

UNIVERSITÉ DE MONTRÉAL

MÉCANISMES D'ALLOCATION DE RESSOURCES ET FIABILITÉ
DANS LES RÉSEAUX CŒUR DE PROCHAINES GÉNÉRATIONS

HICHEM AYED HARHIRA
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIAE DOCTOR (Ph.D.)

(GÉNIE INFORMATIQUE)

JANVIER 2009



Library and
Archives Canada

Bibliothèque et
Archives Canada

Published Heritage
Branch

Direction du
Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

ISBN: 978-0-494-48889-8

Our file Notre référence

ISBN: 978-0-494-48889-8

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée :

**MÉCANISMES D'ALLOCATION DE RESSOURCES ET FIABILITÉ
DANS LES RÉSEAUX CŒUR DE PROCHAINES GÉNÉRATIONS**

présentée par : HARHIRA Hichem Ayed

En vue de l'obtention du diplôme de : Philosophiae Doctor

a été dûment acceptée par le jury d'examen constitué de :

Mme. BOUCHENEB Hanifa, Doctorat, présidente

M. PIERRE Samuel, Ph.D., membre et directeur de recherche

M. QUINTERO Alejandro, Doct., membre

M. MOUFTAH Hussein, D.Sc., membre

*À mes chers parents
À ma chère femme
À ma chère fille Chaima
À mes frères et ma sœur*

REMERCIEMENTS

Ma reconnaissance va en premier à ma mère et à mon père dont l'éducation, la confiance, l'appui moral et financier m'ont permis de m'épanouir. Je suis également fort reconnaissant à ma femme qui a supporté mes humeurs changeantes avec dévouement et attention. À mes frères Tarek et Mohamed et à ma sœur Fatma, je dis merci pour tous ces moments où vous m'avez fait ressentir la chaleur fraternelle.

Je remercie également M. Samuel Pierre, mon directeur de recherche, dont l'encadrement et les conseils m'ont guidé tout au long de ma recherche.

À tous mes amis et mes collègues au LARIM, je dis merci pour l'ambiance chaleureuse et enrichissante du laboratoire.

ABSTRACT

Nowadays, telecommunication networks are no more intended to support a unique type of traffic (Voice, data, etc.). We are however attending to a gradual convergence of different services and applications to be supported by a common network infrastructure. Nevertheless, the heterogeneity of the actual infrastructures and access technologies (*DOCSIS*, *xDSL*, 802.11, 802.16, etc.) makes their integration challenging. This has motivated the international standardization groups to propose and adopt new standards and network architectures offering a logical and functional separation between the forwarding technologies and the services, and a compliance with several access technologies. Among the layers of the *TCP/IP* stack, the *IP* technology is the most suited to tackle the interoperability issues for next generations networks (*NGNs*). This technology is however designed to convey best-effort traffic and thus not intended to support multimedia and real-time applications having strict end-to-end Quality of Service (*QoS*) requirements.

This problem is all the more important as new applications, having more stringent *QoS* requirements come into sight. In such a scenario, optical networks embedded with the Wavelength-Division Multiplexing (*WDM*) technology is a key feature to provide high-capacity and cost-effective transport networks, compliant with higher level protocols and architectures.

In this thesis, we focus on the problem of resource allocation in *IP* based core networks. This theme implies the long-term resources allocation mechanisms, i.e., global resources optimization performed cyclically or due to a particular event

(failures or congestion) as well as admission control mechanisms ensuring, on a greedy fashion, the resources availability and the required *QoS*. Several architectures and control mechanisms were proposed in the literature involving resources allocation and *QoS* support. Nevertheless, such architectures are not well suited to Next Generations Networks, mainly characterized by the standardization and centralization of the control plane. For that, we address the following problems: admission control with *QoS* support in *MPLS* and *GMPLS* multi-layer networks; survivable routing in *WDM* optical networks. The body of this thesis encompasses three journal papers.

In the first paper, we propose a novel mechanism of routing and admission control in *GMPLS* based optical networks with *QoS* guarantees. As *GMPLS* technology is considered, routing new *IP* traffics involves different mechanisms at different network layers. In this first paper, we present a centralized algorithm that routes *IP* traffic considering the potential signal power penalty of all-optical communications. This algorithm consists of resolving to optimality an Integer Linear Programming model that routes the new *LSP* so that the signal quality and propagation delay constraints are guaranteed. In order to minimize the *LSP*'s set-up delay, the algorithm first tries to route the request over a subset of ongoing lightpaths. If no feasible path is available, a new lightpath is set up, involving free wavelengths over the physical fibers. Simulation results show that our mechanism outperforms other mechanisms presented in the literature, while having low computation delays.

The second paper addresses the problem of routing and admission control of new *LSPs* in *MPLS* networks with statistical delay and jitter constraints. For that, we first propose an upper-bound on the end-to-end delay and jitter constraints. We then propose a new admission control mechanism in *MPLS*-based networks. This mechanism is based on formulating the problem as an Integer Linear Programming model that performs both the routing and the admission control of the new

connections, taking into account the statistical bounds on the end-to-end delay and jitter.

Finally, our third paper tackles the problem of Survivable Multicast Routing under *SRLG* constraints. Depending on the reliability requirements of the incoming requests, statistical survivability guarantees are offered. For that, we first formulate the problem as an Integer Linear Programming model that is shown NP-Complete. We then propose an algorithm that alleviates the problem's complexity by decomposing it into two sub-problems. Simulations confirm that our algorithm provides for acceptable results and highlight the benefits of considering the differentiated reliability.

RÉSUMÉ

De nos jours, les réseaux des télécommunications ne sont plus dédiés au transport d'un seul type d'application ou de trafic (voix, données, etc.). Nous assistons en effet à une convergence graduelle des différents services pour être supportés par une infrastructure de réseau commune. Toutefois, l'hétérogénéité des infrastructures et des technologies d'accès (*DOCSIS*, *xDSL*, 802.11, 802.16, etc.) suscite un intérêt particulier pour leur intégration et leur interopérabilité. Ceci a incité les groupes internationaux de normalisation à proposer et adopter de nouveaux standards et architectures de réseaux offrant d'une part une séparation logique et fonctionnelle entre le transport, les services et les applications et d'autre part le support de plusieurs technologies d'accès et l'indépendance de l'accès avec le type de service offert. Parmi les couches de la pile de protocoles *TCP/IP*, la technologie *IP* est celle qui a été adoptée par les réseaux de prochaines générations afin d'assurer la convergence des différents services et technologies d'accès. La technologie *IP*, initialement dédiée au transport à moindre effort (*best-effort*) des données, se voit attribuer la responsabilité de fournir une gestion adéquate de la qualité de service (*QoS*) de bout-en-bout.

La problématique s'accroît davantage si on considère le besoin d'évolutivité des réseaux de prochaines générations, qui devront supporter de plus en plus d'applications avec des besoins grandissants en qualité de service. Dans un tel contexte, les réseaux optiques à multiplexage de longueurs d'ondes constituent une solution clé, offrant une bande passante assez large et à moindre coût.

Ainsi, nous nous intéressons à l'optimisation de l'allocation des ressources dans les réseaux cœur à commutation de paquets *IP*. Cette optimisation implique, d'un côté, des mécanismes de gestion de ressources à long terme, i.e., optimisation périodique des ressources où suite à un évènement particulier (pannes ou congestions) et de l'autre, des mécanismes de contrôle d'admission assurant, d'une manière gloutonne, la disponibilité des ressources et le niveau de service souhaité. Plusieurs mécanismes et architectures ont été proposés dans la littérature permettant de fournir des garanties strictes ou statistiques de *QoS*. Ces architectures ne sont toutefois pas bien adaptées aux réseaux de prochaines générations, caractérisés principalement par l'uniformisation et la centralisation du plan de contrôle et le support de la qualité de service. Dans ce contexte, nous attaquerons les problèmes clés suivants : contrôle d'admission avec *QoS* dans les réseaux *GMPLS* multicouches et *MPLS*; routage fiable dans les réseaux optiques *WDM*. Afin de résoudre ces problèmes, cette thèse est basée sur trois articles adressant chacun une problématique bien spécifique.

Dans le premier article, nous proposons un nouveau mécanisme de routage et de contrôle d'admission dans les réseaux *GMPLS* avec garantie de *QoS* au niveau optique. En effet, vu le caractère multicouche des réseaux *GMPLS*, l'admission d'un nouveau *LSP* (*Label Switched Path*) au niveau *MPLS* implique d'un côté le routage de cet *LSP* à travers la topologie logique formée par les chemins optiques précédemment établis et la vérification que le ou les chemins optiques empruntés respectent certaines contraintes de *QoS*. Le mécanisme proposé envisage également la création de nouveaux chemins optiques, au cas où la topologie logique actuelle ne permet pas d'admettre le nouveau *LSP*. Le mécanisme de routage et de contrôle d'admission proposé est un mécanisme centralisé, basé sur la modélisation mathématique du problème par un programme linéaire en nombres entiers. L'évaluation des performances montre que le mécanisme proposé génère des résultats meilleurs que ceux disponibles dans la littérature.

Le deuxième article traite le problème de contrôle d'admission avec contraintes de délai et de gigue dans les réseaux *MPLS* et propose une nouvelle borne supérieure sur les contraintes de gigue et de délai de bout-en-bout. La borne obtenue est basée sur des données empiriques explicitant l'état instantané du réseau (charge des liens et délais de traitement des paquets, etc.) et permet de fournir des garanties statistiques pour les métriques de *QoS* considérées. En se basant sur le résultat obtenu, nous proposons un mécanisme de contrôle d'admission basé sur la formulation mathématique du problème par un programme linéaire en nombres entiers que nous proposons de résoudre d'une manière exacte avec l'outil de résolution mathématique ILOG CPLEX. Le mécanisme proposé a permis d'améliorer le taux d'acceptation des nouvelles connexions en fournissant les garanties statistiques de *QoS*.

Finalement, le troisième article aborde la problématique de routage fiable dans les réseaux optiques *WDM*. Dans cet article, nous proposons un algorithme de routage *multicast* avec fiabilité différentielle en considérant des groupes de liens à risque partagé ou *SRLGs*. Afin de pallier la complexité du problème présenté, l'algorithme proposé est basé sur une méthode de décomposition qui décortique le problème en deux sous-problèmes résolus séparément. Les résultats de l'algorithme sont initialement comparés aux solutions exactes fournies par ILOG CPLEX, pour de petites instances de tests. Une évaluation comparative des performances a également été conduite et a permis, entre autres, de confirmer l'avantage de considérer la fiabilité différentielle.

TABLE DES MATIÈRES

DÉDICACES	iv
REMERCIEMENTS	v
ABSTRACT	vi
RÉSUMÉ	ix
TABLE DES MATIÈRES	xii
LISTE DES FIGURES.....	xvi
LISTE DES TABLEAUX.....	xviii
LISTE DES SIGLES ET ABRÉVIATIONS	xix
 CHAPITRE 1 INTRODUCTION.....	 1
1.1 Définitions et concepts de bases	2
1.2 Eléments de problématique.....	8
1.3 Objectifs de recherche.....	11
1.4 Principales contributions.....	12
1.5 Plan de la thèse.....	15
 CHAPITRE 2 REVUE DE LITTÉRATURE	 17
2.1 Modèles de services	18
2.1.1 Services intégrés (<i>IntServ</i>)	18
2.1.2 Services différenciés (<i>DiffServ</i>)	19
2.1.3 Notion de <i>Stateless Core</i>	20
2.2 Routage avec Qualité de Service.....	20
2.2.1 Protocoles à commutation d'étiquettes (<i>MPLS</i>).....	21
2.2.2 Ingénierie de trafic avec MPLS.....	22

2.2.3	Generalized <i>MPLS</i>	22
2.2.4	Routage multi-chemin	23
2.2.5	Protocole de routage utilisant plusieurs métriques	23
2.3	Ingénierie de trafic	24
2.4	Contrôle d'admission avec Qualité de Service	27
2.4.1	Contrôle d'admission dans un domaine <i>DiffServ</i>	30
2.4.2	Contrôle d'admission dans les réseaux multicouches <i>GMPLS</i>	32
2.5	Fiabilité des réseaux	34
2.5.1	Mécanismes de fiabilité dans les réseaux optiques	35
2.5.2	Fiabilité dans les réseaux optiques avec ressources à risque partagé..	37
CHAPITRE 3 A NOVEL ADMISSION CONTROL MECHANISM IN GMPLS- BASED IP OVER OPTICAL NETWORKS		40
3.1	Introduction	41
3.2	Problem Statement	45
3.2.1	Node model	45
3.2.2	End-to-end delay	46
3.2.3	Signal quality	46
3.2.4	Mathematical formulation	47
3.3	Numerical Results	52
3.4	Conclusion	58
CHAPITRE 4 JOINT ROUTING AND ADMISSION CONTROL PROBLEM UNDER STATISTICAL DELAY AND JITTER CONSTRAINTS IN MPLS NETWORKS		59
4.1	Introduction	60
4.2	Related Works	61
4.3	Problem Statement	64
4.3.1	The end-to-end delay distribution: mean and variance computation ..	67

4.3.2	End-to-end jitter and delay constraints	67
4.3.3	Approximating the new delay distribution after the admission of a new flow	69
4.3.4	Admission control mathematical formulation.....	72
4.4	Simulation Results	76
4.5	Conclusion	81
CHAPITRE 5 A SURVIVABLE MULTICAST ROUTING MECHANISM IN WDM OPTICAL NETWORKS		83
5.1	Introduction	84
5.2	Survivable Routing Under SRLG Constraints	87
5.2.1	SRLG Sharing	87
5.2.2	Resources sharing.....	88
5.2.3	Problem Statement	89
5.2.4	Network Reliability and Failure Probability	91
5.2.5	Mathematical Formulation	92
5.3	GR-SMRS: Greedy Heuristic for Survivable Multicast Routing under SRLG constraints	95
5.3.1	Complexity Analysis of GR-SMRS	100
5.4	Simulation Results	101
5.4.1	Comparative Results: CPLEX vs. <i>GR-SMRS</i>	102
5.4.2	Comparative Results: <i>GR-SMRS</i> vs. <i>MSS</i>	105
5.5	Conclusion	109
CHAPITRE 6 DISCUSSION GÉNÉRALE		111
6.1	Synthèse des travaux	111
6.2	Méthodologie	113
6.3	Analyse des résultats	114

CHAPITRE 7	CONCLUSION	115
7.1	Sommaire des contributions.....	116
7.2	Limitations des travaux	117
7.3	Indication des travaux futurs.....	118
CONTRIBUTIONS À LA RECHERCHE		120
BIBLIOGRAPHIE		122

LISTE DES FIGURES

Figure 1.1 Plan de contrôle GMPLS	5
Figure 1.2 La hiérarchie dans un SRLG.....	7
Figure 2.1 Processus d'ingénierie de trafic.....	25
Figure 2.2 Topologie physique avec SRLGs	37
Figure 2.3 Partage des ressources par plusieurs chemins de secours.....	38
Figure 3.1 GMPLS control and forwarding plan	42
Figure 3.2 Construction of the network graph model using the logical and physical topologies	47
Figure 3.3 Comparative results: CPLEX vs. MTQA for a network mean load of 55%	54
Figure 3.4 Comparative results: CPLEX vs. MTQA for a network mean load of 80%.....	55
Figure 3.5 Effect of the number of wavelengths converters in the network on the number of admitted connections	56
Figure 3.6 Effect of the number of wavelengths converters in the network on the percentage of setting up new lightpaths for new LSPs	57
Figure 4.1 Effect of admitting a new connection on the delay's distribution	65
Figure 4.2 Average delay and variance with respect to the link's load	66
Figure 4.3 Jitter violation probability for a given delay's distribution <i>pdf</i>	68
Figure 4.4 Accuracy of the mean delay bound given by Equation (4.5)	71
Figure 4.5 Acceptance rate for an average network load of 60%	77
Figure 4.6 Accepted rate for an average network load of 75%.....	78
Figure 4.7 Accepted rate for an average network load of 90%.....	79

Figure 4.8 Number of accepted connections with respect to the QoS violation probability for the network having 40 Nodes having 60% of load.....	80
Figure 5.1 Risk hierarchy of an SRLG.....	87
Figure 5.2 Example of an SRLG.....	88
Figure 5.3 Example of backup resources sharing	89
Figure 5.4 Auxiliary graph for selecting the routing configurations	97
Figure 5.5 Comparative acceptance rate GR-SMRS vs. CPLEX for PT1	104
Figure 5.6 Comparative acceptance rate GR-SMRS vs. CPLEX for PT1	104
Figure 5.7 Comparative ratios of protected paths	105
Figure 5.8 Comparative acceptance rates for different local reliability requirements with D=3.....	106
Figure 5.9 Comparative acceptance rates for different global reliability requirements with D=3.....	107
Figure 5.10 Comparative acceptance rates for different local reliability requirements with D=7.....	107
Figure 5.11 Comparative acceptance rates for different global reliability requirements with D=7.....	109

LISTE DES TABLEAUX

Table 2.1 Classification des méthodes de contrôle d'admission	30
Table 3.1 Considered physical topologies	54
Table 4.1 Tests used.....	76
Table 5.1 Computation delays	100
Table 5.2 Used physical topologies	101
Table 5.3 Computation delays (ms)	102

LISTE DES SIGLES ET ABRÉVIATIONS

AC	Admission Control
AF	Assured Forwarding
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BP	Backup Path
DiffServ	Differentiated Services
DOCSIS	Data Over Cable Systems
DSCP	DiffServ Code Point
ECMP	Equal Cost MultiPath
EF	Expedited Forwarding
ETRI	European
GMPLS	Generalized MultiProtocol Label Switching
IETF	Internet Engineering Task Force
ILP	Integer Linear programming
IntServ	Integrated Services
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate system
LER	Label Edge Router
LMP	Link Management Protocol
LSP	Label Switched Path
LSR	Label Switch Router
MPLS	MultiProtocol Label Switching
MPLS-TE	MultiProtocol Label Switching-Traffic Engineering Extensions

NGN	Next Generation Networks
NP	Polynomial Non deterministic
OSNR	Optical Signal to Noise Ratio
OSPF	Open Shortest Path First
OXC	Optical Cross Connector
PCE	Path Computation Element
PHB	Per Hop Behaviour
QoS/QdS	Quality of Service/Qualité de Service
QOSPF	QoS Open Shortest Path First
RACS	Resource Allocation and Admission Control Subsystem
RSVP	Reservation Protocol
RSVP-TE	Reservation Protocol-Traffic Engineering Extension
SLA	Service Level Agreement
SRLG	Shared Risk Link Group
SRRG	Shared Risk Resource Group
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UMTS	Universal Mobile Telecommunications System
VC	Virtual Clock
VoIP	Voice over IP
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queuing
WIMAX	World Wide Interoperability for Microwave Access
WLAN	Wireless Local Area networks
WP	Working Path

CHAPITRE 1

INTRODUCTION

De nos jours, les télécommunications modernes se dirigent de plus en plus vers la standardisation des technologies utilisées au sein des réseaux afin de mieux gérer l'hétérogénéité des terminaux ainsi que des types de trafic supportés. En effet, avec la croissance fulgurante d'Internet en termes de quantité de données véhiculées et du nombre d'abonnés, L'utilisation de la technologie *IP* affiche un bénéfice indéniable. Cependant, le protocole, dédié initialement au "best-effort", se voit attribuer des fonctions autres, à savoir, le transport d'une panoplie de types de trafics et la nécessité de garantir la qualité de service (*QoS*) requise. En effet, la grande proportion de trafic que supporteront les réseaux de données dans le futur émane principalement d'applications, non seulement avides en ressources, mais aussi très exigeantes en terme de performance exprimée en termes de requis de *QoS*. Ces requis de *QoS* sont généralement traduits en termes de bande passante à long terme, de délai de bout-en-bout, de gigue et de probabilité de perte des paquets. Afin de garantir la *QoS*, la solution communément adoptée dans les réseaux de données est celle qui consiste à sur-dimensionner la capacité de ces derniers. Cependant, dans le cadre des réseaux cœur IP, cette solution n'est plus viable vu que ces derniers sont de plus en plus sollicités (quantité énorme de données véhiculées, nouvelles applications distribuées très avides en bande passante, etc.). Ce problème s'accroît d'avantage

lorsqu'on considère plusieurs types d'accès (*UMTS*, *Ethernet*, *WLAN*, *WIMAX*, *DOCSIS*, etc.).

En outre, les réseaux ne sont plus exclusivement dédiés au transport à moindre effort (Best-effort) des données mais se voient plutôt attribuer des fonctions autres. Par exemple, les opérateurs de télécoms utilisent de plus en plus des réseaux à commutation de paquets afin de transporter des flux avec des contraintes strictes de qualité de service (*QoS*). Ceci a ramené ces opérateurs à améliorer, d'un côté, leur infrastructure de transport afin de lui permettre de supporter le besoin grandissant en bande passante et en survivabilité et d'un autre côté, fournir des garanties strictes de qualité de service (débits, délai, taux de perte, gigue) dans un domaine à commutation de paquets, en implantant des mécanismes dédiés. Ces garanties permettront l'émergence et l'intégration de nouvelles applications (voix sur *IP*, vidéoconférence ...) qui ne peuvent se contenter du service de type "best-effort" comme c'est le cas pour l'Internet classique. Le déficit devient d'autant plus important avec un contrôle unifié des deux couches transport et *IP*, dont la technologie *GMPLS* constitue un exemple.

1.1 Définitions et concepts de bases

L'explosion du trafic numérique dans les réseaux, principalement engendré par la croissance d'Internet, le changement progressif des habitudes des usagers ainsi que la convergence des réseaux et des services, ont incité les groupes internationaux de normalisation à proposer et adopter de nouveaux standards et architectures de réseaux. Les caractéristiques de cette génération de réseaux, nommés de prochaine génération (*NGN*), sont entre autres :

- la séparation logique et fonctionnelle entre le transport, les services et les applications ;

- le support de plusieurs technologies d'accès et l'indépendance de l'accès avec le type de services offerts ;
- la gestion de *QoS* de bout-en-bout ;
- l'utilisation de la technologie par paquets.

Plusieurs architectures de *NGN* ont été proposées et étudiées (*3GPP*, *IETF*, *ETSI*). L'architecture *TISPAN* (*Telecommunications and Internet Converged Services and Protocols for Advanced Networking*) d'*ETSI* (Gritella & Boswarthick, 2008) représente un exemple parmi d'autres d'une architecture de prochaine génération, qui définit un réseau multi-accès, multiservices, multi-protocoles et basé sur la technologie *IP*. En amont du sous-système d'accès (formé de plusieurs technologies d'accès), un réseau d'agrégation ou réseau cœur prend place dans l'architecture. Ce sous-système est basé sur la technologie *IP* et interconnecte d'un côté plusieurs types d'accès, et de l'autre, différents autres réseaux cœur, appartenant à différents opérateurs. Outre les fonctionnalités de transport classiques attribuées à cette entité, un sous-système logique (qui peut être physiquement centralisé ou distribué) a été défini afin d'assurer les tâches d'allocation de ressources et de contrôle d'admission intra-domaine. Cette entité, intitulée *RACS* (*Resource Allocation and admission Control Sub-system*), est un gestionnaire de ressources qui veille principalement à assurer les fonctions de contrôle d'admission, de réservation, d'optimisation de l'allocation de ressources, de contrôle des politiques, etc. au niveau du domaine *IP*.

L'allocation de ressources dans les réseaux *IP* comprend aussi bien les fonctions de routage, de classification, de réservation, de contrôle d'admission, etc. et ce dans le but de faire un usage adéquat des ressources tout en respectant les contraintes de *QoS* du trafic transporté. Le routage dans les réseaux *IP* actuels est généralement basé sur des protocoles distribués qui calculent un plus court chemin vers une certaine destination en fonction d'une métrique généralement statique (nombre de sauts, capacités des liens, etc.). Plusieurs protocoles ont d'ailleurs été

proposés afin d'adapter dynamiquement ces métriques afin de refléter l'état instantané des ressources. Ceci engendre toutefois une surcharge de signalisation et de calcul ce qui ralentit la convergence de ces protocoles de routage.

Comme discuté précédemment, les réseaux de prochaines générations sont généralement dotés d'un module de gestion des ressources (le RACS dans l'architecture TISPAN). Ce module intègre, entre autres, les fonctions de routage. Une séparation fonctionnelle et parfois physique existe entre le plan de contrôle (dont ce module fait partie) et le plan des données (qui comprend l'acheminement des paquets suivant un certain nombre de politiques de routage et de *QoS* déjà établies). Dans un tel contexte, le routage explicite a été utilisé, notamment avec l'avènement de la technologie de commutation d'étiquettes *MPLS (Multiprotocol Label Switching)*. Outre la rapidité de commutation et la résilience aux pannes qu'elle offre, cette technologie permet de choisir les *LSP (Label-Switched Path)* d'une manière plus adéquate en tenant compte, dans la mesure du possible, de la charge du réseau et en faisant appel à des notions d'ingénierie de trafic. Cette dernière notion est très importante dans le processus d'allocation des ressources dans les réseaux prochaines générations.

Le principal objectif de l'ingénierie de trafic est d'éviter la congestion de certaines parties fortement sollicitées du réseau en contrôlant et en optimisant les fonctions de routage en plaçant, simplement, le trafic là où la capacité le permet. Le défi de l'ingénierie de trafic est donc de bien s'adapter au caractère dynamique de la topologie (cas de pannes) et de la demande. En outre, afin de faire un usage adéquat des ressources, la notion de multiplexage statistique doit être considérée. Cette dernière est généralement étudiée localement au niveau d'un lien unique et permet, vu la distribution du trafic considéré, les contraintes probabilistes de *QoS* et la faible probabilité que toutes les connexions multiplexées sur un même lien soient à leurs débits maximaux, de mieux partager la bande passante offerte par le lien. Cette notion

n'est généralement pas évoquée lors du processus global d'allocation de ressources. Néanmoins, plusieurs algorithmes de contrôle d'admission, généralement basés sur les mesures, s'en servent afin d'élargir la zone d'acceptation du lien tout en respectant les contraintes de QoS du trafic à admettre.

Plan de contrôle	Plan d'acheminement
GMPLS	MPLS : ensemble de LSPs
	Optique : ensemble de chemins optiques
	Physique : Ensemble de fibres avec multiplexage WDM

Figure 1.1 Plan de contrôle GMPLS

Au niveau de la couche optique, le multiplexage de longueurs d'ondes WDM constitue la solution par excellence permettant d'augmenter la capacité de la fibre optique en transportant simultanément plusieurs canaux disjoints. Ainsi, un ensemble de chemins, appelé chemins optiques (*lightpaths*) est établi, afin d'émuler l'interconnectivité des commutateurs optiques, perçue par la couche *IP* ou *MPLS*. Cependant, les réseaux de haute vitesse et fortement connectés sont d'autant plus avantageux lorsqu'ils sont munis de mécanismes d'ingénierie de trafic. Cette fonction doit être intégrée à différents niveaux du réseau tel que montré à la figure 1.1. C'est à cette fin que *GMPLS* (*Generalized Multi-Protocol Label Switching*) a été développé afin d'unifier le plan de contrôle du réseau tant au niveau optique que que *IP* et *MPLS*. Le défi principal de la technologie *GMPLS* est d'intégrer les fonctionnalités d'ingénierie de trafic (étalés sur plus d'un niveau dans le réseau) et de contrôle d'admission au sein d'une seule et même entité unifiée. Ceci est particulièrement intéressant pour les réseaux optiques dans lesquels le multiplexage temporel (*TDM*) et de longueurs d'ondes (*WDM*) sont régis par un même plan de contrôle *GMPLS* pour une topologie physique arbitraire.

Lors de l'établissement de circuits commutés (*LSP*), la conception inter-couches faisant intervenir les mécanismes optiques et *IP*, améliore nettement l'utilisation des ressources dans le réseau. Au niveau optique, il est très important de garantir, non seulement un certain débit minimal, mais aussi un seuil maximal de dégradation du signal optique, due aux imperfections des équipements optiques (convertisseurs de longueurs d'ondes, commutateurs optiques et amplificateurs optiques) ainsi qu'un délai acceptable de propagation optique d'un bout à l'autre du chemin optique. En effet, vu la non linéarité des supports de transmission optiques et l'introduction des convertisseurs optiques de longueurs d'ondes, le signal subit du bruit et de la distorsion qui s'accumulent tout au long du chemin optique.

Au niveau *MPLS*, les *LSPs* sont constitués d'un ou plusieurs chemins optiques en cascade (formant la topologie logique du réseau). Lors de l'établissement d'un *LSP* et dépendamment du type de trafic transporté (données, voix, etc.), il est important de s'assurer qu'un certain nombre de contraintes de *QoS* soit bien respecté. Ces contraintes sont généralement le débit binaire, le délai de bout en bout, la probabilité de perte de paquets et la gigue. Ces contraintes de *QoS* ne sont généralement pas additives tout au long du chemin physique et le calcul de l'admissibilité d'une connexion dans le réseau requiert ainsi un calcul plus ou moins complexe, dépendamment du type de la contrainte. D'un autre côté, la majorité des trafics véhiculés dans le réseau ne requièrent pas de contraintes strictes de *QoS* mais plutôt des contraintes statistiques. Dans ce cas, le réseau doit garantir les contraintes de *QoS* pour au moins une proportion du trafic incluant ainsi une nouvelle métrique : la probabilité de violation des contraintes de *QoS*. Les opérateurs de réseaux peuvent inclure cette métrique lors de l'établissement des contrats de service, connus aussi sous le nom de *SLA* (*Service Level Agreement*). Les termes d'un tel contrat de service sont généralement traduits en des spécifications techniques des mécanismes de *QoS* en place. Dans la littérature, deux modèles principaux de service sont cités : les services intégrés (*IntServs*), les services différenciés (*DiffServ*).

IntServ (Braden *et al.*, 1994) est un mécanisme de *QoS* qui offre des garanties strictes aux flux individuellement. Il représente une véritable mutation des services *IP* traditionnels à moindre effort vers un support strict des différentes métriques de *QoS*. Le modèle *IntServ* requiert donc que les routeurs maintiennent les états de toutes les connexions actives tout en implémentant des mécanismes additionnels de contrôle d'admission, de classification et d'ordonnancement des paquets. Le principal avantage du modèle *IntServ* réside en son aptitude à garantir des performances de bout en bout pour chacun des flux individuellement. Cependant, un tel niveau de granularité peut engendrer une quantité énorme d'informations stockée dans les routeurs et limite, du fait, l'évolutivité de cette architecture. Le modèle *DiffServ* (Black *et al.*, 1999) représente une alternative à *IntServ* traitant le problème d'évolutivité en groupant l'ensemble des connexions véhiculées en un certain nombre de classes de trafic. À chaque type de trafic est associée une priorité. Le trafic transitant par un domaine *DiffServ* est d'abord classifié, marqué et contrôlé (*traffic shaping*) au niveau du routeur d'entrée (*Ingress*). Par la suite, le champ *DSCP* (*DiffServ Code Point*) de l'entête *IP* est consulté par chaque nœud intermédiaire afin de déterminer le niveau de priorité du trafic ainsi que le traitement auquel il est souscrit : le *PHB* (*Per Hop Behavior*).

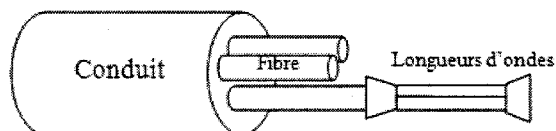


Figure 1.2 La hiérarchie dans un SRLG

D'un autre côté, la fiabilité des réseaux n'en demeure pas moins un aspect très important à considérer lors du développement des mécanismes de contrôle et d'acheminement dans le réseau. En effet, certains types d'applications, tels que les services gouvernementaux et bancaires, requièrent une connectivité permanente. Les

technologies *MPLS* et *GMPLS* ont bien adressé ce besoin en permettant l'établissement à l'avance d'un ou plusieurs *LSPs* de secours (*backup*), qui peuvent être soit dédiés (1+1 ou 1 : 1) ou partagés par plusieurs *LSPs* primaires (1:N). De plus, comme il est très rare que des pannes simultanées arrivent, la plupart des travaux ne considèrent que les pannes simples d'équipements (liens ou nœuds). Cependant, la panne d'une seule fibre au niveau optique engendre la rupture de plus d'un chemin optique, et à un niveau plus élevé, la déconnexion de plusieurs *LSPs*. Ceci est d'autant plus important lors de la rupture d'un conduit, transportant plusieurs fibres optiques, tel que montré à la Figure 1.2. Les fibres optiques partageant un même conduit forment un groupe de liens à risque partagé *SRLG* (*Shared-Risk Link Group*). La rupture d'un seul *SRLG* engendre ainsi le dysfonctionnement d'un grand nombre de fibres optiques, comprenant, chacune, un certain nombre de canaux utilisés potentiellement par des chemins optiques déjà établis. L'établissement d'un circuit fiable nécessite ainsi l'établissement d'un circuit de secours disjoint en termes de *SRLGs*. Ce problème est d'autant plus important et complexe lorsque des sessions *multicast* sont considérées.

1.2 Éléments de problématique

En dépit du nombre croissant d'applications très exigeantes en termes de *QoS* et de bande passante sur Internet, les mécanismes reliés à la technologie *IP* restent plutôt élémentaires pour assurer adéquatement des contraintes strictes de *QoS*. De plus, vu le nombre grandissant de données véhiculées, des notions telles que l'ingénierie de trafic et l'allocation adéquate des ressources doivent être prises en compte afin de maximiser la capacité effective du réseau tout en garantissant aux applications la *QoS* demandée. Plusieurs mécanismes compatibles avec la technologie *IP* ont été proposés et standardisés afin d'optimiser l'utilisation des ressources dans le réseau tout en garantissant un certain degré de *QoS*. Ces mécanismes investiguent

aussi bien le partage des ressources au niveau du routeur *IP* (*IntServ*, *DiffServ*, etc), que l'allocation des ressources du réseau d'une manière globale en optimisant les solutions de routage (*MPLS*, *QOSPF*, etc.) et en tenant compte des différents scénarios de pannes. De plus, la notion de multiplexage statistique est rarement considérée et le provisionnement à long terme des ressources se fait simplement en fonction du débit maximal des flux. Cette dernière notion est très importante vu que la capacité effective du réseau est considérablement améliorée (par rapport aux approches conservatrices) et ce, en fonction du nombre de connexions multiplexées et des contraintes probabilistes de *QoS* (probabilité de perte de paquets ou probabilité de violation des contraintes de *QoS*, etc.).

D'un point de vue architectural, le support de la *QoS* dans les réseaux cœur de prochaine génération implique la mise en œuvre de plusieurs mécanismes, à différents niveaux du réseau (optique, *IP*, *MPLS*, etc.), qui doivent être contrôlés via une architecture unifiée, telle que *GMPLS*. Ceci permettrait en fait d'offrir des solutions nettement plus optimisées, en termes d'utilisation des ressources du réseau, en tenant compte notamment de l'incorporation de la conception inter-couche. Dans un tel contexte et afin d'assurer, d'une manière stricte ou statistique, les besoins de *QoS* du trafic véhiculé, la phase de contrôle d'admission est très importante. En effet, la décision d'admettre un nouveau trafic dans le réseau doit non seulement tenir compte des besoins de ce dernier en termes de débit et de *QoS*, mais aussi, s'assurer que le service offert aux trafics préalablement admis soit dégradé. Ceci implique donc le besoin de prévoir l'état des ressources (bande passante disponible, état des files d'attentes des routeurs) du réseau, une fois le trafic admis.

Les mécanismes de contrôle d'admission appartiennent généralement à trois différentes classes (Gerla *et al.*, 2001). Certains sont analytiques ou basés sur les paramètres (*parameter-based AC*) et peuvent être soit déterministes ou stochastiques. D'autres sont basés sur les mesures (*Measurement-based AC*). Dans ce cas, la

décision est prise en fonction des mesures empiriques recueillies pour un réseau en opération. Enfin, d'autres utilisent les paquets de vérification (*probing packets*) pour vérifier l'admissibilité d'un flux en sollicitant le réseau instantanément afin de vérifier un certain nombre de paramètres (délai de bout-en-bout, perte de paquets, etc.).

De plus, les mécanismes de contrôle d'admission peuvent être distribués ou centralisés. Les approches distribuées sont généralement basées sur des protocoles de signalisation. Quant aux approches centralisées, elles sont régies par un gestionnaire de ressources central qui prend les décisions d'acceptation en fonction des données recueillies périodiquement sur l'état du réseau. Pour l'architecture *TISPAN* présentée précédemment, le sous-système *RACS* est responsable de la gestion des ressources du réseau. Il est donc impératif de définir la portée de ce système ainsi les mécanismes qui lui permettent de communiquer et de se synchroniser avec les équipements du réseau.

Cependant, les mécanismes de contrôle d'admission reposent généralement sur des données de routages déjà établies et s'assurent, de différentes manières, de la faisabilité du chemin à emprunter vis-à-vis des contraintes de *QoS*. Dans un tel contexte, la sélection des chemins peut être incorporée à la phase de contrôle d'admission. Cette possibilité est d'autant plus intéressante dans un environnement *MPLS* où il est possible de créer des *LSPs* dynamiquement, en indiquant aux routeurs de bordure d'amorcer la phase de distribution d'étiquettes pour le, ou les, nouveaux *LSPs*. Dans ce dernier cas, le problème de contrôle d'admission se voit également attribué la fonction de sélection de route pour le nouveau trafic, de manière à respecter les contraintes de *QoS*, aussi bien de ce dernier, que des trafics déjà admis.

En outre, assurer un service permanent, fiable et sans rupture, devient de plus en plus un besoin crucial pour un grand nombre d'applications. Dans un tel contexte, la

conception inter-couches, régie par un plan de contrôle unifié, doit absolument inclure des mécanismes performants de gestion de pannes, qui peuvent être soit réactifs, soit proactifs. Dans le premier cas, aucune ressource de secours n'est considérée à l'avance et seuls les trafics (ou *LSPs* dans un domaine *MPLS*) atteints par la panne sont ré-routés. Le calcul et l'établissement des nouvelles routes (ou *LSPs* de secours) se fait ainsi instantanément en temps-réel. Pour ce qui est de la gestion proactive de pannes, des *LSPs* de secours sont calculés et établis à l'avance en anticipant généralement les cas des pannes les plus probables (généralement les pannes simples). Il est cependant important, lors de l'établissement de nouveaux *LSPs* de secours, de s'assurer que les contraintes de *QoS* des trafics atteints ne soient pas violées. De plus, afin d'optimiser l'utilisation des ressources dans le réseau, il est important de considérer le partage des ressources de secours tout en s'assurant qu'assez de ressources sont disponibles pour chaque *LSP*, pour les différents scénarios de pannes.

La résilience aux pannes est extrêmement importante dans les réseaux optiques *WDM* où la perte d'une fibre engendre la rupture de plusieurs chemins optiques. L'effet est d'autant plus accentué lorsque plusieurs fibres sont regroupées dans un même conduit ou *SRLG*, comme montré à la Figure 1.2. Cependant, les clients peuvent négocier un contrat de service offrant des garanties statistiques de fiabilité, techniquement appelée "fiabilité différentielle" (Guo & Li, 2007).

1.3 Objectifs de recherche

Cette thèse traite principalement le problème d'allocation des ressources dans les réseaux de prochaines générations. Notre objectif principal est de proposer des mécanismes efficaces de routage et de contrôle d'admission à différents niveaux de la hiérarchie du réseau (*MPLS*, *GMPLS*, *WDM*) et offrant des garanties de qualité de

service (*QoS*) strictes ou statistiques. Plus spécifiquement, cette thèse vise les objectifs suivants :

- analyser les protocoles et mécanismes proposés dans la littérature pour l'optimisation de l'allocation des ressources et le contrôle d'admission avec support de la *QoS* dans les réseaux cœur de prochaines générations, afin de déceler les faiblesses et les problèmes qui ne sont pas encore adressés ou résolus adéquatement ;
- analyser les besoins en fiabilité et survivabilité des réseaux optiques *WDM* et étudier les mécanismes de routage fiables proposés dans la littérature.
- concevoir de nouveaux mécanismes pour le contrôle d'admission dans les réseaux *MPLS* et *GMPLS*, le support statistique et strict de *QoS* et le routage dans les réseaux *WDM* avec des contraintes strictes ou statistiques de fiabilité ;
- évaluer les performances des mécanismes et algorithmes proposés en tenant compte des exigences et spécifications des réseaux *NGNs*. Cette évaluation sera basée sur une comparaison avec les travaux existants qui abordent les mêmes problèmes.

1.4 Principales contributions

Les principales contributions de cette thèse touchent une grande partie des défis posés par les réseaux de prochaines générations, à savoir, l'optimisation de l'allocation des ressources, le contrôle d'admission, le support de la *QoS* de bout-en-bout et la fiabilité. Ces contributions sont en nombre de trois :

1. un mécanisme de contrôle d'admission dans les réseaux multicouches *GMPLS* ;
2. une étude analytique de la qualité de service de bout-en-bout permettant un contrôle plus adéquat de l'admissibilité des connexions dans les réseaux cœur *IP* basés sur la commutation d'étiquettes ;
3. un algorithme évolué pour le routage multicast à fiabilité différentielle dans les réseaux cœur *WDM*.

Ces dernières peuvent être résumées comme suit :

- *Mécanisme de contrôle d'admission dans les réseaux multicouches GMPLS* : dans les réseaux de prochaines générations, un plan de gestion (ou contrôle) unifié permettra d'uniformiser et de centraliser les tâches de contrôle des différentes couches du réseau (*IP*, *MPLS*, Transport). Cette gestion centralisée assurera une meilleure utilisation des ressources, en tenant compte de l'interaction entre les différents niveaux de la hiérarchie du réseau. Dans un tel contexte, nous proposons un mécanisme de routage et de contrôle d'admission des chemins optiques dans les réseaux *WDM* régi par un plan de contrôle unifié *GMPLS*. Afin d'offrir un meilleur service aux couches supérieures du réseau, des contraintes de délai de propagation de bout-en-bout et de dégradation maximale du signal optique sont considérées. Le mécanisme proposé repose sur une modélisation mathématique du problème et offre de meilleures performances, comparé aux algorithmes proposés dans la littérature ;
- *Une étude analytique de la qualité de service de bout-en-bout* : les métriques de *QoS* pour certains types de trafic peuvent être soit strictes, soit statistiques. Dans le cas où elles sont statistiques, une certaine violation des contraintes de

QoS est permise. Afin de respecter les garanties statistiques de *QoS* de bout-en-bout, une nouvelle modélisation des métriques de *QoS* est proposée, reposant sur les données empiriques reflétant l'état des équipements du réseau. Cette borne supérieure est applicable aux différents comportements du trafic véhiculé par le réseau (trafic à taux constant ou légèrement variable, trafic en rafale, etc.). Ceci nous permettra de proposer un algorithme centralisé de contrôle d'admission dans les réseaux *MPLS* avec support statistique de *QoS* de bout-en-bout ;

- *Algorithme pour le routage multicast à fiabilité différentielle* : La convergence des différents services vers une seule et même architecture de réseau a incité les chercheurs à proposer des mécanismes évolués pour assurer la fiabilité et la disponibilité des réseaux. Dépendamment du type de trafic transporté et de la clientèle visée, certains contrats de service offrent une garantie statistique de fiabilité, notée également fiabilité différentielle. Dans ce contexte, nous proposons un algorithme pour le routage des connexions *multicast* (ou éventuellement *unicast*) avec fiabilité différentielle. Une formulation mathématique du problème est d'abord proposée. Afin de pallier la complexité du problème, un algorithme basé sur la décomposition du problème est proposé et étudié. Outre la bonne qualité des résultats obtenus, la particularité qui distingue cette contribution est son caractère générique. En effet, le problème abordé faisant intervenir plusieurs facteurs (routage multicast ou unicast, fiabilité stricte ou différentielle, différents paramètres de fiabilité, propriétés des réseaux *WDM*, etc.), la solution proposée permet de tenir compte de la totalité ou de seulement une partie de ces facteurs.

1.5 Plan de la thèse

Le reste de cette thèse est organisé comme suit. Suite au présent chapitre d'introduction, le Chapitre 2 présente une revue critique et sélective de la littérature sur les problèmes clés des réseaux de prochaines générations, à savoir, l'optimisation de l'allocation des ressources, le contrôle d'admission, le support de la *QoS* de bout-en-bout et la fiabilité. Les différents algorithmes et mécanismes rencontrés dans la littérature sont abordés, ainsi que les défis et les problèmes qui en découlent.

Ayant opté pour une thèse par articles, les Chapitres 3 à 5 contiennent respectivement les différents articles qui décrivent nos principales contributions.

Plus précisément, le Chapitre 3 présente l'article intitulé *A Novel Admission Control Mechanism in GMPLS Based IP over Optical Networks* qui a été accepté et publié dans la revue *Computer Networks* dans son Volume 52, Numéro 6, édition d'Avril 2008. Dans cet article, nous proposons un nouveau mécanisme d'allocation des ressources et de contrôle d'admission dans les réseaux *IP* et *WDM* dotés d'un plan de contrôle unifié GMPLS. L'article intitulé *Joint Routing and Admission Control Problem under Statistical Delay and Jitter Constraints in MPLS Networks* accepté et publié dans la revue *Computer Communications* dans son Volume 31, Numéro 1 et édition de Septembre 2008, est présenté au Chapitre 4. Dans cet article, nous proposons une nouvelle expression des bornes supérieures des contraintes statistiques de *QoS*. À partir de ces bornes, nous proposons une modélisation mathématique du problème de contrôle d'admission avec garanties statistiques de *QoS* dans un réseau *MPLS*.

Le Chapitre 5 intitulé *A Survivable Multicast Routing Mechanism in WDM Optical Networks* est un article qui a été soumis à la revue *Photonic Network Communications*. Dans cet article, un algorithme heuristique pour le routage des

connexions multicast avec fiabilité différentielle est proposé et évalué. Dans le Chapitre 6, une discussion générale des différents résultats obtenus et une synthèse de nos contributions sont faites. Le Chapitre 7 conclut la présente thèse en mettant l'accent sur les principales contributions apportées et en ressortissant les limitations de ces dernières. Des recommandations des travaux futurs seront également évoquées dans la Conclusion.

CHAPITRE 2

REVUE DE LITTÉRATURE

La coexistence de différentes technologies de transport et l'hétérogénéité des infrastructures actuelles des réseaux de communication constituent le fondement de la conception et du déploiement des réseaux convergés de prochaines générations (NGN). Toutefois, cette hétérogénéité apporte plusieurs défis auxquels il faut faire face. Parmi ces défis, on peut citer l'interopérabilité des différentes technologies de transport, la gestion uniformisée des ressources, l'ingénierie de trafic, la garantie d'une meilleure qualité de service de bout-en-bout et la conception d'architectures et protocoles. Plusieurs travaux ont été entrepris dans la littérature afin de solutionner ces défis. Cependant, plusieurs problèmes restent à aborder et à étudier. Dans ce chapitre, une brève revue de littérature des différents mécanismes de qualité de service dans les réseaux de prochaines générations sera présentée. Plus précisément, les aspects d'allocation de ressources, d'ingénierie de trafic et fiabilité des réseaux ainsi que les différentes techniques de contrôle d'admission feront l'objet du présent chapitre.

2.1 Modèles de services

Dans la littérature, deux principaux modèles de service ont été cités et standardisés (Barden *et al.*, 1994 et Black *et al.*, 1999): les services intégrés (*IntServs*), les services différenciés (*DiffServ*). Afin de pallier les inconvénients de ces deux modèles, un modèle hybride a été proposé et standardisé (Duan *et al.*, 2004).

2.1.1 Services intégrés (*IntServ*)

Le mécanisme *IntServ* (Barden *et al.*, 1994) garantit la qualité de service des flux individuels. Il représente une véritable mutation des services IP traditionnels à moindre effort vers un support stricte des caractéristiques de la QoS. *IntServ* définit deux classes de services : *Guaranteed service* et *Controlled-load service* dépendamment des exigences en matière de qualité de service des flux. Dans le modèle *IntServ*, les routeurs doivent faire une réservation de ressources (bande passante, tampons, etc.) pour chacun des flux y passant. Le modèle *IntServ* requiert donc que les routeurs maintiennent les états des connexions tout en implémentant des mécanismes additionnels de contrôle d'admission, de classification et d'ordonnancement de paquets. En effet, afin d'offrir des garanties de services de bout-en-bout, des mécanismes de gestion du plan de données du réseau (*network data plane*), tels que l'ordonnancement des paquets, et des mécanismes de contrôle du réseau (*network control plane*), tels que le contrôle d'admission et les réservations de ressources doivent intervenir. Basés sur le modèle de service *IntServ*, plusieurs algorithmes d'ordonnancement tels que *WFQ*, *VC*, *RC-EDF* ont été développés afin de supporter les services garantis (Zhang *et al.*, 2000). En outre, le protocole de signalisation RSVP (Braden *et al.*, 1997) a été standardisé afin de faire la réservation des ressources de bout-en-bout.

Le principal avantage du modèle *IntServ* est son aptitude à garantir des performances strictes de bout-en-bout pour chacun des flux véhiculés. Cependant, un

tel niveau de granularité peut engendrer une quantité énorme d'informations à stocker dans les routeurs et limite du fait, l'extensibilité de cette architecture.

2.1.2 Services différenciés (*DiffServ*)

Le modèle *DiffServ* (Black *et al.*, 1999) représente une alternative à *IntServ* traitant le problème d'extensibilité en rassemblant et agrégeant plusieurs flux en un certain nombre de classes de trafic. À chaque classe de trafic est associée une priorité, et ainsi, la priorité la plus élevée (*premium traffic*) correspond au flux requérant la plus grande qualité de service et la priorité la plus basse correspond aux flux sans contraintes particulières de *QoS*. Les équipements du réseau distinguent les classes des paquets véhiculés en consultant le champ *DSCP* (*DiffServ Code Point*) au niveau de l'entête *IP*. Les paquets rentrant dans un domaine *DiffServ* sont d'abord classifiés, marqués et contrôlés (*traffic shaping*) au niveau du routeur d'entrée (*Ingress*). Par la suite, le champ *DSCP* est consulté par chaque nœud intermédiaire afin de déterminer les privilèges d'acheminement (file d'attente de la classe correspondante) qui lui seront appliqués : le PHB (*Per Hop Behavior*).

L'IETF a standardisé trois niveaux de services :

- a) le service « *best effort* » ou à moindre effort qui ne nécessite aucun traitement particulier, sauf qu'il ne doit pas être en famine ;
- b) Le service « *expedited forwarding* » qui garantie une bande passante avec de faibles taux de perte, délai et gigue;
- c) Le service « *Assured Forwarding* » regroupant plusieurs PHB (12) garantissant un acheminement meilleur que le service à moindre effort. Cette famille est scindée en quatre classes de priorités différentes. Chacune comprend 3 de sous-classes indiquant la probabilité relative de perte de paquets (*Drop Precedence*).

Le principal avantage de *DiffServ* est son extensibilité, vu que seulement une quantité limitée d'informations doit être maintenue au niveau des routeurs (limitées aux classes de trafic). Cependant *DiffServ* n'offre aucune garantie du niveau de la qualité de service qu'un trafic recevra. Des mécanismes plus complexes de gestion de ressources et de contrôle d'admission sont ainsi nécessaires.

2.1.3 Notion de *Stateless Core*

Duan *et al.* (2004) proposent une technique permettant de pallier les lacunes d'extensibilité de *IntServ* tout en assurant des garanties strictes de *QoS* de bout-en-bout. Cette technique repose sur la notion d'état dynamique des paquets (*DPS*). En effet, les réseaux *IP* sont de plus en plus mandatés à offrir un service plus sophistiqué et garanti que les services traditionnels à moindre effort. Il est donc impératif de pouvoir implémenter des mécanismes aussi performants que les réseaux où les états des flux sont maintenus dans chaque routeur intermédiaire (*Stateful*), et aussi évolutifs et robustes que les réseaux qui font de l'agrégation de flux en un certains nombre de classes de services, sans en maintenir les détails au niveau des routeurs intermédiaires (*stateless*). Les auteurs considèrent une architecture similaire à *DiffServ*, appelée *SCORE* (*Scalable Core*) dans laquelle, seuls les routeurs de bordure (*Edge Router*) peuvent gérer les flux individuels. Ceci est fait en incluant, dans l'entête *IP*, des champs d'informations sur les besoins en *QoS* des paquets, qui sont mis à jour par les routeurs intermédiaires. Les auteurs montrent que cette architecture permet d'offrir les mêmes garanties de délais et de bande passante que l'architecture *IntServ* tout en bénéficiant de l'évolutivité de l'architecture *DiffServ*.

2.2 Routage avec Qualité de Service

Les différents types de protocoles de routage (état des liens, vecteur distant, etc.) permettent de construire les tables de routage en se basant uniquement sur les coûts ou métriques statiques associés aux liens du réseau et en calculant les plus

courts chemins vers chacune des destinations dans le réseau. Il s'agit néanmoins d'un choix simpliste et inadapté aux besoins de qualité de service, d'une part, et à l'équilibre de la charge à travers le réseau (parties congestionnées et parties peu exploitées), d'autre part. Vu le support d'applications multimédia avec des contraintes strictes de *QoS* par les réseaux de prochaines générations, il est impératif de développer des mécanismes d'acheminement plus évolués. Plusieurs protocoles de routage avec qualité de service ont ainsi été développés dans la littérature. Certains travaux se sont basés sur la modification des protocoles de routage existant, tels *qu'OSPF* ou *IS-IS*. Dans ce contexte, une extension au protocole *OSPF* a été proposée (Gerin *et al.*, 1999) et nommée *QOSPF (Quality of Service Path First)*. Plusieurs messages ont été ajoutés à ce protocole afin d'informer les routeurs des états des liens et des ressources utilisées dans le réseau. D'un autre côté, les réseaux de neurones ont également été utilisés pour assurer les fonctions de routage (Pierre *et al.*, 2000). Ceci a donné naissance à plusieurs algorithmes de routage adaptatifs utilisant des techniques d'apprentissage.

2.2.1 Protocoles à commutation d'étiquettes (*MPLS*)

MPLS (MultiProtocol Label Switching) (Macolm *et al.*, 1999) est un protocole basé sur le paradigme de commutation d'étiquettes dérivé directement de l'expérience acquise avec les réseaux *ATM*. Les objectifs principaux de *MPLS* sont :

- Permettre un acheminement rapide des paquets *IP* en remplaçant la fonction de routage par une fonction de commutation rapide ;
- Faciliter les fonctions d'ingénierie de trafic en fournissant aux opérateurs la maîtrise de l'acheminement des données, qui s'avère très complexe avec des protocoles de routage classiques ;
- Implémenter des mécanismes de résiliences aux pannes.

Ainsi, le routage peut être fait de manière à privilégier, dans le domaine *MPLS*, les flux ayant une classe de service plus élevée. De plus, l'un des aspects les plus intéressants de *MPLS* est la possibilité de construire des routes explicites, nommés *LSP* (*Label-Switched Paths*). La construction de telles routes repose généralement sur les notions d'ingénierie de trafic afin de respecter les contraintes requises de qualité de service.

2.2.2 Ingénierie de trafic avec MPLS

MPLS-TE (Malcolm *et al.*, 1999) est basé sur le concept de routage de tunnels (*traffic trunks*). Ce dernier est unidirectionnel et est appliqué au niveau du premier routeur *MPLS*, noté également *LER* (*Label Edge Router*), en attribuant une classe de trafic, ou *FEC* (*Forwarding equivalent class*), qui détermine le *LSP* à emprunter et le type de service à travers le chemin. Plusieurs tunnels peuvent partager un seul *LSP*.

Une fois le tunnel déterminé, il faut lui créer une route au sien du cœur du réseau. Il est possible de fournir une route pré-calculée (en fonction de la charge du réseau et des contraintes de qualité de service de la classe de trafics transportés) pour chaque *LSP*. Dans ce cas, il faut donner la liste des routeurs à traverser afin que *RSVP-TE* (protocole de distribution des labels), sans faire de réservations, configure les tables d'étiquettes des routeurs. Il est également possible de ne rien spécifier ou de spécifier uniquement une partie de la route. En outre, plusieurs mécanismes de protection de *LSPs* ont été étudiés et développés pour *MPLS* (Pan *et al.*, 2005).

2.2.3 Generalized MPLS

La technologie *GMPLS* (*Generalized Multiprotocol Label Switching*) (Berger, 2003) permet d'améliorer l'architecture *MPLS* en offrant une séparation complète des plans de contrôle et de données. *GMPLS* offre également une convergence logique et non-couteuse des architectures hétérogènes des réseaux de transport (permettant ainsi le provisionnement de bout-en-bout de la *QoS*), des mécanismes de contrôle et de l'ingénierie de trafic. *GMPLS* est basé sur l'adressage et routage *IP*. Le plan de

contrôle unifié fourni par la technologie *GMPLS* permet de simplifier les opérations de gestion et de veille du réseau en automatisant le provisionnement de bout-en-bout des ressources. Il est ainsi nécessaire de définir une certaine correspondance, entre les différentes technologies de transport, pour assurer le provisionnement des ressources et la *QoS*, de bout-en-bout.

GMPLS étend son plan de contrôle (signalisation et routage) aux différents domaines de commutation (paquets, *TDM*, *WDM*, etc.). *GMPLS* est également basé sur les extensions de l'ingénierie de trafic de *MPLS* (*MPLS-TE*) et définit un protocole générique de signalisation, noté *LMP* (*Link Management Protocol*), afin d'établir, libérer et gérer la connectivité entre deux nœuds *GMPLS* adjacents.

2.2.4 Routage multi-chemins

Les algorithmes de routage classiques utilisent une route unique pour acheminer les paquets d'une source à une destination. Afin de mieux équilibrer la charge et d'utiliser adéquatement les ressources du réseau, il serait intéressant d'effectuer un routage multi-chemin (Apostolopoulos *et al.*, 1998 ; Gerin *et al.*, 1999). En effet, le nombre de plus courts chemins entre une source et une destination croît exponentiellement avec la taille du réseau. Le choix de l'un de ces chemins est actuellement arbitraire. Plusieurs techniques nommées *ECMP* (*Equal Cost Multi-Path*) ont été proposées afin de répartir équitablement le trafic sur ces chemins. D'autres proposent une répartition inégale sur les différentes routes (*Optimized Multi-Path*).

2.2.5 Protocole de routage utilisant plusieurs métriques

L'utilisation d'une métrique unique peut s'avérer insuffisante pour satisfaire les besoins en *QoS* d'une application. Ce problème peut être adressé soit en utilisant une métrique mixte (fonction de plusieurs métriques) ou en résolvant le problème de plus-courts chemins à plusieurs métriques (multi-contraintes) qui est NP-Complet (Pasias *et al.*, 2004).

2.3 Ingénierie de trafic

Le principal objectif de l'ingénierie de trafic est d'éviter la congestion de certaines parties fortement sollicitées du réseau en contrôlant et optimisant les fonctions de routages, donc, tout simplement, de placer le trafic là où la capacité le permet (Girish *et al.*, 2000). Le déficit de l'ingénierie de trafic est de bien s'adapter au caractère dynamique de la topologie (cas de pannes) et de la demande. Cependant un compromis entre l'optimalité, la stabilité et la charge supplémentaire de signalisation doit être fait.

Les protocoles de routage courants sont conçus pour être simples et robuste et ne visent généralement pas à optimiser l'utilisation des ressources. Les deux protocoles intra-domaine les plus utilisés sont *OSPF (Open Shortest Path First)* et *IS-IS (Intermediate System to Intermediate System)*, et sont basés sur l'état des liens et dont la métrique est typiquement le nombre de sauts. Quoiqu'ils soient simples, distribués et extensibles, ils ne considèrent pas l'utilisation du réseau et ne font donc pas bon usage des ressources disponibles. Des extensions à ces protocoles comme *ECMP (Equal Cost Multi Path)* qui distribue le trafic à travers plusieurs routes à distances égales ont été proposés mais ne résolvent pas le problème à la base.

L'ingénierie de trafic consiste donc à maintenir un certain niveau de disponibilité pour un réseau opérationnel. Ceci est généralement atteint en évitant la congestion du réseau et en assurant une meilleure exploitation des ressources libres, et donc en adaptant le routage aux situations instantanées des ressources. Le processus d'ingénierie de trafic peut être divisé en trois phases (voir Figure 2.1) : évaluation de l'état du réseau (collecte des caractéristiques statistiques du trafic prédit et en place ainsi que des changements de topologie), optimisation et routage. La phase d'optimisation peut englober plusieurs objectifs tels la minimisation des coûts

d'opération, l'élimination des congestions, la balance de la charge à travers le réseau, spécifications des routes uniques ou multiples, la survivabilité, etc.

Plusieurs travaux mettent l'emphasis sur l'importance de la collecte empirique d'informations sur l'état des ressources afin de faire les choix adéquats de routage (Qian *et al.*, 2004 ; Gopalan *et al.*, 2003; Abuali *et al.*, 2005). Cette opération consiste à recueillir assez d'informations sur les statistiques du trafic véhiculé par le réseau afin de détecter certaines tendances cycliques ou patrons de trafics. Les mécanismes d'ingénierie de trafic peuvent être sans connexion (comme les protocoles de routage distribués *OSPF*, *IS-IS*, etc.), ou orientés connexion (technologie à commutation d'étiquettes permettant un routage explicite comme *MPLS*).

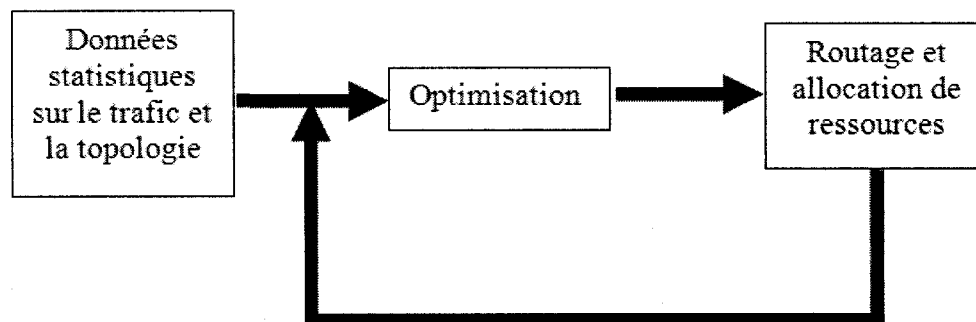


Figure 2.1 Processus d'ingénierie de trafic

Différentes approches d'ingénierie de trafic peuvent être considérées. Une classification des ces dernières est possible suivant plusieurs critères :

- 1- Solutions centralisées vs. distribuées : une solution centralisées est généralement de meilleure qualité, mais implique une plus grande charge additionnelle. Ainsi, Movsichoff *et al.* (2005) ont proposé une étude analytique du problème de routage optimal utilisant la théorie de contrôle non linéaire, mettant en valeur les avantages d'une architecture de routage

distribuée. D'un autre côté, Trimintzios *et al.* (2001) ont proposé une architecture centralisée pour la gestion de ressources et le calcul de chemins dans les réseaux *DiffServ* et *MPLS*. Ho *et al.* (2004) se sont basé sur la précédente architecture afin de proposer un mécanisme centralisé pour l'ingénierie de trafic inter-domaines. Trimintzios *et al.* (2003) ont également proposé une méthode de routage centralisée basée sur une modélisation mathématique du problème de routage ;

- 2- Informations globales vs. locales : l'utilisation d'informations globales sur le trafic et l'état du réseau permet d'optimiser d'avantage l'utilisation des ressources du réseau. Cependant, un effort supplémentaire de signalisation est requis afin d'assurer la collecte d'informations. Flegkas *et al.* (2003) ont proposé une architecture unifiée basée sur les politiques pour l'allocation centralisée des ressources. Ils définissent également la portée du gestionnaire du ressource et le type d'informations collectées à partir du réseau ;
- 3- Méthodes hors-ligne vs. en-ligne : Pour les méthodes en-ligne, le calcul de routes est fait d'une manière réactive, et doit donc être simple et rapide. Ainsi, c'est au moment de l'admission d'un nouvel *LSP* que le calcul de chemin est fait. Oulai *et al.* (2007) ont proposé un mécanisme basé sur la programmation mathématique afin de résoudre le problème joint de routage et de contrôle d'admission dans les réseaux *MPLS*. Qian *et al.* (2004) se sont basé sur le provisionnement statistique de *QoS* afin d'admettre les nouvelles requêtes. Quant aux méthodes hors-lignes, le routage est fait périodiquement ou suite à un événement spécial. Ces méthodes sont généralement basées sur des heuristiques (Pantias *et al.*, 2004, Balon *et al.*, 2005, Girish *et al.*, 2000);
- 4- Simplicité vs. niveau de granularité : La complexité est un critère très important à considérer en déployant les mécanismes d'ingénierie de trafic.

Dans un contexte *MPLS* par exemple, un plus grand nombre de *LSPs* permet un contrôle plus raffiné du trafic dans le réseau. Cependant un tel nombre requiert un effort additionnel de gestion de ressources. C'est ainsi que les trafics sont généralement regroupés en agrégats afin d'éviter l'effort supplémentaire de signalisation et de gestion.

Le problème d'ingénierie de trafic peut être modélisé comme un problème de flots multiples (Balon & Skivee, 2005). Cette technique prend comme entrée l'information globale sur l'état du réseau (trafic véhiculé, contraintes de *QoS*, capacité des liens, etc.) et permet de calculer la solution optimale. Cependant, vu la charge de calcul accrue et le temps consommé pour trouver de telles solutions, on ne recourt généralement pas aux méthodes exactes.

Vu que le calcul avec contraintes de chemins est le fondement de l'ingénierie de trafic, notamment supportées par *MPLS* et *GMPLS*, il est très important de tenir compte de l'hétérogénéité des différents domaines ou régions empruntés par un *LSP* jusqu'à destination. C'est ainsi qu'un nouveau bloc fonctionnel (Farrel *et al.*, 2006) a été incorporé dans les routeurs multiservices (*ISR*), noté *PCE* (*Path Computation Element*) et permettant non seulement un routage intra-domaine centralisé, mais également des mécanismes évolués pour la synchronisation et la mise en correspondance des métriques de *QoS* à travers plusieurs domaines.

2.4 Contrôle d'admission avec Qualité de Service

La fonction de contrôle d'admission consiste à prendre la décision d'accepter ou de rejeter les nouvelles connexions tout en tenant compte de l'ensemble des requis de ces dernières en termes de *QoS*. L'admission d'un nouveau trafic ne doit toutefois pas dégrader le service des trafics déjà établis. Une classification des algorithmes de

contrôle d'admission est présentée au Tableau 2.1. Les algorithmes de contrôle d'admission appartiennent généralement à trois classes (Gerla *et al.*, 2001):

- Contrôle d'admission basé sur les paramètres (*parameter-based Admission Control*): Ce type d'approches a été investigué pour les réseaux *IntServ* et se base généralement sur les notions du Calcul Réseau (*Network Calculus*). Il s'agit de représenter les ressources du réseau ainsi que les requis de *QoS* des connexions par un certain nombre de paramètres (représentation du trafic par un sceau de jeton, considération de plusieurs algorithmes d'ordonnancement, etc.). Plusieurs algorithmes de contrôle d'admission basé sur les paramètres dans les réseaux *IntServ* ont été proposés dans la littérature (Gerla *et al.*, 2001). Cette notion a également été considérée pour les réseaux *DiffServ* (Fidler *et al.*, 2004), surtout avec la proposition de l'architecture de gestion de ressources centralisée (*Bandwidth Broker*) (Duan *et al.*, 2004). Le contrôle d'admission basé sur les paramètres peut être déterministe ou stochastique. Dans le premier cas, les pires scénarios sont considérés, engendrant ainsi une sous-utilisation des ressources du réseau. D'un autre côté, les approches stochastiques reposent généralement sur la notion de largeur de bande effective proposée par Kelly (1996) et supposent généralement un modèle fluide de trafic. L'approche consiste à assurer des garanties statistiques de qualité de service en évaluant le point d'opération spatio-temporel (Courcoubetis *et al.*, 1999 ; Likhanov *et al.*, 2004) d'un lien du réseau et en supposant que tous les flux ont les mêmes exigences de *QoS*. Le contrôle d'admission est toutefois fait au niveau du lien et les paramètres de *QoS* de bout-en-bout doivent être mappés à travers le chemin emprunté.
- Contrôle d'admission basé sur les mesures (*Measurement-based Admission Control*): Ce type d'approche base la décision d'admission sur

les valeurs empiriques de l'état des ressources du réseau. Ces algorithmes permettent une meilleure utilisation des ressources du réseau en fournissant des garanties statistiques, pour les nouvelles connexions. Plusieurs algorithmes basés sur les mesures ont été étudiés et proposés dans la littérature (Qian *et al.*, 2004 ; Abuali *et al.*, 2005 ; Gopalan *et al.*, 2004). Gopalan *et al.* (2004) ont proposé un mécanisme de contrôle d'admission qui garantie, statistiquement, le délai maximal de bout-en-bout. Ce mécanisme, noté *DDM (Delay Distribution Measurement)*, permet de bâtir, à partir des mesures du délai réel encouru par les paquets, une distribution du délai des paquets sur chaque lien du réseau et dresse une zone d'acceptation en fonction des contraintes statistiques de *QoS*. Abuali *et al.* (2005) ont approximé le délai des paquets sur un lien du réseau par une distribution *Gamma* et se basent sur ce résultat pour proposer un algorithme de contrôle d'admission avec garanties statistiques de délai, noté *SD-MBAC (Statistical Delay- Measurement-Based Admission Control)*. Une étude empirique des délais des paquets *IP* dans des réseaux en production a également été menée par Constantinescu *et al.* (2006).

- Contrôle d'admission basé sur les paquets de vérification (*Probing packets based Admission Control*) : Afin d'évaluer l'état des ressources du réseau et de valider l'admissibilité d'un trafic (sujet à des contraintes de *QoS*), le nœud d'entrée du réseau peut créer et envoyer des paquets de vérification. Au retour de la réponse, le routeur peut estimer le délai, la gigue ainsi que le taux de perte de paquets d'un bord à l'autre du réseau (Filder *et al.*, 2004 ; Rhee *et al.*, 2004).

Les approches de contrôle d'admission peuvent être soit distribuées ou centralisées. Les approches distribuées sont généralement basées sur des protocoles

de signalisation (*RSVP* par exemple). Quant aux approches centralisées, elles sont effectuées dans un gestionnaire de ressources central qui prend les décisions d'acceptation en fonction des données globales sur le réseau. Un tel gestionnaire de ressource est installé dans chaque domaine *DiffServ* (*Bandwidth Broker* par exemple). Dans ce cas, des mécanismes de synchronisation et de communication entre les équipements du réseau d'une part, et leur gestionnaire de ressources central, d'autre part, doivent exister.

Table 2.1 Classification des méthodes de contrôle d'admission

	Méthode de CA		Avantages	Inconvénients
Méthodes distribuées	CA basé sur les paramètres		Garanties de <i>QoS</i> pour les services temps réel	Problèmes d'extensibilité Sous-utilisation des ressources
	CA basé sur les mesures	Mesures sur les paquets réels	Extensibilité Utilisation optimale des ressources	Problème de précision des mesures du trafic
		Mesures sur les paquets de vérification	Extensibilité Simplicité des mesures et contrôle d'admission	Délai additionnel pour le contrôle d'admission
Méthodes centralisées	Provisionnement statique		Contrôle d'admission relativement simple	Congestion Sur dimensionnement
	Provisionnement dynamique		Éviter les congestions Multiplexage statistique	Plus complexe

2.4.1 Contrôle d'admission dans un domaine *DiffServ*

L'architecture *DiffServ* repose sur le principe de classification du trafic en un nombre limité de classes, définies selon les besoins de l'opérateur. Plusieurs travaux dans la littérature adressent le problème de contrôle d'admission dans les réseaux *DiffServ* (Stoica *et al.*, 1999 ; Flegkas *et al.*, 2004 ; Trimintzios *et al.*, 2001 ; Trimintzios *et al.*, 2003 ; Angulo *et al.*, 2005 ; Qian *et al.*, 2004). Les fonctions de contrôle d'admission peuvent soit être faites par le nœud d'entrée au réseau (*ingress node*) (Rhee *et al.*, 2004 ; Qian *et al.*, 2004 ; Georges *et al.*, 2004), ou assurées par un

gestionnaire central de ressources (Trimintzios *et al.*, 2003). Vu que seulement un nombre limité de classes est considéré, les mécanismes de contrôle d'admission sont relativement plus complexes, comparés à un provisionnement par flux individuel. Parmi les approches distribuées de contrôle d'admission, Hill *et al.* (2001) ont proposé un algorithme de contrôle d'admission basé sur les paquets de vérification avec garanties strictes de *QoS*. Le mécanisme a été étendu plus tard par Yang (2005) pour des sessions multicast. Nonobstant les garanties strictes de délai de bout-en-bout, les deux algorithmes altèrent considérablement le module *DiffServ* en permettant aux routeurs de reconnaître les paquets de vérification et leur inférer un traitement spécial. Dans ce même contexte, Mäs *et al.* (2007) ont proposé un algorithme décentralisé de contrôle d'admission basé également sur les paquets de vérification. Le mécanisme offre des garanties strictes sur le taux maximal de perte de paquet. Le résultat est basé sur une étude analytique qui borne le taux de perte de paquets de bout-en-bout, en considérant le modèle *M/D/1* de files d'attente. Georges *et al.* (2004) ont également proposé un mécanisme évolué d'allocation de ressources au niveau du routeur d'entrée, basé sur la notion de multiplexage statistique. Les auteurs ont montré que l'algorithme permet une meilleure utilisation de la bande passante des liens tout en garantissant un délai minimal au premier nœud. D'un autre côté, Georgoulas *et al.* (2003) ont proposé un mécanisme de contrôle d'admission basé sur les mesures pour les trafics temps-réels. Ce mécanisme permet de calculer une borne supérieure sur le nombre maximal de connexions concurrentes pour assurer la *QoS* requise. Le mécanisme est cependant local à un nœud et ne garantit pas la *QoS* de bout-en-bout.

Avec l'avènement du modèle *DiffServ*, plusieurs propositions d'architectures centralisées de gestion de ressources ont été proposées et standardisées (*BB*, *PCE*). Ceci a permis le développement de plusieurs mécanismes centralisés de contrôle d'admission, assurant notamment la *QoS* de bout-en-bout. Dans ce contexte, Flegas *et al.*, (2002) ont présenté une architecture de contrôle admission basée sur les

politiques et faisant intervenir un gestionnaire central de ressources (*Bandwidth Broker*). Ce gestionnaire de ressources incorpore le plan de contrôle du réseau *DiffServ*. Basé sur cette architecture centralisée, Mardena *et al.* (2007) ont récemment traité le problème joint de routage et de contrôle d'admission des nouveaux *SLAs* multicast en considérant une probabilité de surréservation (*overbooking*) des classes de services *AF* (*Assured Forwarding*). Ils proposent ainsi une heuristique gloutonne de contrôle d'admission qui permet de prendre les décisions de routage pour un nouvel *SLA* de façon à respecter les contraintes statistiques de bande passante. Le routage est basé sur le calcul de tous les plus-courts chemins entre la source et l'ensemble des destinations. Afin de considérer l'état instantané des ressources, ils reposent sur le modèle analytique proposé par Melia *et al.* (2002) pour l'approximation de la distribution de bande passante occupée sur chaque lien du réseau.

Dans une architecture centralisée de gestion de ressources, le contrôle d'admission consiste à assurer certaines contraintes de *QoS* (délai, bande passante, etc.) en performant du routage explicite à la lumière de l'état instantané des ressources du réseau. Cette approche est notamment implémentée grâce à la technologie *MPLS*, permettant l'établissement à la demande des nouveaux *LSPs*. Dans ce contexte, Oulai *et al.* (2007) ont proposé un algorithme de contrôle d'admission centralisé qui fait le calcul de chemins en fonction du délai maximal de bout-en-bout. Le délai sur les liens est cependant approximé par une file d'attente *M/M/1* et la méthode de routage repose sur la programmation mathématique. Ce dernier utilise le logiciel mathématique *CPLEX* pour la résolution du problème, en montrant la validité de leur méthode pour des réseaux de tailles réelles.

2.4.2 Contrôle d'admission dans les réseaux multicouches *GMPLS*

GMPLS offre une convergence logique et non-couteuse des architectures hétérogènes de réseaux de transport (permettant ainsi le provisionnement de bout-en-

bout de la *QdS*) et permet une gestion multicouche des ressources. Au niveau optique, la technologie de multiplexage de longueurs d'onde *WDM* constitue un moyen à faible coût d'augmenter la bande passante de la fibre en supportant plusieurs canaux ou longueurs d'onde instantanément. Basé sur cette topologie, un ensemble de chemins optiques pré-calculé est construit entre les routeurs *IP*. Ceci permet d'améliorer la connectivité logique du réseau en rendant des nœuds *IP*, physiquement non adjacents, voisins. La topologie ainsi construite est appelée topologie logique du réseau.

Le principal défi de la technologie *GMPLS* consiste à intégrer des fonctions d'ingénierie de trafic multicouche au sein d'un même et unique plan de contrôle, au lieu de les implémenter séparément au niveau de chaque couche (physique, optique, *MPLS*, *IP*, etc.).

Ce design inter-couches intégrant des mécanismes optiques et *IP* permet d'améliorer l'allocation des ressources du réseau et de bénéficier de la quasi-totalité de la bande passante offerte par le support physique. Il est cependant important, lors de l'établissement des *LSPs* au niveau *MPLS*, de tenir compte, non seulement des garanties de bande passante, mais aussi de la qualité de la transmission optique, au niveau *WDM*. En effet, les fibres optiques étant des supports de transmission non linéaires (Salvadori & Battiti, 2004), du bruit et de la distorsion du signal optique, causés principalement par les équipements intermédiaires (amplificateurs, commutateurs, convertisseurs de longueurs d'ondes, etc.), sont accumulés à travers le chemin optique.

Plusieurs algorithmes de contrôle d'admission ont été proposés dans la littérature pour les réseaux *MPLS* et *GMPLS*. Anjali *et al.* (2007) ont exploité le module intégré d'ingénierie de trafic de *GMPLS* pour adresser le problème du contrôle d'admission fiable. Ils proposent une méthode basée sur les politiques qui opère à

deux niveaux différents du réseau : *MPLS* (en choisissant un *LSP* faisable) et optique (en sélectionnant un chemin optique respectant la contrainte de continuité de longueurs d'ondes). L'objectif de la méthode est de créer un nouvel *LSP* entre deux nœuds du réseau quand le trafic véhiculé sur le *LSP* principale dépasse une certaine limite. Le nouvel *LSP* est disjoint à tous les *LSPs* précédemment créés pour la paire source-destination, ce qui leur permet de partager également un même *LSP* de secours.

Les réseaux *GMPLS* étant multicouches, certains travaux ont recouru à l'ingénierie de trafic inter-couches pour prendre les décisions de routage des *LSPs*. En effet, Cardillo *et al.* (2005) ont proposé un schéma de routage avec *QdS* dans les réseaux *GMPLS*. Dans cette approche, le routage d'un nouvel *LSP* est contraint à un nombre maximal de chemins optiques (*lightpaths*). L'approche proposée a permis de démontrer que l'intégration des métriques optiques pendant le routage améliore nettement les performances du réseau (en termes de taux de blocage des *LSPs* et de requis *QdS*). Dans cette même optique, Colliti *et al.* (2007) ont proposé un schéma de routage dynamique dans les réseaux *GMPLS*. Il développe un algorithme heuristique qui prend en compte différentes métriques des différentes couches du réseau (optique, physique, *MPLS*). Ce mécanisme garanti non seulement assez de bande passante pour le nouvel *LSP*, mais aussi une certaine qualité du signal optique et un délai maximal de propagation. Afin de prendre les décisions de routage des nouveaux *LSPs*, les auteurs proposent l'algorithme heuristique, nommé *MTQA* (*Minimum Transmission Quality Algorithm*), qui modifie la métrique de routage de manière à tenir compte de la qualité du signal et du délai de propagation.

2.5 Fiabilité des réseaux

Une des préoccupations majeures des concepteurs de réseaux optiques, et de réseaux en général, est de pouvoir faire face aux pannes pouvant survenir dans les

réseaux. Cela est d'autant plus important pour les réseaux optiques que leurs débits sont énormes. En effet, puisque ces réseaux se retrouvent assez souvent au niveau dorsal, une panne prolongée peut entraîner la perte d'une grande quantité d'information. L'objectif est donc de pouvoir reconfigurer le réseau très rapidement en utilisant les ressources encore fonctionnelles.

2.5.1 Mécanismes de fiabilité dans les réseaux optiques

Il existe deux types de pannes : panne de liens et panne de nœuds. Les pannes de liens sont généralement dues à des bris de liens tandis que les pannes de nœuds peuvent avoir diverses causes (Chamberland, 2004). D'autre part, les pannes de nœuds sont plus complexes à traiter car elles impliquent la désactivation de tous les liens liés au nœud, tandis qu'une panne de lien reste circonscrite à ce lien. Aussi, il apparaît plus judicieux de tenir compte des scénarios d'intérêt pour les administrateurs de réseaux. Comme la probabilité d'avoir deux éléments ou plus en panne simultanément est faible, on s'intéresse principalement aux pannes simples, dans la littérature.

De plus, lors d'une panne, il est possible de faire une reconfiguration totale de toutes les connexions ou simplement de re-router les connexions touchées par la panne. Bien que la reconfiguration totale puisse permettre de trouver globalement une meilleure solution, il est préférable de garder telles quelles les connexions qui sont encore fonctionnelles et d'essayer d'acheminer les autres.

Pour pallier les défaillances des réseaux optiques, deux types de méthodes sont utilisés : la protection et la restauration. La protection consiste à réserver des ressources du réseau qui seront utilisées comme *chemins de secours* (backups) en cas de panne. Cette approche est dite *proactive*. Généralement, les chemins de secours sont disjoints d'arcs des chemins principaux pour garantir la restauration en cas de

bris simple de lien (Anjale *et al.*, 2007 ; Gangxiang, 1999). Voici quelques exemples de protection (Stern *et al.*, 2000) :

- *Protection optique (1+1)* : les données sont envoyées simultanément sur le chemin principal et le chemin de secours. En cas de panne, le récepteur se syntonise sur le chemin de secours. Cette technique minimise le temps de résilience à la panne ;
- *Protection optique (1:1)* : Dans ce cas, un chemin de secours disjoint d'arc est réservé pour chaque chemin principal. Contrairement au (1+1), les informations ne sont pas envoyées simultanément sur les deux canaux. On n'émet sur le chemin de secours que lorsqu'une panne est déclarée sur le chemin principal ;
- *Protection optique (1:N)* : N chemins principaux partagent le même chemin de protection. En cas de défaillances touchant plusieurs chemins principaux, seul le trafic de plus haute priorité est re-routé. Afin de minimiser le nombre de chemins affectés, les chemins principaux qui sont protégés par un même chemin de secours doivent être disjoints de liens (pour les pannes simples de lien).

Comme on peut le constater, la protection est un moyen efficace et rapide de réponse face aux pannes de réseaux, vu que les ressources de secours sont réservées à l'avance d'une manière proactive. La restauration, quant à elle, calcule le nouveau chemin et y réserve les ressources après la panne, d'une manière réactive. La restauration peut être locale (appelée aussi restauration de lien) ou de bout-en-bout (appelée aussi restauration de chemin). Dans le premier cas, seule la partie défectueuse du chemin est contournée.

Bien que la restauration permette une meilleure utilisation de la bande passante du réseau, elle a pour principal inconvénient les délais relativement élevés pour

l'établissement réactif des nouveaux chemins de secours. En plus de cela, il n'y a aucune garantie d'acheminement car les ressources du réseau peuvent être épuisées, au moment de la panne.

2.5.2 Fiabilité dans les réseaux optiques avec ressources à risque partagé

Un groupe de ressources à risque partagé *SRRG* (*Shared Risk Resource Group*) consiste en un ensemble de ressources du réseau (liens, nœuds, etc.) qui sont regroupés dans un même contenant physique (salles d'équipements ou conduits pour les fibres). Dans le cas d'un conduit de fibres par exemple, le bris du conduit engendre le bris de toutes les fibres qui y passent, formant ainsi un group à risque partagé. Dans un tel cas, le groupe est nommé *SRLG* (*Shared Risk Link Group*). Si la technologie *WDM* est considérée, le bris du conduit engendre le bris de tous les chemins optiques véhiculés par chaque fibre. La Figure 2.2 montre un exemple de topologie physique contenant deux groupes de liens à risque partagé.

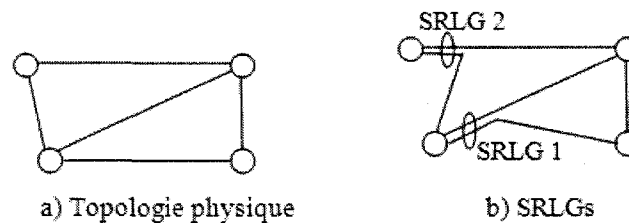


Figure 2.2 Topologie physique avec SRLGs

Le routage fiable d'un chemin optique consiste à trouver une paire de chemins (primaire et de secours) disjoints en termes de *SRLGs* (connu comme *Diverse Routing*). Le problème de routage avec *SRLGs* disjoints a été démontré NP-Complexe (Hu, 2003). Dans la littérature, plusieurs algorithmes heuristiques ont été proposés et permettent de faire un routage fiable avec contraintes de ressources à risque partagé (Datta *et al.*, 2004 ; Todimali *et al.*, 2004 ; Rostami *et al.*, 2007). Des travaux ont été également menés pour le routage fiable des arbres multicast, notamment par Li *et al.*

(2006) et Singhal *et al.* (2005). Afin de maximiser l'utilisation des ressources du réseau, Guo *et al.* (2007) ont proposé d'intégrer la notion de partage de ressources dans le routage fiable. Ils ont défini formellement les conditions pour lesquelles une même ressource (longueur d'onde sur une fibre) peut être partagée par différents chemins optiques. Un exemple simplifié de partage des ressources optiques est présenté à la Figure 2.3. Vu que les deux chemins primaires sont disjoints en termes de *SRLGs*, leurs chemins de secours peuvent partager le même canal sur la fibre *l*. En résumé, il est possible de partager un même canal sur une fibre par :

- deux chemins optiques de secours de deux connexions *t* et *tI*, si les chemins optiques primaires correspondants sont disjoints, en termes de *SRLGs* ;
- un chemin optique primaire pour une connexion *t* et un ensemble de chemins optiques de secours *tI* acheminés sur la même fibre, si chaque *SRLG* du chemin optique primaire de *t* appartient au moins à l'un des chemins optiques primaires de *tI*.

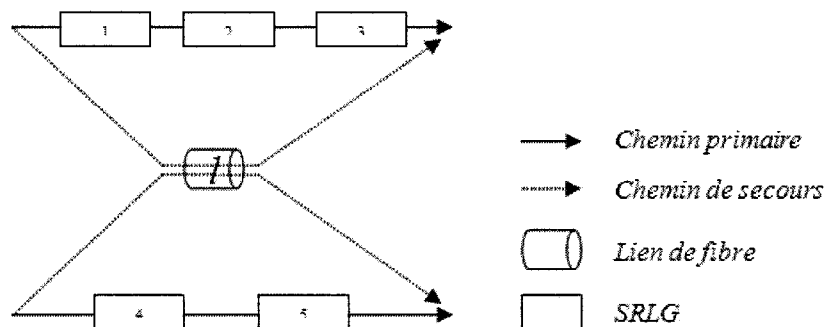


Figure 2.3 Partage des ressources par plusieurs chemins de secours

De plus, afin de minimiser le taux de blocage des nouvelles connexions, Guo *et al.* (2007) ont également considéré la notion de fiabilité différentielle. Il s'agit de considérer une garantie statistique de fiabilité, incluse généralement dans le contrat de

service ou *SLA*. Ainsi, pour chaque chemin optique, une probabilité maximale de panne est considérée. Dans ce cas, dépendamment du nombre de *SRLGs* empruntés par le chemin optique, il est parfois inutile de considérer un chemin de secours. Guo *et al.* (2007) ont ainsi proposé un algorithme heuristique, nommé *PSDP (Partial SRLG Disjoint Protection)* qui fait le routage des chemins optiques avec fiabilité différentielle. Les auteurs supposent que les pannes des *SRLGs* sont équiprobables et définissent la notion de fiabilité des chemins optiques. Dépendamment des requis de fiabilité des nouvelles connexions, une solution de routage peut comprendre soit un seul chemin optique primaire, soit une paire de chemins optiques (primaire et de secours).

CHAPITRE 3

A NOVEL ADMISSION CONTROL MECHANISM IN GMPLS-BASED IP OVER OPTICAL NETWORKS

Hichem Ayed Harhira and Samuel Pierre

Computer Engineering Department

Ecole Polytechnique de Montreal

CP. 6079 Succ. Centre Ville, Montreal (Qc), H3C 3A7, Canada

{hichem-ayed.harhira, samuel.pierre}@polymtl.ca

Abstract

With the migration of real-time and high-priority traffic in *IP* networks, dynamic admission control mechanisms are very important in high capacity networks where *IP* and optical technologies have converged with a *GMPLS*-based control plane. In this paper proposes, we propose an integrated Multi-layer Traffic Engineering framework that considers both physical and logical (optical layer) topologies for dynamically admitting new Label switched paths (*LSPs*) in *GMPLS* networks. The dynamic admission control mechanism is based on an optimal resolution of an Integer Linear Programming model that takes into account both lightpaths availability, wavelength

continuity and routing constraints. In order to minimize *LSPs* set-up delays, this mechanism first considers the logical topology (set of lightpaths) that is already in place before setting up a new lightpath for the incoming *LSP*, resulting in an additional set-up signalling delay. When tested by simulations, results confirm that the proposed formulation effectively improves the network performance by reducing the connection blocking rate, while guaranteeing strict delay and noise constraints.

Key words

Admission control, Generalized Multi-Protocol Label Switching (*GMPLS*), Quality of Service (*QoS*), optical transmission impairments, Dynamic routing.

3.1 Introduction

As the number of Internet users and the supported multimedia applications grow exponentially, new mechanisms, required to provide a certain level of Quality of Service (*QoS*) are becoming critical features for *IP* networks. In fact, over the last decade, new *QoS* requirements for traffic have emerged, due to the overwhelming demand for real-time and multimedia applications that involve data, voice, video, telephony, *IPTV*, etc. to be conveyed on the same network. In such a scenario, optical networks embedded with Wavelength-Division Multiplexing (*WDM*) technology is a key feature to provide high-capacity and cost-effective transport networks that are compatible with current higher level protocols such as Multiprotocol Label Switching (*MPLS*) and *IP*.

In classical *IP* routing, packet forwarding is conducted through routers, independently of their peers and only according to the destination address enclosed in the packet's *IP* header. Recently, research efforts have been deployed to enhance conventional *IP*-based architectures and protocols with *QoS* support, using

Multiprotocol Label Switching (*MPLS*). One of the attractive aspects of *MPLS* resides in the support of traffic engineering, by explicitly routing paths named Label Switched Paths (*LSP*) based on the *QoS* parameters of aggregated traffic. Another important component for providing *QoS*, however, is the ability to transport data in a reliable and efficient manner.

Control Plan	Forwarding Plan
GMPLS	MPLS: Set of LSPs
	Optical: Set of lightpaths
	Physical: Set of Fibers and Wavelength multiplexing

Figure 3.1 GMPLS control and forwarding plan

In the optical layer, WDM yields a cost-effective way to harness the fiber bandwidth by providing several parallel channels or wavelengths. In the upper level, a set of pre-computed end-to-end paths, called lightpaths, are set up between *IP* routers. This increases the network's logical connectivity, physically turning non adjacent nodes into adjacent ones (one hop) at the *IP* level. However, the advantages of high speed and highly connected networks must be accompanied by adequate traffic engineering mechanisms. Since the latter function is performed at different levels as shown in Figure 3.1, Generalized Multi-Protocol Label Switching (*GMPLS*) was developed to unify the network control-plane functions, encompassing both optical and *IP* levels. One of the main functionality challenges related to *GMPLS* consists of integrating the multi-layer traffic engineering functions into a unique control-plane instead of performing them separately at each layer (Physical, optical, *MPLS*). This is particularly relevant for optical networks that consist of Time-division Multiplexing *TDM* and Optical Cross-Connects (*OXC*s), all belonging to a same *GMPLS*-controlled domain and being connected through a general topology.

This cross-layer design integrating both *IP* and optical mechanisms when establishing traffic engineered *LSPs* improves the network throughput and resource usage. It is however important to take into account not only the bandwidth guarantees, but also the optical transmission quality when routing lightpaths to accommodate *IP* traffic. In fact, since the optical fiber is a nonlinear transmission medium, noise and signal distortions caused by non ideal transmission devices (*OXC*s, amplifiers, etc.) are accumulated along the physical path (Colliti *et al.*, 2006 ; Cardillo *et al.*, 2005 ; Savadori *et al.*, 2004).

On the other hand, it is important also to consider the end-to-end propagation delay while setting up a new *LSP*. For that, our proposed mechanism accommodates an *LSP* request on a path with strict noise and propagation delay constraints. We consider that not only bandwidth availability must be guaranteed, but also transmission quality in terms of signal noise and propagation delay, have to be satisfied. Our mechanism is based on optimally solving an Integer Linear Programming model that aims to route the new *LSP* over both the logical (set of lightpaths) and physical topologies, while guaranteeing a given level of transmission quality.

A multitude of admission control mechanisms have been proposed for *MPLS* and *GMPLS* over optical *WDM* networks (Ajmon *et al.*, 2007 ; Anjali *et al.*, 2006 ; Elias *et al.*, 2007 ; Hu & Muftah, 2006). Oulai *et al.* (2007) proposed a mathematical formulation for the admission control problem named JRAC, based on a given logical topology (set of *LSPs* in an *MPLS* domain). Mathematical model aims to minimize the global delay in the network while admitting a new connection. The admission control procedure includes not only bandwidth availability, but also delay constraints for the new and the already admitted connections. End-to-end delay is evaluated using the *M/M/1* queuing model. This NP-Hard problem can be solved easily by

CPLEX (Ilog., 2005) software suite for authentic instances (which are relatively small). Anjali *et al.* (2006) exploit the Integrated Traffic Engineering capabilities of the *GMPLS* technology to address issues of connection admission control and protection, based on the actual network state. They propose a policy-based decision framework that operates at two different levels: the *MPLS* network level, to choose or create a feasible *LSP*, and the optical level, to select a given wavelength-routed lightpath. The main goal consists of creating a new adjacent *LSP* when traffic surpasses a given threshold, computed according to the length of the new path and certain cost coefficients (including the signalling, switching and the network's connectivity costs).

Nevertheless, a few papers in the literature propose and discuss strategies where the admission control and routing decisions also involve physical and optical metrics (Colliti *et al.*, 2006 ; Cardillo *et al.*, 2005 ; Salvadori *et al.*, 2004). In fact, Cardillo *et al.* (2005) propose a *QoS* routing scheme for *GMPLS* networks. The *QoS* requirements of the *LSPs* are the number of lightpaths, and the number of physical hops (fibers). Their routing approach aims to demonstrate that the use of optical metrics for Multilayer Traffic Engineering improves the routing decisions.

Colliti *et al.* (2006) propose an online Multilayer Traffic Engineering scheme for *GMPLS* networks. Their mechanism guarantees sufficient bandwidth, a certain optical transmission quality and maximal propagation delays. To establish new *LSPs*, the *RSVP-TE* signalling protocol is deployed. Their approach is very interesting as it takes into account the physical properties of *GMPLS* networks and makes use of existing protocols for resources reservations. In order to perform the path selection for the new connection, authors propose an heuristic called *MTQA* (*Minimum Transmission Quality Algorithm*) that selects the shortest-path between the source and destination based on a routing metric that takes into account the signal noise and propagation delay. In spite of being simple and distributed, their mechanism does not

offer strict transmission quality for new connections as it merely attempts to minimize a linear combination of some *QoS* metrics over the selected path.

In this paper, we present a centralized algorithm that routes *IP* traffic considering the potential signal power penalty of all-optical communications. This algorithm consists of resolving to optimality an Integer Linear Programming model for routing new *LSPs* so that the signal quality and propagation delay constraints are guaranteed. In order to minimize the *LSP* set up delay, the algorithm first tries to route the request over a subset of ongoing lightpaths. If no feasible path is available, a new lightpath is set up involving free wavelengths on physical fibers.

The remainder of this paper is organized as follows. In Section 3.2 we state the considered admission control problem and formulate it mathematically. In Section 3.3 we show the performance evaluation and analyze the simulation results. Section 3.4 concludes this paper and points out some future research directions.

3.2 Problem Statement

In this section, we formulate the problem of joint routing and admission control in GMPLS networks. For that, we propose a new mathematical model for the admission control problem. The main idea is to take into account the maximum end-to-end delay as well as the maximum optical noise level while building the new admission control model.

3.2.1 Node model

By integrating both *IP/MPLS* packet switching and wavelength switching fabrics, a GMPLS node can be an end point or a switching point for both electronic *LSPs* and optical *Lambda-LSPs* or lightpaths. We assume that dynamic and continuous

information exchange is ensured between the *GMPLS* node controllers and the logical resource manager module that can be distributed over edge nodes, or centralized in stand alone equipment that holds a Path Computation Element (*PCE*) which is capable of accommodating a new connection request taking into account cross layer parameters.

On the other hand, each node is characterized by its number of optical transceivers (in the optical cross-connector *OXC*) and the number of *IP* ports. In our network model, only nodes with at least a free transceiver and port are involved in the routing of the new request.

3.2.2 End-to-end delay

When considering multi-level *GMPLS* networks, the experienced packets' delay is essentially due to:

- Physical layer delay: consisting in the optical signal propagation delay;
- Optical layer delay: including the transmission delay and the all-optical switching delay;
- MPLS layer delay: consisting in the MPLS label switching including the optical-electronic-optical signal conversions.

3.2.3 Signal quality

It is also important to consider the signal quality while routing a new connection request. In fact, the optical transmission quality is a critical issue that needs to be addressed as the optical fibers are non linear media. In fact, this non linearity results in a cumulative noise and signal distortion, that reflects the Optical Signal to Noise Ratio (*OSNR*) that needs to be increased in order to ensure a low Bit Error Rate (*BER*). Practically, the number of optical amplifiers, the number of hops and the number of wavelength conversions are the main contributors to the inherent

signal degradation and noise. In this work, an *LSP* can be routed over multiple lightpaths. As we assume that *LSRs* perform a full signal regeneration (as an optical-electrical-optical conversion is performed), the noise effect is only considered between logically adjacent *LSRs* instead of performing it end-to-end.

3.2.4 Mathematical formulation

The problem consists in choosing a route satisfying the above mentioned delay and signal quality constraints, the *WDM* wavelength continuity constraint and minimizing an objective that reflects the cost of admitting the new connection (establishing a new lightpath).

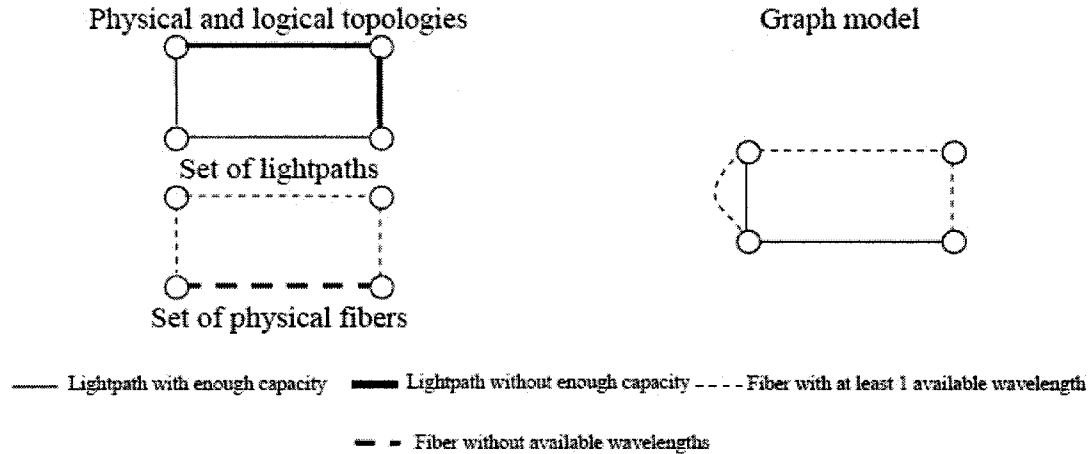


Figure 3.2 Construction of the network graph model using the logical and physical topologies

As shown in Figure 3.2, the considered network topology is represented by an oriented graph $G=(V,E)$, where V is the set of vertices (*LSRs*, *LERs* or *OXC*s) and E the set of both the physical links (fibers) and the logical links (lightpaths) connecting a pair of nodes. For every link $i \in E$, we denote by s_i and d_i , the source and destination nodes of the link i respectively. Note that if a node has no more available transceivers, all physical fibres connected to this node are removed from G .

Moreover, only fibers with available wavelengths and lightpaths with sufficient available bandwidth are considered. Thus, we denote by $E_l \subset E$ the set of lightpaths. The remaining set E_e of E , is the set of physical links. We assume that every physical link encompasses the same number W of wavelengths. On the other hand, we assume that physical nodes (*LSRs or OXCs*) may be wavelength-conversion capable allowing lightpaths to change their respective wavelengths. Then, let V_c , the subset of V containing all wavelength-conversion-capable nodes. The remaining subset is denoted V_{nc} and contains non wavelength-conversion-capable. Moreover, each lightpath l is defined by its delay D_l , its available bandwidth C_l , its source s_l , its destination d_l and two binary vectors Sw_l and Dw_l such that $Sw_l(k)$ is equal to 1 if and only if the lightpath l uses wavelength k on the source. Similarly, $Dw_l(k)$ is equal to 1 if and only if lightpath l uses wavelength k on its destination. Moreover, a lightpath l is characterized by a noise level n_l , including both the noise of optical amplifiers and wavelength converters. Taking into account the set of lightpaths already established, we can define the binary matrix F such that $F_{ek}=1$, if and only if wavelength k is free on link e .

Similarly, every physical link e is characterized by its source s_e , its destination d_e , its delay D_e , a noise level n_e (that depends on the number of optical amplifiers) and a set of free wavelengths, given by the matrix F , as shown above.

The new connection is characterized its source s , its destination d , the end-to-end propagation delay D_{max} and the maximum optical noise N_{max} . Thus, admitting a new connection consists in finding a feasible path, satisfying the *QoS* constraints (end-to-end delay and optical noise) and the wavelength continuity constraint across non-converter nodes.

It is important to note that the lightpath delay D_l encompasses the fibers propagation delays as well as the optical switching delay but does not include the

optical-electronic-optical conversion and label switching delay. For that, we define D_{o-e-o} as the delay encountered by both the optical-electronic-optical conversion and the label switching. Moreover, we denote by n_c the signal degradation due to a wavelength conversion along the physical path.

At this stage, we can present a mathematical formulation of the joint routing and admission control problem in *GMPLS* networks. For that, we define the binary variables $V_{ik}, \forall i \in V_x - \{s, d\}$ and $\forall k \in W, X_l, \forall l \in E_l, Y_{ek}, \forall e \in E_s$ and $\forall k \in W$ and Z as following:

$$V_{ik} = \begin{cases} 1, & \text{if the wavelength } k \text{ is optically converted through node } i \text{ in the new lightpath} \\ 0, & \text{otherwise} \end{cases}$$

$$X_l = \begin{cases} 1, & \text{if the lightpath } l \text{ is selected} \\ 0, & \text{otherwise} \end{cases}$$

$$Y_{ek} = \begin{cases} 1, & \text{if the wavelength } k \text{ over the fiber } e \text{ is selected} \\ 0, & \text{otherwise} \end{cases}$$

and

$$Z = \begin{cases} 1, & \text{if a new lightpath is set up} \\ 0, & \text{otherwise} \end{cases}$$

As argued above, the objective of the model is to minimize the cost of admitting the new connection by minimizing the length of the new path and implying a penalty P_{NL} as a new lightpath is set up. The mathematical model is thus presented as follows:

$$\text{Minimize } \sum_{l \in E_l} X_l + Z.P_{NL} \quad (3.1a)$$

Subject to:

$$Y_{ek} \leq F_{ek} \quad \forall e \in E_e, \forall k \in W \quad (3.1b)$$

$$Z \geq Y_{ek} \quad \forall e \in E_e, \forall k \in W \quad (3.1c)$$

$$Z \leq \sum_{e \in E_e} \sum_{k \in W} Y_{ek} \quad (3.1d)$$

$$\sum_{k \in W} Y_{ek} \leq 1 \quad \forall e \in E_e \quad (3.1e)$$

$$\sum_{l \in E_l} D_l X_l + (Z + \sum_{l \in L} X_l - 1).D_{o-e-o} + \sum_{e \in E_e} \sum_{k \in W} D_e Y_{ek} \leq D_r \quad (3.1f)$$

$$\sum_{e \in E_e} \sum_{k \in W} n_e.Y_{ek} + \sum_{i \in V_c - \{s,d\}} \sum_{k \in W} n_c.V_{ik} \leq N_{\max} \quad (3.1g)$$

$$n_l.X_l \leq N_{\max} \quad \forall l \in E_l \quad (3.1h)$$

$$V_{ik} \leq \sum_{\substack{e \in E_e \\ d_e = i}} Y_{ek} \quad \begin{matrix} \forall i \in V_c - \{s,d\}, \\ \forall k \in W \end{matrix} \quad (3.1i)$$

$$V_{ik} \leq 1 - \sum_{\substack{e \in E_e \\ s_e = i}} Y_{ek} \quad \begin{matrix} \forall i \in V_c - \{s,d\}, \\ \forall k \in W \end{matrix} \quad (3.1j)$$

$$V_{ik} \geq \sum_{\substack{e \in E_e \\ d_e = i}} Y_{ek} - \sum_{\substack{e \in E_e \\ s_e = i}} Y_{ek} \quad \begin{matrix} \forall i \in V_c - \{s,d\}, \\ \forall k \in W \end{matrix} \quad (3.1k)$$

$$\sum_{\substack{l \in E_l \\ i = s_l}} X_l + \sum_{\substack{e \in E_e \\ i = s_e}} \sum_{k \in W} Y_{ek} - \sum_{\substack{l \in E_l \\ i = d_l}} X_l - \sum_{\substack{e \in E_e \\ i = d_e}} \sum_{k \in W} Y_{ek} = \begin{cases} 1, & \text{if } i = s \\ -1, & \text{if } i = d \\ 0, & \text{otherwise} \end{cases} \quad \forall i \in V_c \cup \{s,d\} \quad (3.1l)$$

$$\sum_{\substack{l \in E_l \\ i = s_l}} S w_k.X_l + \sum_{\substack{e \in E_e \\ i = s_e}} Y_{ek} - \sum_{\substack{l \in E_l \\ i = d_l}} D w_k.X_l - \sum_{\substack{e \in E_e \\ i = d_e}} Y_{ek} = 0 \quad \begin{matrix} \forall i \in V_{nc} \cup \{s,d\}, \\ \forall k \in W \end{matrix} \quad (3.1m)$$

$$X_l \in \{0,1\} \quad \forall l \in E_l \quad (3.1n)$$

$$Y_{ek} \in \{0,1\} \quad \forall e \in E_e, \forall k \in W \quad (3.1o)$$

$$V_{ik} \in \{0,1\} \quad \forall i \in V_c \cup \{s, d\}, \quad (3.1p)$$

$$\forall k \in W$$

$$Z \in [0,1] \quad (3.1q)$$

As presented above, the admission control problem is formulated as an integer linear programming model that is NP-Hard. In fact, if we consider for instance that all nodes are equipped with wavelengths converters ($V_c = V$), the constrained-routing problem, that is NP-Hard (Garey & Johnson, 1979), can be merely reduced to our *GMPLS* admission control problem.

The first equation is the objective function of the model. Expressions (3.1b) to (3.1p) are the model constraints. Constraint (3.1b) is the wavelength unicity constraint ensuring that only free wavelengths are considered. The constraints (3.1c) and (3.1d) ensure that the binary variable Z is equal to 1 if and only if a new lightpath is set up for the new connection. Constraint (3.1e) guarantees that a unique wavelength is used for the new lightpath. The equation (3.1f) is the maximum delay constraint ensuring that the end-to-end delay on the selected path does not exceed the connection maximum delay D_{max} . Note that the expression of the delay includes the propagation delay and the switching delay. Similarly, equation (3.1g) is the maximum signal noise constraint ensuring a minimum signal quality level, noted N_{max} . Constraints (3.1h) to (3.1j) ensure that any variable V_{ik} is equal to one, if and only if the wavelength k is converted in node i , for the newly created lightpath. Note that the scope of variables V only includes the wavelength-conversion-capable nodes. Constraints (3.1k) and (3.1l) are the flow conservation constraint along the connection's path for respectively non conversion capable nodes and conversion capable nodes. Note that the first constraint also ensures the wavelength continuity over the connection path, for non-conversion capable nodes. Finally, expressions (3.1i) to (3.1n) give the domains of the model variables.

As a recap, our admission control mechanism consists on two separate phases:

- *Pre-processing phase*: during which the network topology is built from the physical and logical topologies;
- *Admission control phase*: during which the admission control mathematical model is set up and resolved.

3.3 Numerical Results

Despite being NP-Hard, the proposed ILP problem can be optimally solved within reasonable computation time. In fact, the number of integer variables is relatively small for real-size topologies. To do so, the CPLEX (Ilog, 2005) mathematical programming tool is used to solve the model. Note that this solution uses the branch-and-bound algorithm to solve integer problems.

Prior to presenting simulation results and assessing the accuracy of the proposed mechanism, the experimental parameters are first disclosed here:

- We set the penalty $P_{NL} = |E| + 1$, privileging thus the use of the ongoing lightpaths;
- We set $D_e = 0.02ms$, the propagation delay on a single fiber;
- We set $D_l = \sum_{e \in l} D_e$, the propagation delay of lightpath l ;
- We set $D_{o-e-o} = 0.06ms$, the label switching delay;
- We set $n_e = 2$ units, the signal noise introduced by a single fiber, depending on the length and the number of amplifiers in the fiber;
- We set $n_l = \sum_{e \in l} n_e$, the signal noise introduced by lightpath l ;

- We set $n_c = 5$ units, the signal noise introduced by a single wavelength conversion.

To evaluate the performance of our admission control mechanism, we propose to calculate the *LSPs* acceptance rates for different network sizes and configurations. The considered physical topologies are given in Table 3.1. These networks were randomly generated as follows. An hamiltonian cycle was first greedily built around the nodes to ensure that topologies are bi-connected. This fact is very important as it ensures the network's connectivity and maximizes the number of disjoint paths between every pair of nodes. Once the cycle constructed, the remaining edges are randomly placed. As for nodes degrees, the mean nodes' degree decreases as the number of nodes increases. In fact, as we want to reflect real case networks, small networks have usually a higher connectivity than large networks, due to economic, physical and technological considerations. Indeed, the mean nodes' degree is around 65% for N1 and falls to approximately 10% for N5.

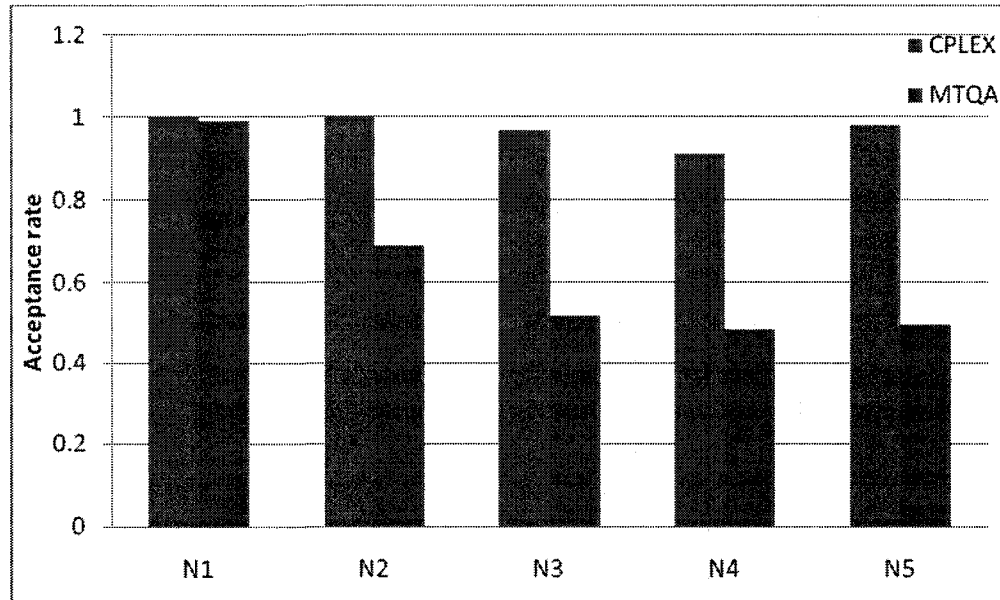
As for the logical topology, we assumed that, over every physical topology, a certain number of lighpaths was randomly setup between every two physically adjacent nodes. As the current network's load is a key parameter, two different values for the mean network's load were considered (55% and 80%). The remaining bandwidth of each lighpath was randomly generated as well and the mean lighpaths occupancy was around 55% and 80% respectively.

In order to evaluate the algorithm blocking rate, we generated all possible connections originating and terminating in an edge node. The total number of these connection depends on the network's size and is equal to $|F|(|F|-1)$. Moreover, we assume that a single connection arrives at a time. These connections have the same following set of parameters:

Table 3.1 Considered physical topologies

<i>Network</i>	$ V $	$ E $	$ F $
N1	10	30	6
N2	30	90	18
N3	50	150	30
N4	70	210	42
N5	90	270	54

- Maximum end-to-end delay $D_{max}=0.2\ ms$;
- Maximum signal noise level $N_{max}=20\ units$;
- Data rate $b = 10Mbps$.

**Figure 3.3 Comparative results: CPLEX vs. MTQA for a network mean load of 55%**

We first compare the performance of our admission control mechanism against the *MTQA* algorithm described above and proposed by Colliti et al. (2006). This latter also tackles the routing problem of *LSPs* in a *GMPLS* controlled network. However, authors do not consider strict bounds neither on the end-to-end delay nor the signal noise. In fact, their algorithm merely finds a path over both the physical and logical topologies that minimizes a linear combination of these two metrics.

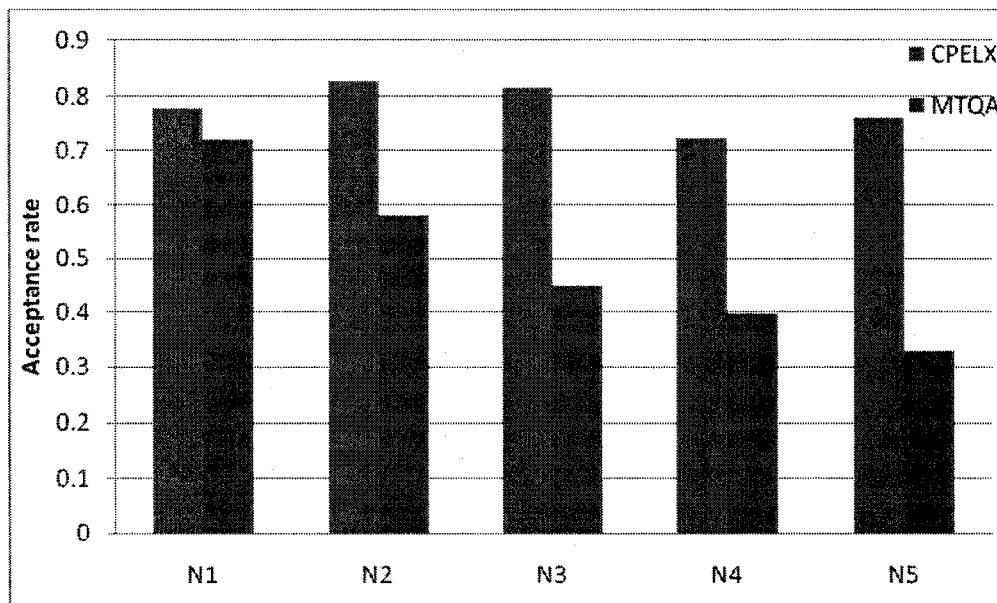


Figure 3.4 Comparative results: CPLEX vs. MTQA for a network mean load of 80%

As Colliti et al. (2006) only consider that all nodes are equipped with wavelength converters, we consider, in the first set of simulations, that $V_c=V$ and show in Figure 3.3 the number of accepted *LSPs* for our scheme versus the *MTQA* algorithm. It is straightforward that our mechanism allows for higher performances and clearly outperforms *MTQA* algorithm in terms of the number of accepted *LSPs*. The gap between the two routing and admission control schemes reaches 60% for the 90 Nodes network. In addition, we can clearly notice this gap increases as the

network size increases. This is mainly due to the fact that *MTQA* algorithm does not consider strict bounds on the delay and the signal quality.

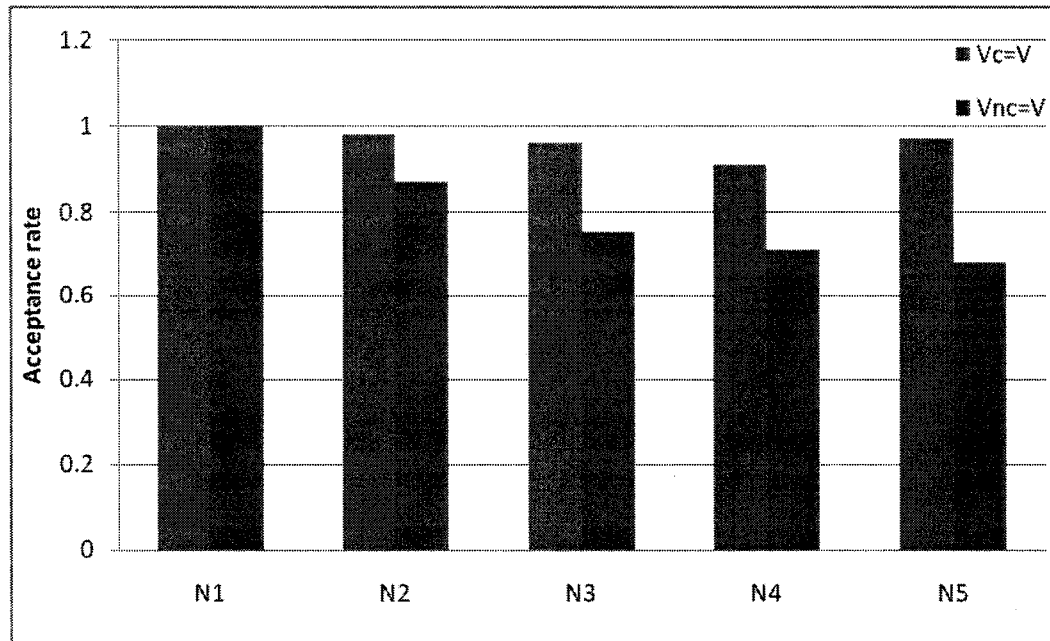


Figure 3.5 Effect of the number of wavelengths converters in the network on the number of admitted connections

Figure 3.5 depicts the number of accepted connections provided by our admission control mechanism for two different levels of wavelength conversion capabilities. In fact, we first consider that all the networks' nodes are equipped with wavelength converters and thus $V_c=V$. We also consider, in a second time, that no wavelength conversion is allowed and thus $V_{nc}=V$. It is quite expected that the number of accepted *LSPs* decreases with lower conversion capabilities. It is however interesting to notice that performances of our mechanism decrease when $V_{nc}=V$ as the network sizes increase. In fact, as the same bounds on the delay and signal noise are considered for all topologies, it becomes harder to find feasible paths (that must be kept relatively small to respect delay and noise bounds) with a continuous wavelength from the source to the destination, as the network size increases.

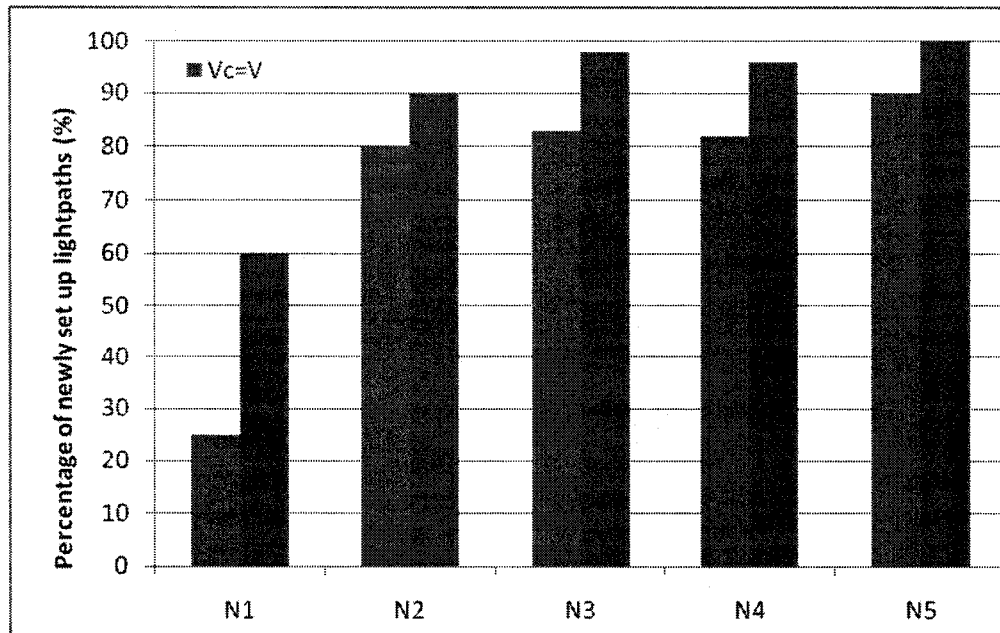


Figure 3.6 Effect of the number of wavelengths converters in the network on the percentage of setting up new lightpaths for new LSPs

As discussed above, the objective function of the *ILP* encompasses a penalty term P_{NL} that penalizes the use of a new lightpath for the incoming *LSP*. In order to minimize this expression, the mechanism tries first to route the *LSP* over the logical topology. If no feasible path is found (due to delay, noise or wavelength continuity constraints), a new lightpath is set up to carry the incoming *LSP*. We then evaluate the percentage of new lightpaths for different levels of wavelength conversion capabilities. As depicted in Figure 3.6, we clearly notice that when no conversion is allowed, the percentage of new lightpaths required to carry incoming *LSPs* is much higher. The main reason is that, in such a case, the wavelength continuity constraint has to be also taken into account in the routing process.

It is finally important to mention that the worst case computation times did not exceed 0.5 second for the 90 Nodes network with no wavelength conversion capabilities. This latency is quite acceptable for making the decision of admitting a

new *LSP* with strict delay and noise level bounds constrained to wavelength continuity. Once the new path is computed, a signalling protocol, such as *RSVP-TE*, can be responsible for spreading the information between *IP* and optical equipments to set up mixed *LSPs*.

3.4 Conclusion

In this paper, we proposed a new routing and admission control mechanism in *GMPLS* controlled networks based on formulating the problem as an *ILP* that satisfies optical delay and transmission quality constraints.

For that, the process of selecting a particular path for the incoming *LSP* depends on the optical propagation delay, the label switching delay in *LSRs*, the signal noise introduced by amplifiers and *OXC*s and possibly wavelength converters. We assume that a new *LSP* is strictly constrained to a maximum delay and signal noise levels. Consequently, we propose a mathematical formulation for the joint routing and admission control problem and solve it to optimality. The proposed mechanism was tested by simulations and compared with other traditional mechanisms found in the literature. The results confirm that the proposed formulation effectively improves the network performance by reducing the connection blocking rate, while guaranteeing strict delay and noise constraints.

Future research directions include plans to consider additional *QoS* constraints while admitting and routing new *LSPs*. Multi-fiber networks will also be considered in future work.

CHAPITRE 4

JOINT ROUTING AND ADMISSION CONTROL PROBLEM UNDER STATISTICAL DELAY AND JITTER CONSTRAINTS IN MPLS NETWORKS

Hichem Ayed Harhira and Samuel Pierre

Computer Engineering Department

Ecole Polytechnique de Montreal

CP. 6079 Succ. Centre Ville, Montreal (Qc), H3C 3A7, Canada

{hichem-ayed.harhira, samuel.pierre}@polymtl.ca

Abstract

Admission control algorithms are crucial for ensuring a near optimal resource allocation while guaranteeing the required Quality of Service (*QoS*) constraints. In this paper, a new routing and Admission Control mechanism in Multi-Protocol-label-switching (*MPLS*) based networks is proposed. The proposed mechanism relies on the packets' delay distributions that are empirically built on every link, to make adequate admission decisions. As a new connection request arrives, the admission control mechanism computes a feasible path, satisfying the connection's statistical *QoS* constraints (the maximum end-to-end delay, jitter and the *QoS* violation probability). For that, we formulate this problem as an Integer Linear Programming (*ILP*) model that is solved to

optimality using the *CPLEX* mathematical programming tool for real-size networks. Simulation results show that the new admission control mechanism allows for low blocking rates while statistically satisfying the *QoS* constraints for both the new and the ongoing connections.

Key words

Admission control, Multiprotocol Label Switching (*MPLS*), dynamic routing, Quality of Service (*QoS*), mathematical programming.

4.1 Introduction

When it was first designed, *IP* was not intended to provide *QoS* guarantees and was limited to best-effort services. In fact, *IP* routing is mainly based on *OSPF* (Open Shortest Path First) protocol which does consider neither links' capacity nor connection's *QoS* requirement. In the last decade, new *QoS* requirements have emerged due to the overwhelming demand for real-time and multimedia applications which involve data, voice, video, telephony, *IPTV*, etc. to be conveyed by the same network. Consequently, traffic engineering, as well as dynamic connections' admission control are settling down as new important tools to optimize *IP* networks.

In classical *IP* routing, packet forwarding is operated by routers independently of their peers and it is only based on the destination address enclosed in the packet's *IP* header. Recently, research efforts have been deployed to enhance conventional *IP*-based architectures and protocols with *QoS* support using Multi-Protocol Label Switching (*MPLS*). One of the attractive aspects of *MPLS* is the support of traffic engineering, that is, explicitly routing paths named Label Switched Paths (*LSP*) based on *QoS* parameters of aggregated traffic.

In this paper, we consider an *MPLS*-based network offering traffic engineered routing. We also consider that, in addition to the bandwidth constraints, real-time applications (voice, video, etc.) may need end-to-end *QoS* guarantees such as bounds on the delay and jitter. Consequently, dynamic admission control mechanisms are very important to make real-time decisions while considering both bandwidth availability and end-to-end *QoS* constraints. For that, we propose a new admission control mechanism in *MPLS*-based networks. This mechanism relies on formulating the problem as an Integer Linear Programming (*ILP*) model that performs both the routing and the admission control of the new connections, taking into account the statistical end-to-end delay and jitter constraints.

The remainder of this paper is organized as follows: in Section 4.2, some relevant related works are exposed and explained. In Section 4.3, the mathematical formulation of the joint routing and admission control problem is presented. In Section 4.4, the proposed mechanism is implemented and numerical results are discussed. Section 4.5 concludes this paper and points out some future researches.

4.2 Related Works

Admission control algorithms in fixed *IP* networks can be divided into three types (Gerla *et al.*, 2001): parameter-based, measurement-based and probe-based. Parameter-based algorithms can be deterministic or stochastic. In the former case, worst-case scenarios are considered, leading to an under-utilization of the network resources. Measurement-based algorithms are usually more appropriate for resource utilization (Gopalan *et al.*, 2004 ; Abuali *et al.*, 2005). These algorithms base their decisions on real-time measurements (collecting information on the network and the traffic). Finally, in probe-based algorithms, probing packets are sent in order to empirically evaluate

some *QoS* parameters such as the mean round-trip time, the packet loss rate, the mean jitter, the available bandwidth, etc. (Qian *et al.*, 2003).

In general, admission control schemes can be distributed or centralized. Distributed approaches are generally based on distributed signaling protocols (for example, RSVP for resource reservation). As far as centralized approaches are concerned, decisions are made within a Centralized Resource Manager (*CRM*), responsible for collecting and compiling operational information on the whole Autonomous System (*AS*), in order to take adequate actions in real-time.

A multitude of admission control algorithms were proposed in the literature (Gopalan *et al.*, 2004 ; Qian *et al.*, 2004 ; Harhira & Pierre 2007 ; Rhee *et al.*, 2004 ; Abuali *et al.*, 2005). Some parameter-based approaches use the analytical concept of effective bandwidth (Courcoubetis *et al.*, 1999) and assume a preliminary knowledge of the fluid traffic distribution. Measurement-based approaches are rather based on a signaling protocol where decisions are made locally for each considered link. Such a decision is mainly based on the amount of free bandwidth and on the live delay distributions on the links for a given class of traffic.

Gopalan *et al.* (2004) proposed to empirically build a cumulative distribution function of the delay on every link, using the histogram technique. They also make an approximation of the effect of changing the link's load (by admitting a new connection) on the computed distribution. Abuali *et al.* (2005) showed that delay distribution can be approximated by a Gamma distribution. The shape and scale parameter of the Gamma distribution are obtained empirically and are shown to be dependent mainly on the actual link's load. Authors also propose a Statistical Delay - Measurement based Admission Control algorithm (*SD-MBAC*) that satisfies the statistical delay constraints for all the ongoing connections. Similarly, Gopalan *et al.* (2004) proposes the Delay Distribution Measurement algorithm (*DDM*) that builds an acceptance zone depending on the

statistical *QoS* constraints. Despite of having attractive results, their algorithms are rather local do not consider neither path allocation nor end-to-end *QoS* guarantees.

Anjali *et al.* (2006) exploited the Integrated Traffic Engineering capabilities of the *GMPLS* technology to address the problem of connections admission control and protection based on the actual network state. They proposed a policy-based decision framework that operates at two different levels: the *MPLS* network level, for choosing or creating a feasible *LSP*, and the optical level, for choosing a given wavelength-routed lightpath. The main idea is to create a new adjacent *LSP*, whenever traffic exceeds a given threshold, computed with respect to some cost coefficients (including the signaling cost, the switching cost, the network's connectivity cost) and to the length of the new path. Nevertheless, their policy-based algorithm only ensures bandwidth requirements and does not consider other *QoS* requirements such as end-to-end delay and jitter.

On the other hand, Casetti *et al.* (2007) proposed an admission control mechanism performing path allocation for Service Level Agreements (*SLA*) in a *DiffServ* domain for the Assured Forwarding (*AF*) class. Authors assume that a load probability distribution function is already built on every link. This probability function is approximated in (Mellia *et al.*, 2002) with respect to the intrinsic characteristics of the set of carried *SLAs* (Maximum data rate, probability of serving a given destination d , maximum overbooking probability, etc.). Their admission control algorithm computes a feasible tree (for multicast traffic), such that the overbooking probability is not exceeded on every selected link.

Elias *et al.* (2007) proposed a new service model for intra-domain *QoS* provisioning and develop online dynamic bandwidth allocation algorithms based on the statistical traffic characteristics. They first proposed a mathematical formulation of the extra-bandwidth allocation problem that maximizes network revenue and obtain upper

bounds on the optimal bandwidth allocation problem. Authors however do not address end-to-end *QoS* issues, in terms of the delay, packet loss probability or jitter.

We also proposed (Harhira et Pierre, 2007) a mathematical formulation of the admission control problem aiming to minimize the overall network delay. We assumed that the logical topology (set of *LSPs* in an *MPLS* domain) was already constructed. The admission control algorithm consists of finding a feasible set of paths such that the end-to-end delay constraint is satisfied for both the new and the ongoing connections. The delay on every link is the mean delay undergone by a packet of a fixed length in an *M/M/1* queue (depending on the capacity and the actual load of the link).

In this paper, we propose a new admission control mechanism in *MPLS*-based networks. This mechanism is formulated as an Integer Linear Programming (*ILP*) model that performs both, routing and admission control of the new connections, taking into account the end-to-end statistical delay and jitter constraints. For that, we assume that the statistical description of the delay is empirically known on every link and accordingly develop the end-to-end requirements for statistically guaranteeing the delay and jitter constraints.

4.3 Problem Statement

In this section, we describe our mathematical model for the admission control problem under statistical delay and jitter constraints. As discussed above, the delay encountered by the data packets on a given router's interface generally depends on several parameters such as the corresponding link's load, the mean size of packets, etc. In order to guarantee statistical delay and jitter constraints, we assume that each router builds a delay distribution for each enabled interface using the histogram method as in (Gopalan *et al.*, 2004). Several works in the literature focused on approximating the delay distribution nature obtained empirically. In most of these works, the random

variable describing the packets' delay was shown to follow the Gamma distribution (Abuali *et al.*, 2005 ; Costantiescu et Popescu, 2006). In our model, the distribution nature is not an issue as only the first and the second moments (the mean and the variance respectively) are needed to approximate the end-to-end jitter and delay violation probabilities.

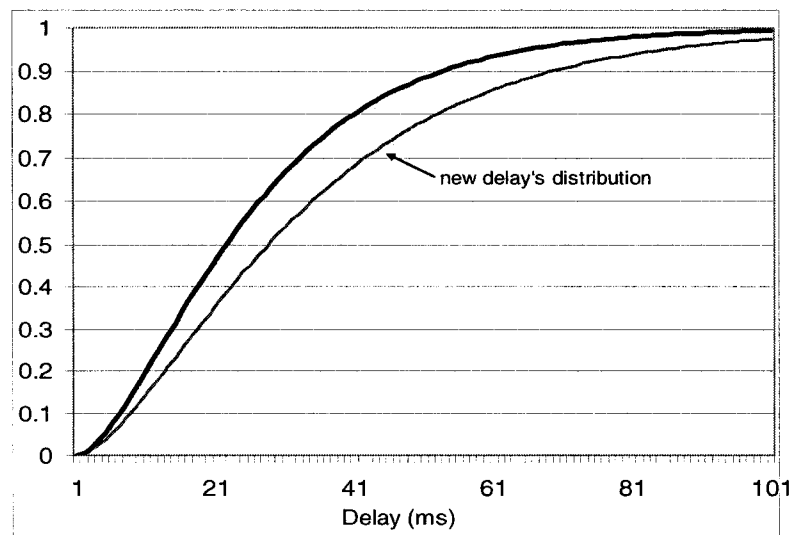


Figure 4.1 Effect of admitting a new connection on the delay's distribution

We assume that the delay distribution is already built on every link (interface) using the histogram method and that routers empirically compute the means and variances of the delay distributions.

Moreover, admitting a new flow on a given link alters the delay distribution on that particular link. Figure 4.1 shows an example of a cumulative distribution function (*cdf*) of the delay distribution before and after admitting the new flow (Gopalan *et al.*, 2004). Because admitting a new flow through a given link increases its mean delay, the corresponding *cdf* moves slightly to the right as depicted in Figure 4.1. This translation depends on the current link's load and the new flow's data rate. An example of the mean

and variance of the delay distribution empirically obtained function of the link's load is given in Figure 4.2, as provided by Gopalan *et al.* (2004). We notice that the more the link is loaded (and thus the *cdf* given in Figure 4.1 translates to the right), the greater is the mean. However, we notice that the variance slightly decreases as the link becomes loaded. In fact, the variance depends directly on the burstiness of the overall traffic that is attenuated as the link becomes loaded.

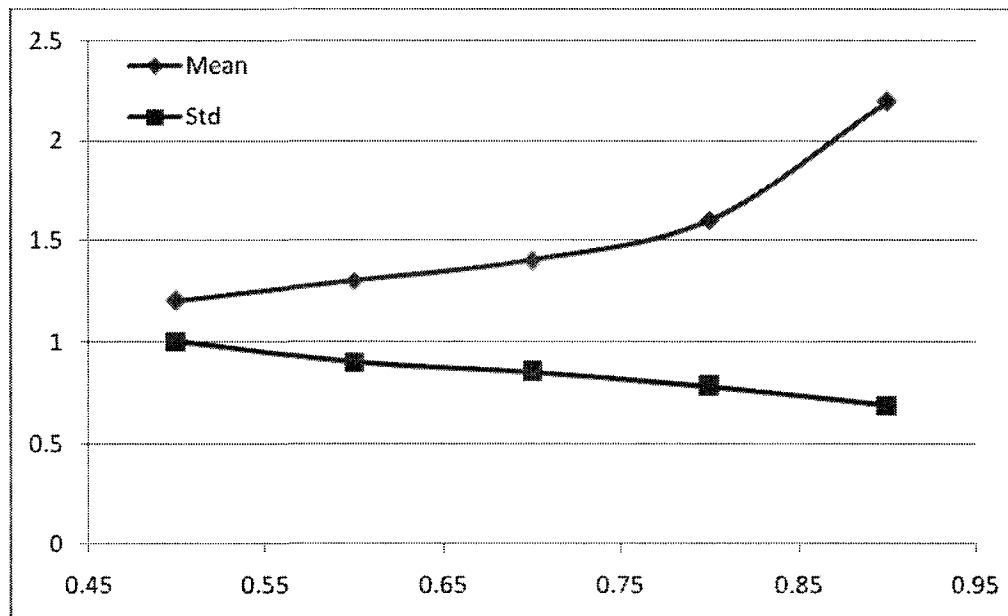


Figure 4.2 Average delay and variance with respect to the link's load

Moreover, Abuali *et al.*, (2005) showed that the delay distribution can be approximated by a Gamma random variable and empirically measured the parameters of the obtained distribution with respect to the link's utilization. In our further developments, we assume that the delay distribution for a given link has an unknown distribution and we only base our approximations on its empirically obtained mean and variance.

4.3.1 The end-to-end delay distribution: mean and variance computation

Let denote by D_i the random variable of the packets delay for the interface connected to the physical link i . This random variable is characterized by its mean $\overline{D_i}$ and its variance σ_i^2 . Let also M be the path taken by a connection characterized by its end-to-end statistical delay and jitter constraints. Let G_{max} be the maximum jitter, D_{max} the maximum delay and P the maximum QoS violation probability (violation of the delay and jitter constraints). It is however very difficult to approximate the end-to-end delay distribution D as it is the sum of $|M|$ random variables of unknown nature. Nevertheless, we can assume that the delays on the different links are independently distributed and thus we merely obtain the parameters of the end-to-end delay distribution as follows (Daveport, 1970):

$$\overline{D} = \sum_{i=1}^{|M|} \overline{D_i} \text{ and } \sigma_D^2 = Var \sum_{i=1}^{|M|} D_i = \sum_{i=1}^{|M|} \sigma_i^2 \quad (4.1)$$

In equation (4.1) the end-to-end delay's mean is merely the sum of the means on every link of the path. Similarly, the variance of the end-to-end delay's distribution is the sum of the local variances in every link, as the mentioned distributions are assumed to be independent.

4.3.2 End-to-end jitter and delay constraints

As depicted in Figure 4.3, the jitter is defined as the maximum gap between the real packet delay and the mean delay computed empirically. The example given in Figure 4.3 shows the probability distribution of the packets' delay and the according value of the jitter violation probability, corresponding to the highlighted area under the curve.

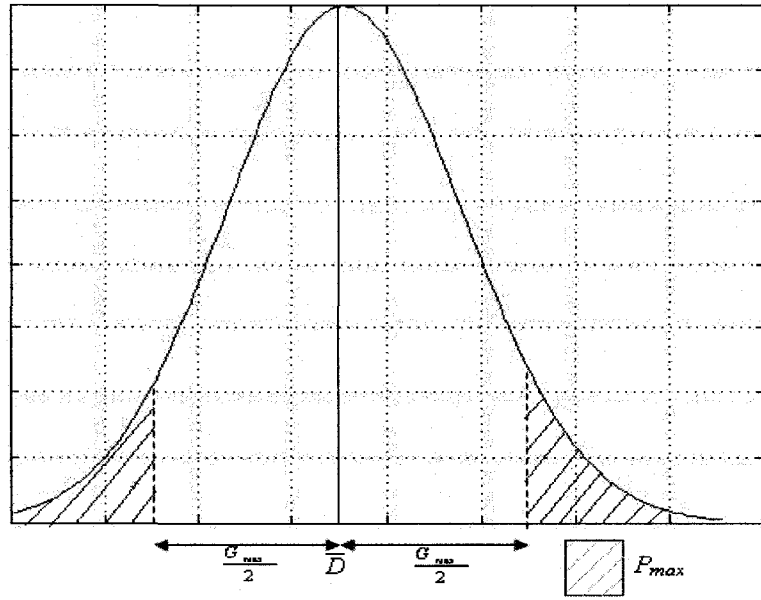


Figure 4.3 Jitter violation probability for a given delay's distribution *pdf*

As the delay distributions on the different network's links are assumed independent, an upper bound on the jitter violation probability can be obtained as follows:

$$P_{\max} = 1 - \Pr\left(\bar{D} - \frac{G_{\max}}{2} < D < \bar{D} + \frac{G_{\max}}{2}\right) = \Pr\left(|D - \bar{D}| > \frac{G_{\max}}{2}\right) \quad (4.2)$$

Consequently, by applying the *Tchébitchev* inequality (Daveport, 1970), we merely obtain the following upper-bound on the jitter violation probability:

$$\Pr\left(|D - \bar{D}| > \frac{G_{\max}}{2}\right) \leq \frac{\sigma_D^2}{\left(\frac{G_{\max}}{2}\right)^2} = \frac{4 \cdot \sigma_D^2}{G_{\max}^2} = \frac{4 \cdot \sum_{i=1}^{|M|} \sigma_i^2}{G_{\max}^2} \quad (4.3)$$

Thus, a way to guarantee the jitter violation probability is to ensure

$$\text{that } \frac{4 \cdot \sum_{i=1}^{|M|} \sigma_i^2}{G_{\max}^2} \leq P_{\max}, \text{ on the chosen path.}$$

As far as the maximum delay constraint is concerned, it can merely be controlled by the jitter constraint. In fact, this latter ensures that the end to end delay of a given packet is bounded by $\bar{D} - \frac{G_{\max}}{2}$ and $\bar{D} + \frac{G_{\max}}{2}$ for $(1 - P_{\max}) \times 100\%$ of the cases. Thus, by ensuring that the delay is lower than $\bar{D} + \frac{G_{\max}}{2}$, the delay violation probability is guaranteed consequently.

4.3.3 Approximating the new delay distribution after the admission of a new flow

As discussed previously, admitting or removing a flow on a link alters its packets delay distribution. In order to appraise the new delay distribution through a particular link after admitting a new flow, we approximate the system encompassing the buffer and the link server by a $G/G/I$ queuing system, as the packets' arrival distribution is generally unknown. For that, we assume that routers approximate empirically the packets' inter-arrivals variance, noted σ_T^2 , for every interface. In fact, according to Bose (2001), an upper bound on the delay spent by packets of mean size L on a given link i , can be written as follows:

$$D_i \leq \frac{\lambda(\sigma_T^2 + \sigma_X^2)}{2.L.(1 - \frac{\lambda}{c})} + \frac{L}{c} \quad (4.4)$$

Where λ is the current data rate, c is the serving rate, that is constant in our case and equal to the link capacity and σ_x^2 is the variation of the serving time that is equal to 0, as the serving rate corresponds to the constant link bandwidth.

After admitting a new flow over a link, the delay's upper-bound given in equation (4.4) increases, as parameters λ and σ_T^2 are altered consequently. It is obvious that when a new flow, having a rate of $\Delta\lambda$ is admitted, the incoming data rate increases consequently and is then equal to $\bar{\lambda} = \lambda + \Delta\lambda$. As for the variance of the packets inter-arrival, it can be easily shown to decrease as the link becomes loaded (Bose, 2001). Based on these facts, we can merely approximate the new delay bound as follows:

$$\overline{D_i} \leq \frac{\bar{\lambda} \cdot \sigma_T^2}{2(1 - \frac{\bar{\lambda}}{c}) \cdot L} + \frac{L}{c} \quad (4.5)$$

However, when developing the admission control mathematical model, we are rather interested to evaluate the gap, in terms of the mean delay, before and after admitting the new flow in a given link. Note that the average delay, denoted $\overline{D_i}$ on link I , is empirically evaluated and assumed to be known in advance. After admitting the flow on the link, the increment of the average delay can be written as follows:

$$\Delta \overline{D_i} \approx \frac{\bar{\lambda} \cdot \sigma_T^2}{2(1 - \frac{\bar{\lambda}}{c}) \cdot L} + \frac{L}{c} - D_i \quad (4.6)$$

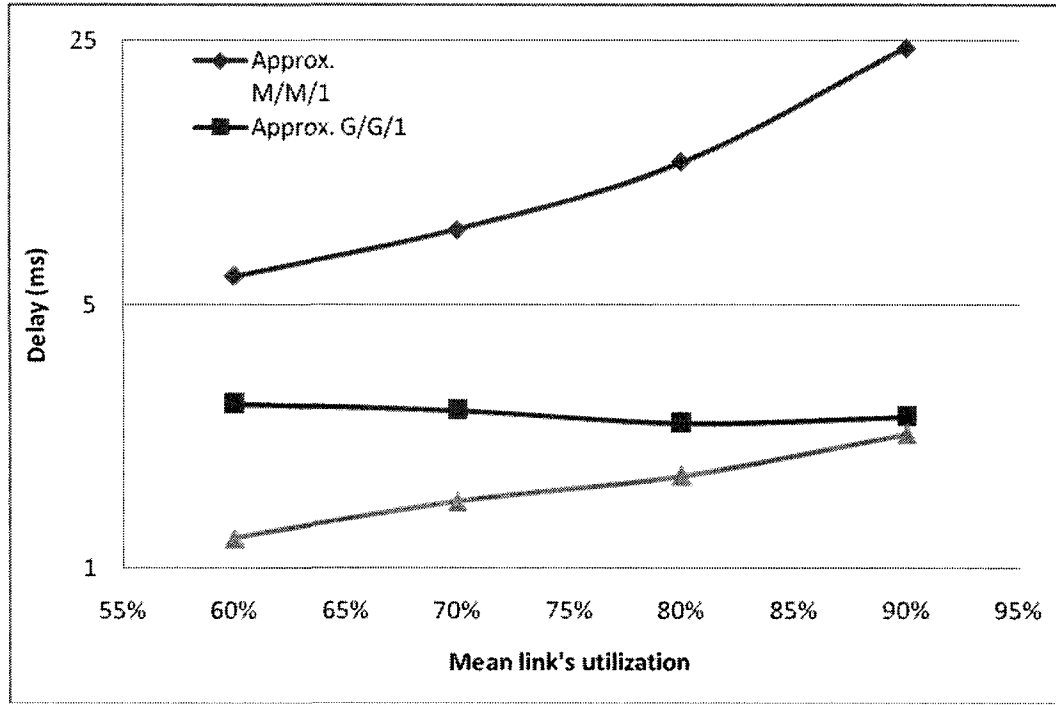


Figure 4.4 Accuracy of the mean delay bound given by Equation (4.5)

On the other hand, to obtain an upper bound on the end-to-end maximum delay, the new variance of the delay distribution after admitting the new flow has also to be approximated. However and as argued above, it is straightforward that increasing the link's load will decrease the variance of the delay distribution, as shown in Figure 4.2. This fact is all the more heightened when the load gets close to 100%, as less variation on the number of packets residing in the link's queue occurs. Taking this fact into consideration, we can consider that the empirically obtained variance σ_i^2 of the delay's distribution can be considered as an upper bound of $\overline{\sigma_i^2}$, the variance of the future delay's distribution after admitting the flow through the link i .

Figure 4.4 shows, in a logarithmic scale, the measured and approximated delays encountered by packets crossing a 10 Mbps link for different loads. For that, using the simulation tool *OPNET*, we measured the mean delay in a router's interface that carries

several sessions of various types (*FTP* sessions, *VOIP* sessions, video sessions and heavy web browsing sessions). We also varied the mean link's utilization from around 60% to 90%, and measured the mean encountered delay. We also measured the variance of the inter-arrival intervals, in order to calculate and assess the accuracy of the approximation given by Equation (4.5), for the different considered scenarios. As shown in Figure 4.4, Equation (4.5) gives effectively an upper-bound on the packets average delay that can be employed to approximate the new average delay, after admitting a new flow. Figure 4.4 also shows that this approximation is considerably better than the *M/M/1* queuing approximation and provides values closer to the real encountered delay, measured by simulations. Note that the approximation gets closer to the real delay as the load tends to 100%. This is mainly due to the fact that the variance of the packets' inter-arrival intervals decreases considerably, as argued above, with respect to the link's load. Moreover, it has been proven (Bose, 2001) that for great values of occupancy, the delay spent on a *G/G/1* queue tends to be exponentially distributed with the mean given by Equation (4.4). Note also that the accuracy of the approximation depends strongly on the nature of the carried traffic in terms of the distribution of the packets' inter-arrival intervals. For example, in case of bursty traffic, the upper bound given by Equation (4.5) remains always valid but the obtained bound is more conservative, as the variance of the inter-arrival intervals increases considerably.

4.3.4 Admission control mathematical formulation

In this section, we formulate the problem of Joint Routing and Admission Control problem under Statistical *QoS* Constraints (*JRACSC*). For that, we propose a new mathematical model for the admission control problem, taking into account the statistical delay and jitter constraints described above.

The physical topology is represented by an directed graph $G=(V,E)$, where V is the set of vertices (routers) and E the set of unidirectional links. Note that we make a difference between edge and core routers. F denotes the set of edge routers and $E-F$ the

set of core routers. Moreover, every link i of E is characterized by its capacity (or bandwidth) C_i , its current load F_i and its delay's distribution function D_i . In our case, we assume that the distributions nature is unknown but only the mean $\overline{D_i}$ and the variance σ_i^2 of the delay are empirically computed. Moreover, we assume that the variance of the packets inter-arrivals $\sigma_{T_i}^2$ is also approximated, in order to bound the increment of the average delay after admitting a new flow. This increment is pre-processed according to Equation (4.6). Note that mean packet size (L) is needed to evaluate this increment. In addition, as argued above, the variance of the delay's distribution will be considered the same, before and after admitting the new flow. Figure 4.2 gives an example of the measured delay's average and variance with respect to the link's load.

Moreover, we assume that the *MPLS* logical topology is already built and a single *LSP* between every edge-node pair exists. The whole set of *LSPs* is denoted by L and encompasses $|F|(|F|-1)$ distinct *LSPs* between edge-node pairs. Each *LSP* j is defined by its source-node s_j and its destination-node d_j . Moreover, let E be a bi-dimensional matrix, such that $E_{ij} = 1$, if and only if the *LSP* j is routed over the physical link i .

On the other hand, the network is assumed operational and already carries a set of ongoing connections T . Each connection t is defined by its path M_t , its data rate or required bandwidth b_t , its end-to-end delay constraint D_t , its end-to-end jitter constraint G_t and its QoS violation probability P_t . Moreover, let T be a bidirectional matrix, such that $T_{it} = 1$, if and only if the connection t is routed over the physical link i .

Similarly, the new connection is characterized by its source v_s , its destination v_d , its data rate b , its maximum delay D_{max} , its maximum jitter G_{max} and its QoS violation probability P_{max} . We assume that connection requests arrive to the network in an ordered way, one at a time.

We then define the set of binary variables $\mathbf{X}$, such that $X_i = 1$ if and only if the new connection is routed over the physical link i . In addition, we define the set of binary variables $\mathbf{Y}$, such that $Y_j = 1$ if and only if the new connection is routed over the LSP j . As the delay distribution depends principally on the link's load, the objective function of the mathematical model is chosen to minimize the sum, over the selected links, of their respective loads, privileging consequently slightly loaded links.

Thus, the Joint Routing and Admission Control problem Under Statistical Delay Constraints mathematical formulation can be written as follows:

$$\text{Minimize } \sum_{i=1}^{|E|} \frac{b + F_i}{C_i} \cdot X_i \quad (4.7a)$$

Subject to:

$$Y_j - E_{ij} X_i \leq 0 \quad \forall i \in E, \forall j \in L \quad (4.7b)$$

$$X_i - \sum_{j=1}^{|L|} E_{ij} Y_j \leq 0 \quad \forall i \in E \quad (4.7c)$$

$$\sum_{j=1}^{|L|} Y_j \leq N \quad (4.7d)$$

$$\sum_{i=1}^{|E|} \sigma_i^2 \cdot X_i \leq \frac{G_{\max}^2}{4} \cdot P_{\max} \quad (4.7e)$$

$$\sum_{i=1}^{|E|} (\overline{D_i} + \Delta \overline{D_i}) \cdot X_i \leq D_{\max} - \frac{G_{\max}}{2} \quad (4.7f)$$

$$\sum_{i=1}^{|E|} (\overline{D_i} T_{it} + \Delta \overline{D_i} T_{it} X_i) \leq D_t - \frac{G_t}{2} \quad \forall t \in T \quad (4.7g)$$

$$\sum_{\substack{j=1 \\ d_j=v}}^{|L|} Y_j - \sum_{\substack{j=1 \\ s_j=v}}^{|L|} Y_j = \begin{cases} 1, & \text{if } v = v_s \\ -1, & \text{if } v = v_d \\ 0, & \text{otherwise} \end{cases} \quad \forall v \in F \quad (4.7h)$$

$$X \in \{0,1\}^{|E|}, Y \in \{0,1\}^{|L|} \quad (4.7i)$$

The expression (4.7a) is the objective function of the model that balances the load over the network by minimizing the sum of the selected links utilizations. Equations (4.7b) to (4.7i) are the model constraints. The constraints (4.7b) and (4.7c) ensure that when a new connection is routed through a given *LSP*, it occupies its entire links. The constraint (4.7d) limits the number of *LSPs* for the new connection. Constraints (4.7e) and (4.7f) are respectively the jitter and the delay statistical constraints for the new connection. Constraint (4.7g) is the end-to-end delay constraint for the ongoing connections. It is important to mention that no jitter constraint is considered for these connections, as it was shown that the variance, and consequently the jitter, decreases as the link load increases. The equation (4.7h) is the flow conservation constraint over the *LSPs*. Finally, expression (4.7i) gives the domains of the model's decision variables.

As presented above, the formulated admission control problem is NP-Hard (Garey et Johnson, 1979). In fact, a polynomial reduction of the problem of constrained-routing can be merely deduced. Note however that the number of binary variables is relatively small for real-sized networks.

As a recap, our admission control mechanism consists on two separate phases:

- *Preprocessing phase*: during which the delay probability distributions parameters are gathered and approximated. These parameters are the mean and variance of the delay distribution over the links and the variance of the packets inter-arrival intervals, necessary to bound the expected average of the delay. The increment on the average delay is then computed on every link.
- *Admission control phase*: during which the admission control mathematical model is set up and resolved.

4.4 Simulation Results

In this section, we propose to solve to optimality JRACSC problem using the mathematical programming tool CPLEX (Ilog, 2005). In fact and as argued above, despite of being NP-Complete, the presented *ILP* can be resolved to optimality within very low computation times, as the number of integer variables are quite small for real size instances. Note that CPLEX uses the branch-and-bound algorithm for integer problems. The default settings of CPLEX are used.

As shown above, the mean and variance of the delay distribution are obtained empirically on every link during the preprocessing phase.

Table 4.1 Tests used

<i>Network</i>	$ V $	$ E $	$ F $
N1	10	30	6
N2	20	60	12
N3	40	120	24
N4	60	180	36

To evaluate the performance of our admission control mechanism, we propose to evaluate the connections acceptance rates for different network sizes and configurations. The considered physical topologies are shown in Table 4.1. The networks N1 to N4 were randomly generated as follows. A Hamiltonian cycle was first greedily built around the nodes to ensure that topologies are bi-connected. This fact is very important as it ensures the network's connectivity and maximizes the number of disjoint paths between every pair of nodes. Once the cycle constructed, the remaining edges are randomly placed. As for nodes degrees, the mean nodes' degree decreases as the number of nodes increases. In fact, as we want to reflect real case networks, small networks have usually

a higher connectivity than large networks, due to economic, physical and technological considerations.

As for the logical topologies, we assumed that a single *LSP* is setup between every pair of edge nodes. The set *T* of ongoing connections are routed over that logical topology.

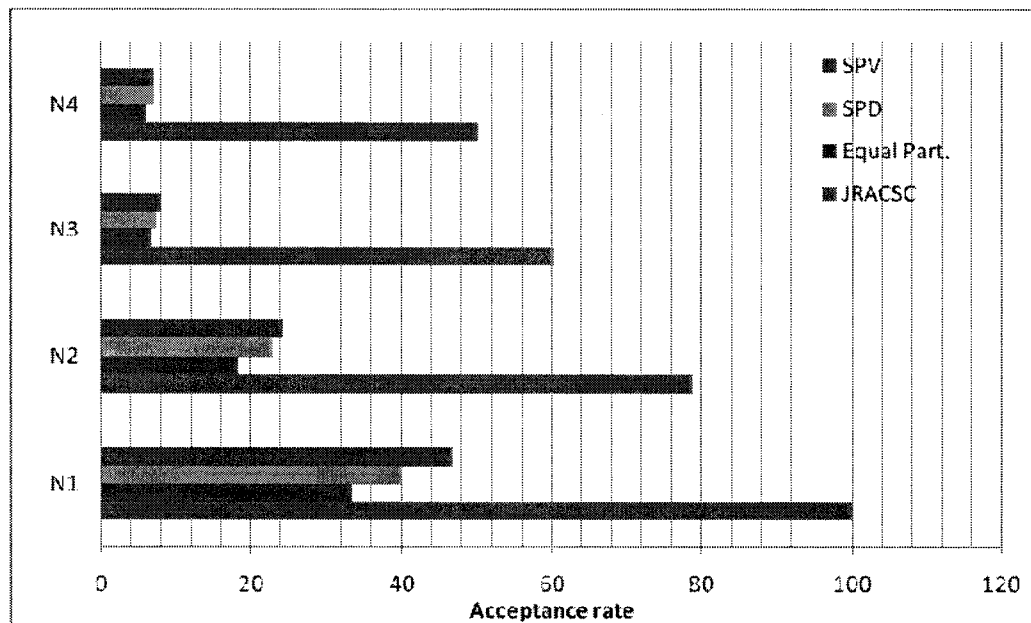


Figure 4.5 Acceptance rate for an average network load of 60%

Before discussing simulations results and appraising the accuracy of the proposed mechanism, we first present the experimental parameters:

- The end-to-end delay $D_{\max} = 150ms$;
- The end-to-end jitter $G_{\max} = 50ms$;
- The QoS violation probability $P_{\max} = 0.1$;

- The data rate $b = 1$ Mbps;
- The maximum number of LSPs $N_{\max} = 5$.

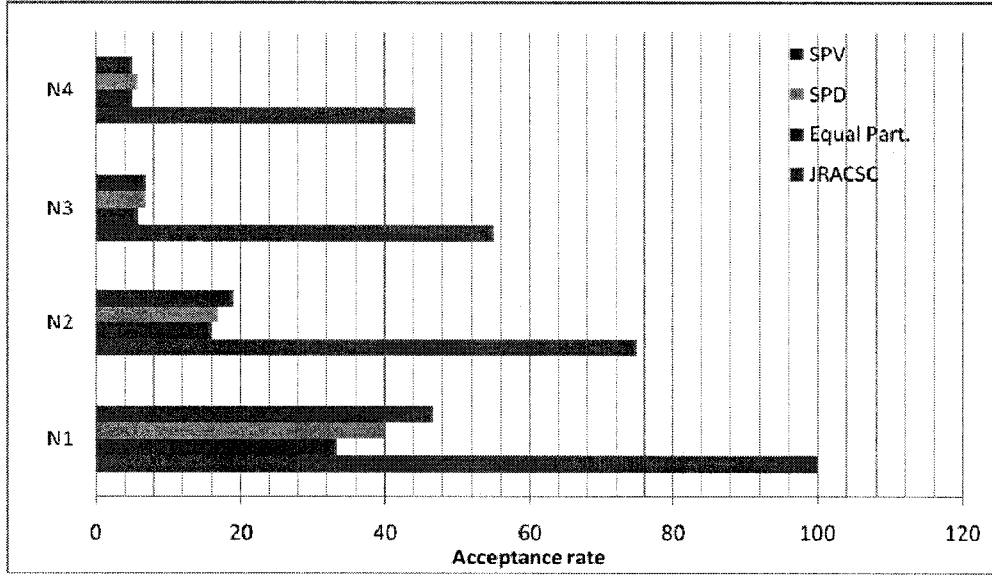


Figure 4.6 Accepted rate for an average network load of 75 %

In order to evaluate the *JRACSC* connections acceptance rate, we generate a single connection between every different pair of edge nodes, as input. These connections have the same set of parameters described above. The number of generated connections is then equal to $|F|(|F|-1)$.

In order to assess the accuracy of our proposed mechanism, we compare its performances against an equal partitioning technique. This latter consists of equally partitioning the *QoS* constraints over the selected path (path computed by *JRACSC*). Thus, if the path is composed of $|M|$ links, the end-to-end delay and jitter parameters are mapped to the corresponding links such that $D_{\max}^i = \frac{D_{\max}}{|M|}$ and $G_{\max}^i = \frac{G_{\max}}{|M|}$. Moreover, we also evaluated the connection acceptance rate considering a shortest path routing.

Note that we considered two different metrics to compute the shortest path: the link's mean delay and the link's delay variance. We named the first technique *SPD* (shortest path in terms of the mean delay) and second one *SPV* (shortest path in terms of the delay variance). Note that the *Dijkstra* algorithm was performed to obtain the shortest paths.

Moreover, as the delay spent on a given link depends strongly on its load, we propose to evaluate the acceptance rate of the proposed admission control mechanism for different loads that are respectively 60%, 75% and 90%. Figures 4.5, 4.6 and 4.7 depict the comparative results, in terms of the acceptance rate, for the different studied mechanisms.

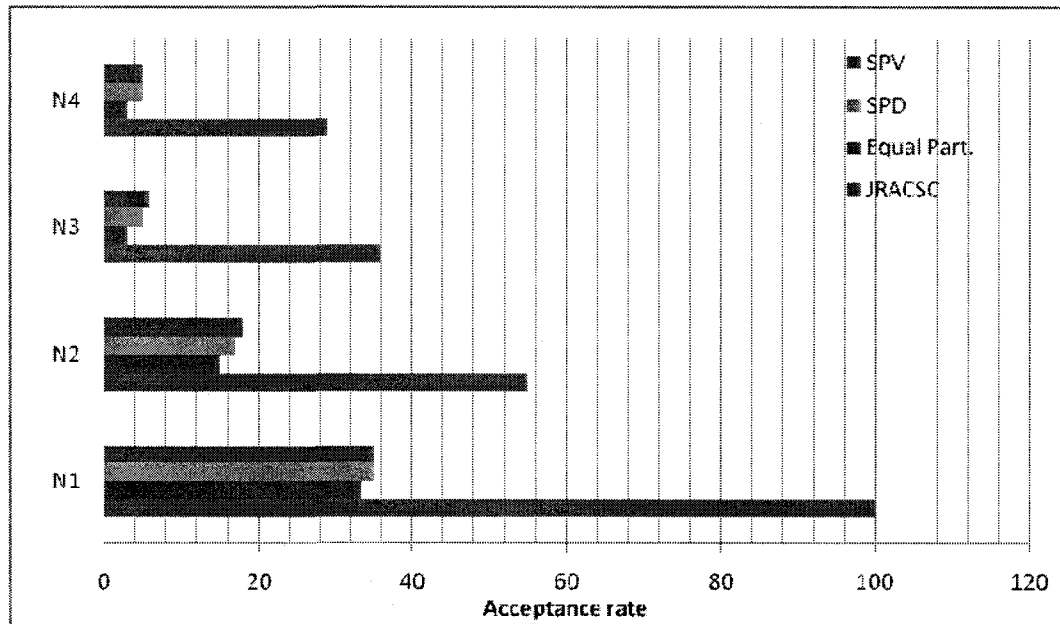


Figure 4.7 Accepted rate for an average network load of 90%

We clearly notice that the number of accepted connections is quite higher for *JRACSC* as end-to-end *QoS* parameters are considered. We also notice that the gap between our mechanism and the reference ones increases as the network size increases.

In fact, as far as the *QoS* equal partitioning is concerned, the low acceptance rate for relatively large networks is mainly due to the increasing paths' lengths, making the locally partitioned delay and jitter constraints more restrictive. The same observation is noted for *SPD* and *SPV*. In fact, even when choosing the shortest path in terms of the links' mean delays, we only take into account the end-to-end delay constraint. The end-to-end jitter constraint depends however on the variance. Similarly for the *SPV*, choosing links with low delay variances implies choosing links with high utilization and thus, high delays.

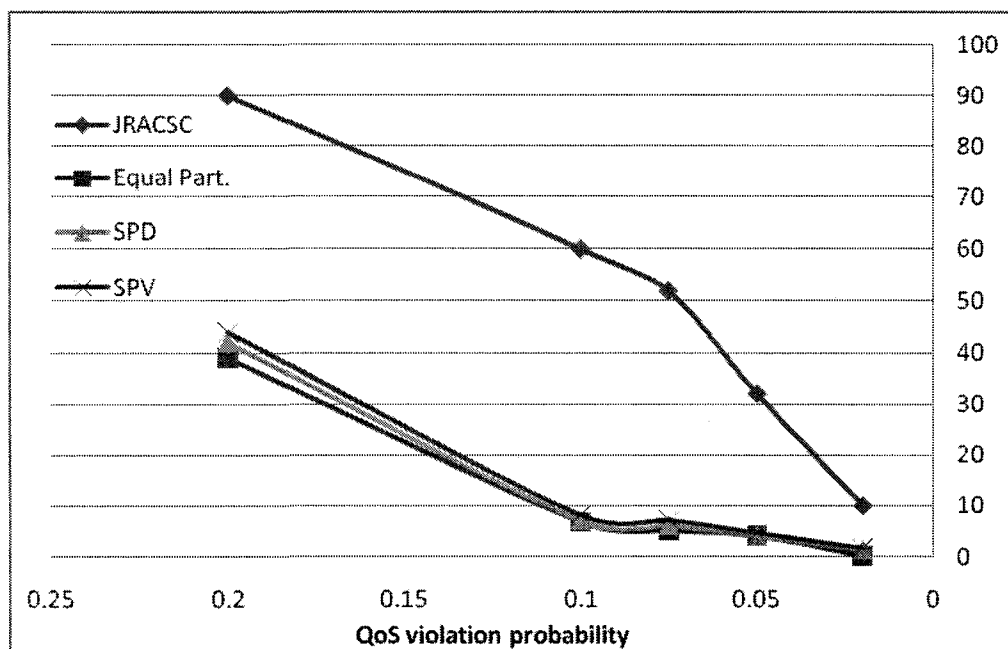


Figure 4.8 Number of accepted connections with respect to the *QoS* violation probability for the network having 40 Nodes having 60% of load

We also note that when the average network's utilization increases, the acceptance rate of the studied mechanisms decreases. This is quite expectable as the average delay on a given link increases considerably as the load increases. This is emphasized when the link's load gets close to 100%.

We also evaluate the effect of the *QoS* violation probability on the number of accepted connections, for an average network load of 60%. Results are depicted in Figure 4.8. It is straightforward that the number of accepted connections decreases as the *QoS* violation probability decreases, for all schemes. Note that the effect of the *QoS* violation probability depends on the average network's load. We also notice that as the violation probability decreases, performances of all studied mechanism weaken, as no feasible solutions guaranteeing these stringent delay and jitter constraints exist.

Finally, we evaluated computation times spent by CPLEX to resolve the model for the network having 60 nodes with a mean load of 75%. We noticed that in the worst cases this time did not exceed 350 ms which is very reasonable even for real-time based decisions.

4.5 Conclusion

In this paper, we presented a new admission control mechanism in *MPLS* networks based on formulating the problem as an *ILP* model that guarantees statistical *QoS* constraints.

For that, we assume that a delay distribution is empirically built on every link and that a new connection is characterized by an end-to-end delay, an end-to-end jitter and a *QoS* violation probability. We also proposed an upper bound on the average delay using the *G/G/I* queuing model and showed its validity, by simulations. We consequently propose a mathematical formulation for the joint routing and admission control problem and solve it to optimality. The constraints of the mathematical model are the *QoS* constraints of the new and the ongoing connections and it aims to balance the network's load.

The proposed mechanism was tested by simulations and compared with other mechanisms. The results confirm that the proposed formulation effectively improves the network performance by increasing the connection acceptance rate, while statistically guaranteeing the connections' delay and jitter constraints.

As future works, we first intend to evaluate our proposed mechanism by implementing it in a real test network. We also intend to propose a similar admission control mechanism guaranteeing the end-to-end delay and jitter constraints for multicast sessions.

CHAPITRE 5

A SURVIVABLE MULTICAST ROUTING MECHANISM IN WDM OPTICAL NETWORKS

Hichem Ayed Harhira and Samuel Pierre

Department of Computer and Software Engineering

Ecole Polytechnique de Montreal

CP. 6079 Succ. Centre Ville, Montreal (Qc), H3C 3A7, Canada

{Hichem-ayed.harhira, samuel.pierre}@polymtl.ca

Abstract

In Next Generation Networks, survivability and availability are more and more becoming key features. Reliability gains more importance in high capacity networks where *IP* and optical technologies have converged toward a common control plane, such as *GMPLS*. In most previous research works, survivability aspects were mainly limited to a single fiber failure and a few considered the differentiated reliability concepts when routing new connection requests. In this paper, a novel survivable multicast routing mechanism under *SRLG* constraints is proposed. We first formulate the problem as an Integer Linear Programming (*ILP*) model that is shown NP-Complete. We then propose a heuristic algorithm that alleviates the problem's complexity by decomposing it into two sub-problems resolved separately. Compared with another algorithm proposed in the

literature, our algorithm allows for higher acceptance rates even for stringent reliability requirements.

Key words

Wavelength Division Multiplexing (*WDM*), Shared Risk Link Group (*SRLG*), differentiated reliability, survivability, mathematical programming.

5.1 Introduction

As Next Generation Networks (*NGN*) are more and more becoming multi-services, new mechanisms for providing a certain level of Quality of Service (*QoS*) and failure resilience are indispensable. In fact, in the last decade, stringent *QoS* and reliability requirements have emerged due to the overwhelming demand for real-time and multimedia applications that involve data, voice, video, telephony, *IPTV*, etc. to be conveyed over the same network. In such a scenario, optical networks embedded with the Wavelength Division Multiplexing technology is a key feature for providing high-capacity and cost-effective transport networks.

The physical layer in a *WDM* network consists of a set of nodes interconnected by multiple optical fibers. Fibers are generally grouped and inserted into a single conduit such that every single fiber can belong to different conduits, depending on its physical length. Such fibers are said to be in the same Shared Risk Link Group (*SRLG*) as the failure of the conduit results in the failure of all fibers inside.

At the optical level, circuits or connections are set up between peer Optical Cross Connectors (*OXC*) and named lightpaths. Lightpaths are generally protected using either a dedicated or a shared protection, depending on the reliability requirements.

A multitude of survivable routing mechanisms have been proposed for *WDM* optical networks (Li *et al.*, 2006 ; Markidis & Tzanakaki, 2008 ; Guo & Li, 2007 ; Gui *et al.*, 2007 ; Rostami *et al.*, 2007 ; Todimala *et al.*, 2004 ; Datta *et al.*, 2004 ; Pan *et al.*, 2006). Li *et al.* (2006) proposed a greedy heuristic for multicast protection under *SRLG* constraints. Their algorithm constructs a tree from the source to the set of destinations using the Shortest Path Tree (*SPT*) algorithm and computes, for every branch, an *SRLG* protected path, such that the whole tree is well protected. Before computing the protection tree, the links' metrics are altered in order to take into account the backup resources sharing. In fact, if a set of backup lightpaths share a same link but their corresponding primary lightpaths do not share common *SRLGs*, a single channel (wavelength) can be reserved for all these paths. Details on the resources sharing are discussed by Gui *et al.* (2007) and Ou *et al.* (2004).

On the other hand, Rostami *et al.* (2007) extended a high performance link disjoint routing algorithm to adapt it to the *SRLG* protection scenario. Their algorithm iteratively separates the network nodes into two sets and computes the working and backup paths respectively from each set. Todimala *et al.* (2004) also proposed an iterative heuristic for diverse routing under *SRLG* constraints that computes the least cost *SRLG* diverse paths pair.

Despite of obtaining interesting results, the proposed mechanisms discussed above did not consider the differentiated reliability feature, allowing for statistical survivability and reliability guarantees.

The differentiated reliability was deeply investigated and considered for providing different levels of failure resilience within the same network, mainly depending in the applications requirements, in terms of reliability. Markidis & Tzanakaki (2008) tackled the problem of survivable routing and wavelength assignment in *WDM* optical networks. They proposed a reactive algorithm that provides different

levels of resilience, and classifies the incoming traffic accordingly. The algorithm also allows for the high-priority and high-resilience traffic to pre-empt lower-priority traffics. Authors however considered only simple fibers failure and did not investigate the effect of loosing a bundle of fibers sharing the same *SRLG*.

On the other hand, Guo & Li (2007) proposed a survivable routing algorithm called Partial *SRLG* Disjoint Protection (*PSDP*), based on the *SRLG* constraints. The algorithm considers the differentiated reliability when making routing decisions. Depending on the reliability requirements, a routing configuration consists of a standalone working path or a working path protected by a backup path. Authors considered an equal failure probability for all the *SRLGs* in the networks and defined the reliability coefficient for a path as the probability that no failure occurs in any of its physical links. Their algorithm is based on a greedy heuristic that computes the k shortest paths for the new connection request and chooses a working and backup paths that satisfy the reliability needs. Authors however only considered unicast requests and did not address the case of multicast request.

In this paper, we tackle the problem of Survivable Multicast Routing under *SRLG* constraints (*SRMS*). Depending on the reliability requirements of the incoming request, statistical survivability guarantees are offered. For that, we first formulate the problem as an Integer Linear Programming model that is shown NP-Complete. We then propose an algorithm that alleviates the problem's complexity by decomposing it into two sub-problems.

The remainder of the paper is organized as follows. In Section 5.2, the problem definition and the mathematical formulation are presented and detailed. In Section 5.3, a heuristic algorithm having low computation delays is proposed and studied. Section 5.4 shows the simulation results and appraises the performances of the proposed mechanism. Conclusions are given in Section 5.5.

5.2 Survivable Routing Under SRLG Constraints

In the scenario presented in Figure 5.1, a large number of optical fibers are carried inside one or multiple conduits. In its turn, a single optical fiber carries a large number of lightpaths each on a different wavelength. Due to the layered architecture, lightpaths connecting two distinct pairs may traverse the same conduit in the physical network.

5.2.1 SRLG Sharing

An *SRLG* is a group of links sharing some same resources and thus the same failure risks. In survivable routing schemes, the working (primary) and backup paths are *SRLG* disjoint. In fact, the failure of a single *SRLG* is equivalent to the failure of all the links in the *SRLG*. The problem of finding a minimum cost and *SRLG* disjoint working and backup paths is known NP-Complete (Hu, 2003).

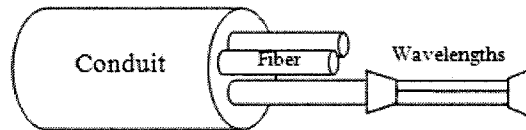


Figure 5.1 Risk hierarchy of an SRLG

An example of a physical topology is depicted in Figure 5.2a. We can see that there are three physical links sharing the same conduit and thus belonging to the same *SRLG* 1.

In this work, we consider that each *SRLG* has a failure probability that should be taken into account when routing incoming connection requests. Such a statistical survivability requirement is referred as differentiated reliability in the literature (Guo & Li, 2007 ; Markidis & Tzanakaki, 2008). When considering the differentiated reliability,

the incoming connection requests are also characterized by some reliability requirements that must be fulfilled when making routing decisions. More details on the differentiated reliability are discussed later in this paper.

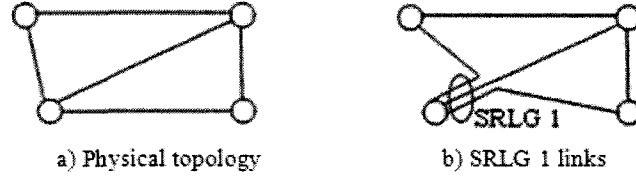


Figure 5.2 Example of an SRLG

We also define the reliability of the network as the probability that no failure occurs. The considered problem then consists of finding a minimal cost reliable multicast routing fulfilling the reliability requirements of the incoming multicast connections.

5.2.2 Resources sharing

In order to maximize the resources utilization, we take into account the concept of backup resources sharing, when simple failure scenarios are considered. In fact, when routing a backup path for a given connection t through a physical link l , no additional resources (wavelengths or channels) are needed if one of the following cases occurs (Li *et al.*, 2006 ; Gui *et al.*, 2007):

- There exists a backup path for another connection t' routed through the link l such that the working paths of t and t' are respectively SRLG disjoint.
- Every SRLG taken by the working path of t is shared with at least a working path that is routed over the link l . In such a case, for any simple failure scenario, there will be at least one working path routed over l that is consequently broken down, freeing its resources to the backup path of t .

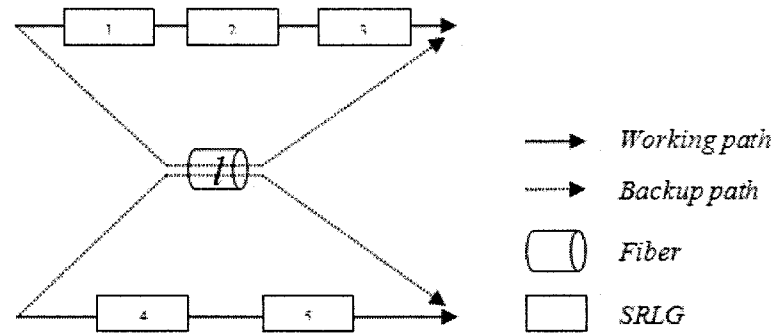


Figure 5.3 Example of backup resources sharing

Figure 5.3 depicts a network topology where backup resources can be shared through a physical link by two different connections. We clearly see that the two working paths are never affected by a simple *SRLG* failure simultaneously, and thus, their respective backup paths can share the same resources over the physical link *L*.

5.2.3 Problem Statement

We assume that the given *WDM* optical network is represented by a directed graph $G=(V,E)$, where V is the set of nodes (*OXC*s) and E is the set of unidirectional fibers, having each W channels or wavelengths. We also assume that the network is operational and contains no failures. Connections requests arrive to the network in an ordered way so that only a single connection arrives at a time. Each multicast connection is characterized by its source node s , its set of destination nodes D and a set of reliability requirements UR (explained below in more details). For sake of simplicity, we assume that the bandwidth for each incoming request is equal to a single unit (single channel). Assuming a single *SRLG* failure as discussed above, the problem consists of finding a primary working path and possibly a backup path between the source and every destination guaranteeing the required reliability UR . Some important notations are introduced as follows:

WP_d	Working path for the destination d
BP_d	Backup path for the destination d
S	Set of SRLGs in the network
UR	Required reliability
P	Probability of failure of the network
$PF(.)$	Probability of failure for a set of links
$R(.)$	The reliability of a set of links.

On the other hand, we define the binary matrix LS such that $\forall i \in E, \forall j \in S, LS_i^j = 1$ if and only if the link i belongs to the $SRLG$ j . Moreover, let T be the set of ongoing multicast sessions. Every $t \in T$ has its source s_t , its destination set D_t and its primary and backup trees TP_t and TB_t , respectively. Then, we merely compute the state of the network resources for any scenario of simple $SRLG$ failure. For that, we denote by F the resources availability matrix that gives the number of available wavelengths on every link for all network scenarios (no failures or with a simple $SRLG$ failure) such that $\forall i \in E, \forall j \in \{0, 1, 2, \dots, |SRLG|\}$, F_{ij} gives the number of available channels over the physical link i for the network scenario j (scenario 0 indicates no failure and scenario $j \in \{1, 2, \dots, |SRLG|\}$ indicates the failure of the $SRLG$ j).

Note that we only consider single failure scenarios and thus the probability of failure of the network is merely the probability of any single $SRLG$ failure. We also assume that the failure distribution function over the network's $SRLGs$ is uniform, meaning that the probability of failure of any $SRLG$ is constant and equal to $\frac{P}{|S|}$. As discussed by Li *et al.* (2006), the probability of failure of a given path depends on the number of distinct $SRLGs$ of that path. Thus we define the set of $SRLGs$ for a given set of links as $SRLG(.)$; $SRLG(WP_d)$ is then a subset of S taken by the working path to the destination d .

5.2.4 Network Reliability and Failure Probability

As discussed above, the network reliability is known in advance and is merely $1-P$. In this section, we aim to express the reliability needs of the incoming multicast requests in terms of a set of bounds on the number of *SRLGs* taken by a path or a routing configuration. For that, we first evaluate the probability of failure of a given working path *WP* as follows:

$$PF(WP) = \frac{|SRLG(WP)|}{|S|} \cdot P \quad (5.1)$$

The reliability of a given path *WP* is merely defined as the probability that no failure occurs on any of the path's links. Thus, the reliability of a working path is defined as follows:

$$R(WP) = 1 - PF(WP) = 1 - \frac{|SRLG(WP)|}{|S|} \cdot P \quad (5.2)$$

If a backup path *BP* is computed, the reliability of the routing configuration (*WP+BP*) toward a given destination has exactly the same expression below:

$$\begin{aligned} R(WP + BP) &= 1 - PF(WP \cup BP) \\ &= 1 - \frac{|SRLG(WP) \cap SRLG(BP)|}{|S|} \cdot P \end{aligned} \quad (5.3)$$

In this paper, we assume that the required reliability for an incoming multicast connection request, denoted by *UR*, is twofold:

- *Local reliability*: denoted by UR_b and describes the reliability requirements toward every single destination, i.e., the probability that every destination is fed interruptedly for any simple failure scenario. Computing the local reliability for

every destination is straightforward and is given by equation (5.3). The local reliability limits the maximum number of *SRLGs* taken by the working and backup paths toward a destination d as follows:

$$\begin{aligned} R(WP_d + BP_d) \geq UR_l &\Leftrightarrow \frac{|S| - |SRLG(WP_d + BP_d)|}{|S|} \cdot P \geq UR_l \\ \Rightarrow |SRLG(WP_d + BP_d)| &\leq \left\lfloor \frac{|S| (1 - UR_l)}{P} \right\rfloor \end{aligned} \quad (5.4)$$

- *Global reliability*: denoted by UR_g , and describes the reliability of the overall routing solution. This global reliability defines the vulnerability of the whole multicast tree. It is computed as follows:

$$1 - \frac{|\bigcup_{d \in D} (SRLG(WP_d) \cap SRLG(BP_d))|}{|S|} \cdot P \geq UR_g \quad (5.5)$$

In this paper, we propose a mechanism that relies on the differentiated reliability for dynamic multicast routing of the incoming multicast requests under *SRLG* constraints in *WDM* optical networks. This problem is first formulated as an *ILP* in the next section.

5.2.5 Mathematical Formulation

Once the matrix F pre-computed, we formulate the problem of reliable routing of multicast sessions under *SRLG* constraints in *WDM* optical networks as an Integer Linear Programming (*ILP*) model. For that, we define the binary variables X, Y, V, W, U and Z as follows:

$$X_{id} = \begin{cases} 1, & \text{if the primary path to the destination } d \text{ takes the link } i \\ 0, & \text{otherwise} \end{cases} \quad \forall i \in E, \forall d \in D$$

$$\begin{aligned}
Y_{id} &= \begin{cases} 1, & \text{if the protection path to the destination } d \text{ takes the link } i \\ 0, & \text{otherwise} \end{cases} & \forall i \in E, \forall d \in D \\
V_{jd} &= \begin{cases} 1, & \text{if the primary path to the destination } d \text{ takes SRLG } j \\ 0, & \text{otherwise} \end{cases} & \forall j \in S, \forall d \in D \\
W_{jd} &= \begin{cases} 1, & \text{if the protection path to the destination } d \text{ takes SRLG } j \\ 0, & \text{otherwise} \end{cases} & \forall j \in S, \forall d \in D \\
U_d &= \begin{cases} 1, & \text{if a BP is considered for the destination } d \\ 0, & \text{otherwise} \end{cases} & \forall d \in D \\
Z_j &= \begin{cases} 1, & \text{if a routing configuration takes the SRLG } j \\ 0, & \text{otherwise} \end{cases} & \forall j \in S
\end{aligned}$$

The last variable Z is used to compute the global reliability given by the equation (5.5). It is defined as follows:

$$Z_j \geq V_{jd} W_{jd} \quad \forall j \in S, \forall d \in D \quad (5.6a)$$

$$Z_j \leq \sum_{d \in D} V_{jd} \cdot W_{jd} \quad \forall j \in S \quad (5.6b)$$

The survivable routing of multicast connections under SRLG constraints can be formulated as follows:

$$\text{Minimize} \quad \sum_{d \in D} U_d \quad (5.7a)$$

Subject to

$$V_{jd} \geq LS_{ij} X_{id} \quad \forall j \in S, \forall i \in E, \forall d \in D \quad (5.7b)$$

$$V_{jd} \leq \sum_{i \in E} LS_{ij} \cdot X_{id} \quad \forall j \in S, \forall d \in D \quad (5.7c)$$

$$W_{jd} \geq LS_{ij} Y_{id} \quad \forall j \in S, \forall i \in E, \forall d \in D \quad (5.7d)$$

$$W_{jd} \leq \sum_{i \in E} LS_{ij} \cdot Y_{id} \quad \forall j \in S, \forall d \in D \quad (5.7e)$$

$$U_d \geq Y_{id} \quad \forall d \in D, \forall i \in E \quad (5.7f)$$

$$U_d \leq \sum_{i \in E} Y_{id} \quad \forall d \in D \quad (5.7g)$$

$$Z_j \geq V_{jd} W_{jd} \quad \forall j \in S, \forall d \in D \quad (5.7h)$$

$$Z_j \leq \sum_{d \in D} V_{jd} \cdot W_{jd} \quad \forall j \in S \quad (5.7i)$$

$$\sum_{k \mid s_k=i} X_{id} - \sum_{k \mid d_k=i} X_{id} = \begin{cases} 1, & \text{if } i=s \\ -1, & \text{if } i=d \\ 0, & \text{else} \end{cases} \quad \forall d \in D, \forall k \in V \quad (5.7j)$$

$$\sum_{k \mid s_k=i} Y_{id} - \sum_{k \mid d_k=i} Y_{id} = \begin{cases} U_d, & \text{if } i=s \\ -U_d, & \text{if } i=d \\ 0, & \text{else} \end{cases} \quad \forall d \in D, \forall k \in V \quad (5.7k)$$

$$\sum_{j \in S} V_{jd} \leq (1 - U_d) \cdot \left\lfloor \frac{|S|(1 - UR_l)}{P} \right\rfloor \quad \forall d \in D \quad (5.7l)$$

$$\sum_{j \in S} V_{jd} W_{jd} \leq U_d \cdot \left\lfloor \frac{|S|(1 - UR_l)}{P} \right\rfloor \quad \forall d \in D \quad (5.7m)$$

$$\sum_{j \in S} Z_j \leq \left\lfloor \frac{|S|(1 - UR_g)}{P} \right\rfloor \quad (5.7n)$$

$$X_{id} \leq F_{ij} + V_{jd} \quad \forall i \in E, \forall d \in D, \forall j \in S \quad (5.7o)$$

$$X_{id} \leq F_{i0} \quad \forall i \in E, \forall d \in D \quad (5.7p)$$

$$Y_{id} \leq F_{ij} + W_{jd} \quad \forall i \in E, \forall d \in D, \forall j \in S \quad (5.7q)$$

$$X_{id} \in \{0,1\}, Y_{id} \in \{0,1\}, V_{jd} \in [0,1], W_{jd} \in [0,1], Z_j \in [0,1], \quad \forall j \in S, \forall i \in E, \forall d \in D \quad (5.7r)$$

$$U_d \in [0,1]$$

As formulated above, the problem of Survivable Multicast Routing under *SRLGs* constraints is a variant of the classical problem of diverse routing under *SRLG* constraints that can be shown NP-Complete (Hu, 2003 ; Garey & Johnson, 1979). Note that to prove that the problem of Diverse routing under *SRLG* constraints is NP-Complete, a polynomial reduction of the well known set-splitting problem is shown by Hu (2003).

Equation (5.7a) is the objective function of the model aiming to minimize the size of the backup tree, composed of *BPs* toward every destination d in D . In fact, as we consider statistical reliability guarantees, the path toward every destination could be

routed through a reliable enough working path, suitably chosen. Equations (5.7b) to (5.7r) are the model constraints. The constraints (5.7b) to (5.7i) are indispensable for defining the binary variables V , W , U and Z . The constraint (5.7j) ensures that a continuous working path exists toward every destination. The constraint (5.7k) ensures that if a backup path is needed for a given destination, it is suitably routed. Constraints (5.7l), (5.7m) and (5.7n) guarantee the reliability requirements for the incoming multicast tree. The local reliability requirements are given by constraints (5.7l) and (5.7m) whereas the constraint (5.7n) guarantees the global required reliability. Finally, equations (5.7o) to (5.7q) are the resources availability constraints ensuring that enough resources (wavelengths) are free along both the working and backup paths.

Due to the constraints (5.7h), (5.7i) and (5.7m), the mathematical model formulated above is not linear. In order to linearize it, we define the new variables Q , such that $Q_{jd} = W_{jd}V_{jd}$, $\forall d \in D, \forall j \in S$. The mathematical model is modified accordingly and the following constraints are appended:

$$Q_{jd} \leq V_{jd} \quad \forall j \in S, \forall d \in D \quad (5.8a)$$

$$Q_{jd} \leq W_{jd} \quad \forall j \in S, \forall d \in D \quad (5.8b)$$

$$Q_{jd} \geq V_{jd} + W_{jd} - 1 \quad \forall j \in S, \forall d \in D \quad (5.8c)$$

5.3 GR-SMRS: Greedy Heuristic for Survivable Multicast Routing under SRLG constraints

In order to resolve the Survivable Multicast Routing under *SRLG* constraints problem formulated above, we propose to heuristically decompose the problem into two different sub-problems resolved separately. This proposed heuristic provides acceptable enough upper-bounds on the optimal solution within reasonable computation times. In fact, as the problem is NP-Complete, resolving it to optimality (with a mathematical

programming tool such as CPLEX) is not feasible for real-sized networks and consumes massive computation delays and resources.

The proposed heuristic encompasses two principle phases as follows:

- *Paths computation phase*: during which a set of shortest paths is computed from the source toward every destination d in D . As the number of shortest paths increases exponentially with the size of the network, we limit the number of shortest paths computed for every destination to a certain number N . For that, the *Dijkstra* algorithm is performed.

Thus, toward every destination d of D , a maximum of N different paths is computed. We then build the set of “reliable enough” routing configurations denoted by RP_d (Reliable enough paths toward the destination d). According to the reliability needs, a routing configuration can be either a standalone working path, or a working path protected by a backup path.

First the resources availability for every single path is checked, under different failures scenarios. The reliability of every single path is then checked and if it guarantees the required reliability UR_l , it is put in RP_d . Every remaining path (not enough reliable to be considered without a BP) is then checked against every other path not in RP_d and every resulting feasible configuration ($WP + BP$) is then added to the set RP_d . Having a maximum of N different paths toward a

destination d in D , the set RP_d contains at most $2.C_N^2 = \frac{N!}{(N-2)!} = N(N-1)$.

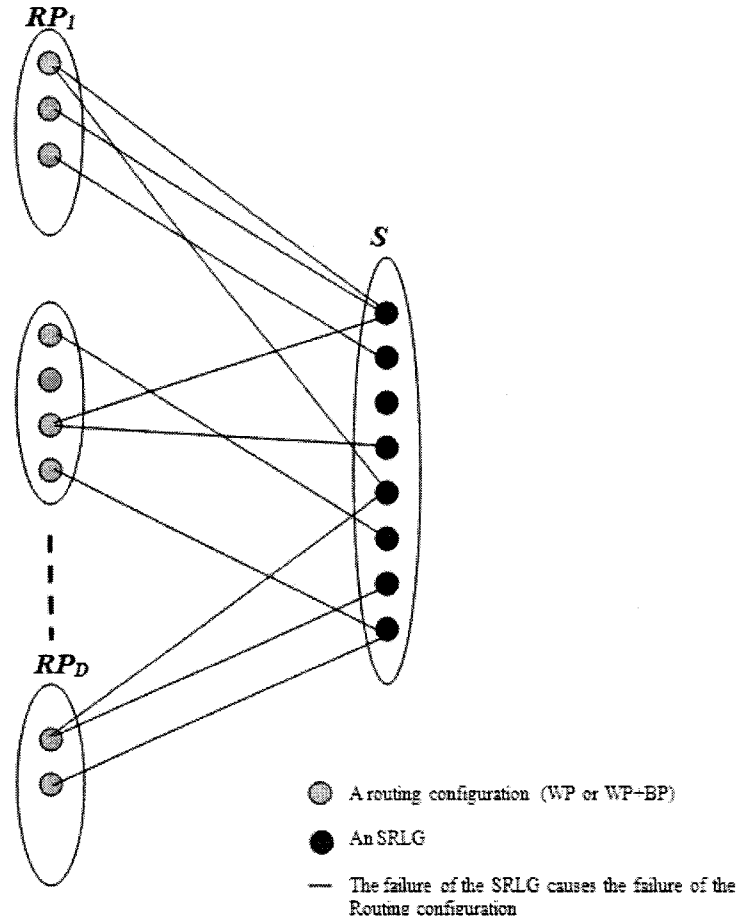


Figure 5.4 Auxiliary graph for selecting the routing configurations

- Routing configurations selection:** Once the sets RP constructed and filled, an auxiliary bipartite graph $G_l=(V1,V2,E1)$ is built as shown in Figure 5.4. The set $V1$ encompasses the left side of the graph and is composed of the RP s, having each a set of routing configurations toward a destination d in D . Similarly, the set $V2$ encompasses the right part of G_l and is composed of the set S of SRLGs. The set of edges $E1$ of this graph reflects the vulnerability of the routing configurations to every $SRLG$. Indeed, if a routing configuration $v1$ of $V1$ (a node in the left side of the graph) is adjacent to an $SRLG$ $v2$ of $V2$ (a node in the right side of the graph), the failure of the $SRLG$ $v2$ causes the failure of the routing

configuration vI (even if protected by a BP). As the number of disjoint $SRLGs$ to be taken by a routing configuration is constrained by the equations (5.7l) and (5.7m), the maximum degree of nodes belonging to $V1$ is $\left\lfloor \frac{|S|(1-UR_l)}{P} \right\rfloor$.

Moreover, the number of $SRLGs$ taken by the whole multicast tree is upper-bounded by $\left\lfloor \frac{|S|(1-UR_g)}{P} \right\rfloor$, as shown in equation (5.7n). In order to guarantee both local and global reliability needs, a single routing configuration is selected toward every destination d (from the set RP_d), so that the number of $SRLGs$ upon which the multicast tree is vulnerable does not exceed the bound $\left\lfloor \frac{|S|(1-UR_g)}{P} \right\rfloor$ given by equation (5.7n). The route selection problem is then formulated as an ILP as shown below. For that, we define the following binary variables:

$$X_i = \begin{cases} 1, & \text{if the routing configuration } i \text{ is selected} \\ 0, & \text{otherwise} \end{cases} \quad \forall i \in V1$$

$$Z_s = \begin{cases} 1, & \text{if the multicast tree is vulnerable to } SRLG \ s \\ 0, & \text{otherwise} \end{cases} \quad \forall s \in V2$$

In addition, every routing configuration is characterized by its cost, computed according to the objective function (5.7a). For that, we denote by C a known vector such that, C_i gives the cost of the routing configuration i , $\forall i \in V1$. We also define the known binary matrices M and R as follows:

$$M_{ij} = \begin{cases} 1, & \text{if the routing configuration } i \text{ belongs to } RP_j \\ 0, & \text{otherwise} \end{cases} \quad \forall i \in V1, \forall j \in D$$

$$\quad \quad \quad \forall i \in V1, \forall s \in V2$$

$$R_{is} = \begin{cases} 1, & \text{if the routing configuration } i \text{ depends on SRLG } s \\ 0, & \text{otherwise} \end{cases}$$

The route selection problem is then formulated as follows:

$$\text{Minimize} \quad \sum_{i \in V1} C_i \cdot X_i \quad (5.9a)$$

$$\text{Subject to} \quad \sum_{i \in V1} M_{ij} \cdot X_i = 1 \quad \forall j \in D \quad (5.9b)$$

$$Z_s \leq \sum_i R_{is} \cdot X_i \quad \forall s \in V2 \quad (5.9c)$$

$$Z_s \geq R_{is} \cdot X_i \quad \forall s \in V2, \forall i \in V1 \quad (5.9d)$$

$$\sum_{s \in V2} Z_s \leq \left\lfloor \frac{|S| (1 - UR_g)}{P} \right\rfloor \quad (5.9e)$$

$$X \in \{0,1\}^{|V1|}, Z \in [0,1]^{|V2|} \quad (5.9f)$$

The objective function of this *ILP* aims to minimize the cost of the selected routing configurations. The constraint (5.9b) ensures that only a single routing configuration is selected toward every destination of the multicast tree. The constraints (5.9c) and (5.9d) define the set of variables Z . Finally, the constraint (5.9e) ensures that the global reliability requirement is guaranteed, by limiting the number of SRLGs for which the tree is vulnerable.

In order to resolve the above presented *ILP*, we propose to use the CPLEX mathematical programming tool (Ilog, 2005) that relies on the Branch-and-bound algorithm to resolve integer mathematical models. As the number of binary variables is limited for real-sized instances, the *ILP* is resolved to optimality within negligible computation delays. Table 5.1 gives the computation delays for different sizes of the graph G_l .

Table 5.1 Computation delays

$ V1 $	$ V2 $	Delays (ms)
50	20	20
100	40	31
200	40	32
300	60	45

5.3.1 Complexity Analysis of GR-SMRS

This subsection evaluates the overall complexity of the *GR-SMRS* heuristic using the graph transformation technique as described above. The computational complexity can be broken into three parts.

The first part is the one involved in finding shortest paths using the *Dijkstra's* algorithm. The best known implementations of the *Dijkstra's* algorithm have a complexity of $O(|E|.log|E|+|V|)$. As a set of shortest paths are computed toward every destination, the complexity of the routing phase is $O(D.|E|.log|E|+|V|)$.

The second part consists of selecting feasible paths, in terms of the resources availability and the local reliability requirements. Thus, at most $O(N^2)$ different routing configurations are obtained for every destination of the multicast tree and are checked against the resources availability (for all the $|S|$ failures scenarios). This process has a complexity in the order of $O(N^2.D.|S|.|E|)$.

Finally, the third part of the computational complexity involves the resolution to optimality of the *ILP* for selecting feasible routing configurations. As the *CPLEX* mathematical tool is used to resolve the model, we limit our complexity assessment to

empirically obtaining computation delays, as shown in Table 5.1.

5.4 Simulation Results

In this section, we propose to implement the proposed algorithm in order to assess its accuracy. We also propose to resolve to optimality the *ILP* model for the Survivable Multicast Routing under *SRLG* constraints problem, presented above, using the CPLEX mathematical programming tool (Ilog, 2005). The set of used physical topologies are given in Table 5.2. In addition to the *ARPANET* network, we considered four different physical topologies, that were randomly generated and having respectively 10, 20, 40 and 60 nodes. Physical links were randomly generated such that the physical graph remains bi-connected. This fact is very important, first to ensure the network's connectivity and second to maximize the number of disjoint paths between every pair of nodes. For that, we first greedily constructed a *Hamiltonian* cycle around the nodes to ensure that our topologies are bi-connected. Once the cycle constructed, the remaining edges are randomly placed. Details on the physical topologies are presented in Table 5.2.

Table 5.2 Used physical topologies

<i>Network</i>	$ V $	$ E $	$ S $
PT1	10	30	5
PT2	20	60	10
PT3	40	120	20
PT4	60	180	30
ARPANET	20	64	10

Before discussing simulation results and appraising the accuracy of the proposed mechanism, we first present the experimental parameters:

- The probability of the network failure is $P=0.05$;
- The number of wavelengths within a fiber $W=10$;
- All optical nodes are wavelength-conversion capable;
- The maximum number of shortest paths computed toward every destination $N=5$.

In order to evaluate the connections acceptance rate for the proposed mechanism, we randomly generated 200 connections as input. Moreover, different values of the reliability requirements were considered in simulations.

5.4.1 Comparative Results: CPLEX vs. GR-SMRS

In order to evaluate the quality of the obtained routing configurations provided by *GR-SMRS*, we propose to compare its performances to the optimal solutions, obtained by resolving the global problem, using the CPLEX mathematical programming tool. As the problem is NP-Complete, we limited our tests to the relatively small-sized networks (PT1, PT2 and ARPANET). Table 5.3 gives the computation delays taken by CPLEX to resolve the *ILP*.

Table 5.3 Computation delays (ms)

<i>Network</i>	<i>CPLEX</i> (ms)	<i>GR-SMRS</i> (ms)
PT1	6000	<100
PT2	74000	<300
ARPANET	40000	<300

We first compared the connections acceptance rates function of the local reliability requirement UR_l , for the network PT1. Note that the size of the destination set D is 3 and the considered global reliability requirement $UR_g=0.96$. We then compared the connections acceptance rates function of the global reliability requirement UR_g for the same physical topology and with a local reliability requirement of $UR_l=0.96$. Results are depicted in Figures 5.5 and 5.6 respectively. We notice that for relatively tight reliability requirements, the performances of the proposed heuristic decrease and the gaps between it and the optimal solutions increase. We however notice that our heuristics gets very interesting performances when the reliability requirements decrease. For example, GR-SMRS is capable of reaching the optimal acceptance rate when $UR_l=0.95$.

As the objective function of the model aims to minimize the size of the backup tree formed of BPs , it is interesting to evaluate and compare the ratio of the protected paths (with a BP) to the total number of accepted requests. Figure 5.7 compares this ratio for different physical topologies. For the first two physical topologies, as we only consider shortest paths, it is straightforward that we obtain a greater number of protected configurations. However, for the ARPANET physical topology, we notice that there are less protected configurations provided by *GR-SMRS*. In fact, as the acceptance rate is lower for *GR-SMRS*, the routing configurations can be totally different from those obtained by CPLEX. Thus, CPLEX would more likely find feasible routing configurations (in terms of resources availability and reliability requirements) having high costs (protected by BPs) than dropping the request.

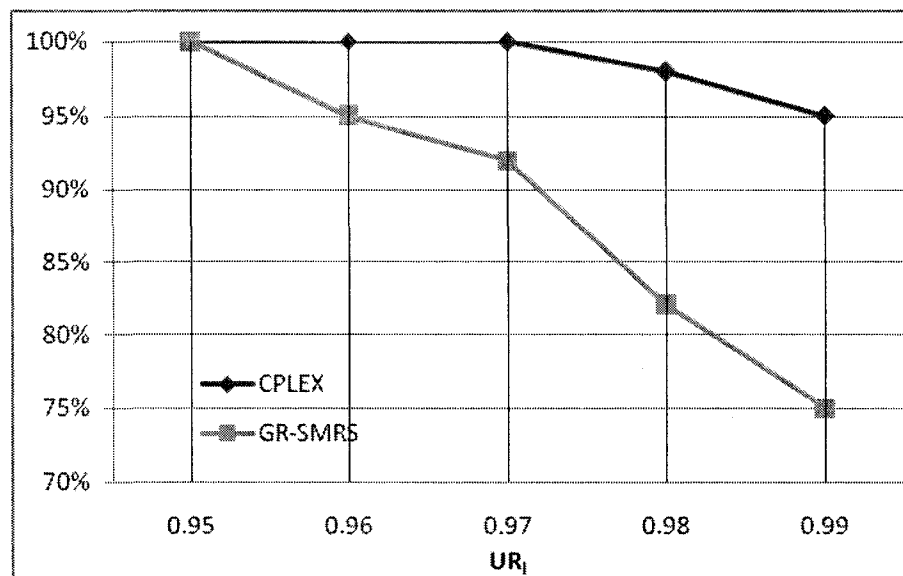


Figure 5.5 Comparative acceptance rate *GR-SMRS* vs. CPLEX for PT1

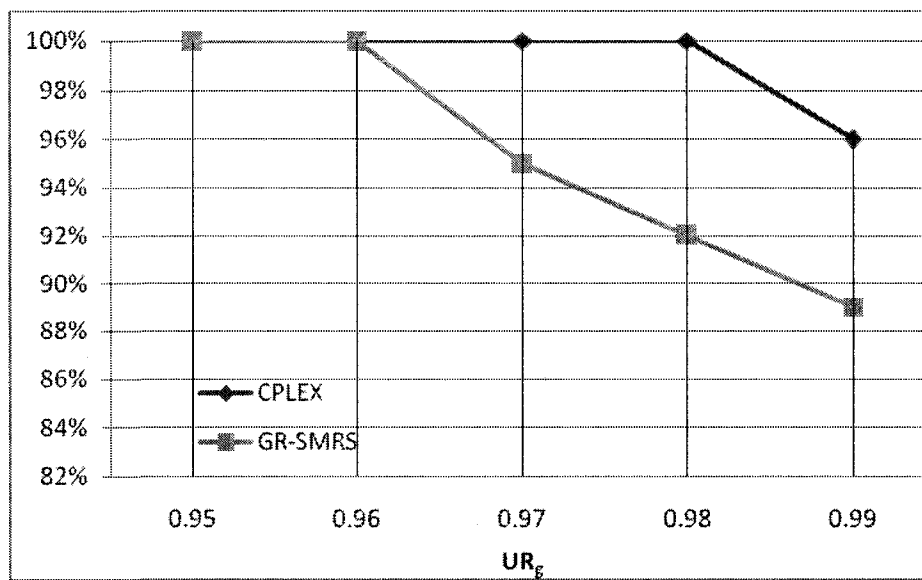


Figure 5.6 Comparative acceptance rate *GR-SMRS* vs. CPLEX for PT1

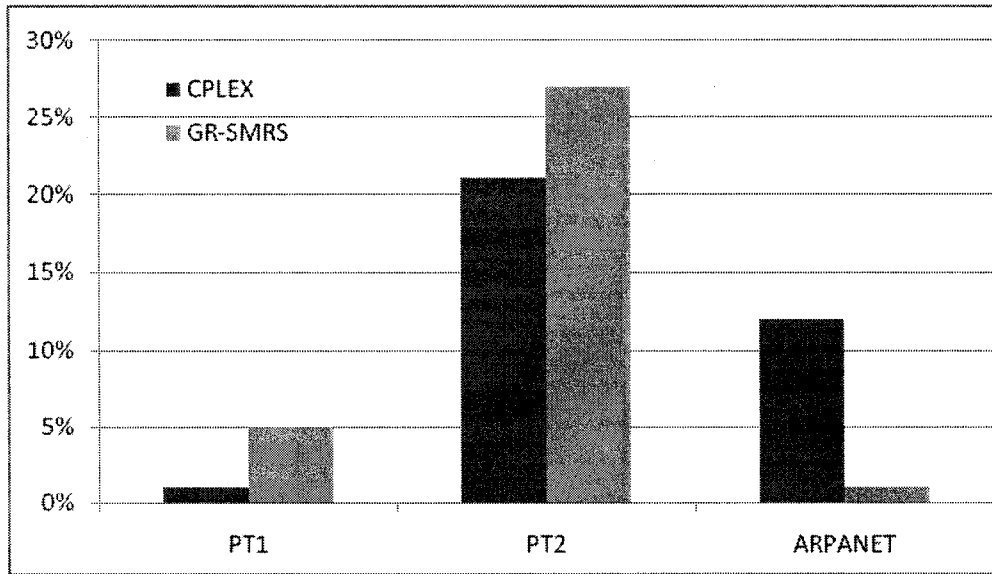


Figure 5.7 Comparative ratios of protected paths

5.4.2 Comparative Results: *GR-SMRS* vs. *MSS*

In this subsection, we propose to evaluate the performances of *GR-SMRS* for the different physical topologies and with different values of the reliability requirements. Moreover, in order to highlight the benefits of considering differentiated reliability when computing survivable routing configurations, we propose to compare the performances of our heuristic to an algorithm, named *MSS*, proposed by Li *et al.* (2006). This latter constructs a tree from the source to the set of destinations using the Shortest Path Tree (*SPT*) algorithm and computes for every branch an *SRLG*-disjoint protected path, such that the whole tree is well protected. Before computing the protection tree, the links' metrics are modified in order to take into account the backup resources sharing, discussed earlier.

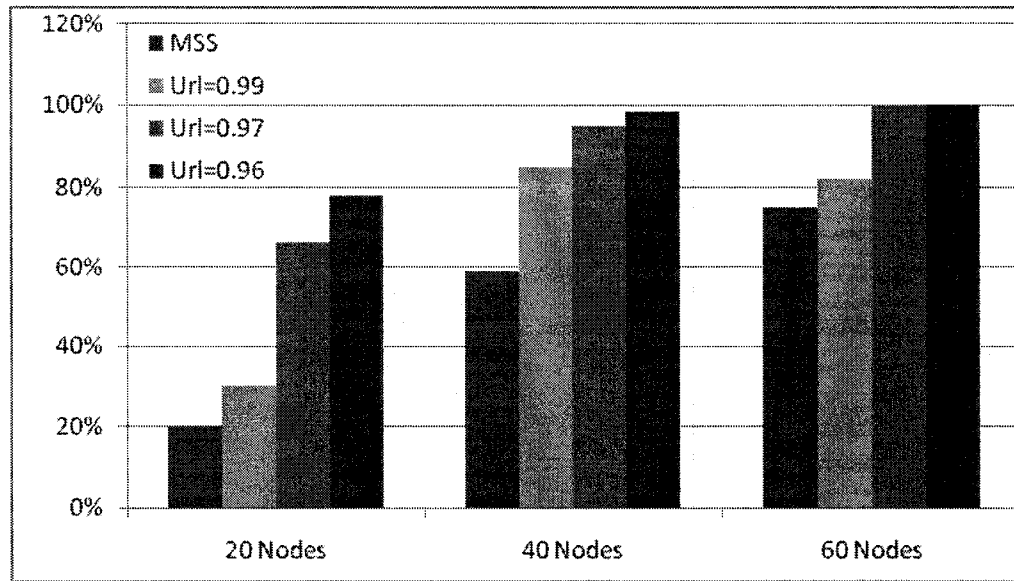


Figure 5.8 Comparative acceptance rates for different local reliability requirements with $D=3$

We first generated multicast requests having 3 destinations. Figure 5.8 depicts the acceptance rates, for the different considered topologies, function of the local reliability requirement UR_l . It is straightforward that when the reliability requirement becomes tighter, the acceptance rate decreases accordingly. Moreover, we clearly notice the advantages of considering the differentiated reliability. In fact, the gap on the acceptance rate between *MSS* and *GR-SMRS* with a reliability requirement of 0.99, reaches 40% for the 40 nodes network.

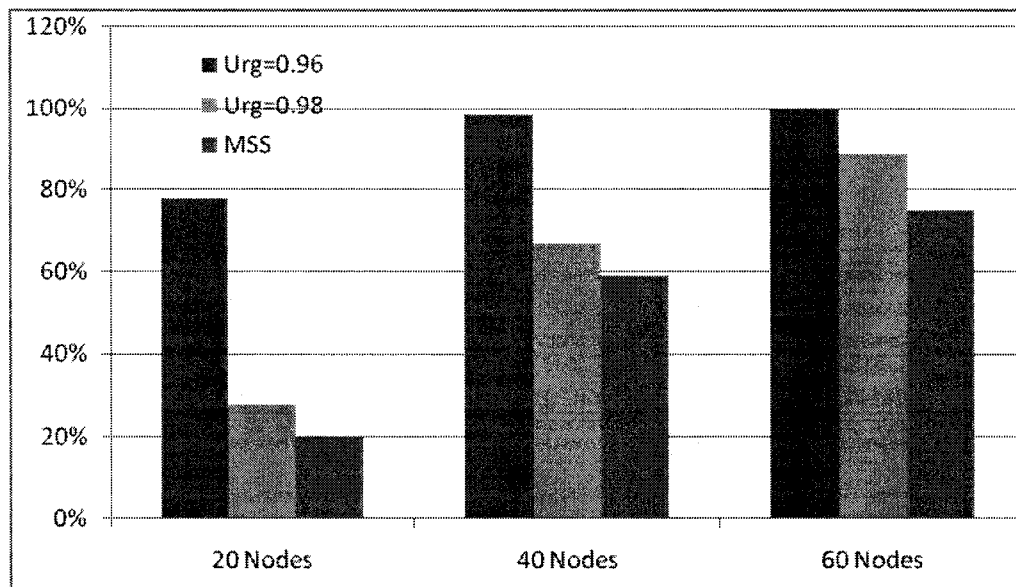


Figure 5.9 Comparative acceptance rates for different global reliability requirements with D=3

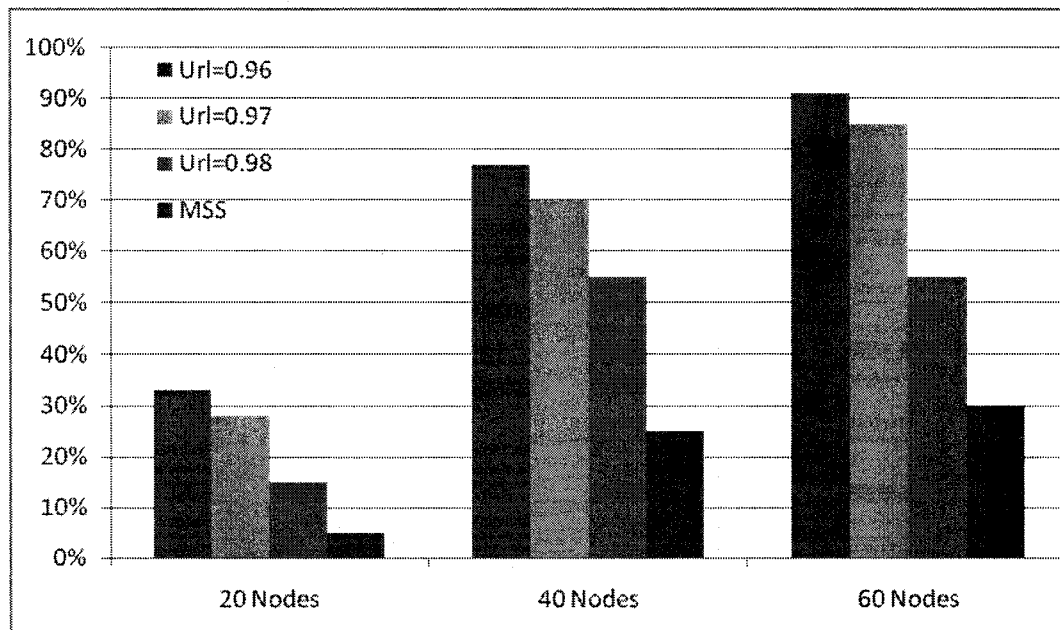


Figure 5.10 Comparative acceptance rates for different local reliability requirements with D=7

We also evaluated the effect of the global reliability on the acceptance rates provided by *GR-SMRS*. The obtained results are depicted in Figure 5.9. It is again straightforward that increasing the reliability requirements impacts the acceptance rates. In fact, when we decrease UR_g from 0.98 to 0.96, the acceptance rate is improved by about 200% for the 20 Nodes network.

We also notice that having tight global reliability requirements, compared to local ones, impacts more the performances of the algorithm. In fact, the performances of *GR-SMRS* are clearly better in Figure 5.8 where they reach greater acceptance rates. Indeed, if we consider similar values for UR_g and UR_l , there can exist some routing configurations guaranteeing only the local reliability requirements and not the global ones. In the contrary, there can not exist configurations ensuring UR_g and violating UR_l .

We also evaluated the acceptance rates when the size of the destinations set is increased and equals to 7. As we kept the same reliability requirements and physical topologies, the acceptance rates are decreased accordingly. However, the advantage of the differentiated reliability is again highlighted as depicted in Figures 5.10 and 5.11.

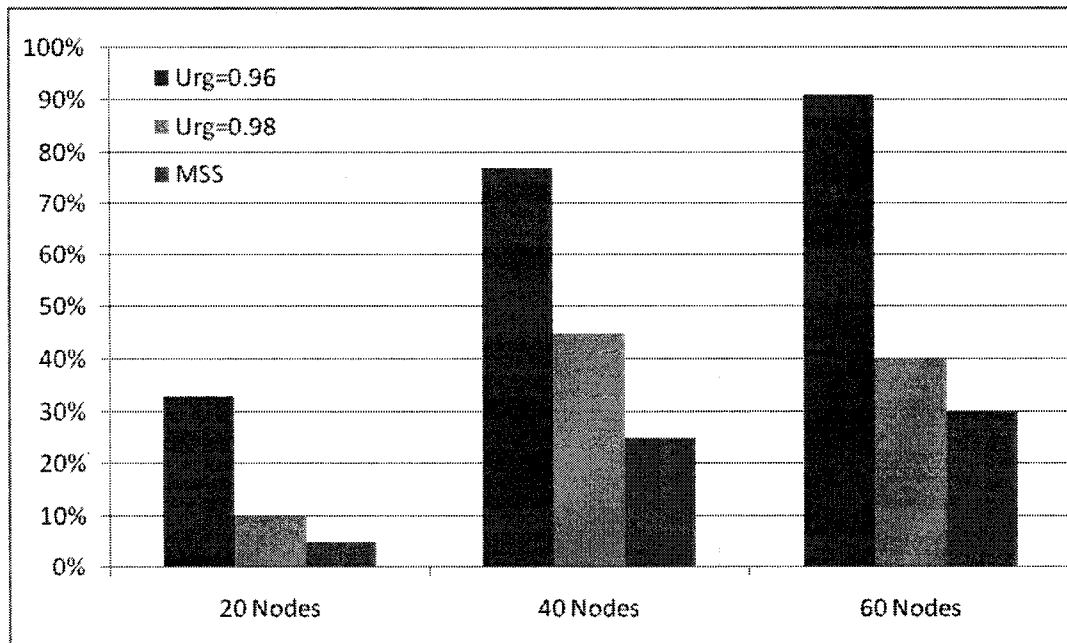


Figure 5.11 Comparative acceptance rates for different global reliability requirements with $D=7$

5.5 Conclusion

In this paper, we have tackled the problem of Survivable Multicast Routing under *SRLG* constraints (*SMRS*). For that, we first formulated the problem as an Integer Linear Programming model that is shown NP-Complete. We then proposed a heuristic named *GR-SMRS* that relies on a decomposition technique to alleviate the complexity of the problem.

Our mechanism acts as a reliable admission controller that provides reliable enough multicast routing configurations for the incoming multicast requests. This mechanism was tested through simulations and was proven to provide good performances, especially when compared to another algorithm that does not consider the differentiated reliability when taking routing decisions.

As future results, we first intend to develop a local search heuristic to tackle the *SMRS* problem. We also intend to consider other quality of service requirements (propagation delay and optical signal quality) while reliably routing new lightpaths.

CHAPITRE 6

DISCUSSION GÉNÉRALE

Dans ce chapitre, nous commençons par une synthèse de nos objectifs de recherche et notre contribution en regard des différents défis évoqué à travers les problématiques abordées. Par la suite, nous discutons l'approche méthodologique considérée. Enfin, nous analysons les résultats obtenus et de leurs portées.

6.1 Synthèse des travaux

La recherche menée dans cette thèse a donné lieu à cinq articles principaux de revue, dont trois présentés comme chapitres de cette thèse, une demande de brevet et plusieurs articles de conférences internationales avec comité de lecture. Chacun de ces articles de revue traite un ou plusieurs points évoqués dans nos objectifs de recherche et dont la récapitulation est donnée ci-dessous. Deux de nos articles de revue sont déjà publiés tandis que les autres sont actuellement en cours d'évaluation.

Le premier objectif de tout travail de recherche porte sur l'analyse de la littérature pertinente dans le domaine. Ainsi, nous avons consacré le Chapitre 3 à une revue de littérature exhaustive des mécanismes et architectures d'allocation de ressources, de contrôle d'admission et de support de *QoS* dans les réseaux de prochaines

génération. Ceci nous a permis de déceler les faiblesses et les lacunes de ces mécanismes afin de les traiter plus tard dans nos travaux de recherche.

Dans un premier lieu, nous nous sommes concentrés sur le thème assez large de l'allocation dynamique des ressources et du contrôle d'admission dans les réseaux *GMPLS* et *MPLS*. Ainsi, notre première contribution a été de proposer un mécanisme de routage et de contrôle d'admission dans les réseaux multicouches *GMPLS*. Outre la problématique de routage, le problème consiste également à fournir certaines garanties de *QoS* aux couches supérieures du réseau, à savoir le délai de propagation optique de bout-en-bout et la qualité du signal optique. Le mécanisme de contrôle d'admission proposé repose sur une modélisation en nombres entiers du problème et une résolution exacte avec le logiciel de programmation mathématique ILOG CPLEX. L'analyse comparée des performances a montré que le mécanisme proposé améliore le taux de blocage des nouvelles connexions.

Le deuxième volet de nos contributions porte sur le contrôle d'admission dans les réseaux *MPLS* avec support de *QoS* de bout-en-bout. En effet, les mécanismes rencontrés dans la littérature n'offrent généralement pas de garanties de *QoS* de bout-en-bout et même les approches analytiques sont très conservatrices et ne permettent généralement pas une utilisation optimale des ressources du réseau. Nous avons d'ailleurs publié deux articles de conférences traitant le problème de contrôle d'admission en modélisant les délais sur les liens du réseau comme des files d'attente *M/M/1*. Nous avons également démontré que cette approximation du délai est inadéquate et s'avère conservatrice. Afin de pallier ce problème, nous avons d'abord proposé une borne supérieure sur le délai et la gigue maximale de bout-en-bout, qui repose sur une certaine probabilité de violation des contraintes de *QoS*. Un tel résultat peut être utilisé aussi bien pour des mécanismes centralisés (où le contrôle est centralisé dans un gestionnaire de ressources) que des mécanismes distribués (avec des protocoles de signalisation ou de réservation de ressources). Nous avons par la suite proposé une

modélisation mathématique du problème de contrôle d'admission dans les réseaux *MPLS* avec contraintes statistiques de *QoS*. Le mécanisme proposé peut être catégorisé comme basé sur les mesures (*Measurement-based Admission Control*). En effet, des données empiriques sur les distributions des délais des paquets sur chaque équipement du réseau sont utilisées dans l'évaluation de l'admissibilité des nouveaux trafics.

Le troisième volet de nos contributions porte sur la fiabilité des réseaux optiques *WDM*. En effet, la famille de technologies *WDM* a permis une exploitation optimale de la bande passante de la fibre en multiplexant plusieurs canaux simultanément. Ce grand gain en bande passante accentue davantage les effets d'une panne éventuelle de cette fibre, vu la quantité énorme de données véhiculées. Pour cela, il est très important, lors de l'établissement de chemins optiques, de prévoir des mécanismes performant de protection. Ce dernier point a donné lieu à trois articles de revue dont seulement un est présenté dans cette thèse. Dans ce dernier, nous avons traité le problème de routage *multicast* des chemins optiques avec fiabilité différentielle. L'algorithme proposé peut cependant s'appliquer aux cas de chemins optiques *unicast*. Une étude comparative des résultats de simulations a permis, entre autres, de démontrer les avantages de la prise en considération de la fiabilité différentielle.

6.2 Méthodologie

La proposition de nouveaux mécanismes et algorithmes doit être validée par une preuve de concept. Nous avons choisi, afin d'évaluer les performances des mécanismes proposés, d'utiliser une validation par simulations. Pour ce faire, les logiciels MATLAB et CPLEX, le simulateur de réseaux OPNET ainsi que l'environnement de développement Visual C++.Net ont été utilisés. De plus, plusieurs batteries de tests ont été effectuées pour la validation des algorithmes proposés suivant un plan d'expérience clair et assez complet.

6.3 Analyse des résultats

La validation numérique et par simulations des mécanismes et algorithmes proposés montre que les résultats obtenus sont très satisfaisants. Outre les performances prometteuses, nous avons veillé à ce que les algorithmes proposés soient compatibles avec les architectures des réseaux de prochaines générations en reposant sur des protocoles déjà standardisés et implantés, afin d'assurer une intégration à moindre coût.

De plus, afin d'inférer plus de crédibilité à nos travaux, nous avons procédé à des analyses comparatives pour les différents algorithmes et mécanismes proposés. Les mécanismes auxquels nous nous sommes comparés étaient généralement proposés dans des publications scientifiques récentes. Les résultats des simulations montrent une amélioration nette des performances et ce, pour les différents problèmes abordés. En effet, le mécanisme de contrôle d'admission proposé pour les réseaux *GMPLS* a permis de diminuer considérablement le taux de blocage des connexions en minimisant la charge supplémentaire de création de nouveaux chemins optiques. D'autre part, les résultats analytiques obtenus pour borner les contraintes de délai et de gigue maximales ont abouti au développement de l'algorithme de contrôle d'admission dans les réseaux *MPLS* avec contraintes statistiques de *QoS*. Cet algorithme a permis encore une fois de minimiser le taux de blocage des nouvelles connexions tout en respectant les contraintes statistiques de *QoS*. Les mécanismes également proposés pour le routage fiable des chemins optiques ont également fait l'objet d'une évaluation comparative et ont permis, en plus de diminuer le taux de blocage des chemins optiques, de mettre en exergue les avantages de la fiabilité différentielle.

CHAPITRE 7

CONCLUSION

Les réseaux de communication de prochaines générations s'orientent de plus en plus vers la convergence des services et des technologies de transport et d'accès. De ce fait, les réseaux deviennent de plus en plus fort sollicités, surtout que la croissance de la demande en bande passante des applications supportées dépasse nettement l'augmentation de la capacité de transport. Ceci a ainsi écarté certaines solutions antérieurement adoptées telles que le surdimensionnement des réseaux. En outre, l'engouement des utilisateurs vers des applications multimédia et temps-réel contraint les opérateurs de réseaux à garantir de nouvelles exigences de qualité de service (*QoS*). D'un autre côté, la criticité de certains types de trafic a fait de la fiabilité des réseaux de prochaines générations une recommandation cruciale. Cette thèse avait pour objectif d'apporter des solutions à ces différents problèmes en proposant des mécanismes de contrôle d'admission avec support de la qualité de service ainsi que des algorithmes de routage fiable dans les réseaux optiques. Dans ce chapitre de conclusion, nous allons mettre en évidence les contributions de cette thèse. Par la suite, nous exposerons les limites de notre travail avant de terminer par une ébauche de recommandations pour des travaux futurs.

7.1 *Sommaire des contributions*

Le premier but de cette thèse était de proposer des mécanismes et des algorithmes pour l'optimisation de l'allocation des ressources et de contrôle d'admission dans les réseaux de prochaines générations. Le but étant d'offrir des garanties de qualité de service aux trafics véhiculés. Cet objectif a été atteint grâce aux contributions suivantes :

- Proposition d'un mécanisme de contrôle d'admission des nouveaux chemins optiques dans les réseaux *GMPLS*. Cette proposition est précédée par une étude sommaire des requis de *QoS*, pour l'établissement de chemins optiques ;
- Développement d'une borne supérieure théorique pour les contraintes statistiques de délai et de gigue de bout-en-bout. Le calcul de cette borne est basé sur les données empiriques des distributions des délais des paquets sur les équipements du réseau ;
- Proposition d'un mécanisme de contrôle d'admission dans les réseaux *MPLS* avec contraintes statistiques de qualité de service. La modélisation des contraintes de qualité de service repose sur le résultat théorique obtenu précédemment.

Le second but de la thèse était d'adresser le problème de fiabilité dans les réseaux optiques *WDM* en proposant des algorithmes de routage fiable (*unicast* et *multicast*) avec des garanties statistiques ou strictes de fiabilité. Plus spécifiquement, nos contributions sont définies comme suit :

- Proposition d'un mécanisme, basé sur la programmation mathématique, de routage des chemins optiques *unicasts* dans les réseaux *WDM* avec garanties statistiques de fiabilité notée également *fiabilité différentielle* ;
- Proposition d'un mécanisme, basé sur la programmation mathématique, de routage des chemins optiques *multicasts* dans les réseaux *WDM* avec garanties strictes de fiabilité ;
- Proposition d'un algorithme pour le routage des chemins optiques *multicasts* dans les réseaux *WDM* avec fiabilité différentielle. Le problème a d'abord été formulé comme un modèle mathématique linéaire en nombre entiers. Un algorithme heuristique a été proposé par la suite ;

Toutes les solutions proposées ont été validées par simulations. Cette validation a permis d'avoir des résultats qui montrent une amélioration des performances par rapport aux mécanismes de référence, disponibles dans la littérature.

7.2 Limitations des travaux

Notre travail présente quelques limitations, que nous allons présenter ci-dessous. Une première limitation pourrait venir de la nature centralisée des algorithmes proposés. En effet, les mécanismes de contrôle d'admission proposés reposent sur des données sur l'état du réseau, collectées et acheminées à un gestionnaire de ressources central, responsable du contrôle d'admission. Cependant, cette limitation peut être surmontée étant donné que les architectures des réseaux de prochaines générations prévoient des gestionnaires de ressources centralisés (*PCE* pour l'IETF et *RACS* pour ETSI, etc.).

Une deuxième limitation serait l'absence explicite d'un mécanisme, ou protocole, permettant la communication entre le gestionnaire des ressources et les

équipements du réseau, afin de recueillir certaines mesures et renforcer les décisions d'acceptation ou de rejet des nouveaux trafics. En effet, nos solutions font l'hypothèse de l'existence d'un tel mécanisme sans en donner la description.

Finalement, étant donné que certains de nos mécanismes de contrôle d'admission reposent sur une résolution optimale du problème modélisé, l'applicabilité de ces mécanismes est ainsi contrainte à la taille des réseaux à contrôler. En effet, cette résolution optimale a été démontrée adéquate pour des réseaux de tailles réelles. L'augmentation éventuelle de la taille des réseaux des fournisseurs de service et l'intégration de deux ou plusieurs réseaux peut rendre une telle résolution optimale non faisable. Cependant, ceci peut être en partie compensé par l'augmentation continue de la puissance de calcul et de traitement des équipements informatiques modernes.

7.3 Indication des travaux futurs

Les réseaux de prochaines générations (*NGN*) étant encore dans une phase de conception, plusieurs problèmes restent encore non-abordés. Il existe ainsi plusieurs pistes de travaux futurs à la présente thèse. Nous allons présenter quelques unes qui s'inscrivent dans la continuité logique du travail entrepris dans cette thèse.

Une première piste qui découle directement de nos travaux serait d'implémenter les algorithmes et mécanismes proposés soit à l'aide d'un simulateur de réseau (OPNET ou NS2) ou d'un réseau test (*testbed*) qui permettrait d'évaluer des indices de performance reliés aux opérations du réseau (tels que la surcharge de calcul et de signalisation, la latence réelle de calcul, etc.).

Une seconde possibilité serait d'exploiter la borne théorique sur les contraintes statistiques de qualité de service afin de développer un protocole distribué de contrôle

d'admission. Ce protocole peut simplement être une extension à des mécanismes existants tels que *RSVP-TE*. Ceci permettra une compatibilité du protocole avec les architectures existantes des réseaux cœur.

De plus, étant donné que les réseaux de prochaines générations convergent vers un plan de contrôle unifié, tel que *GMPLS*, une étude pourrait être menée afin d'intégrer les efforts d'optimisation à différents niveaux des couches du réseau (*IP*, *MPLS*, *WDM*), dans le but de proposer un mécanisme générique pour le contrôle d'admission. Dans un tel cadre, une étude approfondie des recommandations et des besoins de chacune des technologies impliquées doit être menée. De plus, une énumération exhaustive des différents types de trafics ainsi que de leurs requis de qualité de services devra également être investiguée.

CONTRIBUTIONS À LA RECHERCHE

Le travail mené lors de cette thèse a donné lieu à plusieurs contributions scientifiques.

Nous donnons ci-dessous la liste des différents articles :

- **Articles de revues acceptés et publiés**

J1) H. A. Harhira & S. Pierre. 2008. Joint Routing and Admission Control Problem Under Statistical Delay and Jitter Constraints in MPLS Networks, *Computer Communications*. 31(15), 3700-3706.

J2) H. A. Harhira & S. Pierre. 2008. A Novel Admission Control Mechanism in GMPLS-Based IP Over Optical Networks, *Computer Networks*, 52(6), 1281-1290.

- **Articles de revues soumis**

J1) H. A. Harhira & S. Pierre. A Survivable Multicast Routing Mechanism in WDM Optical Networks. Submitted to *Photonic Communication Networks*.

J2) H. A. Harhira & S. Pierre. Survivable Routing of Multicast Trees under SRLG Constraints in WDM Optical Networks. Submitted to *Journal of Optical Networks*.

J3) H. A. Harhira & S. Pierre. Survivable Routing Under SRLG Constraints with Differentiated Reliability in WDM Optical Networks. Submitted to *IEEE journal of Lightwave Technology*.

- **Articles de conférences**

C1) H.A. Harhira & S. Pierre. 2007. Multi-Path Dynamic Admission Control in MPLS Networks with End-to-end Delay Guarantees. Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks. Chania, Greece (1, 45-49).

C2) H.A. Harhira & S. Pierre. 2008. A Novel Connection Admission Control Mechanism with Statistical Delay Constraints in MPLS Networks. Proceedings of International Conference on High Performance Computing, Networking and Communication Systems. USA (Vol. 1, pp. 146-153).

C3) H.A. Harhira & S. Pierre. 2007. A Mathematical Model for the Admission Control Problem in MPLS Networks with End-to-end Delay Guarantees. Proceedings of IEEE International Conference on Computer Communications and Networks. Hawaii, USA (Vol. 1, pp. 1193-1197).

C4) H.A. Harhira & S. Pierre. 2007. Global Cluster Based Planning of Wireless Sensor Networks. Proceedings of IEEE international Conference on Internet ICI. Tashkand, Uzbekistan (Vol. 1, pp. 1-6).

- **Demandes de brevets techniques**

B1) H.A. Harhira & Y. Lemieux. Improved resources allocation plan in a network. P24163.

BIBLIOGRAPHIE

AbuAli, N., Muftah, H. T. & Gazor, S. (2005). Online Distributed Statistical Delay MBAC with QoS Guaranteed for VPLS Connections. Proceeding of International Conference on Telecommunications. Zagreb, Croatia, (Vol. 1, pp. 383-390).

Ajmone, M., Casetti, C., Mardente, G. & Mellia, M. (2007). A Framework for Admission Control and Path Allocation in DiffServ Networks, International Journal of Computer and Telecommunications Networking, (51), 2738-2752.

Angulo, M., Torres-Roman, D., Turrubiarres, M. & Munoz-Rodriguez, D. (2005). Admission Control of a Stateless Network: Effective Bandwidth Approach. Proceedings of the IEEE International Conference on Electronics Communications and Computers. Mexico, Mexique (Vol. 2, pp. 183-187).

Anjali, T. & Scoglio, C. (2006). A Novel Method for QoS Provisioning with Protection in GMPLS Networks, Computer Communications, (29), 757-764.

Apostolopoulos, G., Guerin, R., Kamat, S. & Tripathi, S. (1998). Quality of Service Routing: A Performance Perspective. Proceedings of ACM SIGCOMM. Vancouver, British Columbia (Vol. 1, pp. 1-8).

Balon, S., Skivee, F. & Leduc, G. (2005). Comparing Traffic Engineering Objective Functions. Proceedings of the CoNext ACM conference. Toulouse, France, (Vol. 1, pp. 224-225).

Berger, L. (2003). Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description. RFC 3471. [En ligne]. USA : Internet Engineering Task Force (IETF).

Black, D., Black, S., Carlson, M., Davids, E., Wand, Z. & Weiss, W. (1998). An Architecture for DiffServ Services. RFC 2475. [En ligne]. USA : Internet Engineering Task Force (IETF).

Bose S.K. (2002). An Introduction to Queuing Systems. Kluwer/Plenum Publishers.

Braden, R., Clark, D. & Shenker, S. (1994). Integrated Services in the Internet Architecture: An Overview. RFC 1633. [En ligne]. USA : Internet Engineering Task Force (IETF).

Braden, R., Zhang, L., Berson, S., Herzog, S. & Jamin, S. (1997). Resource ReSerVation Protocol (RSVP). RFC 2205. [En ligne]. USA : Internet Engineering Task Force (IETF).

Cardillo, R., Curri, V. & Mellia, M. (2005). Considering Transmission Impairments in Wavelength Routed Networks, Proceedings of the Optical Networks Design and Modelling. Milan, Italie (Vol. 1, pp. 421-429).

Chamberland, S., (2004). On the Joint Link Dimensioning and Routing Metric Assignment Problem for Reliable WDM Networks, Computer & Electrical Engineering, 30(5), 383-401.

Colliti, W., Steenhaut, K., Nowe, A. & Tran, T.N.L. (2006). Integrated Multilayer Traffic Engineering in the GMPLS based IP over Optical Networks. Proceedings of the IASTED International Conference on Networks and Communication Systems. Chiang Mai, Thailand, (Vol. 1, pp. 396-401).

Constantinescu, D. & Popescu, A. (2006). Modeling of One Way Transit Time in IP Routers. Proceedings of the IEEE Advanced International Conference on Telecommunications. (Vol. 1, pp. 16-17).

Courcoubetis, C., Siris, V. A. & Stamoulis, G. D. (1999). Application of the Many Sources Asymptotic and Effective Bandwidths to Traffic Engineering, Telecommunication System Modeling, Analyzing and Management, 2(12), 167–191.

Datta, P. & Somani, A. K. (2004). Diverse Routing for Shared Risk Resource Groups (SRRG) Failures in WDM Optical Networks. Proceedings of the First IEEE Conference on Broadband Networks. San Jose, USA (Vol. 1, pp. 120-129).

Davenport, W.B. (1970). Probability and Random Processes: An Introduction for Applied Scientists and Engineers. New York: McGraw-Hill.

De Veciana, G. & Kesidis, G. (1996). Bandwidth Allocation for Multiple Quality of Service using GPS, IEEE Transactions on Information Theory, 1(42), 268-272.

Duan, Z., Zhang, Z. L., Hou, Y. T. & Gao, L. (2004). Core Stateless Bandwidth Broker Architecture for Scalable Support of Guaranteed Services, IEEE Transactions on Parallel and Distributed Systems, 2(15), 167–182.

Elias, J., Martignon, F., Capone A. & Pujolle, G. (2007). A New Approach to Dynamic Bandwidth Allocation in Quality of Service Networks: Performance and Bounds, Journal of Computer and Telecommunications Networking, (51), 2833-2853.

Farrel, A., Vasseur, J.P. & Ash., J. (2006). A Path Computation Element (PCE)-Based Architecture. RFC 4655. [En ligne]. USA : Internet Engineering Task Force (IETF).

Fidler, M. & Sander, V. (2004). A Parameter Based Admission Control for Differentiated Services Networks, *Computer Networks*, 4(44), 463-479.

Flegkas, P., Trimintzios, P., Pavlou, G. & Liotta, A. (2003). Design and Implementation of a Policy-based Resource Management Architecture, *Journal on Integrated Network Management*, 1(24), 215-229.

Georgoulas, S., Pavlou, G., Borcoci, E., Ho, K.H. & Vraha, E. (2008). Enabling Quality of Service for End-to-end Multimedia Content Delivery Through Admission Control: Placement, Functionality and Benefits. *Proceedings of the IEEE International Conference on Automation, Quality and testing, Robotics*. Cluj-Napoca, Romania (Vol. 1, pp. 369-374).

Gerla, M., Cassette, C., Seongwook, S. & Reali, G. (2001). Resource Allocation and Admission Control Styles in QoS DiffServ Networks. *Proceeding of the International Workshop on Quality of Service in Multiservice IP Networks*. Londre, UK (Vol. 1, pp. 113-128).

Girish, M.K., Zhou, B. & Hu, J.Q. (2000). Formulation of the Traffic Engineering Problems in MPLS Based IP Networks. *Proceedings of the IEEE symposium on Computers and Communications*. Antibes, France (Vol. 1, pp. 214-215).

Gopalan, K., Chiueh, T. & Lin, Y. J. (2004). Probabilistic Delay Guarantees Using Delay Distribution Measurement. *Proceedings of ACM Multimedia Conference*. New York, USA (Vol. 1, pp. 900-907).

Gritella, G. & Boswarthick, D. (2008). *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability*

Requirements. TS_181_005, [En ligne], France, European Telecommunications Standards Institute (ETSI).

Guerin, R. & Orda, A. (1999). QoS-based Routing in Networks with Inaccurate Information: Theory and algorithms, *IEEE/ACM Transactions on Networking*, 7(3), 350-364.

Gui, L., Cao, J., Yu, H. & Li, L. (2007). A New Shared-risk Link Groups (SRLG)-disjoint path Provisioning with Shared Protection in WDM Optical Networks, *Journal of Network and Computer Applications*, 2(30), 650-661.

Gunreben, S. & Rambach, F. (2008). Assessment and Performance Evaluation of PCE-Based Inter-layer Traffic Engineering. *Proceedings of the International Conference on Optical Network design and Modeling. Barcelone, Espagne (Vol. 1, pp. 1-6).*

Guo, L. & Li, L. (2007). A Novel Survivable Routing Algorithm With Partial Shared Risk Link Groups (SRLGs)- Disjoint Protection Based on Differentiated Reliability Constraints in WDM Optical Mesh Networks, *IEEE Journal of Lightwave Technology*, 6(25), 1410-1415.

Harhira, H. A. & Pierre, S. (2007). A Mathematical Model for the Admission Control Problem in MPLS Networks with End-to-end Delay Guarantees. *Proceedings of IEEE International Conference on Computer Communications and Networks. Hawaii, USA (vol. 1, pp. 1193-1197).*

Harhira, H. A. & Pierre, S. (2007). Multi-path Dynamic Admission Control in MPLS Networks with End-to-end Delay Guarantees. *Proceedings of the 2nd ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks. Chania, Greece (Vol. 1, pp. 45-49).*

Harhira, H. A. & Pierre, S. (2008). A Novel Admission Control Mechanism in GMPLS-Based IP over Optical Networks, *Computer Networks*, 52(6), 1281-1290.

Harhira, H. A. & Pierre, S. (2008). A Novel Connection Admission Control Mechanism with Statistical Delay Constraints in MPLS Networks. *Proceedings of International Conference on High Performance Computing, Networking and Communication Systems. USA* (Vol. 1, pp. 146-153).

Harhira, H. A. & Pierre, S. (2008). Joint Routing and Admission Control Problem Under Statistical Delay and Jitter Constraints in MPLS Networks, *Computer Communications*. 31(15), 3700-3706.

Ho, K.H., Wang, N., Trimintzios, P. & Pavlou, G. (2004). Multi-objective Egress Router Selection Policies for Inter-domain Traffic with Bandwidth Guarantees, *IEEE journal of Networking*, (1), 271-283.

Hu, J.Q. (2003). Diverse Routing in Optical Mesh Networks, *IEEE Transactions on Communications*, 3(51), 489-494.

Hu, T. & Muftah, H.T. (2006). Dynamic Constrained Multicast Routing in WDM Networks: Blocking Probability, QoS and Traffic Engineering. *Proceedings of the IEEE International Symposium on Computers and Communications. Cagliari, Italy* (Vol. 1, pp. 974-980).

ILOG, Inc. (2005) *Using the CPLEX Callable Library and CPLEX Mixed Integer Library*.

Kelly, F.P. (1996). Notes on effective bandwidths. In Stochastic Networks: Theory and applications. In Oxford University Press. Royal Statistical Society Lecture Notes. (Vol. 4, pp. 141-168) Londre, U.K.

Kunz, R., Nielson, S., Clement, M. & Snell, Q. (2001). Effective Bandwidth for Traffic Engineering. Proceedings of the IEEE Workshop on High Performance Switching and Routing. Dallas, USA (Vol. 1, pp. 119-123).

Li, Y., Jin, Y. L. & Li, L. L. (2006). On Finding the Multicast Protection Tree Considering SRLG in WDM Optical Networks, ETRI journal, 4(28), 517-520.

Likhanov, N., Mazumdar, R. R. & Theberge, F. (2004). Providing QoS in Large Networks: Statistical Multiplexing and Admission Control. In K. Boukas and R.P. Malhamé (éd.) Analysis, Control and Optimization of Complex Dynamic Systems (137-167). Berlin: Springer.

Malcolm, J., Agogbua, J., O'Dell, M. & McManus, J. (1999). Requirements for Traffic Engineering Over MPLS. RFC 2702. [En ligne]. USA : Internet Engineering Task Force (IETF).

Markidis, G. & Tzanakaki, A. (2008). Network Performance Improvement Through Differentiated Survivability Services in WDM Optical Networks, Journal of Optical Networking, 6(7), 564-572.

Movsichoff, B. A., Lagoa, C.M. & Che, H. (2005). Decentralized optimal Traffic engineering in Connectionless networks, IEEE Journal on Selected Areas in Communications, 2(23), 293-303.

Ou, C., Zhang, J. & Zhang, H. (2004). New and Improved Approaches for Shared-path Protection in WDM Mesh Networks, *Journal of Lightwave Technology*, 5(22), 1223-1232.

Oulai, D., Chamberland, S. & Pierre, S. (2007). A New Routing-Based Admission Control for MPLS Networks, *IEEE Communication Letters*, (11), 216-218.

Pan, P., Swallow, G. & Atlas, A. (2005). Fast Reroute Extensions to RSVP-TE for LSP Tunnels. RFC 4090. [En ligne]. USA : Internet Engineering Task Force (IETF).

Pan, X. & Xiao, G. (2006). Heuristics for Diverse Routing in Wavelength-routed Networks with Shared Risk Link Groups, *Photonic Network Communications*, 1(11), 29-38.

Pasias, V., Karras, D.A. & Papademetriou, R.C. (2004). Traffic Engineering in Multi-service Networks comparing Genetic and Simulated Annealing Optimization Techniques. *Proceedings of the IEEE Conference on Neuronal Networks*. Budapest, Hongrie (Vol. 1, pp. 25-29).

Pierre, S., Said, H. & Probst, W. G. (2000). Routing in Computer Networks using Artificial Neural Networks, *AI Journal in Engineering*, 14(4), 295-305.

Qian, L., Krishnamurthy, A., Wang, Y., Tang, Y., Dauchy, P. & Conte, A. (2004). A New Traffic Model and Statistical Admission Control Algorithm for Providing QoS Guarantees to On-Line Traffic. *Proceedings of the IEEE Globecom 2004*, Texas, USA, (Vol. 2, pp. 1401-1405).

Rostami, M. J., Khorsandi, S. & Khodaparast, A. A. (2007). Cose: A SRLG-Disjoint Routing Algorithm. Proceedings of the Fourth IEEE European Conference on Universal Multiservice Networks. Toulouse, France (Vol. 1, pp. 86-92).

Salvadori, E. & Battiti, R. (2004). A Traffic Engineering Scheme for QoS and Routing in GMPLS Networks Based on Transmission Quality, In the Proceedings Of the Optical Networks Design and Modelling. Ghent, Belgium, (Vol. 1).

Singhal, M. K., Canhui, O. & Mukherjee, B. (2005). Shared Protection for Multicast sessions in Metropolitan WDM Ring Networks. Proceedings of the OFC, (Vol. 1, pp. 218-220).

Stoica, I. & Zhang, H. (1999). Providing Guaranteed Services Without Per Flow Management. Proceedings of the ACM SIGCOMM '99. Cambridge, USA (Vol. 1, pp. 81-94).

Todimala, A. & Ramamurthy, B. (2004). IMSH: An Iterative Heuristic for SRLG Diverse Routing in WDM Mesh Networks. Proceedings of the 13th IEEE Conference on Computer Communications and Networks. Chicago, USA (Vol. 1, pp. 199-204).

Trimintzios, P., Andrikopoulos, I., Pavlou, G., Flegkas, P., Griffin, D., Georgatsos, P., Goderis, D., T'Joens, Y., Georgiadis, L., Jacquenet, C. & Egan, R. (2001). A Management and Control Architecture for Providing IP Differentiated Services in MPLS-Based Networks, IEEE Communications Magazine, 5(39), 80–88.

Trimintzios, P., Pavlou, G., Flegkas, P., Georgatsos, P., Asgari, A. & Mykoniati, E. (2003). Service-driven Traffic Engineering for Intra-domain Quality of Service Management, IEEE Journal of Networks, 3(17), 29–36.

Zhang, B., Zheng, J., & Mouftah, H. T. (2007). A scalable multicast routing protocol for building shortest path trees, *International Journal of Communication Systems*, 20(8), 993-1109.

Zhang, Z. L., Duan, Z. & Hou, Y.T. (2000). Virtual Time Reference System: A Unified Scheduling Framework for Scalable Support of Guaranteed Services. *IEEE Journal on Selected Areas in Communications*, 12(18), 2684-2695.