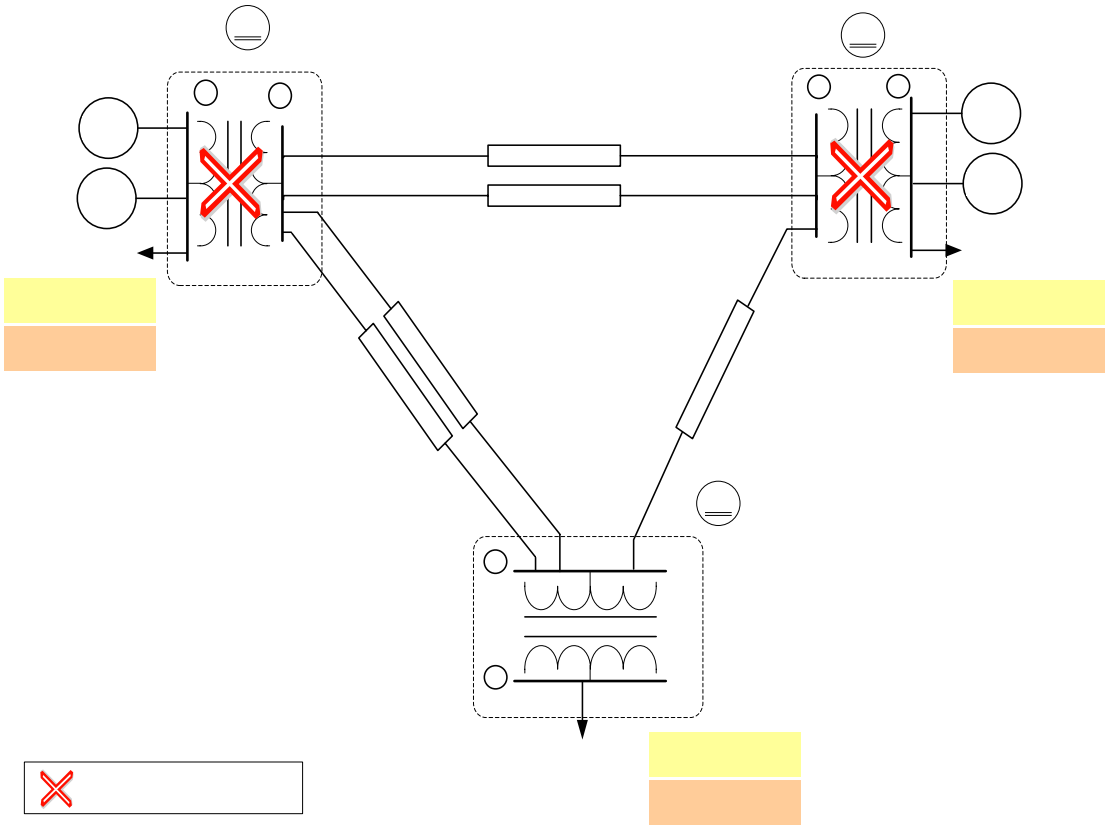
Se puede apreciar que con un recurso de ataque *M=4*, el algoritmo *VEGA 1.0 modificado* encuentra más atractivo realizar un ataque en la subestación 2 y la línea que conecta el nodo 2 con el nodo 5. Esto logra producir pérdidas de 3.8p.u., a diferencia de la simulación realizada con la metodología original que no encuentra atractiva ninguna subestación para un ataque, por no considerar la desconexión de los generadores acoplados directamente a estas, en este caso las pérdidas son de 2.5 p.u.

Los resultados de ataque obtenidos para un recurso terrorista *M=6* son los mismos ataques para las dos metodologías, como se muestra en la figura 5.2, pero las pérdidas de potencia varían dependiendo de la modelación utilizada.

Las pérdidas obtenidas con el algoritmo modificado son mayores al considerar la desconexión de los generadores conectados a las subestaciones 1 y 2, por esta razón hay pérdidas en los nodos 1, 4 y 6, a diferencia de las pérdidas obtenidas con el algoritmo original que sólo se presentan en el nodo 6.

Es importante aclarar, que estos resultados están determinados por la configuración del sistema.

Figura 5.2. Ataque óptimo para un recurso terrorista *M=6*



5.2. SISTEMA DE PRUEBA IEEE RTS-96

El sistema de confiabilidad IEEE RTS-96 realmente consta de tres áreas: el sistema completo tiene 73 nodos, 120 líneas y 96 unidades de generación con una capacidad de generación total de 10.215 MW (3.405 MW en cada área) para una carga pico total de 8.550 MW (2.850 MW en cada área).

Se hizo la simulación del algoritmo modificado solamente tomado la primera área de este sistema de prueba (24 nodos, 2 subestaciones, 38 líneas y 33 generadores), para ser comparada con los resultados mostrados en el artículo [2].

Los valores de los datos del sistema para correrlos en la programación realizada, se pueden consultar en los anexos A-D.

Figura 5.3. Esquema sistema de prueba IEEE RTS-96

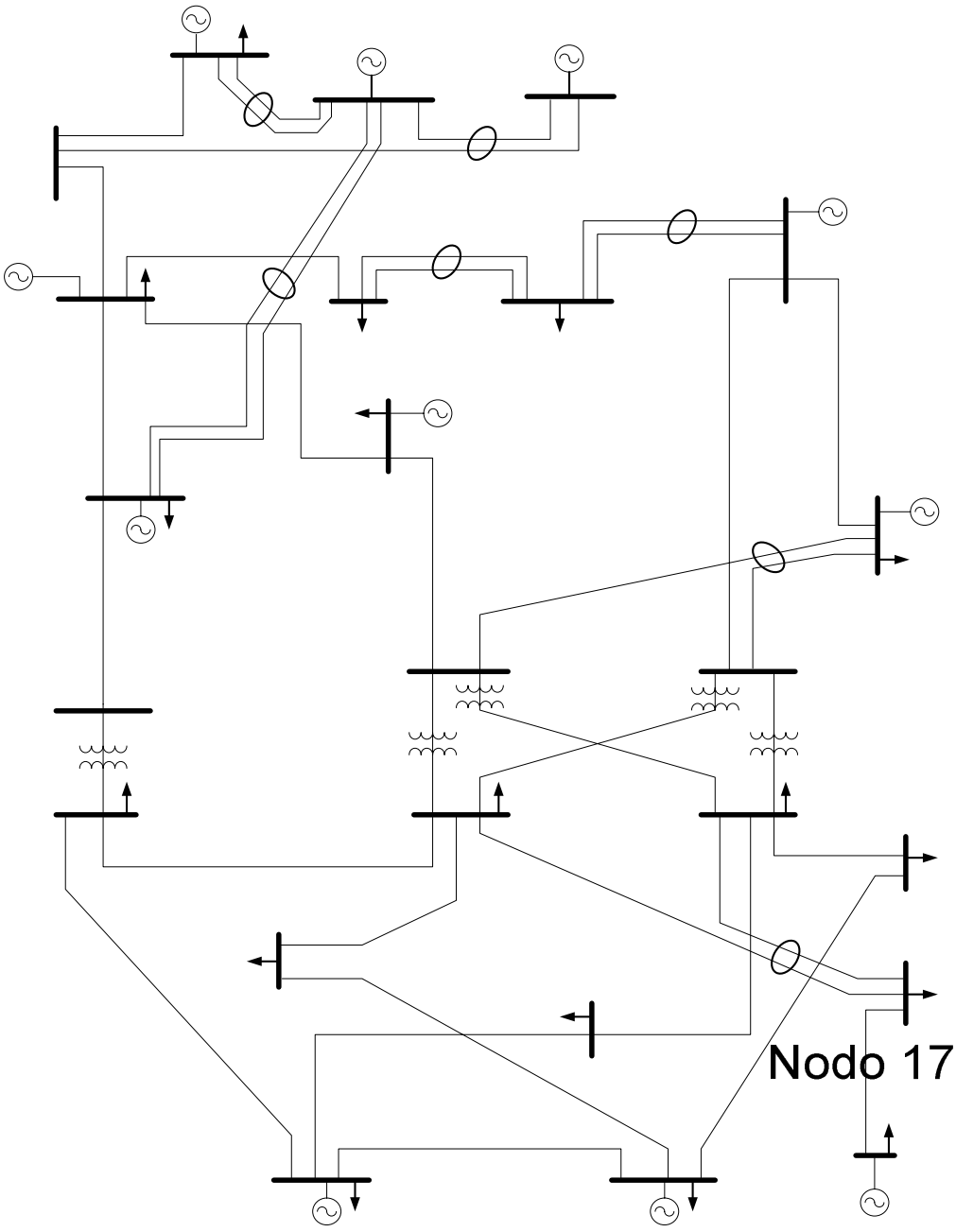


Figure 1 - IEEE One Area RTS-96. “The IEEE Reliability Test System – 1996”. A report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee”. IEEE Transactions on Power Systems, Vol. 14, No. 3, August 1999 [8].

Los datos se introducen al sistema de la misma forma como en el sistema de prueba *Salle-06*. Adicional a estos datos, este sistema tiene líneas en paralelo que no tienen el mismo nodo de destino o de origen (ver figura 5.3, representado por círculos con las letras *A, E* y *F*). Los pasos a seguir para introducir la información de las líneas en paralelo anteriormente mencionadas son:

- Crear una matriz de ceros con dimensión *(n,n)* donde *n* es el número total de líneas (38), con el nombre *delL*.

- Darle el valor de 1 a los elementos de la intersección de la fila y la columna que representa cada par de líneas en paralelo, por ejemplo para el caso de las líneas en paralelo *F* (líneas 12 y 13, como se muestra en los anexos A-D).

```
delL=zeros(38,38);
delL(18,20)=1; delL(20,18)=1;  →(E)
delL(12,13)=1; delL(13,12)=1;  → (F)
delL(30,34)=1; delL(34,30)=1;  → (A)
```

5.2.1. Análisis y comparación de resultados sistema de prueba IEEE RTS-96. Se hace una comparación de los resultados conseguidos de la programación realizada en esta investigación por medio de la herramienta computacional Toolbox Optimization 3.1 (MATLAB) con los resultados consultados en artículo [2], para el caso 1 (área 1) con un recurso de *M=6*.

Para la simulación de este sistema se muestra solamente el *algoritmo VEGA 1.0* porque su configuración física no cuenta con generadores conectados directamente a las subestaciones. Razón por la cual los resultados del algoritmo *VEGA 1.0 modificado* no varían con respecto a los del *algoritmo VEGA 1.0*.

En la tabla 5.4 se observan los resultados de la simulación para un *M=6*, al lado izquierdo se encuentran los resultados obtenidos con el Toolbox AVSP y al lado derecho se encuentran los resultados extraídos de la referencia [2], estos dos grupos de resultados tienen los mismos valores.

Tabla 5.4. Comparación de resultados sistema de prueba IEEE RTS-96

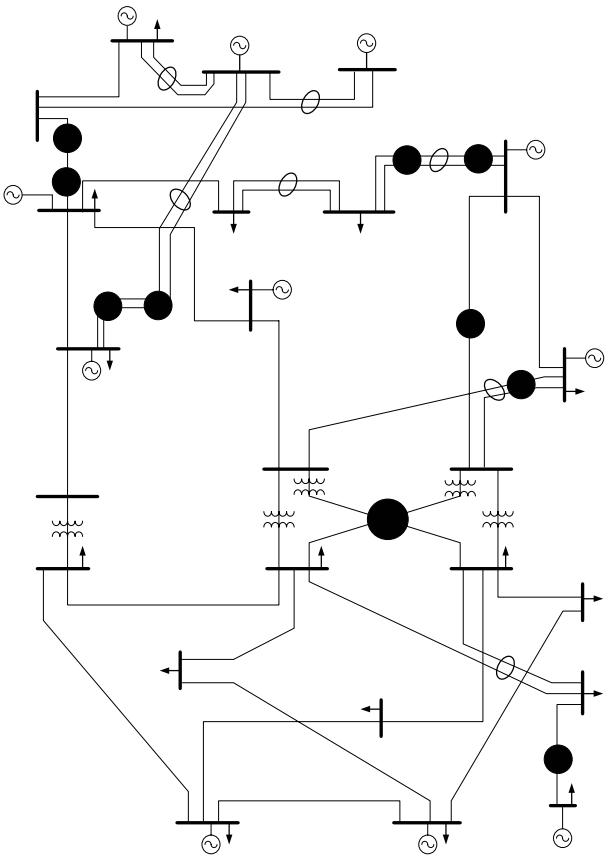
Resultados obtenidos simulación

Nodo	Pérdida (MW)	Ataques PLAN 2		
		Línea		Sub
1	53,59	Origen	Destino	
2	47,96	7	8	
3	114,69	11	13	
4	51,82	12	23	0
5	50,43	15	21	
6	93,47	16	17	
7	0	20	23	
8	128,48	**Ataques PLAN 1**		
9	123,41	**Línea**		**Sub**
10	135,4	Origen	Destino	
13	0	15	21	
14	133,07	16	17	2
15	150,65	20	23	
16	64,4			
18	0			
19	127,4			
20	98,22			
Total:	1372,99			

Este grupo de resultados se obtiene haciendo invulnerables las subestaciones, en un número de iteraciones t=182.

Cuando se consideran vulnerables las subestaciones se alcanzan resultados de ataque iguales al plan 1 en un número de iteraciones t=37.

Resultados extraídos del artículo



"*Analysis of Electric Grid Security Under Terrorist Threat"*, IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 19, NO. 2, MAY [2].

Dos planes de interdicción (representados por 1 y 2) para RTS1 (área 1 sistema RTS-96) usando $M = 6$.
La carga total es 2850 MW. El plan 1 produce una demanda no satisfecha de 1258 MW y el plan produce una demanda no satisfecha de 1373 MW.
El "número 1 grande" indica que los cuatro transformadores y nodos en la subestación están interdictos.

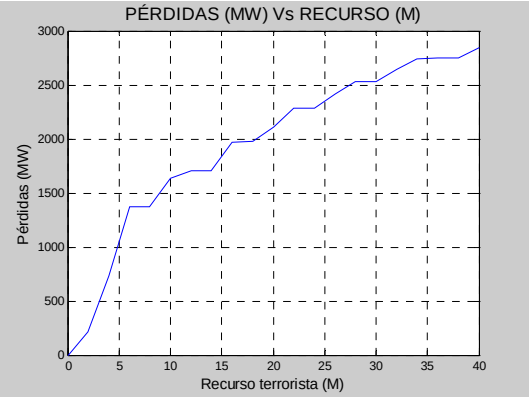
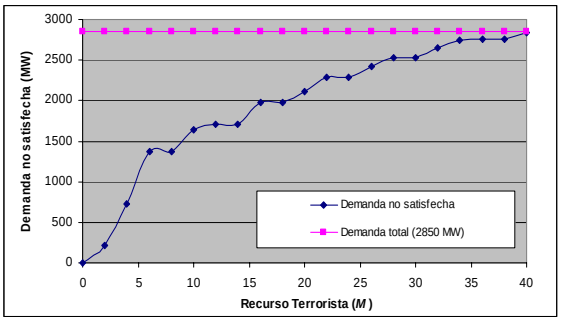
Los resultados obtenidos en el *plan 2* pueden conseguirse sin necesidad de hacer inatacables las subestaciones. Se presume que para esto se necesitaría un número mayor de iteraciones, ya que la herramienta computacional utilizada no es

eficiente para la solución de problemas con demasiadas variables, por esta razón tarda demasiado tiempo en encontrar este plan de ataque.

Esto se debe a que el sistema es notablemente más grande que el sistema de prueba *Salle-06*. Asimismo los autores no hacen claridad sobre la forma en que consiguieron llegar a estos dos planes de ataque.

Igualmente se comparó la tendencia de las pérdidas con respecto al recurso terrorista por medio de una gráfica, mostrada en la tabla 5.5.

Tabla 5.5. Comparación de gráficas de Pérdida vs. Recurso terrorista

Resultados obtenidos simulación	Resultados extraídos del artículo
	
	"*Analysis of Electric Grid Security Under Terrorist Threat*", IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 19, NO. 2, MAY [2].
	El deslastre de carga para el sistema RTS 96 área 1 en función del recurso terrorista *M* (número de atacantes), donde la carga total del área es de 2850 MW.

Al comparar las dos gráficas se puede observar una tendencia creciente aproximadamente exponencial en ambas gráficas, es decir, las pérdidas (demanda no satisfecha) son directamente proporcionales a la cantidad de recurso terrorista. Para recursos de ataque pequeños la curva presenta una pendiente grande en comparación con la pendiente cuando el recurso terrorista es mayor.

En este capítulo se mostró cómo la metodología objeto de estudio pudo ser exitosamente implementada usando MATLAB y el toolbox de optimización 3.1. Además, es necesario cambiar la restricción (2-11) para incluir un caso no considerado en el sistema de prueba IEEE RTS-96.

6. ANÁLISIS DE VULNERABILIDAD INCLUYENDO RECURSO DE PROTECCIÓN

Otro aporte que esta investigación hace al modelo de análisis de vulnerabilidad de los sistemas de potencia es introducir un nuevo objetivo, que consiste en agregarle al modelo una nueva consideración que pretende satisfacer la necesidad de protección del sistema ante posibles ataques.

6.1. MODELO DE PROTECCIÓN

El propósito de este modelo es establecer cuál o cuáles serían las componentes más críticas del sistema que se podrían proteger ante un plan de ataque determinado por un recurso de interdicción específico, claro está contando con el recurso necesario para protegerlo, es decir, utilizar el recurso del que se disponga para la protección del sistema de manera óptima. Para realizar una protección adecuada se debe tener en cuenta las siguientes consideraciones:

- *Componentes a proteger.* Estas son las líneas, nodos, transformadores, o subestaciones, que bajo unas condiciones de ataque determinadas serían afectadas directamente.

- *Componentes protegidas.* Son las componentes del sistema que como resultado de correr el modelo, estarán protegidas.

- *Líneas Protegidas.* Si una línea es protegida, todas las líneas que se encuentren físicamente en paralelo también lo estarán, siempre y cuando estas estén sostenidas en la misma estructura.

- *Subestaciones protegidas.* Todos los nodos y transformadores que hagan parte de la subestación protegida también estarán protegidos.

Las restricciones del modelo relacionadas con el recurso de protección deberán ser determinadas por información de los grupos de inteligencia militar, para el caso Colombiano, el ejercito Nacional, DAS, F2, SIJIN, etc. Pero esto sería el objeto de investigaciones futuras que tendrían que involucrar diferentes disciplinas. Por esta razón, y para propósitos de demostración, se adoptó el mismo modelo de restricción que el proyecto *VEGA 1.0* plantea para el caso del recurso de ataque.

En este orden de ideas se plantean los siguientes parámetros adicionales requeridos para el modelo de protección:

- $\mathrm{Pr}_g^{Gen}, \mathrm{Pr}_l^{Line}, \mathrm{Pr}_i^{Bus}, \mathrm{Pr}_s^{Sub}$ **:** Recurso en unidades de protección de la fuerza pública o privada necesario para proteger el generador g, la línea l, el nodo i o la subestación s, respectivamente.

- Pr : Recurso total disponible para la protección de la infraestructura eléctrica, también en unidades de protección.

La forma en que se plantea optimizar el recurso de protección en esta investigación, es maximizando la pérdida de capacidad del sistema únicamente en función de las componentes más críticas (componentes a proteger) para un panorama específico, ósea, las componentes del sistema que serían más atractivas desde el punto de vista de un ataque óptimo, limitado por el recurso disponible para la protección.

Lo anterior busca determinar las componentes del sistema que son más importantes de proteger. A continuación se muestra el planteamiento matemático del modelo de protección.

$$\max_{\substack{\delta Gen,\delta Line,\\ \delta Bus,\delta Sub}} \sum_{g\in \mathrm{I}^*} V_g{}^{Gen}\delta_g^{Gen} + \sum_{l\in L^*} V_l{}^{Line}\delta_l^{Line} + \sum_{i\in I^*} V_i{}^{Gen}\delta_i^{Gen} + \sum_{s\in S^*} V_s{}^{Sub}\delta_s^{Sub} \tag{6-1}$$

Sujeto a:

$$\sum_{g\in G^*} \mathrm{Pr}_g^{Gen} + \sum_{l\in L^*} \mathrm{Pr}_l^{Line}\ \delta_l^{Line} + \sum_{i\in I^*} \mathrm{Pr}_i^{Bus}\ \delta_i^{Bus} + \sum_{s\in S^*} \mathrm{Pr}_s^{Sub}\ \delta_s^{Sub} \le \mathrm{Pr} \tag{6-2}$$

$$\delta_i^{t,ileso} = 0 \qquad \forall\ i \tag{6-3}$$

$$\delta_g^{t,ileso} = 0 \qquad \forall\ g \tag{6-4}$$

$$\delta_l^{t,ileso} = 0 \qquad \forall\ l \tag{6-5}$$

$$\delta_s^{t,ileso} = 0 \qquad \forall\ s \tag{6-6}$$

La ecuación (6-1) es la función objetivo y es la misma utilizada para el problema principal en cada iteración. La restricción (6-2) se encarga de garantizar que el

recurso utilizado en proteger al sistema no exceda el recurso total disponible (*Pr*). Las restricciones (6-3) a (6-6), garantizan que no sea protegido un componente del sistema que no sea atractivo $\delta^{t,ileso} = \left(\delta_i^{t,ileso}, \delta_g^{t,ileso}, \delta_l^{t,ileso}, \delta_s^{t,ileso}\right)$, es decir, que sólo se puedan proteger los componentes del sistema más críticos en cada iteración.

6.2. MODELO COMPLETO INCLUYENDO PROTECCIÓN DEL SISTEMA

Podría considerarse que el modelo es prácticamente el mismo que se utilizó para determinar el ataque más disruptivo, sólo que al adicionarle la protección el modelo se extiende un poco de la siguiente manera.

En cada iteración se determina el ataque más disruptivo, de la misma manera que se ha venido haciendo hasta ahora. Luego se utilizan los resultados obtenidos en el problema principal para construir las restricciones (6-3) a (6-6), del modelo de protección y con estas se determina cuál o cuáles serían las componentes a proteger del sistema $\delta^{t,\Pr ot} = \left(\delta_i^{t,\Pr ot}, \delta_g^{t,\Pr ot}, \delta_l^{t,\Pr ot}, \delta_s^{t,\Pr ot}\right)$ en esta iteración.

Continúa el proceso iterativo hasta determinar el conjunto de ataques más disruptivos con su respectivo grupo de componentes más críticas a proteger.

Finalmente se protegen estas componentes, es decir, se modifica la restricción (2-20) y se obtiene el análisis de vulnerabilidad bajo estas condiciones (con las componentes más críticas protegidas) pero esta vez con el modelo *VEGA 1.0 modificado*.

El resultado que se obtiene de este proceso son las componentes que se deben proteger para utilizar el recurso de protección de la manera óptima y las pérdidas del sistema bajo un ataque con las condiciones de protección.

6.2.1. Algoritmo del modelo incluyendo protección. A continuación se describe el algoritmo del modelo completo.

- *Inicio del problema:*
    - Se establece como plan de ataque inicial

      $\hat{\delta}^1 = \left(\hat{\delta}^{Gen,1}, \hat{\delta}^{Line,1}, \hat{\delta}^{Bus,1}, \hat{\delta}^{Sub,1}\right) \leftarrow (0,0,0,0)$,
      $\delta^{t,\Pr ot,t} \leftarrow (0)$, las componentes iniciales más críticas a proteger.

- Se nomina el plan de ataque más disruptivo hasta ahora, y, $\hat{\Delta}^1 \leftarrow \left\{\hat{\delta}^1\right\}$
- Se establece como el costo del mejor plan hasta ahora $\gamma^* \leftarrow 0$.
- Se le da el primer valor a *t* (numero de iteración) $t \leftarrow 1$.

- *Se resuelve el subproblema:*
  - Se resuelve el flujo de potencia óptimo incluyendo variables de ataque con $\left(\hat{\delta}^t\right)$, para determinar, $\gamma\left(\hat{\delta}^t\right)$ y las constantes del problema principal $\hat{P}^t = \left(\hat{P}^{Line,t}, \hat{P}^{Gen,t}, \hat{S}^t, \hat{\theta}^t\right)$ necesarias para formar la función objetivo del problema principal.
  - Se compara el valor del costo obtenido con el del costo del plan de ataque más disruptivo hasta el momento para determinar, si $\gamma\left(\hat{\delta}^t\right) > \gamma^*$, entonces, $\gamma^* \leftarrow \gamma\left(\hat{\delta}^t\right)$, el nuevo costo del plan de ataque más disruptivo hasta el momento, $\hat{\delta}^* \leftarrow \hat{\delta}^t$, el nuevo plan de ataque más disruptivo hasta el momento y $\hat{\delta}^{*,prot} \leftarrow \hat{\delta}^{prot,t}$, las componentes más críticas a proteger .
  - Se revisa el número de iteraciones corridas hasta el momento y si es igual al número máximo establecido se detiene el proceso iterativo.

- *Se resuelve el problema principal:*
  - Se calculan los valores estimados usando $\hat{P}^{t'}, t' = 1..., t$ $V^t \equiv \left(V^{Gen,t}, V^{Line,t}, V^{Bus,t}, V^{Sub,t}\right) = \frac{1}{t}\sum_{t'=1}^{t}\left(V^{Gen,t'}, V^{Line,t'}, V^{Bus,t'}, V^{Sub,t'}\right)$ para formar la función objetivo del problema principal.
  - Se resuelve el problema principal $PP\left(V^t, \hat{\Delta}^t\right)$ para determinar $\hat{\delta}^{t+1}$, y si este no tiene una solución factible se detiene el proceso iterativo.

- Se guardan los resultados de $\hat{\delta}^{t+1}$ obtenidos en el conjunto de resultados $\hat{\Delta}^{t+1} \leftarrow \hat{\Delta}^{t} \cup \left\{\hat{\delta}^{t+1}\right\}$.

- Se generan las restricciones del problema de protección utilizando $\hat{\delta}^{t+1}$.

- *Se resuelve el problema de protección:*

  - Para esto se utiliza la misma función objetivo del problema principal de esta iteración

$$\max_{\substack{\delta Gen,\delta Line,\\ \delta Bus,\delta Sub}} \sum_{g\in\Gamma^{*}} V_g^{\,Gen}\delta_g^{Gen} + \sum_{l\in L^{*}} V_l^{\,Line}\delta_l^{Line} + \sum_{i\in I^{*}} V_i^{\,Gen}\delta_i^{Gen} + \sum_{s\in S^{*}} V_s^{\,Sub}\delta_s^{Sub},$$

    para determinar los componentes del sistema a proteger $\delta^{t,\mathrm{Pr}ot}$, en la siguiente iteración.

  - Se incrementa en uno el valor de $t \leftarrow t+1$.

  - Se retorna al subproblema continúa el proceso iterativo.

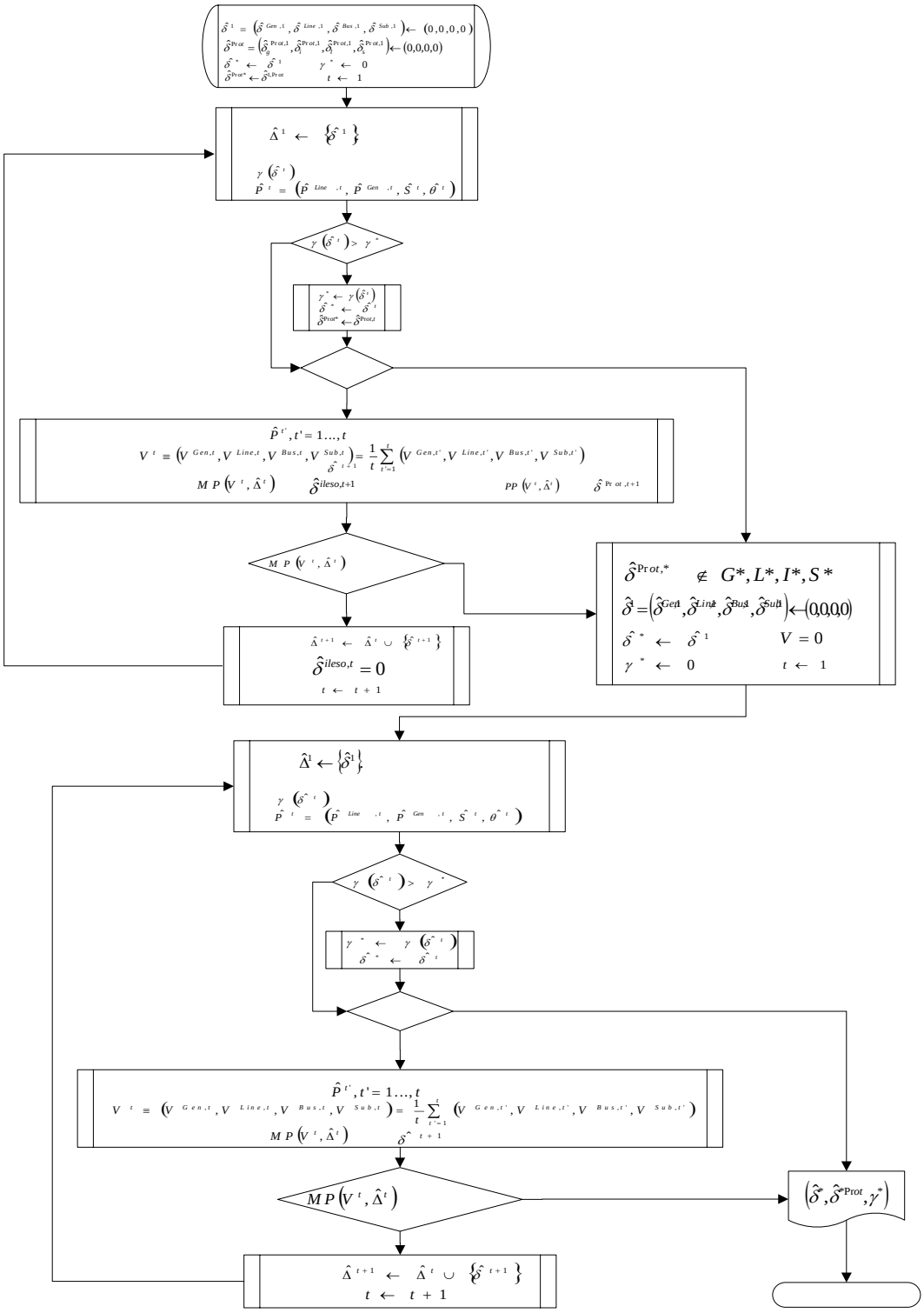
- *Al finalizar el modelo se realiza el análisis de vulnerabilidad del sistema:*

  - Primero se hacen invulnerables las componentes más críticas a proteger, es decir, se hace $\delta^{*,\mathrm{Pr}ot} = 0$.

  - Se ejecuta la modelación original con las componentes más críticas protegidas.

Un diagrama de flujo de este algoritmo se ilustra en la figura 6.1.

Figura. 6.1. Diagrama de flujo Algoritmo del modelo incluyendo protección



6.3. SIMULACIÓN Y ANÁLISIS DE RESULTADOS

A continuación se muestra una simulación utilizando el modelo que incluye protección, en el sistema de prueba *Salle-06 con dos áreas*, donde cada área tiene una configuración igual a la que se trabajó en el capítulo 5 y están interconectadas por dos líneas, este sistema se ilustra en la figura 6.2 y un reporte completo de los valores de sus datos se pueden ver en la tabla 6.1.

La simulación se realizó bajo las mismas condiciones (recurso de ataque *M=12*), variando el recurso de protección y considerando que la cantidad de recurso necesario para proteger cada componente es igual a la que se necesita para atacarla:

($M_g^{Gen} = \mathrm{Pr}_g^{Gen}$, $M_l^{Line} = \mathrm{Pr}_l^{Line}$, $M_i^{Bus} = \mathrm{Pr}_i^{Bus}$, $M_s^{Sub} = \mathrm{Pr}_s^{Sub}$) . Esto se hizo para facilitar el análisis de resultados.

Figura 6.2. Esquema sistema de potencia S*alle- 06 con 2 áreas*

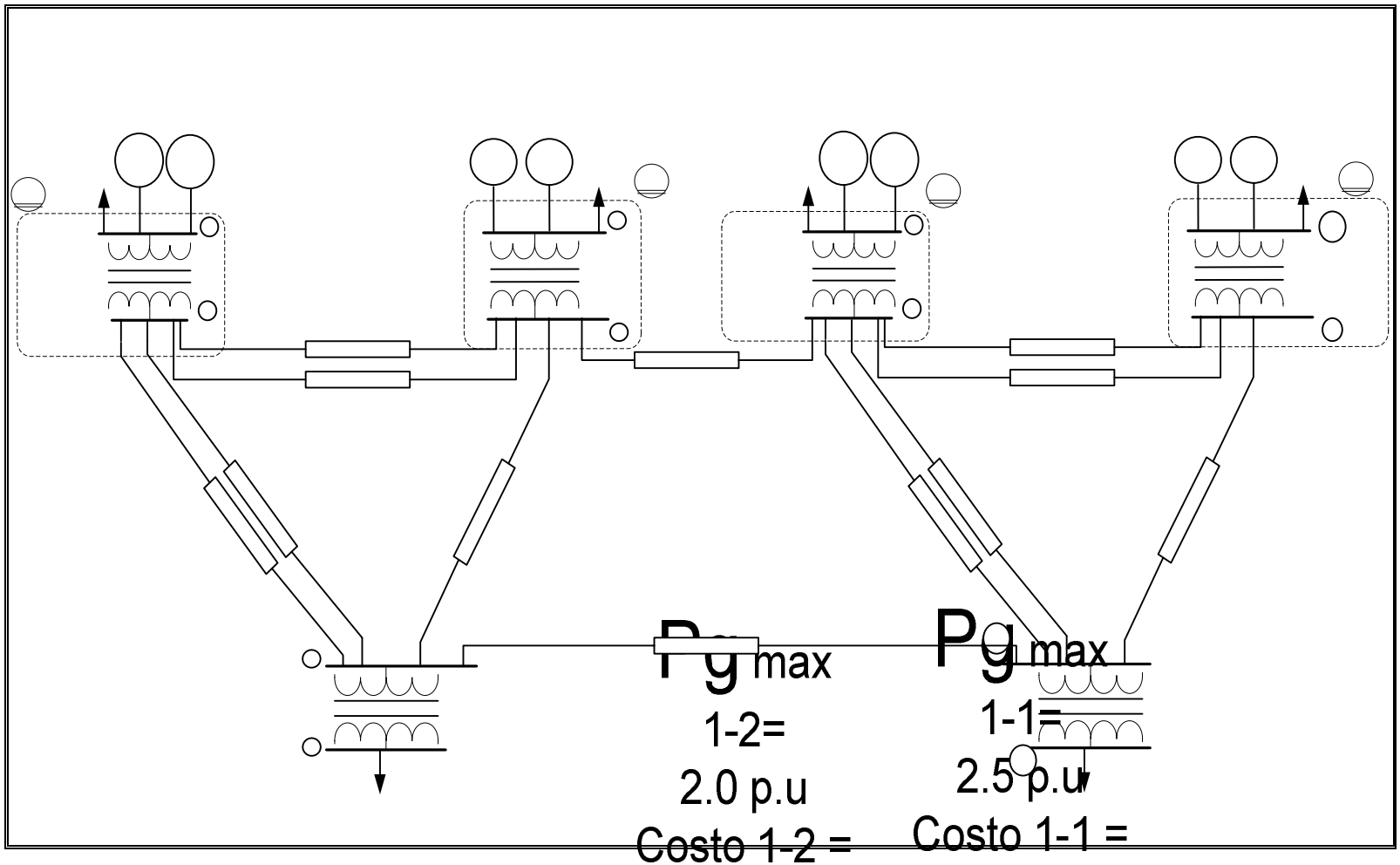


Tabla 6.1. Datos del sistema de prueba *Salle-06 con dos áreas*

Componente			Pot. Máxima	Costo	Susceptancia
Líneas	L 2-3		2 p.u	N/A	19,96 p.u
	L' 2-3		2 p.u	N/A	19,96 p.u
	L 2-5		2 p.u	N/A	19,96 p.u
	L' 2-5		2 p.u	N/A	19,96 p.u
	L 3-5		2 p.u	N/A	19,96 p.u
	L 3-8		2 p.u	N/A	19,96 p.u
	L 5-11		2 p.u	N/A	19,96 p.u
	L 8-9		2 p.u	N/A	19,96 p.u
	L’ 8-9		2 p.u	N/A	19,96 p.u
	L 8-11		2 p.u	N/A	19,96 p.u
	L’ 8-11		2 p.u	N/A	19,96 p.u
	L 9-11		2 p.u	N/A	19,96 p.u
Subestaciones	S. 1	Tr. 1-2	2 p.u	N/A	6,67 p.u
		Dem. Bus 1	1 p.u	100 [$/kWh]	N/A
	S. 2	Tr. 3-4	2 p.u	N/A	6,67 p.u
		Dem. Bus 4	1,3 p.u	100 [$/kWh]	N/A
	S. 3	Tr. 7-8	2 p.u	N/A	6,67 p.u
		Dem. Bus 7	1 p.u	100 [$/kWh]	N/A
	S. 4	Tr. 9-10	2 p.u	N/A	6,67 p.u
		Dem. Bus 10	1,3 p.u	100 [$/kWh]	N/A
Generadores	Bus1	G 1-1	2,5 p.u	5 [$/kWh]	N/A
		G 1-2	2 p.u	6 [$/kWh]	N/A
	Bus4	G 2-1	3 p.u	7 [$/kWh]	N/A
		G 2-2	1,5 p.u	8 [$/kWh]	N/A
	Bus7	G 7-1	2,5 p.u	5 [$/kWh]	N/A
		G 7-2	2 p.u	6 [$/kWh]	N/A
	Bus10	G 10-1	3 p.u	7 [$/kWh]	N/A
		G 10-2	1,5 p.u	8 [$/kWh]	N/A

En las tablas 6.2, 6.3, 6.4, 6.5, 6.6 y 6.7 se encuentra un reporte de los resultados obtenidos en las simulaciones con un recurso de ataque de *M=12* y con recursos de protección *Pr=0, Pr=3, Pr=6, Pr=9, Pr=12* y *Pr=15*, respectivamente. El análisis de los resultados para cada simulación se hace después de cada tabla.

Tabla 6.2. Resultados para un recurso de protección *Pr=0*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
0	1	1 p.u.	0	1	2	0	0	1	A
	2	0	0	2	3	0	0	2	A
	3	0	0	2	5	0	0	3	A
	4	1,3 p.u.	0	3	4	0	0	4	A
	5	0	0	3	5	0	0	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	0	3	8	0	0		
	7	1 p.u.	0	5	6	0	0		
	8	0	0	5	11	0	0		
	9	0	0	7	8	0	0		
	10	1,3 p.u.	0	8	9	0	0		
	11	0	0	8	11	0	0		
	12	2,5 p.u.	0	9	10	0	0		
	Total Pérdidas	9,6 p.u.		9	11	0	0		
				11	12	0	0		
				2	3	0	0		
				2	5	0	0		
				8	9	0	0		
				8	11	0	0		

Este es el caso de un ataque sin ninguna protección, será de gran utilidad en el análisis de los posteriores casos pues sirve como punto de partida para poder apreciar el efecto que tiene el incremento del recurso de protección en el sistema.

Se puede apreciar que el total de pérdidas es igual a la carga total del sistema y el recurso de ataque de *M=12*, se ha utilizado en su totalidad, ya que son atacadas las cuatro subestaciones y el recurso necesario para atacar a cada una de ellas es de *Ms=Prs=3*. Se hace esta aclaración ya que es de gran importancia para el análisis de los siguientes casos.

Tabla 6.3. Resultados para un recurso de protección *Pr=3*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
3	1	1 p.u.	0	1	2	0	0	1	A
	2	0	0	2	3	0	0	2	A
	3	0	0	2	5	0	0	3	P
	4	1,3 p.u.	0	3	4	0	0	4	A
	5	0	0	3	5	0	0	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	0	3	8	0	0		
	7	0	0	5	6	0	A		
	8	0	0	5	11	0	A		
	9	0	0	7	8	0	0		
	10	1,3 p.u.	0	8	9	0	0		
	11	0	0	8	11	0	0		
	12	2,5 p.u.	0	9	10	0	0		
	Total Pérdidas	8,6 p.u.		9	11	0	0		
				11	12	0	A		
				2	3	0	0		
				2	5	0	0		
				8	9	0	0		
				8	11	0	0		

Se realiza el análisis con un recurso de protección *Pr=3*, sin ver los resultados de tener recursos de protección de 1 y 2, esto se hizo dado que, la componente más crítica que se puede proteger es la subestación 3 que requiere de un recurso de *Prs=3* para ser atacada, entonces al tener una disponibilidad de recurso inferior a 3, la protección del sistema no tendría ninguna incidencia en el total de las pérdidas para el recurso de ataque planteado *M=12*.

El comportamiento es similar para los casos siguientes y por esta razón, y para no hacer tan extenso el análisis, sólo se verá la protección del sistema con recursos múltiplos de tres.

Las pérdidas en este caso fueron de 8.6 p.u. en comparación del caso donde no existe recurso de protección.

Tabla 6.4. Resultados para un recurso de protección *Pr=6*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
6	1	0	0	1	2	0	0	1	P
	2	0	0	2	3	0	0	2	A
	3	0	0	2	5	0	0	3	P
	4	1,3 p.u.	0	3	4	0	0	4	A
	5	0	A	3	5	0	0	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	0	3	8	0	0		
	7	0	0	5	6	0	0		
	8	0	0	5	11	0	0		
	9	0	0	7	8	0	0		
	10	1,3 p.u.	0	8	9	0	0		
	11	0	0	8	11	0	0		
	12	2,5 p.u.	0	9	10	0	0		
	Total Pérdidas	7,6 p.u.		9	11	0	0		
				11	12	0	A		
				2	3	0	0		
				2	5	0	0		
				8	9	0	0		
				8	11	0	0		

En este caso cuando dispone de un *Pr=6*, lo utiliza para proteger las subestaciones 1 y 3, bajo estas condiciones el recurso de ataque restante, es decir, el que no se utilizó para atacar las subestaciones fue utilizado en atacar el nodo 5 y la línea que va del nodo 11 al 12.

Este conjunto de ataques resultante produce pérdidas por 7.6 p.u consiguiendo disminuir las pérdidas en 2 p.u con respecto al caso de recurso de protección *Pr=0*.

Tabla 6.5. Resultados para un recurso de protección *Pr=9*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
9	1	0	0	1	2	0	0	1	P
	2	0	0	2	3	0	0	2	P
	3	0	0	2	5	0	A	3	P
	4	0	0	3	4	0,0392 p.u.	0	4	A
	5	0	0	3	5	-0,0392 p.u.	0	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	A	3	8	0	A		
	7	0	0	5	6	0	0		
	8	0	0	5	11	-0,0392 p.u.	0		
	9	0	0	7	8	0,0392 p.u.	0		
	10	1,3 p.u.	0	8	9	0	0		
	11	0	0	8	11	0,0196 p.u.	0		
	12	2,5 p.u.	0	9	10	0	0		
	Total Pérdidas	6,3 p.u.		9	11	0	0		
				11	12	0	A		
				2	3	0	A		
				2	5	0	0		
				8	9	0	0		
				8	11	0,0196 p.u.	0		

Se observa que las pérdidas disminuyen a 6.3 p.u al aumentar el recurso de protección a 9 unidades de protección utilizados para proteger las subestaciones 1, 2 y 3.

Tabla 6.6. Resultados para un recurso de protección *Pr=12*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
12	1	0	0	1	2	0,0575 p.u.	0	1	P
	2	0	0	2	3	0,0287 p.u.	0	2	P
	3	0	0	2	5	0	A	3	P
	4	0	0	3	4	0,0575 p.u.	0	4	P
	5	0	0	3	5	0	A	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	0	3	8	0	A		
	7	0	0	5	6	0	A		
	8	0	0	5	11	0	0		
	9	0	0	7	8	0	0		
	10	0	0	8	9	0	0		
	11	0	0	8	11	0	A		
	12	2,5 p.u.	A	9	10	0	0		
	Total Pérdidas	5 p.u.		9	11	0	A		
				11	12	0	0		
				2	3	0,0287 p.u.	0		
				2	5	0	0		
				8	9	0	A		
				8	11	0	0		

En este caso se observa que las pérdidas disminuyen a 5 p.u al aumentar el recurso de protección a 15 unidades de protección utilizadas para proteger todas las subestaciones del sistema.

El nuevo ataque óptimo bajo estas condiciones busca cortar el flujo de potencia hacia las cargas ubicadas en los nodos 12 y 6 para lo cual utiliza un recurso de ataque igual a 5 para atacar el nodo 12, y el recurso de ataque restante es invertido en desconectar las líneas que le pueden suministrar potencia a la carga ubicada en el nodo 6.

Tabla 6.7. Resultados para un recurso de protección *Pr=15*

Recurso de Protección (*Pr*)	Nodos			Líneas				Subestaciones	
	Nodo #	Pérdida	Estado	N origen	N destino	Potencia	Estado	Sub #	Estado
15	1	0	0	1	2	0,0575 p.u.	0	1	P
	2	0	0	2	3	0,0287 p.u.	P	2	P
	3	0	0	2	5	0	A	3	P
	4	0	0	3	4	0,0575 p.u.	0	4	P
	5	0	0	3	5	0	0	**A**=Atacado **P**=protegido	
	6	2,5 p.u.	A	3	8	0	P		
	7	0	0	5	6	0	0		
	8	0	0	5	11	0	0		
	9	0	0	7	8	0,0575 p.u.	0		
	10	0	0	8	9	0,0287 p.u.	P		
	11	0	0	8	11	0	A		
	12	2,5 p.u.	A	9	10	0,0575 p.u.	0		
	Total Pérdidas	5 p.u.		9	11	0	0		
				11	12	0	0		
				2	3	0,0287 p.u.	0		
				2	5	0	0		
				8	9	0,0287 p.u.	0		
				8	11	0	0		

Para este caso se observa la misma cantidad de pérdidas que en el caso anterior (*Pr=12*), esto obedece a la configuración del sistema porque existen muchas posibles combinaciones de ataques que se podrían realizar con un recurso de ataque *M=12* bajo estas condiciones. El recurso de protección restante, es decir, las 3 unidades de protección restantes no son suficientes para proteger todas las posibles alternativas de ataque con un recurso de *M=12*.

Así mismo se puede ver que se necesitaría una gran cantidad de unidades de protección para cubrir los posibles planes de ataque que ocasionen una pérdida de 5 p.u. En este orden de ideas, el comportamiento de las pérdidas con respecto a un recurso de protección mayor de 12 unidades de protección es permanecer constante en 5 p.u. mientras que este sea suficiente para cobijar todos los posibles planes de ataque.

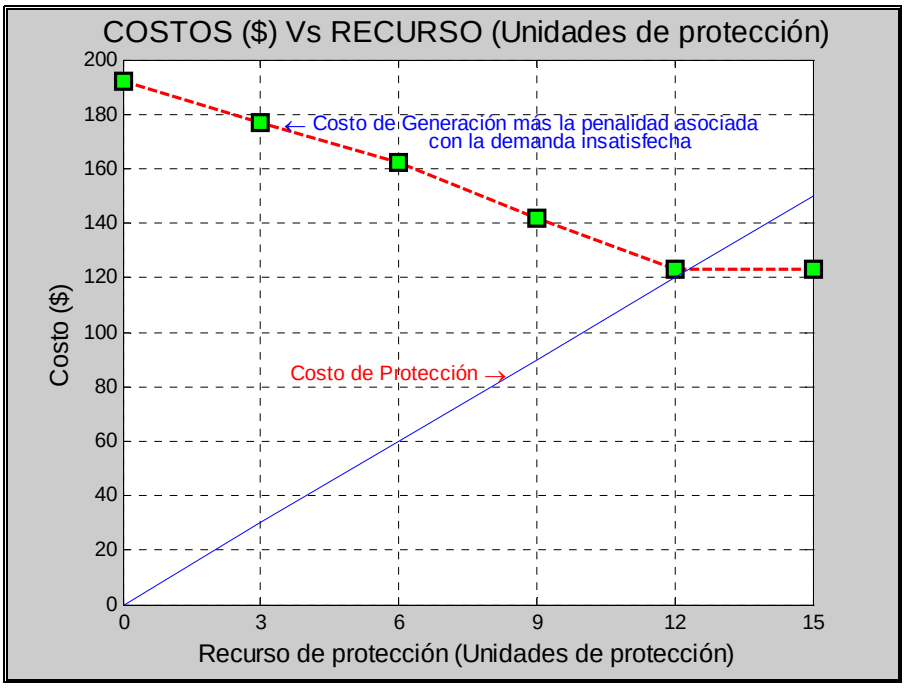
6.3.1. Metodología de análisis del recurso de protección óptimo. Ahora se estudia la posibilidad de optimizar el recurso de protección en función de los costos.

Dado que, el hecho de incluir los costos de protección en el modelo implicaría que este dejaría de ser lineal, se plantea un análisis gráfico a partir de la información recopilada del modelo de protección de la siguiente manera:

Supóngase que el recurso de protección tiene un costo, entonces este es directamente proporcional a la cantidad de recurso, mientras que los costos de generación más la demanda insatisfecha son inversamente proporcionales a la cantidad de recurso de protección. Se plantea un método que busca el recurso óptimo de protección, un recurso que no exceda los costos de protección o los de operación del sistema (encontrar el punto óptimo).

A continuación se hace el análisis de el recurso óptimo del ejemplo simulado en la sección 6.3 de este capítulo, para el sistema *Salle-06 con dos áreas* y un recurso de ataque *M=6*. Utilizando los resultados obtenidos en la sección anterior se obtiene la siguiente gráfica asumiendo que el costo del recurso de protección es igual a 10 pesos/unidad de protección.

Figura 6.3. Gráfica del punto óptimo de los costos de recurso de protección.



Como se puede ver el punto óptimo de protección se obtiene al utilizar un recurso de aproximadamente de 12 unidades de protección.

CONCLUSIONES

En este capítulo, se darán a conocer las conclusiones finales de éste trabajo de grado. En primer lugar se resumen las conclusiones obtenidas de las simulaciones realizadas, posteriormente se enumeran las contribuciones originales para el análisis de la vulnerabilidad de los sistemas de potencia ante ataques terroristas.

El objeto de estudio de éste trabajo fue indagar sobre diferentes metodologías que se estén desarrollando desde los últimos 5 años para el análisis de la vulnerabilidad de los sistemas de potencia ante un eventual ataque terrorista, para profundizar su modelamiento matemático y computacional, mirar la complejidad y el uso de software especializados para el desarrollo de cada una. De esta manera se eligió la metodología del proyecto VEGA 1.0 para modelarla en una herramienta computacional diferente a la utilizada por sus autores, para realizar simulaciones que permitieran analizar el comportamiento de la metodología seleccionada en un sistema de potencia sencillo, ver sus fallas y fortalezas.

De las simulaciones, se pudo concluir:

1. Se modeló y programó adecuadamente la misma metodología del proyecto *VEGA1.0* y fue aplicada en el mismo sistema de prueba (IEEE RTS-96, primera área) que fue analizado por los autores Salmerón, Wood y Baldick [2], comprobando su buen funcionamiento al obtener los mismos resultados utilizando una herramienta computacional diferente a GAMS, para este caso fue implementado en el toolbox de optimización 3.1 de MATLAB.

2. Al simular un recurso de ataque *M=6* en la primera área del sistema de prueba IEEE RTS-96 en 37 iteraciones se logró llegar a uno de los dos resultados obtenidos que se muestran el artículo de la referencia [2], llamado por los autores como el *plan 1*.

   Aunque en la referencia [2] no aclara como se obtienen los resultados del *plan 2* y la diferencia de las condiciones de simulación para obtener los resultados del *plan 1* (llamados así por los autores); para alcanzar los valores del *plan 2* se hicieron las subestaciones inatacables, es decir, que los valores correspondientes a sus variables binarias sean siempre cero; estos resultados se consiguieron en 182 iteraciones.

3. Se propuso una modificación a la metodología original de VEGA 1.0 considerado que en esta no se tenía en cuenta una configuración tal que tuviera generadores conectados directamente a uno de los nodos de una subestación.

En el momento de ser atacada, los generadores que estén entregando su potencia a los nodos de ella, deberían ser desconectados a consecuencia del ataque.

4. Se diseñó un sistema de potencia de 6 nodos con las características descritas anteriormente llamado S*alle-06*.

   Se analizó su vulnerabilidad con la metodología original (*VEGA 1.0*) y con la modificación propuesta (*VEGA 1.0 modificado*) justificando la importancia de tener en cuenta las consecuencias de un ataque en una subestación a la cual está acoplado directamente un generador; porque esto haría ver menos atractivo un ataque en esta subestación.

5. De los resultados obtenidos se puede establecer qué componentes de un sistema lo hacen más vulnerable y estos resultados son inherentes a cada sistema, siendo una gran herramienta para el diseño de sistemas más robustos y el fortalecimiento de sistemas con alto índice de vulnerabilidad.

6. El toolbox de optimización 3.1 de MATLAB, al ser más de uso académico que una herramienta especializada en la solución de problemas de optimización, no es el más apropiado para hacer la simulación de la metodología en sistemas grandes, debido a que crece el número tanto de variables como de restricciones en los problemas de optimización.

7. Es de gran importancia tener en cuenta la reglamentación del sector eléctrico colombiano para determinar tanto los costos de no satisfacción de la demanda como las restricciones pertinentes a la potencia máxima que podría generar cada unidad generadora desde el punto de vista de el despacho de energía (bolsa de energía) y no sólo desde el punto de vista de la capacidad de las plantas generadoras.

Los aportes que en esta investigación se hicieron para complementar la metodología propuesta en el proyecto VEGA 1.0, son los siguientes:

1. Se modificó la metodología original del proyecto VEGA 1.0 para incluir el efecto de un ataque contra una subestación conectada a un nodo con generación.

2. Se extendió el modelo para considerar y optimizar el recurso de protección físico, es decir, la protección que brinda las fuerzas militares o el sector de seguridad privada a la infraestructura del sistema eléctrico.

RECOMENDACIONES Y TRABAJOS FUTUROS

Finalmente, emitimos algunas recomendaciones para trabajos posteriores:

1. En la Facultad de Ingeniería Eléctrica de la Universidad de La Salle hay un gran interés de incentivar la investigación para el desarrollo integral de los alumnos para su vida profesional.

   Es importante la adquisición de la licencia de un software especializado en optimización, el que sería de gran utilidad para investigaciones futuras, no sólo en proyectos de grado sino también en proyectos de investigación de la Facultad. Se recomienda el paquete GAMS, reconocido a nivel mundial para la solución de problemas de optimización a nivel profesional y académico.

2. Despertar la inquietud por el tema del *análisis de la vulnerabilidad de los sistemas de potencia ante ataques terroristas* tanto en los estudiantes como en los investigadores de la Facultad.

   En los últimos años Colombia ha estado sumergida en un panorama sociopolítico que desató un conflicto interno, el cual afecta por medio de ataques directos o indirectos el sistema eléctrico. Este tipo de investigaciones ayudaría a mitigar las consecuencias de estos atentados y proporcionar diferentes alternativas a los estudios dirigidos a la solución de los impactos sociales y económicos que ocasiona en una sociedad el no tener un fluido eléctrico confiable. Además, este es un tema actual que se encuentra en vía de desarrollo a nivel mundial.

3. Seguir investigando y desarrollando metodologías alternas a la que fue objeto de estudio en este trabajo, con el fin de determinar la alternativa que se ajuste a las condiciones del sistema eléctrico colombiano, o en su defecto la creación de metodologías resultado de la combinación de metodologías propuestas, como las expuestas en el capítulo 1, con el fin de extraer de cada una sus principales ventajas.

Quedan numerosos temas para trabajos futuros, se proponen los siguientes:

1. Extender la metodología para que, además de la vulnerabilidad de sistemas eléctricos en función de las pérdidas de energía (MW/h) como objetivo

primordial, también considere la vulnerabilidad del sistema desde el punto de vista económico incluyendo los costos de reparación del sistema.

2. Hacer las adaptaciones pertinentes y necesarias para implementar esta metodología al sistema eléctrico colombiano, esto incluiría la modelación dentro de la metodología estudiada de los siguientes aspectos a considerar:

   - Ubicación geográfica de las componentes del sistema.
   - La accesibilidad a las componentes del sistema.
   - Influencia de los grupos atacantes en la zona donde se encuentra ubicada la infraestructura.
   - La reglamentación del sector eléctrico colombiano respecto a las penalidades asociadas con la carga no satisfecha y al despacho de energía.
   - Información de grupos de inteligencia que permita determinar las restricciones propias tanto del recurso terrorista y el recurso de protección.

La adaptación de los anteriores aspectos no revestiría mayor complejidad. Por ejemplo, se propone para los aspectos referentes a la ubicación geográfica y la influencia de los grupos terroristas que la modelación debe obedecer a la determinación de los valores del peso (*wl, wi, ws, wg, wt*) para hacer más o menos atractiva una componente según las características de la localización de cada componente.

Para el caso de la accesibilidad a las diferentes componentes del sistema será necesario investigar sobre la seguridad de cada una de ellas y de esta manera determinar si son o no atacables.

Es aconsejable que este tipo de investigación cuente con el apoyo de personal de inteligencia militar o alguna disciplina afín, para poder determinar las restricciones del recurso terrorista y de protección.

BIBLIOGRAFÍA

[1] VEGA (Vulnerability of Electric Power Grids Analysis Project); Monterrey California (USA): Navy website Naval Postgraduate School, 2005 Last updated October 17 – [citado 8 de febrero de 2006]. Página Web: http://www.nps.navy.mil/orfacpag/resumePages/projects/index.htm

[2] Salmerón, J., Word R. K. and Baldick, R., (2004), *"Analysis of electric grid security under terrorist threat"*, IEEE transactions on Power Sistems, vol. 19, pág. 905-912.

[3] Optimization Toolbox 3.1 [online]; Math Works, 1994-2006 – [citado 13 de junio de 2006]. Página Web: http://www.mathworks.com/products/optimization/

[4] Univirtual, Investigación operativa I [online], Bogotá (Colombia): Universidad Nacional de Colombia, 2000- [citado 30 de marzo de 2006]. Página Web: http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060014/index.html.

[5] Taha. Hamby A., Investigación de Operaciones, México, Alfaomega, segunda edición, cap 8, pág.333-360.

[6] Systems Optimization Laboratory (SOL), Terman Engineering Center Stanford, CA 94305-4026, 2006 – [citado 8 de agosto de 2006]. Página Web: http://www.stanford.edu/group/SOL/

[7] The mathworks, *Optimization Toolbox 3.1 for Use with MATLAB*, User's Guide Version 3.

[8] "*The IEEE Reliability Test System – 1996 Application of Probability Methods Subcommittee A report prepared by the Reliability Test System Task Force of the*", IEEE Transactions on Power Systems, Vol. 14, No. 3, August 1999, pág. 1010-120.

[9] J. M. S. Pinheiro, C. R. R. Dornellas, M. Th. Schilling, A. C. G, Melo, J. C. 0. Mello, (1998), *"Probing the new IEEE reliability test system (RTS-96): HL-II assessment"*, IEEE Transactions on Power Systems, Vol. 13, No. 1, February 1998, pág. 171-176.

[10] Tranchita C., Hadjsaid N., Torres A., (2006), *"Ranking Contingency Resulting from Terrorism by Utilization of Bayesian Networks in general"*, Electrotechnical Conference. MELECON 2006, IEEE Mediterranean 16-19 May 2006, pág. 964-967 ISBN: 1-4244-0087-2.

[11] Tranchita C. Torres A., *"Events classification and operation states considering terrorism in security analysis"*, Power Systems Conference and Exposition, 2004. IEEE PES 10-13 Oct. 2004, pág.1265- 1271 vol.3 ISBN: 0-7803-8718-X.

[12] Tranchita C., Hadjsaid N., Torres A., (2006), *"Security assessment of electrical infrastructure under terrorism"*, CRIS, Third International Conference on Critical Infrastructures, Alexandria, VA, September 2006.

[13] Tranchita C., Hadjsaid N., Torres A., (2006), *"Using Fuzzy Arithmetic for Power Flow Analysis with Uncertainty"*, International Review of Electrical Engineering (I.R.E.E.), vol. 1, n.3.

[14] Reka Albert, Istvan Albert, Gary L. Nakarado, (2004), *"Structural vulnerability of the North American power grid"*, PHYSICAL REVIEW E 69, 025103 (R) (2004).

[15] Ake J. Holmgren, (2006), *"Using Graph Models to Analyze the Vulnerability of Electric Power Networks"*, Risk Analysis, Vol. 26, No. 4, 2006.

[16] Salmerón, J., Word R. K. and Baldick, R. (2003), *"Optimizing electric grid design under asymmetric threat"*, Prepared for: Department of Justice Office of Justice Programs and Office of Domestic Preparedness, under the aegis of the Naval Postgraduate School Homeland Security Leadership Development Program.

[17] Casasus, T.; Mocholi, M.; Sanchis, V. y Sala, R., *"Optimización económica con GAMS"*, Universidad de Valencia, [citado 20 de agosto de 2006] Página Web: www.sosig.ac.uk/cticce/cheer/ch102/ch102p02.htm, pág. 2-4.

[18] The MOSEK Optimization Software, The MOSEK optimization toolbox for MATLAB version 3.2 (Revision 8) User's guide and reference manual, (2006) – [citado 9 de agosto de2006].
Página Web: http://www.mosek.com/products/3/tools/doc/html/toolbox/index.html.

[19] Wikipedia, La enciclopedia libre, Red bayesiana, [online], (2006) – [citado 19 de septiembre de 2006]. Página Web: http://es.wikipedia.org/wiki/Red_bayesiana

[20] Díaz, G; Murcia, F; Cortés, C; (2006), Grupo Colposalle, en proceso de publicación. "Estudio de flujos de potencia al instalar un FACTS en la línea de transmisión circo - Guavio perteneciente al sistema de transmisión colombiano" por Fredy Murcia, Guillermo Díaz, y Camilo Cortés [20].

[21] IEEE Reliability Test Data. [online], (1999-II) – [citado 27 de Julio de 2006]. Página Web: www.ee.washington.edu/ research/pstca/

Anexo A. Datos de las líneas IEEE RTS-96 [21]

Línea #	Origen	Destino	R	X	B
1	1	2	0,003	0,014	68,293
2	1	3	0,055	0,211	4,438
3	1	5	0,022	0,085	11,026
4	2	4	0,033	0,127	7,376
5	2	6	0,05	0,192	4,878
6	3	9	0,031	0,119	7,869
7	3	24	0,002	0,084	11,898
8	4	9	0,027	0,104	9,008
9	5	10	0,023	0,088	10,637
10	6	10	0,014	0,061	15,573
11	7	8	0,016	0,061	15,338
12	8	9	0,043	0,165	5,675
13	8	10	0,043	0,165	5,675
14	9	11	0,002	0,084	11,898
15	9	12	0,002	0,084	11,898
16	10	11	0,002	0,084	11,898
17	10	12	0,002	0,084	11,898
18	11	13	0,006	0,048	20,513
19	11	14	0,005	0,042	23,477
20	12	13	0,006	0,048	20,513
21	12	23	0,012	0,097	10,154
22	13	23	0,011	0,087	11,313
23	14	16	0,005	0,059	16,828
24	15	16	0,002	0,017	58,020
25	15	21	0,006	0,049	20,107
26	15	24	0,007	0,052	18,888
27	16	17	0,003	0,026	37,956
28	16	19	0,003	0,023	42,751
29	17	18	0,002	0,014	70,000
30	17	22	0,014	0,105	9,357
31	18	21	0,003	0,026	37,956
32	19	20	0,005	0,04	24,615
33	20	23	0,003	0,022	44,625
34	21	22	0,009	0,068	14,453
35	15	21	0,006	0,049	20,107
36	18	21	0,003	0,026	37,956
37	19	20	0,005	0,04	24,615
38	20	23	0,003	0,022	44,625

Anexo B. Datos de las cargas en los nodos IEEE RTS-96 [21]

Área/Número de nodo			% de la carga del sistema	Carga		Si la carga pico es superior al 10%	
1	2	3		MW	MVar	MW	MVar
101	201	301	3.8	108	22	118.8	24.2
102	202	302	3.4	97	20	106.7	22.0
103	203	303	6.3	180	37	198.0	40.7
104	204	304	2.6	74	15	81.4	16.5
105	205	305	2.5	71	14	78.1	15.4
106	206	306	4.8	136	28	149.6	30.8
107	207	307	4.4	125	25	137.5	27.5
108	208	308	6.0	171	35	188.1	38.5
109	209	309	6.1	175	36	192.5	39.6
110	210	310	6.8	195	40	214.5	44.0
113	213	313	9.3	265	54	291.5	59.4
114	214	314	6.8	194	39	213.4	42.9
115	215	315	11.1	317	64	348.7	70.4
116	216	316	3.5	100	20	110.0	22.0
118	218	318	11.7	333	68	366.3	74.8
119	219	319	6.4	181	37	199.1	40.7
120	220	320	4.5	128	26	140.8	28.6
Total			100	2850	580	3135	638

Anexo C. Datos de los generadores en cada nodo IEEE RTS-96 [21]

Nombre del Nodo	Tipo de unidad generadora	ID#	PG (MW)	QG (MVAR)	Q^{MAX} (MVAR)	Q^{MIN} (MVAR)	Vs p.u.
101	U20	1	10	0	10	0	1.035
101	U20	2	10	0	10	0	1.035
101	U76	3	76	14.1	30	-25	1.035
101	U76	4	76	14.1	30	-25	1.035
102	U20	1	10	0	10	0	1.035
102	U20	2	10	0	10	0	1.035
102	U76	3	76	7.0	30	-25	1.035
102	U76	4	76	7.0	30	-25	1.035
107	U100	1	80	17.2	60	0	1.025
107	U100	2	80	17.2	60	0	1.025
107	U100	3	80	17.2	60	0	1.025
113	U197	1	95.1	40.7	80	0	1.020
113	U197	2	95.1	40.7	80	0	1.020
113	U197	3	95.1	40.7	80	0	1.020
114	Sync Cond	1	0	13.7	200	-50	0.98
115	U12	1	12	0	6	0	1.014
115	U12	2	12	0	6	0	1.014
115	U12	3	12	0	6	0	1.014
115	U12	4	12	0	6	0	1.014
115	U12	5	12	0	6	0	1.014
115	U155	6	155	0.05	80	-50	1.014
116	U155	1	155	25.22	80	-50	1.017
118	U400	1	400	137.4	200	-50	1.050
121	U400	1	400	108.2	200	-50	1.050
122	U50	1	50	-4.96	16	-10	1.050
122	U50	2	50	-4.96	16	-10	1.050
122	U50	3	50	-4.96	16	-10	1.050
122	U50	4	50	-4.96	16	-10	1.050
122	U50	5	50	-4.96	16	-10	1.050
122	U50	6	50	-4.96	16	-10	1.050
123	U155	1	155	31.79	80	-50	1.050
123	U155	2	155	31.79	80	-50	1.050

Anexo D. Rata de Calor e incremento de la Rata de Calor IEEE RTS-96 [21]

Capacidad MW	Tipo	Combustible	Salida %	MW	Rata de calor de la planta Btu/kWh	Incremento de la rata de calor Btu/kWh
12	Vapor	#6 petróleo	20	2.40	16017	10179
			50	6.00	12500	10330
			80	9.60	11900	11668
			100	12.00	12000	13219
20	Turbina de combustión	#2 petróleo	79	15.80	15063	9859
			80	16.00	15000	10139
			99	19.80	14500	14272
			100	20.00	14499	14427
50	Hídrica		100	50.00	No aplica	
76	Vapor	Carbón	20	15.20	17107	9548
			50	38.00	12637	9966
			80	60.80	11900	11576
			100	76.00	12000	13311
100	Vapor	#6 petróleo	25	25.00	12999	8089
			50	50.00	10700	8708
			80	80.00	10087	9420
			100	100.00	10000	9877
155	Vapor	Carbón	35	54.25	11244	8265
			60	93.00	10053	8541
			80	124.00	9718	8900
			100	155.00	9600	9381
197	Vapor	#6 petróleo	35	68.95	10750	8348
			60	118.20	9850	8833
			80	157.60	9644	9225
			100	197.00	9600	9620
350	Vapor	Carbón	40	140.00	10200	8402
			65	227.50	9600	8896
			80	280.00	9500	9244
			100	350.00	9500	9768
400	Nuclear	LWR	25	100.00	12751	8848
			50	200.00	10825	8965
			80	320.00	10170	9210
			100	400.00	10000	9438