

Université de Montréal

**Dimensionnement GRWA et protection par segment
dans les réseaux optiques WDM**

par
Alexandre Bouffard

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

novembre, 2005

© Alexandre Bouffard, 2005.



QA

76

U54

2006

V.004



Direction des bibliothèques

AVIS

L'auteur a autorisé l'Université de Montréal à reproduire et diffuser, en totalité ou en partie, par quelque moyen que ce soit et sur quelque support que ce soit, et exclusivement à des fins non lucratives d'enseignement et de recherche, des copies de ce mémoire ou de cette thèse.

L'auteur et les coauteurs le cas échéant conservent la propriété du droit d'auteur et des droits moraux qui protègent ce document. Ni la thèse ou le mémoire, ni des extraits substantiels de ce document, ne doivent être imprimés ou autrement reproduits sans l'autorisation de l'auteur.

Afin de se conformer à la Loi canadienne sur la protection des renseignements personnels, quelques formulaires secondaires, coordonnées ou signatures intégrées au texte ont pu être enlevés de ce document. Bien que cela ait pu affecter la pagination, il n'y a aucun contenu manquant.

NOTICE

The author of this thesis or dissertation has granted a nonexclusive license allowing Université de Montréal to reproduce and publish the document, in part or in whole, and in any format, solely for noncommercial educational and research purposes.

The author and co-authors if applicable retain copyright ownership and moral rights in this document. Neither the whole thesis or dissertation, nor substantial extracts from it, may be printed or otherwise reproduced without the author's permission.

In compliance with the Canadian Privacy Act some supporting forms, contact information or signatures may have been removed from the document. While this may affect the document page count, it does not represent any loss of content from the document.

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé:

**Dimensionnement GRWA et protection par segment
dans les réseaux optiques WDM**

présenté par:

Alexandre Bouffard

a été évalué par un jury composé des personnes suivantes:

Bernard Gendron,	président-rapporteur
Brigitte Jaumard,	directeur de recherche
Alain C. Houle,	codirecteur
Abdelhakim Hafid,	membre du jury

Mémoire accepté le: 5 décembre 2005

RÉSUMÉ

Chaque minute que dure une panne de service dans un réseau optique de télécommunications occasionne aux grandes entreprises des pertes de revenu substantielles. Lors du dimensionnement de ces réseaux, il est donc impératif de prévoir leur survie aux bris d'équipements pour éviter le maximum de ces pannes. Le coût des équipements d'interconnexion nécessaires pour y arriver constitue également une priorité.

Une métaheuristique a alors été développée pour résoudre conjointement les problèmes GRWA et protection par segment sur les réseaux optiques WDM. L'objectif fixé est celui de minimiser le coût des équipements d'interconnexion nécessaires, lequel est évalué à travers le coût dominant des cartes MSPP. Étant donnée la complexité de ces problèmes, une attention spéciale a été portée pour s'assurer de l'efficacité de la métaheuristique. La comparaison des approches conjointe et séquentielle a permis de démontrer que l'optimisation conjointe réussit à obtenir des solutions à coût moindre que l'optimisation séquentielle.

Mots clés: routage, affectation de longueurs d'onde, groupage de trafic, optimisation combinatoire, métaheuristique, recherche tabou.

ABSTRACT

Every service outage in an optical telecommunications network causes significant revenue losses to major corporations relying on the network for business activities. Therefore, survivability must be a foremost consideration in the network provisioning to ensure that the network will be able to survive as many failures as possible. The cost of interconnection equipment required to protect the network is also a priority.

In response to these concerns, a metaheuristic was developed to solve the joint optimization of the GRWA and segment protection problems on WDM optical networks. The objective of minimizing the cost of interconnection equipment is evaluated through the dominating cost of MSPP cards. Due to the complexity of these problems, special attention was brought to the runtime efficiency of the metaheuristic. The comparison of joint and sequential optimization approaches showed that jointly optimizing both problems gives lower cost solutions than optimizing one problem after the other.

Keywords: WDM optical networks, provisioning, routing, wavelength assignment, grooming, segment protection, combinatorial optimization, metaheuristic, Tabu search.

TABLE DES MATIÈRES

RÉSUMÉ	iii
ABSTRACT	iv
TABLE DES MATIÈRES	v
LISTE DES TABLEAUX	viii
LISTE DES FIGURES	ix
LISTE DES SIGLES	xi
NOTATION	xii
REMERCIEMENTS	xiii
CHAPITRE 1 : INTRODUCTION	1
CHAPITRE 2 : GÉNÉRALITÉS SUR LES RÉSEAUX OPTIQUES	3
2.1 Terminologie	3
2.2 Topologies	4
2.3 Réseaux optiques WDM	6
2.3.1 Multiplexage	6
2.3.2 Plateforme MSPP	7
2.4 Survie des réseaux	11
2.4.1 Protection des réseaux en anneau	11
2.4.2 Protection des réseaux maillés	13
2.5 Problèmes d'optimisation	18
2.5.1 GRWA	18

2.5.2	Protection par segment	20
CHAPITRE 3 : DESCRIPTION DU PROBLÈME		22
3.1	Énoncé	22
3.2	Question de recherche	23
3.3	Objectifs	23
3.4	Hypothèses de travail	24
3.4.1	Hypothèses générales	24
3.4.2	Hypothèses pour la protection	26
CHAPITRE 4 : REVUE DE LA LITTÉRATURE		27
4.1	Problème GRWA	27
4.2	Optimisation conjointe	28
4.2.1	Cas statique	28
4.2.2	Cas dynamique	33
4.3	Résumé	37
CHAPITRE 5 : MÉTAHEURISTIQUE PROPOSÉE		39
5.1	Introduction à la méthode de recherche tabou	39
5.2	Utilitaires	40
5.2.1	Utilitaires pour l'opération	41
5.2.2	Utilitaires pour la protection	44
5.3	Méthode de recherche tabou	46
5.3.1	Mouvements	46
5.3.2	Stratégies	50
5.3.3	Tentatives infructueuses	52
5.4	Réalisation	55
5.4.1	Architecture	55
5.4.2	Programmation dynamique	56

5.4.3	Structures de données	60
CHAPITRE 6 : EXPÉRIMENTATION		63
6.1	Validation	63
6.1.1	Réalisabilité	63
6.1.2	Qualité	64
6.2	Paramètres	66
6.2.1	Réseaux	66
6.2.2	Métaheuristique	67
6.3	Résultats et analyse	68
6.3.1	Comparaison des stratégies	69
6.3.2	Comparaison des approches	71
6.3.3	Performance	75
CHAPITRE 7 : CONCLUSION		80
BIBLIOGRAPHIE		83

LISTE DES TABLEAUX

4.1	Résumé des articles étudiés	38
5.1	Fonction d'évaluation pour le routage des connexions	43
5.2	Fonction d'évaluation de l'algorithme de programmation dynamique	60
6.1	Valeur numérique des paramètres de la métaheuristique	68
6.2	Temps d'exécution de la métaheuristique selon la stratégie	69
6.3	Comparaison du coût (k\$) des approches	72
6.4	Coût (k\$) et amélioration de la solution par la métaheuristique	76

LISTE DES FIGURES

2.1	Réseau en anneau	5
2.2	Regroupement de deux anneaux	5
2.3	Réseau maillé	6
2.4	Équipements d'interconnexion présents au nœud 2	8
2.5	UPSR	12
2.6	BLSR	13
2.7	Protection par connexion	14
2.8	Protection par canal	14
2.9	Partage de la protection	16
2.10	Contingence sur un tronçon longeant le p-Cycle	17
2.11	Contingence sur un tronçon enjambant le p-Cycle	17
2.12	GRWA : solution 1	19
2.13	GRWA : solution 2 - affectation	19
2.14	GRWA : solution 3 - groupage	20
2.15	Protection par segment : solution 1	21
2.16	Protection par segment : solution 2 - partage	21
4.1	Algorithme de programmation dynamique [20]	36
5.1	Fusion de segments suite au retrait d'une protection	46
5.2	Diagramme de classes	55
5.3	Exemple de route pour l'algorithme de programmation dynamique	59
6.1	Topologie de EON	67
6.2	Topologie de NSF	67
6.3	Topologie de EON2004	68
6.4	Évolution du coût (k\$) pour l'optimisation séquentielle	70
6.5	Évolution du coût (k\$) pour l'optimisation conjointe	71

6.6	Évolution du coût (k\$) pour les meilleures stratégies	72
6.7	Répartition des connexions et protections par longueur	73
6.8	Taux de partage des segments de protection	74
6.9	Segments non protégés suite à une rupture de chaque tronçon	75
6.10	Répartition des segments d'opération par capacité occupée	77
6.11	Répartition des ports à chaque nœud	78
6.12	Segments non protégés suite à une rupture de chaque tronçon	79

LISTE DES SIGLES

GRWA	Grooming, Routing and Wavelength Assignment
MSPP	MultiService Provisioning Platform
OADM	Optical Add/Drop Multiplexer
OC	Optical Carrier
RWA	Routing and Wavelength Assignment
STS	Synchronous Transport Signal
WDM	Wavelength Division Multiplexing

NOTATION

- A Critère d'arrêt de la recherche tabou.
- f^{eval} Fonction d'évaluation.
- L_o Pourcentage des connexions dans la liste tabou pour le mouvement *Éliminer un segment d'opération*.
- L_p Pourcentage des segments d'opération dans la liste tabou pour le mouvement *Éliminer un segment de protection*.
- P_o Nombre de mouvements exécutés lors d'une phase dédiée à l'opération.
- P_p Nombre de mouvements exécutés lors d'une phase dédiée à la protection.
- R_o Nombre de routes réalisables à considérer pour l'opération.
- R_p Nombre de routes réalisables à considérer pour la protection.
- S_o Fraction des segments considérés par le mouvement *Éliminer un segment d'opération*.
- S_p Fraction des segments considérés par le mouvement *Éliminer un segment de protection*.

REMERCIEMENTS

Merci d'abord à mon directeur de recherche Madame Brigitte Jaumard, de l'Université de Montréal. Elle a défini le projet de maîtrise puis m'a donné l'opportunité de le réaliser. Merci pour son ouverture à mes idées et merci pour sa disponibilité tout au long du projet pour orienter et corriger mes travaux.

Merci ensuite à mon codirecteur Monsieur Alain C. Houle, de l'Université de Sherbrooke. Il a contribué au projet en partageant sa connaissance des aspects pratiques. Merci pour m'avoir encouragé à choisir l'alternative plus avant-gardiste lorsque j'hésitais entre protection par connexion et par segment.

Merci également aux étudiants suivants : Yannick Solari, Manon Bélanger et Pierre-Marc Fournier. La métaheuristique proposée dans ce mémoire est grandement inspirée des travaux de Yannick, tandis qu'elle repose sur des librairies développées par Manon et Pierre-Marc.

Merci finalement à ma mère Claire Vincent pour avoir participé à la correction de ce mémoire.

CHAPITRE 1

INTRODUCTION

À chaque année, les grandes entreprises américaines perdent plus de 500 millions de dollars en revenu à cause de pannes dans les réseaux optiques de télécommunications [9]. Il est donc essentiel de protéger ces réseaux pour éviter le maximum de pannes. Définissons une *contingence* comme la défaillance de certaines ressources dans un réseau optique. En introduction, nous verrons les principales causes des contingences, les différents types, ainsi que leur impact. À titre de référence, la terminologie est présentée en section 2.1.

Les réseaux optiques sont constitués de nœuds reliés entre eux par des fibres optiques, lesquelles sont souvent enfouies dans le sol. Malgré toutes les mesures prises pour protéger ces fibres, il arrive qu'elles soient rompues lors de travaux d'excavation. Annuellement, on observe en moyenne 8 ruptures de fibres par 1000 km sur les réseaux métropolitains, et 2 ruptures par 1000 km sur les réseaux à grande distance. Ces taux peuvent paraître négligeables mais, sur un réseau à grande distance comportant par exemple 50 000 km de fibres, on parle d'une rupture tous les trois à quatre jours [9].

Les ruptures de fibres représentent la principale cause des contingences sur les réseaux optiques. Mais d'autres événements causent également la défaillance de certaines ressources du réseau. Divers équipements d'interconnexion peuvent cesser de fonctionner, affectant en partie ou en totalité le trafic circulant sur une fibre. Aussi, un nœud entier peut tomber en panne, privant de service tous les clients locaux en plus de paralyser le trafic qui transitait par le nœud.

Divisons les contingences en deux types : simples et multiples.

- Les contingences dites *simples* affectent le trafic sur un seul tronçon. Les ruptures de fibres en font partie, ainsi que les bris d'équipement d'interconnexion qui n'affectent qu'un tronçon. Une connexion peut survivre à une contingence simple en

empruntant une route disjointe du tronçon affecté.

- Les contingences *multiples* affectent le trafic sur plusieurs tronçons. Ce type de contingence comprend la panne de tous les équipements à un nœud. La disponibilité d'une route disjointe ne garantit pas la survie à une contingence multiple.

Un nombre de plus en plus grand d'applications vitales reposent sur le bon fonctionnement des réseaux optiques. On assiste en même temps à une dépendance grandissante de la société envers les télécommunications. En conséquence, les pannes ont un impact majeur sur la clientèle d'un réseau. On estime en effet qu'elles durent en moyenne une dizaine d'heures et occasionnent des pertes de revenu de l'ordre de 100 k\$ par minute [9].

Lors du dimensionnement d'un réseau, il est donc impératif de prévoir sa survie aux contingences afin d'éviter que celles-ci ne résultent en pannes de service. Nous verrons les deux principales stratégies de survie (section 2.4) au chapitre regroupant les notions de base sur les réseaux optiques. Suivront la description du problème traité par ce mémoire (chapitre 3) et une revue de la littérature (chapitre 4). Une métaheuristique sera ensuite proposée au chapitre 5 et le chapitre 6 présentera l'expérimentation effectuée. Finalement, quelques conclusions clôtureront ce mémoire.

CHAPITRE 2

GÉNÉRALITÉS SUR LES RÉSEAUX OPTIQUES

Avant de s'attaquer à la description du problème étudié par ce mémoire (chapitre 3), passons en revue certaines généralités sur les réseaux optiques. À titre de référence, la terminologie est présentée en section 2.1. Suivront la présentation des topologies (section 2.2) et des réseaux optiques WDM (section 2.3). Finalement, la section 2.4 introduira la survie des réseaux, et la section 2.5 décrira deux problèmes d'optimisation.

2.1 Terminologie

Pour les besoins de ce mémoire, la terminologie suivante s'applique.

Canal (channel, link)

Longueur d'onde (λ) sur une fibre.

Chemin (path)

Suite de canaux.

Connexion (connection)

Capacité occupée sur un chemin par une requête.

Dimensionnement (provisioning)

Opération consistant à déterminer et installer sur un réseau les ressources qui lui sont nécessaires pour fonctionner efficacement.

Nœud (node)

Interface entre le client et le réseau optique à travers une plateforme MSPP.

Régénération (regeneration)

Traitement optique-électrique-optique d'un signal par un MSPP.

Requête (request)

Demande de trafic d'une certaine capacité entre une source et une destination.

Routage (routing)

Détermination d'un chemin pour une connexion.

Route (route)

Suite de tronçons.

Segment (regeneration segment, wavelength segment)

Section toute optique d'un chemin bornée par un traitement électrique.

Segment d'opération (working segment)

Segment d'un chemin d'opération.

Segment de protection (protection segment)

Segment d'un chemin de protection.

Topologie (topology)

Représentation schématique des différents nœuds et de leurs liaisons physiques.

Tronçon (span)

Ensemble des canaux reliant deux nœuds voisins. Correspond à une paire de fibres pour un réseau monofibre.

2.2 Topologies

Dans une topologie en anneau, chaque nœud est connecté à ses deux voisins pour former une boucle (figure 2.1).

Généralement, le trafic y circule soit sur une fibre en orientation horaire ou anti-horaire, soit sur deux fibres (chaque connexion empruntant la route la plus courte).

Étant donnée sa simplicité, la topologie en anneau est prédominante dans les réseaux de télécommunications. Mais les dernières années ont vu une expansion rapide des réseaux, de telle sorte qu'il a été nécessaire de regrouper des anneaux pour former des

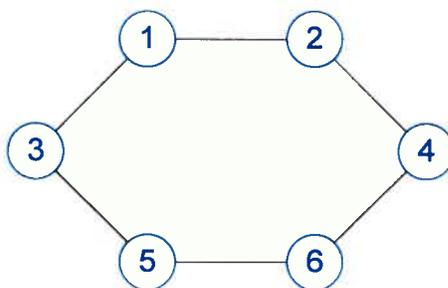


Figure 2.1 – Réseau en anneau

réseaux de plus grande taille. Malheureusement, cette transformation enlève un peu à la simplicité de la topologie en anneau. Prenons par exemple, en figure 2.2, un réseau formé de deux anneaux dans lesquels le trafic circule en orientation horaire. Seul le nœud 6 fait le pont entre les anneaux. Pour se rendre du nœud 5 à 7, on voit que la connexion doit emprunter une route relativement longue.

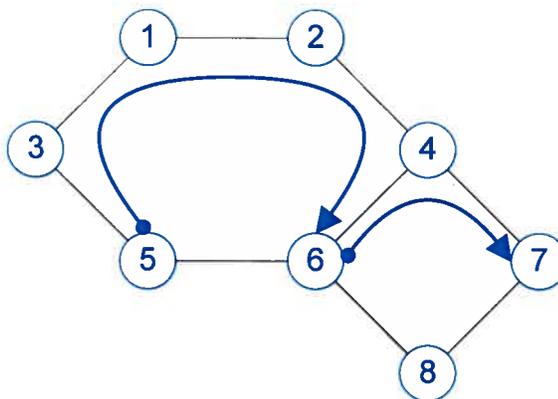


Figure 2.2 – Regroupement de deux anneaux

La topologie maillée, inspirée des réseaux de données, permet quant à elle une meilleure intégration des anneaux. À la base, chaque anneau constitue une maille du réseau auquel on peut ajouter des tronçons supplémentaires pour en augmenter la connectivité. Dans un réseau maillé, le trafic circule sur une route arbitraire qui peut être la plus courte ou toute autre, en fonction de l'objectif à atteindre lors du routage. En se référant à la figure 2.3, on constate que la connexion allant de 5 à 7 profite de la flexibilité

de la topologie maillée pour voyager sur une route plus directe qu'avec la topologie en anneau.

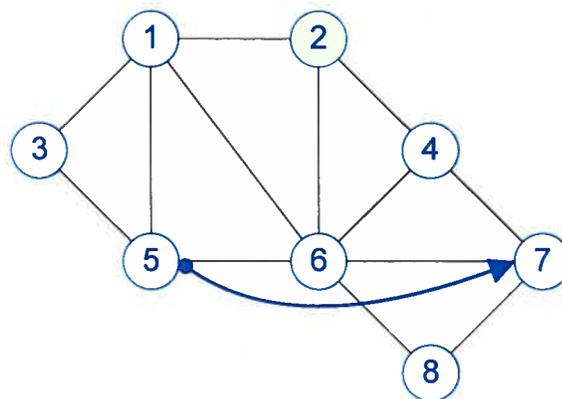


Figure 2.3 – Réseau maillé

Sauf indication contraire, la suite de ce mémoire s'intéresse aux réseaux maillés.

2.3 Réseaux optiques WDM

La présente section est dédiée aux particularités des réseaux optiques WDM. Il sera d'abord question du multiplexage utilisé par de tels réseaux, puis d'une implantation récente : la plateforme MSPP.

2.3.1 Multiplexage

Atout majeur des réseaux optiques modernes, le multiplexage permet de maximiser la capacité transmise sur chaque fibre optique [17]. Nous verrons les deux types de multiplexage utilisés : en longueur d'onde et temporel.

2.3.1.1 Multiplexage en longueur d'onde

Le multiplexage en longueur d'onde ou WDM (Wavelength Division Multiplexing) permet de faire passer plusieurs ondes de longueur d'onde différente sur une même fibre

optique. Présentement, une norme ITU (International Telecommunication Union) définit une grille de 81 longueurs d'onde espacées à intervalle de 50 GHz pour le multiplexage DWDM (Dense WDM). Puisque les équipements modernes peuvent transmettre jusqu'à 10 Gbps par longueur d'onde (canal WDM), le multiplexage en longueur d'onde permet d'atteindre une capacité totale de l'ordre de 1 Tbps sur une seule fibre optique.

On note la capacité de transport d'un canal sous la forme OC- x (Optical Carrier x), x étant un multiple de la capacité de base, qui est environ 50 Mbps. Les deux capacités considérées dans ce mémoire sont OC-48 et OC-192, ou respectivement 2,5 Gbps et 10 Gbps.

2.3.1.2 Multiplexage temporel

Chaque canal transportant une capacité de l'ordre de 10 Gbps gagne aussi à être subdivisé dans le but de grouper plusieurs signaux clients qui, individuellement, atteignent rarement une telle capacité. C'est la norme SONET (Synchronous Optical NETWORKing) qui définit l'implantation du multiplexage temporel [8]. Les signaux clients sont entrelacés et occupent une plus ou moins grande portion de chaque bloc d'une durée normalisée de 125 μ s, en fonction de leur capacité.

La capacité d'un signal client est notée STS- y (Synchronous Transport Signal y). On considère dans ce mémoire les capacités STS-1, 3, 12 et 48, lesquelles vont de 50 Mbps à 2,5 Gbps. La somme des capacités des signaux sur un canal ne peut excéder sa capacité de transport (OC-48 ou OC-192).

À noter que STS-48 et OC-48, par exemple, correspondent à la même capacité (2,5 Gbps). Utiliser des termes différents permet de distinguer la capacité d'un signal client (STS) et la capacité de transport d'un canal WDM (OC).

2.3.2 Plateforme MSPP

Nous étudierons maintenant la plateforme MSPP (MultiService Provisioning Platform) [3]. Il sera d'abord question des équipements d'interconnexion qui réalisent le

multiplexage décrit ci-haut, puis des contraintes imposées par ces équipements sur la détection des pannes.

2.3.2.1 Équipements d'interconnexion

Pour décrire les équipements d'interconnexion présents à un nœud, nous nous référerons à la figure 2.4 qui illustre la situation au nœud 2, voisin de 1, 3 et 4. Afin de simplifier la figure, on omet les fibres allant vers 1 et provenant de 3 et 4.

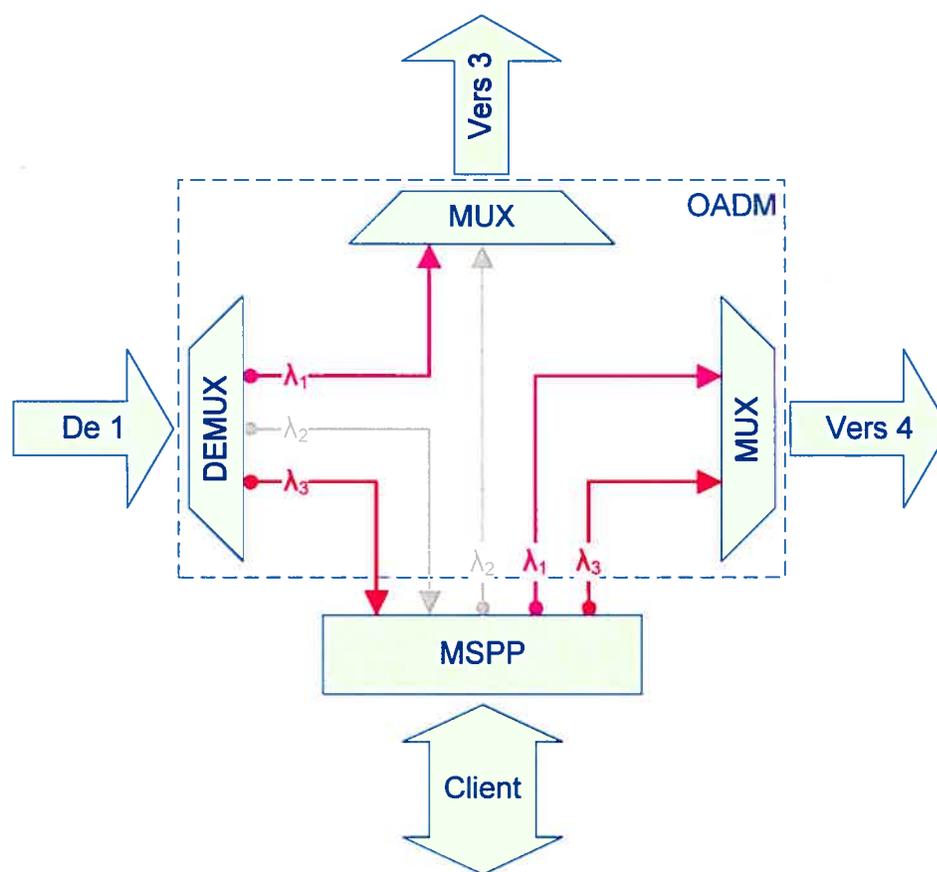


Figure 2.4 – Équipements d'interconnexion présents au nœud 2

Le OADM (Optical Add/Drop Multiplexer) réalise deux tâches :

1. Multiplexage en longueur d'onde. Les démultiplexeurs donnent accès à chaque

longueur d'onde d'une fibre qui entre au nœud, tandis que les multiplexeurs combinent les longueurs d'onde qui partageront la même fibre en sortie.

2. Extraction des longueurs d'onde. Une fois les longueurs d'onde démultiplexées à l'entrée du nœud, certaines sont envoyées directement à un multiplexeur pour quitter le nœud. C'est le cas par exemple de λ_1 qui est dirigée vers le nœud 3. Le trafic dirigé de la sorte devra nécessairement poursuivre sur la même longueur d'onde. Seules les longueurs d'onde qui doivent passer par le MSPP (λ_2 et λ_3) y sont dirigées.

Le MSPP combine les fonctions SOADM (SONET Add/Drop Multiplexer) et DXC (Digital Cross-Connect) pour réaliser le multiplexage temporel. Il fait l'interface entre les clients locaux et le réseau optique. D'un côté, il accepte les connexions des clients. De l'autre côté, chaque longueur d'onde provenant du OADM entre dans un récepteur (port d'entrée) et chaque longueur d'onde quittant vers le OADM est générée par un émetteur (port de sortie).

Cinq situations obligent une longueur d'onde à être dirigée vers le MSPP.

1. Un signal client est destiné au nœud présent. Le MSPP doit alors convertir la longueur d'onde du domaine optique au domaine électrique afin d'en extraire ce signal et le transmettre au client. Les signaux clients qui ne sont pas destinés au nœud sont régénérés vers le domaine optique, puis envoyés au OADM pour continuer vers leur prochaine destination (exemple : λ_2).
2. Un signal client débute au nœud présent et doit être ajouté au trafic de la longueur d'onde. Comme pour la situation précédente, la longueur d'onde doit être convertie au domaine électrique pour que le signal client soit inséré.
3. Le trafic de la longueur d'onde poursuit sa route sur un canal de longueur d'onde différente. Le OADM ne faisant que diriger les longueurs d'onde vers un multiplexeur ou le MSPP, le changement de longueur d'onde est effectué en régénérant le signal (exemple : λ_3 provenant du nœud 1 et λ_1 vers 4).

4. Le trafic de la longueur d'onde est divisé vers plusieurs canaux de sortie. Encore une fois, une régénération est nécessaire pour assembler dans le domaine électrique les signaux clients qui partageront un canal (exemple : λ_3 provenant du nœud 1 et λ_1 et λ_3 vers 4).
5. Le trafic de la longueur d'onde est joint à celui d'une autre longueur d'onde et les deux poursuivent leur route ensemble. Il s'agit du contraire de la situation 4.

On alloue des ports d'entrée ou de sortie à un MSPP en y installant des cartes de transport. Chaque carte comprend un port d'entrée et un port de sortie de même capacité, une carte OC-48 et une carte OC-192 coûtant environ respectivement 4 k\$ et 10 k\$. Pour chaque capacité, le nombre de cartes nécessaires en fonction du nombre de ports est alors le suivant : $\max\{\text{entrée}, \text{sortie}\}$.

À titre d'exemple, évaluons le coût des cartes nécessaires pour réaliser la configuration de la figure 2.4. En supposant que les canaux sur λ_2 sont de capacité OC-48 et que les autres sont de capacité OC-192, il faut d'abord une carte OC-48 pour un port d'entrée et un port de sortie OC-48. Ensuite, on a besoin de deux cartes OC-192 même si un port d'entrée demeurera inutilisé. Le coût total est donc $1 \times 4 \text{ k\$} + 2 \times 10 \text{ k\$} = 24 \text{ k\$}$.

2.3.2.2 Détection des pannes

En pratique, une connexion ne visite pas le MSPP de chaque nœud sur sa route, mais seulement lorsque nécessaire (voir les situations énumérées à la section précédente). Rien n'empêche le contraire mais, dans les réseaux métropolitains, le coût des équipements aux nœuds constitue la majeure partie de l'investissement initial. Régénérer chaque signal à chaque nœud nécessiterait beaucoup trop de cartes.

Par contre, comme il a été expliqué à la section précédente, tout traitement des signaux autre que le multiplexage des canaux par le OADM doit être effectué par le MSPP dans le domaine électrique. Cela comprend l'analyse des signaux pour la détection des pannes.

Ces deux éléments mis ensemble font en sorte que, de façon générale, il n'est pas possible d'analyser une connexion à chaque nœud intermédiaire pour détecter une interruption de service. Il faudra tenir compte de cette contrainte lors de l'exploration des stratégies de survie du réseau.

2.4 Survie des réseaux

Deux stratégies principales permettent la survie d'un réseau à une contingence : la restauration et la protection [9].

La *restauration* consiste à réserver une enveloppe de capacité résiduelle lors du dimensionnement du réseau. Cette capacité est répartie de sorte que, peu importe le lieu de la panne, un chemin alternatif puisse être alloué à chaque connexion affectée. Le fait que le chemin de protection soit évalué suite à la panne pose deux problèmes relatifs à la gestion du réseau. Premièrement, cela augmente le délai de rétablissement. De plus, le client ne peut être informé à l'avance du chemin de protection, ce qui lui donne moins confiance en la survie du réseau.

La *protection*, quant à elle, permet de prévoir à l'avance le chemin alternatif ainsi que de réserver la capacité nécessaire à son établissement. Les prochaines sections décrivent plus en détail cette stratégie qui est au cœur du mémoire. Dans un premier temps, deux schémas de protection des réseaux en anneau sont présentés. Suivront quelques schémas de protection des réseaux maillés (section 2.4.2). Tous les schémas présentés permettent la survie du réseau à une contingence simple.

2.4.1 Protection des réseaux en anneau

Comme on l'a vu en section 2.2, les réseaux en anneau sont très simples à gérer. Par contre, leur protection nécessite plus de capacité que celle des réseaux maillés. En effet, on doit doubler la capacité d'un réseau en anneau pour sa protection. Nous passons ici en revue les deux principaux schémas de protection des réseaux en anneau, soient UPSR

et BLSR.

2.4.1.1 UPSR

Le schéma UPSR (Unidirectional Path-Switched Ring) est dit de configuration 1 + 1. Chaque connexion voyage sur deux routes en même temps, une première fibre circulant l'information en orientation horaire et une seconde en sens anti-horaire. La destination reçoit donc deux signaux, mais ne conserve que celui de meilleure qualité. Ainsi, aucune signalisation n'est nécessaire au moment d'un bris, ce qui donne un court délai de rétablissement de l'ordre de 50 ms.

La figure 2.5 illustre une connexion de 1 vers 4 voyageant simultanément par 2 et 3.

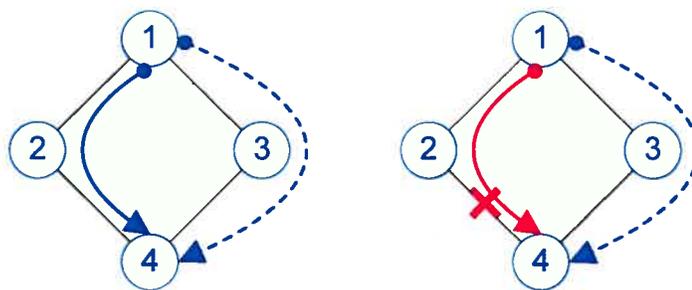


Figure 2.5 – UPSR

Dans le cas d'une contingence au tronçon 2-4, la destination basculera au signal provenant du nœud 3 qui n'est pas affecté par la panne.

2.4.1.2 BLSR

Le schéma BLSR (Bidirectional Line-Switched Ring) est quant à lui appelé de type 1 : 1. En temps normal, deux fibres (une dans chaque orientation) sont utilisées pour router les connexions par la route la plus courte. Lorsque survient un bris à un tronçon, les nœuds voisins signalent la panne puis détournent le trafic vers les deux fibres de protection.

Retournons à l'exemple d'une connexion de 1 vers 4 qui voyage normalement sur la route 1-2-4. Si le tronçon 2-4 tombe en panne sous le schéma BLSR (figure 2.6), le trafic allant de 2 à 4 empruntera la route 2-1-3-4 sur une fibre de protection (trait hachuré). La nouvelle route de la connexion sera alors 1-2-1-3-4.

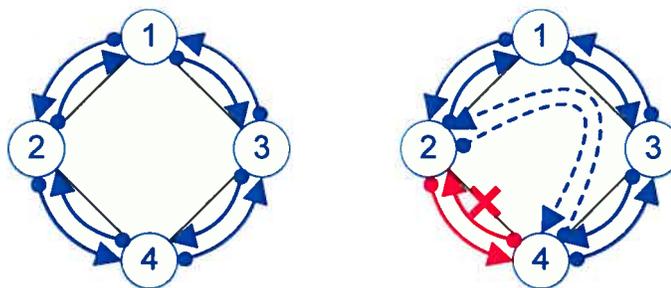


Figure 2.6 – BLSR

2.4.2 Protection des réseaux maillés

La protection des réseaux maillés est généralement plus efficace que celle des réseaux en anneau. D'abord, il est plus facile d'y trouver deux courtes routes disjointes dans un réseau maillé que dans un réseau en anneau, où l'on doit faire le tour d'un côté puis de l'autre. Aussi, le partage des ressources de protection (section 2.4.2.4) est souvent possible grâce à la plus grande connectivité des réseaux maillés.

Nous passerons en revue les principaux schémas de protection, soient la protection par connexion, par canal, par segment, et finalement les p-Cycles.

2.4.2.1 Protection par connexion

La protection par connexion consiste à protéger chaque connexion individuellement. Pour ce faire, en prévision d'une panne, on réserve la capacité de la connexion sur une route disjointe de la route d'opération. La figure 2.7 présente une connexion ayant comme route d'opération 1-2-3 et comme route de protection 1-4-5-3.

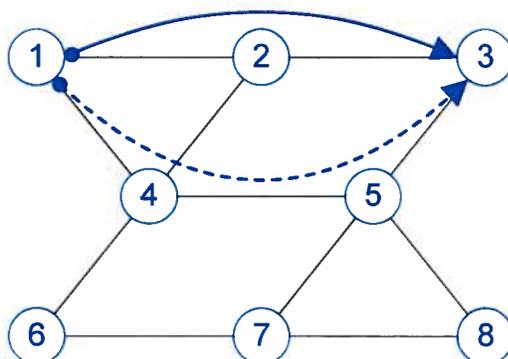


Figure 2.7 – Protection par connexion

Lorsque survient un bris, un signalement est envoyé aux source et destination de chaque connexion affectée afin qu'elles basculent au chemin de protection.

2.4.2.2 Protection par canal

La protection par canal consiste à protéger chaque canal dans son ensemble, peu importe les connexions qui y voyagent. Les deux canaux occupés par la connexion 1-2-3 pourraient être protégés tel qu'illustré en figure 2.8.

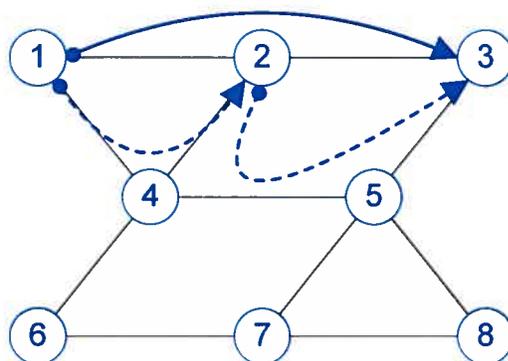


Figure 2.8 – Protection par canal

La connexion aurait alors 1-4-2-3 comme route de protection lors d'une contingence sur le premier tronçon, ou la route 1-2-4-5-3 si la contingence affectait le deuxième tronçon.

Le délai de rétablissement causé par la signalisation est beaucoup plus court que pour la protection par connexion, puisque seulement une paire de nœuds source-destination doit être informée du bris, et non une paire par connexion affectée. De plus, la source et la destination d'un canal ne peuvent être plus éloignées l'une de l'autre que la source et la destination d'une connexion.

Par contre, la protection par canal nécessite plus de capacité additionnelle pour la protection. En comparant les figures 2.7 et 2.8, on voit que la capacité de la connexion doit être réservée sur 5 tronçons pour sa protection par canal au lieu de 3 dans le cas de la protection par connexion.

De plus, le type d'équipements considérés dans ce mémoire pose un problème majeur. La protection par canal n'est simplement pas envisageable avec la plateforme MSPP à moins de régénérer chaque signal à chaque nœud, ce qui est beaucoup trop coûteux (voir section 2.3.2.2).

2.4.2.3 Protection par segment

La protection par segment est une généralisation des deux schémas étudiés précédemment. Chaque chemin à protéger est divisé en une suite de segments, qui peuvent se chevaucher ou non. Une connexion peut par exemple être protégée en un seul segment (protection par connexion), ou encore en un segment par canal (protection par canal).

Cette définition a fait l'objet de plusieurs études, mais les équipements d'interconnexion n'y sont pas souvent pris en compte. Puisque cet aspect est central dans ce mémoire, nous définissons les segments de façon plus stricte. Chaque section toute optique d'un chemin d'opération bornée par un traitement électrique sera appelée segment et devra avoir un chemin de protection disjoint. Ce sont donc les passages par un port MSPP qui définissent le début et la fin de chaque segment.

Plus de détails sur la protection par segment seront donnés en section 2.5.2 lors de la description du problème d'optimisation associé.

2.4.2.4 Partage de la protection

Un concept particulièrement important pour la protection des réseaux maillés est celui du partage de la protection. L'objectif est simple : réduire la capacité nécessaire à la protection. Pour ce faire, on permet que les protections de deux chemins d'opération disjoints partagent une même capacité. Cela est possible seulement si l'on ne considère que les contingences simples.

À titre d'exemple, en figure 2.9, un canal du tronçon 4-5 est partagé entre les protections des routes 1-2-3 et 6-7-5.

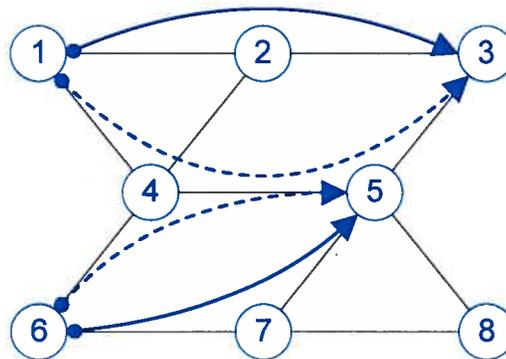


Figure 2.9 – Partage de la protection

Si le premier chemin est affecté par un bris, il utilisera le canal partagé. L'autre chemin fera de même en cas de bris. Mais le cas où ces deux chemins tomberaient en panne simultanément n'est pas couvert par une protection face aux contingences simples. En pratique, le chemin affecté par la première panne s'approprierait d'abord le canal partagé et le second ne pourrait survivre à sa panne. Ou encore, on pourrait établir différents niveaux de qualité de service et la capacité partagée irait à la protection ayant priorité.

2.4.2.5 p-Cycles

Les cycles de protection préconfigurée, appelés p-Cycles, ont été découverts par W.D. Grover et son équipe [10]. Il sont réalisables à différents niveaux, par canal ou

encore par fibre, et protègent les tronçons longeant ou enjambant le cycle.

Un p-Cycle est formé en réservant une unité de protection, par exemple un canal, sur un cycle. La figure 2.10 illustre un p-Cycle en trait hachuré, avec une contingence sur un tronçon longeant le p-Cycle.

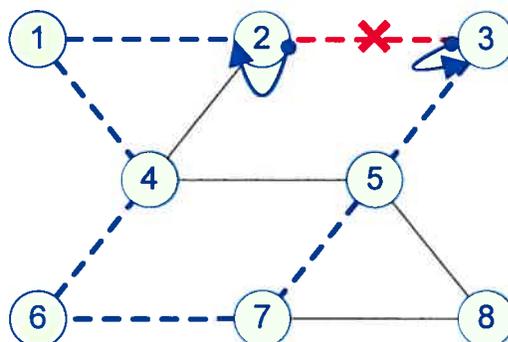


Figure 2.10 – Contingence sur un tronçon longeant le p-Cycle

Chaque canal du p-Cycle protège un canal d'opération sur le même tronçon, à la manière de la protection BLSR (section 2.4.1.2). Si par exemple le tronçon 2-3 tombe en panne, la capacité du p-Cycle sera utilisée pour détourner le trafic.

La protection des tronçons enjambant le cycle constitue le fait saillant des p-Cycles. En se référant à la figure 2.11, on observe que le tronçon 4-5 peut être protégé par le p-Cycle même s'il n'en fait pas partie.

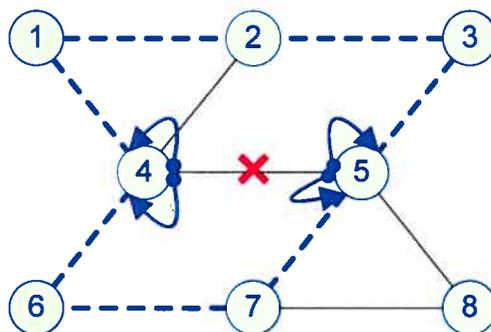


Figure 2.11 – Contingence sur un tronçon enjambant le p-Cycle

De plus, deux canaux peuvent être protégés : un dont la protection emprunterait la

partie supérieure du cycle, puis un second dont la protection passerait par le bas. Certains tronçons peuvent alors être protégés sans même offrir de capacité à la protection, simplement en enjambant suffisamment de p-Cycles.

On voit que les p-Cycles sont apparentés à la protection par canal, et ils en héritent le court délai de rétablissement. Mais malheureusement, ils présentent le même problème étant donné le type d'équipements considérés dans ce mémoire. Comme on l'a vu en section 2.3.2.2, les pannes sont détectées dans le domaine électrique par un port MSPP. Puisque des ports ne sont pas placés à la sortie de chaque canal, il est impossible d'implanter ce schéma de protection dans sa forme la plus simple (protection par canal).

2.5 Problèmes d'optimisation

Après avoir passé en revue les principaux concepts concernant les réseaux optiques, nous sommes en mesure de définir les deux problèmes d'optimisation qui sont au centre de ce mémoire : GRWA et protection par segment.

2.5.1 GRWA

Les paramètres d'entrée du problème GRWA (Grooming, Routing and Wavelength Assignment) sont la description d'un réseau (nœuds, tronçons, nombre de longueurs d'onde) et une matrice de trafic pour chaque capacité de signal client (STS). Pour une capacité donnée, la matrice indique le nombre de requêtes entre chaque paire de nœuds. Remarquons que la matrice n'est généralement ni uniforme ni symétrique.

À partir de ces informations, il s'agit d'allouer un chemin à chaque requête. Par le fait même, cette allocation impose la présence d'équipements d'interconnexion aux nœuds, comme spécifié en section 2.3.2. La capacité occupée sur un canal ne doit pas dépasser la capacité de transport établie par ces équipements.

Plusieurs objectifs peuvent être fixés. Par exemple minimiser le taux de blocage [22], défini comme la capacité totale des requêtes qui ne peuvent être routées par manque de

capacité. On peut aussi associer un revenu à chaque requête et maximiser le revenu [24].

Mais, dans ce mémoire, on s'intéresse aux situations où toutes les requêtes peuvent être routées. L'objectif fixé est celui de minimiser le coût des équipements nécessaires pour y arriver. Dans la littérature, il est assez répandu de relier le coût à la capacité totale utilisée [4] (somme de la capacité utilisée sur chaque canal). Par contre, une fois les fibres optiques enfouies, la capacité disponible est constante et c'est le coût des équipements d'interconnexion qui varie selon le routage. Nous préférons alors minimiser le coût des cartes MSPP.

Pour illustrer l'impact du groupage et de l'affectation de longueurs d'onde sur le coût des cartes, on considère la solution de la figure 2.12 pour les connexions STS-12 suivantes : C_1 de 1 à 2, C_2 de 2 à 3, et C_3 de 1 à 3.

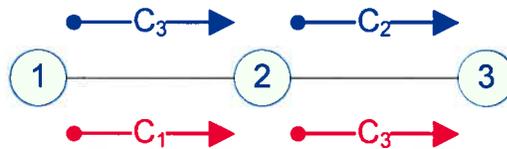


Figure 2.12 – GRWA : solution 1

On voit que C_1 emprunte la longueur d'onde rouge, tandis que C_2 utilise la bleue. La connexion C_3 visite tant qu'à elle le MSPP au nœud 2 pour changer de longueur d'onde. Deux cartes OC-48 sont nécessaires à chaque nœud, pour un total de 6 cartes.

On peut améliorer la solution précédente en plaçant C_2 sur la longueur d'onde rouge (figure 2.13). Cela permet à la connexion C_3 de n'utiliser qu'un segment et d'économiser une carte.

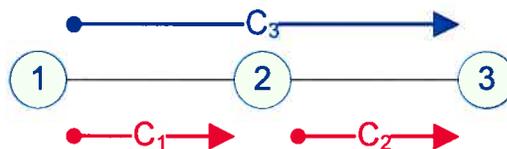


Figure 2.13 – GRWA : solution 2 - affectation

Le groupage des connexions s'avère une solution encore plus intéressante, car les ca-

naux OC-48 ne sont pas utilisés à pleine capacité. Puisque des segments sont nécessaires de 1 à 2 et de 2 à 3 pour C_1 et C_2 , alors aussi bien y grouper C_3 pour économiser deux autres cartes (figure 2.14).

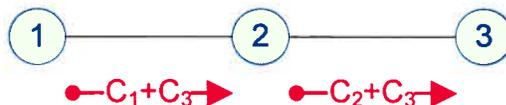


Figure 2.14 – GRWA : solution 3 - groupage

Comme on l'a vu par un exemple assez simple, le groupage et l'affectation de longueurs d'onde influencent significativement le coût des cartes nécessaires. D'autres éléments qui compliquent le problème s'ajoutent à la liste, tels le choix de la route et le fait que plusieurs capacités de transport soient considérées. Mentionnons que le problème GRWA avec l'objectif de minimiser la capacité totale utilisée est NP-complet, puisque le sous-problème RWA a déjà été prouvé NP-complet [2].

2.5.2 Protection par segment

Étant donnée la description d'un réseau et des connexions qui y voyagent, le problème de protection par segment vise à protéger le réseau tel qu'expliqué en section 2.4.2.3 tout en minimisant le coût. De la même façon que pour le problème de GRWA, on définit le coût comme celui des cartes MSPP.

La figure 2.15 illustre deux segments d'opération en trait plein, et leur protection en trait hachuré sur une route disjointe.

La protection par segment ne s'intéresse pas aux connexions qui occupent les segments d'opération. Par exemple, les deux segments illustrés pourraient transporter des connexions allant de 4 à 7 ou bien des connexions de 4 à 5 et d'autres connexions de 5 à 7, le résultat serait le même du point de vue de la protection. À noter que la protection d'un segment peut être constituée d'un ou plusieurs segments de protection.

La figure 2.16 montre comment on peut tirer profit du partage de la protection dans le but de minimiser le coût des cartes.

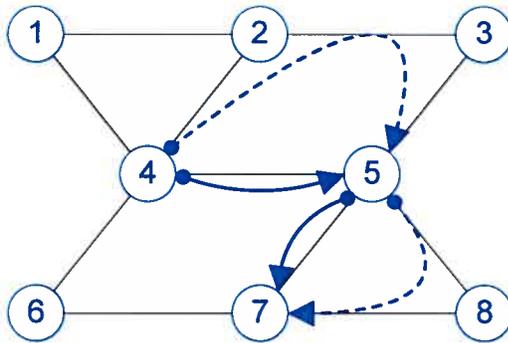


Figure 2.15 – Protection par segment : solution 1

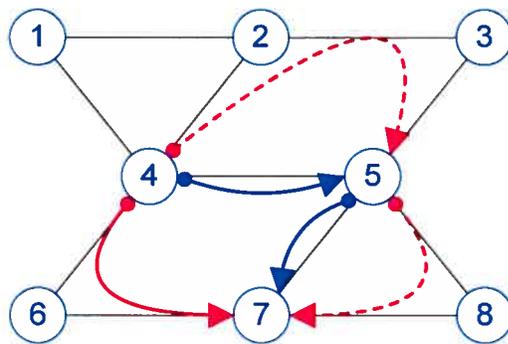


Figure 2.16 – Protection par segment : solution 2 - partage

Un segment d'opération a été ajouté (4-6-7), mais aucune carte additionnelle n'est nécessaire à sa protection. En effet, puisque sa route est disjointe des deux autres segments, sa protection peut partager leurs deux segments de protection.

Tout comme pour GRWA, il a été démontré que le problème de protection avec l'objectif de minimiser la capacité totale utilisée est NP-complet [11].

CHAPITRE 3

DESCRIPTION DU PROBLÈME

3.1 Énoncé

Comme on l'a vu en introduction, la protection d'un réseau optique constitue un aspect essentiel de son dimensionnement. Suite aux travaux de [12] qui traitaient le problème GRWA en minimisant le coût des cartes MSPP, il est alors logique de poursuivre dans la même voie en s'intéressant maintenant à la protection. Quoique la protection des réseaux optiques WDM ait déjà fait l'objet de plusieurs études, c'est l'objectif de minimisation du coût des cartes MSPP qui rend un tel projet innovateur. En effet, les études publiées à ce jour dans le domaine visent plutôt à minimiser la capacité utilisée ou le taux de blocage.

La section 2.4.2 recensait les principaux schémas de protection des réseaux maillés. On y mentionnait que la protection par tronçon et les p-Cycles se prêtent mal à un objectif de minimisation du coût des cartes. Il reste donc à choisir entre la protection par connexion et par segment. Du point de vue de la gestion du réseau, la protection par segment est plus simple à réaliser puisqu'elle fait abstraction des connexions pour se concentrer sur les segments d'opération. Mais pour ce faire, on doit protéger toute la capacité de transport d'un segment, même si celui-ci n'est pas pleinement utilisé. En conséquence, la protection par segment nécessite plus de capacité que la protection par connexion qui protège seulement la capacité de chaque signal client. C'est la protection par segment qui est finalement retenue, car le concept est plus récent et a fait l'objet de moins de recherche.

Un tel problème de protection s'apparente à GRWA de par sa complexité. Ainsi, étant donné qu'il est trop coûteux en temps d'obtenir une solution optimale ou du moins une borne intéressante, on préfère développer une métaheuristique qui obtiendra en quelques

minutes, on l'espère, une solution de qualité.

Le problème s'énonce alors comme suit : *développer une métaheuristique pour le dimensionnement GRWA et la protection par segment dans les réseaux optiques WDM.*

3.2 Question de recherche

Lors du dimensionnement d'un réseau, on doit planifier les chemins d'opération et de protection. La façon la plus simple de procéder est de résoudre d'abord le problème GRWA, et ensuite celui de protection par segment. Mais il serait peut-être intéressant de résoudre les deux problèmes en même temps, en routant les connexions de telle sorte que le coût de protection soit moindre. Cela soulève la question suivante : *est-il avantageux de planifier conjointement les chemins d'opération et de protection ?*

D'une part, l'optimisation conjointe est intrinsèquement plus complexe. Mais de l'autre, si cette complexité est bien gérée, il est à espérer qu'une solution de moindre coût sera obtenue en procédant conjointement. L'hypothèse suivante est alors formulée : *l'optimisation conjointe permet d'obtenir une solution à moindre coût que l'optimisation séquentielle.*

3.3 Objectifs

Pour résoudre le problème énoncé plus haut et vérifier l'hypothèse de recherche, nous nous sommes fixés les trois objectifs suivants.

1. *GRWA et protection par segment.* Avant tout, il faut développer une métaheuristique qui résout conjointement et séquentiellement les problèmes GRWA et protection par segment, ce qui est déjà un défi de taille. Le chapitre 5 sera dédié à la présentation de la métaheuristique proposée. La réalisabilité ainsi que la qualité des solutions obtenues seront validées au cours de l'expérimentation (chapitre 6).
2. *Efficacité de la métaheuristique.* Étant donnée la complexité du problème, une attention particulière doit être portée afin de s'assurer de l'efficacité de la méta-

heuristique. Lors de sa réalisation, il est primordial que les algorithmes aussi bien que les structures de données soient choisies de telle façon à minimiser le temps de calcul. Cela permettra d'obtenir la meilleure solution possible pour un temps d'exécution donné. Cet aspect sera couvert en section 5.4.

3. *Comparaison des deux approches.* Une fois la métaheuristique efficace développée, il sera enfin possible de comparer les approches conjointe et séquentielle. Une portion importante des résultats présentés au chapitre 6 permettra de conclure si l'optimisation conjointe permet ou non d'obtenir une solution à un coût moindre que l'optimisation séquentielle.

3.4 Hypothèses de travail

La présente section énumère les principales hypothèses de travail considérées pour résoudre le problème décrit précédemment. D'abord, les hypothèses qui s'appliquent tant aux chemins d'opération que de protection sont présentées. Suivront les hypothèses de travail spécifiques à la protection.

3.4.1 Hypothèses générales

3.4.1.1 Réseaux bidirectionnels et monofibres

Les réseaux étudiés dans ce mémoire comportent une fibre dans chaque direction entre des nœuds voisins. Par contre, la métaheuristique qui sera proposée pourrait être généralisée aux réseaux avec plus d'une fibre en même direction. En considérant chaque fibre comme un tronçon, il suffirait d'identifier les fibres qui partagent un même conduit et donc les tronçons qui ne sont pas disjoints.

3.4.1.2 Maximum de régénérations permises

Puisque dans un réseau optique l'information voyage à la vitesse de la lumière, le temps de propagation ne constitue pas le facteur dominant du délai de transit. C'est

plutôt le traitement électrique à un nœud qui coûte cher en termes de délai.

Dans le but d'assurer une certaine qualité de service, on limite chaque connexion à deux régénérations, ou encore à trois sauts optiques. On pose aussi le nombre maximum de régénérations d'une protection à deux. Ainsi, une connexion voyagera sur un maximum de trois segments sur son chemin d'opération, et sur un maximum de cinq segments si elle doit emprunter le chemin de protection d'un de ses segments d'opération.

3.4.1.3 Discontinuité de longueur d'onde

Lorsque du trafic visite le MSPP d'un nœud et est ensuite régénéré, aucune contrainte n'est posée sur la longueur d'onde à utiliser. Ceci est en opposition aux travaux précédant ce mémoire [12], où le trafic était contraint à poursuivre sur la même longueur d'onde. La discontinuité était seulement considérée en post-optimisation, ce qui ne permettait pas d'exploiter pleinement la possibilité de changer de longueur d'onde suite à une régénération.

3.4.1.4 Chemins élémentaires

Aucune contrainte n'est posée sur le chemin d'une connexion ou protection, mais on contraint les segments aux chemins élémentaires (qui ne visitent aucun nœud à deux reprises). Puisqu'un segment voyage uniquement dans le domaine optique, un segment qui boucle n'apporte aucun avantage tandis qu'il requiert plus de capacité.

3.4.1.5 Flots non bifurqués

Toute la capacité d'une connexion ou d'une protection doit utiliser le même chemin. Autrement dit, il est interdit qu'une connexion ou une protection bifurque à un nœud vers plusieurs canaux.

3.4.2 Hypothèses pour la protection

3.4.2.1 Topologies biconnexes

Il existe au moins deux routes disjointes entre chaque paire de nœuds.

3.4.2.2 Protection disjointe par tronçon

Puisque seulement les contingences simples sont considérées, la protection n'est pas conçue pour survivre à une panne à un nœud. En conséquence, une protection peut visiter sans problème un même nœud que le chemin d'opération, en autant que les deux routes soient disjointes par tronçon.

3.4.2.3 Partage permis

Le partage d'un segment de protection entre les protections de segments disjointes est permis.

3.4.2.4 Groupage interdit

Il est interdit de grouper les protections. Par exemple, les protections de deux segments OC-48 ne peuvent être combinées sur un segment de protection OC-192. Le partage constitue la seule façon pour plusieurs protections d'utiliser un même segment.

3.4.2.5 Cartes distinctes

Lors du calcul du nombre de cartes requises à un nœud ($\max\{\text{entrée}, \text{sortie}\}$), on évalue distinctement les cartes d'opération et de protection. En pratique, les équipements de protection sont physiquement séparés des équipements d'opération. En conséquence, on ne permet pas qu'une carte fournisse un port à l'opération et l'autre à la protection.

CHAPITRE 4

REVUE DE LA LITTÉRATURE

Avant de décrire la métaheuristique proposée (chapitre 5), on passe en revue les travaux récents les plus pertinents. Les articles étudiés sont divisés selon qu'ils couvrent uniquement le problème GRWA (section 4.1) ou encore le problème d'optimisation conjointe (section 4.2). Un résumé de ces articles clôturera le chapitre en section 4.3.

4.1 Problème GRWA

Le premier article étudié dans le cadre de cette revue de la littérature ne couvre pas la protection, mais demeure tout de même un des plus pertinents. Contrairement à la majorité des travaux publiés dans le domaine, celui des auteurs Jaumard, Solari et Houle [12] traite le problème GRWA avec la même fonction objectif que le présent mémoire, c'est-à-dire minimiser le coût des cartes MSPP.

Parmi les autres similarités entre l'article et ce mémoire, on note les suivantes :

- les segments peuvent être de capacité OC-48 ou OC-192 ;
- une contrainte est imposée sur le nombre maximum de régénérations pour une connexion ;
- les mêmes réseaux maillés et matrices de trafic sont considérés.

Tant de ressemblances, mais surtout au niveau de la fonction objectif, font en sorte que la démarche empruntée par les auteurs est une excellente référence. Les caractéristiques suivantes de leur résolution du problème seront réintroduites plus tard dans ce mémoire (section 5.3).

Une métaheuristique de recherche tabou est proposée. La solution initiale est obtenue en routant les connexions par le plus court chemin possible sur des segments de plus grande capacité possible. Par la suite, les deux mouvements considérés sont le déplacement d'une connexion et le retrait d'un port pour déplacer toutes les connexions qui y

transitaient.

Les résultats obtenus pour les réseaux en anneau ne seront pas discutés ici. Pour ce qui est des réseaux maillés, l'un ou l'autre des mouvements proposés permet d'améliorer significativement la solution initiale. Mais une amélioration de l'ordre de la somme des améliorations pour chaque mouvement est obtenue en utilisant une stratégie qui tire profit des deux mouvements, ce qui démontre l'intérêt de développer une bonne stratégie qui combine plusieurs mouvements.

4.2 Optimisation conjointe

La présente section passe en revue les travaux des dernières années concernant l'optimisation conjointe de l'opération et de la protection. Les problèmes GRWA ou RWA sont abordés pour l'opération, tandis que la protection est effectuée par segment ou par connexion. Les articles étudiés sont présentés selon qu'ils traitent le cas statique (prochaine section) ou dynamique (section suivante).

4.2.1 Cas statique

4.2.1.1 W. Yao et B. Ramamurthy

Deux articles récents de W. Yao et B. Ramamurthy sont parmi les plus pertinents, étant donné l'objectif de ce mémoire. Ils font état du travail réalisé pour résoudre l'optimisation conjointe de l'opération (GRWA plus précisément) et de la protection, dans le cas statique. Les deux articles traitent le problème de manière similaire, à l'exception du type de protection. Tandis que le premier étudie la protection par connexion [22], le second explore la protection par segment [23].

Ces articles considèrent les contraintes SRLG (*Shared Risk Link Group*), ou groupe de liens partageant un risque. Au minimum, une protection doit emprunter une route disjointe de ce qu'elle protège. Mais en pratique, il peut arriver que plusieurs fibres soient enfouies dans un même conduit, ou encore qu'un ensemble de conduits d'une même

région partagent un risque de rupture suite à un tremblement de terre. Les contraintes SRLG sont donc plus générales, puisqu'elles permettent d'identifier les groupes de liens qui partagent un risque. Sous ces contraintes, l'opération et la protection doivent être disjointes quant aux risques, et une protection ne peut être partagée par des chemins d'opération qui ont un risque en commun.

Brièvement, voici quelques autres caractéristiques du problème abordé :

- l'objectif est de minimiser le taux de blocage ;
- des contraintes donnent la quantité de paires émetteur-récepteur à chaque nœud ;
- les flots bifurqués sont interdits ;
- les segments empruntés par une connexion ou une protection peuvent être de longueur d'onde différente, mais aucune conversion n'est permise à l'intérieur d'un segment ;
- deux scénarios sont envisagés : avec ou sans partage de la protection.

Les auteurs proposent des formulations avec des programmes en nombres entiers mais, en raison de leur trop grande complexité, on s'attarde ici aux heuristiques. Ces dernières sont au nombre de trois et sont décrites ci-dessous.

1. SGA (*Separated Grooming Algorithm*) établit d'abord les segments pour ensuite y placer le maximum de connexions et/ou de protections. D'un point de vue opérationnel, cette approche correspond à une gestion du routage en deux couches.
2. IGA (*Integrated Grooming Algorithm*) traite les connexions une par une, en mettant en place les segments au fur à mesure. Ici, la gestion des segments et des connexions est intégrée.
3. TSGA (*Tabu Search Grooming Algorithm*) débute avec une solution générée par SGA ou IGA et tente de l'améliorer à l'aide d'une méthode de recherche tabou. L'ajout ou le retrait d'une connexion constitue le mouvement utilisé. Le nombre de fois qu'une connexion a été déplacée est inclus comme pénalité dans la fonction d'évaluation d'un mouvement, ce qui agit comme technique de diversification.

Les résultats obtenus pour les programmes en nombres entiers ne sont pas discutés ici, puisque limités aux réseaux de très petite taille. Par contre, les heuristiques ont été exécutées sur un réseau de plus grande taille, soient 24 nœuds et 2208 connexions.

Pour la protection par connexion, IGA donne un meilleur rendement que SGA. En effet, il accommode 50 % plus de connexions sans partage de la protection, et 15 % avec partage. Il est à noter que lorsque le nombre de longueurs d'onde augmente, le taux de blocage pour les deux heuristiques tend vers 0 et ainsi l'écart de performance diminue. Finalement, avec ou sans partage, TSGA est environ 5 % meilleur que IGA.

De façon générale, les résultats pour la protection par segment vont dans le même sens. Mais il est intéressant de comparer les deux types de protection entre eux. Avec la protection par connexion, TSGA nécessite 40 % moins de longueurs d'onde pour atteindre un taux de blocage nul. Les auteurs avaient prévu cet avantage puisqu'ils mentionnent que la protection par segment simplifie le signalement des pannes et raccourcit le délai de rétablissement, tandis que la protection par connexion est plus flexible et nécessite moins de ressources.

4.2.1.2 J. Fang et A.K. Somani

Alors que les articles présentés à la section 4.2.1.1 traitent conjointement les problèmes GRWA et protection par connexion/segment dans le but de minimiser le taux de blocage, J. Fang et A.K. Somani les abordent avec comme objectif de minimiser la capacité utilisée [4]. Voici quelques autres différences relatives à la description du problème :

- les contraintes SRLG ne sont pas considérées, l'opération et la protection doivent simplement être disjointes quant aux tronçons ;
- aucune contrainte n'est imposée sur les équipements ;
- les connexions et protections doivent voyager sur la même longueur d'onde d'un bout à l'autre.

La principale contribution de l'article est l'élaboration d'un programme en nombres entiers. Par contre, aucune heuristique n'est proposée. L'expérimentation a donc été ef-

fectuée sur de petits graphes, avec une matrice de trafic limitée à quelques dizaines de connexions.

4.2.1.3 X. Yang, L. Shen et B. Ramamurthy

Contrairement aux autres travaux étudiés pour le cas statique, lesquels traitent le problème GRWA, ceux de X. Yang, L. Shen et B. Ramamurthy se limitent au problème RWA. Tout de même, il est intéressant d'en faire mention car ils mettent l'accent sur les équipements d'interconnexion, autant au niveau des contraintes que de l'objectif.

Un premier article, paru en 2003, introduit la contrainte de longueur maximale d'un chemin, dans le but de donner une certaine qualité de service [19]. Les contraintes SRLG telles que décrites en section 4.2.1.1 sont aussi considérées. Deux objectifs sont abordés : maximiser le profit (chaque requête a un revenu potentiel), ou minimiser la capacité utilisée.

On se concentrera plutôt sur un deuxième article, paru en 2005, qui donne une place centrale aux équipements d'interconnexion [21].

Les auteurs mentionnent que par rapport aux réseaux opaques, où la régénération a lieu sur chaque longueur d'onde à chaque nœud, les réseaux translucides permettent d'économiser près de 80 % des coûts de régénération en utilisant des équipements de régénération seulement là où nécessaire. Par le fait même, le problème se complexifie puisqu'on doit déterminer l'emplacement de ces équipements. L'objectif du problème présenté dans l'article est alors de minimiser la quantité de modules de régénération. Minimiser la capacité utilisée fait office d'objectif secondaire en cas d'égalité.

Relativement aux équipements d'interconnexion, deux contraintes linéaires de qualité de signal sont imposées à chaque segment :

1. dispersion des modes de polarisation (PMD) ;
2. bruit causé par l'émission spontanée amplifiée (ESA noise).

Suivent quelques autres contraintes du problème abordé.

- Aucune conversion n'est permise à l'intérieur d'un segment.
- L'opération et la protection doivent être disjointes quant aux tronçons.
- Les bris aux nœuds ne sont pas considérés. Il est donc possible de partager un module de régénération entre un segment d'opération et sa protection, ou encore entre plusieurs protections.
- Le partage de la capacité d'un segment de protection est aussi permis.

Encore une fois, on s'intéresse aux heuristiques proposées plutôt qu'à la formulation avec un programme en nombres entiers. La solution initiale est obtenue en traitant les requêtes selon l'ordre décroissant de plus courte route. Pour chaque requête, les K plus courtes routes sont évaluées jusqu'à ce qu'une route réalisable soit trouvée. Puis, la protection est calculée par la même procédure. La fonction d'évaluation d'une route tient compte de la quantité de modules de régénération et de longueurs d'onde disponibles.

Une heuristique de recherche locale a été développée. Elle consiste essentiellement à reconfigurer une connexion après l'autre, en choisissant celle qui améliore le plus la fonction objectif, jusqu'à ce qu'un optimum local soit atteint.

Finalement, une méthode de recherche tabou est élaborée. Elle se base sur la recherche locale, mais avec l'ajout d'une liste tabou et de mesures pour en améliorer la performance. Pour faciliter la diversification, le nombre de fois qu'une connexion a été reconfigurée est inclus comme pénalité dans la fonction d'évaluation d'un mouvement. Aussi, le paramètre K varie dynamiquement pour accroître la rapidité de la recherche. Lorsque la solution stagne, K est incrémenté mais il est divisé par deux suite à un mouvement qui améliore la solution.

Les résultats obtenus sur un réseau de 24 nœuds avec 170 connexions et 8, 16 ou 32 longueurs d'onde démontrent que la méthode de recherche tabou améliore d'environ 5 % la meilleure solution trouvée par la recherche locale. En plus, grâce à la variation dynamique du paramètre K , la méthode de recherche tabou a besoin de 200 secondes pour dépasser en qualité la recherche locale qui prend 2000 secondes à exécuter. Un autre résultat intéressant nous indique que plus de 60 % des modules de régénération et

30 % de la capacité sont partagés.

4.2.2 Cas dynamique

4.2.2.1 C. Ou, J. Zhang, H. Zang, L. H. Sahasrabuddhe et B. Mukherjee

Deux articles, parus en 2003, abordent l'optimisation conjointe de l'opération et de la protection par connexion dans l'objectif de minimiser le taux de blocage.

Un premier article s'attarde au problème de trouver deux chemins disjoints de bonne qualité tout en évitant les impasses, dans le cadre d'un RWA pour l'opération [15]. Par impasse, on entend une situation où il est impossible de trouver un chemin de protection en raison du choix de l'ensemble de l'opération. Les auteurs observent que trop souvent on sélectionne quelques chemins d'opération candidats pour ensuite déterminer le chemin de protection, mais que cette technique n'évite pas efficacement les impasses. Ils proposent alors un algorithme d'optimisation conjointe, qui réévalue en boucle la protection étant donnée l'opération, puis l'opération étant donnée la protection, jusqu'à obtenir un optimum local pour la paire de chemins. En pratique, ils observent une amélioration significative du taux de blocage pour les topologies favorables aux impasses, mais qui est compensée par des chemins plus longs en moyenne.

Un second article se concentre sur le problème GRWA pour l'opération, avec l'hypothèse de travail que la conversion est possible à tous les nœuds [16]. Par contre, la quantité de modules de régénération est limitée. L'intérêt principal de cet article vient du fait qu'il compare plusieurs approches, en faisant varier certains paramètres du problème.

Trois schémas de protection sont définis.

1. PAL (Protection-At-Lightpath level). Ce schéma est semblable à la protection par segment décrite en section 2.4.2.3, à deux différences près. D'abord, seulement le bris des fibres est considéré. Les modules de régénération pour les segments d'opération peuvent alors être réutilisés pour la protection. De plus, la commu-

tation des longueurs d'onde peut se faire en temps réel aux nœuds. Aucun équipement de régénération n'est donc nécessaire pour partager une longueur d'onde entre plusieurs protections. Ces deux différences mises ensemble font en sorte que la protection ne requière aucun module de régénération.

2. MPAC (Mixed Protection-At-Connection level). À chaque connexion sont associés des chemins d'opération et de protection disjoints, chacun traversant une série de segments. La capacité d'un segment peut servir à la fois à l'opération et à la protection.
3. SPAC (Separate Protection-At-Connection level). À la différence de MPAC, le chemin de protection traverse une série de segments d'un seul tronçon de longueur. Ces segments sont réservés exclusivement à la protection. Ils sont de longueur unitaire puisque généralement les protections qui les empruntent ne parcourent pas le même chemin.

De façon qualitative, on observe que, puisque PAL ne nécessite pas de modules de régénération pour la protection, ce schéma compense une faible efficacité en capacité par une plus petite utilisation des modules. Aussi, PAL est plus facile à implanter et à gérer en pratique, car l'information sur les connexions n'est plus nécessaire une fois que les segments sont établis. D'un autre côté, SPAC offre de meilleures opportunités de partage de la protection grâce à la petite taille des segments. Par contre, cet avantage s'accompagne d'un plus grand nombre de modules nécessaires.

Après avoir développé des heuristiques associées aux trois schémas de protection, les auteurs effectuent des expériences quantitatives en faisant varier le nombre de modules de régénération. Ils concluent que SPAC a le plus petit taux de blocage lorsqu'il y a suffisamment de modules, tandis que PAL donne de meilleurs résultats lorsqu'il y en a peu ou moyennement.

Une autre expérience fait varier le nombre de plus courtes routes K . Des résultats intéressants sont obtenus pour PAL, dont le rendement diminue lorsque K augmente. La raison est que l'heuristique privilégie la réutilisation de segments existants. Alors

plus K est grand, plus il est probable qu'une très longue route soit choisie parce qu'elle ne nécessite l'ajout d'aucun segment à ce moment. Mais après le routage de plusieurs connexions, l'effet pourrait être négatif si une trop grande capacité était inutilement allouée, ce qui augmenterait la fréquence des blocages.

4.2.2.2 D. Xu, Y. Xiong et C. Qiao

Les auteurs D. Xu, Y. Xiong et C. Qiao s'intéressent au problème de protection par segment, avec la particularité que les segments sont non pas dictés par les contraintes du problème telle la régénération, mais plutôt par l'algorithme. Le découpage d'une connexion en segments se fait alors au moment de sa protection en fonction de l'objectif, lequel est de minimiser la capacité utilisée.

L'optimisation s'effectue dans le cadre d'un trafic additif, c'est-à-dire où les connexions sont mises en place l'une après l'autre pour y rester jusqu'à la fin de la simulation. Aussi, les connexions sont groupées sur une seule longueur d'onde par fibre. Il ne s'agit donc pas d'un problème de type RWA ou GRWA, mais simplement d'un routage.

Leur approche innovatrice, nommée PROMISE (PROtection using Multiple SEgments) [20], vise par sa flexibilité à utiliser la capacité plus efficacement que les autres approches, lesquelles imposent une certaine structure aux segments. Certaines approches vont en fixer la longueur, tandis que d'autres requièrent que les segments ne se chevauchent pas. Le but est donc de se rapprocher le plus possible des performances de la protection par connexion, tout en offrant un plus court délai de rétablissement, puisque celui-ci dépend entre autres de la longueur du chemin de protection.

Puisque l'optimisation conjointe du chemin d'opération puis de la protection est trop coûteuse, l'algorithme proposé traite les deux problèmes séquentiellement, mais non sans prévoir la protection lors de l'établissement de l'opération.

1. Le chemin à plus faible coût est d'abord sélectionné pour l'opération. Le calcul du coût comprend le coût potentiel de la protection, ce qui donne en pratique de meilleurs résultats sur un ensemble de requêtes qu'un programme en nombres en-

tiers qui choisirait la paire opération-protection optimale pour une requête donnée.

2. La connexion retenue est ensuite découpée en segments protégés de façon à user le plus efficacement du partage et ainsi minimiser la capacité supplémentaire requise pour la protection.

Pour exécuter la deuxième étape, un programme en nombres entiers est proposé. Mais étant donnée sa complexité exponentielle, l'article présente également un algorithme de programmation dynamique illustré en figure 4.1.

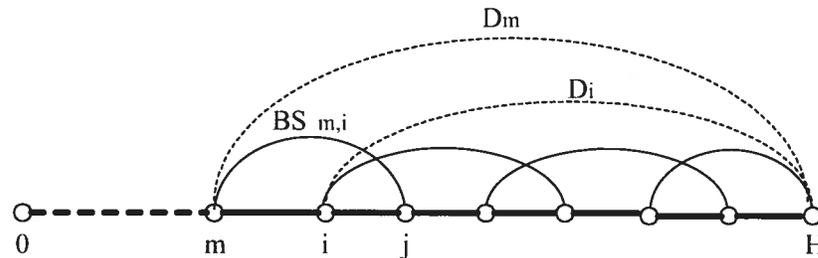


Figure 4.1 – Algorithme de programmation dynamique [20]

Le problème D_m correspond à protéger la connexion entre les nœuds m et H , D_0 étant le problème à résoudre. L'algorithme évalue toujours la protection par le plus court chemin réalisable. Il choisit l'option la moins coûteuse entre protéger l'intervalle de m à H comme un seul segment, ou protéger d'abord de m jusqu'à i et réutiliser la solution au sous problème D_i , pour tout i entre m et H .

Deux principales métriques permettent de comparer des approches entre elles, en expérimentant avec quelques centaines de requêtes aléatoires sur des réseaux de taille moyenne. Premièrement, en mesurant la capacité nécessaire à la protection, PROMISE atteint la performance des meilleurs schémas de protection par connexion. Ensuite, en se basant sur la longueur moyenne du chemin de protection, l'approche proposée réduit le délai de rétablissement par rapport aux autres approches de protection par segment existantes.

On peut donc conclure que PROMISE donne de très bons résultats étant donné le

problème étudié. La programmation dynamique appliquée à ce problème est innovatrice, le concept sera réutilisé dans la métaheuristique proposée (section 5.4.2).

4.3 Résumé

Le tableau 4.1 résume les articles jugés les plus pertinents au moment de la rédaction de ce mémoire. Pour chaque article, l'information suivante est présentée : la référence, les problèmes considérés pour l'opération et la protection, si le cas statique est étudié, si des formulations avec des programmes en nombres entiers ou si des heuristiques sont proposées, si des contraintes relatives aux équipements sont considérées, et l'objectif d'optimisation.

De plus, on retrouve en dernière ligne les éléments souhaités pour résoudre le problème qui nous intéresse (chapitre 3). D'un coup d'œil, on observe que chacun de ces éléments se retrouve dans un article ou un autre, mais qu'aucun article ne les traite tous en même temps. Cela permet de souligner la pertinence de ce mémoire, car il innove dans la combinaison des aspects étudiés (problèmes GRWA et protection par segment avec objectif de minimiser le coût des cartes MSPP). Mais en même temps, puisque ces aspects ont déjà été traités séparément, il est intéressant de puiser dans ces travaux pour en retirer les idées intéressantes, comme la métaheuristique proposée dans [12] et l'algorithme de programmation dynamique dans [20].

Article	Opération	Protection	Statique	PNE	Heuristique	Contraintes	Objectif
Jaumard et al. [12]	GRWA		✓		✓	régénérations	cartes MSPP
Yao et Ramamurthy [22]	GRWA	connexion	✓	✓	✓	modules OEO	blocage
Yao et Ramamurthy [23]	GRWA	segment	✓	✓	✓	modules OEO	blocage
Fang et Somani [4]	GRWA	connexion	✓	✓			capacité
Shen et al. [19]	RWA	connexion	✓	✓	✓	longueur des chemins	capacité, blocage
Yang et al. [21]	RWA	connexion	✓	✓	✓	qualité du signal	modules OEO
Ou et al. [15]	RWA	connexion			✓		blocage
Ou et al. [16]	GRWA	connexion			✓	modules OEO	blocage
Xu et al. [20]	R	segment		✓	✓		capacité
Souhaité	GRWA	segment	✓		✓	régénérations	cartes MSPP

Tableau 4.1 – Résumé des articles étudiés

CHAPITRE 5

MÉTAHEURISTIQUE PROPOSÉE

La métaheuristique proposée étant de type recherche tabou, la première section du chapitre introduit les concepts fondamentaux de cette méthode. Pour être ensuite en mesure de décrire la stratégie et les mouvements employés par la métaheuristique (section 5.3), nous étudierons en section 5.2 les utilitaires qui en sont les éléments d'assemblage. Finalement, nous nous intéresserons en section 5.4 aux principaux aspects de la réalisation de la métaheuristique qui lui donnent son efficacité.

5.1 Introduction à la méthode de recherche tabou

La méthode de recherche tabou, introduite par F. Glover [6, 7], est une métaheuristique d'optimisation de type recherche locale. Étant donné un vaste espace de solutions, ces métaheuristicques fonctionnent en se déplaçant itérativement d'optimum local en optimum local voisin.

On appelle *mouvement* l'opération effectuée sur une solution pour passer à la suivante. La nature du mouvement définit la relation de voisinage. Par exemple, dans le cadre du problème qui nous intéresse, un mouvement pourrait être de modifier le chemin d'une protection. Toutes les solutions atteignables à partir de la solution courante par l'application de ce mouvement en seraient voisines. Il est possible de varier la taille du voisinage (méthode VNS ou Variable Neighborhood Search [14]), pour obtenir le compromis désiré entre la qualité de la solution et le temps de calcul.

La recherche se poursuit jusqu'à ce que le critère d'arrêt soit rencontré, lequel peut être par exemple un nombre fixe d'itérations, ou encore un nombre d'itérations sans amélioration de la meilleure solution. La méthode de recherche tabou de base n'est constituée que d'un seul type de mouvement. Par contre, plusieurs mouvements peuvent aussi être envisagés. Il faut alors développer une *stratégie* qui dictera leur séquençement et le choix

de l'élément de la solution sur lequel les utiliser.

Lorsqu'un mouvement est appliqué, on se déplace vers la solution voisine améliorant le plus la fonction d'évaluation, ou la détériorant le moins si aucune ne l'améliore. Le danger est donc bien réel de toujours retomber sur les mêmes solutions et ainsi de ne pas se sortir des optima locaux. Pour y remédier, on garde en mémoire dans une file, appelée liste tabou, les dernières solutions visitées. Principale caractéristique de la méthode de recherche tabou, il est alors interdit de revisiter une solution tant qu'elle se retrouve dans la liste. La taille de la liste est un paramètre important, à déterminer expérimentalement. Une liste trop courte ne remplit pas son mandat, tandis qu'une liste trop longue contraint trop l'exploration de l'espace des solutions.

Le défi de la méthode de recherche tabou consiste à caractériser une solution pour déterminer ce qui pourrait être amélioré et de quelle façon. Ce défi nous mène à renforcer continuellement notre compréhension du problème pour en arriver à une stratégie performante, et constitue la principale raison pour avoir choisi ce type de métaheuristique. Aussi, parmi la panoplie de métaheursistiques disponibles aujourd'hui [18], R.C. Marett et M.B. Wright montrent que la méthode de recherche tabou donne de très bons résultats pour des problèmes combinatoires complexes [13].

5.2 Utilitaires

Dans un premier temps, les utilitaires concernant l'opération seront présentés. Suivront ceux relatifs à la protection. La plupart de ces utilitaires supposent qu'il existe un algorithme évaluant, pour une route donnée, la séquence de longueurs d'onde à fonction d'évaluation (f^{eval}) minimum. On réserve la description de cet algorithme pour la section 5.4.2.

5.2.1 Utilitaires pour l'opération

5.2.1.1 Router une connexion

L'utilitaire *Router une connexion* détermine le chemin à f^{eval} minimum sur lequel placer une connexion, de sa source à sa destination. Il prend comme paramètre le nombre de routes réalisables à considérer (noté R_o).

Soit la liste des routes reliant la source de la connexion à sa destination, triées en ordre croissant de leur longueur (nombre de tronçons). Pour limiter le temps de calcul, on se restreint aux routes qui ont au plus 4 tronçons de plus que la route la plus courte. On a préalablement retiré de la liste toutes les routes qui n'ont pas de route disjointe dans la liste, dans le but d'éviter l'impasse au moment de la protection.

L'utilitaire traverse cette liste et mémorise le chemin avec le plus petit f^{eval} . Lorsque le meilleur chemin sur la route courante donne un f^{eval} plus petit que celui en banque, il le détrône comme meilleur chemin jusqu'à date. Ainsi, en cas d'égalité de fonction d'évaluation, le plus court chemin est retenu. La recherche se termine lorsque R_o routes donnant au moins un chemin réalisable ont été considérées, ou lorsque la liste est épuisée.

Il reste finalement à définir le calcul de la fonction d'évaluation sur un chemin. Intuitivement, on pourrait le définir comme le coût des cartes nécessaires à l'établissement de la connexion sur le chemin. En posant qu'un port coûte la moitié d'une carte aux fins du calcul, le coût des ports pourrait ensuite départager les égalités.

Malheureusement, ce calcul pose problème. Prenons le coût unitaire des cartes tel que défini auparavant (4 k\$ pour OC-48 et 10 k\$ pour OC-192), et considérons d'augmenter la capacité d'un segment au-delà de OC-48. On remarque qu'il est moins coûteux de déboursier 8 k\$ pour ajouter une paire de cartes OC-48 et ainsi créer un nouveau segment que de remplacer les cartes OC-48 par des OC-192 (une différence de 12 k\$). Quoiqu'optimal sur le fait, le choix de la première option pourrait avoir des conséquences négatives après avoir routé plusieurs connexions. Par exemple, on pourrait se

retrouver avec 4 paires de cartes OC-48 (32 k\$) au lieu d'une seule paire de cartes OC-192 (20 k\$) car, à court terme, il n'aurait jamais été avantageux d'augmenter la capacité d'un segment.

Pour remédier à la situation, deux visions sont proposées : vision locale et vision globale. La vision locale représente le calcul suggéré ci-haut, c'est-à-dire le coût réel des cartes, puis des ports s'il y a égalité.

La vision globale, quant à elle, permet d'espérer obtenir un plus petit coût total des cartes une fois plusieurs connexions routées. La différence consiste en un rabais de 50 % accordé à l'augmentation de la capacité d'un segment. Pour ce faire, le calcul de f^{eval} est basé sur les ports. En appliquant cette vision à l'exemple précédent, la différence pour l'augmentation de la capacité est réduite de 6 k\$ à 3 k\$, ce qui est maintenant moins coûteux que d'ajouter des ports OC-48 (4 k\$). Bref, avec la vision globale, on n'obtient plus nécessairement le chemin à coût minimum pour la connexion en cours. Mais il s'agit d'un moyen efficace pour éviter l'étalement des connexions.

En pratique, le rabais de 50 % fonctionne bien pour un ratio du coût des cartes de 10 : 4. Il faudrait pousser l'analyse plus loin pour généraliser le concept, ce qui n'a pas été fait dans le cadre du présent mémoire. De plus, il faudrait considérer l'ajout d'une troisième capacité de transport, par exemple OC-768, et voir si le rabais est toujours efficace.

Il aurait aussi été possible d'opter pour l'approche opposée. Au lieu de passer à un segment OC-192 par prévention, on aurait pu ajouter un deuxième segment OC-48 puis attendre que ce dernier soit saturé avant de tenter de les combiner en un seul segment OC-192. Quelques raisons justifient d'avoir choisi la première approche. Puisque les cartes OC-192 sont moins dispendieuses par unité de capacité, il est à espérer que la solution finale en contiendra en grande majorité. De plus, deux segments OC-48 coûtent moins cher qu'un OC-192 mais requièrent deux protections au lieu d'une. Il n'est donc pas évident que le coût total incluant la protection serait moindre.

Le tableau 5.1 présente un résumé des deux visions, auxquelles fera référence la

prochaine section.

Vision	Fonction d'évaluation
Globale	Ports avec un rabais à l'augmentation de la capacité.
Locale	Cartes, ports si égalité.

Tableau 5.1 – Fonction d'évaluation pour le routage des connexions

5.2.1.2 Router plusieurs connexions

L'utilitaire *Router plusieurs connexions* reçoit en entrée une liste de connexions et doit les placer de façon à minimiser la fonction d'évaluation.

La première étape consiste à trier ces connexions dans le but de faciliter la recherche d'une bonne solution. Elles sont donc classées en ordre croissant de la longueur du plus court chemin reliant la source à la destination, puis en ordre lexicographique (par paire source-destination) si égalité, et par ordre décroissant de capacité si l'égalité persiste. Cet ordonnancement a été retenu puisqu'il s'est avéré le plus efficace en pratique. Prioriser les connexions entre les nœuds voisins permet de créer de petits segments qui pourront être empruntés par des connexions plus longues.

La deuxième étape consiste à parcourir la liste triée à deux reprises, d'abord avec une vision globale, puis avec une vision locale (se référer au tableau 5.1).

Le parcours de la liste avec une vision globale s'effectue en formant des groupes de connexions de même source-destination pouvant cohabiter sur un même segment (autrement dit, de capacité totale n'excédant pas OC-192). Pour chaque groupe, on compare deux alternatives : (1) router chaque connexion séparément une après l'autre, ou (2) router le groupe sur un seul chemin comme s'il s'agissait d'une superconnexion. On préfère la deuxième alternative si elle engendre un plus petit coût des cartes. L'idée d'avoir deux alternatives est de pouvoir choisir un routage en fonction du coût des cartes malgré que chacune soit évaluée sous la vision globale qui est basée sur le coût des ports. De plus, la deuxième alternative apporte une faible pénalité en temps de calcul, puisque plusieurs

connexions sont traitées comme une seule. On verra en section 5.3.2.1 que cette alternative est employée pour la solution initiale.

Lors du second parcours de la liste de connexions, celles-ci sont retirées puis routées tour à tour, avec une vision locale. Comme il a été expliqué au cours de la section précédente, la vision globale est nécessaire pour éviter l'étalement des connexions. Mais elle n'est pas parfaite non plus. Par exemple, elle privilégie un segment OC-192 (10 k\$) à deux segments OC-48 (8 k\$). C'est pourquoi la vision locale est appliquée ici afin d'étaler les quelques connexions qui permettraient de réduire le coût, une fois toutes les connexions routées.

Finalement, si l'utilitaire est appelé dans le cadre d'une optimisation conjointe, les segments d'opération créés sont protégés en appelant l'utilitaire *Protéger plusieurs segments d'opération* (section 5.2.2.2).

5.2.2 Utilitaires pour la protection

5.2.2.1 Protéger un segment d'opération

Très semblable à l'utilitaire *Router une connexion*, il détermine le chemin à f^{eval} minimum sur lequel protéger un segment d'opération. Le paramètre est le nombre de routes disjointes et réalisables à considérer (noté R_p).

Voici les deux principales différences par rapport à *Router une connexion*.

1. Seule la vision locale est utilisée, puisqu'on n'est pas confronté au problème du groupage de capacité sur un segment.
2. Un critère d'arrêt est ajouté au parcours de la liste des routes : on arrête aussitôt qu'on obtient un chemin avec un coût des ports nul. Un tel coût indique que la protection est partagée d'un bout à l'autre, sans recours à des ports supplémentaires, et donc que le coût des cartes est également nul. Cette mesure a pour effet de diminuer significativement le temps d'exécution de l'utilitaire, en entraînant une perturbation quasi nulle de la qualité de la solution. En effet, il a été observé

que les chemins de protection avec un coût des cartes négatif sont très rares. Un coût négatif survient à un nœud lorsqu'en augmentant la capacité d'un segment de OC-48 à OC-192, on élimine une carte OC-48 pour utiliser un port OC-192 libre. Mais, en pratique, les segments de protection OC-48 sont très peu nombreux.

5.2.2.2 Protéger plusieurs segments d'opération

L'utilitaire *Protéger plusieurs segments d'opération* reçoit en entrée une liste de segments d'opération et doit les protéger tout en minimisant la fonction d'évaluation.

Cette liste est triée en ordre décroissant de capacité, et en ordre décroissant de plus court chemin si égalité, puis en ordre lexicographique (par paire source-destination). Elle est ensuite traversée pour appeler l'utilitaire *Protéger un segment d'opération* (section 5.2.2.1) avec chaque élément.

5.2.2.3 Retirer une protection

Lorsqu'une protection est retirée, il y a peut-être matière à réduire le nombre de ports en éliminant certains segments de protection. Le cas le plus évident se produit si la protection était la dernière à occuper un segment. Le segment peut alors être éliminé, ainsi que les ports à ses extrémités. Cette procédure est exécutée automatiquement et ne fait pas partie de l'utilitaire proprement dit.

Par contre, une réduction du nombre de ports est aussi possible même si le segment est encore occupé. Il faut premièrement que toutes les protections occupant encore le segment poursuivent leur chemin sur un segment commun, de part ou d'autre du segment, pour qu'il y ait une opportunité de fusionner ces segments et ainsi économiser une carte. Ensuite, il suffit qu'une même longueur d'onde soit disponible d'un bout à l'autre des deux segments.

Par exemple, après avoir retiré la protection P_1 (figure 5.1), le segment qu'elle occupait est seulement utilisé par la protection P_2 qui continue sur un deuxième segment.

Puisque λ_1 est libre sur la route de ce segment, il est possible de remplacer les deux segments de P_2 par un seul dans le but d'économiser une carte.

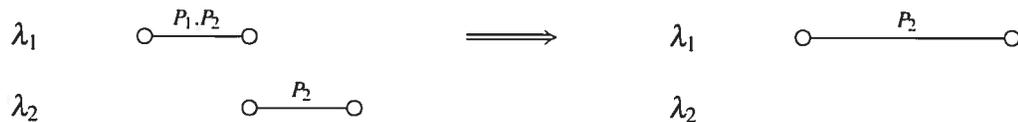


Figure 5.1 – Fusion de segments suite au retrait d'une protection

L'utilitaire *Retirer une protection* applique cette analyse sur chaque segment constituant la protection à être retirée pour fusionner le plus de segments possible. Un utilitaire homologue aurait pu être conçu pour le retrait d'une connexion mais, après observation, trop de connexions sont groupées par segment et la fusion n'est pratiquement jamais possible.

5.3 Méthode de recherche tabou

La présente section décrit le cœur de la métaheuristique proposée. C'est ici qu'on tentera, à partir d'une solution initiale, de faire progresser la solution le plus près possible de l'optimum. Au cours des prochaines sections, nous verrons les mouvements proposés pour la méthode de recherche tabou, suivis de quelques stratégies envisagées tant pour l'optimisation séquentielle que conjointe (section 5.3.2) pour terminer avec les plus importantes tentatives infructueuses (section 5.3.3).

La structure générale de la méthode de recherche tabou ainsi que les mouvements sont grandement inspirés des travaux présentés dans [12].

5.3.1 Mouvements

5.3.1.1 Éliminer un segment d'opération

Le mouvement *Éliminer un segment d'opération* a pour but de déplacer plusieurs connexions. On s'y prend en retirant un segment d'opération et les ports à ses extrémités,

pour ensuite replacer sur un nouveau chemin toutes les connexions qui y voyageaient.

Ici, la liste tabou ne contient pas des solutions (section 5.1) mais des connexions auxquelles on ne doit pas retoucher. Il existe un trop grand nombre de solutions quasi équivalentes à une permutation près, de telle sorte qu'on doive prendre des mesures plus radicales pour éviter de stagner. Modifier la longueur d'onde d'un segment, par exemple, donnerait une solution différente sans être plus intéressante. On note L_o le paramètre de la métaheuristique qui détermine le pourcentage des connexions qui se retrouvent dans la liste tabou.

Voici donc la description du mouvement.

1. Trier les segments d'opération en ordre croissant de taux d'occupation. Le taux d'occupation étant défini comme la capacité totale des connexions voyageant sur un segment divisée par sa capacité de transport. Moins le taux est grand, moins le segment est utilisé efficacement et plus il est à espérer qu'il sera possible d'économiser des ports en groupant ses connexions autrement. Le tri représente le critère de sélection du segment d'opération sur lequel appliquer le mouvement.
2. Choisir le premier segment d'opération dont aucune connexion ne figure dans la liste tabou.
3. Retirer les connexions passant par le segment, ainsi que les ports à ses extrémités.
4. Appeler l'utilitaire *Router plusieurs connexions* (section 5.2.1.2) pour replacer les connexions, mais en interdisant de créer un segment débutant et terminant aux mêmes tronçons que l'original. Cette mesure vise à empêcher qu'un segment d'opération soit recréé sur un chemin trop semblable, comme par exemple sur la même route mais en utilisant une autre longueur d'onde.
5. Ajouter les connexions à l'arrière de la liste tabou et en retirer celles qui sont expirées. La taille relative de la liste tabou étant fixée à L_o , celle-ci est implantée sous forme de file.

Un critère de sélection alternatif est aussi proposé. Au lieu de se baser sur le taux

d'occupation pour prévoir quel segment devrait être retiré, on tente d'en retirer un certain nombre pour en calculer la fonction d'évaluation. Il est alors possible de retenir le segment d'opération donnant le meilleur f^{eval} une fois le mouvement appliqué. On introduit le paramètre S_o , défini comme la fraction des segments d'opération à évaluer de la sorte. Si $S_o > 0$, on évalue le retrait de ce pourcentage des segments ; si $S_o = 0$, on se base sur le taux d'occupation décrit plus haut.

Bref, éliminer un segment permet de faire évoluer les chemins d'opération en routant et groupant différemment les connexions. Il aurait également été possible de développer un mouvement qui ne retire qu'une connexion à la fois, mais l'impact s'avèrerait trop mineur pour être intéressant.

5.3.1.2 Éliminer un segment de protection

Le mouvement *Éliminer un segment de protection* est très semblable à celui pour les segments d'opération. Sa fonction est de retirer un segment de protection pour replacer sur un nouveau chemin toutes les protections qui s'y trouvaient. Se référer à la section 5.3.1.1 pour plus de précisions.

Cette fois, la liste tabou contient les segments d'opération dont les protections ne doivent pas être modifiées, et sa longueur relative est déterminée par le paramètre L_p .

Cinq étapes constituent le mouvement.

1. Trier les segments de protection en ordre croissant du nombre de segments protégés.
2. Choisir le premier segment de protection dont aucun segment d'opération protégé ne figure dans la liste tabou.
3. Retirer les protections passant par le segment, ainsi que les ports à ses extrémités.
4. Appeler l'utilitaire *Protéger plusieurs segments d'opération* (section 5.2.2.2) pour reprotéger les segments d'opération, mais en interdisant de créer un segment de protection débutant et terminant aux mêmes tronçons que l'original.

5. Ajouter les segments d'opération à l'arrière de la liste tabou et en retirer autant du devant, pour maintenir une file de taille fixe L_p .

Tout comme le mouvement pour éliminer un segment d'opération, un critère de sélection alternatif (contrôlé par le paramètre S_p) permet de tester le mouvement sur plusieurs segments dans le but de l'appliquer sur le plus intéressant.

Nous avons maintenant vu les mouvements proposés pour faire bouger et améliorer une solution tant du côté de l'opération que de la protection. Nous nous pencherons finalement sur un mouvement qui tente de profiter d'une optimisation conjointe.

5.3.1.3 Déplacer un segment d'opération

L'objectif du mouvement *Déplacer un segment d'opération* est de diminuer le coût de la protection sans pour autant affecter négativement l'opération. Contrairement aux deux mouvements précédents, il ne fait pas partie de la méthode de recherche tabou à strictement parler, car aucune liste tabou n'est utilisée. La méthode de recherche tabou s'en sert tout de même pour améliorer et faire évoluer la solution.

Voici le travail effectué sur chacun des segments d'opération.

1. Retirer la protection du segment.
2. Déterminer f^{eval} suite à la protection du segment.
3. Réévaluer la fonction d'évaluation mais en considérant toutes les routes pour la protection, et non seulement celles disjointes de la route d'opération.
4. Si la deuxième protection a un f^{eval} inférieur, il suffit de trouver un chemin disjoint sur lequel placer le segment d'opération pour qu'il puisse profiter de cette protection. Donc, choisir la deuxième protection à condition qu'il y ait une longueur d'onde libre sur une route disjointe.
5. Sinon, choisir la première protection.

L'idée derrière le mouvement est qu'un segment d'opération nécessite deux ports peu importe la route empruntée. Mais la protection doit être disjointe de l'opération, et

accorder une route plus courte à l'opération pour ensuite protéger le segment n'est pas toujours optimal. Ce mouvement fait au contraire dépendre l'opération sur la protection : la meilleure protection est choisie, puis un chemin d'opération disjoint est déterminé.

Un autre effet bénéfique du mouvement est ce qu'on appelle le raffinement de la protection. Même dans le cas où il n'est pas avantageux de déplacer le segment d'opération pour améliorer sa protection, simplement le fait de reprotéger peut diminuer le coût de la solution. On définit *raffinement de la protection* le fait de traverser la liste des segments d'opération pour replacer leur protection à leur optimum local.

5.3.2 Stratégies

5.3.2.1 Solution initiale

Grâce à l'utilitaire *Router plusieurs connexions* décrit en section 5.2.1.2, il est maintenant facile de générer une première solution. Il suffit d'appeler cet utilitaire tout en prenant quelques précautions.

Tout d'abord, tel que mentionné lors de la description de l'utilitaire, on préfère toujours la deuxième option de routage afin de grouper les connexions au maximum. Il a été observé en pratique que cette mesure permet d'accroître la performance de la méthode de recherche tabou qui suivra.

De plus, dans le cas d'une optimisation conjointe, on se restreint à la moitié des longueurs d'onde lors du routage initial des connexions. L'idée est de se réserver suffisamment de longueurs d'onde sur chaque tronçon pour la protection. Sans cette précaution, le cœur du réseau s'engorge et il arrive que certains segments d'opération ne peuvent être protégés.

Finalement, après avoir appelé l'utilitaire, on s'assure d'une solution initiale réalisable en revisitant les connexions ou protections qui dépassent le nombre maximum de régénérations permises. Mentionnons qu'en tout temps, il est interdit de placer une connexion (ou protection) sur un chemin non-réalisable. Mais après avoir placé plusieurs

connexions, certains segments sont fragmentés de telle sorte que le nombre de segments d'une connexion peut dépasser le maximum permis. On remédie à la situation en routant à nouveau les connexions ou protections concernées.

5.3.2.2 Optimisation séquentielle

Définissons d'abord comme paramètres le nombre de mouvements exécutés lors d'une phase dédiée à l'opération (P_o) ou à la protection (P_p). On définit également un critère d'arrêt : la méthode de recherche tabou termine dès qu'aucune amélioration de la meilleure solution n'est observée pendant A mouvements.

Voici les stratégies proposées pour l'optimisation séquentielle.

- S1. – Tant qu'il y a eu amélioration de la meilleure solution lors des derniers A mouvements, effectuer le mouvement *Éliminer un segment d'opération*.
- Appeler une première fois l'utilitaire *Protéger plusieurs segments d'opération* afin de protéger la meilleure solution trouvée à l'étape précédente, puis l'appeler 3 autres fois pour raffiner la protection.
- S2. – Tant qu'il y a eu amélioration de la meilleure solution lors des derniers A mouvements, effectuer le mouvement *Éliminer un segment d'opération*.
- Appeler l'utilitaire *Protéger plusieurs segments d'opération* afin de protéger la meilleure solution trouvée à l'étape précédente. On obtient ainsi la solution initiale pour l'étape suivante.
 - Tant qu'il y a eu amélioration de la meilleure solution lors des derniers A mouvements, effectuer le mouvement *Éliminer un segment de protection*.

Par rapport à S1, la stratégie S2 vise à obtenir une meilleure solution pour la protection en remplaçant le raffinement par une méthode de recherche tabou.

5.3.2.3 Optimisation conjointe

Voici les stratégies proposées pour l'optimisation conjointe.

C1. – Tant qu’il y a eu amélioration de la meilleure solution lors des derniers A mouvements :

- (a) effectuer P_o fois le mouvement *Éliminer un segment d’opération* ;
- (b) appeler le mouvement *Déplacer un segment d’opération* pour raffiner la protection.

Le raffinement de la protection avec le mouvement *Déplacer un segment d’opération* donne la priorité à la protection pour contrebalancer l’autre phase qui favorise l’opération.

C2. – Tant qu’il y a eu amélioration de la meilleure solution lors des derniers A mouvements :

- (a) effectuer P_o fois le mouvement *Éliminer un segment d’opération* ;
- (b) appeler P_p fois le mouvement *Éliminer un segment de protection*.

Cette stratégie est similaire à S2, mais les mouvements sur l’opération et la protection sont alternés pour profiter de l’optimisation conjointe.

5.3.3 Tentatives infructueuses

Parmi les tentatives d’améliorer la métaheuristique qui n’ont pas porté fruit, on s’attardera ici à l’exploitation d’un effet domino et à la non-réalisabilité. Mais d’abord, deux tentatives de post-optimisation sont présentées.

5.3.3.1 Post-optimisation

Une mesure de post-optimisation a été envisagée mais n’a pas été retenue. Par défaut, les segments sont maintenus à la capacité minimale nécessaire pour accommoder les connexions ou protections qui y voyagent. Par contre, étant donné que le calcul du coût des cartes se fait par capacité, il est possible qu’à un nœud donné, il y ait un excédent de

ports OC-48 en sortie mais un excédent de ports OC-192 en entrée. Il serait alors peut-être avantageux d'augmenter la capacité d'un segment OC-48 à OC-192 pour utiliser moins de cartes et ainsi diminuer le coût de la solution.

Un utilitaire fut alors développé pour tenter d'améliorer le coût des cartes en augmentant la capacité de certains segments, mais en vain. D'abord, la situation ne se produit que très rarement. Aussi, un segment d'opération dont on augmente la capacité devra avoir une protection de plus grande capacité, ce qui ne va pas dans le sens d'une réduction de coût.

Par ailleurs, une autre tentative a visé les segments d'opération OC-192 occupés à capacité inférieure ou égale à OC-96. Suite à la méthode de recherche tabou, il est envisageable de remplacer ces segments par deux segments OC-48 pour réduire le coût de la solution. Malheureusement, les rares segments qui rencontrent ce critère ne gagnent pas à être remplacés. La plupart du temps, aucune carte OC-192 n'est retirée tandis qu'on doit presque toujours ajouter des cartes OC-48. Autrement dit, ces segments OC-192 bénéficiaient de ports gratuits donc il est moins préoccupant que ceux-ci ne soient pas utilisés à pleine capacité.

5.3.3.2 Effet domino

La métaheuristique proposée applique des mouvements sur des segments d'opération et de protection. Elle choisit le prochain segment à traiter en se basant sur un critère de sélection ou sur le hasard. Par contre, les mouvements consécutifs ne sont pas coordonnés entre eux, ce qui pourrait permettre à un mouvement de tirer profit du travail effectué lors des mouvements précédents.

Il a toutefois été tenté de profiter d'un tel effet domino. Au lieu de balayer linéairement la liste des segments pour le mouvement *Déplacer un segment d'opération*, on essaya un ordre plus élaboré. Après le déplacement d'un segment d'opération, les segments qui partageaient sa protection étaient traités en priorité. Ainsi, le mouvement n'était pas appliqué dans un ordre arbitraire mais selon les chaînes de partage de la protection. En

vain, aucune amélioration significative du coût de la solution n'a été observée.

5.3.3.3 Non-réalisabilité

Il est parfois intéressant de tolérer la non-réalisabilité à l'intérieur de la méthode de recherche tabou. Cela peut être utile lorsqu'il est difficile d'obtenir une solution réalisable à chaque itération. De plus, si l'espace des solutions réalisables n'est pas convexe, la non-réalisabilité peut permettre d'atteindre plus directement la solution optimale. Il faut par contre développer un mécanisme pour empêcher la solution courante de toujours être non-réalisable. Par exemple, en incluant la non-réalisabilité à la fonction d'évaluation avec un facteur de pénalité qui augmente lorsque la solution demeure non-réalisable, et diminue quand elle est réalisable.

Afin d'incorporer la non-réalisabilité dans la méthode de recherche tabou, il faut identifier au moins une contrainte qu'on se permet de violer. Pour le problème qui nous intéresse, deux contraintes ont été considérées :

1. *Le nombre maximum de longueurs d'onde sur une fibre.* En permettant d'excéder temporairement la limite de longueurs d'ondes sur une fibre, il est possible d'éviter les régénérations nécessaires au changement de longueur d'onde lorsqu'aucune longueur d'onde n'est disponible d'un bout à l'autre d'une route. Par contre, les matrices de trafic considérées ne sont pas assez volumineuses pour que cette tentative soit intéressante.
2. *Le nombre maximum de régénérations pour une protection.* Les connexions ont tendance à n'emprunter qu'un segment pour que le coût soit le plus petit possible. D'un autre côté, les protections ont besoin de plusieurs segments pour profiter pleinement du partage. Il a donc été tenté de permettre plus de deux régénérations aux protections. Malheureusement, le coût de la solution obtenue avec trois régénérations tolérées est plus élevé que celui avec deux régénérations au maximum. En conséquence, l'expérimentation n'a pas été poussée plus loin dans cette direction.

5.4 Réalisation

Cette section du mémoire s'intéresse à la réalisation de la métaheuristique, laquelle a été programmée en C++ et compilée avec GCC sous Windows (à l'aide de MinGW) ainsi que sous Linux. Les aspects couverts constituent les principaux facteurs donnant l'efficacité à la métaheuristique.

La section 5.4.1 décrit sommairement l'architecture du programme mais surtout les relations entre les classes. La section 5.4.2 couvre ensuite la fonction sur laquelle le plus d'effort a été investi afin de réduire son temps d'exécution : l'algorithme de programmation dynamique qui détermine un chemin à f^{eval} minimum. La section 5.4.3 fait finalement état de certaines particularités des structures de données rendant celles-ci plus performantes.

5.4.1 Architecture

Plusieurs des termes définis à la section 2.1 se sont vus attribuer une classe au même nom dans le programme. Le diagramme de classes en figure 5.2 présente les relations entre ces classes.

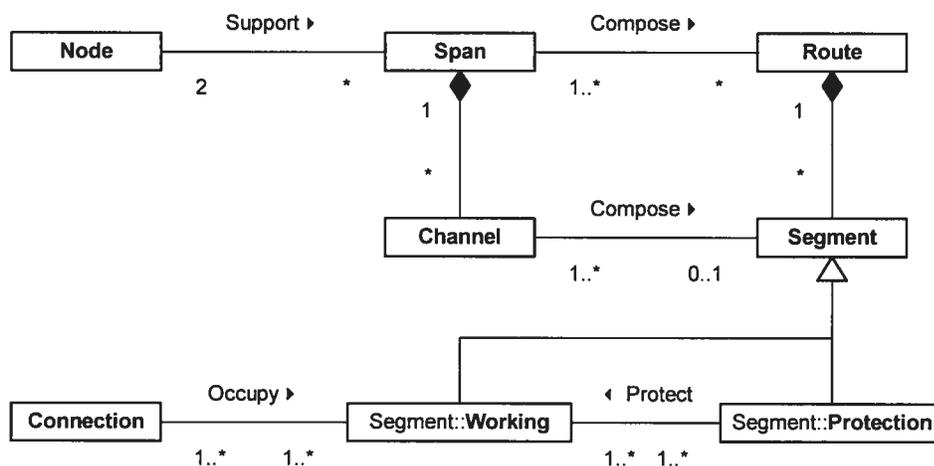


Figure 5.2 – Diagramme de classes

On remarque que le concept de segment est central. Il aurait été possible de l'exclure de l'implantation puisque les connexions voyagent sur des canaux et, en mémorisant quelle connexion occupe chaque canal, il est possible de retrouver où débute et termine chaque segment. Mais étant donné que la protection se fait par segment, mémoriser explicitement les segments d'opération et de protection facilite beaucoup la programmation au coût d'un peu plus de redondance.

Les instances de ces classes sont gérées par deux classes maîtresses dans le programme :

Network contient les objets sur la première rangée de la figure 5.2. Ces données, soient les nœuds, tronçons et routes, sont constantes pour un réseau donné.

Solution mémorise toute l'information relative à une solution particulière et qui se retrouve sur les deux dernières rangées : l'occupation des canaux, la présence de segments, le routage des connexions.

Cette division des objets permet de manipuler facilement plusieurs solutions différentes pour un même réseau, tout en ne gardant en mémoire qu'un seul exemplaire de la configuration du réseau.

Une troisième classe maîtresse, *Heuristic*, implante la méthode de recherche tabou. Cette classe peut gérer simultanément plusieurs descriptions de réseaux et plusieurs solutions pour chacune.

5.4.2 Programmation dynamique

Pour déterminer la séquence de longueurs d'ondes à moindre f^{eval} le long d'une route, tant pour l'opération que la protection, on propose un algorithme de programmation dynamique. Énumérer toutes les possibilités aurait pris un temps exponentiel : en posant n le nombre de tronçons de la route et d le nombre de longueurs d'ondes, on obtient d^n chemins à évaluer.

5.4.2.1 Concept

On se base sur l'observation suivante (sous-structure optimale) pour démontrer qu'un algorithme de programmation dynamique peut également trouver la solution optimale : étant données une route sur les tronçons numérotés de 0 à $n - 1$ et une régénération fixée entre les tronçons k et $k + 1$, la solution optimale globale contient les solutions optimales pour les sous-routes $0, \dots, k$ et $k + 1, \dots, n - 1$. Autrement dit, poser une régénération à un nœud donné sépare le problème en deux sous-problèmes dont les solutions optimales donnent la solution optimale globale pour une régénération à cet endroit. Il reste alors à considérer une régénération à tous les endroits possibles.

Si on définit la fonction d'évaluation en termes de ports supplémentaires, cette affirmation est juste ; mais en termes de cartes, un problème se pose en raison du calcul $\max\{\text{entrée}, \text{sortie}\}$. On traitera cette difficulté au cours des sections suivantes, en espérant tout de même obtenir une solution optimale dans la plupart des cas rencontrés.

5.4.2.2 Sans régénération

Définissons d'abord $SR(i, j, \lambda)$ comme la fonction d'évaluation minimum pour occuper sans régénération intermédiaire (en un seul saut) le chemin décrit par la sous-route i, \dots, j et la longueur d'onde λ .

On évalue comme suit le coût des ports au début du chemin, un calcul similaire étant effectué à la fin du chemin. Soit c le coût des ports de capacité requise pour occuper le chemin.

- Si le chemin n'est pas disponible sans régénération, le coût est ∞ .
- Si le chemin est libre, le coût est c pour un port de sortie.
- Si le chemin est déjà occupé par un segment mais qu'il est disponible (groupage pour l'opération ou partage pour la protection), on note c' le coût des ports de ce segment.
- Si la régénération n'a pas lieu au début du chemin, le coût est de $c + c'$ pour un

port d'entrée et un port de sortie afin de fractionner le segment existant.

- Si la régénération a déjà lieu, le coût est de $c - c'$ pour l'augmentation de la capacité du port.

Un calcul similaire est ensuite effectué pour le coût des cartes, mais en tenant compte du nombre de ports d'entrée et de sortie présents à chaque extrémité. L'ajout ou le retrait de ports n'affecte pas linéairement le coût des cartes, il faut passer par le calcul $\max\{\text{entrée, sortie}\}$.

5.4.2.3 Récurrence

On définit $C(i)$ comme la fonction d'évaluation minimum pour occuper la route $i, \dots, n-1$, $C(0)$ étant le problème à résoudre :

$$C(i) = \min_{\lambda} \left\{ SR(i, n-1, \lambda), \min_{i \leq j < n-1} \{ SR(i, j, \lambda) + C(j+1) \} \right\} \quad (5.1)$$

Le premier terme représente le cas sans régénération, tandis que le second désigne une première régénération à un des nœuds intermédiaires (entre les tronçons j et $j+1$).

Si on évalue le coût des cartes, la somme $SR(i, j, \lambda) + C(j+1)$ doit être ajustée. En effet, les ajouts ou retraits de cartes au nœud entre j et $j+1$ auraient pu être mal comptabilisés en raison de l'indépendance du calcul. Par exemple, s'il y a au départ autant de ports d'entrée que de sortie au nœud, une carte devrait être ajoutée dans la solution $C(j+1)$ pour un nouveau port de sortie. Mais indépendamment, la solution $SR(i, j, \lambda)$ pourrait aussi requérir une nouvelle carte pour l'ajout d'un port d'entrée au même nœud, tandis qu'en réalité une seule carte serait nécessaire et non deux.

L'ajustement permet alors d'évaluer correctement $C(i)$ dans tous les cas. Par contre, lorsque l'algorithme détermine la meilleure sous-solution pour $C(j+1)$, il n'est pas en mesure de connaître le nombre de ports qui seront ajoutés ou retirés au nœud source. Il n'y a donc pas assurance d'obtenir la solution optimale quant au coût des cartes. Lors de travaux ultérieurs, il serait intéressant d'explorer ce problème plus en profondeur

pour déterminer dans quelles situations l'optimum n'est pas atteint et à quelle fréquence surviennent ces situations.

5.4.2.4 Complexité

Soient n le nombre de tronçons de la route et d le nombre de longueurs d'ondes. Il y a n sous-problèmes. Pour chacun, on doit étudier d longueurs d'onde et pour chacune, $\Theta(n)$ tronçons et une position de régénération par tronçon. La complexité globale en temps est donc $\Theta(n^2d)$. Ce résultat est de beaucoup meilleur à celui d'une approche naïve qui énumère toutes les possibilités en temps $\Theta(d^n)$.

5.4.2.5 Exemple

Nous avons à la figure 5.3 une route à 3 tronçons (0, 1 et 2) et 3 longueurs d'onde (λ_1 , λ_2 et λ_3). Les traits bornés par des cercles représentent les segments déjà en place, mais seulement le segment hachuré est disponible (groupage pour l'opération ou partage pour la protection). Afin de simplifier le problème, on évalue la quantité de ports supplémentaires nécessaires.

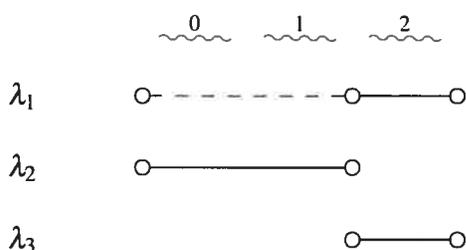


Figure 5.3 – Exemple de route pour l'algorithme de programmation dynamique

On débute par le plus petit sous-problème, $C(2)$, égal à 2 en utilisant λ_2 qui est la seule disponible.

Pour $C(1)$, aucune longueur d'onde n'est disponible de bout en bout alors au moins une régénération est nécessaire entre les tronçons 1 et 2, ce qui donne $2 + C(2) = 4$ en passant par λ_3 puis λ_2 .

Finalement, on évalue $C(0)$ qui correspond au problème à résoudre. Ne pas régénérer est impossible. Régénérer une première fois entre les tronçons 0 et 1 donnerait un coût de $2 + C(1) = 6$. Par contre, régénérer une première fois entre 1 et 2 nous permet de prendre λ_1 sans ajouter de port et donc d'obtenir un coût total de $0 + C(2) = 2$.

5.4.2.6 Fonction d'évaluation

Afin de départager les égalités tout en favorisant des solutions de meilleure qualité, des critères secondaires sont considérés dans la fonction d'évaluation. Le tableau 5.2 présente leur ordre de priorité. Se référer au tableau 5.1 pour une description des deux visions.

Vision	Fonction d'évaluation
Globale pour l'opération	Ports, nombre de régénérations.
Sinon	Cartes, ports, nombre de régénérations.

Tableau 5.2 – Fonction d'évaluation de l'algorithme de programmation dynamique

5.4.3 Structures de données

5.4.3.1 Structure sur mesure

Comme il a été expliqué précédemment (section 5.4.1), l'information propre à une solution est regroupée dans un objet de la classe *Solution*. Cet objet mémorise l'occupation des canaux, la présence de segments et le routage des connexions.

Attardons-nous ici aux segments d'opération et de protection. La structure de données qui les contient devra répondre aux deux critères suivants.

1. Insertion et suppression efficace de tout segment. Lorsque la solution évolue, des segments sont régulièrement créés ou effacés.
2. Accès rapide à partir d'un indice. La copie de la structure de données, par exemple pour mémoriser une bonne solution, doit être rapide. Si les segments sont accédés

par un pointeur, il faudra aller modifier l'adresse des pointeurs étant donné le nouvel emplacement des segments en mémoire.

Deux structures de données classiques respectent très bien un des critères, mais pas l'autre :

Vecteur ne permet pas l'insertion et la suppression efficace de tout élément.

Liste ne permet pas l'accès rapide à partir d'un indice.

Une structure de données sur mesure est alors implantée pour résoudre ce problème. Il s'agit essentiellement d'un vecteur auquel on ajoute une mémoire des positions supprimées pour permettre l'insertion et la suppression efficace. Lorsqu'on en retire un segment, la structure mémorise son indice comme étant maintenant inoccupé sans pour autant éliminer un espace mémoire. On accède donc encore aux autres segments par le même indice. Lorsqu'on ajoute un segment, il sera placé dans le premier espace libre, ou alors le vecteur sera allongé s'il était déjà à pleine capacité.

5.4.3.2 Liste d'association

Les listes d'association (*map* en anglais) permettent de programmer assez facilement des opérations complexes. Leur caractéristique : à chaque élément est associée une clé qui permettra d'accéder à celui-ci. La forme la plus répandue d'une liste d'association consiste à ranger toutes les clés dans un arbre, ce qui donne un temps d'accès d'ordre logarithmique.

Il a été tenté de faire appel à ces listes d'association pour comptabiliser les modifications aux ports d'un nœud lors de l'évaluation d'un chemin pour l'opération ou la protection. La clé étant la capacité, l'élément associé donnait la différence de ports en entrée et en sortie. On y emmagasinait l'information concernant les ports retirés ou ajoutés, pour ensuite être en mesure de savoir quel serait l'impact sur le nombre de cartes de chaque capacité.

Utiliser cette structure de données rendait le code très simple. Mais après avoir profilé

le programme (étudié son temps d'exécution) à l'aide de GNU prof, il est apparu évident que la liste d'association n'était pas la structure la plus efficace. En effet, la moitié du temps d'exécution du programme servait à y accéder.

C'est pourquoi la liste d'association a été éliminée. Maintenant, on ne fait plus référence aux capacités mais plutôt à des indices de capacité. Par exemple, on a l'indice 1 pour OC-48 et 2 pour OC-192. Ceci permet de mémoriser les différences de ports dans un vecteur. Les clés ne sont plus des capacités arbitrairement grandes mais des indices variant de 0 à 2.

Grâce à ce changement, le programme roule deux fois plus rapidement. Une exécution qui prenait 30 secondes avec la liste d'association en prend maintenant 15 avec un vecteur.

CHAPITRE 6

EXPÉRIMENTATION

L'expérimentation est divisée en trois sections. D'abord, on décrit les mesures qui ont été prises pour valider la réalisabilité et la qualité des solutions (section 6.1). Ensuite sont donnés les paramètres de la métaheuristique ainsi que les réseaux tests (section 6.2). Finalement, la section 6.3 est dédiée à la présentation et à l'analyse des résultats obtenus.

6.1 Validation

Étant donnée la complexité du problème étudié, il est essentiel de valider à certains égards les solutions obtenues. Dans un premier temps, on doit s'assurer que chaque solution est réalisable (section 6.1.1), c'est-à-dire qu'elle respecte les contraintes du problème. Aussi, on doit être en mesure d'en évaluer la qualité (section 6.1.2).

6.1.1 Réalisabilité

Un utilitaire a été développé pour valider la réalisabilité d'une solution. Pierre-Marc Fournier a conçu la version initiale qui vérifiait les chemins d'opération [5], puis Manon Bélanger y a ajouté la validation des chemins de protection [1]. Le travail accompli par ces deux étudiants est indispensable car il permet de certifier que les solutions obtenues sont réalisables en pratique. Voici les caractéristiques d'une solution qui sont validées par l'utilitaire :

- les connexions, protections et segments sont cohérents (source-destination, tronçons ou segments qui les constituent, pas de boucle dans les segments, pas de flots bifurqués) ;
- la capacité occupée sur un canal ne dépasse pas sa capacité de transport ;
- aucun canal n'est utilisé à la fois pour l'opération et la protection ;

- le nombre maximal de longueurs d’ondes à utiliser est respecté ;
- le nombre maximal de régénérations est respecté ;
- chaque segment d’opération a une protection disjointe ;
- le partage des protections est valide ;
- aucune protection n’est groupée.

6.1.2 Qualité

Comme on l’a vu à plusieurs reprises, le problème qui nous intéresse est très difficile à résoudre. C’est pourquoi le développement d’une métaheuristique a été préféré à la formulation d’un programme en nombres entiers. Par le fait même, il n’est pas facile de déterminer la qualité des solutions obtenues, puisqu’aucune borne n’a été calculée.

En effet, même en mettant de côté l’optimisation conjointe, il est difficile d’obtenir une borne de qualité pour l’un ou l’autre des sous-problèmes. D’un côté, il n’existe à ce jour aucune méthode efficace pour calculer une borne intéressante au problème GRWA avec minimisation du coût des cartes. Pour ce qui est de la protection par segment, étant donné que le groupage de la protection est interdit, on pourrait croire que ce problème se rapproche de RWA et qu’il est donc plus facile d’obtenir une borne. Malheureusement, plusieurs facteurs font en sorte que le problème ne s’apparente pas à un simple RWA : l’objectif de minimisation du coût des cartes, la pluralité des capacités de transport, la protection qui doit être disjointe du segment d’opération, le partage de la protection.

On doit alors s’en remettre à des métriques pour juger de la qualité d’une solution. Débutons avec deux métriques qui se révèlent intéressantes quand l’objectif est de minimiser la capacité totale utilisée, et voyons pourquoi elles sont moins révélatrices pour l’objectif qui nous intéresse.

1. *Longueur par rapport à la route la plus courte.* La capacité utilisée par une connexion ou protection est calculée en multipliant sa capacité par la longueur de sa route. Ainsi, plus on réussit à placer les connexions et protections sur une courte route, moins on utilise de capacité pour ce faire. Outre les considérations de par-

tage de la protection, on voit que cette métrique est directement liée à la qualité d'une solution où l'on veut minimiser la capacité totale utilisée. Par contre, placer une connexion sur une route plus longue peut permettre d'économiser des cartes, si on y trouve une longueur d'onde disponible d'un bout à l'autre par exemple. Lorsqu'on minimise le coût des cartes, on ne veut pas nécessairement minimiser la capacité totale. Au contraire, il faut utiliser au mieux la capacité offerte par le réseau pour atteindre notre objectif.

2. *Taux de partage de la protection.* La capacité totale nécessaire à la protection est inversement proportionnelle au taux de partage. Cette métrique est donc tout à fait pertinente quand l'objectif est de minimiser la capacité totale utilisée. Mais lorsqu'il est question de minimiser le coût des cartes utilisées, le partage n'est pas bénéfique à tout coup. La raison est la suivante : la commutation des protections qui partagent un segment s'effectue dans le domaine électrique. Aux deux extrémités du segment partagé, il faut donc allouer un port à chaque protection qui doit atteindre le MSPP pour être commutée. En conséquence, il arrive qu'il soit moins coûteux pour une protection de ne pas être partagée pour économiser ces ports intermédiaires.

Les deux métriques suivantes sont proposées pour mieux répondre aux particularités de l'objectif étudié dans ce mémoire.

1. *Taux d'occupation des segments d'opération.* Le taux d'occupation d'un segment est calculé en divisant la capacité totale des connexions y voyageant par sa capacité de transport. Plus le taux est grand, plus le segment est utilisé efficacement. En considérant que chaque segment d'opération nécessite deux ports MSPP, une solution de qualité utilisera le plus efficacement possible chacun de ses segments.
2. *Répartition des ports à chaque nœud.* Étudier l'écart entre le nombre de ports d'entrée et de sortie à un nœud permet d'évaluer la qualité de la solution. Idéalement, l'écart devrait être le plus petit possible de telle sorte qu'il y ait le moins de ports

inutilisés. Par contre, surtout pour les ports d'opération, il faut aussi tenir compte de la matrice de trafic. Si par exemple le trafic entrant à un nœud est deux fois plus important que le trafic sortant, on doit s'attendre à un certain excédent de ports d'entrée même dans une très bonne solution.

6.2 Paramètres

Passons maintenant en revue les paramètres qui encadrent l'expérimentation. Les paramètres de la métaheuristique suivront la description des réseaux sur lesquels des expériences seront effectuées.

6.2.1 Réseaux

Pour chacun des trois réseaux qui suivent, 32 longueurs d'onde sont disponibles sur chaque fibre optique.

La majeure partie des expériences sera effectuée sur EON, un réseau européen du milieu des années 1990 dont la topologie est présentée en figure 6.1. On considère des matrices de trafic STS-1, 3, 12 et 48 qui sont asymétriques et générées aléatoirement, pour un total de 2406 connexions. Ces matrices proviennent des travaux de [12].

Le second réseau, NSF (figure 6.2), est plus petit et moins maillé que EON. Les matrices de trafic STS-1, 3, 12 et 48 contiennent au total 1667 connexions et proviennent de la même source que celles de EON.

La topologie du troisième réseau, EON2004, est illustrée à la figure 6.3. Les tronçons noirs représentent la topologie originale, à laquelle on a ajouté les tronçons rouges pour en augmenter la connectivité. Toutes les connexions, au total de 38 873, sont de capacité STS-1. La matrice n'est pas générée aléatoirement : le trafic est inversement proportionnel à la distance entre chaque paire de villes (nœuds) et proportionnel à leur population.

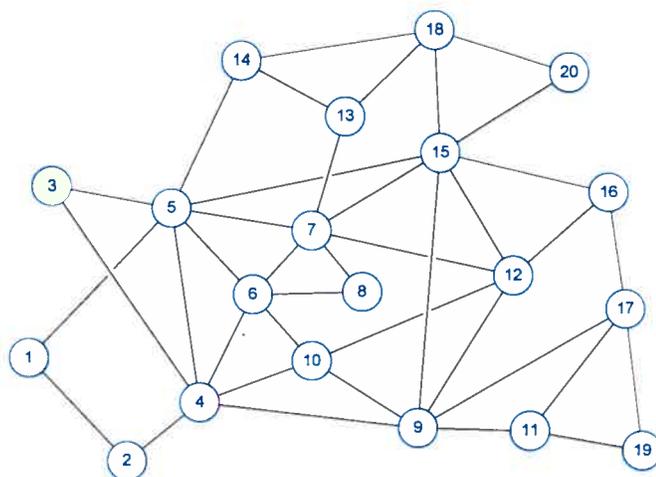


Figure 6.1 – Topologie de EON

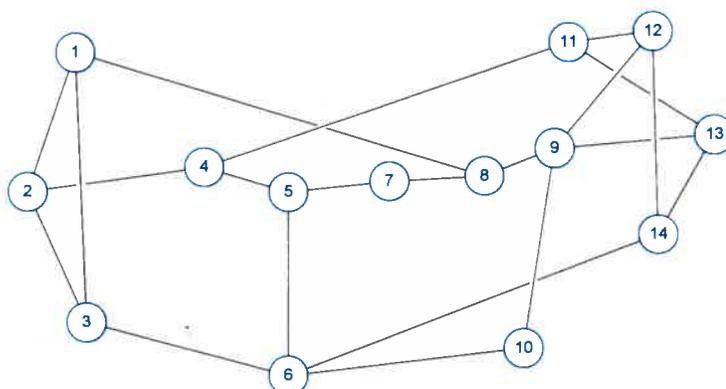


Figure 6.2 – Topologie de NSF

6.2.2 Métaheuristique

Le tableau 6.1 recense les paramètres de la métaheuristique ainsi que la valeur numérique qui leur est affectée. Aucune justification du choix de ces valeurs n'est par contre donnée, au-delà de mentionner que chacune a été ajustée à l'aide d'expériences pratiques.

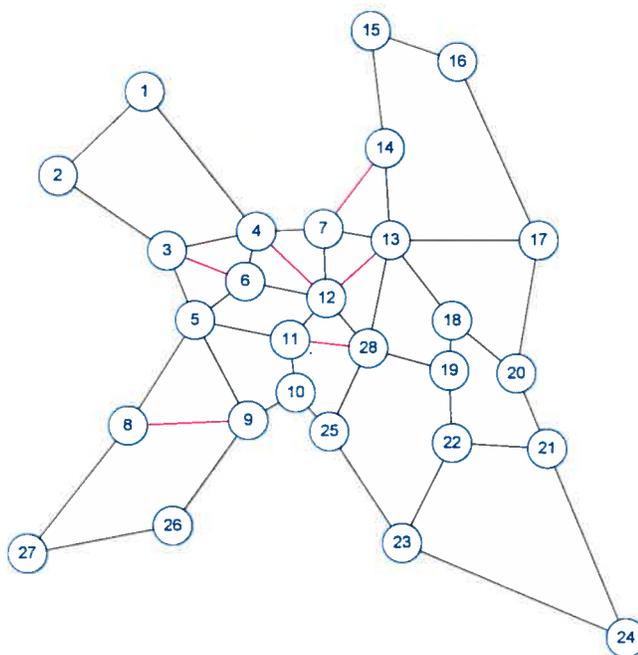


Figure 6.3 – Topologie de EON2004

Paramètre	Valeur numérique
A	150 itérations
L_o	30 %
L_p	20 %
P_o	10 mouvements
P_p	15 mouvements
R_o	20 routes
R_p	45 routes
S_o	5 %
S_p	5 %

Tableau 6.1 – Valeur numérique des paramètres de la métaheuristique

6.3 Résultats et analyse

La présentation des résultats et de leur analyse est divisée en trois sections. D'abord, on compare les stratégies entre elles pour déterminer quelle est la meilleure stratégie d'optimisation séquentielle et d'optimisation conjointe. Ensuite, on compare les

meilleures stratégies de chaque approche (section 6.3.2) pour conclure si l'optimisation conjointe permet ou non d'obtenir une solution à moindre coût que l'optimisation séquentielle. Finalement, une étude plus poussée de la meilleure approche est effectuée pour juger de la performance de la métaheuristique (section 6.3.3).

Sauf indication contraire, les résultats présentés concernent le réseau EON. Les deux autres réseaux serviront fondamentalement à corroborer les résultats obtenus avec EON.

6.3.1 Comparaison des stratégies

Avant de comparer les stratégies entre elles, référons-nous au tableau 6.2 qui présente le nombre d'itérations et le temps d'exécution nécessaires pour atteindre le critère d'arrêt selon la stratégie. Ces résultats ont été obtenus avec un ordinateur pourvu d'un processeur x86 cadencé à 2 GHz et d'un gigaoctet de mémoire vive.

Stratégie	Nombre d'itérations	Temps d'exécution (s)
S1	534	167
S2	966	224
C1	869	457
C2	1875	524

Tableau 6.2 – Temps d'exécution de la métaheuristique selon la stratégie

On observe que les temps d'exécution varient entre 2 et 9 minutes mais qu'ils ne sont pas directement proportionnels au nombre d'itérations. Remarquons que les stratégies utilisent plus d'un mouvement et que ceux-ci diffèrent pour chaque stratégie. En conséquence, une échelle d'itérations permet d'illustrer l'évolution d'une solution au fil des mouvements mais on ne peut y rattacher un temps d'exécution.

Voici des moyens mnémoniques pour se remémorer les caractéristiques de chaque stratégie qui seront maintenant comparées :

- S → séquentiel, C → conjoint ;
- 1 → raffinement, 2 → recherche tabou (protection).

6.3.1.1 Optimisation séquentielle

La figure 6.4 illustre l'évolution du coût au fil des itérations de la métaheuristique pour les deux stratégies d'optimisation séquentielle. Le coût total n'est présenté qu'à partir de l'itération 531, car auparavant le réseau n'est pas protégé.

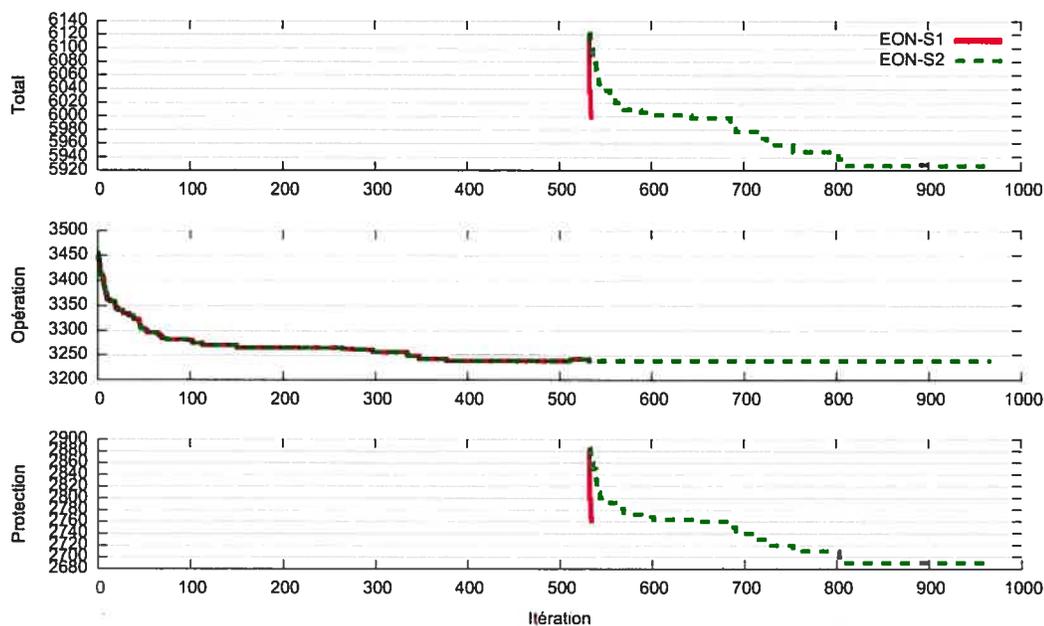


Figure 6.4 – Évolution du coût (k\$) pour l'optimisation séquentielle

Puisque les stratégies sont identiques pour l'opération, elles atteignent le même coût après 530 itérations (3238 k\$).

Pour la protection, le raffinement de S1 diminue le coût d'environ 120 k\$ par rapport à la solution initiale. De son côté, S2 plafonne une première fois au même coût pour ensuite descendre jusqu'à 2690 k\$. La méthode de recherche tabou réussit donc à se sortir de l'optimum local suite au premier plafonnement et S2 obtient de meilleurs résultats par une marge de 2 % pour la protection et 1 % au total.

6.3.1.2 Optimisation conjointe

Étudions le comportement des deux stratégies d'optimisation conjointe en figure 6.5.

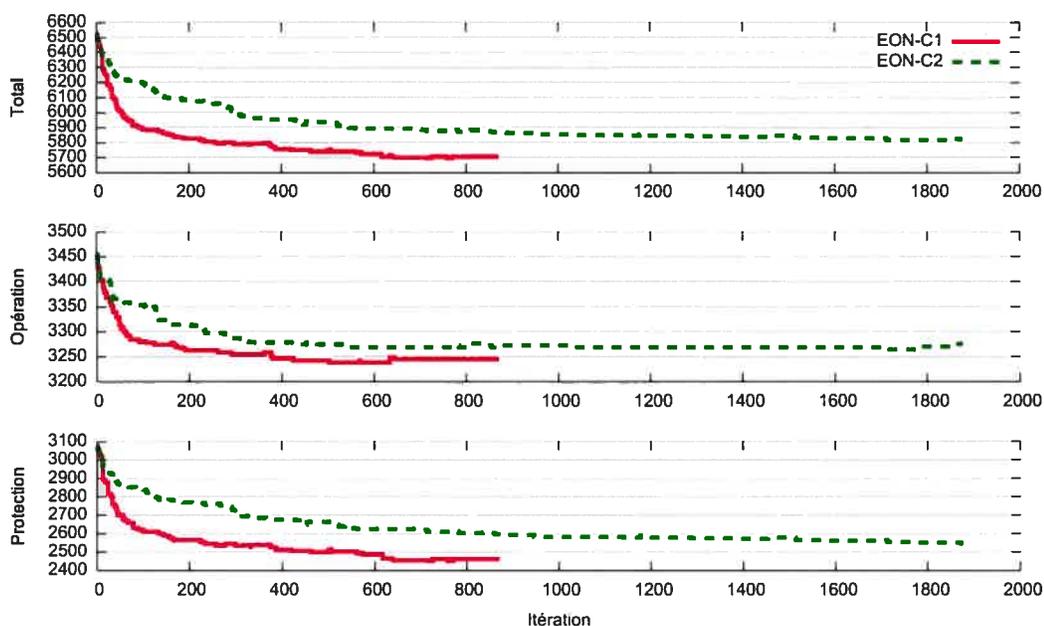


Figure 6.5 – Évolution du coût (k\$) pour l'optimisation conjointe

On observe que C2 requiert beaucoup plus d'itérations que C1 pour converger. Au-delà de l'itération 600, les coûts d'opération sont semblables (une différence de 22 k\$). Mais l'écart demeure plus considérable pour la protection, soit 100 k\$. Globalement, on préfère la stratégie C1 à C2 car elle donne un coût 2 % inférieur. De plus, C1 a un plus court temps d'exécution que C2.

6.3.2 Comparaison des approches

On est maintenant en mesure de comparer la meilleure stratégie séquentielle (S2) et la meilleure stratégie conjointe (C1) pour déterminer la meilleure approche. La figure 6.6 présente l'évolution du coût pour chacune d'elle, toujours sur le réseau EON.

Tandis que les deux approches atteignent à peu près le même coût d'opération, l'approche séquentielle protège le réseau pour un coût d'environ 2700 k\$ alors que l'approche conjointe le fait au coût de 2450 k\$, une différence de 9 %.

Nous verrons prochainement ce qui peut expliquer ce comportement. Mais avant,

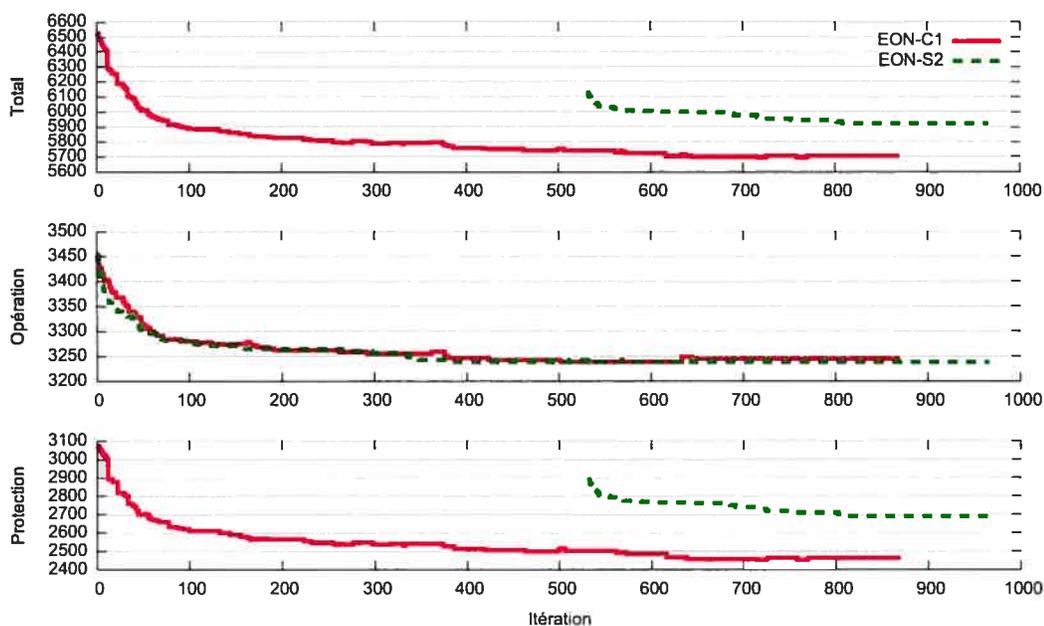


Figure 6.6 – Évolution du coût (k\$) pour les meilleures stratégies

il est intéressant de corroborer ces résultats par des expériences sur d'autres réseaux. Le tableau 6.3 présente donc une comparaison du coût des approches séquentielle et conjointe sur EON, NSF et EON2004.

Approche	EON	NSF	EON2004
Séquentielle	5928	3852	6492
Conjointe	5694 (-4 %)	3820 (-1 %)	6032 (-7 %)

Tableau 6.3 – Comparaison du coût (k\$) des approches

Pour EON, l'écart de 9 % au niveau de la protection se traduit au total par un avantage de 4 % de l'approche conjointe. Pour NSF, un réseau plus petit, la différence est minime (1 %) mais favorise encore l'optimisation conjointe. Finalement, sur EON2004, le plus gros des trois réseaux, l'écart atteint 7 % toujours dans le sens favorable à l'optimisation conjointe.

Pour tenter de mieux comprendre ce qui fait en sorte que l'approche conjointe réussit mieux que l'approche séquentielle, on s'attarde à trois aspects des meilleures solutions

obtenues dans chaque cas. La figure 6.7 illustre le premier de ces aspects, c'est-à-dire la répartition des connexions et protections par longueur.

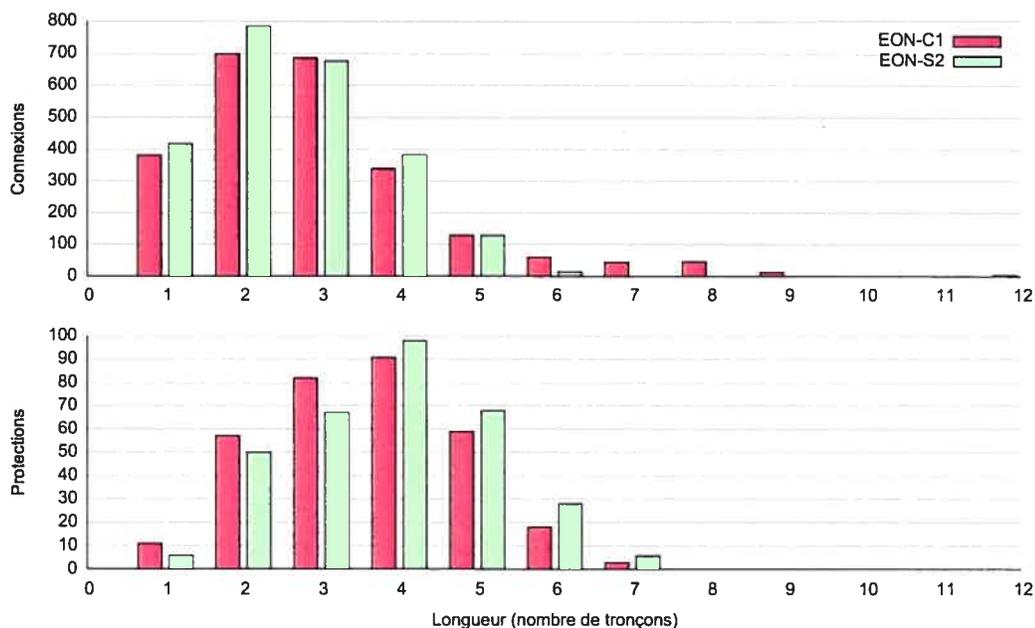


Figure 6.7 – Répartition des connexions et protections par longueur

Tandis que la solution C1 a plus de protections courtes (longueur 1, 2 et 3), elle a en même temps plus de connexions longues (longueur 6, 7, 8 et 9). On peut l'expliquer par le mouvement de raffinement de l'approche conjointe. En général, la route à moindre coût la plus courte est choisie pour placer la connexion. Ainsi, les protections qui doivent emprunter une route disjointe se retrouvent généralement sur une plus longue route. Mais le mouvement *Déplacer un segment d'opération* de la stratégie C1 recherche d'abord une protection en commençant par les routes les plus courtes, pour ensuite placer le segment d'opération. Résultat, l'approche conjointe donne un plus petit coût global en privilégiant à l'occasion la protection, ce qui rend les protections en moyenne plus courtes et les connexions plus longues.

Le deuxième aspect, le taux de partage des segments de protection, est représenté en figure 6.8.

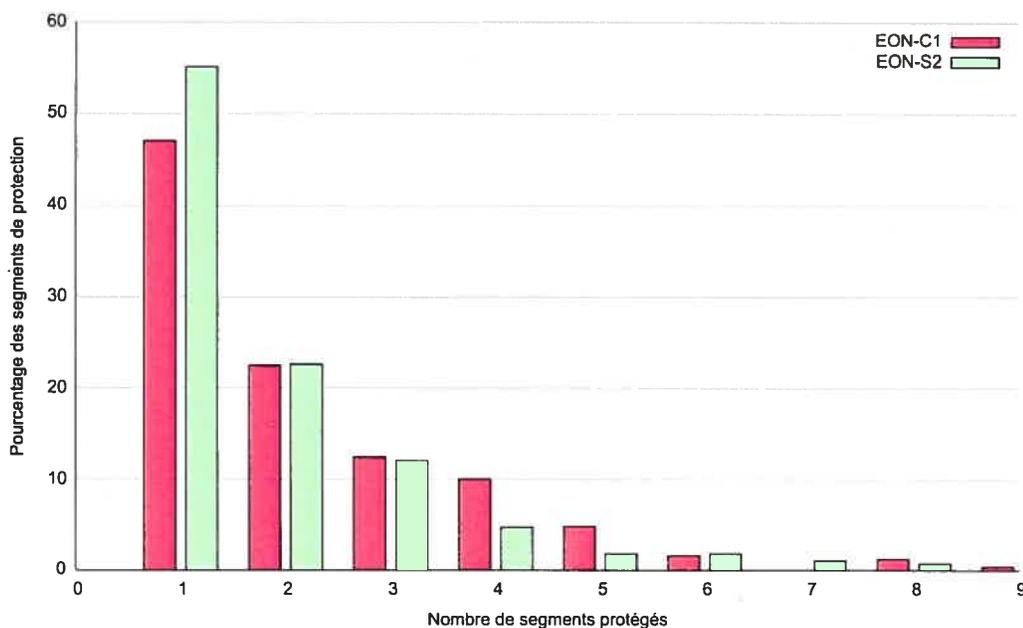


Figure 6.8 – Taux de partage des segments de protection

On observe que 55 % des segments ne sont pas partagés dans la solution S2, contre moins de 50 % pour C1. Aussi, la solution C1 a plus de segments qui sont partagés entre 3, 4 et 5 protections. Encore une fois, l'optimisation conjointe tire profit du mouvement qui permet de placer les segments d'opération pour améliorer le partage et réduire le coût de protection.

En troisième lieu, on s'intéresse au nombre de segments non protégés suite à une rupture d'un tronçon, pour quantifier la vulnérabilité à une seconde contingence. Lorsqu'un tronçon est rompu, trois familles de segments ne sont plus protégés :

1. ceux dont la protection empruntait le tronçon ;
2. ceux qui étaient sur le tronçon et qui doivent basculer à leur protection ;
3. ceux dont la protection partagée a été utilisée par les segments de la deuxième famille.

Quoique cet aspect n'a été pris en compte ni dans la description du problème ni dans le développement de la métaheuristique, il est intéressant de voir si le plus petit coût de

la solution C1 vient avec une pénalité à un autre niveau.

La figure 6.9 montre le nombre de segments non protégés suite à une rupture de chaque tronçon.

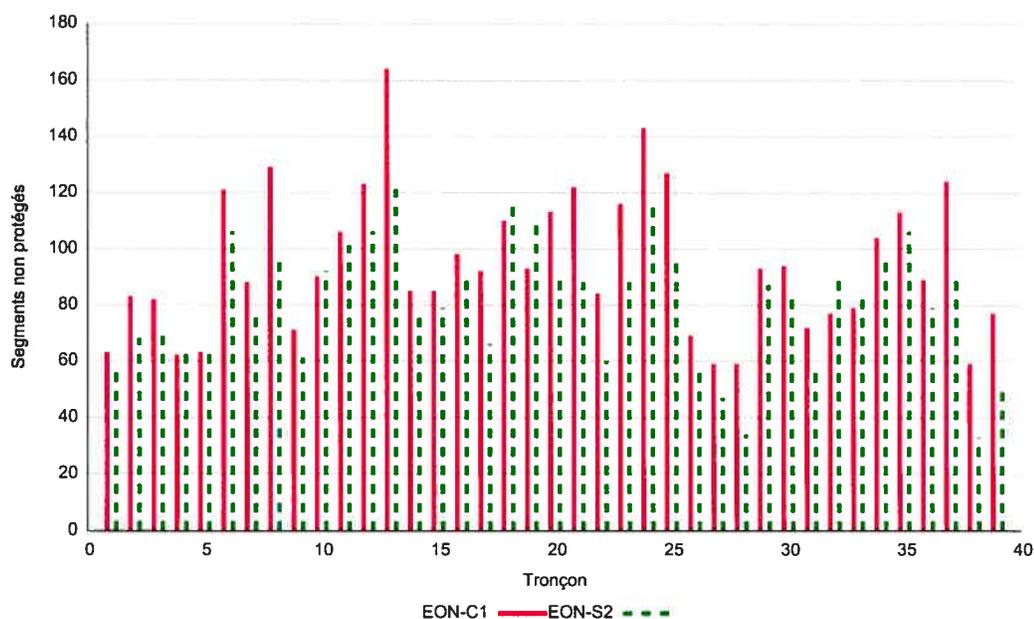


Figure 6.9 – Segments non protégés suite à une rupture de chaque tronçon

Pour la presque totalité des tronçons, c'est la solution C1 qui en a le plus. En moyenne, on parle de 94 segments pour l'approche conjointe et 81 pour l'approche séquentielle, sur un total d'environ 320 segments d'opération. On peut donc conclure que, bien que l'approche conjointe donne un coût total 4 % inférieur, elle est plus vulnérable à une seconde contingence par une marge de 16 %.

6.3.3 Performance

Passons maintenant à l'étude de la performance de la métaheuristique, en évaluant la qualité de la meilleure solution (stratégie C1). Le tableau 6.4 présente le coût et l'amélioration de la solution par la métaheuristique.

En première ligne du tableau, on retrouve le coût d'une solution initiale avec la route

Solution	Opération	Protection	Total
Route la plus courte	3990	4426	8416
C1 initiale	3454 (-13 %)	3074 (-31 %)	6528 (-22 %)
C1 finale	3244 (-6 %)	2450 (-20 %)	5694 (-13 %)

Tableau 6.4 – Coût (k\$) et amélioration de la solution par la métaheuristique

la plus courte pour chaque connexion et protection. L'algorithme de programmation dynamique est tout de même utilisé pour choisir la meilleure séquence de longueurs d'onde sur cette route. Sur la deuxième ligne, on constate le gain obtenu par la solution initiale de C1. Dans ce cas, les 20 routes réalisables les plus courtes sont considérées pour l'opération, et les 45 plus courtes pour la protection. Le coût est alors réduit de près du tiers pour la protection et de 22 % globalement. Finalement, la méthode de recherche tabou (solution C1 finale) permet de réduire le coût davantage : 20 % pour la protection et 13 % au total par rapport à la solution C1 initiale.

On tire deux conclusions de ces résultats.

1. La performance de la méthode de recherche tabou est intéressante. Une réduction du coût de près de 1 M\$ par rapport à la solution C1 initiale est sûrement la bienvenue si on est prêt à accorder quelques minutes à l'exécution de la métaheuristique.
2. La solution par la route la plus courte n'est pas nécessairement de bonne qualité. Plusieurs travaux dans le domaine supposent, pour simplifier le problème, que les connexions ou protections sont placées sur la route la plus courte. Pour le problème qui nous intéresse, on peut gagner plus de 20 % simplement en évaluant plusieurs routes, ce qui est considérable. En conséquence, si on ne désire pas attendre quelques minutes pour la solution finale, la solution initiale donne déjà en quelques secondes un bien meilleur coût que celle par la route la plus courte.

La métaheuristique est aussi efficace : augmenter considérablement le temps d'exécution en multipliant le critère d'arrêt par 10 (de 150 à 1500 itérations sans amélioration) ne réduit le coût de la solution que de 2 %. Ce résultat reflète en même temps la qualité

de la solution obtenue car il est difficile de l'améliorer significativement.

Revenons maintenant aux métriques discutées en section 6.1.2. La figure 6.10 illustre la répartition des segments d'opération par capacité occupée. À noter que les segments OC-192 occupés à pleine capacité, au nombre d'une centaine, en sont exclus afin d'augmenter la lisibilité.

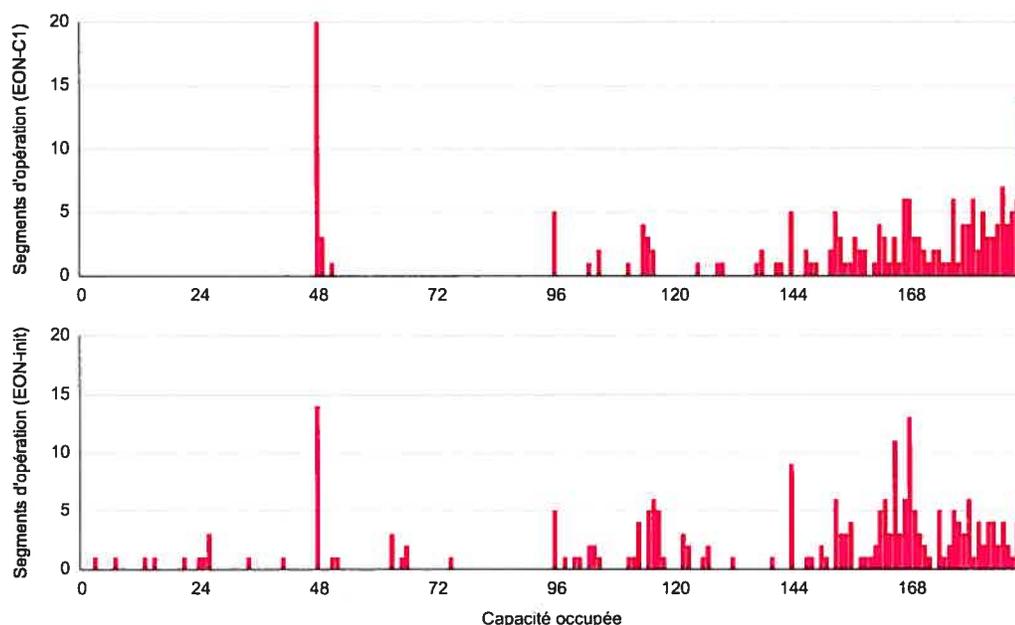


Figure 6.10 – Répartition des segments d'opération par capacité occupée

Le taux d'occupation de la solution initiale (graphique du bas) est de 86 %, tandis que celui de la solution finale (haut) atteint 91 %. Graphiquement, cet écart s'observe par une meilleure utilisation des segments OC-48. En effet, tous les segments OC-48 de la solution finale sont remplis à pleine capacité. De plus, on remarque une plus grande concentration des segments OC-192 vers la pleine utilisation.

La deuxième métrique, soit la répartition des ports à chaque nœud, est présentée en figure 6.11. Les courbes indiquent le nombre de ports aux nœuds, et la surface colorisée représente l'écart entre les ports d'entrée et les ports de sortie à chaque nœud.

En général, peu de ports d'opération OC-192 demeurent inutilisés, à l'exception des

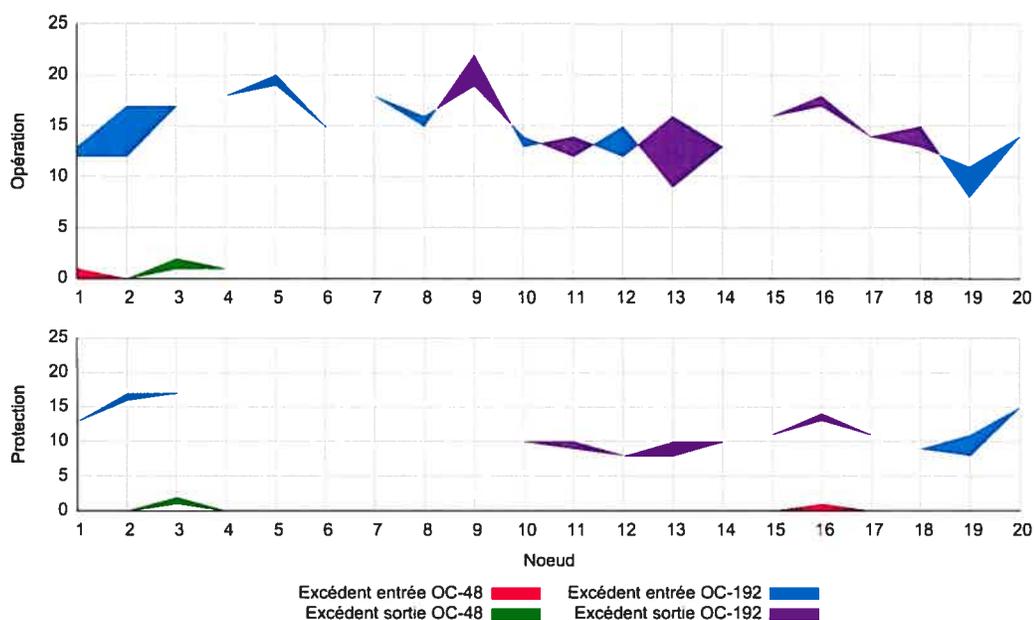


Figure 6.11 – Répartition des ports à chaque nœud

nœuds 2 et 13 qui ont respectivement un excédent de 5 en entrée et 7 en sortie. Mais ces excédents s'avèrent tout à fait raisonnables si l'on considère que trois fois plus de trafic est destiné au nœud 2 qu'il en provient, et que le ratio sortie à entrée au nœud 13 est de 2 : 1.

Pour ce qui est de la protection, c'est le partage qui permet de réduire le nombre de ports inutilisés malgré le déséquilibre plus important des ports d'opération. On retrouve en effet des ports OC-192 inutilisés à seulement 5 des 20 nœuds du réseau.

Ce graphique permet en même temps d'observer que la grande majorité des segments sont de capacité OC-192. Comme on l'avait vu, les cartes OC-192 sont moins coûteuses par unité de capacité que les OC-48, et la métaheuristique en a tiré profit.

Finalement, on fait un retour sur la vulnérabilité du réseau à une seconde contingence. Parmi les 3 familles de segments qui ne sont plus protégés suite à une rupture de fibre, ce sont les protections partagées qui jouent un rôle dominant car pour chaque segment d'opération qui doit basculer sur sa protection partagée, plusieurs autres segments

perdent leur protection. Observons alors ce qui se produit si l'on interdit le partage de la protection (figure 6.12).

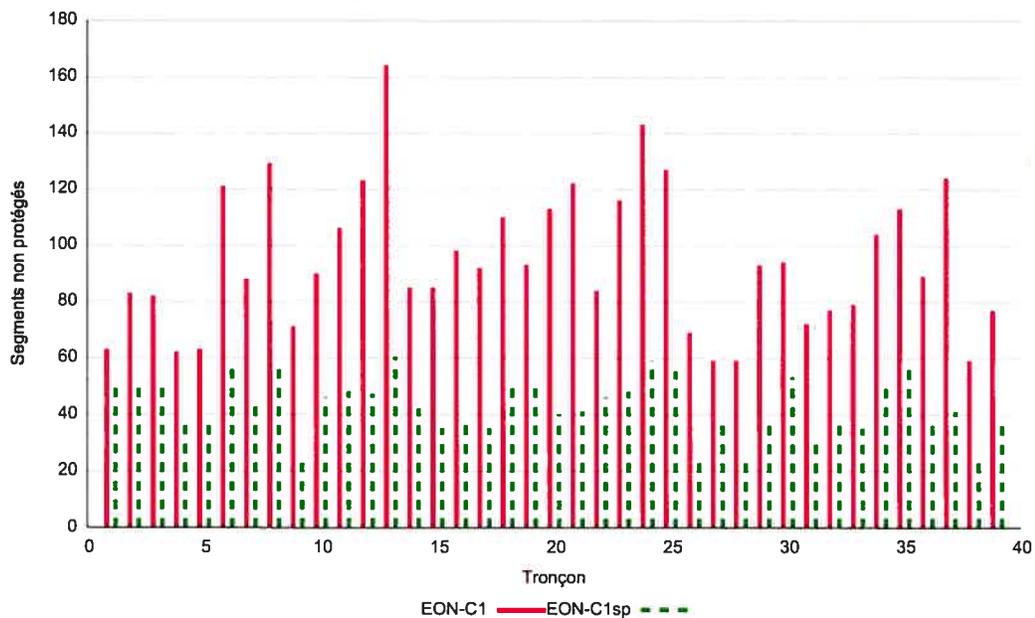


Figure 6.12 – Segments non protégés suite à une rupture de chaque tronçon

Contrairement à l'écart entre la solution C1 et S2 qui était de 16 %, celui entre C1 et C1sp (sans partage) est beaucoup plus important : 94 segments en moyenne pour C1 contre 43 pour C1sp. Ceci confirme que le partage de la protection accroît considérablement la vulnérabilité du réseau à une seconde contingence (119 % dans le cas présent). D'autre part, au moins un segment est nécessaire par protection lorsque le partage est interdit, ainsi le coût de protection ne peut être inférieur au coût d'opération. En conséquence, au lieu d'avoir un coût de protection 25 % inférieur au coût d'opération (solution C1), il sera au minimum égal, ce qui est cher payé pour une plus grande robustesse à une seconde contingence.

CHAPITRE 7

CONCLUSION

La démarche poursuivie par ce mémoire s'inscrit dans le contexte où la protection des réseaux optiques WDM avec l'objectif de minimisation du coût des cartes MSPP n'avait pas encore été explorée. Pour s'attaquer à ce problème, la protection par segment a été préférée à la protection par connexion. Étant donné qu'il était trop coûteux en temps d'obtenir une solution optimale ou du moins une borne intéressante, on a préféré développer une métaheuristique qui obtient en quelques minutes une solution de qualité.

En tout état de cause, les trois objectifs énumérés au chapitre 3 ont été atteints.

1. Une métaheuristique qui résout conjointement et séquentiellement les problèmes GRWA et protection par segment a été développée avec succès et proposée au chapitre 5. De plus, la réalisabilité ainsi que la qualité des solutions obtenues ont été validées au cours de l'expérimentation.
2. Une attention spéciale a été portée à l'efficacité de la métaheuristique (section 5.4). En particulier, l'algorithme de programmation dynamique évalue toutes les combinaisons de longueurs d'onde sur une route en un temps très court. Puisque cet algorithme est au centre de la métaheuristique, son efficacité a permis de développer des mouvements plus complexes tout en gardant un temps d'exécution raisonnable de quelques minutes.
3. Les approches conjointe et séquentielle ont été comparées en section 6.3.2. Cette comparaison a permis de répondre à la question de recherche et ainsi de vérifier l'hypothèse : *l'optimisation conjointe permet en effet d'obtenir une solution à coût moindre que l'optimisation séquentielle*. On a vu que la stratégie C1 (approche conjointe) tire profit du mouvement *Déplacer un segment d'opération* pour privilégier à l'occasion la protection. En conséquence, les protections sont en moyenne plus courtes, les connexions plus longues, le taux de partage plus élevé, et surtout

le coût des cartes plus bas. Autre conclusion de la comparaison : quoique la solution de l'approche conjointe soit moins coûteuse, elle est plus vulnérable à une seconde contingence.

Le concept de vulnérabilité à une seconde contingence a été introduit au cours de l'expérimentation, mais n'a pas été pris en compte dans le développement de la méta-heuristique. Il s'agit toutefois d'une préoccupation des gestionnaires d'un réseau lors de son dimensionnement. Puisque l'optimisation conjointe a permis d'obtenir une solution à moindre coût, il est à se demander si l'on pourrait également en tirer profit pour rendre le réseau plus robuste à une seconde contingence. Deux objectifs pourraient être considérés : minimiser le coût en préférant une solution moins vulnérable, ou encore minimiser simultanément le coût et la vulnérabilité. Le travail à effectuer serait divisé en deux étapes.

1. Définir précisément la vulnérabilité à minimiser. Ce pourrait être par exemple la quantité moyenne de segments non protégés suite à une première contingence sur un tronçon, ou encore la capacité moyenne des connexions non protégées.
2. Élaborer une stratégie qui profite de l'optimisation conjointe pour minimiser la vulnérabilité à une seconde contingence. Le mouvement *Déplacer un segment d'opération* pourrait être modifié pour prévoir une protection qui réduit la vulnérabilité en plus du coût.

Autre perspective d'avenir, les p-Cycles constituent un schéma de protection qu'il serait intéressant d'étudier lors de travaux futurs. Il a été observé que ceux-ci se forment naturellement pour la protection d'un réseau avec l'objectif de minimiser la capacité totale utilisée [10]. Par contre, il est difficile de prévoir si le même comportement serait observé avec l'objectif de minimisation du coût des cartes MSPP. Des essais préliminaires ont été effectués en ce sens. Il a d'abord été tenté de trouver des p-Cycles à même les solutions générées lors de l'expérimentation. En vain, très peu ont été identifiés. Il a aussi été tenté de construire une solution initiale à base de p-Cycles. Malheureusement,

le processus s'est révélé ardu et la solution n'était à prime abord pas très intéressante en raison de son coût trop élevé. On conclut que le concept de p-Cycles n'est pas simple à intégrer à la minimisation du coût des cartes. Les résultats obtenus ne sont donc pas très significatifs, et un travail de plus grande envergure devrait être entrepris pour juger du réel potentiel des p-Cycles.

BIBLIOGRAPHIE

- [1] Manon Bélanger. Validation de la réalisabilité des chemins de protection. Communication personnelle, 2005. Stage étudiant.
- [2] I. Chlamtac, A. Ganz et G. Karmi. Purely optical networks for terabit communication. Dans *Proceedings of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 1989)*, volume 3, pages 887–896, 1989.
- [3] Cisco Systems. Cisco multiservice SONET/SDH product migration and strategy. White Paper, 2003.
- [4] Jing Fang et A.K. Somani. Enabling subwavelength level traffic grooming in survivable WDM optical network design. Dans *IEEE Global Telecommunications Conference (GLOBECOM 2003)*, volume 5, pages 2761–2766, 2003.
- [5] Pierre-Marc Fournier. Validation de la réalisabilité des chemins d’opération. Communication personnelle, 2004. Stage étudiant.
- [6] Fred Glover. Tabu search, part I. *ORSA Journal on Computing*, 1:190–206, 1989.
- [7] Fred Glover. Tabu search, part II. *ORSA Journal on Computing*, 2:4–32, 1990.
- [8] Walter Goralski. *SONET/SDH*. Osborne/McGraw-Hill, 3^{ème} édition, 2002.
- [9] Wayne D. Grover. *Mesh-based Survivable Transport Networks : Options and Strategies for Optical, MPLS, SONET and ATM Networking*. Prentice Hall, 2003.
- [10] W.D. Grover et D. Stamatelakis. Cycle-oriented distributed preconfiguration : ring-like speed with mesh-like capacity for self-planning network restoration. Dans *IEEE International Conference on Communications (ICC 1998)*, volume 1, pages 537–543, 1998.

- [11] Jian Qiang Hu. Diverse routing in optical mesh networks. *IEEE Transactions on Communications*, 51(3):489–494, 2003. ISSN 0090-6778.
- [12] B. Jaumard, Y. Solari et A. Houle. Dimensioning WDM optical networks with minimum MSPP configuration. Dans *Optical Communications Systems and Networks (OCSN 2004)*, 2004.
- [13] Richard Marett et Mike Wright. A comparison of neighborhood search techniques for multi-objective combinatorial problems. *Computers and Operations Research*, 23(5):465–483, 1996. ISSN 0305-0548.
- [14] N. Mladenovic et P. Hansen. Variable neighborhood search. *Computers and Operations Research*, 24(11):1097–1100, 1997.
- [15] Canhui Ou, Jing Zhang, Hui Zang, L.H. Sahasrabudde et B. Mukherjee. Near-optimal approaches for shared-path protection in WDM mesh networks. Dans *IEEE International Conference on Communications (ICC 2003)*, volume 2, pages 1320–1324, 2003.
- [16] Canhui Ou, Keyao Zhu, Hui Zang, L.H. Sahasrabudde et B. Mukherjee. Traffic grooming for survivable WDM networks - shared protection. *IEEE Journal on Selected Areas in Communications*, 21(9):1367–1383, 2003. ISSN 0733-8716.
- [17] Rajiv Ramaswami et Kumar Sivarajan. *Optical Networks : A Practical Perspective*. Morgan Kaufmann, 2ème édition, 2001.
- [18] Colin R. Reeves, éditeur. *Modern heuristic techniques for combinatorial problems*. John Wiley & Sons, Inc., New York, NY, USA, 1993. ISBN 0-470-22079-1.
- [19] Lu Shen, Xi Yang et Byrav Ramamurthy. Shared-risk link group (SRLG)-diverse path provisioning under hybrid service level agreements in wavelength-routed optical mesh networks : formulation and solution approaches. Dans *Proceedings of the SPIE OptiComm 2003*, volume 5285, pages 126–138. SPIE, 2003.

- [20] Dahai Xu, Yizhi Xiong et Chunming Qiao. Novel algorithms for shared segment protection. *IEEE Journal on Selected Areas in Communications*, 21(8):1320–1331, 2003. ISSN 0733-8716.
- [21] Xi Yang, Lu Shen et Byrav Ramamurthy. Survivable lightpath provisioning in WDM mesh networks under shared path protection and signal quality constraints. *Journal of Lightwave Technology*, 23:1556–1567, 2005.
- [22] Wang Yao et B. Ramamurthy. Survivable traffic grooming with path protection at the connection level in WDM mesh networks. Dans *First International Conference on Broadband Networks (BroadNets 2004)*, pages 310–319, 2004.
- [23] Wang Yao et B. Ramamurthy. Survivable traffic grooming in WDM mesh networks under SRLG constraints. Dans *IEEE International Conference on Communications (ICC 2005)*, volume 3, pages 1751–1755, 2005.
- [24] Keyao Zhu et B. Mukherjee. Traffic grooming in an optical WDM mesh network. *IEEE Journal on Selected Areas in Communications*, 20(1):122–133, 2002. ISSN 0733-8716.