Protection optimale des installations contre des attaques intentionnelles : une approche basée sur la théorie des jeux

NAJI BRICHA, MUSTAPHA NOURELFATH

Centre Interuniversitaire de Recherche sur les Réseaux d'Entreprise,
la Logistique et le Transport (CIRRELT)
Département de génie mécanique, université Laval, Québec
G1K7P4, Canada

Naji.bricha.1@ulaval.ca
Mustapha.Nourelfath@gmc.ulaval.ca

Résumé **- L'article présente une approche de modélisation de l'allocation optimale des ressources de protection des installations des réseaux logistiques contre des attaques intentionnelles. Cet article considère le problème d'optimisation de la localisation des installations à capacité limitée pour tenir compte de la protection contre ce type d'attaques dès l'étape de conception. L'estimation des dégâts causés par la destruction d'une installation passe par le calcul de sa vulnérabilité qui tient compte de la fonction de succès de compétition caractérisant l'intensité de la compétition entre l'attaquant et la défense. L'article considère le problème comme un jeu non coopératif min-max à deux périodes dans lequel le défenseur joue en premier. Cela signifie que le défenseur choisit une stratégie à la première période qui minimise le dégât maximal que l'attaquant pourrait causer à la seconde période. Les dégâts estimés sont calculés en fonction des frais encourus en raison de l'augmentation du coût de transport et le coût permettant de restaurer les installations endommagées**.

Abstract **- The article presents an optimization modeling approach for allocating protection resources among a system of facilities so that the disruptive effects of possible intentional attacks to the system. This article considers the uncapacitated fixed charge location problem to deal with defence resource allocation. The vulnerability of each facility is determined by an attacker-defender contest success function. The article considers a two-period min-max game where the defender invests in the first period, and the attacker moves in the second period. This means that the defender selects a strategy in the first period that minimizes the maximum loss that the attacker may cause in the second period. The loss incurred by the defender is evaluated of the increasing in transportation cost, and the cost necessary to restore the disabled facility.**

Mots clés **- installations, attaque, protection, théorie des jeux, optimisation.**

Keywords **- facility location, attack, protection, games theory, optimization.**

1 INTRODUCTION

Les installations des réseaux logistiques constituent des infrastructures vulnérables à différentes perturbations pouvant affecter leur performance : accidents, pannes d'équipements, catastrophes naturelles, incendies, attaques intentionnelles, etc. Parmi les facteurs ayant contribué à l'augmentation de la vulnérabilité des réseaux logistiques de notre société moderne, on peut citer par exemple les risques liés à l'utilisation des nouvelles technologies de l'information et de la communication, l'augmentation de leur complexité et la mondialisation des échanges.

Les catastrophes causées par l'homme et par la nature ont augmenté en nombre et en intensité au cours des dernières années (les événements du 11 septembre 2001 étant parmi les plus connus du grand public). Dans le monde actuel, déterminer la meilleure façon de protéger les infrastructures critiques devient de plus en plus important. La protection de ces infrastructures contre des attaques stratégiques et intentionnelles est en fait devenue un sujet important pour les concepteurs.

Les installations des réseaux logistiques font partie des infrastructures critiques qui sont potentiellement vulnérables à des attaques intentionnelles par des adversaires intelligents (terroristes ou autres) [Bier et al., 2007]. Il est donc crucial de les protéger contre ce type d'attaques dès l'étape de conception. Or, la protection contre des attaques intentionnelles est fondamentalement différente de la protection contre des accidents aléatoires ou des désastres naturels [Hausken et al., 2009]. Habituellement, les méthodes de conception basées sur les défaillances probabilistes des composantes ne tiennent pas compte de la possibilité d'attaques intentionnelles. L'attaquant est avantagé par rapport au défenseur dans le sens qu'il peut choisir le temps, la place et les moyens d'attaque. Un adversaire intelligent peut par exemple choisir d'attaquer la partie la plus vulnérable du réseau de façon à causer le maximum de dégâts, ou encore essayer de contourner les moyens de sécurité mis en place et d'adapter ses tactiques en exploitant tous les points faibles de

l'infrastructure. Il en résulte que les méthodes d'allocation des ressources de défense contre ces attaques doivent tenir compte de la nature intelligente et adaptative de la menace.
Cet article s'inscrit dans le cadre d'une problématique générale de conception robuste des réseaux logistiques en tenant compte du risque d'attaques, de la stratégie de l'attaquant et de la valeur des entités ciblées.

2 REVUE DE LA LITTERATURE

La protection des réseaux logistiques contre des attaques stratégiques est un domaine qui a été abordé par des communautés de recherche différentes. Notre revue de littérature va porter sur les deux axes complémentaires à savoir l'analyse de risque et sécurité des installations des réseaux logistiques et la conception robuste des réseaux logistiques.

2.1 Analyse de risque et sécurité des installations des réseaux logistiques

Les perturbations aléatoires menaçant les installations des réseaux logistiques peuvent porter sur les atteintes aux personnes, les dommages aux biens physiques, les pertes d'informations, les dommages aux partenariats, ou les pertes de revenus. Afin de pouvoir gérer les risques, il faut au préalable identifier les vulnérabilités de chaque installation. La vulnérabilité représente le niveau d'exposition de l'entreprise à une perturbation interne ou externe. Dans [Sheffi, 2005], l'auteur explique que la vulnérabilité d'une entreprise face à un environnement inquiétant peut être repérée grâce à la combinaison de la probabilité de la perturbation et de sa gravité. Dans [Martz et Johnson, 1987], les auteurs identifient quatre solutions génériques pour réduire la criticité des risques d'une attaque stratégique : l'évitement, la prévention, la protection et le transfert.
Les premières applications de l'analyse de risque pour assurer la sécurité et lutter contre le terrorisme, ont été réalisées dans [Cox, 1990]. Plusieurs autres travaux [Haimes, et al., 1998] [Ezell et al., 2000] ont été aussi réalisés avant même le 11 Septembre, spécifiquement sur les menaces contre les infrastructures sensibles. Après le 11 Septembre, plusieurs analystes ont proposé l'utilisation de l'analyse de risque pour la sécurité interne d'un pays [Pate-Cornell et Guikema, 2002]. L'accent a été mis principalement sur la prise de décisions fondée sur des analyses de risque pour cibler la sécurité des investissements et isoler les menaces les plus importantes.

2.2 Conception robuste des réseaux logistiques

2.2.1 Modèles de conception d'un réseau logistique

La conception d'un réseau logistique concerne la détermination de sa structure. En d'autres termes, la définition des liens entre les différents processus et activités d'approvisionnement, de production et de distribution. Il s'agit de déterminer le type, le nombre et la localisation des sites, de même que leurs relations d'affaires. Le problème de conception d'un réseau logistique peut être caractérisé comme un problème d'allocation-localisation [Martel, 2005]. Les modèles déterministes fournissent une base pour la conception d'un réseau logistique qui exige des décisions stratégiques sur le nombre, l'endroit, la capacité et la mission d'équipements de production et de distribution [Owen et Daskin, 1998][Daskin et al., 2005]. Dans [Vidal et Goetschalckx, 1997][Vidal et Goetschalckx, 2000], les auteurs ont fait une synthèse de ces travaux et ont montré que la tendance et le défi portent sur la considération de l'incertitude et des perturbations dans les modèles de configuration des réseaux logistiques.

2.2.2 Conception de réseaux logistiques fiables, robustes et résilients

Un réseau logistique est robuste [Martel et al., 2010] s'il peut continuer à créer de la valeur, quels que soient les événements aléatoires et périlleux qui surviennent en mettant en place des politiques de réponse et des stratégies de résilience. Ces dernières permettent au réseau de retomber rapidement sur pied lorsque des ruptures se produisent. Lorsque la résilience est atteinte, l'organisation est alors plus performante ce qui devient un avantage concurrentiel face à l'environnement instable qui auparavant était susceptible d'ébranler le réseau logistique. Dans ce contexte, le critère fiabilité est un critère très pertinent parce qu'il permet d'évaluer la robustesse des configurations du réseau. La notion de fiabilité d'un réseau logistique est liée à la théorie de la fiabilité d'un réseau quelconque. Dans [Shier, 1991], l'auteur a développé un ensemble de méthodes permettant de maximiser la probabilité qu'un graphe reste longtemps connecté après une défaillance.
Portant principalement sur la connectivité, les modèles d'optimisation de la fiabilité des réseaux considèrent le coût de construction du réseau, et non le coût qui résulte d'une rupture. Notons aussi qu'il s'agit souvent d'une fiabilité a posteriori du réseau logistique qui est une évaluation des performances enregistrées par le réseau. Elle est mesurée après la réalisation de l'affaire contractée avec le client. Plusieurs travaux existants portent ainsi sur la conception des réseaux logistiques en tenant compte de la fiabilité [Goetschalckx et al., 2002], la robustesse [Snyder, 2006] et la réactivité [Christopher et Peck, 2004].

2.2.3 Modèles de fortification et de protection des réseaux logistiques

Ces modèles permettent d'identifier les investissements importants de protection et les mesures de sécurité afin d'améliorer la fiabilité des réseaux logistiques et leurs fortifications. Le premier modèle de base est dit RIMF (pour *R-Interdiction Median model with Fortification en anglais*). Il est basé sur le problème *P*-médian. C'est un problème de programmation en nombres entiers mixtes à deux niveaux (niveau du défenseur et niveau de l'attaquant) qui vise la répartition optimale des ressources limitées de protection pour un ensemble d'installations, afin de minimiser les coûts de transport [Scaparra et Church, 2008].
Il existe relativement peu de travaux traitant de l'allocation optimale des ressources de défense contre des attaques intentionnelles. Dans le domaine de la fiabilité, la majorité des travaux existants mettent l'emphase sur l'identification des risques, la fortification des cibles vulnérables et l'augmentation de la probabilité de survie du système. La détermination de stratégies de réduction du risque suppose souvent que la menace est statique [Levitin, G., 2003]. Alors que ces travaux sont très importants et essentiels, ils ignorent la nature intelligente et dynamique d'une menace [Cox, 1990] [Bier et al., 2007]. Le problème d'optimisation ainsi considéré ne tient pas compte de la stratégie de l'attaquant.
La prise en considération à la fois des points de vue du défenseur et de l'attaquant, dans la protection d'infrastructures critiques, constitue actuellement un thème de recherche en pleine émergence dans la communauté des fiabilistes. Dans un travail récent [Hausken, 2011], les auteurs montrent l'importance d'utiliser la théorie des jeux comme cadre conceptuel pour tenir compte des actions d'adversaires

intelligents. Au début, la théorie des jeux a été appliquée pour résoudre des problèmes liés à des applications militaires. Dans [Haywood, 1954][Berkovitz et Dresher, 1960], les auteurs ont appliqué la théorie des jeux à l'emploi optimal des tactiques de guerre dans l'armé de l'air sous forme d'un jeu à multi-périodes entre les deux côtés opposés. Dans ce jeu, chaque côté cherche le plus grand profit possible.

Sachant que les probabilités de comportement attendu de l'attaquant peuvent être calculées, il est normal d'appliquer les techniques de la théorie des jeux pour développer des stratégies permettant d'optimiser la défense de l'infrastructure, en tenant compte du fait que les antagonistes peuvent adapter leurs actions afin d'exploiter les faiblesses des infrastructures. Dans [Hausken et al., 2009], les auteurs ont développé plusieurs méthodes permettant d'affecter des ressources parmi les composantes d'infrastructures critiques pour les défendre contre des antagonistes intelligents en tenant compte de la nature intelligente et adaptative de la menace, ainsi d'autres méthodes pour la protection contre des accidents et des phénomènes naturels.

Plusieurs autres travaux existants se concentrent sur les jeux probabilistes traitant des modèles qui ne considèrent que les probabilités de succès d'attaques, étant donné que les attaquants semblent prendre la probabilité de succès en considération dans leur choix de cibles (ressources les plus précieuses). En combinant la théorie de la fiabilité des systèmes et les techniques de la théorie des jeux, certains auteurs [Levitin et Hausken, 2010] ont récemment développé un ensemble de méthodes et d'algorithmes permettant l'allocation optimale des ressources de protection (défense) contre des attaques stratégiques pour des structures séries et parallèles. Enfin, certains travaux ont aussi analysé l'amélioration de la stratégie de défense par le déploiement des fausses cibles dans le système [Hausken et Levitin, 2009] [Levitin et Hausken, 2009].

La revue de la littérature montre qu'il n'existe pas de méthode d'allocation optimale des ressources de défense qui tient compte de la stratégie de l'attaquant dans un contexte de conception des réseaux logistiques.

L'objectif de cet article est de développer une méthode d'allocation optimale des ressources de défense qui tient compte de la stratégie de l'attaquant. Cette méthode sera développée dans le contexte de l'optimisation de la localisation des installations.

L'objectif de la localisation optimale des installations est d'aider les entreprises à situer leurs installations pour répondre de façon optimale aux demandes de leurs clients.

Nous allons considérer plusieurs installations et un ensemble de points de demandes (clients). Le problème consiste à déterminer les installations à ouvrir, leurs emplacements et les flux des produits de façon à minimiser le coût total, composé du coût fixe des installations et du coût de transport.

Nous calculons les dégâts et nous évaluons la valeur d'une cible critique. Quand une usine qui doit servir un ensemble de clients donnés est hors service suite à une attaque, ces clients devront être servis par une autre usine qui se trouve plus loin. Il en résulte que les coûts engendrés vont correspondre non seulement aux coûts de restauration, mais aussi aux coûts de transport additionnels. Notre objectif ici est de proposer un modèle d'évaluation du dégât engendré par l'attaque d'une ou plusieurs installations.

Sachant que la protection de toutes les installations d'un réseau logistique exposées à des attaques intentionnelles serait trop coûteuse, on considère le cas dans lequel le concepteur doit répartir un budget limité pour les protéger de façon optimale. Une telle protection doit tenir compte non seulement de la valeur des entités ciblées, mais aussi de la stratégie de l'attaquant. Il s'agira de répartir un budget limité de façon optimale entre les différentes installations, tout en intégrant le caractère stratégique de l'attaquant. Dans le passé, c'est dans le domaine de la défense militaire que cette question a été étudiée en utilisant des concepts issus de la théorie des jeux [Berkovitz et Dresher, 1959]. Notre objectif sera d'étendre ou d'adapter ces concepts au domaine de la protection des installations d'une chaîne logistique.

3 LOCALISATION DES INSTALLATIONS

Dans le modèle utilisé pour l'optimisation de la localisation des installations, nous n'avons pas considéré de limites sur la capacité des installations (*Uncapacitated Facility Location Problem*). La fonction de l'objectif à minimiser correspond à la somme des coûts fixes d'acquisition des installations et des coûts de transport. En absence de toute attaque, ce modèle nous permet de déterminer les installations à ouvrir, leurs emplacements et les flux des produits. Selon [Balinski, 1965], en utilisant les notations définies ci-dessous :

i	point de demande client
j	localisation de l'installation (usine, entrepôt)
h_i	demande du produit par le client i
f_j	coût fixe de l'installation j
ρ_{ij}	coût unitaire de distribution entre l'installation j et le client i
X_j	1 si l'installation j est utilisée, 0 autrement
Y_{ij}	fraction de demande client i s'il est servi par l'installation j.

La formulation du problème est définie ainsi:

$$\text{Min } \sum_j f_j X_j + \sum_j \sum_i h_j \rho_{ij} Y_{ij}, \quad (1)$$

Sujet. à

$$\sum_j Y_{ij} = 1 \qquad \forall i, \quad (2)$$

$$Y_{ij} \leq X_j \qquad \forall i, j, \quad (3)$$

$$X_j \in \{0, 1\} \qquad \forall j, \quad (4)$$

$$Y_{ij} \geq 0 \qquad \forall i, j, \quad (5)$$

La fonction de l'objectif (1) minimise la somme des coûts fixes d'acquisition des installations et des coûts de transport. La contrainte (2) exige que chaque client i puisse être servi par une ou plusieurs installations j. La contrainte (3) interdit à un client d'être affecté à une installation qui n'a pas été ouverte. La contrainte (4) exige que les variables de localisation des installations doivent être binaires et la contrainte (5) est une contrainte de non-négativité.

Ce modèle est un problème NP-durs [Garey et Johnson, 1979] et il y a un certain nombre d'approches de solutions qui ont été proposées pour le résoudre. Pour bien comprendre ce problème, le lecteur peut être référé par exemple aux travaux de [Cornuéjols et al., 1990]. Dans cet article, le problème de localisation des installations sera résolu en utilisant CPLEX.

Si nous notons n le nombre d'installations et k l'index de chaque scénario d'attaque alors 2^n-1 est le nombre de tous les scénarios possibles d'attaque (k =1,…, 2^n-1). Par exemple, pour deux installations, le nombre de scénarios d'attaque est 3 (k = 1: l'installation 1 est endommagée et l'installation 2 est opérationnelle, k = 2: l'installation 2 est endommagée et l'installation 1 est opérationnelle, k = 3: les deux installations sont endommagées).

4 LE MODELE

4.1 L'investissement du défenseur et de l'attaquant

Sachant que les installations sont assujetties à des attaques intentionnelles, on suppose que plusieurs installations peuvent être attaquées en même temps et que chaque installation peut être attaquée une seule fois. Le défenseur doit choisir la meilleure façon de répartir ses efforts de protection entre les différentes installations. Il dispose pour cela de plusieurs alternatives de protection ayant des coûts différents (mise en place de procédures de sécurité, engagement d'experts, investissements technologiques, surveillance de composantes critiques, etc.).

Chaque type de protection est indexé par la variable p (p = 0, 1, 2,…, β_j). p = 0 signifie l'absence de toute protection. Le choix d'un type de protection p d'une installation j, représente la stratégie de protection de cette installation.

On introduit la variable binaire λ_{jp} qui est égale à 1 si l'installation j est protégée par un et un seul type de protection p telle que:

$$\sum_{p=0}^{\beta_j} \lambda_{jp} = 1, \quad \forall j \qquad (6)$$

La protection d'une installation localisée au site j avec le type protection p, nécessite un investissement ou un effort B_{jp} à un coût unitaire b_{jp}. On définit le coût investi par le défenseur en sécurité comme suit : $\overline{B_{jp}} = b_{jp}B_{jp}$

L'attaquant dispose aussi de plusieurs alternatives d'attaques ayant des coûts différents (contournements des moyens de sécurité mis en place, destruction, vol, etc.).

Chaque type d'attaque est indexé par la variable m (m = 0, 1, 2,…,α_j). m = 0 signifie l'absence de toute attaque. Le choix d'une action d'attaque m, représente la stratégie d'attaque d'une installation localisée au site j.

On introduit la variable binaire μ_{jm} qui est égale à 1 si l'installation j est attaquée en utilisant l'action d'attaque m telle que:

$$\sum_{m=1}^{\alpha_j} \mu_{jm} = 1, \quad \forall j \qquad (7)$$

L'attaque d'une installation localisée au site j avec une action d'attaque m, nécessite un investissement ou un effort Q_{jm} à un coût unitaire q_{jm}. On définit le coût investi par l'attaquant comme suit: $\overline{Q_{jm}} = q_{jm}Q_{jm}$.

4.2 Fonction de succès de compétition

Alors que l'objectif du défenseur est de minimiser les dégâts, l'attaquant va chercher à maximiser ces dégâts. Le problème a été défini comme un jeu non coopératif min-max à deux périodes dans lequel le défenseur joue en premier. Cela signifie que le défenseur choisit une stratégie à la première période qui minimise le dégât maximal que l'attaquant pourrait causer à la seconde période. Cette façon de faire permet de tenir compte du point de vue de l'attaquant dans l'allocation optimale des ressources par le défenseur.

La solution de ce jeu non coopératif nécessite l'évaluation des fonctions utilités des deux joueurs (le défenseur et l'attaquant). Ces utilités dépendent des dépenses encourus par les joueurs et des dégâts espérés. Or, l'estimation des dégâts causés par la "destruction" d'une installation j passe par le calcul de sa vulnérabilité notée $\nu_{pm}(j)$. Il y a un conflit sur cette vulnérabilité entre le défenseur et l'attaquant. Si l'on considère que les efforts de l'attaque et de la défense ont un impact proportionnel, cette vulnérabilité peut être calculée par :

Vulnérabilité = Effort d'attaque / (Effort d'attaque + Effort de défense).

Dans la théorie des jeux [Levitin et Hausken, 2010], l'interaction entre joueurs conflictuels est habituellement modélisée en introduisant le concept de fonction de succès de compétition (*contest sucess function*) [Hausken, 2005][Nitzan, 1994]. La forme usuelle de cette fonction consiste selon [Skaperdas, 1996] [Tullock, 1980], en un rapport utilisant un paramètre ($c_j \geq 0$) caractérisant l'intensité de la compétition tel que :

Vulnérabilité = $(\text{Effort d'attaque})^{c_j}$ / $[(\text{Effort d'attaque})^{c_j} + (\text{Effort de défense})^{c_j}]$

Dans notre contexte, cette vulnérabilité s'écrit :

$$\nu_{pm}(j) = \frac{\left(Q_{jm}\right)^{c_j}}{\left(B_{jp}\right)^{c_j} + \left(Q_{jm}\right)^{c_j}}, \qquad (8)$$

Le cas de Q_{jm}= B_{jp} = 0 ne peut se produire parce que chaque partie à intérêt à exercer plus d'effort pour plus de profit. La figure 1 illustre comment la probabilité $\nu_{pm}(j)$ varie en fonction de l'investissement B_{jp} du défenseur pour différentes valeurs de c_j lorsque Q_{jm} = 1. Lorsque le paramètre c_j est nul, les efforts d'attaque et de défense ont un impact égal indépendamment des tailles respectives des efforts, ce qui donne une vulnérabilité de 50%. Lorsque c_j = 1, la probabilité $\nu_{pm}(j)$ dépendra de l'investissement de chaque partie. Une valeur de c_j supérieure à 1 donne un avantage disproportionnel à celui qui exerce plus d'effort que son adversaire. c_j= ∞ donne une fonction échelon: ″le gagnant prend tout″ ("*winner-takes-all*").

4.3 Les utilités du défenseur et de l'attaquant

Une fois les vulnérabilités des installations sont estimées, il devient possible d'évaluer les utilités du défenseur et de l'attaquant. Ces utilités dépendent non seulement des efforts et de leurs efficacités, mais aussi des frais encourus en raison de l'augmentation de coût de transport et le coût nécessaire pour restaurer l'installation endommagée.

Les dégâts estimés sont calculés en fonction des trois coûts suivants :

- Le coût total Cr de restauration des installations endommagées. Si R(j) est le coût permettant de restaurer l'installation endommagée j, alors ce coût est définit comme suit:

$$C_R = \sum_j \sum_m \sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j \qquad (9)$$

- Le coût C_B encouru lorsque la demande est non satisfaite, dans le cas si toutes les installations sont hors service. Si B est le coût (*backorder*) alors ce coût peut être calculé par la relation suivante :

$$C_B = B\prod_j \left[\sum_m \sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j) \right] \qquad (10)$$

- Le coût ΔC encouru en raison de l'augmentation du coût de transport suite à une attaque. Si une installation non fortifiée est endommagée, il faut assurer la satisfaction de la demande de ses clients par d'autres plus éloignées, ce qui va augmenter le coût de transport.

L'estimation des dégâts est calculée par la relation suivante:

$$D=\sum_j\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j+B\prod_j\left[\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)\right]+\Delta C \quad (11)$$

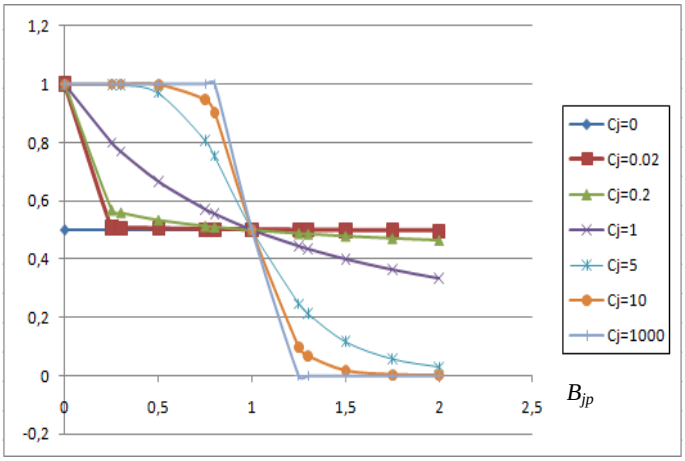

Figure 1. Probabilité $\nu_{pm}(j)$ en fonction de l'investissement B_{jp} pour différentes valeurs de c_j lorsque Q_{jm} = 1

L'évaluation de ΔC nécessite la définition de tous les scénarios d'attaque. On note T_k le coût encouru en raison de l'augmentation du coût de transport pour un scénario d'attaque k. A titre d'exemple illustratif, le tableau 1 présente tous les scénarios d'attaque possibles des trois installations désignées par I1, I2 et I3. Dans ce cas, il ya 7 scénarios indexés par k = 1,...,7.

Tableau 1. Scénarios d'attaque de trois installations.

Scénario	k
I1 est hors service et les deux autres installations sont fonctionnelles	1
I2 est hors service et les deux autres installations sont fonctionnelles	2
I3 est hors service et les deux autres installations sont fonctionnelles	3
I1 et I2 sont hors service, et I3 est fonctionnelle	4
I1 et I3 sont hors service, et I2 est fonctionnelle	5
I2 et I3 sont hors service, et I1 est fonctionnelle	6
I1, I2 et I3 sont hors service	7

Le coût ΔC peut être calculé en fonction des probabilités de destruction qui sont désignées par $\Psi_{mp}(k)$ et le coût T_k comme suit:

$$\Delta C=\sum_k\sum_m\sum_p T_k\psi_{mp}(k) \quad (12)$$

Le tableau 2 illustre ces probabilités pour chaque scénario d'attaque. Par exemple pour le scenario d'attaque 5, les installations I1 et I3 sont hors service et l'installation I2 est fonctionnelle.
Donc pour ce scénario, la probabilité de destruction est $\Psi_{mp}(5) = \nu_{mp}(1)\nu_{mp}(3)(1-\nu_{mp}(2))$ et $\Delta C = T_5\,\Psi_{mp}(5)$.

Tableau 2. Probabilités de destruction pour le cas de trois installations.

Scénario k	$\psi_{mp}(k)$
0	0
1	$\nu_{mp}(1)(1-\nu_{mp}(2))(1-\nu_{mp}(3))$
2	$\nu_{mp}(2)(1-\nu_{mp}(1))(1-\nu_{mp}(3))$
3	$\nu_{mp}(3)(1-\nu_{mp}(1))(1-\nu_{mp}(2))$
4	$\nu_{mp}(1)\nu_{mp}(2)(1-\nu_{mp}(3))$
5	$\nu_{mp}(1)\nu_{mp}(3)(1-\nu_{mp}(2))$
6	$\nu_{mp}(2)\nu_{mp}(3)(1-\nu_{mp}(1))$
7	$\nu_{mp}(1)\nu_{mp}(2)\nu_{mp}(3)$

L'utilité du défenseur notée U_d est calculée come suit:

$$U_d=-D-\sum_j\overline{B_j}=-\left[\sum_j\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j\right.$$

$$\left.+B\prod_j\left[\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)\right]+\sum_k\sum_m\sum_p T_k\psi_{mp}(k)\right]-\sum_j\overline{B_j} \quad (13)$$

L'utilité de l'attaquant notée U_a est calculée come suit:

$$U_a=D-\sum_j\overline{Q_j}=\sum_j\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)R_j$$

$$+B\prod_j\left[\sum_m\sum_p \lambda_{jp}\mu_{jm}\nu_{pm}(j)\right]+\sum_k\sum_m\sum_p T_k\psi_{mp}(k)-\sum_j\overline{Q_j} \quad (14)$$

4.4 Résolution du problème

Notations

U_{min}	L'utilité minimale du défenseur
U_{max}	L'utilité maximale de l'attaquant
Mat $(\Theta^n \times (\beta+1)^n \times (\alpha+1)^n, 3n)$	Matrice de $\Theta^n \times (\beta+1)^n \times (\alpha+1)^n$ lignes et $3n$ colonnes. Ses éléments sont composés de la combinaison des valeurs de la fonction de succès de compétition qui sont combinés aux types de protection *p*, qui sont eux même combinés aux types d'attaque *m*.
u	Numéro de la ligne de la matrice
r_a	Numéro de la ligne de la matrice qui correspond à l'utilité maximale de l'attaquant.
r_d	Numéro de la ligne de la matrice qui correspond à l'utilité minimale du défenseur.
$M(j)$	Vecteur solution optimale de l'attaquant, qui contient les différents types d'attaque.
$P(j)$	Vecteur solution optimale du défenseur qui contient les différents types de protection.

La répartition optimale des ressources limitées de protection est obtenue par résolution d'une double boucle de jeu à deux périodes. L'ensemble de l'algorithme de résolution est définie ci-dessous:

1. $U_{min} = \infty$
2. $U_{max} = 0$
3. pour $u = 1,\ldots, \Theta^n \times (\beta+1)^n \times (\alpha+1)^n$ faire
   - 3.1. pour $j = 1,\ldots,N$ faire
     - 3.1.1. $c_j = Mat(u, j)$
     - 3.1.2. déterminer $v_{pm}(j)$ par (8)
     - 3.1.3. déterminer C_R par (9)
     - 3.1.4. déterminer C_B par (10)
   - 3.2. pour $k = 1,\ldots,2^n-2$ faire
     - 3.2.1. déterminer ΔC par (12)
   - 3.3. déterminer D par (11)
   - 3.4. déterminer U_a par (14)
     - 3.4.1. si $U_a > U_{max}$ alors $U_{max} = U_a$, $r_a = u$
       - 3.4.1.1. pour $j = 1,\ldots,N$ faire
         - $M(j) = Mat(r_a, j+2n)$
4. répéter instructions de 3. jusqu'à 3.3.
   - 4.1. déterminer U_d par (13) en fonction de $M(j)$
     - 4.1.1. si $|U_d| < U_{min}$ alors $U_{min} = |U_d|$, $r_d = u$
       - 4.1.1.1. pour $j = 1,\ldots,n$ faire
         - $P(j) = Mat(r_d, j+n)$

5 APPLICATION NUMERIQUE

Dans cette section, un exemple numérique est présenté pour illustrer l'application du modèle. Nous considérons 5 installations et 10 points de demande (clients). Les tableaux 3, 4 et 5 contiennent les données de cet exemple, pour une période de 20 ans. La figure 2, présente la solution optimale, dans une situation normale (aucune attaque). Dans cette situation, le coût fixe est \$163 millions et le coût de transport est \$103.02 millions. Si par exemple l'installation 1 est endommagée (figure 3), à cause d'une attaque, le coût de transport deviendra \$ 175.12 millions, et augmentera de 70%. Le tableau 6, présente la variation du coût T_K/semaine pour tous les scénarios d'attaque. Le coût (*backorder*) B est \$1.6 millions. Le tableau 7, présente les types de protection et le tableau 8, les types d'attaque. Le coût (en million de \$) de restauration des installations endommagées est illustré dans le tableau 9.

Tableau 3. Coûts fixes d'acquisition des installations

Site *j*	fixed cost (Million \$)
1	42
2	48
3	24
4	32
5	17

Tableau 4. Demande des clients

Client *i*	Demande
1	15000
2	1000
3	800
4	18000
5	700
6	2000
7	12000
8	900
9	28000
10	13000

Tableau 5. Coût unitaire de distribution de la marchandise entre l'installation *j* et le client *i*.

Instal *j*		1	2	3	4	5
Client *i*	1	0.0016	0.0061	0.0063	0.0078	0.0074
	2	0.0010	0.0056	0.006	0.0072	0.007
	3	0.0042	0.0019	0.0042	0.0075	0.0056
	4	0.0050	0.0017	0.0044	0.0061	0.0049
	5	0.0066	0.0049	0.0031	0.0076	0.0028
	6	0.0058	0.0048	0.0013	0.0066	0.0029
	7	0.0060	0.0051	0.0009	0.0048	0.0027
	8	0.0070	0.0079	0.0038	0.0006	0.0031
	9	0.0076	0.0082	0.0051	0.0007	0.0041
	10	0.0075	0.0071	0.0046	0.0069	0.0008

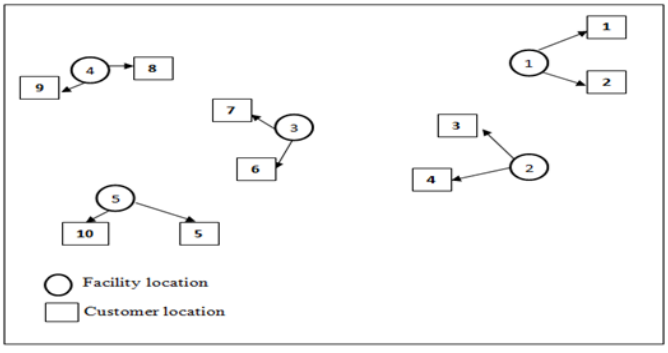

Figure 2. Solution optimale dans une situation normale

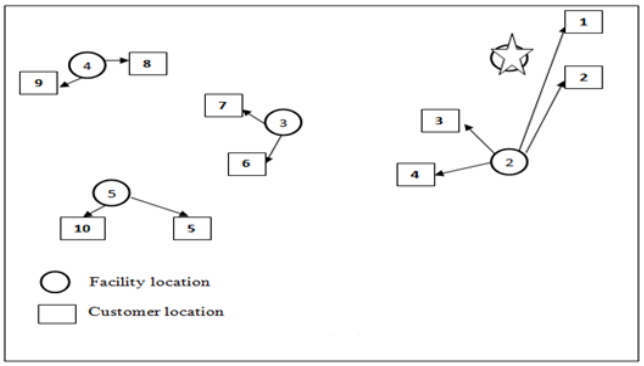

Figure 3. Solution optimale lorsque l'installation 1 est endommagée

Tableau 6. Coût T_K/semaine pour tous les scénarios d'attaque

Scénario k	Installation j endommagée	T_K/semaine
1	1	0,069326923
2	2	0,0485
3	3	0,023846154
4	4	0,093701923
5	5	0,047701923
6	1 _ 2	0,121096154
7	1_3	0,093173077
8	1_4	0,163028846
9	1_5	0,117028846
10	2_3	0,081
11	2_4	0,142201923
12	2_5	0,096134615
13	3_4	0,117548077
14	3_5	0,129394231
15	4_5	0,168932692
16	1_2_3	0,1715
17	1_2_4	0,214798077
18	1_2_5	0,168798077
19	1_3_4	0,186875
20	1_3_5	0,198721154
21	1_4_5	0,238259615
22	2_3_4	0,174701923
23	2_3_5	0,191346154
24	2_4_5	0,217432692
25	3_4_5	0,412192308
26	1_2_3_4	0,265201923
27	1_2_3_5	0,310519231
28	1_2_4_5	0,290028846
29	1_3_4_5	0,412923077
30	2_3_4_5	0,404

Tableau 7. Stratégies du défenseur

Stratégies	b_{jp}	B_{jp}	$\overline{B_{jp}}$
1	0,38	1,6	0,608
2	0,3	1,3	0,39
3	0,4	1,9	0,76
4	0,36	1,5	0,54

Tableau 8. Stratégies de l'attaquant

Stratégies	q_{jm}	Q_{jm}	$\overline{Q_{jm}}$
1	0,157	0,7	0,11
2	0,15	0,8	0,12
3	0,35	0,2	0,07
4	0,25	0,4	0,1

Tableau 9. Coûts de restauration des installations endommagées

l'installation endommagée j	Coût de restauration $R(j)$
1	0,250
2	0,275
3	0,125
4	0,150
5	0,075

Le tableau 10 présente la solution optimale pour différentes valeurs de la fonction de succès de compétition c_j. Par exemple, lorsque c_j =1, la solution optimale pour le défenseur est :

- L'utilité *Ud* = 2,18
- La stratégie de protection (3 3 4 4 2) : les installations 1 et 2 sont protégées par le type 3, les installations 3 et 4 sont protégées par le type 4 et l'installation 5 par le type 2.

Et pour l'attaquant :

- L'utilité *Ua* = 0,8
- La stratégie d'attaque (2 2 2 2 2) : toutes les installations sont protégées par le type 2.

Dans notre cas, le choix d'une stratégie de protection avec un investissement très important (augmentation de l'effort de protection par rapport à l'effort d'attaque), permet de minimiser le dégât maximal causé par l'attaquant. Selon cette stratégie de protection, les résultats donnés dans le tableau 10, montrent que la fonction d'utilité diminue au fur et à mesure que la fonction de succès de compétition c_j augmente.

Tableau 10. Solution optimale pour différentes valeurs de la fonction de compétition c_j

c_j	Type d'attaque m					U_a	Type de Protection p					U_d
0,02	3	3	3	3	3	1,125	2	2	2	2	2	2,45
0,2	1	1	3	3	3	1,024	2	2	2	2	2	2,33
1	2	2	2	2	2	0,8	3	3	4	4	2	2,18
5	2	2	2	2	2	0,65	3	3	4	4	4	1,95
10	0	2	0	0	0	0,6	2	4	2	2	2	1,92
100	0	0	0	0	3	0,58	2	2	2	2	2	1,88

6 CONCLUSION

Le problème de la protection des installations des réseaux logistiques est extrêmement important au point de vue économique et social. Comme ces installations sont des

infrastructures critiques (distribution de médicaments par exemple aux entreprises et aux citoyens), elles doivent être protégées efficacement contre des attaques stratégiques. Dans une approche purement fiabiliste, on ne tient pas compte de la nature intelligente et adaptative de la menace. Une telle approche fonctionne bien quand il s'agit de protéger les installations contre des accidents ou des désastres naturels. Elle est aussi essentielle pour évaluer les installations vulnérables du réseau. Cependant, elle ne permet pas d'anticiper et de quantifier les risques provenant d'un attaquant intelligent et obstiné. Dans le paradigme adopté dans cet article, la théorie des jeux est utilisée pour optimiser la défense tout en tenant compte de la stratégie de l'adversaire.

Un certain nombre de questions importantes reste à explorer comme l'étude de l'importance de l'information intelligente (sur la stratégie de l'attaquant) pour la réduction du dommage : afin d'obtenir de l'information, l'attaquant attribue une partie de ses ressources dans l'activité de renseignements. Le défenseur doit allouer aussi, une partie de ses ressources dans l'activité de contre-espionnage. Ces aspects feront l'objet de travaux futurs.

7 REFERENCES

Balinski, M., (1965) Integer programming: methods, uses, computation. Management Science 12, 254-313.

Berkovitz, L., Dresher, M., (1959) A game-theory analysis of tactical air war. Military Operations Research, 599–620.

Berkovitz, L., Dresher, M., (1960) Allocation of two types of aircraft in tactica. Military Operations Research, 694–706.

Bier, V., Oliveros, S., Samuelson, L., (2007) Choosing What to Protect: Strategic defensive Allocation Against an Unknown Attacker. Journal of Public Economic Theory, 563-587.

Christopher, M., Peck, H., (2004) Building the resilient supply chain. International Journal of Logistics Management, 1–13.

Cornuéjols G.P., Nemhauser G.L., Laurence A. Wolsey., (1990) The uncapacitated facility location problem. In Discrete Location Theory, 119-171.

Cox, L., (1990) A probabilistic risk assessment program for analyzing security risks. In New risks: Issues and management, New York, Plenum Press.

Daskin, M., Snyder, L., Berger, R., (2005) Facility Location in Supply Chain Design. Logistics Systems: Design and Operation. Springer, New York, 39–66.

Ezell, B., Farr, J. and Wiese, I., (2000) Infrastructure risk analysis of municipal water distribution system. Journal of Infrastructure Systems, 118–122.

Garey M.R., Johnson D.S., (1979) Computers and Intractability. A Guide to the Theory of NP-Completeness. Freemann, San Francisco.

Goetschalckx, M., Vidal, C., Dogan, K., (2002) Modeling and design of global logistics systems: A review of integrated strategic and tactical models and design algorithms. European Journal of Operational Research, 1–18.

Haimes, Y., Matalas, N., Lambert H., Jackson, et Fellows, (1998) A. Reducing vulnerability of water supply systems to attack. Journal of Infrastructure Systems, 164–177.

Hausken K., (2005) Production and conflict models versus rent seeking models. Public Choice, 123:59–93.

Hausken, K., Bier, V., Zhuang, J., (2009) Defending against Terrorism, Natural Disaster, and All Hazards. Game Theoretic Risk Analysis of Security Threats. Springer, New York, 65-97.

Hausken, K., Levitin, G., (2009) Protection vs. False Targets in Series Systems. Reliability Engineering and System Safety, 973-981.

Hausken, K., (2011) Protecting complex infrastructures against multiple strategic attackers, International Journal of Systems Science, 42: 1, 11-29.

Haywood, O., (1954) Military decision and game theory. Journal of the Operations Research Society of America, 365–385.

Owen S., Daskin M., (1998) Strategic Facility Location: A Review. European Journal of Operational Research, 423-447.

Levitin, G., (2003) Optimal multilevel protection in series-parallel systems, Reliability Engineering and System Safety, 93-102.

Levitin, G., Hausken, K., (2009) Redundancy Vs. Protection in Defending Parallel Systems Against Unintentional and Intentional Impacts. IEEE Transactions on Reliability, 679-690.

Levitin, G., Hausken, K., (2009) False Targets Efficiency in Defense Strategy. European Journal of Operational Research, 155-162.

Levitin, G., Hausken, K., (2010) Defence and attack of systems with variable attacker system structure detection probability. Journal of the Operational Research Society, 124-133.

Martel, A., (2005) The design of production-distribution networks: A mathematical programming approach. In: Geunes, J., Pardalos, P. (Eds.), Supply Chain Optimization. Springer, 265–306.

Martel, A., Walid, K., Guitouni, A., (2010) The design of robust value-creating supply chain networks: A critical review. European Journal of Operational Research, 283–293.

Martz, H., Johnson, M., (1987) Risk analysis of terrorist attacks. Risk Analysis, 35–47.

Nitzan S., (1994) Modelling rent-seeking contests, European Journal of Political Economy, 10, 41–60.

Pate-Cornell, E., Guikema, S., (2002) Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research, 5–20.

Scaparra, M., Church, R., (2008) An exact modeling approach for the interdiction median problem with fortification. European Journal of Operational Research, 76-92.

Skaperdas S., (1996) Contest success functions. Econ Theory, 7, 283–90.

Sheffi, Y., (2005) The Resilient Enterprise, Cambridge, Mass: MIT Press.

Shier, D., (1991) Network Reliability and Algebraic Structures. Clarendon Press, Oxford, England.

Snyder, L., (2006) Facility location under uncertainty: A review. IIE Transactions, 537–554.

Tullock G., (1980) Efficient rent seeking. In: Buchanan. Toward a theory of the rent seeking society, 97-112.

Vidal, C., Goetschalckx, M., (1997) Strategic Production Distribution Models: A critical Review with Emphasis on Global Supply Chain Models. European Journal of Operational Research, 1-18.

Vidal, C., Goetschalckx, M., (2000) Modeling the Effect of Uncertainties on Global Logistics Systems. Journal of Business Logistics, 95-120.