ANÁLISIS DE MODELOS DE INTERDICCIÓN EN REDES PLANARES

Francisco Pérez-Galarce
Centro de Competitividad del Maule, Facultad de Economía y Negocios
Universidad de Talca
franperez@utalca.cl

Alfredo Candia-Véjar **Eduardo Álvarez-Miranda**
Departamento de Modelamiento y Gestión Industrial
Universidad de Talca
{acandia, ealvarez}@utalca.cl

Emilio Carrizosa
Facultad de Matemáticas
Universidad de Sevilla
carrizosa@sevilla.es

RESUMEN

En el siguiente trabajo se presenta un conjunto de modelos de optimización combinatorial que permite evaluar la vulnerabilidad de redes espaciales. Dichos modelos han sido propuestos recientemente en la literatura y su estructura permite obtener interesantes parámetros de vulnerabilidad bajo diversas situaciones. En esta ocasión se analizan aspectos relacionados a su flexibilidad de uso y al impacto de ciertos parámetros en un análisis experimental. Esta categoría de problemas y modelos (interdicción) son relevantes debido a que proveen de modelos de optimización para una gran variedad de problemáticas reales, asociadas a la identificación de infraestructura crítica en redes sometidas a diferentes disrupciones, tales como aquellas provenientes de desastres naturales, ataques terroristas o fallas accidentales.

Palabras claves: Interdicción, Redes Espaciales, Optimización Combinatorial

ABSTRACT

In this paper we study a framework of CO problems for assessing the vulnerability of planar networks. The models have recently been proposed in the literature and their structure allows to obtain interesting vulnerability parameters. Now, we analyze the flexibility of model and the impact of certain parameters through an experimental analysis. This category of problems are relevant because they provide models for a variety of real problems related to the identification of critical infrastructure of networks under various disruptions such as those from natural disasters, terrorist attacks or accidental failures.

Keywords: Interdiction, Spatial Networks, Combinatorial Optimization

1. Introducción

El problema de *Interdicción en Redes* es definido como un problema de optimización en redes en el cual un agente (**interdictor**) se esfuerza por perjudicar o destruir el objetivo original de una contraparte (**evasor**). Un tradicional ejemplo en el contexto del transporte es el problema del camino más corto (***SPP Shortest Path Problem***) donde el evasor intenta encontrar la ruta más corta en una red desde un nodo origen *s* a un nodo destino *t*, en tanto, el interdictor tiene la posibilidad de modificar algunos elementos de la red (nodos y/o aristas) e intenta maximizar el largo de la ruta más corta a seleccionar por el evasor.

Este problema ha sido estudiado durante los últimos 50 años, no obstante se ha intensificado en la reciente década. La incorporación de los elementos de interdicción a los problemas clásicos en redes, generalmente adicionan complejidad tanto del punto de vista del modelamiento matemático como de la resolución algorítmica.

Esta categoría de problemas y modelos son relevantes debido a que proveen de alternativas de solución para una gran variedad de problemáticas reales, asociadas a la identificación de infraestructura crítica en redes, que pueden ser sometidas a diferentes disrupciones, provenientes de: desastres naturales, ataques terroristas o fallas accidentales. Algunos ejemplos de sistemas donde estos modelos han sido estudiados son: cadenas de suministro, telecomunicaciones, control de enfermedades infecciosas y aplicaciones militares.

Las devastadoras consecuencias provocadas tanto por los desastres naturales como por los ataques terroristas han sido difundidas extensamente, lo anterior, debido a algunos eventos puntuales, como el ataque a las torres gemelas en Estados Unidos en 2011 y el terremoto-tsunami que afecto a Japón en 2011. Para más ejemplos en eventos naturales ver [1] y para ataques intencionales ver [2].

A la fecha se han estudiado modelos de interdicción asociados a clásicos problemas de Optimización en Redes, algunos ejemplos son, el problema de máximo flujo, ver [3] [4] [5] [6], problemas de localización, ver [7] [8] [9] [10] y problemas de árbol de cobertura, ver [11] [12] [13] [14].

En este trabajo se estudiará el problema de camino más corto bajo interdicción, donde como se mencionó anteriormente, el objetivo del interdictor es maximizar el largo de la ruta más corta. Este problema ha sido abordado en algunos trabajos previos; en Israeli and Wood [15] se presentan modelos de programación lineal entera y se aplican técnicas de descomposición para resolverlo. Bell [16] propone un modelo de Teoría de Juegos que identifica los componentes de la red donde la disrupción podría generar mayor daño. Por otra parte, Bell et al. [17] analizan la vulnerabilidad de los caminos de una red bajo escenarios de disrupción. Yates and Sanjeevi [18] estudian una variante y presentan una aplicación en el sector transporte. Bayrak y Bailey [19] estudian el problema con información asimétrica. Matisziw y Murray [20] notan que en presencia de daño en una red, evaluar el potencial flujo entre s y t requiere la verificación de disponibilidad de un camino operacional s − t. Los modelos propuestos recientemente para identificar la infraestructura crítica se basan en la enumeración de todos los caminos s − t. Para abordar ello Matisziw y Murray [20] proponen una alternativa de modelamiento que no requiere la completa enumeración, generando beneficios computacionales sobre los modelos existentes.

En Álvarez et al. [21] se propone un esquema de modelos de optimización combinatorial donde las soluciones pueden ser utilizadas para evaluar la vulnerabilidad de una red espacial desde diferentes perspectivas (complementarias). Particularmente, se presentan modelos flexibles para el problema interdicción de camino más corto en redes espaciales, basado en características geométricas de la red. Se reportan resultados computacionales en instancias realistas donde se muestra la versatilidad de los modelos propuestos para caracterizar la robustez de la infraestructura de la red.

Contribución: Este trabajo tiene como objetivos: (i) analizar la versatilidad del esquema propuesto en Álvarez et al. [21] y (ii) caracterizar su desempeño computacional en relación a algunos parámetros del modelo. A partir del primer objetivo se pretende identificar problemas que requieren ser abordados por diferentes modelos en el esquema mencionado. A partir del segundo objetivo se pretende dar indicios de la complejidad computacional y potenciales requerimientos de algoritmos más sofisticados.

En la sección 2 se presenta el esquema con los modelos matemáticos en estudio, posteriormente en la sección 3 se realizan los experimentos y se analizan las propiedades de adaptabilidad del modelo y, finalmente, en la sección 4 se entregan las principales conclusiones y se entregan algunos lineamientos para trabajos futuros.

2. Modelos Matemáticos para el Análisis de Vulnerabilidad de Redes

A continuación se entregarán los componentes principales de los modelos presentados en Álvarez et al. [21].

Notación: Sea $G = (V, E)$ una red planar tal que $|V| = n$ y $|E| = m$. Sean además, $s, t \in V$ un nodo origen y un nodo destino; l_e, $\forall e: \{i, j\} \in E$ será el costo de la arista e y ℓ será el costo del camino más corto entre s y t.

Sea $\chi \subset \mathbb{R}^2$ una sub-región arbitraria de $\mathbb{R}^2$. Un elemento $x \in \chi$ es un punto en χ; para un punto x y una arista e dados, $d(x, e)$ representará la mínima distancia entre x y el segmento de línea definido por e. Para un $R \in \mathbb{R}^{>0}$ y un $x \in \chi$ dado, se definirá $E_x = \{e \in E | d(x, e) > R\}$ y $\bar{E}_x = \{e \in E | d(x, e) \leq R\}$. En otras palabras E_x es el conjunto de aristas que no son tocados por el disco de radio R y centro x $\rho(x, R)$ (*disco de falla o disrupción*), y $\bar{E}_x$ es el conjunto de aristas interdictadas. Nos referiremos a $G_x = (V, E_x)$ como *red operativa* con respecto a $\rho(x, R)$. Es importante considerar que G_x puede ser no conexo.

i. *Problema de máximo impacto de una falla en el camino más corto* (*The Max-Cost Single-Failure Shortest Path Problem*) **MCSFSPP**

El **MCSFSPP** está muy relacionado a algunos modelos de interdicción estudiados en la literatura [22] [23] [24] [25] [15]. La solución de este modelo entrega la localización del único disco de falla con radio de impacto R, que provoca el mayor daño en el camino más corto, y adicionalmente entrega la ruta $s - t$, en el caso de existir.

Sea $\mathbb{f} \in [0,1]^m$ un vector de variables de flujo. Un camino $s - t$ en G es inducido por las variables de flujo $\mathbb{f}$, si las siguientes restricciones son satisfechas.

$$\sum_{k \in V | e:\{j,k\} \in E} f_{i,k} - \sum_{i \in V | e:\{i,j\} \in E} f_{i,j} = \begin{cases} 1, & \text{si } j = s \\ 0, & \text{si } j \in V \backslash \{s, t\} \\ -1, & \text{si }, j = t \end{cases} \qquad \text{(SP1)}$$

Para un dado $x \in \chi$, ℓ_x será el costo del camino más corto $s-t$ sobre G_x con costo de aristas l_e^x, definido como $l_e^x = l_e$ si $e \in E_x$ $l_e^x = M$ si $e \in \bar{E}_x$ con $M = O(m\max_{e\in E} l_e)$, en tanto, $\Omega = \max_{e\in E} l_e$. Si $\Omega >$ M entonces existe al menos un punto x que desconecta todo camino $s-t$.

Luego, para un dado $x \in \chi$ el problema de encontrar ℓ_x puede ser definido como:

$$\ell_x = \min\left\{\sum_{e\in E} l_e^x f_e \mid (\text{SP. 1}) \text{ y } \mathbb{f} \in [0,1]^m\right\} \qquad (\ell_x)$$

A continuación se presentará el modelo matemático para el MCSFSPP, cabe considerar que para llegar a esta formulación se debe recurrir a una linealización del modelo original, pues éste se representa a través de un modelo del tipo max-min. En tanto, se recurre a la dualización del problema interno para abordarlo como un problema de maximización puro.

Sea $\mathbb{y} \in \{0,1\}^{|\chi|}$ un vector de variables binarias tal que $y_x = 1$ si el disco de falla es centrado en x y en el caso contrario $y_x = 0$. Por otra parte, sea $\mathbb{z} \in \{0,1\}^{|m|}$ un conjunto de variables binaria tal que $z_e = 1$ si la arista e está operativa y en caso contrario e $z_e = 0$. M representa un valor muy grande.

$$\Omega = \max\ \gamma_t - \gamma_s$$

$$y_x + z_e \leq 1, \qquad \forall e \in E | d(x,e) \leq R, \forall x \in \chi \qquad (\text{M. 1})$$

$$\sum_{\forall x\in\chi | d(x,e)>R} y_x - z_e \leq 0, \qquad \forall e \in E \qquad (\text{M. 2})$$

$$\sum_{x\in\chi} y_x = 1 \qquad (\text{M. 3})$$

$$\gamma_j - \gamma_j \leq\ l_{ij} z_{ij} + (1 - z_{ij})M, \forall e: \{i,j\} \in E \qquad (\text{M. 4})$$

$$(\mathbb{z}, \mathbb{y}) \in \{0,1\}^{m+|\chi|}\ \ y\ \ \gamma \in \mathbb{R} \qquad (\text{M. 5})$$

En el modelo anterior una disrupción representa el hecho que una arista queda no operativa (M.4), no obstante, fácilmente se puede generalizar a que la falla represente un tiempo de retraso $d_{ij} > 0\ \forall e \in E$, reemplazando (M.4) por (M.4b).

$$\gamma_j - \gamma_j \leq\ l_{ij} z_{ij} + (1 - z_{ij}) d_{ij}, \forall e: \{i,j\} \in E \qquad (\text{M. 4b})$$

ii. *El problema del máximo impacto de múltiples fallas en el camino más corto* (*The Max-Cost Multi-Failure Shortest Path Problem*) **MCMFSPP.**

Este modelo busca modelar la situación en la cual el interdictor tiene k puntos potenciales con radio de impacto R. Luego la solución de este modelo entrega la localización de los k discos de falla $\rho(x_1, R), \rho(x_2, R) \ldots \rho(x_k, R)$ que provocan el mayor daño en el camino más corto y la ruta $s-t$ en el caso de existir.

$$\Omega^k = \max \gamma_t - \gamma_s$$

(M. 1), (M. 4) y (M. 5)

$$\sum_{\forall x \in \chi | d(x,e) > R} y_x - z_e \leq 1 - \sum_{\forall x \in \chi} y_x, \qquad \forall e \in E \qquad \text{(M. 2b)}$$

$$\sum_{x \in \chi} y_x = k \qquad \text{(M. 3b)}$$

iii. *Máxima disrupción para un presupuesto de interdicción* (*Maximal Disruption for an interdiction Budget*)

Otra forma de modelar la situación anterior consiste en asumir que el interdictor tiene una presupuesto B y que cada interdicción tiene un costo asociado c_x , $\forall x \in \chi$.

$$\Omega^k = \max \gamma_t - \gamma_s$$

(M. 1), (M. 4), (M. 2b) y (M. 5)

$$\sum_{x \in \chi} c_x y_x \leq B \qquad \text{(M. 3c)}$$

iv. *Mínimo de fallas simultáneas para completa vulnerabilidad* (*Minimum Simultaneity for Complete Vulnerability*): k crítico

El último modelo propuesto busca determinar el número de fallas óptimo que genera la completa vulnerabilidad de la ruta $s - t$.

$$k^c = \min k$$

(M. 1), (M. 4), (M. 2b), (M. 3b) y (M. 5)

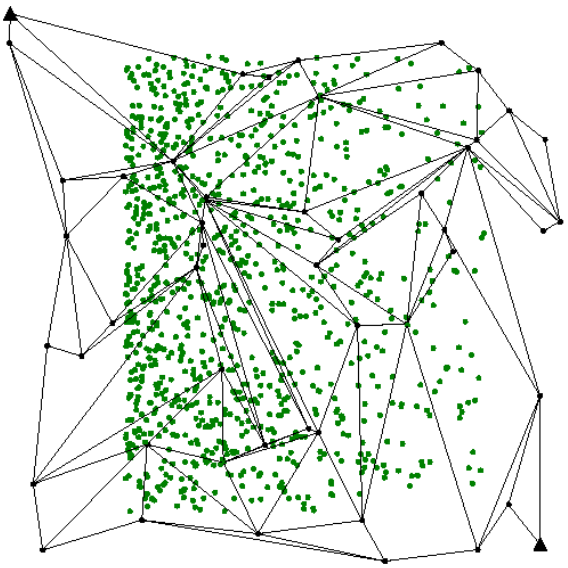
$$\gamma_t - \gamma_s \geq \theta \text{ y } k \in \mathbb{Z}$$

En resumen, a través de los modelos anteriores se puede medir impacto único, impactos múltiples, impacto bajo presupuesto y el número de impactos que genera máxima vulnerabilidad. Ahora, es importante recordar que cada uno de los impactos puede ser ajustado a situaciones particulares a través del disco de falla $\rho(x, R)$, ya sea por su radio R o por la política de falla $x \in \chi$.

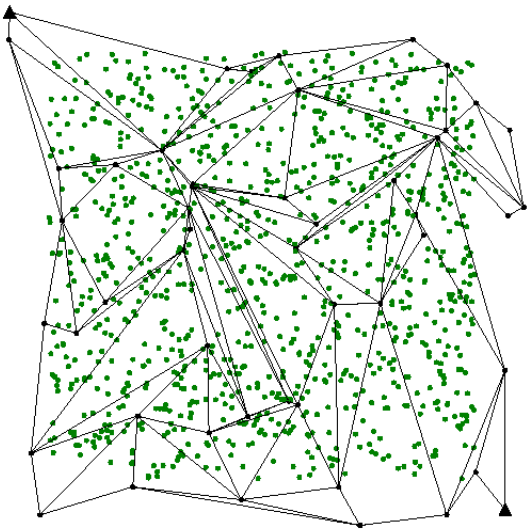
En la Figura 1 se puede apreciar una de las bondades de la estructura de los modelos antes presentados, esto tiene relación con la flexibilidad en las políticas de falla, que de acuerdo a la definición inicial corresponde a fallas aleatorias dentro de χ (Figura 1.b) No obstante, pueden tener un comportamiento probabilístico (Figura 1.a), o particularmente, estar localizadas en las aristas (Figura 1.c) o bien en los nodos del grafo (Figura 1.d). Lo anterior, da la posibilidad estudiar los potenciales usos de éste y el grado de generalización que se puede dar a los problemas de interdicción a través de este esquema. Junto a lo anterior, surge la interrogante respecto al nivel de complejidad computacional que asocian dichos

modelos. Ambos tópicos serán abordados a través de la experimentación presentada en la sección posterior.

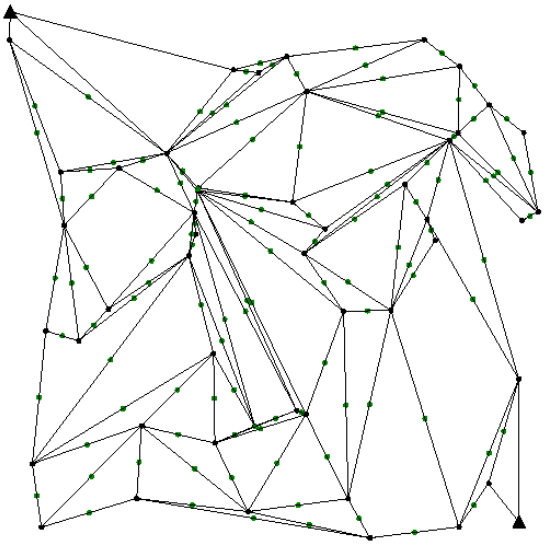
Figura 1. Posibles políticas de falla para modelos propuestos



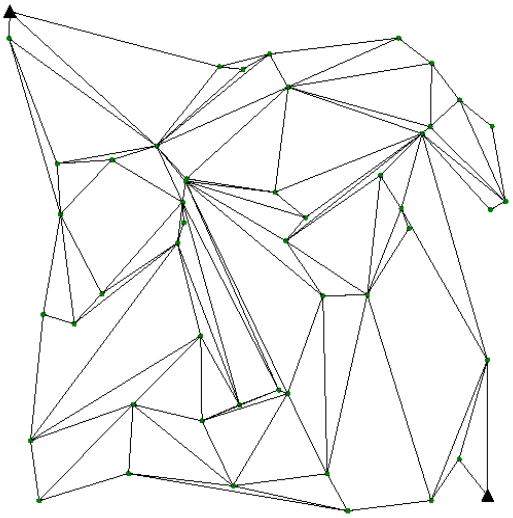
a) Fallas probabilísticas



b) Fallas aleatorias



c) Fallas localizadas en las aristas



d) Fallas localizadas en los nodos

3. Experimentación computacional

Para la experimentación se utilizan instancias ND, que son generadas de acuerdo al siguiente procedimiento: (i) se generan n puntos localizados en el plano euclidiano; (ii) se conectan todos los puntos a través de un árbol de expansión mínima; (iii) $\beta \times n$ aristas son agregadas, una arista e es agregada si y solo si la distancia euclidiana es menor a $a/\sqrt{\mathrm{n}}$ y se mantiene la planaridad de la red; (iv) Se crea el conjunto χ. Para la generación de éste se consideran cuatro opciones:

1) Generación aleatoria de K puntos entre (x_1, y_1), (x_2, y_1),(x_2, y_1)y (x_2, y_2). (Fig. 1b)
2) Generación probabilística de K puntos entre (x_1, y_1),(x_2, y_1),(x_2, y_1)y(x_2, y_2). (Fig. 1a)
3) Asignar fallas al centro de cada arista. (Fig. 1c)

4) Asignar falla al centro de cada nodo. (Fig. 1d)
Detalles computacionales: Todos los experimentos se realizaron usando el solver CPLEX (todos los parámetros por defecto). El equipo utilizado fue un Intel Core i7-3610QM con 8 GB RAM.

La experimentación computacional se dividió en dos grandes áreas, en primer lugar se presentan ejemplos particulares de experimentación que permite demostrar dos casos que se derivan del planteamiento general del modelo, posteriormente, se presentan resultados del desempeño computacional del modelo bajo distintas combinaciones de parámetros.

En la tabla 1 se presenta un análisis de vulnerabilidad utilizando un modelo multi falla, se consideran instancias con $n = 50$, $\beta = 2$, $\alpha = 1.6$. Para el primer caso las fallas se localizan en el centro de una arista (descartando aristas con conexión directa a s o t) y para el segundo caso en el centro de los nodos (excluyendo s y t). En la columna 2 y 7 se presenta el valor de la ruta obtenida Ω^k para k interdicciones, en las columnas 3 y 8 se presenta porcentaje de aumento en los costos $\Delta\%\Omega^k$ respecto de la situación sin interdicción, en las columnas 4 y 9 se presenta el tiempo de ejecución y, finalmente, en las columnas 5 y 10 el número de interdicciones. Como era de esperar el efecto de que las fallas se produzcan en los nodos genera un impacto mucho mayor en la vulnerabilidad de la red (cada nodo asocia un conjunto de aristas). Para el caso de las fallas en las aristas la red tolera la interdicción en 3 aristas. Para el caso de las fallas en los nodos la red tolera solo una interdicción. Los mismos resultados son presentados gráficamente en la ilustraciones 3 y 4, donde las fallas seleccionadas por el interdictor son presentadas como círculos rojos y la ruta seleccionada por el evasor como línea continua. De forma complementaria, en la figura 4 se grafica el resultado del modelo del mínimo k para ambas instancias.

Tabla 1. Uso de modelo multi falla con fallas localizadas en nodos y aristas

	Ω^k	$\Delta\%\Omega^k$	t (seg)	k		Ω^k	$\Delta\%\Omega^k$	t (seg)	k
Aristas	742		0,41	0	Nodos	742		0,14	0
	790	6%	1,23	1		790	6%	0,39	1
	795	7%	1,54	2		-	-	0,19	2
	925	25%	1,45	3					
	-	-	0,47	4					

Figura 2. Presentación de resultados de modelo multi falla para fallas localizadas en los nodos.

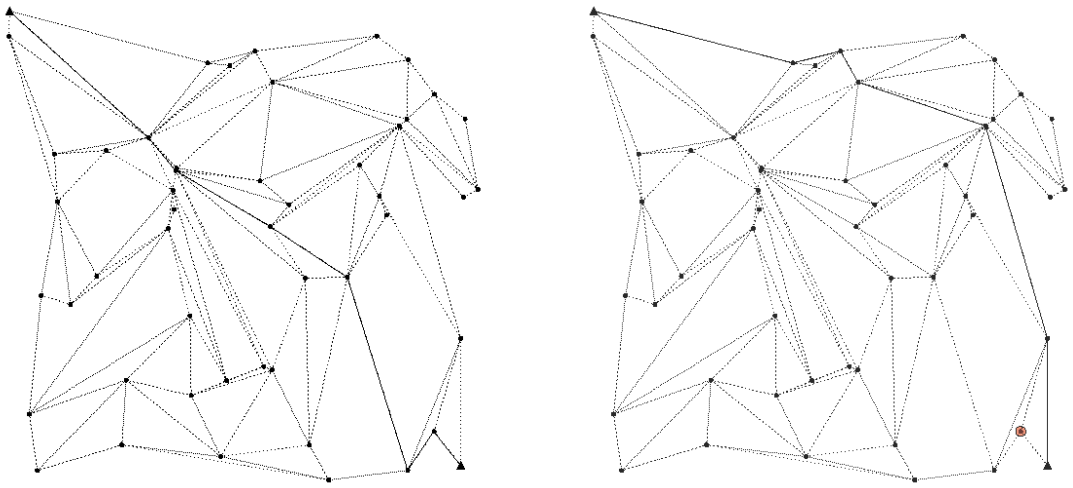


Figura 3. Presentación de resultados de modelo multi falla para fallas localizadas en las aristas.

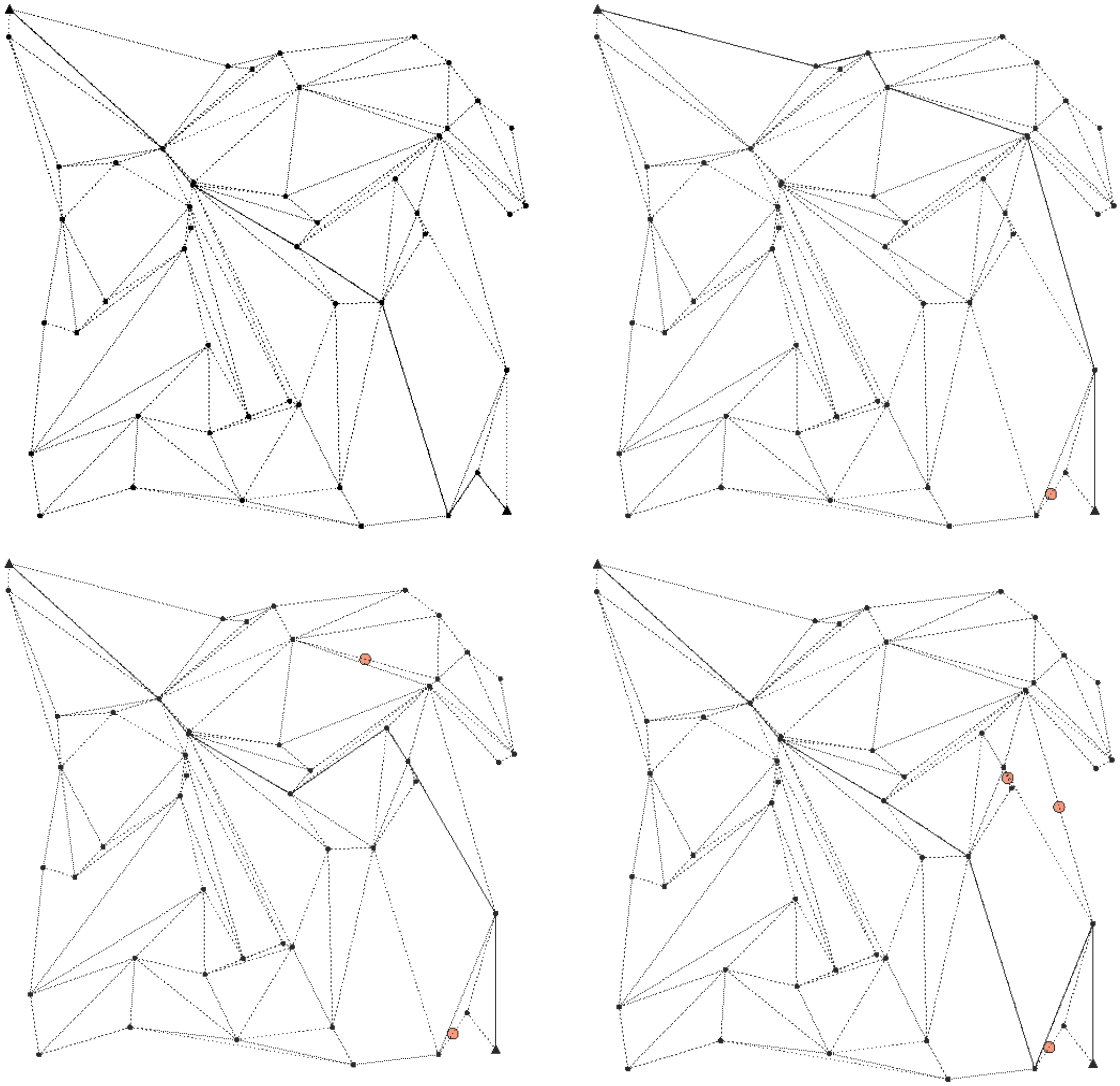
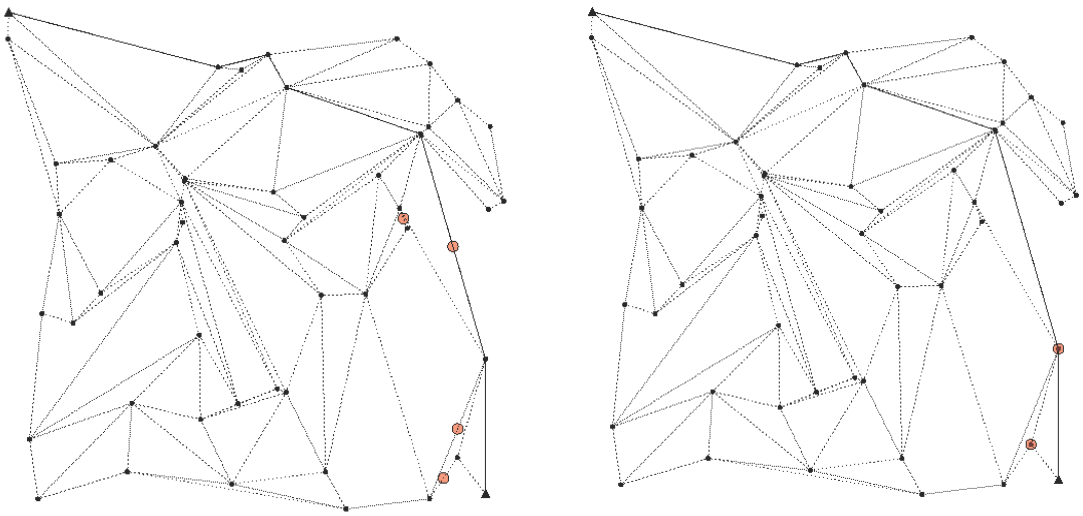


Figura 4. Modelo mínimo k para fallas localizadas en aristas (izquierda) y nodos (derecha).



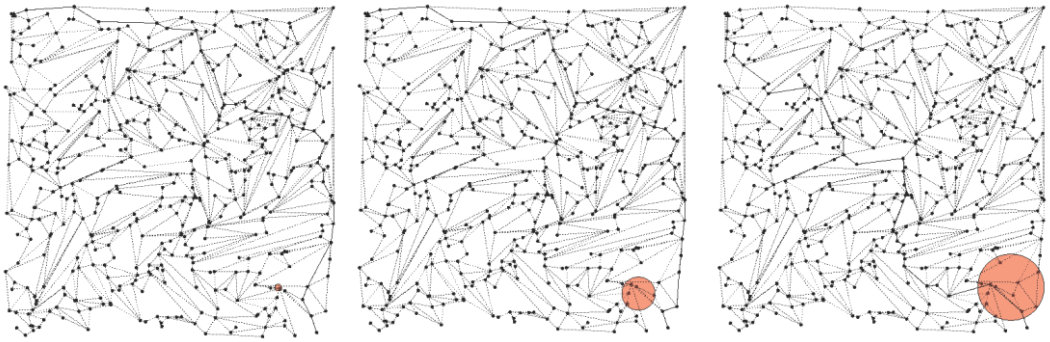
Con respecto a la complejidad computacional, el primer análisis consiste en evaluar el comportamiento del tiempo de ejecución en relación a una variación en el radio disco de falla $\boldsymbol{\rho}(\boldsymbol{x}, \boldsymbol{R})$ com $\boldsymbol{R}$: $\{\mathbf{0.01}, \mathbf{0.025}, \mathbf{0.05}, \mathbf{0.075}, \mathbf{0.1}\}$, se consideran 5 conjuntos de $\boldsymbol{ND}$ cada uno contiene 10 instancias con $\boldsymbol{n} = \mathbf{500}$, $\boldsymbol{\beta} = \mathbf{2}$, $\boldsymbol{\alpha} = \mathbf{1.6}$, $\boldsymbol{K} = \mathbf{1000}$, puntos de falla aleatorios en $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{y_1}, \boldsymbol{y_2}) = (\mathbf{0.1}, \mathbf{0.9}, \mathbf{0.1}, \mathbf{0.9})$. Para este análisis se utilizó el modelo de una falla.

En la Tabla 2 se presenta un identificador por cada grupo de instancias, el radio de falla **R**, los tiempos de ejecución mínimo (**min**), promedio ($\bar{\mathbf{t}}$) y máximo (**Max**) y el número de instancias del conjunto que se ve afectado por vulnerabilidad máxima ($\boldsymbol{V_{max}}$). A partir de la Tabla 2 se puede observar que el comportamiento del tiempo promedio es creciente hasta el grupo ID=3 y posteriormente, baja. Adicionalmente, la instancia que alcanza el mayor tiempo de ejecución la única que no es afectada en vulnerabilidad máxima para un $\boldsymbol{R} = \mathbf{0.75}$, en palabras simples, el tiempo aumenta en proporción a $\boldsymbol{R}$ hasta que la instancia es afectada por la vulnerabilidad máxima. En la Figura 5 se presenta un ejemplo del alcance de radios $\boldsymbol{R}$: $\{\mathbf{0.01}, \mathbf{0.05}, \mathbf{0.1}\}$ de izquierda a derecha.

Tabla 2. Comportamiento de tiempo de ejecución respecto al radio del disco de falla

ID	*R*	t (seg.)			V_{max}
		min	$\bar{t}$	Max	
1	0,010	421,13	535,95	827,90	0
2	0,025	521,53	664,40	846,71	0
3	0,050	554,69	848,92	1.079,57	0
4	0,075	282,02	442,69	1.352,75	9
5	0,100	325,42	476,34	845,28	10

Figura 5. Ejemplo de diferentes radios de falla



Un segundo análisis busca caracterizar el comportamiento del tiempo de ejecución en relación a una variación en el número de nodos, se consideran 6 conjuntos de $\boldsymbol{ND}$ cada uno contiene 10 instancias con $\boldsymbol{\beta} = \mathbf{2}$, $\boldsymbol{\alpha} = \mathbf{1.6}$, $\boldsymbol{K} = \mathbf{100}, \boldsymbol{R} = \mathbf{0.02}$ y puntos de falla aleatorios en $(\boldsymbol{x_1}, \boldsymbol{x_2}, \boldsymbol{y_1}, \boldsymbol{y_2}) = (\mathbf{0.1}, \mathbf{0.9}, \mathbf{0.1}, \mathbf{0.9})$. $\boldsymbol{P}$ara este análisis se utilizó el modelo de una falla. Se presenta un identificador por cada grupo de instancias y los tiempos de ejecución mínimo (**min**), promedio ($\bar{\mathbf{t}}$) y máximo (**Max**). De la Tabla 3 se puede observar que la variabilidad en los tiempos mínimos y máximos va aumentando de forma progresiva con el aumento del número de nodos, por otra parte, el tiempo promedio máximo bordea los 350 segundos, si bien no es un valor exagerado el crecimiento en el último tramo demuestra la pérdida de efectividad de algoritmo exacto usado por defecto desde el solver CPLEX.

Tabla 3. Comportamiento del tiempo computacional respecto del número de nodos

ID	Nodos	t (seg.)		
		min	$\bar{t}$	Max
1	100	1,20	1,33	1,68
2	250	4,42	5,34	6,21
3	500	16,75	18,52	21,08
4	750	40,83	47,15	60,61
5	1000	67,85	79,91	101,76
6	2000	253,21	346,60	512,81

Finalmente, se presenta un análisis del tiempo de ejecución en función de una variación en el número de puntos de falla $|\boldsymbol{\chi}|$ potenciales. Para este análisis se utiliza el modelo del mínimo número de fallas para vulnerabilidad total. Se consideran 7 conjuntos de $\boldsymbol{ND}$ cada uno contiene 10 instancias con $\boldsymbol{n = 250}$, $\boldsymbol{\beta = 2}$, $\boldsymbol{\alpha = 1.6}$, $\boldsymbol{R = 0.1}$, puntos de falla aleatorios en $(\boldsymbol{x_1, x_2, y_1, y_2}) = (\boldsymbol{0.1, 0.9, 0.1, 0.9})$. En la tabla 4 se presenta un identificador por cada grupo de instancias, el número de fallas potenciales $|\boldsymbol{\chi}|$, el $\boldsymbol{k}$ crítico promedio promedio $(\overline{\boldsymbol{k^c}})$, el número de instancias para las cuales existe $\boldsymbol{k}$ crítico ($\#\exists \boldsymbol{k^c}$) y los tiempos de ejecución mínimo (**min**), promedio ($\bar{\mathbf{t}}$) y máximo (**Max**).

Una primera conclusión es que cuando $|\boldsymbol{\chi}|$ es pequeño los resultados del modelo son inestables, es decir, para un conjunto nodos y aristas fijos al cambiar $\boldsymbol{\chi}$ (nuevos números aleatorios dentro de la misma zona) podríamos tener soluciones totalmente diferentes, no obstante a medida que vamos aumentando $|\boldsymbol{\chi}|$ los resultados alcanzan un valor estable, sin tener que llegar a excesos. Respecto al tiempo computacional, como era de esperar, es sensible a $|\boldsymbol{\chi}|$, no obstante, para valores muy grandes los tiempos de ejecución bordean los 300 segundos.

Tabla 4. Comportamiento del tiempo computacional respecto a los puntos de falla

ID	$\lvert\chi\rvert$	$\overline{k^c}$	$\#\exists k^c$	t (seg.)		
				min	$\bar{t}$	Max
1	50	2.1	7	8,30	21,84	41,23
2	100	1.7	10	17,47	37,31	89,83
3	150	1.6	10	27,22	57,36	160,96
4	200	1.0	10	36,96	39,45	46,33
5	400	1.0	10	91,95	120,38	244,67
6	800	1.0	10	123,38	141,16	171,59
7	1000	1.0	10	228,71	275,30	320,57

4. Conclusiones

En este trabajo se ha presentado un análisis experimental con modelos de optimización combinatorial para el problema de interdicción tipo *Camino más Corto*, incluyendo fallas individuales localizadas en nodos y en aristas. Además, se propone una política de falla probabilística que considera zonas con mayor concentración de interdicciones potenciales.

A través de lo anterior, se avanzó en su uso como modelo general de interdicción, que puede considerar fallas únicas y fallas múltiples, distintas superficies del disco de falla

(mayor o menor radio), dispersión de las potenciales fallas aleatoria o probabilísticas y casos particulares donde las potenciales fallas están localizadas en las aristas o los nodos.

De los tres parámetros estudiados, el modelo mostró mayor sensibilidad con el radio del disco de falla, superando los 1.300 segundos en una ocasión. No obstante, el modelo también demostró cierta sensibilidad con el número de nodos y el número de fallas potenciales. Se deduce que al someter al modelo a exigencia en los tres parámetros el desempeño del algoritmo exacto del solver va a perder su efectividad en mayor grado.

Como futuras líneas de trabajo vinculadas, se proponen algunas extensiones de los modelos matemáticos relacionados a incorporación de radio de falla diferenciados y costo de interdicción asociado al radio de falla. Desde el punto de vista algorítmico parece fundamental el diseño de algoritmos tanto exactos como heurísticos para la resolución de este problema o del modelo de interdicción a otros modelos subyacentes. Finalmente, es importante tener evidencias teóricas respecto al status de complejidad computacional de este conjunto de modelos.

5. Bibliografía

[1] S. An, N. Cui, Y. Li y X. Ouyang, «Ouyang, Location planning for transit-based evacuation under the risk of service disruptions,» *Transportation Research Part B*, vol. 54, pp. 1-16, 2013.

[2] J. Salmerón, K. Wood y R. Baldick, «Analysis of electric grid security under terrorist thread,» *Transactions on Power Systems IEEE*, vol. 19, nº 2, p. 905–912, 2004.

[3] R. Wollmer, «Removing arcs from a network,» *Operations Research*, vol. 12, p. 934–40, 1964.

[4] R. Wood, «Deterministic network interdiction,» *Mathematical and Computer Modelling*, vol. 17, nº 2, p. 1–18, 1993.

[5] D. Altner, Ö. Ergunb y N. Uhan, «The Maximum Flow Network Interdiction Problem: Valid inequalities, integrality gaps, and approximability,» *Operations Research Letters*, vol. 38, pp. 33-38, 2010.

[6] J. Royset y R. Wood, «Solving the Bi-Objective Maximum-Flow Network-Interdiction,» *INFORMS Journal of Computing*, vol. 19, nº 2, pp. 175-184, 2007.

[7] R. Church y M. Scaparra, «Protecting critical assets: the r-interdiction median problem with fortification,» *Geographical Analysis*, vol. 19, p. 129–46, 2006.

[8] C. Losada, M. Scaparra y J. O´Henley, «Optimizing system resilience: a facility protection model with recovery time,» *European Journal of Operational Research*, vol. 217, nº 3, pp. 519-530, 2012.

[9] T. Grubesic y A. Murray, «Vital nodes, interconnected infrastructures and the geographies of network survivability,» *Annals of the Association of American Geographers*, vol. 96, nº 1, pp. 64-83, 2006.

[10] C. Bazgan, S. Toubaline y D. Vanderpooten, «Complexity of determining the most vital elements for the p-median and p-center location problems,» *J. Combinatorial Optimization*, vol. 26, nº 1, pp. 178-189, 2013.

[11] C. Bazgan, S. Toubaline y D. Vanderpooten, «Critical edges/nodes for the minimum spanning tree problem: complexity and approximation,» *J. Combinatorial Optimization*, vol. 26, nº 1, pp. 178-189, 2013.

[12] H. Corly y D. Sha, «Most vital links and nodes in weighted networks,» *Operations Research Letters*, vol. 1, p. 157–160, 1982.

[13] G. Frederickson y R. Solis-Oba, «Increasing the weight of minimum spanning trees, In: Proceedings of the seventh ACM-SIAM symposium on discrete algorithms,» *Journal of Algorithms*, vol. 33, nº 2, p. 244–66, 1999.

[14] «Efficient algorithms for finding the most vital edge of a minimum spanning tree,» *Information Processing Letters*, vol. 48, nº 5, p. 211–213, 1993.

[15] E. Israeli y R. Wood, «Shortest-path network interdiction,» *Networks*, vol. 40, nº 2, p. 97–111, 2002.

[16] M. Bell y C. Cassir, «Risk-averse user equilibrium traffic assignment: an application of game theory,» *Transportation Research Part B - Methodological*, vol. 36, pp. 671-681, 2002.

[17] M. Bell, U. Kanturska, J. Schmöcker y A. Fonzone, «Attacker-defender models and road network vulnerability,» *Philosophical Transactions of the Royal Society A*, vol. 366, p. 1893–1906, 1998.

[18] J. Yates y S. Sanjeevi, «A length-based, multiple-resource formulation for shortest path network interdiction problems in the transportation sector,» *International Journal of Critical Infrastructure Protection*, vol. 6, p. 107–119, 2013.

[19] H. Bayrak y M. Bailey, «Shortest Path Network Interdiction with Asymmetric Information,» *Networks*, vol. 53, nº 2, p. 133–140, 2008.

[20] T. Matisziw y A. Murray, «Modeling s–t path availability to support disaster vulnerability assessment of network infrastructure,» *Computers & Operations Research*, vol. 36, p. 16 – 26, 2009.

[21] E. Álvarez–Miranda, A. Candia-Véjar, E. Carrizosa y F. Pérez-Galarce, «Vulnerability Assessment of Spatial Networks: Models and Solutions,» de *LNCS series*, Springer-Verlag, 2014.

[22] D. Fulkerson y G. Harding, «Maximizing the minimum source-sink path subject to a budget constraint,» *Mathematical Programming*, vol. 13, nº 1, p. 116–118, 1977.

[23] B. Golden, «A problem in network interdiction,» *Naval Research Logistics Quarterly*, vol. 25, nº 4, p. 711–713, 1978.

[24] C. Phillips, «The network inhibition problem,» *In Proceedings of the Twentyfifth Annual ACM Symposium on Theory of Computing, STOC '93,* p. 776–785, 1993.

[25] K. Cormican, D. Morton y R. Wood, «Stochastic network interdiction,» *Operations Research*, vol. 46, nº 2, p. 184–197, 1998.