ISSN 1748-7595 (Online)

Kent Business School

Working Paper Series

Optimization and Analysis of Protection Strategies for Supply Chains: Comparing Regret and Expected Models

Federico Liberatore
Kent Business School

Maria Paola Scaparra
Kent Business School

University of Kent

Working Paper No.186
November 2009

Optimization and analysis of protection strategies for supply chains: Comparing regret and expected models.

Federico Liberatore[*], Maria Paola Scaparra[†]

May 12, 2009

Abstract

The inherent and growing complexity characterizing today's infrastructure systems has considerably increased their vulnerability to external disruptions. Recent world events have demonstrated how the damage of one or more infrastructure components can result in disastrous political, social and economical effects. This, in turn, has fostered the development of sophisticated quantitative methods that identify cost-effective ways of strengthening supply systems in the face of disruption. Stochastic and robust optimization can be used for this purpose. An example of a protection model which explicitly takes into account the uncertainty characterizing the extent of disruptive events is the Stochastic R-Interdiction Median Problem with Fortification (S-RIMF) [26]. The objective of this model is to optimally protect facilities in a supply system so as to minimize the expected operational costs resulting from the loss of an uncertain number of system components. In this article, we analyze how protection strategies vary when using different measures of optimization under uncertainty. We propose two regret models and show how to solve them by extending the bounds based approach developed for

[*]Kent Business School Annexe, University of Kent, CT2 7PE Canterbury, Kent, United Kingdom. fl51@kent.ac.uk

[†]Kent Business School, University of Kent, CT2 7PE Canterbury, Kent, United Kingdom. m.p.scaparra@kent.ac.uk

S-RIMF. Also, we discuss how to build a reliability envelope for the models considered, which can be used to identify the range of possible impacts associated with different protection strategies. The new regret models and the original S-RIMF are tested on a new data set which was built using the Census 2001 data of the United Kingdom. We analyze and compare the protection plans generated by the models, and provide some useful insights related to the robustness of the different modeling approaches.

1 The need of countering disruptions in supply systems

Supply systems are distribution infrastructures consisting of a set of manufacturing, storage, and transportation facilities with the purpose of delivering goods and services. The fact that approximately 10 percent of the gross domestic product in the United States is dedicated to supply related activities [39] demonstrates how the efficient and effective functioning of supply systems is a crucial issue in our society. Because of their importance, the consequences of possible interruptions to their normal functioning can be catastrophic. Supply systems can be victim of natural catastrophes (such as earthquakes, hurricanes, and floods), intentional disruptions (such as terrorist attacks, sabotage, and labor strikes), and accidental failures (such as industrial accidents, plant fire, and system component breakdowns).

As demonstrated by many recent events, intentional or accidental disruptions can have an enormous ripple effect on infrastructure systems with resulting deleterious social, political, financial, and economic consequences. As an example, a strike at two part plants of General Motors in 1998 caused the shutdowns of twenty six assembly plants, which ultimately resulted in a production loss of over 500,000 vehicles and an 809 million dollars quarterly loss for the company ([6], [40], [41]). An eight-minute fire at a Philips semiconductor plant in 2001 brought Ericsson to a virtual standstill [24]. In 2002, the west-coast port lockout plagued the U.S. retailers's supply lines, caused some factories to close and threatened to derail the U.S. economy [17]. In August 2003, an electrical system failure in Ohio resulted in a subsequent loss of power in many states of the Northeast United States [19]. The power outage's effects on international air transport, communication, production operations and financial markets were widespread. The suspension of the license of the Chiron plant in Liverpool, England, resulted in a reduction of the U.S. supply of the influenza vaccine by nearly 50 percent during the 2004-2005 flu season [32]. Hurricanes Katrina and Rita, which hit the U.S. Gulf Coast in 2005, caused the shutdown of several oil refineries, profound damage of offshore platforms and pipeline facilities as well as the closure of multiple ports. This had devastating repercussions on U.S. oil and gas production, on the shipping industry and the movement of fresh produce and agricultural products across the country ([31], [3], [25]). Smaller-scale disruptions occur much more frequently: Wal-Mart's Emergency Operations Center receives a call virtually every day from a store or other facility with some sort of crisis [25].

The large number and substantial economic repercussions of recent disruptive events highlight the importance of devising effective supply system protection strategies, able to mitigate the effects of disruption and improve the effectiveness of contingency plans. In fact, security and contingency planning can notably reduce the effects of a disruption, as confirmed by the following examples. Thanks to its highly effective risk management strategy and prompt action, Nokia weathered the 2001 Philips fire without suffering any significant sale loss and ultimately captured a substantial portion of Ericsson's large market share [24]. Home Depot's policy of planning for various types of disruptions based on territorial and geographical features allowed it to reopen twnety three of its thirty three stores within Katrina's impact zone after one day and twenty nine after one week [15]. Wal-Mart's stock prepositioning became a model for post-hurricane recovery [25].

In all the aforementioned cases, the analysis of critical system components and vulnerabilities and the consequent development of risk management and protection plans resulted in a winning strategy to ensure the proper working of supply chains even when facing the disruption of some critical infrastructure components. In recent years academics and practitioners have both demonstrated a growing interest in this topic, in recognition of the urgent need of developing tools and methodologies to address issues of system vulnerability, resiliency and security ([22], [34], [38]). However, the research in this area only dates back a few years and it is still at an embryonic stage. Roughly, the investigation can be split into two main streams of research ([44]). The first one concerns the development of *design models*, i.e. optimization models for planning supply chain configurations which have a high degree of performance both normally and when an interdiction occurs. The second one focuses on the development of optimization models for improving the reliability of infrastructure systems which are already in place and for which a complete reconfiguration would be prohibitively costly. The literature has defined these models as *fortification models*. Besides these two main research streams, a few other models have been proposed to face disruption in different scenarios, and to respond to the multitude of objectives of decision makers. As an example, Fox et al. [16] discuss an agent-based supply-chain architecture to evaluate coordination strategies in the presence of perturbations caused by stochastic events, such as facility breakdowns. Yu et al. [50] analyze and compare different sourcing strategies to cope with unreliable supply and disruption risks.

This article makes the following contributions to the literature on supply chain reliability models. First, we present two novel stochastic models for the planning of protection efforts in median supply systems when the number of possible disruptions is uncertain. To the best of our knowledge, the only protection model that involves an uncertain number of losses within the location analysis framework is the Stochastic R-Interdiction Median Problem with Fortification (S-RIMF) [26]. The models presented in this work extend the S-RIMF by considering different objective functions based on regret rather than on expected costs. Second, we discuss how to build a reliability envelope for these models so as to identify the range of impacts of different protection strategies and quantify possible efficiency losses of suboptimal protection plans. Third, we propose some model reduction techniques to solve efficiently both the best-case and worst-case models used to identify the boundaries of the reliability envelopes. Forth, we introduce a novel data set, based on the information of the main UK urban areas obtained from the last census of the United Kingdom, and use this data set to test our modeling approaches. Finally, we provide some insights on the protection strategies produced by the different models and compare their robustness to possible misestimations of the uncertain parameters.

The reminder of the article is organized as follows. The next section presents a selection of previous contributions to the field of fortification of supply systems. Section 3 presents the R-Interdiction Median Problem with Fortification. The models based on regret are introduced in Section 4. Next we explain how to compute the reliability envelope for all the models under consideration. In Section 6, the new data set is presented as well as the results of the computational tests. Finally, the article is concluded with a summary of the main findings of the analysis and some conclusive remarks.

2 Configuration of protection strategies

Although the development of mathematical models for protection planning is a relatively new research area, a fair number of articles on this topic has appeared in the literature in the last decade. Most of the fortification models developed so far focus on the identification of economical and efficient protection plans to reduce the impact of worst-case losses. To this end, they generally use the information provided by an underlying model, referred to as an *interdiction problem*, to identify the most critical system components or disruption scenarios.

Identification of critical system components. The first interdiction model has been introduced in 1964 by Wollmer [49] to study the effect of the removal of some arcs on the maximum flow through a network. Starting from this pioneering work, the majority of the studies in the field of interdiction have addressed problems within the context of networks, considering different reliability measures, such as connectivity [18], distance or cost [4] and capacity [27]. A multitude of early network interdiction models are surveyed by Church et al. [12]. A survey of the latest contributions can be found in Losada et al. [28]. To the best of our knowledge, the article by Church et al. [12] is also the first work to contextualize interdiction problems in the framework of location analysis. The authors consider systems based on two service protocols, the P-Median Problem [20] and the Max Covering Problem [10], and formulate the respective interdiction programs: the r-Interdiction Median Problem (RIM) and the r-Interdiction Covering Problem (RIC). The aim of the RIM model is to ascertain the set of the r most critical facilities in an existing system which comprises P facilities and where the demands of the customers are always served by the closest facility. After interdiction, the customers which were formerly serviced by an interdicted facility, are reallocated to the closest operating facility to preserve the feasibility of the system configuration according to the constraints of the P-Median Problem. In the RIC model there is no reassignment of the customers to the closest working facility and the aim of this program is to find the subset of r facilities which, when removed, maximizes the resulting drop in demand coverage.

Planning for protection. Most of the existing works addressing the problem of optimizing protection strategies use a game theoretic approach, where interdiction models are embedded within multi-level programs. The outer program models the defender decisions whereas the inner interdiction program identifies the worst-case scenarios in response to a given protection strategy. These multi-level programs are also known as *leader-follower* or *Stackelber* games [45]. As an example, Brown et al. [8] propose several bilevel and trilevel models to analyze the vulnerabilities of electric power grids, subways, airports and other critical infrastructures. Another work on critical infrastructures is the article by Qiao et al. [33], who use a min-max model to optimize the allocation of a security budget to a water supply network so as to make it more resilient to physical attacks. Zhuang and Bier [51] take up the issue of balancing protection against both terrorism and natural disasters. They propose basic equilibrium models for both sequential and simultaneous games between an attacker and a defender. Azaiez and Bier [1] study the problem of optimally allocating defensive resources to maximize the minimum expected cost of a feasible attack. Bier [5] proposes a game-theoretic model of security investment where the goals of the attacker are uncertain. The findings of her analysis suggest that it is desirable to publicize how the security investment are allocated so that the attacker is attracted towards less damaging targets. Building upon the interdiction models proposed in [12], Church and Scaparra [13] formulate a defender-attacker model that explicitly includes protection decisions constrained by a defensive budget. The objective is to optimally fortify (protect) Q facilities in such a way that the cost of the worst-case loss is minimized. They assume that protected facilities are no longer vulnerable to disruptions. The authors propose two different solution approaches to solve the resulting r-Interdiction Median Problem with Fortification (RIMF): a reformulation of the problem as a maximal covering model with precedence constraints [36] and a tree search algorithm [35]. Extensive computational tests shows that there is no clear dominance of one methodology over the other and that both the approaches can be useful depending upon the problem at hand and the application setting. Recently, some extensions of the RIMF have been presented. Scaparra and Church [37] consider the problem where the facilities have a limited capacity. Cappanera and Scaparra [9] apply a game theoretic approach like RIMF to shortest path networks. Finally, Liberatore et al. [26] introduce a stochastic component by considering uncertain numbers of interdictions. This is the base for the current work and will be discussed in more details in the next section.

3 Edging against an uncertain number of disruptions

Although the RIMF model can help identify sound protection practices, it relies on some strong assumptions that may result in suboptimal solutions and/or limit its practical applicability. One of these premises is that the protection planner knows with certainty the number of losses that the system may incur. This is clearly an assumption that over-simplifies the reality as malicious attacks, as well as acts of nature, are often characterized by a strong uncertainty in terms of number of targets.

Liberatore et al. [26] extend the RIMF model to include a stochastic component and consider the problem of hardening systems against a range of possible numbers of attacks, varying between 1 and a maximum number R. Every outcome occurs with some probability and the objective is to minimize the expected costs after a worst-case loss of a random number of facilities. The problem, named the Stochastic R-Interdiction Median Problem with Fortification (S-RIMF), is a bilevel problem in nature where the leader optimally allocates defensive resources in order to counter the action of the follower, who in turn chooses which facilities to disrupt, for each number of attacks, to increase the expected cost of the system as much as possible. For an extensive treatment of bi-level programs the reader is referred to [2] and [14]. Discrete bilevel programs are intrinsically difficult to solve, as explained in [29] and [47]. A way of solving bilevel programs with integer restrictions is via reformulation [30]. S-RIMF can be reformulated as a single-level maximum covering problem by explicitly enumerating all the possible ways of disrupting r of the P facilities operating within the system, with $r = 1, \ldots, R$ ([26]). The problem formulation uses the following notation. Let H^r, indexed by h, be the set of interdiction patterns where exactly r facilities are interdicted, and I_h be the set of facilities interdicted in pattern h. The cost c_h associated with an interdiction pattern h represents the cost of the system when the facilities in I_h are disabled. This cost can be easily computed by assigning each customer $i \in N$, where N is the set of customers, to the closest working facility $j \in F/I_h$, where F is the set of initial facilities. The total operational cost of the system is given by the demand weighted sum of distances between customers and facilities. The demand of customer i is denoted in the following by a_i, whereas d_{ij} is the distance between customer i and facility j.

A pattern h is defined as *covered* if any of the facilities in I_h is fortified. Therefore, in order to reduce the impact of worst-case losses on the network, it is necessary to protect the facilities in such a way that the most disruptive patterns (i.e., the patterns with the higher costs) are covered.

The single-level S-RIMF model uses the following decision variables:

$$z_j = \begin{cases} 1, & \text{if facility } j \text{ is fortified,} \\ 0, & \text{otherwise.} \end{cases}$$

$$y_h = \begin{cases} 1, & \text{if the interdiction pattern } h \text{ is covered,} \\ 0, & \text{otherwise.} \end{cases}$$

W_r : cost of the worst-case interdiction pattern when exactly r facilities are interdicted.

The Max Covering formulation of the S-RIMF is as follows:

$$\min\ Z^\star = \sum_{r=1}^{R} p_r W_r \tag{1}$$

$$\sum_{j \in F} z_j \leq Q \tag{2}$$

$$\sum_{j \in I_h} z_j \geq y_h \ \forall h \in H_r,\ \forall r = 1, \dots, R \tag{3}$$

$$W_r \geq c_h \left(1 - y_h\right)\ \forall h \in H_r,\ \forall r = 1, \dots, R \tag{4}$$

$$z_j \in \{0, 1\}\ \ \forall j \in F \tag{5}$$

$$0 \leq y_h \leq 1\ \forall h \in H_r,\ \forall r = 1, \dots, R \tag{6}$$

The objective (1) is to minimize the expected worst-case operational cost, given by the probability weighted sum of the worst-case costs W_r. The cardinality constraint (2) bounds the number of fortified facilities to be at most Q. The covering constraints (3) impose that a pattern h is covered when at least one of the facilities in its interdiction set I_h is fortified. The worst-case loss value W_r for each number of attacks r is determined by constraint (4) as the largest cost among all the uncovered patterns. Constraints (5) and (6) impose the conditions of integrality and non-negativity of the relevant variables.

As the number of constraints and variables in the formulation (1)-(6) depends on the number of interdiction patterns, solving this model with general purpose optimization solvers may be computationally impractical for problem instances of realistic size. Liberatore et al. [26] propose some efficient optimal and heuristic approaches to solve the S-RIMF which rely on the computation of effective upper and lower bounds to reduce the dimensionality of the problem. We show how a similar approach based on bounding procedures can be developed to solve stochastic RIMF models with different objectives.

4 Regret models

The uncertainty issue tackled in the stochastic RIMF undoubtedly represents an important addition to the protection modeling literature. An in-depth analysis of the stochastic nature of RIMF, in fact, showed that the impact of taking into account the uncertainty in the number of losses in the optimization process may be substantial [26].

Nevertheless, an expected cost model such as S-RIMF may produce inefficient protection strategies under various scenarios. The use of an expected cost objective, in fact, tends to favor scenarios with a high number of interdictions, as a high number of losses always corresponds to a non-inferior damage to the system than a low number. If, for example, equal probabilities are used for each scenario, the optimal protection strategy identified by the model may be efficient against high numbers of facility losses, but may be highly sub-optimal if the effective number of losses is small. Obviously, if low probabilities are associated with higher numbers of losses, this effect is partially alleviated. However, when planning defense against extreme events such as terrorist actions, a concerted attack on several facilities may be as likely as an attack on a single target. Additionally, a reliable estimation of the probability that a given number of losses will take place may not be feasible due to the lack of historical data regarding the disruption of critical system components caused by rare events.

Another criterion other than cost, commonly used in stochastic and robust optimization, is *regret* [43]. Regret can be described as *opportunity loss* [42], that is the difference (either absolute or relative) between the quality of a given strategy, and the quality of the strategy that would have been applied if the future had been known. Considering the regret rather than the cost of a scenario may help overcoming the aforementioned limits of the S-RIMF. In those settings where the probabilities can be estimated from historical data, an expected regret model can be adopted to remove the bias introduced by the costs. If a good estimation of the probability function is not available, a minimax regret model can be used to obtain solutions which perform fairly well no matter which scenario is realized.

We define the relative regret associated with a given number of interdictions r as the percentage difference between the cost of the worst-case interdiction pattern in the optimal stochastic strategy, W_r, and the cost of the optimal solution to the deterministic problem where exactly r losses are considered, $\overline{W}_r$. Hence, the relative regret for a given r is:

$$\frac{W_r - \overline{W}_r}{\overline{W}_r}.$$

Note that $W_r \geq \overline{W}_r$ and that, without loss of generality, we can assume $\overline{W}_r > 0$ for all r.

In this section, we present the problems of minimizing the expected and the maximum regret, and show how some efficient lower and upper bounds, similar to the ones developed to solve S-RIMF, can be used to reduce the size of the formulations and, therefore, expedite the solutions of the regret models by general purpose optimization solvers.

Minimizing the expected regret

The problem of minimizing the expected regret can be formulated mathematically as follows:

$$\min\ \Delta^{\star} = \sum_{r=1}^{R} p_r \frac{W_r - \overline{W}_r}{\overline{W}_r} \tag{7}$$

$$(2)\text{-}(6)$$

Note that the above model is equivalent to an expected cost model with a modified probability distribution. The objective function, in fact, can be rewritten as:

$$\Delta^{\star} = \left(\sum_{r=1}^{R} \frac{p_r}{\overline{W}_r} W_r \right) - 1.$$

By ignoring the constant term -1, the problem of minimizing the expected regret is equivalent to the problem of minimizing the expected cost with probabilities $p'_r = \frac{p_r}{\overline{W}_r}$.

Not all the possible interdiction patterns must be considered in the sets H_r. More specifically, all the interdiction patterns h whose cost c_h is strictly less than $\overline{W}_r$ can be ignored. In fact, a pattern h such that $c_h < \overline{W}_r \leq W_r$ will never generate the worst case cost W_r in constraints (4). Therefore, all the variables y_h associated with these patterns can be safely removed from the formulation together with the constraints (3) and (4) associated with them.

The solutions $\overline{W}_r$ to the deterministic RIMF problems can be used to compute valid upper bounds to the regret model and identify additional model reductions. Let us denote by $\overline{z}^r$ the optimal fortification set obtained by solving the deterministic RIMF with exactly r interdictions. Each $\overline{z}^r$, with $r = 1, ..., R$, is obviously a feasible solution to the problem of minimizing the expected regret. To compute the regret associated with these solutions, we need to solve R independent RIM problems [12] with an additional constraint that forbids the interdiction of the protected facilities $\overline{z}^r$. Let $h_m\left(\overline{z}^r\right)$ be the optimal interdiction pattern found by solving the RIM problem when exactly m facilities are interdicted and facilities $\overline{z}^r$ are fortified, and let $c_{h_m(\overline{z}^r)}$ be the associated cost. The expected regret of the solution $\overline{z}^r$ is:

$$\widetilde{\Delta}_r = \sum_{m=1}^{R} p_m \frac{c_{h_m(\overline{z}^r)} - \overline{W}_m}{\overline{W}_m}. \tag{8}$$

An upper bound $\widetilde{\Delta}$ to the optimal regret $\Delta^\star$ can then be obtained by selecting the best (lowest) $\widetilde{\Delta}_r$, $r = 1, \ldots, R$. Namely,

$$\widetilde{\Delta} = \min_{r=1,\ldots,R} \widetilde{\Delta}_r. \tag{9}$$

The main steps of the procedure used to compute the upper bound are illustrated in the following example.

Example. Let us consider an instance of the data set *UKMainIsland* (see Section 6 for further details on this data set) with 20 facilities, 2 fortifications, and 3 maximum possible interdictions, i.e. parameters $P = 20$, $Q = 2$ and $R = 3$. The probabilities associated with each interdiction number were chosen as $p_1 = 0.5, p_2 = 0.\overline{3}$, and $p_3 = 0.1\overline{6}$. $F = \{1, \ldots, 20\}$ is the set of open facilities in the initial configuration.

1. The first step of the procedure is to solve R deterministic RIMF problems to optimality. Table 1 shows the results. For each possible number of interdictions r reported in the first column, the second and third columns display the optimal fortification set $\overline{z}^r$, and the optimal objective function value $\overline{W}_r$, respectively. For example, the best facilities to protect when exactly 3 interdictions are assumed are facilities 1 and 11 (solution $\overline{z}^3$). The worst-case loss of 3 facilities after protection results in a total weighted distance or cost of about 946,700.

2. For each fortification set $\overline{z}^r$ identified in step 1, we can compute an upper bound $\widetilde{\Delta}_r$ to the expected regret. In order to do so, we have to solve R RIM problems, one for each value of $m = 1, \ldots, R$, where we forbid the interdiction of the facilities in $\overline{z}^r$. Table 2 displays the results for this second step. The first column shows the number of interdictions in the RIM problems, m. Subsequently, each pair of columns

presents the interdiction set $I_{h_m(\overline{z}^r)}$ and the associated cost $c_{h_m(\overline{z}^r)}$ corresponding to each fortification set $\overline{z}^r$. For example, when the protection strategy $\overline{z}^3$ is considered (last two columns), the worst-case loss of a single facility (facility 2) results in a cost of about 615,585. This represents a 2.3 percent cost increase as compared to the solution obtained when using the optimal protection strategy for a single loss, $\overline{z}^1$ (601,800).

Note that although $\overline{z}^2$ and $\overline{z}^3$ differ by one facility, the solutions to the RIM problems are identical, suggesting that the two fortification plans are in fact equivalent. The upper bounds $\widetilde{\Delta}_r$ corresponding to each fortification set $\overline{z}^r$ can be computed using formula (8). They are: $\widetilde{\Delta}_1 = 0.0424$, and $\widetilde{\Delta}_2 = \widetilde{\Delta}_3 = 0.0115$.

3. Using formula (9), we select the best (lowest) upper bound $\widetilde{\Delta}_r$ calculated in step 2. The final upper bound to the optimal expected regret is $\widetilde{\Delta} = 1.15\%$.

■

To further speed up the solution of the expected regret model, we can use the upper bound $\widetilde{\Delta}$ to compute an upper bound to the optimal cost of the worst-case interdiction patterns for each value of r, as stated in the following proposition.

Proposition 4.1 *Let $W_r^\star$ be the cost of the worst-case interdiction pattern with r interdictions in the optimal solution to the expected regret model. An upper bound $\widetilde{W}_r$ to $W_r^\star$ can be computed as follows.*

$$\widetilde{W}_r = \overline{W}_r \left(1 + \frac{\widetilde{\Delta}}{p_r}\right). \tag{10}$$

Proof. In order to prove the correctness of (10), let us consider the following sequence of inequalities:

$$\widetilde{\Delta} \geq \Delta^\star = \sum_{m=1}^{R} p_m \frac{W_m^\star - \overline{W}_m}{\overline{W}_m} \geq \sum_{\substack{m=1,\\ m\neq r}}^{R} p_m \frac{\overline{W}_m - \overline{W}_m}{\overline{W}_m} + p_r \frac{W_r^\star - \overline{W}_r}{\overline{W}_r} = p_r \frac{W_r^\star - \overline{W}_r}{\overline{W}_r}.$$

By rearranging the first and last terms in the sequence, we obtain:

$$W_r^\star \leq \frac{\overline{W}_r}{p_r}\widetilde{\Delta} + \overline{W}_r = \overline{W}_r \left(1 + \frac{\widetilde{\Delta}}{p_r}\right).$$

Therefore:

$$\widetilde{W}_r = \overline{W}_r \left(1 + \frac{\widetilde{\Delta}}{p_r}\right)$$

is a valid upper bound to $W_r^\star$.

■

The upper bounds $\widetilde{W}_r$ can be used to fix some of the variables in the expected regret model to their optimal values. In fact, all the patterns h whose cost c_h exceeds the associated upper bound $\widetilde{W}_r$ must be covered (i.e., thwarted by the protection strategy) in an optimal solution. Consequently, we can set the variable y_h associated with those patterns to 1 and remove the relevant constraints (4) from the formulation.

Minimizing the maximum regret

We now introduce a maximum regret model that can be used to plan against multiple numbers of attacks even when the probability distribution that models the behavior of the attacker in terms of number of interdictions is not known. As a consequence, the solutions produced will not focus on countering only scenarios with associated high probabilities but will have a more homogeneous behavior over all the possible futures. This is one the most common approaches used in robust optimization [43]. The formulation of the problem of minimizing the maximum regret is:

$$\min \Delta \tag{11}$$

$$\Delta \geq \frac{c_h - \overline{W}_r}{\overline{W}_r} (1 - y_h) \ \forall h \in H_r, \forall r = 1, \ldots, R \tag{12}$$

(2)-(6)

This formulation is slightly more compact than the previous one in terms of number of variables. Constraints (12), which replace constraints (4), assign the value to the maximum regret: for every scenario, Δ must be greater or equal than the regret of the worst uncovered pattern.

Also for this program, the solutions to R deterministic RIMF problems can be used to compute lower and upper bounds to the maximum regret, to fix some of the variables to their optimal values and remove some of the constraints. Namely, as in the expected regret model, all the patterns h whose cost c_h is strictly less than $\overline{W}_r$ can be disregarded. An upper bound $\widetilde{\Delta}$ to the maximum regret can be easily obtained from the optimal fortifications of the RIMFs by following the same procedure described in Section 4 where formula (8) is replaced by:

$$\widetilde{\Delta}_r = \max_{m=1,\ldots,R} \frac{c_{h_m(\overline{z}^r)} - \overline{W}_r}{\overline{W}_r}. \tag{13}$$

Finally, the upper bound $\widetilde{\Delta}$ can be used to fix to 1 the variables y_h associated with the patterns h whose cost c_h is higher than $\overline{W}_r \left(\widetilde{\Delta} + 1\right)$ and remove the corresponding constraints (12).

5 The reliability envelope

The models described so far find the optimal protection plan for a p-median system, according to different objective functions (expected cost, expected regret or maximum regret). When considering suboptimal ways of protecting one or more facilities, the basic question is what happens to the resulting performance of the system after the loss of some critical facilities.

We can measure this loss of efficiency by calculating the distance from the optimal solution value. For a fixed maximum number of losses R, we can represent the increase in weighted distance (or loss of system efficiency) as shown in Figure 1. The values on the x-axis represent the level of protection or number of fortifications Q. The values on the y-axis display the resulting system efficiency. For this example, the number of facilities P is equal to 20, and the maximum number of losses R is set to 3, therefore is not possible to protect more than 17 facilities. The system efficiency is 100 percent when all the facilities are operating. If one ore more facilities are lost, the efficiency is consequently decreased. Figure 1 shows two trends: the upper trend displays the best-case efficiency, i.e., the system efficiency when implementing an optimal protection plan for different values of Q, whereas the lower trend depicts the worst-case efficiency, i.e., the efficiency obtained when the least effective protection plan is implemented. It can be easily seen that the two trends define a range of losses, from the best-case to the worst-case, that encompasses all the possible ways of protecting Q facilities. This region is referred to as the *reliability envelope*. Prior examples of depicting the reliability envelope in other application settings can be found in Urban and Keit [46], Kim and O'Kelly [23], and Church and Scaparra [11].

Knowing the structure of the envelope can be an asset to defense planning decisions. The upper curve represents a situation of complete control: the decision-maker has full knowledge of the mechanics of the system in terms of parameters and, in the relevant models, of the probability function. Thus, the optimal fortification strategy can be devised. On the other hand, the lower curve shows the effects of a highly inefficient protection plan. This second trend can represent a situation where either the data representing the model, or the probability function, or both are misestimated. The thickness of the envelope provides valuable information regarding the impact range of different protection strategies using the same amount of resources and the extent to which protection and mitigation efforts may be dissipated if sub-optimal plans are implemented. As an example, if resources are available to harden half of the facilities, the reliability envelope in Figure 1 highlights the fact that an efficient protection plan can cap the worst-case efficiency loss at 10 percent of the original efficiency. On the other side of the spectrum, if the protective resources are invested on the wrong assets, the efficiency loss can be as high as 50 percent in the worst-case. This is equivalent to the worst-case efficiency loss obtained without protection, to indicate a completely wasteful use of the resources. The system planner can exploit the information provided by the reliability envelope to compare alternative interventions and evaluate the potential benefits of corrective plans, such as changes in the number of protected sites, or investments in the analysis of the system to acquire a better definition of the data and the parameters.

The computation of the worst-case curve requires solving a maximization version of the minimization problems used to find the optimal protection plans. The solutions to the maximization problems have also been employed to compare the solution gaps across different models, as further discussed in Section 6.

Maximizing the expected cost

The maximization problem can be formulated as a single-level, mixed-integer program. The formulation uses the definition of the set $T_{ij} = \{k \in F \,|k \neq j \,\wedge\, d_{ik} > d_{ij}\}$, i.e., the set of existing site (not including j) that are farther than j from demand i. Also, it employs the following additional decision variables:

$$s_j^r = \begin{cases} 1, & \text{if facility } j \text{ is interdicted in scenario } r, \\ 0, & \text{otherwise.} \end{cases}$$

$$x_{ij}^r = \begin{cases} 1, & \text{if demand } i \text{ is served by facility } j \text{ after interdiction in scenario } r, \\ 0, & \text{otherwise.} \end{cases}$$

The formulation of the maximization version of the S-RIMF is:

$$\max\ \hat{Z}^{\star} = \sum_{r=1}^{R} p_r \sum_{i} \sum_{j \in F} a_i d_{ij} x_{ij}^{r} \tag{14}$$

$$\sum_{j \in F} z_j \geq Q \tag{15}$$

$$\sum_{j \in F} s_k^r \leq r,\ \forall r = 1, \ldots, R \tag{16}$$

$$\sum_{r=1}^{R} s_j^r \leq R\left(1 - z_j\right),\ \forall j \in F \tag{17}$$

$$\sum_{j \in F} x_{ij}^{r} \leq 1,\ \forall i \in N,\ \forall r = 1, \ldots, R \tag{18}$$

$$\sum_{h \in T_{ij}} x_{ih}^{r} \leq s_j^r,\ \forall i \in N,\ \forall j \in F,\ \forall r = 1, \ldots, R \tag{19}$$

$$z_j \in \{0, 1\}\ \ \forall j \in F \tag{20}$$

$$s_j^r \in \{0, 1\}\ \ \forall j \in F,\ \forall r = 1, \ldots, R \tag{21}$$

$$x_{ij}^{r} \in \{0, 1\}\ \ \forall i \in N,\ \forall j \in F,\ \forall r = 1, \ldots, R \tag{22}$$

The model objective is to maximize the expected cost of the system (14). Constraints (15) and (16) limit the number of possible fortifications and interdictions, respectively. Constraints (17) bind the fortification variables z_j to the interdiction ones s_j^r, in such a way that a fortified facility cannot be interdicted. The covering constraints (18) impose that each customer cannot be assigned to more than one facility in every scenario. Constraints (19) are the closest assignment constraints, which impose that each customer is served by the closest operating facility. Finally, (20), (21) and (22) are the integrality constraints.

Maximizing the expected regret

The problem of maximizing the expected regret can be obtained from the previous model by simply replacing the objective function. Namely,

$$\max\ \hat{\Delta}^{\star} = \sum_{r=1}^{R} p_r \frac{\left(\sum_i \sum_{j\in F} a_i d_{ij} x_{ij}^r\right) - \overline{W}_r}{\overline{W}_r} \tag{23}$$

$$(15)\text{-}(22)$$

As previously seen, $\overline{W}_r$ represents the cost of the optimal fortification solution when exactly r interdictions are considered.

Maximizing the maximum regret

There is no need to explicitly formulate the problem of maximizing the maximum regret across all the possible outcomes of r. In fact, in order to do so, it is sufficient to choose to protect the facilities that do not appear in the interdiction set with the highest associated regret. As, without loss of generality, we assumed $Q + R \leq P$, this is always possible. Let Z_r^{RIM} be the optimal solution value for the RIM problem when the number of interdiction is exactly r, and I_r its corresponding interdiction set. We can solve R independent RIM problems, one for each possible value of r, and calculate the maximum regret as

$$\hat{\Delta} = \max_r \frac{Z_r^{RIM} - \overline{W}_r}{\overline{W}_r}. \tag{24}$$

The chosen fortification set is any subset of cardinality Q of the set $F \backslash I_{r'}$, where r' is the scenario corresponding to the highest regret interdiction:

$$r' = \arg\max_{r} \frac{Z_r^{RIM} - \overline{W}_r}{\overline{W}_r}.$$

Solving the maximization problems

It is clear that the maximization problems used to define the lower bounds of the reliability envelopes are much easier to solve than their minimization counterparts. The expected cost and expected regret models, in fact, do not require an explicit enumeration of all the possible interdiction patterns and, therefore, their size is significantly smaller than the one of the minimization versions. The max regret problem is even easier and, as previously explained, does not even require an explicit formulation. In addition, under a specific condition, the optimal solution to the maximization problems can be identified by simply solving R interdiction problems (RIM). The sufficient condition is based upon the following consideration.

Following the metaphor of the bi-level formulation, in the maximization program the interdictor decides not only which facilities to destroy, but also how to allocate the fortification resources in such a way that the impact of the protection is minimized. Therefore, for each possible number of attacks r, he will try to strike as hard as possible the system, and protect the facilities which are unaffected in every scenario r, if possible. For a sufficiently large number of facilities P, this is always possible.

In our algorithm, therefore, we first solve R independent RIM problems to find the best interdiction plan $I_r^\star$ for each number of attacks r. We then consider the set of facilities which are interdicted in at least one interdiction plan:

$$I^\star = \bigcup_{r=1}^{R} I_r^\star.$$

If the number of facilities P is greater or equal to the sum of the possible fortifications Q and the cardinality of the interdiction set $I^\star$ ($P \geq Q + |I^\star|$), then it is possible for the interdictor to optimally destroy facilities while protecting facilities that do not affect the interdictions. Thus, the optimal interdiction sets in the maximization problems are exactly $I_r^\star$, and the cost of the system when r interdictions occurs is Z_r^{RIM} (i.e., the optimal solution value of the corresponding RIM).

This condition is usually verified when considering sufficiently large systems, i.e. systems with a large number of facilities. For small systems, the time to solve the maximization problems by general-purpose optimization software is generally noncritical.

6 Comparison of protection criteria

Through a computational analysis of the solutions of the models, we provide in this section some insights on the protection strategies produced by the three different programs. In the first subsection we present a new data set specifically created for this article. Next we explain in details the computational tests which were performed.

A new data set

We produced a novel data set for facility location problems based on the 2001 Census of the United Kingdom and Scotland [1]. The data set has been named *UKMainIsland*.

Customers and demands. A very popular data set in facility location analysis is the USCities data set, containing the largest cities in the United States according to the 2000 census [2]. This data set includes 263 cities. In a similar way, we created a data set that takes into account the 250 largest urban areas in Britain (England, Wales and Scotland) in terms of number of citizens. As for the USCities data set, the demands in UKMainIsland correspond to the number of inhabitants of each urban area, expressed in thousands of citizens.

[1] UK Census 2001. http://www.statistics.gov.uk/census2001/census2001.asp (last accessed date 8 May 2009)

[2] United States Census 2000. http://www.census.gov/main/www/cen2000.html (last accessed date 8 May 2009)

Calculating the distances. In the USCities data set the distances correspond to the great-circle distances in miles between the cities. Similarly, in our new data set the distances between the demand points were generated by using the Vincenty formula [48]. The Vincenty formula was chosen among others because of its accuracy. Let $\phi_s, \lambda_s;\ \phi_f, \lambda_f$ be the geographical latitude and longitude of two points (a base s and a destination f), respectively, and $\Delta\phi, \Delta\lambda$ their differences. Also let $\Delta\widehat{\sigma}$ represent the (spherical) angular difference/distance, or central angle. The Vincenty formula for the calculation of the central angle is:

$$\Delta\widehat{\sigma} = \arctan\left(\frac{\sqrt{(\cos\phi_f \sin\Delta\lambda)^2 + (\cos\phi_s \sin\phi_f - \sin\phi_s \cos\phi_f \cos\Delta\lambda)^2}}{\sin\phi_s \sin\phi_f + \cos\phi_s \cos\phi_f \cos\Delta\lambda}\right).$$

If ρ is the great-circle radius of the sphere, then the great-circle distance is $\rho\,\Delta\widehat{\sigma}$. For our data set ρ has been set to $3,956.562$, which corresponds to the average between the equatorial radius $a = 3,963.205$ and the polar radius $b = 3,949.919$ in miles, according to the geodesic measures by Fischer [7].

The resulting data set UKMainIsland is illustrated in Figure 2. The black dots represent the location of the demand points. Most of the cities are located in the south of the island. A second group is located in Scotland, with a higher concentration along the axis connecting Glasgow to Edinburgh. A smaller cluster is located in the area of Newcastle-Upon-Tyne, in North East England. Therefore this data set present three main groups with different characteristics: wide and well distributed in the south, small and compact in the center, and sparse in the north.

Computational tests

The algorithms resulting from the models have been implemented in C++ and compiled with gcc version 3.4.2 for win32. We used the generic MIP solver CPLEX 11.1 [21] to solve the mixed integer programs. The tests have been run on a computer equipped with a Genuine Intel(R) CPU T2500 @ 2.00GHz and 1 GB of RAM. All the tests had a time and a memory limit of one hour and 1 GB, respectively. The algorithms have been tested on the data set UKMainIsland on a wide array of combinations of the parameters P, Q and R. Specifically, P takes on values of 10, 20 and 30. The P facilities in the initial configuration correspond to the ones in an optimal solution to the P-Median Problem. Q is calculated as a percentage of P rounded up to the closest integer when fractional. We consider the following percentage values: 10 percent, 15 percent, 20 percent, 25 percent, and 30 percent. To avoid unnecessary repetition, for $P = 10$, only the cases where Q is equal to 10 percent, 20 percent, and 30 percent are considered. Finally, R ranges between 2 and 5. For the S-RIMF and the expected regret model, we employ two different probability distributions. The first distribution, referred in the following as *probability up*, is monotonically increasing in the values of r. Namely,

$$p_r = 2\frac{r}{R\,(R+1)}, \tag{25}$$

The second distribution, called *probability down*, is monotonically decreasing.

$$p_r = 2\frac{R-r+1}{R\,(R+1)}. \tag{26}$$

With the first choice, higher probabilities are associated with higher values of r, to indicate that more emphasis is placed on countering scenarios with a large number of losses. The second function (26) is monotonically decreasing and consequently assigns higher probabilities to lower values of r.

In summary, we tested the five following models over 52 instances:

- S-RIMF with probability up (SRIMF-U),
- S-RIMF with probability down (SRIMF-D),
- Expected regret model with probability up (MOD1-U),
- Expected regret model with probability down (MOD1-D),

- Minimax regret model (MOD2).

Analysis of the gaps

In order to evaluate the quality and the robustness of the solutions produced by the different models, we consider the optimal fortification set obtained from the solution of each formulation and calculate the cost of that protection strategy for all the remaining objective functions. Therefore, for each model and each instance we obtain an upper bound to all the other models, that can be used to compare the quality of the solutions by mean of gaps. As the objective value of the regret models can take value zero and, hence, introduce some indefiniteness in the gap computation, we evaluate the gaps by considering the improvement from the worst solution, i.e., the solution where the interdictor allocates the fortification resources in the worst possible way (Section 5).

Calculating the gaps. For a given data instance and model, let $\hat{Z}$ be the objective function value of the worst solution obtained by solving the maximization version of the model. Also, let $Z^\star$ be the value of the optimal solution and $\widetilde{Z}$ the value of a sub-optimal solution obtained with a different model. We denote by $G^\star$ the percentage gap between the optimal solution $Z^\star$ and the worst solution $\hat{Z}$:

$$G^\star = 100 \cdot \frac{\hat{Z} - Z^\star}{\hat{Z}},$$

Similarly, let $\widetilde{G}$ be the percentage gap between a suboptimal solution $\widetilde{Z}$ and the worst solution $\hat{Z}$:

$$\widetilde{G} = 100 \cdot \frac{\hat{Z} - \widetilde{Z}}{\hat{Z}}.$$

Then, the gap between the optimal solution and the sub-optimal solution can be defined as:

$$G = 100 \cdot \frac{G^\star - \widetilde{G}}{G^\star} = 100 \cdot \frac{\widetilde{Z} - Z^\star}{\hat{Z} - Z^\star}.$$

By using this formula, it is possible to compare objective functions that admit a solution value equal to 0, as without loss of generality we can assume $\hat{Z} > Z^\star$.

Comparing the robustness of the models. Figure 3 shows two pairs of tables and graphs. The tables report the average (a) and the maximum (b) gaps for all the combinations of upper bounds/optimal solutions. The columns of the histograms represent, for each model, the sum of the average (a) and maximum gaps (b) obtained when using the solution of that model to calculate an upper bound for the other models. On average all the models seems to produce similar solutions, in fact the maximum average gap obtained is only 1.49 percent (when using the solution from MOD1-D as an upper bound to SRIMF-U). When looking at the maximum gaps the situation is somewhat different. In five cases, in fact, the maximum gap is higher than 15 percent. This suggests that, depending on the information available, choosing the right strategy may have a strong impact on the protection level provided.

The histograms can help identifying the models which generate the most robust protection sets. Both the graphs present a similar trend. For the instances considered, the regret model MOD1-U gives the best solutions in terms of robustness, with an average gap of about 1 percent, a maximum gap always below 9 percent and an overall maximum gap across all the models below 20 percent. As the second best model is SRIMF-U, we can state that the best performances have been obtained when using the increasing probability function. On the other hand, MOD1-D seems to provide the worst solutions in terms of robustness, as both the sums of the average and maximum gaps are greater than those of the other models. These results confirm a quite intuitive behavior, whereby focusing the protection against a high number of attacks generally gives good results even in the cases where a low number of attacks has more chances to occur, but the reverse may be fallacious and lead to highly inferior solutions. MOD2 presents an interesting behavior, as its average and maximum gaps are very similar across all the other models. Moreover it is the third model in terms of total maximum gap, and on average is not dominated by MOD1-U. This information confirms our initial conjecture that, in the absence of an accurate estimation of the probability of loss, a maximum regret model can be used to identify good quality protection plans.

A final remark is that the robustness of the solutions obtained with an expected cost model are not remarkably different from the ones obtained with an expected regret model. In fact, the maximum and the average gaps between MOD1 and SRIMF when using the same probability distribution are fairly small. The robustness of the solutions seems to be more sensitive to possible misestimations of the probability of disruptions.

Examples of some fortification sets

In this section, we analyze and provide some insights about specific solutions to the models, so as to show how the geographical distribution of the protection resources varies for the different models. Figure 4 shows three different optimal fortification sets, corresponding respectively to the solutions of (a) SRIMF-D and MOD1-D, (b) SRIMF-U and MOD1-U, and (c) MOD2 for the instance with $P = 10$, $Q = 2$ and $R = 5$. The demands are represented with small black dots, the open facilities with big black dots and the fortifications with black point-up triangles. We chose this instance and these models because the comparison of the objective function values produced very high gaps: 17.536 percent for the solutions to SRIMF-D and MOD1-D evaluated for the objective function of MOD2, and 16.749 percent for the solution to SRIMF-D and MOD1-D evaluated for the objective function of SRIMF-U. The picture shows that the majority of the facilities is located in the most densely populated area in the south center of the island. There is then a facility in the South West which serves the south of Wales (Cardiff Urban Area), one which serves the area around Newcastle-Upon-Tyne (Tyneside) and two facilities in Scotland (North Lanarkshire and Aberdeenshire).

It can be noted that there is one facility, located in Greater London, which is fortified in all the solutions. The second protected facility, instead, varies for the three models. Namely, the two models that use the monotonically decreasing probability function, SRIMF-D and MOD1-D (see Figure 4.a), harden the facility in North Lanarkshire (Scotland), in order to counter possible disruptions in the cluster of Scotland, formed by only 2 facilities. When using this probability function, in fact, the simultaneous loss of 4 or 5 facilities is very unlikely, and therefore there is no reason to protect facilities that are located in the southern area where many other facilities are available. As capacities are not taken into consideration, there will always be a backup facility working in the region. On the other hand, the solution to SRIMF-U and MOD1-U (Figure 4.b) protects the facility located in the West Yorkshire urban area. This model, in fact, assumes that large numbers of simultaneous losses are more likely and, therefore, tends to mitigate the impact of possible losses in the southern area characterized by a higher concentration of facilities and demands. Interestingly, MOD2 (Figure 4.c) protects the facility located in Tyneside, that is exactly half way between the northern and southern group of facilities. This is due to the nature of the max regret objective function that equally minimizes the regret among all the possible number of losses.

To summarize, the following conclusions can be drawn:

1. There are some facilities particularly "crucial" (as Greater London in the example) which are chosen by all the models.

2. The choice of which of the remaining facilities to protect can significantly change depending on the model and, in particular, on the probability function.

3. The max regret model produces solutions which are a good trade-off between the expected models with increasing and decreasing probability functions.

7 Conclusions

We have presented and compared models that identify the minimum-expected-cost, the minimum-expected-regret, and the minmax-regret solutions to a stochastic protection problem in the framework of location analysis. The first model, referred to as S-RIMF, was initially formulated and solved in [26]. We have extend the solution procedure used for the S-RIMF to two newly proposed regret problems. The three models have been tested on a novel data set, and the resulting fortification plans have been compared. The first analysis concerned the robustness of the solutions. Our empirical investigation seems to indicate that: 1) the minimum-expected-regret model produces the most robust solutions; 2) the use of an increasing probability distribution yields sound fortification strategies even when biases in the likelihood of disruptions are present; 3) in the absence of information about the probability of loss, the minmax-regret model produces good compromise solutions that have similar performances across all the different objectives used in the tests. In the second analysis, we have visually compared the fortification plans of a specific instance. The analysis showed that there exist some key facilities which are protected in all the models. The choice of the remaining facilities highly depends on the probability function used: the models using an increasing probability distribution tend to allocate protection resources in big, densely populated clusters, while the models with decreasing probabilities spread out the resources among smaller clusters. The minmax-regret model provided a solution which is a trade-off between the two probability functions. Another important contribution of this work is the description of the reliability envelope for the problems considered. The representation of the reliability envelope requires the computation of the worst-case protection plans, which are obtained by solving a maximization variant of the models. The reliability envelope can throw some light on the impact of different protection strategies on the overall system efficiency and highlight the range of worst-case scenario losses associated with sub-optimal defensive plans. We hope that this work will inspire other researchers to conduct similar reliability and protection analysis for other infrastructure systems, such as capacitated or multi-echelon systems.

Acknowledgment

The authors would like to thank EPSRC for the financial support for this research (Grant EP/E048552/1).

References

[1] M. Azaiez and V. M. Bier, *Optimal resource allocation for security in reliability systems*, European Journal of Operational Research, 181 (2007), pp. 773–786.

[2] J. Bard, *Practical bilevel optimization*, Kluwer Academic Publisher, 1998.

[3] A. Barrionuevo and C. H. Deutsch, *A distribution system brought to its knees*, New York Times, Sept. 1 (2005), p. C1.

[4] M. Bell, *The use of game theory to measure the vulnerability of stochastic networks*, IEEE Transactions on Reliability, 52 (2003), pp. 63–68.

[5] V. Bier, *Choosing what to protect*, Rick Analysis, 27 (2007), pp. 606–620.

[6] K. Brack, *Ripple effect from GM strike build*, Industrial Distribution, (8) (1998), p. 19.

[7] F. Branley, *The Earth: Planet Number Three*, T. Y. Crowell Company, 1966.

[8] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, *Analyzing the vulnerability of critical infrastructure to attack and planning defenses*, INFORMS Tutorials in Operations Research, (2005), pp. 102–123.

[9] P. Cappanera and M. Scaparra, *Optimal allocation of protective resources in shortest-path networks*, tech. report, KBS Working Paper n. 177, University of Kent, 2008.

[10] R. Church and C. ReVelle, *The maximal covering location problem*, Papers in Regional Science, 32(1) (1974), pp. 101–118.

[11] R. Church and M. Scaparra, *Critical Infrastructure*, Springer Berlin Heidelberh, 2007, ch. 11, pp. 221–241.

[12] R. Church, M. Scaparra, and R. Middleton, *Identifying critical infrastructure: the median and covering facility interdiction problem*, Annals of the Association of American Geographers, 94 (2004), pp. 491–502.

[13] R. L. Church and M. P. Scaparra, *Protecting critical assets: the R-interdiction median problem with fortification*, Geographycal Analysis, 39 (2006), pp. 129–146.

[14] S. Dempe, *Foundations of bilevel programming*, Kluwer Academic Publishers, 2002.

[15] J. Fox, *Meditation on risk*, Fortune, 152(7) (2005), pp. 50–62.

[16] M. Fox, M.B., and R. Teigen, *Agent-oriented supply-chain management*, International Journal of Flexible Manufacturing Systems, 12 (2000), pp. 165–188.

[17] S. Greenhouse, *Both sides see gains in deal to end port labor dispute*, New York Times, Nov. 25 (2002), p. A14.

[18] T. Grubesic and A. Murray, *Vital nodes, interconnected infrastructures, and the geographies of network survivability*, Annals of the Association of American Geographers, 96 (2006), pp. 64–83.

[19] T. Grubesic, M. O'Kelly, and A. Murray, *A geographic perspective on commercial internet survivability*, Telematics and Informatics, 20 (2003), pp. 51–69.

[20] S. Hakimi, *Optimum locations of switching centers and the absolute centers and medians of a graph*, Operations Research, 12(3) (1964), pp. 450–459.

[21] I. Inc., *Cplex version 11.1.* Mountain View, CA.

[22] U. Jüttner, H. Peck, and M. Christopher, *Supply chain risk management: outlining an agenda for future research*, International Journal of Logistics: Research and Applications, 6(4) (2003), pp. 197–210.

[23] H. Kim and M. O'Kelly, *Survivability of commercial backbones with peering: a case study of Korean networks*, in 51st Annual North American Meetings of the Regional Science Association International, Seattle, WA, Nov. 11-13, 2004.

[24] A. Latour, *Trial by fire: a blaze in Albuquerque sets off major crisis for cell-phone giants - Nokia handles supply chain shock with aplomb as Ericsson of Sweden gets burned - Was Sisu the difference?*, Wall Street Journal, Jan. 29 (2001), p. A1.

[25] D. Leonard, *The only life line was the Wal-Mart*, Fortune, 152 (2005), pp. 74–80.

[26] F. Liberatore, M. Scaparra, and M. Daskin, *Analysis of facility protection strategies against an uncertain number of attacks: the stochastic R-interdiction median problem with fortification*, tech. report, KBS Working Paper n.176, University of Kent, 2007.

[27] C. Lim and J. Smith, *Algorithms for discrete and continuous multicommodity flow network interdiction problems*, IIE Transactions, 39 (2007), pp. 15–26.

[28] C. Losada, M. Scaparra, R. Church, and M. Daskin, *The multiple resource probabilistic interdiction median problem.* KBS Working Paper n.187, University of Kent, 2009.

[29] J. Moore and J. Bard, *The mixed integer linear bilevel programming problem*, Operations Research, 38 (1990), pp. 911–921.

[30] D. Morton, F. Pan, and K. Saegar, *Models for nuclear smuggling interdiction*, in Stochastic Programming E-Print Series (SPEPS), 2006-5.

[31] J. Mouawad, *Katrina's shock to the system*, New York Times, Sept. 4 (2005), p. 2.1.

[32] A. Pollack, *U.S. will miss half its supply of flu vaccine*, New York Times, Oct. 6 (2004).

[33] J. Qiao, D. Jeong, M. Lawley, J. P. Richard, D. M. Abraham, and Y. Yih, *Allocating security resources to a water supply network*, IIE Transactions, 39 (2007), pp. 95–109.

[34] J. Rice and F. Caniato, *Building a secure and resilient supply network*, Supply Chain Mgmt Review, 7(5) (2003), pp. 22–30.

[35] M. Scaparra and R. Church, *A bilevel mixed-integer program for critical infrastructure protection planning*, Computers & Operations Research, 35 (2008), pp. 1905–1923.

[36] ——, *An exact solution approach for the interdiction median problem with fortification*, European Journal of Operational Research, 189 (2008), pp. 76–92.

[37] ——, *A multi-level modeling approach for the capacitated p-median interdiction problem with fortification*, in ISOLDE XI, 2008.

[38] Y. Sheffi, *Supply chain management under the threat of international terrorism*, International Journal of Logistics Management, 12(2) (2001), pp. 1–11.

[39] D. Simchi-Levi, P. Kaminsky, and E. Simchi-Levi, *Designing and managing the supply chain: concepts strategies and case studies*, McGraw-Hill, Irwin, Boston, MA, 2003.

[40] R. L. Simison, *GM contains its quarterly loss at $809 million*, Wall Street Journal, Oct.14 (1998), p. A2.

[41] ——, *GM says strike reduced its earnings by $2.83 billion in 2nd and 3rd periods*, Wall Street Journal, Aug. 17 (1998), p. 1.

[42] L. Snyder, *Facility location under uncertainty: a review*, IIE Transactions, 38(7) (2006), pp. 537–554.

[43] L. Snyder and M. Daskin, *Stochastic p-robust location problems*, IIE Transactions, 38 (2006), pp. 971–985.

[44] L. Snyder, M. Scaparra, M. Daskin, and R. Church, *Planning for disruptions in supply chain networks*, INFORMS Tutorials in Operations Research, (2006).

[45] H. Stackelberg, *The Theory of Market Economy*, Oxford University Press, 1952.

[46] D. Urban and T. Keitt, *Landscape connectivity: a graph theoretic perspective*, Ecology, 82 (2001), pp. 1205–1218.

[47] L. Vincente, G. Savard, and J. Judice, *Discrete linear bilevel programming problem*, Journal of Optimization Theory and Application, 89 (1996), pp. 597–614.

[48] T. Vincenty, *Direct and inverse solutions of geodesics on the ellipsoid with application of nested equations*, Survey Review, 23 (176) (2008), pp. 88–93.

[49] R. Wollmer, *Removing arcs from a network*, Operations Research, 12 (1964), pp. 934–940.

[50] H. Yu, A. Z. Zeng, and L. Zhao, *Single or dual sourcing: Decision-making in the presence of supply chain disruption risks*, Omega, 37 (2009), pp. 788–800.

[51] J. Zhuang and V. Bier, *Balancing terrorism and natural disasters - Defensive strategy with endogenous attacker effort*, Operations Research, 55 (2007), pp. 976–991.

Tables

Table 1: Upper bound procedure example, step 1. Solution to RIMF problems.

r	$\overline{z}^r$	$\overline{W}_r$
1	1 2	601800.56
2	1 8	733601.95
3	1 11	946700.60

Table 2: Upper bound procedure example, step 2. Solutions to RIM problems.

m	$h_m(\overline{z}^1)$	$c_{h_m(\overline{z}^1)}$	$h_m(\overline{z}^2)$	$c_{h_m(\overline{z}^2)}$	$h_m(\overline{z}^3)$	$c_{h_m(\overline{z}^3)}$
1	5	601800.56	2	615585.71	2	615585.71
2	8 11	809010.44	2 7	733601.95	2 7	733601.95
3	8 11 17	992909.66	3 4 6	946700.60	3 4 6	946700.60

Figures

Figure 1: Efficiency of the system as a function of the number of fortifications Q ($P = 20$, $R = 3$).

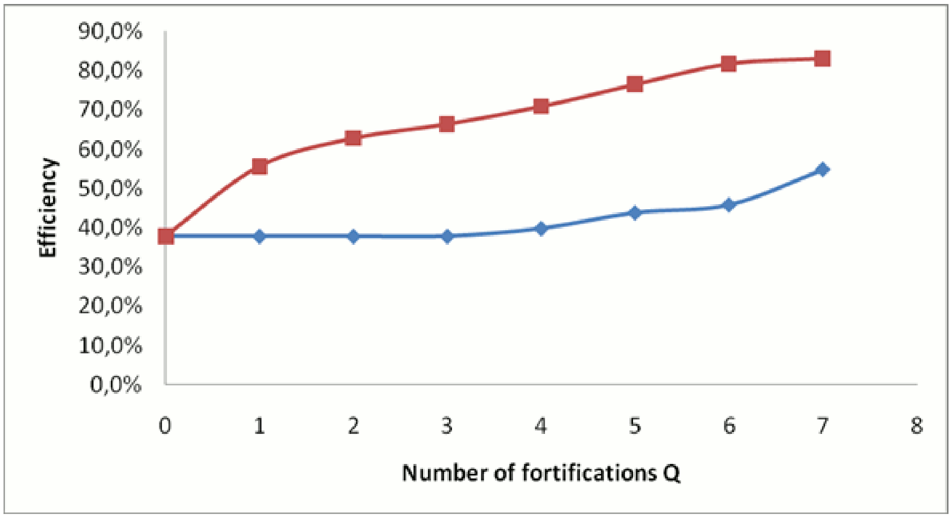


Figure 2: Data set UKMainIsland

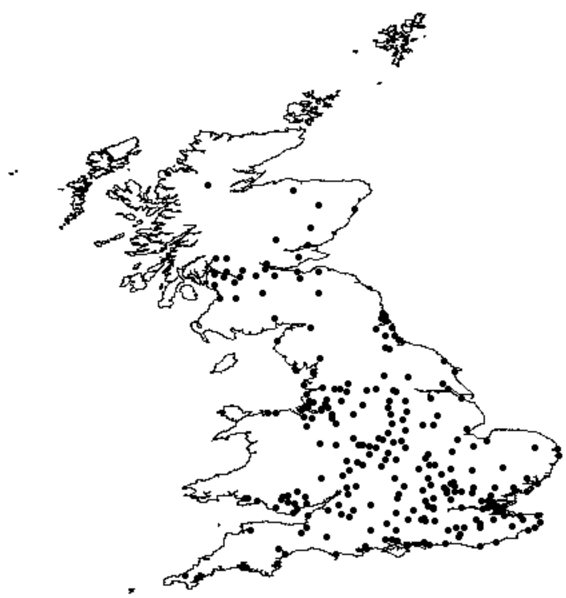
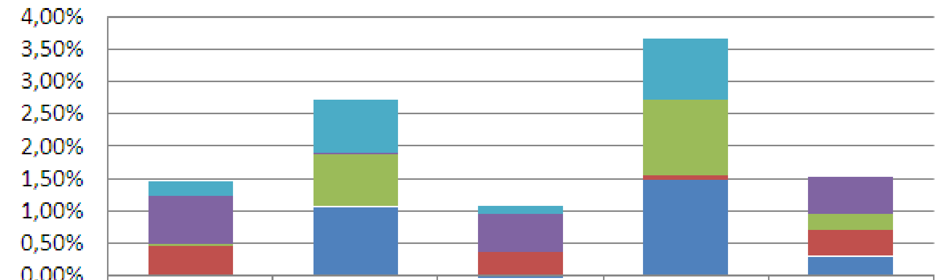
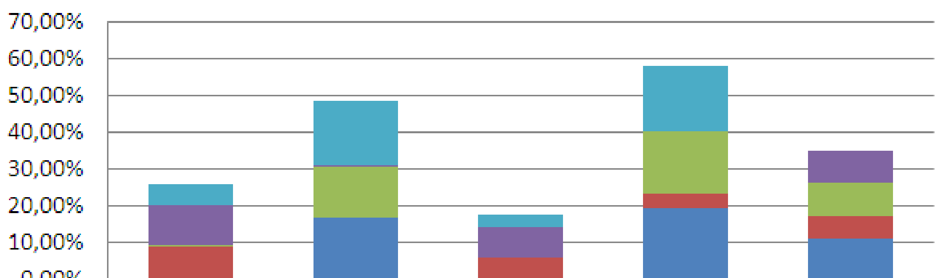


Figure 3: Average and max gap estimations.



	SRIMF-U	SRIMF-D	MOD1-U	MOD1-D	MOD2
MOD2	0,22%	0,83%	0,12%	0,93%	0,00%
MOD1-D	0,74%	0,01%	0,60%	0,00%	0,58%
MOD1-U	0,01%	0,80%	0,00%	1,16%	0,25%
SRIMF-D	0,48%	0,00%	0,36%	0,07%	0,39%
SRIMF-U	0,00%	1,08%	0,01%	1,49%	0,31%

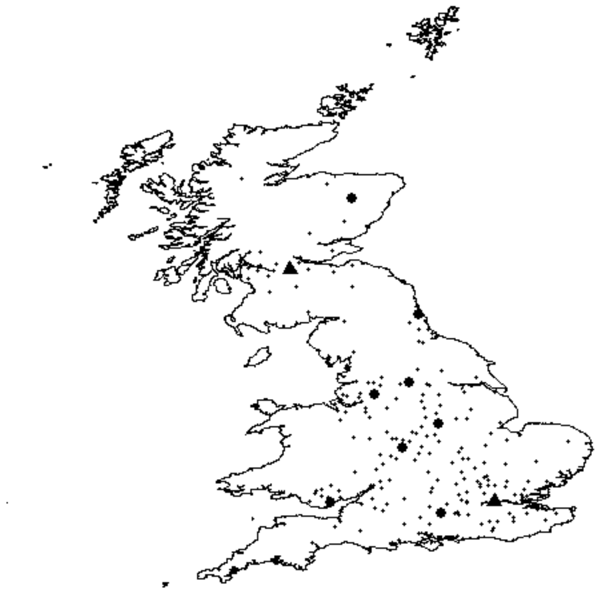
(a) Average gap estimation table and sum histogram.



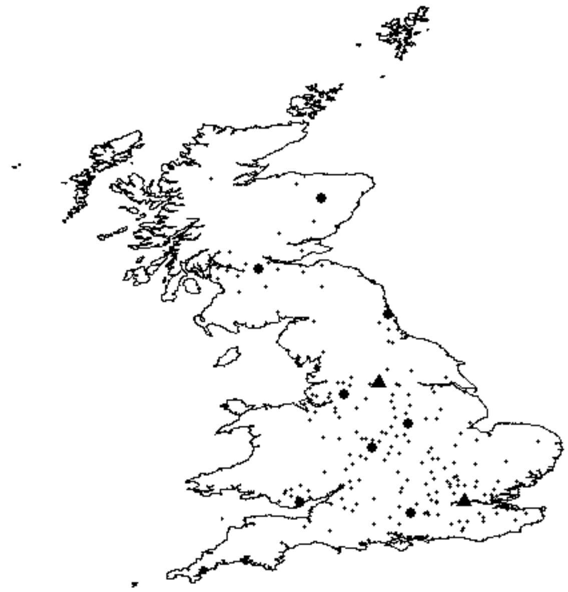
	SRIMF-U	SRIMF-D	MOD1-U	MOD1-D	MOD2
MOD2	5,38%	17,54%	3,33%	17,54%	0,00%
MOD1-D	10,82%	0,43%	8,40%	0,00%	8,68%
MOD1-U	0,58%	13,77%	0,00%	16,97%	9,14%
SRIMF-D	8,99%	0,00%	5,58%	3,76%	5,85%
SRIMF-U	0,00%	16,84%	0,46%	19,52%	11,35%

(b) Max gap estimation table and sum histogram.

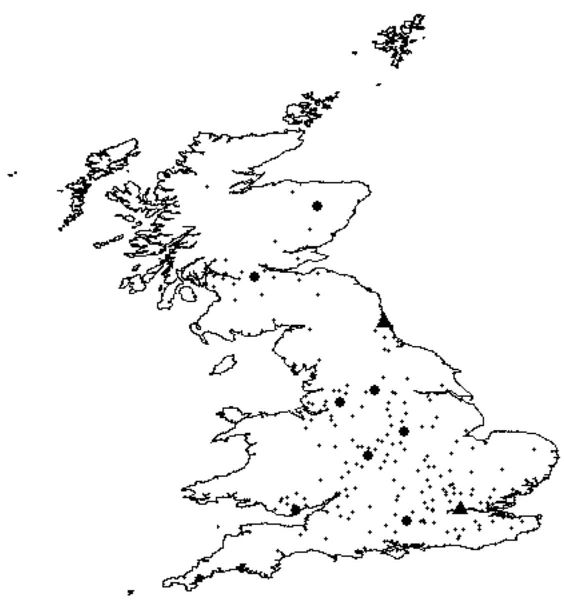
Figure 4: Optimal fortification sets for the instance with parameters $P = 10$, $Q = 2$ and $R = 5$.



(a) Fortification set for SRIMF-D and MOD1-D.



(b) Fortification set for SRIMF-U and MOD1-U.



(c) Fortification set for MOD2.