

Vulnerability Assessment of Spatial Networks: Models and Solutions

Eduardo Álvarez-Miranda^{1,2}, Alfredo Candia-Véjar², Emilio Carrizosa³, and
Francisco Pérez-Galarce²

¹ DEI, Università di Bologna, Italy e.alvarez@unibo.it

² DMGI, Universidad de Talca, Chile {ealvarez,acandia,franperez}@utalca.cl

³ Facultad de Matemáticas, Universidad de Sevilla, Spain ecarrizosa@sevilla.es

Abstract. In this paper we present a collection of combinatorial optimization problems that allows to assess the vulnerability of spatial networks in the presence of disruptions. The proposed measures of vulnerability along with the model of failure are suitable in many applications where the consideration of failures in the transportation system is crucial. By means of computational results, we show how the proposed methodology allows us to find useful information regarding the capacity of a network to *resist* disruptions and under which circumstances the network collapses.

1. Introduction

Shortest path problems correspond to an old and very known class of problems in combinatorial optimization. A variant of one of these basic problem consists on analyzing the effects of removing arcs from a network. In [14] the problem of removing k arcs that cause the greatest decrease in the maximum flow from a source to a sink in a planar network is studied. This problem is a special case of a broad class of network optimization problems known as *interdiction* problems. Applied to the shortest s, t -path problem, the interdiction problem can be defined in the following way. Given a graph $G = (V, E)$ with a non-negative length function on its arcs $l : E \rightarrow \mathbb{R}$ and two terminals $s, t \in V$, the goal is to destroy all (or the *best*) paths from s to t in G by *optimally* eliminating as many arcs of A as possible (usually respecting a so-called *interdiction budget*). Interdiction problems are often used to measure the robustness of solutions of network optimization problems. In [9] several versions of these problems are studied; they consider the case of *total limited interdiction* when a fixed number of k arcs can be removed, and *node-wise limited interdiction* (for each node $v \in V$ a fixed number $k(v)$ of out-going arcs can be removed). For a complete survey on early interdiction problems with different underlying network properties the reader is referred to [2]. For a more general discussion regarding network vulnerability approaches we suggest to see [10].

Based on a well-known network interdiction model we formulate a framework of combinatorial optimization problems whose solutions can be used for assessing the vulnerability of spatial networks in the case of disruptions. We design

a flexible model of network disruption based on the geometric characteristics of spatial networks. This model incorporates the nature of the disruptions present in different situations such as military planning [5, 8], terrorist attacks [12] or emergency control of infectious disease spreading [1]. The proposed problems, along with the model of disruption, span several realizations of network interdiction providing a useful tool to characterize network vulnerability. Our aim is to propose a methodology that uses network optimization problems to characterize the robustness of a network in the presence of multiple failures.

In §2 we present the optimization framework for vulnerability assessment; in §3 we report computational results on realistic instances; these results show the versatility of the proposed models to characterize the robustness of the network infrastructure. Finally, in §4 we draw final conclusions and propose paths for future work.

2. Vulnerability Measures as Optimization Problems

Notation Let $G = (V, E)$ be a spatial network such that $|V| = n$ and $|E| = m$. Let $s, t \in V$ be a source and a target node respectively; $l_e, \forall e : \{i, j\} \in E$, be the cost of edge e (distance between i and j); and ℓ be the cost of the shortest s, t -path on G with edge costs given by $l_e, \forall e \in E$.

Let $\mathcal{X} \subset \mathbb{R}^2$ be an arbitrary sub-region of \mathbb{R}^2 . An element $x \in \mathcal{X}$ is a *point* in \mathcal{X} ; for a given point x and a given edge e , let $d(x, e)$ be the minimum distance between x and the line segment defined by e (recall that $e : \{i, j\}$ links node i with node j , whose positions are given). For a given $R \in \mathbb{R}^{>0}$ and a given $x \in \mathcal{X}$, let $E_x = \{e \in E \mid d(e, x) > R\}$ and $\bar{E}_x = \{e \in E \mid d(e, x) \leq R\}$. In other words, E_x is the set of edges that are not *reached* by the disk of radius R centered at x (the *disruption disk* $\rho(x, R)$), and \bar{E}_x is the set of disrupted or interdicted edges. We will refer to $G_x = (V, E_x)$ as the *operating network* with respect to $\rho(x, R)$. Note that G_x might be disconnected.

The model of failure represented by $\rho(x, R)$ embodies a characteristic of disruption produced by many different sources: instead of having isolated failures, we have a set of failures all of them circumscribed within a delimited area. This naturally occurs in the application contexts that we have already mentioned.

2.1 The Max-Cost Single-Failure Shortest Path Problem

Let us assume that \mathcal{X} is a finite set of points x in \mathbb{R}^2 and that R can take values in \mathcal{R} which is a finite subset of $\mathbb{R}^{>0}$. Given a radius $R \in \mathcal{R}$ and a discrete set \mathcal{X} , we are interested in knowing what is the *maximum* length Ω of a *shortest* s, t -path across all possible locations $x \in \mathcal{X}$ of the disruption disk $\rho(x, R)$.

Knowing Ω is threefold: (i) It tells us how severe a disruption can be by comparing the value of Ω with respect to ℓ ; in other words, the increase of the transportation time between s and t induced by a failure located in the *worst* location $x^* = \arg_{x \in \mathcal{X}} \{\Omega\}$. (ii) From the tactical point of view, *preventive* actions can be taken in order to reduce the chances that a failure can be produced at x^*

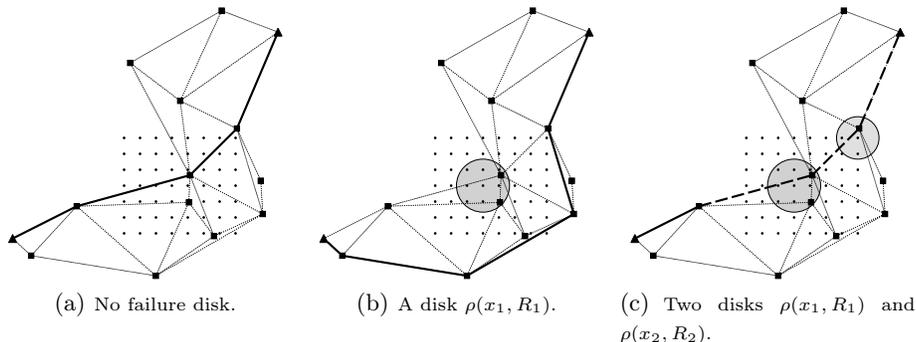


Fig. 1. Example of a network $G = (V, E)$, nodes s and t , a region \mathcal{X} and different interdiction cases.

or the edges \bar{E}_{x^*} can be reinforced to increase their reliability. And (iii) we can know whether the network is *so* vulnerable that s and t might be disconnected, which can be verify if $\Omega = \infty$.

The problem of calculating Ω will be called the Max-Cost Single-Failure Shortest Path Problem (MCSFSPP). Therefore, the MCSFSPP is an optimization problem whose objective function value is a vulnerability measure of the network on which it is solved. Intuitively, the MCSFSPP can be solved as follows. For a given $x \in \mathcal{X}$, let ℓ_x be the cost of the shortest s, t -path on G_x with edge costs l_e^x defined as $l_e^x = l_e$ if $e \in E_x$ and $l_e^x = M$ if $e \in \bar{E}_x$, with $M = O(m \max_{e \in E} l_e)$; therefore, $\Omega = \max_{x \in \mathcal{X}} \ell_x$. If $\Omega > M$ then there is at least one x for which s and t cannot be connected.

In Figure 1(a) it is shown a network $G = (V, E)$ where s and t correspond to the nodes represented with triangles and \mathcal{X} is represented by a grid of 8×7 points in the background of part of G ; an optimal s, t -path is shown with bold edges. In Figure 1(b) we show the case where a disruption disk $\rho(x_1, R_1)$ interdicts the network such that an alternative (an more expensive) s, t -path has to be established ($\Omega < M$). And in Figure 1(c) a more complex situation is shown; here two disruption disks, $\rho(x_1, R_1)$ and $\rho(x_2, R_2)$, are simultaneously interdicting the network. In the latter case all possible s, t -paths (one of them is shown in bold dashed lines) have at least one interdicted edge, i.e., $\Omega > M$.

The MCSFSPP is closely related with the network interdiction problems studied in [4, 5, 11, 3, 8, 7]. In the following, we will use this basic definition to construct generalizations addressing different, but complementary, measures of vulnerability under different models of failure.

Mixed Integer Programming Formulation for the MCSFSPP

Let $\mathbf{f} \in [0, 1]^m$ be a vector of $[0, 1]$ -flow variables. An s, t -path p in G is induced by a given allocation of flows \mathbf{f} if the following constraints are satisfied:

$$\sum_{k \in V | e: \{j, k\} \in E} f_{j, k} - \sum_{i \in V | e: \{i, j\} \in E} f_{i, j} = \begin{cases} 1, & \text{if } j = s \\ 0, & \text{if } j \in V \setminus \{s, t\} \\ -1, & \text{if } j = t. \end{cases} \quad (\text{SP.1})$$

For a given $x \in \mathcal{X}$, the problem of finding ℓ_x can be defined as

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

Let $\mathbf{y} \in \{0, 1\}^{|\mathcal{X}|}$ be a vector of binary variables such that $y_x = 1$ if the failure disc is centered at x and $y_x = 0$ otherwise. Now, let $\mathbf{z} \in \{0, 1\}^m$ be a set of binary variables such that $z_e = 1$ if edge e is *operative* and $z_e = 0$ otherwise for any given $x \in \mathcal{X}$. Variables \mathbf{y} and \mathbf{z} are related as follows

$$y_x + z_e \leq 1, \quad \forall e \in E \mid d(e, x) \leq R, \quad \forall x \in \mathcal{X} \quad (\text{YZ.1})$$

$$\sum_{x \in \mathcal{X} \mid d(e, x) > R} y_x - z_e \leq 0, \quad \forall e \in E. \quad (\text{YZ.2})$$

Constraints (YZ.1) and (YZ.2) state that, for any $x \in \mathcal{X}$, an edge e has to be operative ($z_e = 1$) if it is not reached by the disruption disk $\rho(x, R)$. Since a single disruption disk affects the network, we have that

$$\sum_{x \in \mathcal{X}} y_x = 1. \quad (\text{YZ.3})$$

Using (YZ.1) and (YZ.2), for a given $x \in \mathcal{X}$ the edge costs l_e^x can be written as $l_e^x = l_e z_e + (1 - z_e)M$, $\forall e \in E$. Hence, the MCSFSPP is as follows

$$\Omega = \max_{x \in \mathcal{X}} \left\{ \ell_x \mid (\text{YZ.1}), (\text{YZ.2}), (\text{YZ.3}) \text{ and } (\mathbf{y}, \mathbf{z}) \in \{0, 1\}^{m+|\mathcal{X}|} \right\}. \quad (\Omega)$$

Problem (Ω) , as it is, is non-linear. To linearize it, we will convert the max min objective into a pure max one; to do so, let us consider the dual of (ℓ_x) , which is given by

$$\ell_x = \max \{ \gamma_t - \gamma_s \mid \gamma_j - \gamma_i \leq l_{ij} z_{ij} + (1 - z_{ij})M, \quad \forall e: \{i, j\} \in E \text{ and } \boldsymbol{\gamma} \in \mathbb{R}^n \}. \quad (\lambda)$$

Embedding (λ) into (Ω) , we get the next Mixed Integer Programming Formulation (MILP) formulation for the MCSFSPP:

$$\Omega = \max \quad \gamma_t - \gamma_s \quad (\text{MCSF.1})$$

$$\text{s.t.} \quad (\text{YZ.1}), (\text{YZ.2}) \text{ and } (\text{YZ.3}) \quad (\text{MCSF.2})$$

$$\gamma_j - \gamma_i \leq l_{ij} z_{ij} + (1 - z_{ij})M, \quad \forall e: \{i, j\} \in E \quad (\text{MCSF.3})$$

$$(\mathbf{y}, \mathbf{z}) \in \{0, 1\}^{m+|\mathcal{X}|} \text{ and } \boldsymbol{\gamma} \in \mathbb{R}^n. \quad (\text{MCSF.4})$$

Note that in our approach we assume that $\rho(x, R)$ can be located in any point $x \in \mathcal{X}$ without any stochastic characterization. That is, any point $x \in \mathcal{X}$ is likely to “host” the center of the failure.

In the proposed setting we assume that if an edge e is disrupted by at least one failure disk $\rho(x, R)$, then it becomes inoperative. However, one can easily extend this to a more general case by defining a coefficient $d_e \geq 0 \forall e \in E$ representing the *delay* on edge e in case of interdiction (in our setting $d_e = M \forall e \in E$). The MCSFSPP can be redefined by replacing constraint (MCSF.3) with

$$\gamma_j - \gamma_i \leq l_{ij} + (1 - z_{ij})d_{ij}, \forall e : \{i, j\} \in E. \quad (\text{MCSF.3b})$$

The Shortest-Path Network Interdiction problem presented in [8] is very similar to the definition of the MCSFSPP using (MCSF.3b) instead of (MCSF.3). In that problem, edges can be interdicted without any geometrical pattern among them; instead, they consider interdiction costs so that any feasible disruption of the network should not cost more than a given interdiction *budget*. Later we formally define these concepts and adapt them to our setting.

2.2 The Multiple Failures Case

As described above, in the MCSFSPP only a single failure $\rho(x, R)$ occurs. However, there are applications in which this characteristic does not hold and, instead, multiple failures occur simultaneously. More precisely, we now have that k failure disks $\rho(x_1, R), \dots, \rho(x_k, R)$ of radius R are located in \mathcal{X} , resulting in an operative network $G_{\mathbf{x}^k} = (V, E_{\mathbf{x}^k})$ where $E_{\mathbf{x}^k} = \{e \in E \mid \min_{x \in \{x_1, \dots, x_k\}} d(e, x) \leq R\}$. Under these conditions, finding the maximum cost, across all possible $\{x_1, \dots, x_k\} \in \mathcal{X}^k$, of the shortest s, t -path on $G_{\mathbf{x}^k}$ can be done by modifying MCSFSPP as follows. Instead of (YZ.3), we have

$$\sum_{x \in \mathcal{X}} y_x = k. \quad (\text{YZ.3k})$$

Besides, constraint (YZ.2) should be now adapted in order to impose that $z_e = 1$ if none of the k failure disks reaches e ; the new constraint is

$$\sum_{x \in \mathcal{X} \mid d(e, x) > R} y_x - z_e \leq 1 - \sum_{x \in \mathcal{X}} y_x, \forall e \in E, \quad (\text{YZ.2k})$$

clearly if $k = 1$, then (YZ.2k) corresponds to (YZ.2). Therefore, the Max-Cost Multiple-Failure Shortest Path Problem (MCMFSPP) can be formulated as

$$\Omega^k = \max \{\gamma_s - \gamma_t \mid (\text{YZ.1}), (\text{YZ.3k}), (\text{YZ.2k}), (\text{MCSF.3}) \text{ and } (\text{MCSF.4})\} \quad (\text{MCMF})$$

Note that in formulation (MCMF) it is assumed that $R \in \mathcal{R}$ is known in advance.

Maximal Disruption for an interdiction budget Similar as in [3, 8, 7], let us consider that associated with each point $x \in \mathcal{X}$ there is a disruption *cost*

$c_x > 0$. Assume that the interdictors have a *budget* B of interdiction *resources*, so that they can disrupt the network using several disks $\rho(x, R)$ as long as the total cost does not exceed B . Formally, the interdiction-budget constraint is given by

$$\sum_{x \in \mathcal{X}} c_x y_x \leq B; \quad (\text{IB})$$

so the Budget Constrained MCMFSPP is formulated as

$$\Omega^k = \max\{\gamma_s - \gamma_t \mid (\text{YZ.1}), (\text{YZ.2k}), (\text{IB}), (\text{MCSF.3}) \text{ and } (\text{MCSF.4})\} \quad (\text{B})$$

By solving (B) we can know *how* vulnerable the network is if the interdictors are able to optimally use their resources to disrupt it. Models as the one presented in [8, 7] are particular cases of (B) in which \mathcal{X} coincides with the midpoint of every edge $e \in E$ and $R = \epsilon$ (ϵ being infinitesimally small).

Minimum Simultaneity for Complete Vulnerability: Critical k One might be interested in knowing the minimum number of failures (the *critical k* or k^c) that should occur simultaneously in order to have at least one set $\rho(x_1, R), \dots, \rho(x_k, R)$ that damages the network so that s and t cannot be connected anymore or the shortest length between them is greater than a threshold Θ .

The value k^c and the corresponding collection $\{x_1, \dots, x_{k^c}\}$ will enable a decision maker to perform more general preventive actions to endure the network not in a single but in several areas. In many practical contexts, the possibility of multiple and synchronized failures might be the rule, so knowing k^c might play a strategical role. Clearly, for a given R , the larger k^c is the more robust the network is. Mathematically, one can formulate the search for k^c as

$$k^c = \min \{k \mid (\text{YZ.1}), (\text{YZ.2k}), (\text{YZ.3k}), (\text{MCSF.3}), (\text{MCSF.4}), \gamma_s - \gamma_t \geq \Theta \text{ and } k \in \mathbb{Z}_{\geq 0}\} \quad (k^c)$$

If $\Theta = M$, then (k^c) aims at finding the minimum k such that allocating k disks produces a disconnection between s and t . A similar model is presented in [7] in the context of interdiction in stochastic networks.

If instead of k^c one is interested in knowing the minimum *cost* needed to produce a damage represented by Θ , model (k^c) can be easily modified by replacing the objective function of (k^c) with $C^c = \min \sum_{x \in \mathcal{X}} c_x y_x$.

3. Computational Results

3.1 Instance Benchmark and Solver Setting

Instance Benchmark For our experiments we consider three sets of instances: ND, US and Bangladesh.

In the first set, the instances are generated as follows: (i) n points are randomly located in a unit Euclidean square; (ii) a minimum spanning tree connecting all points is calculated; (iii) $\beta \times n$ additional edges are added to the network

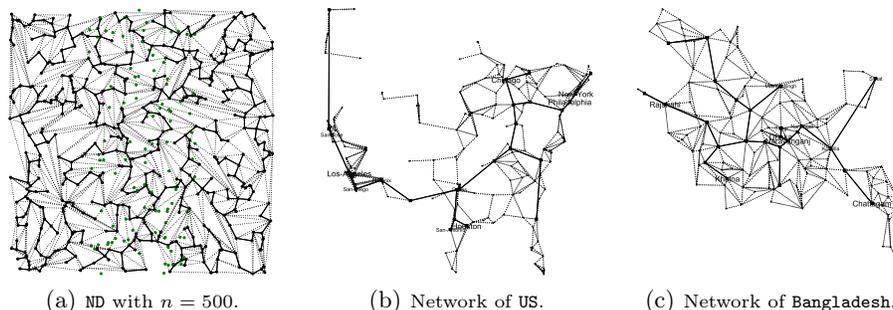


Fig. 2. Representation of the instances used for computations.

such that an edge is added if l_{ij} (euclidean distance) satisfies $l_{ij} \leq \alpha/\sqrt{n}$ and the planarity of the network is still preserved; (iv) the set \mathcal{X} is created by randomly located K points within the area defined by points (x_1, y_1) , (x_2, y_1) , (x_1, y_2) and (x_2, y_2) .

For experiments we have considered $n \in \{500, 1000\}$, $\beta = 1.5$, $\alpha = 1.6$, $(x_1, x_2, y_1, y_2) = (0.3, 0.7, 0.0, 1.0)$ (\mathcal{X}_1) and $(x_1, x_2, y_1, y_2) = (0.1, 0.9, 0.1, 0.9)$ (\mathcal{X}_2), and $K = 100$.

In Figure 2(a) it is shown an example of an instance with 500 nodes and \mathcal{X} contained in $(0.3, 0.0)$, $(0.7, 0.0)$, $(0.3, 1.0)$ and $(0.7, 1.0)$.

In the case of groups **US** and **Bangladesh** we consider the geographical coordinates of the most populated cities in each case [see 13] to define the set V . Then, we used an approximation of their highway and interurban road system with the information available in [6] to approximate the set of edges E . The set \mathcal{X} is created by randomly located K points within the area defined by points (x_1, y_1) , (x_2, y_1) , (x_1, y_2) and (x_2, y_2) . In Figures 2(b) and 2(c) we show the networks used to generate the instances **US** and **Bangladesh** respectively. In the case of **US**, the area \mathcal{X} is given by placing 100 points in the so-called *south* area. With this we intend to represent possible cases of failure produced by hurricanes and other natural disasters. For the **Bangladesh** instances, we have created \mathcal{X} by placing 100 points in squared area in the very center that covers around the 15% of the total area.

In the case of instances **ND**, nodes s and t are selected as those with the longest euclidean distance. In the case of instances **US** we have used $s \in \{\text{NY:New York, CH:Chicago}\}$ and $t \in \{\text{LA:Los Angeles, HS:Houston}\}$; likewise, in the case of instances **Bangladesh** we have used $s = \text{Rajshahi}$ and $t = \text{Silhat}$.

Solver Setting Models (MCSF.1)-(MCSF.4), (MCMF) and (k^c) were solved using CPLEX 12.5 (all CPLEX parameters were set to their default values). The experiments were performed on a Intel Core i7-3610QM machine with 8 GB RAM.

$n = 500$						$n = 1000$					
\mathcal{X}_1			\mathcal{X}_2			\mathcal{X}_1			\mathcal{X}_2		
R	$\Delta\% \Omega$	t[sec]									
0.01	2.17	38.92	0.01	0.00	32.93	0.01	2.48	115.39	0.01	0.14	144.66
0.02	3.93	46.46	0.02	1.64	36.83	0.02	2.93	153.58	0.02	0.69	215.16
0.03	3.93	65.63	0.03	1.64	49.73	0.03	5.38	235.95	0.03	1.52	240.88
0.04	5.15	80.79	0.04	1.64	63.06	0.04	7.31	258.85	0.04	1.52	265.00
0.05	5.15	103.01	0.05	1.64	79.67	0.05	7.17	395.46	0.05	1.52	259.80
0.10	5.15	97.83	0.10	1.64	112.76	0.10	8.69	917.78	0.10	3.87	373.61
0.15	-	53.70	0.15	10.64	111.65	0.15	9.93	587.27	0.15	6.19	843.45

Table 1. Solutions for the MCSFSPP considering different values of R (Instances ND)

3.2 Vulnerability Assessment of Spatial Networks: Solutions

From the operative perspective, the value of R corresponds to the *intensity* of a disruption. If we consider the MCSFSPP or the MCMFSPP we would expect that a *vulnerable* network is such that Ω increases quickly (up to M) when R increases marginally. On the other hand, a *reliable* network is such that the cost of the shortest s, t -path does not change *too much* even if R increases considerably.

In Table 1 we report solutions for the MCSFSPP for instances of group ND considering different values of n , different compositions of set \mathcal{X} and different values of R (columns 1, 4, 7 and 10). In columns $\Delta\% \Omega$ is reported the relative increase of Ω , for a given \mathcal{X} and a given R , with respect to cost of the shortest s, t -path without any failure. In this column, "-" means that all paths have been disrupted. In columns t[sec] are reported the running times in seconds needed to reach optimality. One can observe from this table that when the area where the failure can occur, \mathcal{X} , is such that covers a *stripe* on the network (as \mathcal{X}_1) then it is more vulnerable (see the values $\Delta\% \Omega$ for different R) than a network in which the failure area, although larger, still leaves *corridors* where s, t -paths can be constructed, as for \mathcal{X}_2 . In a warfare context, if we were to be the enemies, this analysis would suggest us that is better to concentrate our resources in a narrower area potentially spanning a complete stripe of the network than in a larger area (which might be more expensive) that does not properly covers the network. On the other hand, who wants to protect the network should concentrate the efforts in protecting at least one corridor connecting s and t .

In Tables 2 and 3, results for (MCMF) and (k^c), respectively, are reported. The analysis is similar as for Table 1. From Table 2 we can see that the increase of $\Delta\% \Omega$ (due to a larger k), is greater for \mathcal{X}_1 than for \mathcal{X}_2 . Along the same lines, we see from Table 3 that the minimum resources needed to disconnect s and t (see columns k^c) are greater for \mathcal{X}_2 than for \mathcal{X}_1 . In Table 3, when results for a given R are not reported (e.g., $R = 0.01$ for $n = 500$ and \mathcal{X}_1) is because not even $|\mathcal{X}|$ failure disks are enough to make the s, t connectivity collapse. This applies for all the remaining Tables.

500								1000							
\mathcal{X}_1				\mathcal{X}_2				\mathcal{X}_1				\mathcal{X}_2			
R	k	$\Delta\% \Omega$	t[sec]	R	k	$\Delta\% \Omega$	t[sec]	R	k	$\Delta\% \Omega$	t[sec]	R	k	$\Delta\% \Omega$	t[sec]
0.01	1	2.17	24.15	0.01	1	0.00	22.51	0.01	1	2.48	88.16	0.01	1	0.01	88.64
	2	3.93	25.07		2	0.00	21.96		2	3.03	94.80		2	0.09	96.35
	3	4.74	25.02		3	0.00	22.11		3	3.03	93.90		3	1.63	93.57
	4	5.56	24.87		4	0.00	22.21		4	3.03	95.08		4	1.63	95.08
	5	6.79	24.52		5	0.00	22.14		5	3.03	94.15		5	1.63	94.4
0.1	1	5.15	59.94	0.1	1	1.64	69.61	0.1	1	8.68	889.61	0.1	1	3.87	222.36
	2	-	26.43		2	13.82	142.93		2	17.89	3448.93		2	8.16	1012.06
	3	-	98.05		3	13.92	297.95		3	21.24	75319.9		3	12.45	5434.01
	4	-	526.47		4	-	63.01		4	28.14	26123.3		4	21.99	13130.3
	5	-	147.39		5	-	149.54		5	-	16576.5		5	-	742.63

Table 2. Solutions for the MCMFSPP considering different values of R and k (Instances ND)

n	\mathcal{X}	R	k^c	t[sec]	n	\mathcal{X}	R	k^c	t[sec]
500	\mathcal{X}_1	0.10	2	170.76	1000	\mathcal{X}_1	0.10	5	628.76
		0.15	1	43.09			0.15	2	805.32
	\mathcal{X}_2	0.03	10	39.05		\mathcal{X}_2	0.02	19	219.38
		0.04	9	109.70			0.03	13	621.60
		0.05	7	161.06			0.04	11	933.85
		0.10	4	274.20			0.05	8	1759.32
		0.15	3	162.47			0.10	5	1277.24
							0.15	3	1214.14

Table 3. Solutions of (k^c) considering different values of R (Instances ND)

From the algorithmic point of view, we can notice in Tables 1, 2 and 3 that the search for an alternative path in a disrupted network is not *for free*. In all cases we see an increase of the algorithmic effort (time) needed to find such a path (if exists). This is due to the high combinatorial nature of the problem when more edges are subject to be interdicted (when R increases and/or when k is either greater than 1 or when it is a variable).

In the case of USA Instances, we report in Table 4 results of the MCSFSPP considering different pairs of s and t and different values of R . In this case, we can see that different combinations of s and t yield to different levels of vulnerability in the system. For instance, the network is considerably more vulnerable when it is intended to host a path from Chicago to Los Angeles than when the path should be established from Chicago to Houston. This is due to the fact that, in our instance, the system of roads connecting the north of the Midwest with the south of the West Coast is composed by relatively few elements. Hence, a single disruption disk (that is optimally placed) is enough to interrupt the communication between the cities. In this case the values of $\Delta\% \Omega$ are particu-

{NY, LA}			{CH, LA}			{NY, HS}			{CH, HS}		
R	$\Delta\% \Omega$	t[sec]									
0.01	9.00	17.22	0.01	0.00	17.43	0.01	13.00	17.25	0.01	0.00	17.22
0.02	10.00	21.42	0.02	20.00	25.05	0.02	13.00	26.83	0.02	2.00	20.12
0.03	10.00	24.77	0.03	20.00	33.17	0.03	15.00	22.25	0.03	2.00	35.27
0.04	10.00	23.57	0.04	20.00	31.29	0.04	18.00	23.07	0.04	2.00	28.31
0.05	10.00	25.30	0.05	20.00	35.51	0.05	19.00	25.04	0.05	8.00	36.15
0.10	30.00	34.16	0.10	-	33.67	0.10	45.00	42.31	0.10	-	30.67
0.15	-	40.22	0.15	-	28.41	0.15	-	29.69	0.15	-	28.17
0.20	-	28.00	0.20	-	48.14	0.20	-	27.16	0.20	-	37.13

Table 4. Solutions for the MCSFSPP considering different values of R (Instances USA)

larly important from the tactic point of view; if it is up to the decision maker to decide where to establish both the source and the target of the transportation system, then it might preferable to have New York - Houston than, for instance, Chicago - Los Angeles. However, this analysis is valid only when a single failure occurs. For an approximate equivalence to real distances in kilometers, R should be multiply by 1700.

In Figure 3(a) we show the solution of the shortest path problem between New York and Houston when there is no disruption. In Figure 3(b) is shown the solution of the MCMFSPP when 5 disruption disks with $R = 0.01$ are optimally located. In Figure 3(c) is shown the solution of the MCMFSPP with $k = 1$ and $R = 0.10$. These figures show how different the optimal s, t -paths can be when the network is disrupted by failures of different magnitude.

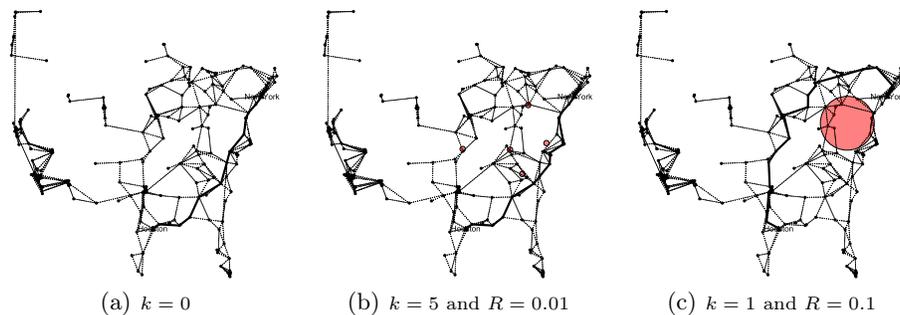


Fig. 3. Solutions for the MCMFSPP for different k and R (Instances USA)

Finally, in Table 5 we report results for the Instances **Bangladesh**. From the solutions of the MCSFSPP (reported in columns 1-3) we can see that the relatively dense road system of this country is able to *resist* (small values of $\Delta\% \Omega$), reasonably well the optimal location of a single failure disk up to $R =$

						$R = 0.01$			$R = 0.1$		
R	$\Delta\% \Omega$	t[sec]	R	k^c	t[sec]	k	$\Delta\% \Omega$	t[sec]	k	$\Delta\% \Omega$	t[sec]
0.01	3.76	8.72	0.05	3	10.06	1	3.76	7.69	1	24.17	8.11
0.02	2.93	7.44	0.10	2	28.52	2	5.48	8.75	2	-	38.28
0.03	3.76	8.99	0.15	1	24.01	3	5.48	8.42	3	-	26.75
0.04	3.76	9.53				4	5.48	8.41	4	-	28.32
0.05	4.78	19.03				5	5.48	7.64	5	-	10.55
0.10	24.17	36.97									
0.15	-	11.19									

Table 5. Solutions for MCSFSPP, MCSFMPP and k^c , s =Rajshahi and t =Silhat (Instances Bangladesh)

0.05. For greater values, the network can be dramatically damaged. This later observation is reinforced by the results reported in columns 4-6 in the same table: a critical k can be found only if $R \geq 0.05$. When looking at the results of the MCSFMPP (columns 7-9 for $R = 0.01$ and 10-12 for $R = 0.1$) we can see that the network resists *well* ($\Delta\% \Omega \approx 5\%$) several failures with $R = 0.01$; however, if $R = 0.1$ then the network collapses even if $k = 2$.

4. Conclusions and Future Work

We have presented a collection of combinatorial optimization problems that in combination allow to measure the vulnerability of a network. Vulnerability is represented by the relative increase of the cost of a s, t -shortest path when part of the network is disrupted. By analyzing the solutions of these problems for different instances, we have highlighted how different aspects of both the failure and the network yield to different levels of vulnerability.

Two main paths of future work can be identified. First, we should consider the case in which \mathcal{X} is not given by a discrete set of points, but rather as continuous area. Second, at the light of the large computational effort needed to solve some of the instance considered here, we think it is important to design and implement more sophisticated algorithmic techniques such as decomposition approach in order to be able to consider larger and more complex instances.

Acknowledgements This research was supported by Fondecyt Project #1121095, CONICYT, Ministerio de Educación, Chile. Eduardo Álvarez-Miranda thanks the Institute of Advanced Studies of the Università di Bologna from where he is a PhD Fellow.

Bibliography

- [1] N. Assimakopoulos. A network interdiction model for hospital infection control. *Computers in Biology and Medicine*, 17(6):413 – 422, 1987.
- [2] R. Church, M. Scaparra, and R. Middleton. Identifying critical infrastructure: The median and covering facility interdiction problems. *Annals of the Association of American Geographers*, 94(3):491–502, 2004.
- [3] K. Cormican, D. Morton, and R. Wood. Stochastic network interdiction. *Operations Research*, 46(2):184–197, 1998.
- [4] D. Fulkerson and G. Harding. Maximizing the minimum source-sink path subject to a budget constraint. *Mathematical Programming*, 13(1):116–118, 1977.
- [5] B. Golden. A problem in network interdiction. *Naval Research Logistics Quarterly*, 25(4):711–713, 1978.
- [6] Google. Google Maps, 2013. URL <https://maps.google.com/>.
- [7] R. Hemmecke, R. Schültz, and D. Woodruff. Interdicting stochastic networks with binary interdiction effort. In D. Woodruff, editor, *Network Interdiction and Stochastic Integer Programming*, volume 22 of *Operations Research/Computer Science Interfaces Series*, pages 69–84. Springer US, 2003.
- [8] E. Israeli and R. Wood. Shortest-path network interdiction. *Networks*, 40(2):97–111, 2002.
- [9] L. Khachiyan, E. Boros, K. Borys, K. Elbassioni, V. Gurvich, G. Rudolf, and J. Zhao. On short paths interdiction problems: Total and node-wise limited interdiction. *Theory of Computing Systems*, 43(2):204–233, 2008. ISSN 1432-4350.
- [10] A. Murray. An overview of network vulnerability modeling approaches. *GeoJournal*, 78(2):209–221, 2013.
- [11] C. Phillips. The network inhibition problem. In *Proceedings of the Twenty-fifth Annual ACM Symposium on Theory of Computing*, STOC '93, pages 776–785. ACM, 1993.
- [12] J. Salmeron, K. Wood, and R. Baldick. Worst-case interdiction analysis of large-scale electric power grids. *IEEE Transactions on Power Systems*, 24(1):96–104, 2009.
- [13] United Nations Statistics Division. UNSD Statistical Databases, 2013. URL <http://millenniumindicators.un.org/unsd/databases.htm>.
- [14] R. Wollmer. Removing arcs from a network. *Operations Research*, 12(6): 934–940, 1964.