

Design and analysis of p-cycle-based fault-restorable optical networks with multicast capability

Zhang, Feng

2009

Zhang, F. (2009). Design and analysis of p-cycle-based fault-restorable optical networks with multicast capability. Doctoral thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/19316>

<https://doi.org/10.32657/10356/19316>



**NANYANG
TECHNOLOGICAL
UNIVERSITY**

**DESIGN AND ANALYSIS OF P-CYCLE-BASED FAULT-
RESTORABLE OPTICAL NETWORKS WITH
MULTICAST CAPABILITY**

ZHANG FENG

SCHOOL OF ELECTRICAL & ELECTRONIC ENGINEERING

2009

DESIGN AND ANALYSIS OF P-CYCLE-BASED FAULT-RESTORABLE
OPTICAL NETWORKS WITH MULTICAST CAPABILITY

ZHANG FENG

2009

Design and Analysis of p -Cycle-Based Fault-Restorable Optical Networks with Multicast Capability

Zhang Feng

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in fulfillment of the requirement for the degree of
Doctor of Philosophy

2009

Statement of Originality

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other university or institution.

张峰

Zhang Feng

25-Nov-2009

Date

Summary

With recent advancement in optical transmission technology, WDM networks are able to offer huge capacity to meet the exponentially increasing demand. However, because network failures are capricious, without an efficient and fast recovery mechanism, they can cause huge data loss and therefore lead to severe disruption to network services and calamitous loss to end users. Hence, survivability is crucial to WDM networks carrying huge amount of unicast and multicast traffic. Compared with unicast traffic, multicast traffic suffers even more in a network failure. If a link/node in a multicast session fails, the traffic to all the downstream destinations of the failed link/node will be affected as well. In the past, extensive research has been directed to unicast traffic protection, due to its predominance. Recently, due to the rapid growth of multicast applications, such as video-conferencing, high definition television (HDTV), distance learning, multi-player on-line gaming, and so on, the problem of multicast traffic protection has started to draw more and more research interests.

To our best knowledge, the preconfigured protection cycle (p -cycle) based approaches, which have been intensively studied for unicast traffic protection, have not been investigated for multicast traffic protection yet. Thus, motivated by the impact of the network failures to the optical multicast traffic and the merits of p -cycles, this thesis focuses on development and investigation of p -cycle based protection approaches for optical multicast traffic protection.

The link-protecting p -cycle based approach for multicast traffic protection against link failure is analyzed first. The link protecting p -cycle based protection approach is shown to offer much better performance, compared with all other approaches. In particular, the joint optimization algorithm of p -cycle based link protection proposed achieves the best capacity efficiency among all algorithms for link failure recovery of static multicast traffic. For link

failure recovery of dynamic multicast traffic, the dynamic p -cycle algorithm proposed achieves the lowest blocking probability; whereas the p -cycle based protected working capacity envelope algorithm offers the fastest computational speed. However, the link-protecting p -cycle based approach cannot handle node failure recovery.

Motivated by the serious impact of node failures, the tree-protecting p -cycle based approach is then proposed, which is an approach for combined node and link failure recovery of multicast traffic. However, the performance of the tree-protecting p -cycle based approach is limited by the difficulty of enumerating all disjoint tree sets.

To further improve the performance of p -cycles for optical multicast traffic protection, the node-and-link protecting p -cycle based approach for optical multicast traffic protection is then proposed for combined node and link failure recovery. The node-and-link protecting p -cycle based protection approach is shown to be superior to the existing multicast protection approaches. In particular, the spare capacity optimization algorithm of the node-and-link protecting p -cycle approach achieves the best capacity efficiency for static traffic; whereas the efficiency score based heuristic algorithm of the node-and-link protecting p -cycle approach provides lowest blocking probability for dynamic traffic.

Through these studies, the p -cycle based protection approaches are proven to be very promising for optical multicast traffic protection, in terms of capacity efficiency and recovery speed. The proposed p -cycle based protection approaches can prevent severe disruptions to network services and calamitous loss to network operator and end users.

Acknowledgement

Throughout my PhD study in Nanyang Technological University, I have been very fortunate to work, meet and enjoy the company of many people. I would like to express my gratitude to them.

I would like to start by expressing my sincere gratitude to my supervisor, Professor Zhong Wen-De, for his constant guide and encouragement throughout my PhD study. Prof. Zhong taught me the way of professional and self-motivated research, which would be life-long beneficial to my career. It is my honor to study under his supervision. I am proud of being one of his PhD students. Many thanks also go to Professor Jin Yao Hui at Shanghai Jiao Tong University for the collaboration, and also suggestions on my research work.

Many thanks go to Nanyang Technological University for the precious research funding and trainings. I would like to thank all the professors in Nanyang Technological University, for their superb teaching and guidance in my tutoring for undergraduate students. I have learned great knowledge and problem solving skills from them. They have also taught me how to give attractive tutorials and design classes to my students. I also would like to thank graduate study office staff and all the EEE administrative staff for their kind support and assistance.

I am also very grateful to many past and current members of Network Technology Research Center (NTRC). I would like to thank Professor Shum Ping, Ms. Koh Lee Min, Mr. Poh Khoon Yong and Mr. Chong Lui Tat for their support. I would like to thank my past and current colleagues, Dr. Fu Song Nian, Dr. Liu Ning, Dr. Xu Zhao Wen, Dr. Tang Ming, Dr. Zhang Zhen Rong, Dr. Chen Bin, Dr. Li Xue Jun, Dr. Sun Jian, Dr. Zhao Lu Ming, Dr. Zhou Yin Zhu, Dr. Yu Xia, Dr. Xia Li, Dr. Ni Na, Ms. Goh Sheng Mei Eunice, Mr. Huang Qi Rui,

Mr. Luo Zheng Qian, Ms. Sona Hassani, Mr. Lin Rong Ping, Mr. Li Yi Hui, Mr. Wang Zi Xiong, Ms. Wu Xuan, Mr. Zhan Han, Mr. Wang Dawei, Ms. Xiong Fei for creating a family-like research environment and for the discussions with them. In particular, I would to express my gratitude to Ms. Goh Sheng Mei Eunice for proof-reading. I wish them all the best in their future career.

Finally, I would like to express my love and gratitude to my parents, for their encouragement and support, which is life-long inspiration to me.

Table of Contents

Summary	i
Acknowledgement	iii
Table of Contents	v
List of Figures	viii
List of Tables	x
List of Acronyms	xii
Chapter 1. Introduction.....	1
1.1 Background and motivation	1
1.2 Objectives.....	6
1.3 Major contribution of the thesis	7
1.4 Organization of the thesis.....	9
Chapter 2. Literature Review.....	11
2.1 Introduction	11
2.2 Network resilience approaches in different layers	11
2.2.1 Physical layer resilience approaches.....	12
2.2.2 Optical layer resilience approaches	13
2.2.3 IP logical layer resilience approaches.....	15
2.2.4 Multi-layer resilience approaches	16
2.3 Optical unicast traffic protection approaches.....	17
2.3.1 Ring based approaches.....	19
2.3.2 Mesh based approaches.....	19
2.3.3 Link/path based restoration approaches.....	21
2.4 p -cycle based protection approaches for optical unicast traffic	22
2.4.1 Link-protecting p -cycle based approach.....	24
2.4.2 Path/segment-protecting p -cycle based approaches.....	28
2.4.3 Node-encircling p -cycle based approach	29
2.4.4 Availability analysis of p -cycle based protection approaches	30
2.5 Optical multicast	31
2.5.1 Optical multicast node architecture (hardware building block).....	32

2.5.2	Optical multicast routing and wavelength assignment (OM-RWA) (algorithmic building block):	36
2.5.3	Control plane functionality and optical multicast performance modeling.....	38
2.6	Optical multicast traffic protection approaches	40
2.6.1	Tree based optical multicast protection approaches	41
2.6.2	Ring based optical multicast protection approaches.....	43
2.6.3	Path/segment based optical multicast protection approaches	44
2.6.4	Performance comparison	45
2.7	Conclusions	48
Chapter 3.	Link-Protecting p -Cycle Based Optical Multicast Protection Approach.....	49
3.1	Introduction	49
3.2	Assumptions, definitions and notations	50
3.3	Protection mechanism of the link protecting p -cycle based approach	52
3.4	Spare capacity optimization algorithm of p -cycle based link protection (SOPL).....	54
3.5	Joint optimization algorithm of p -cycle based link protection (JOPL).....	55
3.6	Non-joint optimization algorithm of p -cycle based link protection (NJOPL)	57
3.7	Efficiency ratio based unity- p -cycle heuristic algorithm (ERH)	59
3.8	Dynamic p -cycle (DpC) algorithm.....	64
3.9	Link protecting p -cycle based protected working capacity envelope (PWCE) algorithm.....	67
3.10	Hybrid DpC and PWCE algorithm.....	70
3.11	Performance Evaluation for static traffic protection	74
3.12	Performance Evaluation for dynamic traffic protection.....	85
3.13	Conclusions	98
Chapter 4.	Tree-Protecting p -Cycle Based Multicast Protection Approach.....	99
4.1	Introduction	99
4.2	Additional notations	101
4.3	Protection mechanism of the tree-protecting p -cycle based approach.....	101
4.4	Spare capacity optimization algorithm of p -cycle based tree protection (SOPT)...	105
4.5	Efficiency score based heuristic algorithm of p -cycle based tree protection (ESHT)	108
4.5.1	ESHT for static traffic protection	108
4.5.2	The matrix algorithm for identification of the disjoint tree sets	110

4.5.3	The p -cycle reconfiguration process in ESHT algorithm for dynamic multicast traffic	112
4.6	Optimal path pair (OPP) based approach.....	114
4.6.1	Integer linear programming based optimal path pair algorithm (ILP-OPP)....	116
4.6.2	The OPP-SDP heuristic algorithm and the OPP-SDS heuristic algorithm.....	119
4.7	Performance evaluation for static traffic protection.....	121
4.8	Performance evaluation for dynamic traffic protection	128
4.9	Conclusions	131
Chapter 5.	Node-and-Link Protecting p -Cycle Based Multicast Protection Approach.....	132
5.1	Introduction	132
5.2	Additional notations	133
5.3	Protection mechanism of the node-and-link protecting p -cycle based approach....	133
5.4	Spare capacity optimization algorithm of the node-and-link protecting p -cycle (SOPN)	137
5.5	Efficiency score based heuristic algorithm of the node-and-link protecting p -cycle (ESHN).....	138
5.6	Performance evaluation for static traffic protection.....	142
5.7	Performance evaluation for dynamic traffic protection	150
5.8	Conclusions	156
Chapter 6.	Conclusions and Future Work	158
6.1	Conclusions	158
6.2	Suggestions for future work	161
References.....		164
Author's Publications.....		180

List of Figures

Figure 1-1: Causes of on-land fiber cable cuts for service breakdown [26].....	3
Figure 1-2: Average service restoration time and cable repair time [26]	4
Figure 2-1: General classification of physical layer resilience approaches.....	12
Figure 2-2: General classification of optical layer resilience approaches	13
Figure 2-3: Optical layer unicast protection approaches	18
Figure 2-4: The link protecting p -cycle concept.....	26
Figure 2-5: Illustration of the concept of protected working capacity envelope (PWCE)	27
Figure 2-6: Three multicast models in a WDM multicast network: (a) MSW; (b) MSDW; (c) MAW [174].....	32
Figure 2-7: Splitter-and-delivery (SAD) switch [170].....	34
Figure 2-8: An VWP-OXC architecture employing SAD switch [170].....	35
Figure 2-9: A simple example illustrating the link-disjoint tree (LDT) protection approach (a) a pair of link-disjoint trees (b) link failure recovery mechanism.....	41
Figure 2-10: Capacity efficiency comparison for static multicast traffic protection for link failure recovery in COST239 network.....	46
Figure 2-11: Comparison of blocking performance for dynamic traffic in COST239 network: (a) the offered network traffic is fixed at 55 Erlang, and (b) the multicast group size is fixed at 5.....	47
Figure 3-1: A simple example illustrating the link protecting p -cycle based approach	53
Figure 3-2: Flow chart of the efficiency ratio (ER) based unity- p -cycle heuristic algorithm..	61
Figure 3-3: A simple network topology containing 6 p -cycles.....	62
Figure 3-4: (a) Initial working units of all the multicast trees on each link, (b) remaining working units on each link.....	63
Figure 3-5: Flow chart of the Dynamic p -Cycle (DpC) algorithm for dynamic provisioning of multicast traffic	65
Figure 3-6: Illustration of the protected working capacity envelope and the spare capacity reserved for p -cycles for the simple network topology shown in Figure 3-3	70
Figure 3-7: Partitioning the total deployed capacity into DpC and PWCE sub-layers.....	71
Figure 3-8: Flow chart of the H- DpC -PWCE algorithm	73
Figure 3-9: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network	75
Figure 3-10: Capacity comparison of optimized designs in COST239 network	78
Figure 3-11: Capacity comparison of optimized designs in NSFNET network	78
Figure 3-12: Capacity comparison of optimized designs in US backbone network.....	79
Figure 3-13: Capacity comparison of the SOPL and the ERH in COST239 network.....	80
Figure 3-14: Capacity comparison of the SOPL and the ERH in NSFNET network.....	81
Figure 3-15: Capacity comparison of the SOPL and the ERH in US backbone network	81
Figure 3-16: Comparison of total capacity required by SOPL in three networks	82
Figure 3-17: Comparison of total capacity required by ERH in three networks	83

Figure 3-18: Effects of the shape factor and the hop limit on the blocking probability of p -cycle based PWCE in the NSFNET network.....	89
Figure 3-19: Effects of the hop limit on the blocking probability in p -cycle based multicast protection algorithms in the COST239 network (Offered traffic is fixed at 55E and γ is fixed at 4): (a) the p -cycle based PWCE, and (b) the dynamic p -cycle (DpC).....	90
Figure 3-20: Comparison of blocking performance for various protection algorithms in the COST239 network: (a) the offered network traffic is fixed at 55 Erlang, and (b) the multicast group size is fixed at 5.	92
Figure 3-21: Comparison of blocking performance for various protection algorithms in the NSFNET network: (a) the offered network traffic is fixed at 28 Erlang, (b) the multicast group size is fixed at 5.	93
Figure 3-22: Comparison of blocking performance in the COST239 network for the unicast traffic case.....	96
Figure 4-1: An example illustrating the tree-protecting p -cycle approach.....	102
Figure 4-2: A simple example of the tree partition algorithm (TPA).....	105
Figure 4-3: Flow chart of the p -cycle reconfiguration process in the ESHT algorithm for dynamic multicast traffic	113
Figure 4-4: An example illustrating the OPP based protection approach.....	115
Figure 4-5: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network	122
Figure 4-6: Capacity efficiency comparison for static multicast traffic protection for combined node and link failure recovery: (a) in COST239 network; (b) in NSFNET network; (c) in US backbone network.	127
Figure 4-7: Blocking performance comparison in COST239 network for dynamic multicast traffic protection: (a) offered traffic is fixed at 55 Erlang, (b) the multicast group size (k) is fixed at 5.	129
Figure 5-1: Illustration of the node-and-link protecting p -cycle approach: (a) a cycle and a tree; (b) link failure recovery; (c) node failure recovery.	134
Figure 5-2: An example illustrating that the no. of copies required for a particular cycle should satisfy the largest node-failure-specific simultaneous use	136
Figure 5-3: Flow chart of the ESHN algorithm for dynamic multicast traffic	140
Figure 5-4: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network	143
Figure 5-5: Total capacity comparison for static multicast traffic protection: ILP algorithms (solid traces) vs. heuristic algorithms (dash traces): (a) in the COST239 network; (b) in the NSFNET network; (c) in the US backbone network.	148
Figure 5-6: Multicast traffic parameter r vs. multicast percentage R with different average multicast group size $E(x)$	152
Figure 5-7: Blocking performance comparison in COST239 network for dynamic multicast traffic protection (the average multicast group size $E(x)$ is 5): (a) r is fixed at 0.6, (b) the network offered traffic load $\lambda\mu$ is fixed at 99 Erlang.	153

List of Tables

Table 1-1: World Internet usage and population statistics (Source: Internet World Statistics (June 30, 2008) [1].....	1
Table 1-2: Internet traffic trends [25]	2
Table 3-1: Identified p -cycles in the simple network topology shown in Figure 3-1	62
Table 3-2: Test multicast sessions	62
Table 3-3: The ER of all the identified unity- p -cycles in Table 3-1	63
Table 3-4: The set of p -cycles chosen by the ERH algorithm	64
Table 3-5: Number of copies required for each unity- p -cycle in PWCE algorithm	69
Table 3-6: Comparison of the ALPWP in COST239 network (k is the multicast group size)	76
Table 3-7: Comparison of the average total computational time for setting up a multicast session in COST239 network ($k=5$)	84
Table 3-8: Comparison of the number of variables and constraints in different ILP formulations	84
Table 3-9: Effects of the shape factor (γ) and the hop limit (H) of p -cycles on the total provisioned working capacity in the p -cycle based PWCE in the COST239 network.....	88
Table 3-10: Effects of the shape factor (γ) and the hop limit (H) of p -cycles on the total provisioned working capacity in the p -cycle based PWCE in the NSFNET network.....	88
Table 3-11: Comparison of the average total computational time per multicast session for different multicast protection schemes in the COST239 network. (The offered network traffic $\lambda\mu$ is fixed at 55 Erlang, and the multicast group size k is fixed at 5.)	97
Table 4-1: The primary-backup path pairs for Φ_l ($\Phi_l = \{8,1,3,4,9\}$)	114
Table 4-2: The final configured primary and backup links for Φ_l ($\Phi_l = \{8,1,3,4,9\}$)	114
Table 4-3: Average splitting frequency (SF) in the COST239 network.....	121
Table 4-4: Total capacity comparison required by 20 random multicast sessions for link failure recovery (LR) and those for combined node and link recovery (CNLR) in COST239 network ($k=5$).....	123
Table 4-5: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in static traffic environment ($k=5$).....	124
Table 4-6: Comparison of the number of variables and constraints in different ILP algorithms	124
Table 4-7: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in dynamic traffic environment ($k=5$, $\lambda\mu=55$ Erlang)	130
Table 5-1: The cycle hop limit (H) effect on the required total capacity for four p -cycle based algorithms in the COST239 network (multicast group size $k=5$)	144

Table 5-2: Comparison between the average total capacity (TC) required by 20 random multicast sessions for link failure recovery (LR) and those for combined node and link recovery (CNLR) in COST239 network ($k=5$)	144
Table 5-3: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in static traffic environment (multicast group size = 5)	146
Table 5-4: Comparison of the number of variables and constraints in different ILP algorithms	146
Table 5-5: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in dynamic traffic environment ($E(x)=5$, $r=0.6$, $\lambda\mu = 60.5$ Erlang)	155

List of Acronyms

Abbreviations	Full Expressions
ADT	Arc Disjoint Tree
APS	Automatic Protection Switching
APWCE	Adaptive Protected Working Capacity Envelope
ATM	Asynchronous Transfer Mode
AWG	Array Waveguide Grating
BER	Bit Error Rate
BGP	Border Gate Way
BLSR	Bidirectional Line Switched Ring
CO	Central Office
CR-LDP	Constraint-based Routing Label Distribution Protocol
CST	Cross-Sharing Tree
CWDM	Coarse Wavelength Division Multiplexing
DpC	Dynamic p -Cycle
DRS	Disjoint Route Set
DTS	Disjoint Tree Set
DWDM	Dense Wavelength Division Multiplexing
EDFA	Erbium-Doped Fiber Amplifier
ER	Efficiency Ratio
ERH	Efficiency Ratio based unity- p -cycle Heuristic algorithm
ES	Efficiency Score
ESHT	Efficiency Score based Heuristic algorithm of p -cycle based Tree protection
ESHN	Efficiency Score based Heuristic algorithm of Node-and-link protecting p -cycle

FDDI	Fiber Distributed Data Interface
FIPP	Failure-Independent Path Protecting
FOADM	Fixed Optical Add/drop Multiplexer
GMPLS	Generalized Multi Protocol Label Switching
HDTV	High Definition Television
IETF	Internet Engineering Task Force
ILP	Integer Linear Programming
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System
JOPL	Joint Optimization design of p -cycle-based Link protection
LDT	Link Disjoint Tree
LEC	Local Exchange Carriers
MAW	Multicast with Any Wavelength
MCCR	Minimum Cost Collapsed Ring
MC-OXC	Multicast Capable - Optical Cross Connects
MC-ROADM	Multicast Capable - Reconfigurable Optical Add/Drop Multiplexor
MEMS	Micro-Electro-Mechanical Systems
MPLS	Multi-Protocol Label Switching
MRLR	Multiple Ring based Local Restoration
MSDW	Multicast with the Same Destination Wavelength
MST	Minimum Spanning Tree
MSW	Multicast with Same Wavelength
NEPC	Node-Encircling p -Cycles
NJOPL	Non-Joint Optimization design of p -cycle-based Link protection
NP	Nondeterministic Polynomial
OADM	Optical Add/Drop Multiplexer
OBS	Optical Burst Switching

OC	Optical Carrier
ODP	Optimal Diverse Routing
OEO	Optical-Electrical-Optical
OFA	One ring For All multicast sessions
OFO	One ring For One multicast session
OFS	Optical Flow Switching
OIF	Optical Internetworking Forum
OLS	Optical Label Switching
OM-RWA	Optical Multicast Routing and Wavelength Assignment
OPP	Optimal Path Pair
OPP-SDP	Optimal Path Pair - based Shared Disjoint Path
OPP-SDS	Optimal Path Pair - based Shared Disjoint Segment
OPS	Optical Packet Switching
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSPT	Optimal Shortest Path Tree
OXC	Optical Cross Connect
P2P	Peer-to-Peer
PON	Passive Optical Network
PWCE	Protected Working Capacity Envelope
PWLE	Protected Working Light-path Envelope
PXC	Photonic Cross Connect
QoS	Quality of Service
ROADM	Reconfigurable Optical Add/Drop Multiplexer
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RWA	Routing and Wavelength Assignment
SAD	Splitter-And-Delivery

SBPP	Shared Backup Path Protection
SDH	Synchronous Digital Hierarchy
SHR	Self-Healing Ring
SLSP	Short Leap Shared Protection
SONET	Synchronous Optical Network
SOPL	Spare Capacity Optimization of p -cycle-based Link protection
SOPT	Spare Capacity Optimization of p -cycle-based Tree protection
SPA	Shortest Path Algorithm
SST	Self-Sharing Tree
ST	Steiner tree
STS	Synchronous Transport Signal
TaC	Tap-and-Continue
ULSR	Unidirectional Line Switched Ring
VoIP	Voice-over-IP
VoD	Video-on-Demand
VWP-OXC	Virtual Wavelength Path Optical Cross Connect
WDM	Wavelength Division Multiplexing
WI-OXC	Wavelength Interchanging - Optical Cross Connect
WP-OXC	Wavelength Path - Optical Cross Connect
WS-OXC	Wavelength Selective - Optical Cross Connect
WSS	Wavelength Selective Switches

Chapter 1. Introduction

1.1 Background and motivation

In the 21st century, people's work and life has been greatly influenced by network technology. Our daily life now becomes very dependent on the networks. Without networks, our life and the world would have been a totally different way today. The Internet, the global network of networks, connects millions of private and public, academic, business, and government networks, enabling users to share information along multiple channels. World Internet usage and population statistics, shown in **Table 1-1**, show that the world internet population has been tripling each year since year 2000 [1]. More and more people around the world are connected by the Internet, generating exponentially increasing demand and therefore rapidly increasing network traffic.

Table 1-1: World Internet usage and population statistics (Source: Internet World Statistics (June 30, 2008) [1])

World regions	Internet Users	% Population	Usage growth 2000-2008
Africa	51,065,630	5.3 %	1,031.2 %
Asia	578,538,257	15.3 %	406.1 %
Europe	384,633,765	48.1 %	266.0 %
Middle east	41,939,200	21.3 %	1,176.8 %
North America	248,241,969	73.6 %	129.6 %
Latin America/Caribbean	139,009,209	24.1 %	669.3 %
Oceania / Australia	20,204,331	59.5 %	165.1 %
World total	1,463,632,361	21.9 %	305.5 %

In the past, people sent emails, chatted using web messengers and surf webpage, with plain text as the dominant content. As the technology advances, these plain-text dominated services have been upgraded to multimedia dominated. For instance, lots of emails are sent with large sized attachments of images, sound or video clips. Besides, people can talk and see each other over the Internet (e.g., voice-over-IP (VoIP) [2], video call [3]). They may also share

their photos or videos in either public websites or their own blogs [4]. Besides those conventional network applications, some other novel network applications ranging from, video-on-demand (VoD) [5, 6], video conferencing [7], E-learning [8, 9], HDTV [10], online virtual community [11], online gaming [12], peer-to-peer (P2P) services [13, 14], Internet banking [13-15], online stock exchange [16], online auctions [17], web search engine [18, 19], file sharing [20], web shopping [21-23], telemedicine [24] and so on, are becoming pervasive as well. However, those emerging multimedia dominated applications will rapidly increase the bandwidth demand of the supporting networks.

Because of the exponentially increasing user-demand for these broadband services due to the need for business, entertainment, information, communication, and so on, network traffic has been increasing drastically over the last two decades, as shown in **Table 1-2** [25]. Wall street journal (June 16, 2008) reported that, Cisco projected a six-fold jump in Internet traffic between 2008 and 2012, as online multimedia has been growing rapidly and becomes the biggest driver of global data communications.

Table 1-2: Internet traffic trends [25]

Trend	Doubling Period
Maximum Internet trunk speed in service	22 months
Internet traffic growth 1969-1982	21 months
Internet traffic growth 1983-1997	9 months
Internet traffic growth 1997-2008	6 months
Internet router/switch max speed until 1997	22 months
Internet router/switch max speed after 1997	6 months

Meanwhile, with recent advancement in optical transmission technology and optical networking technology, the underlying optical WDM networks are able to offer huge bandwidth and process huge amount of data, in order to support exponentially increasing network traffic. However, with such high capacity demand and heavy dependence on optical

WDM networks, any network failure would lead to severe disruption to network services and calamitous loss to both end users and network operators.

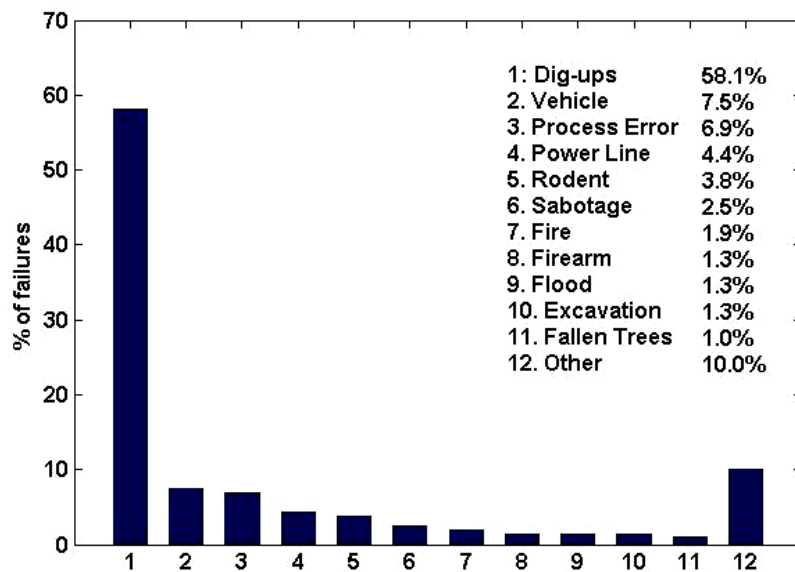


Figure 1-1: Causes of on-land fiber cable cuts for service breakdown [26]

In WDM networks, network failures consist of channel failures, link failures and node failures [27]. Channel failures are caused by the failure of some equipment related to particular channels, such as transmitter or receiver faults. However, channel failures are less frequent and easier to locate and repair. Network links are vulnerable to both human errors and natural hazards, because optical cables expand over long distance through various kinds of geographical areas, such as mountains and oceans. In addition, they are also difficult and costly to monitor and maintain. As a result, link failures are the predominant failures in optical networks. In contrast, node failures are unusual but more severe. A single node failure is logically equivalent to several concurrent link failures. A comprehensive survey, whose results are shown in **Figure 1-1**, carried out by the National Engineering Consortium of USA showed that the major cause of the on-land fiber cable cuts is dig-up [26]. Most of the dig-ups are caused by construction procedure errors in sign placement, road grading/trenching, etc.

For undersea cables, the damages are mainly caused by water leakage, shark bites, ship anchors and earthquakes.

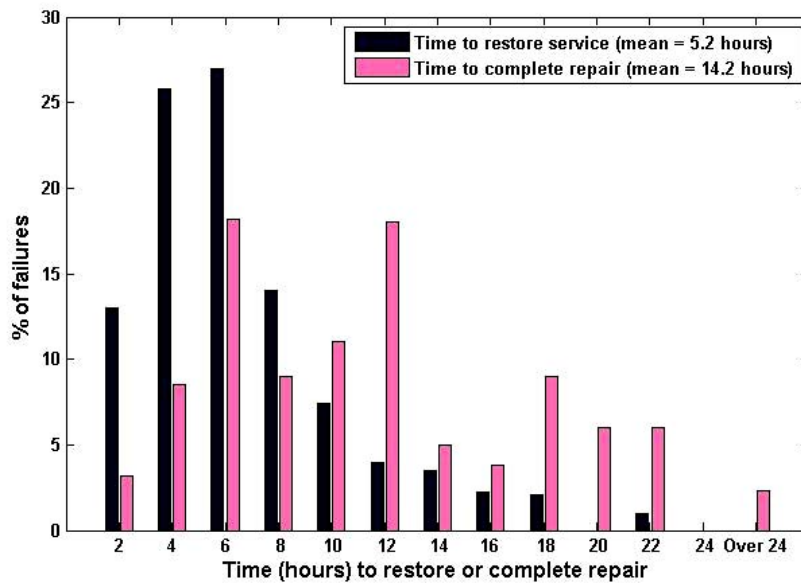


Figure 1-2: Average service restoration time and cable repair time [26]

For metropolitan networks, the average fiber cable cut frequency is 13 cuts/year for 1000 miles; while for long-haul networks, it is about 3 cuts/year for 1000 miles [27]. This implies, for a network with total installed optical cable length of 100,000 miles, it experience 0.822 – 3.562 cuts/day. The average service restoration time and cable repair time are shown in **Figure 1-2**. An average time of 5.2 hours is required for manual service restoration for a network without any protection/restoration schemes; while the average complete cable repair time is 14.2 hours. As such, optical network service outage would cause tremendous revenue loss and service disruption. If the mean restoration time of 5.2 hours is applied, the data loss for 1 Tb/s WDM optical link would be accumulated to 18720 Tb. As direct revenue loss caused by a major optical link is often quoted above US \$ 100,000/minute [27, 28], for a mean 5.2 hours restoration time, the total loss is about US \$ 31.2 million.

These may serve as a warning to us, but they may also serve as a strong motivation to research on network survivability, such as developing fast and efficient protection approaches.

As network traffic mainly consists of unicast traffic and multicast traffic, network survivability is crucial to both unicast and multicast traffic in WDM networks. Nevertheless, multicast traffic suffers even more in a network failure. If a link/node in a multicast session fails, the traffic to all the downstream destinations along the failed link/node would be affected. The closer the link is to the source node, the more destinations would be affected. In the past, extensive research has been directed to unicast traffic protection, due to the predominance of unicast traffic. Recently, due to the rapid growth of multicast applications, such as video-conferencing, high definition television (HDTV), distance learning and multi-player on-line gaming, the problem of multicast traffic protection has started to draw more research interests.

Most of current optical multicast protection approaches may be classified into four major categories: (i) tree-based protection approaches; (ii) ring-based protection approaches; (iii) path-based protection approaches; (iv) segment-based protection approaches. A detailed literature review of the above protection approaches is presented in Chapter 2. Among all the approaches, tree-based protection approaches are most-straightforward, but they were shown to be less efficient, and not suitable for sparse networks. Ring approaches are fast in recovery but the drawback is the inefficiency of resource utilization. Path/segment based approaches are famous for their efficient resource utilization, but they are slow in failure recovery. In path/segment based approaches, the complicated spare capacity sharing and complex restoration process makes the provisioning process too complicated, which is not desired by most network operators. Thus, considerable efforts are required to propose novel multicast protection approaches, which are both cost-effective and fast in recovery speed.

1.2 Objectives

Hence, my research has been focused on developing multicast traffic protection approaches for optical multicast traffic with simpler operation mechanism and faster failure recovery speed, while maintaining comparable capacity efficiency or even to achieve better capacity efficiency. Among most unicast traffic protection approaches, the preconfigured protection cycle (p -cycle) methods offer both fast speed in restoration (because p -cycles are pre-cross-connected) and high efficiency in resource utilization (because p -cycles protect both on-cycle and straddling links). So far, p -cycles based protection approaches have been intensively studied for unicast traffic protection, but have not been investigated for multicast traffic yet, to our best knowledge.

Thus, the objectives of my research are to study and research on p -cycle based approaches, in terms of protection mechanism, optimized integer linear programming (ILP) algorithms and heuristic algorithms to realize each approach, and investigating their effectiveness (e.g., capacity efficiency, blocking probability, etc) for optical multicast traffic protection in optical mesh WDM networks:

Firstly, to investigate and evaluate the link-protecting p -cycle based approach for multicast traffic protection against link failure recovery, in the context of both static multicast traffic and dynamic multicast traffic.

Secondly, to develop more advanced p -cycle based approaches, which are capable of handling combined node and link failure recovery, in the context of both static multicast traffic and dynamic multicast traffic.

1.3 Major contribution of the thesis

The original contributions of this thesis are listed as follows:

- The ILP-based spare capacity optimization of p -cycle based link protection algorithm (SOPL) and efficiency ratio based heuristic algorithm of link-protecting unity- p -cycle design (ERH) are applied to static multicast traffic protection against single link failure first. Results show that the SOPL outperforms the existing multicast protection algorithms for capacity efficiency. The performance of the ERH is close to that of the SOPL, but the ERH is much faster than the SOPL. (Chapter 3)
- In order to achieve the least total capacity consumption, a joint optimization algorithm of p -cycle-based link protection (JOPL), and a non-joint optimization algorithm (NJOPL) are proposed. The JOPL design minimizes the total capacity used for setting up the multicast trees and configuring the p -cycles simultaneously, instead of optimizing the spare capacity only as in the SOPL. The JOPL is superior to the SOPL and the NJOPL, for link failure recovery of static multicast traffic. (Chapter 3)
- For dynamic multicast traffic protection against single link failure, the performance of dynamic p -cycle (DpC) algorithm and p -cycle based protected working capacity envelope (PWCE) algorithm is evaluated first. Compared with the existing multicast protection algorithms, the dynamic p -cycle algorithm achieves the lowest blocking probability, whereas the p -cycle based PWCE algorithm offers the fastest computational speed. (Chapter 3)
- In order to combine the merits of the above two algorithms, a hybrid dynamic p -cycle and protected working capacity envelope (H-DpC-PWCE) algorithm is also proposed for multicast traffic protection, for the benefits of differentiating the multicast requests with different priorities. (Chapter 3)

- As link-protecting p -cycle based approach is not capable of the node failure recovery, this thesis extends the p -cycle concept to tree protection of optical multicast traffic for combined node and link failure recovery. Tree protecting p -cycles protect the multiple mutually disjoint trees (or sub-trees) on end-to-end basis. In this approach, a p -cycle can be shared by multiple mutually disjoint trees. The capacity efficiency of the ILP-based spare capacity optimization of p -cycle based tree protection algorithm (SOPT) is close to that of the optimal path pair based approach. However, the tree-protecting p -cycle based approach provides faster recovery speed, because p -cycles are pre-configured, and only the end nodes of trees (or sub-trees) handle the protection switching. (Chapter 4)
- Since the ILP based algorithm is not scalable to large networks with a large number of multicast sessions, an efficiency score based heuristic algorithm of p -cycle based tree protection (ESHT) is proposed later. Its capacity efficiency is close to that of the SOPT, while offering faster computational speed and can be applied to dynamic multicast traffic protection for combined node and link failure recovery. (Chapter 4)
- To further improve the performance of p -cycles for optical multicast traffic protection, the node-and-link protecting p -cycle based approach for optical multicast traffic protection is investigated in this thesis. The node-and-link protecting p -cycles protect all individual nodes and links, so as to achieve combined node and link failure recovery for multicast trees. The p -cycles are shared by nodes or links. For link failure recovery, the end nodes of the link are responsible for protection switching. For node failure recovery, one of the upstream nodes and one level of the downstream nodes are responsible for the protection switching. If all the nodes and links of all multicast trees are protected, these multicast trees are protected for combined node and link

failure recovery. Among all algorithms, the SOPN achieves the best capacity efficiency in static traffic. (Chapter 4)

- Since the ILP based algorithm is not scalable to large networks with a large number of multicast sessions, an efficiency score based heuristic algorithm of node-and-link protecting p -cycle algorithm (ESHN) is proposed to provide faster computational speed and to be applied to dynamic traffic protection, while retaining the efficiency performance close to that of the SOPN. In the conducted dynamic traffic simulations, the ESHN outperforms the rest of the algorithms. (Chapter 5)
- Finally, a detailed performance evaluation of both the static and dynamic multicast traffic protection for combined node and link failure recovery is provided in this thesis. (Chapter 5)

1.4 Organization of the thesis

This thesis is organized into seven chapters.

Chapter 1 gives a brief introduction on the motivations, objectives, and major contributions of the work presented in the thesis and the organization of the thesis as well.

Chapter 2 reviews the current state of the research work on network resilience techniques in different layers first. The current research work on unicast/multicast traffic protection approaches in optical WDM networks is classified and reviewed for advantages and disadvantages in detail. Special focus is given to the p -cycle based approaches, which have been extensively studied for unicast traffic protection, but have not been investigated for multicast traffic protection yet.

Chapter 3 presents the link-protecting p -cycle based optical multicast traffic protection approach for link failure recovery. Some efficient link-protecting p -cycle based protection algorithms earlier reported for unicast traffic protection are applied for multicast traffic protection. Some other novel link-protecting p -cycle based protection algorithms are also proposed and compared with the existing multicast protection algorithms.

Chapter 4 presents the tree-protecting p -cycle based optical multicast traffic protection approach for combined node and link failure recovery, extending the p -cycle concept to multicast tree protection. Compared with the link-protecting p -cycle based approach, the key advantage of the proposed tree-protecting p -cycle based optical multicast protection approach is the node failure recovery. The novel algorithms proposed are compared with the existing multicast protection algorithms.

Chapter 5 presents the node-and-link p -cycle based optical multicast traffic protection approach for combined node and link failure recovery. The novel algorithms proposed are compared with the existing multicast protection algorithms. The node-and-link p -cycle based optical multicast traffic protection approach is shown to outperform the current existing protection approaches.

Finally, Chapter 6 summarizes the work in this thesis and provides suggestions for the future research.

Chapter 2. Literature Review

2.1 Introduction

This chapter reviews the current state of the research work in network resilience techniques for different layers, with special focus on optical layer protection approaches. Special focus is devoted to the p -cycle based approaches, which have been extensively studied for unicast traffic protection, but have not been investigated for multicast traffic protection yet. The optical multicast technologies and optical multicast protection approaches in optical WDM mesh networks are also discussed in details. The advantages and disadvantages of the existing optical multicast protection approaches are also compared..

This chapter is organized as follows. Section 2.1 gives the overview. Section 2.2 describes the network resilience approaches in different layers. Section 2.3 reviews the optical unicast traffic protection approaches. Section 2.4 discusses the p -cycle based protection approaches for optical unicast traffic. Section 2.5 reviews the optical multicast technologies. Section 2.6 reviews the current state of the research on optical multicast protection approaches.

2.2 Network resilience approaches in different layers

According to the layered network model, network resilience approaches can be classified into four categories: (i) physical layer resilience approaches; (ii) optical layer resilience approaches; (iii) IP logical layer resilience approaches; (iv) multi-layer resilience approaches. Thus, this subsection briefly reviews resilience approaches in different layers.

2.2.1 Physical layer resilience approaches

As shown in **Figure 2-1**, survivability techniques in the physical layer focus on encasement and diversity [27]. In order to reduce the chances of cable cuts, fiber cables are buried deep into the ground. Cable pressurization provides a way to detect the cable break due to the sharp drop of the pressure. However, in order to prevent seepage of water, undersea cables are gel-filled instead of air pressurized.

Another possible way to survive from optical network failures is to duplicate every transmission path. The concept of “red and white” network proposed by T. Sawyer in mid-1990s is to duplicate every component in the network and mark the working components and backup components as “red” and “white”, respectively [27]. A network rule is to ensure that “red” and “white” components are physically apart, in order to prevent “working and backup”-concurrent-failures. Network node failures, such as equipments faults, can also be recovered by redundant design, such as duplication of node equipments.

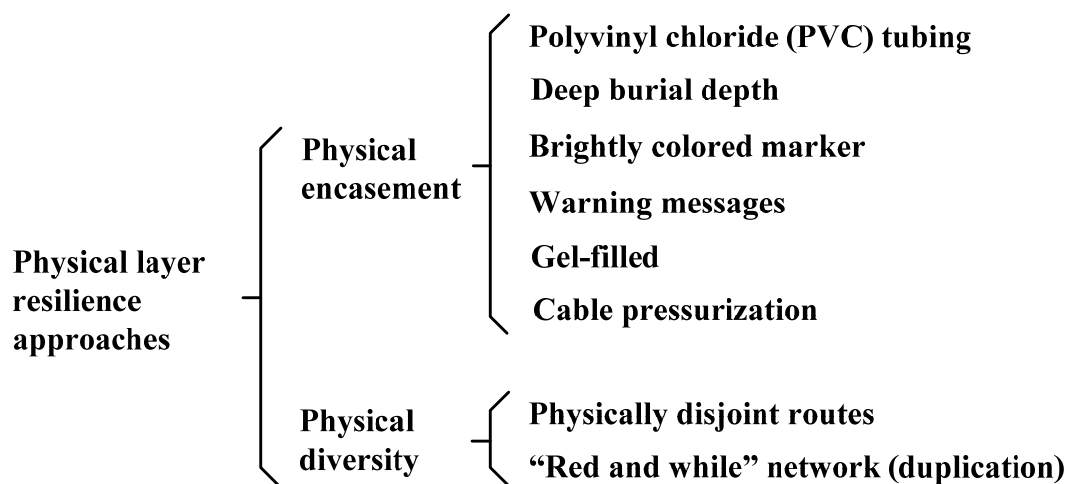


Figure 2-1: General classification of physical layer resilience approaches

Physical layer resilience approaches only serve as the primary guards (or precautionary measures) against physical damages to the telecommunication networks. Higher layer services after network failures cannot be recovered by the physical layer resilience approaches. As a result, survivability schemes at higher layers are compulsory for guaranteeing good network performance.

2.2.2 Optical layer resilience approaches

As shown in **Figure 2-2**, optical layer resilience approaches mainly consist of protection approaches and restoration approaches [27, 29, 30]. Protection approaches [31] are proactive, in which, protection routes are pre-identified and corresponding network resources are reserved in advance of network failures; while restoration approaches [32] are reactive, in which, restoration routes are identified adaptively based on the state of network at the time of failure.

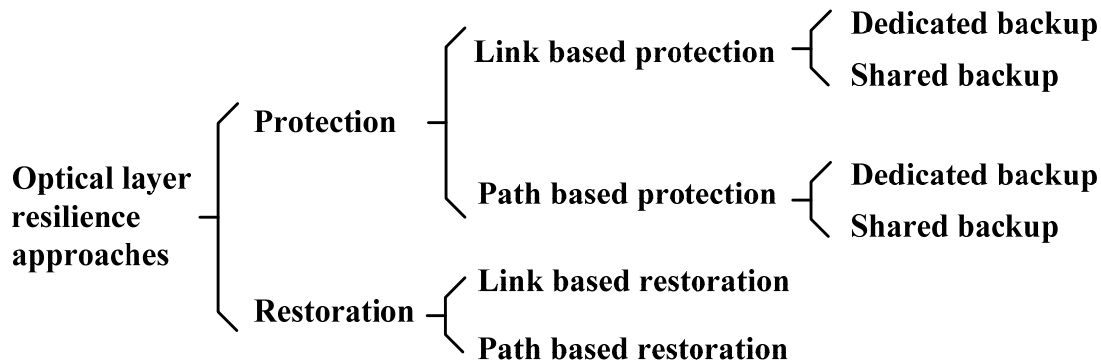


Figure 2-2: General classification of optical layer resilience approaches

Protection approaches are faster in recovery speed (because protection routes are pre-identified and corresponding network resources are reserved in advance of network failures) and can guarantee full recovery, but they may not be efficient in resource utilization; whereas

the restoration approaches may outperform in network resource usage efficiency and flexibility, but they are slow in recovery speed (because restoration routes are identified adaptively based on the state of network at the time of failure).

In dynamic restoration, no spare network resources are reserved during normal operation. The network dynamically searches for the spare network resources available to recover the disrupted network services after a network failure occurs. However, it is slow because of spare network resources searching time and configuration time of the recovery paths. Moreover, full service recovery is not guaranteed, because the network may not have sufficient spare resources at the time of the network failure.

For network designs, there is a trade-off between service recovery time and resource utilization efficiency. A general criterion is to choose the resilience approach based on the most important requirements. In addition, another better proposal is to use a combined strategy, in which, a protection approach serves as primary guard to guarantee fast recovery speed, while a restoration approach can be used as the auxiliary method to increase resource utilization efficiency.

Based on the protection range, resilience approaches in the optical layer can be further classified into link based protection/restoration approaches and path/segment based protection/restoration approaches [33, 34]. Link based approaches are relatively simpler and faster than path based approaches, because only the end nodes of the failed link perform the switching. In contrast, in path/segment based approaches, end nodes of the paths/segments take actions. In general, path based approaches may achieve a better network resource utilization, but they are slow in service recovery [27, 32, 35].

Based on the resource reservation, protection approaches are divided into two categories: (i) dedicated backup approaches; (ii) shared backup approaches. In dedicated backup approaches, also called the “1+1” protection approaches, system resource reserved for a primary light path

cannot be shared by other primary light paths; whereas in shared backup approaches, the resource utilization is more efficient due to the system resource sharing. However, shared protection approaches are not capable of handling multiple concurrent failures sharing the common reserved spare resources.

Another classification is based on the failure independence. In the failure dependent approaches, the backup path is allowed to utilize links/nodes of the primary path except the failed link/node [27, 36]. On one hand, failure dependent approaches are more efficient than failure independent schemes. On the other hand, they are more difficult to implement, because of the complicated signaling process and extensive computing. In failure independent approaches, the backup path is disjoint with the primary path [27, 36]. Hence, the failure recovery is independent of the exact location of the failure on that path. Failure independent approaches are easier to implement at the expense of more spare capacity required, compared with the failure dependent approaches.

2.2.3 IP logical layer resilience approaches

Compared with physical layer and optical layer resilience approaches, the merit of IP logical layer resilience approaches is the ability of differentiating classes (or priorities) of protection. General logical layer resilience approaches include conventional (Internet protocol) IP approach and IP/ multi protocol label switching (MPLS) approach [37-39].

IP based approaches utilize logical topology reconfiguration to recover from logical IP router failures. In contrast to the optical layer resilience approaches, no spare capacity is reserved during normal operations in IP based approaches. In conventional IP restoration approaches, open shortest path first protocol (OSPF) and border gate way protocol (BGP) are used to update the routing tables network-wide for rerouting after the failure, through advertising messages. However, the signaling and updating processes are relatively slow.

The MPLS is a newly introduced tunneling transmission algorithm, which uses label switching for fast forwarding and routing flexibility. It establishes separate label paths with quality of service (QoS) provision to meet different performance requirements of aggregated traffic flows. The MPLS based protection approach uses a preconfigured backup label switched path (LSP) for local protection or path protection, which is similar to link protection and path protection in the optical layer. The upstream label switched router (LSR) or protection switch LSR (PSL) decides whether data are forwarded along the primary (working) LSP or along the backup LSP. The downstream LSR or protection merge LSR (PML) simply merges both primary and backup LSPs into a single outgoing LSP. Merging avoids the need for protection switching in the PML by simply forwarding data through either the working or the backup LSP, along the outgoing LSP. Multiple LSPs are multiplexed into a single composite LSP by label stacking, in which, another aggregate LSP label is inserted before the label of each individual LSP's label. The MPLS restoration approach is efficient in resource utilization, because no spare network resources are reserved during normal operation. Network resources are consumed by an LSP only when carrying traffic. However, similar as IP restoration, the MPLS rerouting suffers from long convergence time, temporary instabilities and looping.

Generally, logical layer approaches are slow and best effort in nature. Besides, higher layer restoration approaches face the problem of unpredictable physical-to-logical fault multiplication.

2.2.4 Multi-layer resilience approaches

Most multi-layer resilience approaches under research deploy the concept of intelligent optical networking [33, 40, 41] by means of global/local logical topology reconfigurations. Designing multi-layer resilience approaches faces some challenges like inter-layer

coordination, inter-approach coordination, spare capacity allocation and so on. For instance, the problem of making the decision between providing resilience at higher or lower layers, or at several layers together. Is the ordered response better or simultaneous response better? In addition, for well-managed coordination, a resilience mechanism must not violate the requirements of another. Currently, there are mainly three approaches for multilayer survivability schemes under research: (i) uncoordinated approach; (ii) sequential approach; (iii) integrated approach. Despite of the simplicity, the risk of uncoordinated approach is the contention of spare capacity and destructive interference, if parallel recovery actions are triggered [40]. For the sequential approaches, because of the implementation complexity, the bottom-up approach is preferred to the top-down approach. By using either a hold-off timer or interlayer signals, protection/restoration responsibility is transferred from one layer to another layer, if the failure cannot be recovered at the current layer. The hold-off timer method is simple, but the drawback is the inefficiency in some scenarios where the higher layer recovery is delayed even if the lower layer is not capable of handling the service recovery.

The integrated approach requires full knowledge of the states of all the network layers. It is the most flexible approach but also the most complicated approach. Integrated multilayer survivability strategy requires inter-layer signaling to prevent the recovery action in one layer if another layer has already taken protection/restoration actions [40].

2.3 Optical unicast traffic protection approaches

Among the resilience approaches in all the layers, optical layer protection approaches draw the most research interests [42]. Due to the physical-to-logical multiplication problem [37], it is preferred to protect against the physical failure in lower layers, before it expands to several simultaneous logical failures in higher layers. Benefits of providing survivability mechanisms

in the optical layer include fast, efficient service recovery and low implementation complexity. Compared with higher layer resilience approaches, optical layer protection approaches recover fewer and larger blocks of traffic, and leading to easier restoration, especially for fiber cuts [33, 43]. Generally, logical layer approaches are best effort in nature. Higher layer resilience approaches may have to wait alarms from lower layers, for recovery switching. Also, the signaling and updating process of the failure within the same layer is relatively complicated (it is usually required to update the routing tables network-wide for rerouting after the failure, through advertising messages, according to the protocols), compared with optical layer approaches. Besides, higher layer restoration approaches face the problem of unpredictable physical-to-logical fault multiplication. An optical layer failure may manifest itself as multiple faults in logical layers. There are two types of optical network traffic, namely, optical unicast traffic and optical multicast traffic.

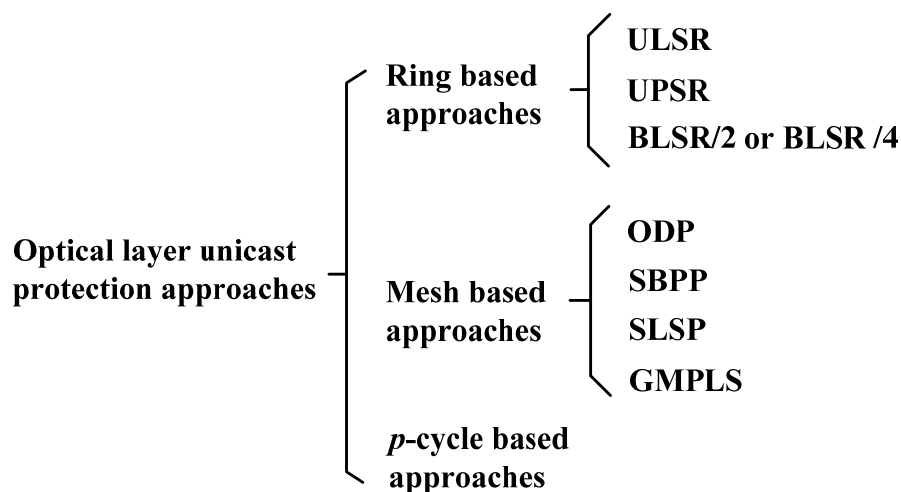


Figure 2-3: Optical layer unicast protection approaches

As shown in **Figure 2-3**, major optical unicast traffic protection approaches include ring based approaches, mesh based approaches and p -cycle based approaches [44], each of which will be discussed later.

2.3.1 Ring based approaches

SONET and SDH networks are generally deployed as a ring topology [45] due to its high degree of network survivability [46]. There are three choices available for ring based protection [47-54]: (i) unidirectional or bidirectional; (ii) line switching or path switching; (iii) two or four fibers in a span. Line switching moves all signal channels of an entire OC-N channel to the protection fiber, whereas path switching moves individual sub-channels within an OC-N channel. The unidirectional line switched ring (ULSR) approach [55-58] deploys a dual ring topology to provide reliability and robustness, in which, the primary ring is used for data transmission, while the secondary ring remains idle during normal operation and is activated in case of failure of primary ring. In the unidirectional path switched ring (UPSR) [59, 60] approach, both fibers carry the identical signals. The destination node continuously compares the quality of each signal and chooses the signal from the protection path in case of severe degradation or loss of the signal in the working path. In the bidirectional line switched ring (BLSR/2 and BLSR/4) [61-64] approach, the shortest path algorithm is implemented.

Because half of the capacity in each fiber is reserved for protection, the redundancy of ring protection approaches is at least 100%. Thus, the drawback of ring protection approaches is the inefficient usage of the expensive bandwidth resources of the network. However, because only the end nodes of the failed link take action, the ring protection approaches is quite fast, less than 50ms. Due to the fast speed, some researchers also have been examining the feasibility and performance of deploying ring protection approaches in the mesh WDM networks [65-68].

2.3.2 Mesh based approaches

Mesh networks, which consist of an arbitrary interconnection pattern, are becoming more and more popular as the backbone choice [69, 70]. As WDM networks are evolving from ring

topologies to mesh topologies, research became active on mesh protection approaches. Several famous mesh protection approaches, such as the shared backup path protection (SBPP) approach [71-75], the optimal diverse routing (ODP) approach [76-78], the short leap shared protection (SLSP) approach, and the generalized multiprotocol label switching (GMPLS) based protection approach were proposed.

Among all the well-known unicast traffic protection approaches, the shared backup path protection (SBPP) approach receives considerable research interests [79]. This approach allows the link-disjoint primary paths to share reserved spare capacity, and thereby achieves high resource efficiency and low blocking probability for dynamic traffic protection [79]. The SBPP approach [79-86] is a kind of failure independent path oriented protection algorithm, so the exact failure location is not important in the SBPP approach. Spare capacity can be shared by mutually failure disjoint (no common failure elements) primary working paths in order to maximize the efficiency. The constraint of disjoint primaries is to ensure that the primaries do not fail simultaneously upon a single failure, so that there is no contention for the common spare capacity simultaneously. The SBPP approach has been intensively studied as the solution to the problem of network survivability under such a dynamic scenario. This is primarily because the SBPP approach can achieve a significant reduction in spare capacity by sharing the spare capacity across multiple failure-independent connections.

However, because resources along the protection paths are shared, cross-connects along the protection paths are not configured at the connection setup; instead they are only configured when a failure actually occurs. This introduces additional delays to signal at the intermediate nodes, thus increasing restoration time significantly compared to those methods where protection paths are pre-configured (pre-fixed) for the intermediate nodes. As a result, similar to other path-oriented approaches, the disadvantage of the SBPP approach is relatively slow service recovery, mainly because of the delay in signaling process and configuration process.

Besides that, because a two-step approach is followed, the performance of the SBPP approach depends on network topology. The SBPP approach is not suitable for network with redundant degree-two nodes, because there are occasions in which the disjoint backup secondary path is not feasible if the shortest route is taken by the primary path.

In contrast to the two step process in the SBPP approach, the ODP approach solves this problem by looking for a pair of disjoint paths concurrently. One of the paths is used for signal transmission, while the other is reserved for backup.

The shared segment protection approach [27, 87-91] (e.g., SLSP approach [92]) protects segments of the paths instead of the whole path. The backup path is only required to be segment-disjoint with the working path rather than fully-disjoint, which improves the resource sharing by relaxing the disjoint requirement at the cost of higher complexity. Single node failure recovery can be recovered by defining overlapping protection domains around the nodes.

The GMPLS approach [93-96], which is an extension of the MPLS logical layer approach in the optical layer, combines the advantages of both MPLS traffic engineering and WDM optical transmission technology [97]. Similar to the automatic protection switching (APS) approach, the GMPLS protection approach also offers 1+1, 1:1, 1:N, M:N options for span protection or path protection [97, 98].

In conclusion, although mesh protection approaches are much more efficient than the ring protection approaches, they also have the limitations of slow service recovery.

2.3.3 Link/path based restoration approaches

The above protection approaches are faster than restoration approaches because the spare capacity is reserved before failures. However, restoration approaches may achieve higher resource utilization efficiency.

Generally, restoration approaches can be divided into two groups: the span restoration approaches and the path restoration approaches [30, 99]. The span restoration approaches [100-102] only look for the restoration paths around the failed link; whereas the path restoration approaches provide service recovery on an end-to-end basis. In the path restoration approaches [103-105], the eligibility of working and restoration paths for all node demand pairs must be considered. All the light paths disrupted by the failure need to be identified and multiple backup paths are required to be produced simultaneously. In the path restoration approaches, service recovery is failure specific/dependent, based on the network state after failures. The restoration path may reuse the survived portions of the failed path by means of stub release or stub reuse. In path restoration approaches with stub release, all the survived portions and the freed capacity become available for restoration process. Path restoration approaches without stub release are like the SBPP approach, but the recovery action is after failure. Stub reuse is a kind of scheme between two extremes: with or without stub release. Path restoration approaches are simplified by using stub reuse, because it is free to choose which survived portion of the failed path to use and which portion to retain. Although stub release/reuse and wider area search make the restoration process more capacity efficient, the actual implementations face some challenges, such as failure location identification and real-time signaling. In general, path restoration approaches are more capacity efficient than span restoration approaches, because restoration is based on a wider region of the network, increasing the alternatives available for optimization.

2.4 *p*-cycle based protection approaches for optical unicast traffic

Two main optical network protection approaches presented above are the ring based approaches and the mesh based approaches. Because only the end nodes of the failed link or

the failed node handle the protection switching, the ring protection approaches offer fast recovery speed (within 50ms) [106]. However, at least half of the capacity is reserved for protection, so the redundancy [27] for ring schemes is at least 100%. Although mesh algorithms offer low redundancy (high efficiency), compared with ring algorithms, they are more complex and slower, because of the signaling, backup paths configuration, and recovery switching.

The preconfigured-cycle (p -cycle) [44], proposed by W.D. Grover in 1998 [106] bridges the ring-mesh dichotomy, combining the rings' simplicity, fast speed in switching, and the meshes' flexibility in routings and efficiency in resource utilization [107]. The original proposal of p -cycle technique is a type of shared link protection approaches for survivable WDM mesh networks. In other words, it is called link-protecting p -cycle based approach. p -cycles, which are closed loop structures, are fully preconfigured at OXCs in the networks. Because p -cycles are formed in the spare capacity of the network [108], the network traffic routing flexibility retains.

The secret behind the achievement of mesh-like efficiency for p -cycle, which is also the most significant and distinguished feature of p -cycles compared to rings, is the protection of straddling links (spans), in addition to on-cycle links (spans). Ref. [107] gives the theoretical substantiation for p -cycles and shows that p -cycles have the same lower bound on redundancy (the ratio of spare capacity to the working capacity [27]) as that of the span-restorable mesh network, namely the well-known limit of $1/(\bar{d}-1)$, (\bar{d} is the average span degree of nodes in the network). The lower bound can be reached if and only if Hamiltonian p -cycles are used [107, 109].

Cycle search is an offline process ahead of any optimization processes [108, 110]. Lots of approaches have been published on identification of p -cycles for a given network. In general, cycles can be identified by four classical approaches [110, 111]: (i) circuit vector space

approach [111]; (ii) backtracking approach [111, 112]; (iii) adjacency matrix approach [111]; (iv) edge-digraph approach [68, 113]. p -cycles can be constructed using either ILP algorithms [114, 115] or heuristic algorithms [116, 117]. One of the heuristic algorithms is to identify cyclic node-disjoint paths pair between two nodes [68]. As the size of the network increases, the number of cycles increases exponentially [110], which makes the algorithm very time-consuming. The straddling link algorithm (SLA) proposed in [110] enumerates a small subset of primary cycles of a network graph first. Operations such as Add and Join in [27], SP-Add, Expand, and Grow in [118] were defined for creating new p -cycles with more straddling span relationships and hence higher efficiency, based on the set of SLA primary cycles. Some other work focuses on enumerating cycles during the ILP optimization [114, 115]. An recursive ILP algorithm is proposed for cycle search in [115]. An improved ILP algorithm is proposed based on flow conservation [114].

Because p -cycle based protection approaches are currently the only protection techniques to enjoy both ring-like speed and mesh-like efficiency [107], they have been drawing more and more research interests. Comprehensive reviews of the p -cycle concept and p -cycle based protection approaches can be found in [27, 44, 119].

In the following three sub-sections, a brief review is presented on the three main types of p -cycle based protection approaches for optical unicast traffic: (i) link-protecting p -cycle based approach; (ii) path/segment-protecting p -cycle based approach; (iii) Node-encircling p -cycle based approach. Lastly, a brief overview of the research on the reliability analysis of p -cycles will be given.

2.4.1 Link-protecting p -cycle based approach

As shown in **Figure 2-4**, link-protecting p -cycles protect any link (span) with both end nodes on the cycle (either an on-cycle link or a straddling link). Similar to other link-oriented

approaches, only the end nodes of the failed link perform the protection switching. Failure detection time, failure localization time, notification time and rerouting time are much shorter than those in path oriented approaches. Also, because p -cycles are preconfigured, the configuration time is eliminated.

Many ILP algorithms and heuristic algorithms [118, 120] were proposed for link failure recovery using link-protecting p -cycles. The ILP optimized designs can be further classified into spare capacity optimized designs [106, 108] and joint optimized designs [121, 122]. Based on the number of concurrent failures to combat, they can be also classified into three categories: (i) single failure recovery algorithms [106, 108, 120]; (ii) double failure recovery algorithms [123-126]; (iii) multiple failure recovery algorithms [127, 128]. Some researchers also work on the problem of shared risk link group (SRLG) protection [129]. In contrast to the conventional p -cycle designs against single network failure, reconfigurable edge-disjoint p -cycle concept was introduced to combat against multiple failures in [130]: one p -cycle can only protect a single on-cycle or straddling link failure; therefore, if the p -cycles are physically disjoint so that multiple link failures happen in such a way where at most one failure on one p -cycle, the p -cycles will be able to protect against such multiple failures. Nevertheless, it is difficult to calculate the probability of failures taking place concurrently. Hence, shorter p -cycles are preferred, because longer p -cycles need more spare capacity and are more vulnerable to network failures [127] (because of more links traversed), although longer p -cycles tend to be more efficient.

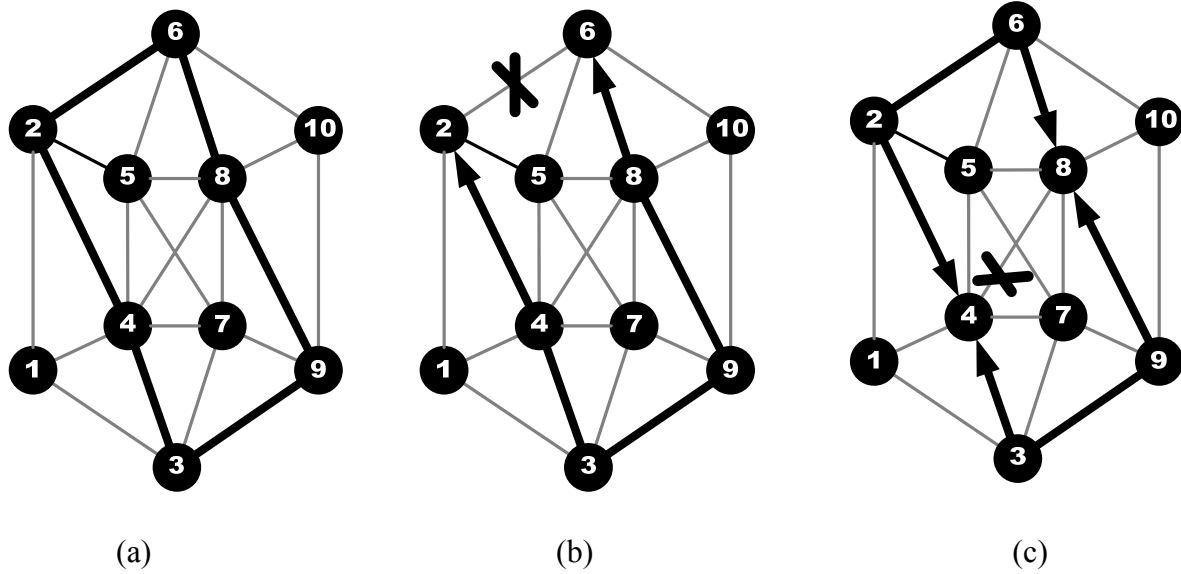


Figure 2-4: The link protecting p -cycle concept

Most of the algorithms reviewed above focus on the static traffic protection. For dynamic traffic, the demands arrive at the network one by one in random manner, without advance information [131]. The p -cycle algorithms for dynamic traffic protection in WDM networks were studied in [131-133]. In [132], three typical p -cycle reconfiguration strategies were presented. Strategy 1 reconfigures all p -cycles upon the arrival of a new request; whereas strategy 2 attempts to reuse the existing p -cycles to protect current demand and add new cycles if required. Results in [132] showed that strategy 1 achieves better blocking performance, while strategy 2 require less computational time. Strategy 3 combines the merits of former 2 strategies and achieves the best blocking performance, which is close to that of the well-known shared backup path protection (SBPP) approach [79]. Compared with SBPP scheme, the advantages of the p -cycle-based protection algorithms lie in its fast restoration speed and simplicity of signaling process [132].

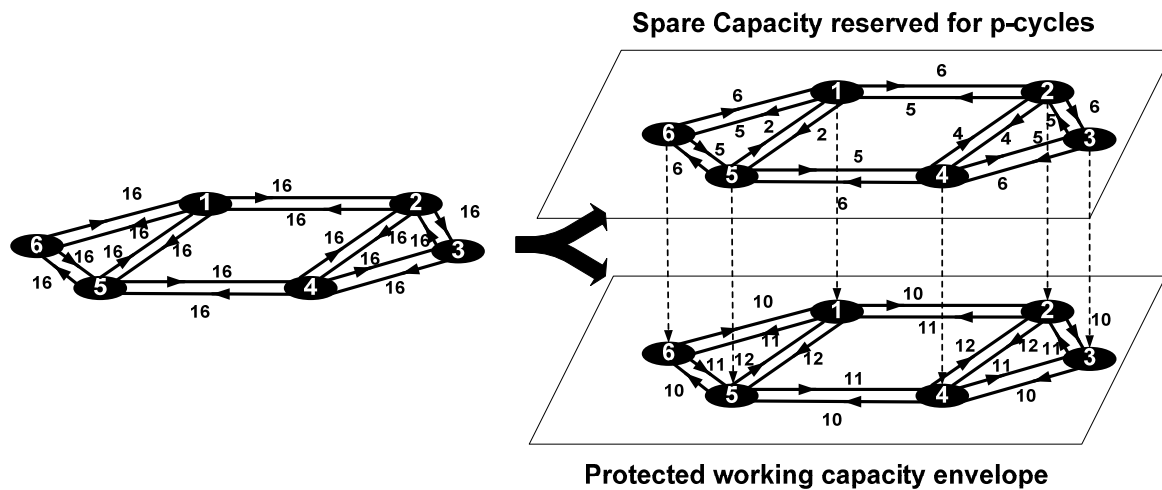


Figure 2-5: Illustration of the concept of protected working capacity envelope (PWCE)

The protected working capacity envelope (PWCE) structure [134] is a milestone in the research of network protection. In the p -cycle based PWCE algorithms proposed in [135, 136], the capacities in the network can be viewed to be partitioned into two sub-layers as shown in the Fig. 2-5. The first step is to reserve some spare capacity on each edge to configure the p -cycles (the right upper sub-layer shown in the Fig. 2-5), in order to form a fixed static optimized envelope of protected working capacities (the right lower sub-layer shown in the Fig. 2-5). The amount of spare capacities reserved on each link are optimized by ILP algorithms [135, 136]. The remaining task is simply to route the dynamic traffic in the preconfigured PWCE. As long as a request can be routed within the preconfigured envelope (lower sub-layer), it is automatically protected, which greatly simplifies network management and reduces the processing complexity.

The fixed PWCE structure performs well in statistically stationary random dynamic traffic, but not in statistically evolutionary traffic [137]. For statistically evolutionary dynamic traffic, a more advanced structure, the adaptive PWCE (APWCE) is proposed in [137], to reconfigure the envelopes to match the actual traffic load pattern, in order to maintain the network blocking performance within an acceptable level. The reconfiguration of the

protected working capacity envelope is either periodically triggered or triggered by alarms of blocking probability measurement.

2.4.2 Path/segment-protecting p -cycle based approaches

Other milestones in the research of p -cycles include the path protecting p -cycle based approach (the failure-independent path protecting (FIPP) p -cycle approach [36] and the protected working light-path envelope (PWLE) approach [138]) and the segment protecting p -cycle based approach (the flow- p -cycle approach [139]). They extended the original link protecting p -cycle concept to path/segment protection. As the names implies, path/segment protecting p -cycles protect path/segment as a whole, instead of protecting each node and link. For link failure recovery, paths/segments have to be mutually disjoint to share the cycle.

There are mainly three strategies for FIPP p -cycle based approach. The first strategy looks for a disjoint route set (DRS) for each candidate cycle in ILP, and then select the most efficient set of cycles by ILP optimization [36]. However, the number of disjoint constraints increases exponentially with the demand. Therefore, the limitation of strategy 1 is the inability of handling large demands.

Instead of forming DRSs for each candidate p -cycle, the second strategy is to generate DRS sets as candidates first and then identify the corresponding most efficient FIPP p -cycles [140]. All possible combinations of DRSs have to be enumerated, strictly for optimization purposes. However, the number of combinations increases exponentially with the demand as well. Hence, an algorithmic approach is proposed in [140] to generate a promising random subset of all DRSs for optimization. Strictly speaking, strategy two is not an optimized design, but it can be called an ILP heuristic algorithm. Although the drawback of strategy two is that its capacity efficiency is inferior to that of the first strategy, it is much faster in computational speed.

The third strategy solves the combination of DRS sets and the selection of the p -cycles concurrently, through ILP joint optimization [141, 142]. The joint optimization strategy provides significant capacity savings, compared with the first two strategies [141]. The limitation of the third strategy is the restriction of the routing: the number of paths for each demand is limited.

Distinct with the PWCE approach which protects link working capacity, the protected working light-path envelope (PWLE) approach [138] protects the light-paths on an end-to-end basis, and was reported to have higher capacity efficiency [138]. However, one of the limitations of the proposed PWLE approach is that the length of light-paths is limited to only 3 physical hops, which is not practical.

Compared with link-protecting p -cycles, path/segment protecting p -cycles can yield significant spare capacity reduction [139] and also provide an inherent means of transit flow protection against node loss.

2.4.3 Node-encircling p -cycle based approach

The concept of node-encircling p -cycle (NEPC) based approach was first introduced in [143] for router failure recovery in the IP layer. A p -cycle is an NEPC for a particular node if it contains all of the node's neighboring nodes (i.e., those nodes connected directly to it with a link) but not the node itself, in order to recover the failure of this node [144]. Upon failure of this particular node, a bidirectional NEPC can provide two backup paths for the affected transiting flow. The cross-layer restoration approach is proposed in [144, 145] to protect against optical layer link failures and IP/MPLS layer router failures using NEPCs.

Three strategies are proposed in [144]. The first strategy looks for a dedicated NEPC for each node, but it is not so cost-effective. It consumes 189% of the spare capacity, compared with the link failure recovery bench mark. In the second strategy, the nodes are able to share

the NEPCs, and a set of link-protecting p -cycles and NEPCs are selected for node failure recovery and link failure recovery respectively, which reduces the spare capacity, compared with the first strategy. In the second strategy, the backup traffic is split evenly on both direction of the NEPCs, whereas in the third strategy, the ILP model can determine which side of the NEPCs the backup traffic would flow, which improves the capacity sharing [144].

The proposal of NEPC based protection approach exploits a new way of node failure recovery. However, it is not so cost-effective to apply the NEPC based protection approach for node failure protection in the optical layer [144].

2.4.4 Availability analysis of p -cycle based protection approaches

The most common aim in designing a survivable network is to achieve restorability against all single link failures, with a minimal investment in spare capacity. This leaves dual-failure situations as the main factor to consider in quantifying how the availability of services benefits from the investment in restorability [146, 147]. Hence, most research publications on availability investigation of p -cycle based protection approaches are mainly based on dual-failure analysis.

The availability (reliability) analysis [148] of link-protecting p -cycles presented in [149, 150] suggests that limiting size of p -cycles allows much higher availability, but at the cost of lower capacity efficiency. The efficiency of p -cycles comes essentially from the protection of straddling spans. However, the more the straddling spans, the lower the service availability. The mean time to failure (MTTF) analysis of link-protecting p -cycles presented in [151-153] showed that although p -cycles are better than traditional protection rings [154] in terms of cost efficiency, the latter surpass the former when the reliability measures are taken into account. Similar to link protecting p -cycles, as the size decreases, FIPP p -cycles tend to be less efficient, but the service unavailability decreases [155]. These results in the literature

suggest that there is a tradeoff between capacity efficiency and availability for network protection design: more spare capacity sharing leads to less unavailability.

2.5 Optical multicast

Unicast is a network method for transmitting information to a single destination, whereas multicast is a network method for the delivery of information to a group of destinations simultaneously, using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the multiple destinations split. The previous sections of this chapter have discussed extensively on optical unicast traffic protection approaches, with special focus on p -cycle based protection approaches. This section and thereafter focus on optical multicast and its protection approaches.

The word "multicast" is typically used to refer to IP multicast [156-159], which is often employed for streaming media and Internet television applications [160, 161]. In IP multicast, the implementation of the multicast occurs on the IP routing level, where routers create optimal distribution paths for data sent to multiple destinations in real-time.

Optical multicast [162-169] is a technique to deliver information to multiple destinations in the optical layer. Optical multicast is realized by light trees [167], which are point-to-multipoint extension of light paths (point-to-point optical connections). The light trees may be implemented by employing multicast capable optical cross connects (MC-OXCs) [164, 170]. Light tree approach is an efficient optical multicast technique, since the same channel (bandwidth) on the tree branches can be shared by multiple destinations [171]. Recently, due to the rapid growth of multicast applications, such as video-on-demand (VoD) [5, 6], video conferencing [7], E-learning [8, 9], HDTV [10], online virtual community [11], online gaming [12], peer-to-peer (P2P) services [172, 173], Internet banking [13-15], online stock exchange [16], online auctions [17], file sharing [20] and so on, the problems of optical

multicast have been drawing strong research interests. The research work on optical multicast can be classified into four categories:

- (1) Optical multicast node structure
- (2) Optical multicast routing and wavelength assignment
- (3) Optical multicast performance modeling and control plane functionality
- (4) Optical multicast protection

The work in each of the first three areas is briefly reviewed below, while a detailed review of the research work belonging to the last category of optical multicast protection is presented in section 2.6.

2.5.1 Optical multicast node architecture (hardware building block)

Optical multicast node architecture is the most important hardware building block to realize optical multicast. Optical multicast can be realized during the OEO conversion at an OXC, creating multiple identical streams only when the links to the multiple destinations split. Optical multicast can be also achieved by just establishing separate light-paths from the source to every destination. To realize a basic multicast connection, a light splitter and some wavelength converters may be needed. A splitter is a passive device used to distribute the input signal to all outputs, providing multicast in the optical domain without buffering.

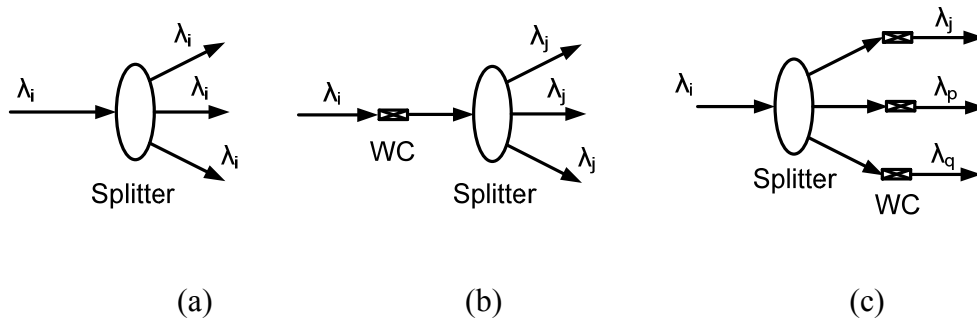


Figure 2-6: Three multicast models in a WDM multicast network: (a) MSW; (b) MSDW; (c) MAW [174]

A light splitter splits a signal on a wavelength to a set of signals on the same wavelength, while a wavelength converter converts a signal on one wavelength to another wavelength. Optical splitters are made of glass and therefore inexpensive; whereas wavelength converters are expensive. Three multicast wavelength conversion architectures are presented in [174], as shown in **Figure 2-6**: (i) the multicast model with same wavelength (MSW); (ii) the multicast model with the same destination wavelength (MSDW); (iii) the multicast model with any wavelength (MAW). The number of wavelength converters needed may vary from one multicast model to another.

In the MSW model, no wavelength converter is required. In the MSDW model, all output signals must use the same wavelength, which may be different from the input wavelength. In the MSDW model, one wavelength converter is needed for each multicast connection, which can be placed just in front of the splitter. The MAW model corresponds to a splitting node with full wavelength conversion (i.e., the incoming signal and the outgoing signals may all use different wavelengths). In the MAW model, the number of wavelength converters needed for each multicast connection is no less than the fan-outs of the multicast connection, since at least one wavelength converter is needed at each output of the splitter. The above discussion suggests that the stronger a multicast model is, the more the number of wavelength converters it may require, and therefore the higher the cost, which implies cost-performance trade-offs.

From the point of view for resource optimization [171], it is more economical to use multicast capable optical cross connects (MC-OXCs) with different degrees of splitting capabilities to eliminate redundant traffic on certain links. The MC-OXC is the key device for optical multicast node and directly affects the performance of the optical multicast services in WDM networks [175-177]. Based on the wavelength conversion capability [174], MC-OXCs can be classified into three categories: (i) without wavelength conversion capability; (ii)

partial wavelength conversion capability; (iii) full wavelength conversion capability. Another useful device is multicast capable – reconfigurable optical add and drop multiplexor (MC-ROADM) [178].

In a WDM network, besides the power splitting and wavelength conversion capabilities, optical switching capability is also required to realize optical multicast. Thus, generally speaking, an MC-OXC consists of two key hardware components: the power splitter and the splitter-and-delivery (SAD) switch [164]. A SAD switch structure is proposed to build MC-OXCs in [170].

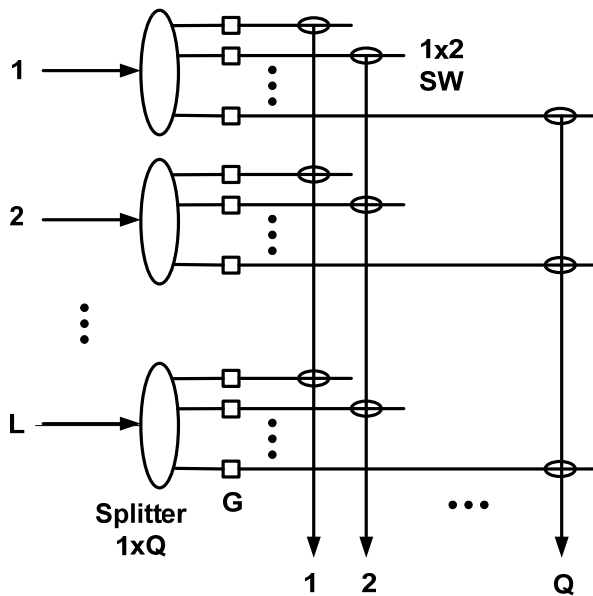


Figure 2-7: Splitter-and-delivery (SAD) switch [170]

Figure 2-7 shows the proposed $L \times Q$ SAD switch structure. An input light-beam is initially split to branches. The optical gate (G) is used to reduce the crosstalk. Each branch is switchable to an associated output port by a 1×2 optical switch (SW). Therefore, any input can be connected to none, one, more or all the output ports. This features a strictly non-blocking property and multicasting capability [170]. The SAD switch can be deployed as a stage of larger OXCs. Three possible structures of OXCs are proposed in [170]: a wavelength

path OXC (WP-OXC) and two virtual wavelength path OXCs (VWP-OXCs), the difference of which depends on the wavelength conversion capability. A WP-OXC is a wavelength selective optical cross connect (WS-OXC), and a VWP-OXC is a wavelength interchanging optical cross connect (WI-OXC). One of the proposed virtual wavelength path VWP-OXC structure in [170] is shown in **Figure 2-8**. It consists of $1 \times M$ splitters, $N \times N$ SAD switches, tunable filters (TFs), wavelength converters (WCs) and $M \times 1$ multiplexers (MUXs). Each of the input links of the SAD switch contains M wavelength channels. Only one is picked out by the tunable filter, subsequently converted to a desired wavelength by the wavelength converter, and finally multiplexed onto the output fiber [170].

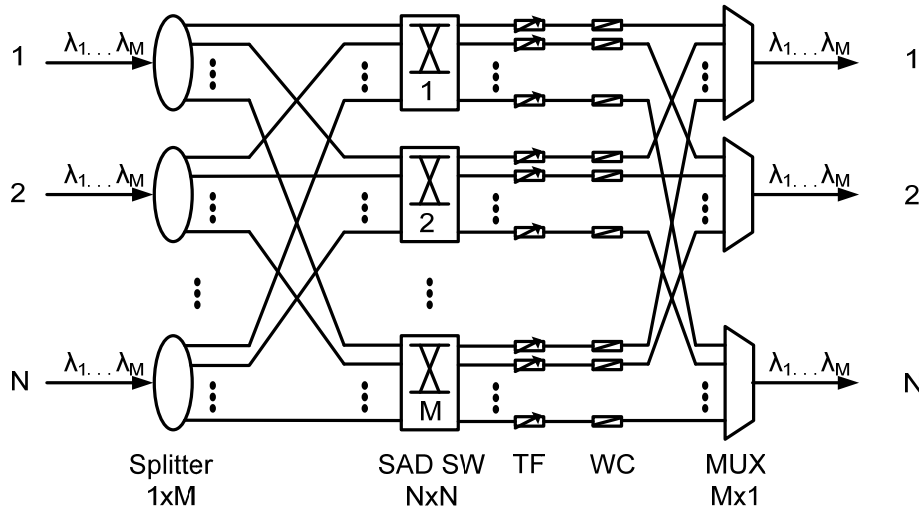


Figure 2-8: An VWP-OXC architecture employing SAD switch [170]

For a signal travelling over a light-tree, the light splitting at MC-OXCs are the main contributors to power loss. The inevitable power loss requires the deployment of amplifiers to compensate for the splitting loss. While the effects of light splitting may be partially mitigated by amplification, incorporating large numbers of optical amplifiers within the hardware components of an MC-OXC to compensate for splitting loss increases the cost and difficulty of fabrication. Besides, optical amplifiers have the serious side-effects of providing gain that is traffic-dependent and generating noise which degrades the bit error rate (BER) of

the connection. Another novel low-cost power budget OXC architecture called Tap-and-Continue (TaC) based on tapping devices is proposed in [179], which is useful for power monitoring. In [180], another novel idea to implement optical multicast operations is proposed by using the optical cross-point switch (OXS), in which, multicast is realized by turning on more than one switch cells in the same column of the OXS.

2.5.2 Optical multicast routing and wavelength assignment (OM-RWA) (algorithmic building block):

Optical multicast routing and wavelength assignment (OM-RWA) is the algorithmic building block to realize optical multicast. Routing unicast connections requires determining a path from the source of the optical signal to its destination. Similarly, routing a multicast connection requires the discovery of a tree rooted at the source which spans all destinations. In addition to determining the route for a connection, a wavelength must be assigned to that connection such that all other connections which share some fiber link with this route are assigned different wavelengths. The problem of optimally assigning wavelengths and routes for a set of multicast connections is referred to as OM-RWA and is NP-complete [179]. Determining a optical multicast tree is often modeled as the Steiner tree problem [171]. However, as Steiner tree routing is an NP hard problem, many OM-RWA algorithms have been proposed [162, 179, 181-184]. In general, OM-RWA algorithms can be classified into two categories: static OM-RWAs and dynamic OM-RWAs.

If the traffic patterns in the network are reasonably well known in advance and any traffic variations take place over a long timescale, the most effective technique for establishing optical connections (light-trees) is by solving a static OM-RWA problem. Since these connections are assumed to remain in place for relatively long period of time, it is worthwhile to optimize the way in which network resources (e.g., physical links and wavelengths) are

assigned to each connection, even though optimization may require considerable computational effort. Typically, routing and wavelength assignment are considered together as an optimization problem using integer linear programming (ILP) formulations. An instance of the static OM-RWA problem with the objective of minimizing the number of wavelengths was considered in [185], and a set of heuristics was presented. In contrast, the objective of the OM-RWA problem formulation in [186] is to maximize the total number of established multicast connections.

The dynamic OM-RWA problem is encountered during the real-time network operation phase. Specifically, users submit requests for light-trees to the network, in some random fashion. The dynamic feature of the multicast connections has many facets [187]. First, the membership of nodes in the multicast group can change during the session lifetime. Secondly, most of the services that require multicast are of dynamic nature by themselves, for example, video, audio or even simple data flows. Hence, the multicast traffic that is carried over the multicast channels to all the group members varies dynamically with time. As a result, this dynamic nature of the multicast is of crucial importance in designing the multicast schedules. As such, features such as session length and destination group size can influence the multicast scheduling technique. Because of the real-time nature of the problem, the OM-RWA algorithms in a dynamic traffic environment must be simple and fast. Since combined routing and wavelength assignment is a hard problem, a typical approach to design efficient algorithms is to decouple the problem into two separate sub-problems: the light-tree routing problem and the wavelength assignment problem. The study in [186] considered the first-fit wavelength allocation policy, in which, wavelengths are considered in a fixed order for each tree. In contrast, the random wavelength assignment was studied in [188]; in addition, multiple classes of requests were considered. A different approach was taken in [189], where an iterative approximation algorithm was developed for completely connected networks

under random wavelength assignment. Since network topologies are not completely connected in general, the results of [189] can be used as lower bounds for more general topologies.

For the networks of full light splitting capability, all nodes are assumed to have ample light splitting capability. Some other research work focus on networks with limited splitting capability [166, 181, 190-193] or limited wavelength conversion capability. In the sparse light splitting networks [194], not all nodes have light splitting capability [195, 196]. In this case, the optical multicast algorithm needs to make full use of the nodes with light splitting capability and avoid those without light splitting capability [165]. A multicast RWA to minimize the number of wavelengths in a WDM network with splitter constraints was studied in [197], while QoS multicast problem with constraint of end-to-end delay was studied in [185]. The problem of multicast routing for dynamic traffic in circuit-switched multi-hop optical networks was studied in [198]. In the absence of converters, a light tree must use the same wavelength on all the links along the branches from source to each destination node (wavelength continuity constraint) [164]. A new class of multi-wavelength multicast wavelength assignment algorithm [195, 196] has been developed based on the multi-wavelength assignment strategy, by allowing multiple available wavelengths in a link to carry the multicast signal. This new multicast wavelength algorithm provides two advantages to the network with limited wavelength conversions, by accommodating more multicast requests and providing good trade-off between wavelength cost and wavelength conversion cost.

2.5.3 Control plane functionality and optical multicast performance modeling

In addition to MC-RWA algorithms, a set of signaling and control protocols must be implemented within the optical network to support the establishment and management of light-trees [164]. The control plane functionality is an important component of an operational

network for supporting the network design objectives and automating the process of light-tree establishment. Currently, a number of standardization activities addressing the control plane aspects of optical networks are underway within the Internet engineering task force (IETF) and the optical Internetworking forum (OIF). Most of these activities take place within the control framework provided by GMPLS. In particular, a number of existing protocols are being extended to support GMPLS and/or to carry network state information relevant to optical networks, including resource reservation protocol - traffic engineering (RSVP-TE), constraint based routing - label distribution protocol (CR-LDP) and routing protocols (open shortest path first (OSPF), intermediate system to intermediate system (IS-IS)). While ongoing work represents an important first step toward seamless integration of Internet and optical network technologies, additional work is required to develop practical control and signaling protocols for the management of multicast connections.

There also has been some work done in modeling the blocking performance of optical multicast using light trees. A path decomposition approach for evaluating the call blocking probability of multicast calls was proposed in [188]. Multicast blocking models for a fully connected network with constraints on the number of hops used for routing were presented in [189], together with the blocking probability analysis for the completely connected WDM switching networks with limited wavelength conversion. Multicast communication in a class of multicast-capable WDM networks with regular topologies under some commonly used routing algorithms was addressed in [199]. The problem of multicast capable node placement in wavelength-routed optical networks was addressed in [200], where this problem was motivated by the expected high cost of MC-OXC's due to fabrication complexity and power considerations. Bounds on the number of wavelength required for multicast in general topologies of WDM networks were presented in [201].

The underlying optical multicast technologies are expected to be further developed and to be mature for commercial implementation, which will also help our collective understanding of optical multicast advance.

2.6 Optical multicast traffic protection approaches

The underlying optical backbone networks provide huge data capacity and fast transmission speed for optical multicast. However, the optical networks are vulnerable to both human errors and natural disasters, which would cause capricious network failures. As the success of optical multicast relies on the underlying optical backbone networks, without an efficient and fast recovery mechanism, a network failure can lead to severe disruption to optical multicast and calamitous loss to end customers. If a link/node in a multicast session fails, the traffic to all the downstream destinations along the failed link/node would be affected. The closer the link/node is to the source node, the more destinations would be affected. Hence, efficient and fast resilience algorithms are very crucial to network survivability for optical multicast.

Most of current optical multicast protection approaches may be classified into four major categories: (i) tree-based protection approaches [202-211]; (ii) ring-based protection approaches [212-216]; (iii) path-based protection approaches [204, 212, 217-224]; (iv) segment-based protection approaches [204, 218, 221, 225-228]. The work on optical multicast protection presented in this thesis can be classified into another new category: *p*-cycle-based protection approaches [229-234]. There is also another interesting work reported on light tree reconfiguration (restoration) approaches [235] and automatic protection switching (APS) approach proposed for optical multicast [236]. The following three sub-

sections briefly review tree-based protection approaches, ring-based protection approaches and path-based protection approaches.

2.6.1 Tree based optical multicast protection approaches

For link failure recovery, the most straightforward way is to identify a link-disjoint primary and backup tree pairs for a multicast session in the network. The key idea behind the link disjoint trees (LDT) approach is that, in the link disjoint tree pairs, we can identify a link-disjoint path pairs from the source to every destination can be identified. The link-disjoint constraint is to avoid the primary tree and the backup tree to fail simultaneously upon a single link failure. In general, a multicast session Φ_i is denoted as $\{s_i, d_{i1}, d_{i2}, \dots, d_{ik}\}$, where s_i is the source node, $d_{i1}, d_{i2}, \dots, d_{ik}$ are the destination nodes, and k is the multicast group size.

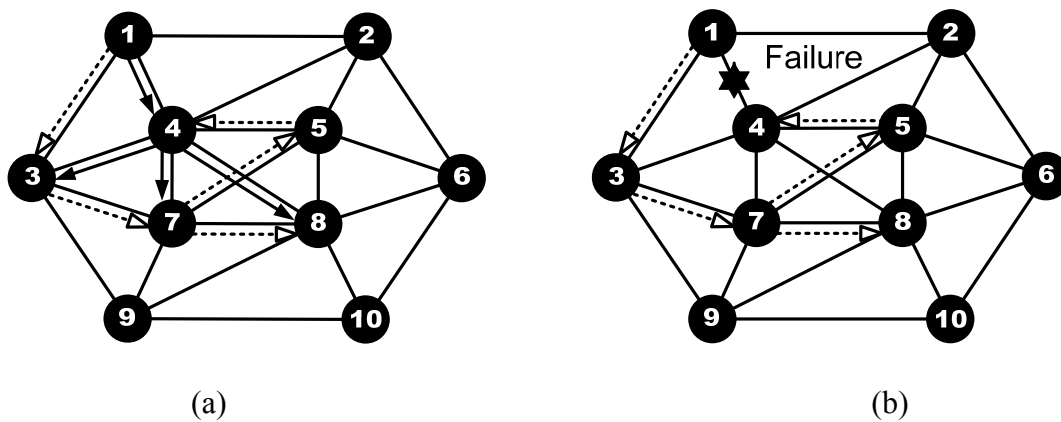


Figure 2-9: A simple example illustrating the link-disjoint tree (LDT) protection approach (a) a pair of link-disjoint trees (b) link failure recovery mechanism

A simple example illustrating the LDT approach is shown in **Figure 2-9**. In **Figure 2-9 (a)**, the primary tree (shown in solid lines with solid arrows) of $\Phi_1 (\Phi_1 = \{1, 3, 4, 7, 8\})$ is protected by its link-disjoint backup tree (shown in dash lines with hollow arrows). In **Figure 2-9 (b)**, upon failure of link 1-4, the multicast traffic on the primary tree is restored on the link-disjoint backup tree.

In [205], the authors proved that an arc-disjoint (directed-link disjoint) tree pairs is also sufficient to protect a multicast session by appropriate protection switching. Ref. [211] further studies the ADT approach with differentiated leaf availability grantee. Although the quality of service is guaranteed, the availability constraints in [211] increases the computational complexity significantly.

One of the problems remaining unsolved of the ADT approach is how the signaling and the protection switching processes can be implemented, because upon the common link failure, the multicast traffic may be delivered from the source to the destinations through parts of the primary tree and parts of backup tree.

One of the common problems of the LDT and the ADT approaches is no capacity sharing and thus not so cost-effective. The most significant drawback of the LDT and the ADT approaches is the inability of identifying such disjoint tree pairs in sparse networks. To improve the capacity efficiency, the authors further proposed the self-sharing tree (SST) approach and the cross-sharing trees (CST) approach [202].

Although this sub-section mainly discusses about tree-based protection approaches, the tree based restoration approaches are included for completeness. Four restoration approaches were presented in [235]. In the light tree reconfiguration (LR) approach [235], upon a single link failure, all light trees are released and reconfigured to avoid traversing failed link. In the light tree interrupted reconfiguration (LIR) approach [235], unlike the LR approach, only the light trees traversing the failed link reconfigure. In the optical branch (OB) approach [235], the optical branches (segments connecting the source or splitting node and the downstream splitting node or destination node) disrupted by the link failure are replaced by newly configured ones. As for the optical branch fixed (OBF) approach [235], a certain number of backup optical branches are employed by ILP optimization to restore the light trees from any single link failure. Both the LR and the LIR approaches are designed based on

reconfiguration of light trees. In contrast, both the LR and the LIR approaches were designed based on reconfiguration of the branches of the light trees. The LR approach was shown to achieve the minimal spare capacity requirement, compared with other reconfiguration approaches [235].

2.6.2 Ring based optical multicast protection approaches

SONET and SDH networks generally deploy ring topology (self-healing ring (SHR)) [237] [238], due to its high degree of network survivability [46]. In ring based protection approaches, the end nodes of the failed link/node handle the protection switching. Two dedicated ring based protection approaches, namely the one ring for one multicast session (OFO) approach and the one ring for all multicast sessions (OFA) approach, were reported in [214]. In both the OFO approach and the OFA approach, the source and all destination nodes must be on one ring. In the OFO approach, each multicast session is protected by a copy of a minimum cost dedicated ring. No other traffic is allowed to share this copy of ring to avoid complicated control and management, according to [214]. In the OFA approach, a Hamiltonian ring (a Hamiltonian ring is defined as a ring which covers all nodes in the network [239].) is identified to protect all multicast sessions. However, each multicast session is protected by one copy of this ring. Hence, the OFO approach and OFA approach are not so capacity efficient, as no capacity sharing is allowed.

The minimum cost collapsed ring (MCCR) approach [212, 213] utilizes a partial bidirectional ring, which is formed by two arc-disjoint ring paths, to provide the dedicated protection to a multicast session. Different from the previous ring based approaches which protect each multicast sessions as a whole, the multiple ring based local restoration (MRLR) approach [216] partitions the multicast tree into several disjoint segment-blocks (sub-trees) for protection. As for comparison with the bidirectional line switched ring (BLSR) approach,

the MCCR approach utilizes less capacity and therefore more cost-effective. However, one of the common drawbacks of the BLSR and the MCCR approaches is that, the working path and protection path of a multicast session from the source to all the destinations are restricted in one ring.

2.6.3 Path/segment based optical multicast protection approaches

In the comprehensive performance evaluation of the multicast protection approaches in [204], the optimal path pair (OPP) optical multicast protection approach was reported to outperform all other approaches. The basic idea of the OPP based protection approach reported in [204] is that, for every multicast session, a link-disjoint path pair from the source to every destination node is sufficient to handle any single link failure. In this case, the primary path and the backup path would not fail simultaneously upon any single link failure in the network. Upon a single failure on the primary path, the end nodes of the failed link send signals to the source and the destination of this path. The source and the destination of this primary path configure the backup path on the reserved spare capacity, and then switch the traffic onto the backup path. The path pairs within the same session are allowed for capacity sharing, because they actually carry the same information. However, OPP based approach only considers the capacity sharing within the same multicast session.

Based on the OPP concept, an OPP based shared disjoint path (OPP-SDP) heuristic algorithm was proposed to handle both static and dynamic traffic protection [204]. Once a multicast request arrives, the OPP-SDP algorithm first identifies a link-disjoint path pair from the source to every destination. In order to reduce the total cost, once a path pair is found, the cost of the arcs along that path pair is updated to be zero to increase the sharing of the new path pairs with the already-found ones within the same session. The OPP-SDP algorithm was reported to be most efficient for link failure recovery, in terms of blocking performance [204].

Besides the OPP-SDP algorithm, another segment based protection algorithm: optimal path pair – shared disjoint segment (OPP-SDS) algorithm was proposed in [204]. In the OPP-SDS algorithm, a multicast tree is partitioned into several segments according to the splitting nodes. A splitting node is an intermediate node (other than the source and destination nodes) with a node degree greater than 2. A segment is defined as a sequence of links from the source (or a splitting node) to a downstream splitting node (or a destination node). It was shown that the OPP-SDS algorithm has a higher blocking probability than the OPP-SDP algorithm for protection against single link failure.

The shared segment protection algorithm was presented in [221]. Compared with the OPP-SDS algorithm, the only difference is that, in the shared segment protection algorithm, backup segments can share spare capacity among different multicast sessions, if and only if their corresponding primary segments are mutually-link-disjoint. Based on the shared segment protection algorithm, the dual-link failure problem was also considered in [221] by re-provisioning the spare capacity for affected primary segments and backup segments after the first link failure.

2.6.4 Performance comparison

To compare the performance of the optical multicast protection approaches presented above, we select the COST239 network (11 nodes and 26 links), whose average node degree (the average number of links connected to a node) is 4.727. Each link is assumed to have two fibers of 64 wavelengths per fiber, transmitting in opposite directions. For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node.

We select the CST approach [202], the OFO approach [214], and the OPP approach [204] for comparison, as they are the typical approaches presented in previous sub-sections. The

results of the comparison of the capacity efficiency of the three approaches for static traffic simulations in COST239 network is shown in **Figure 2-10**. The OPP approach achieves the best capacity efficiency, which is consistent with the results obtained in [204].

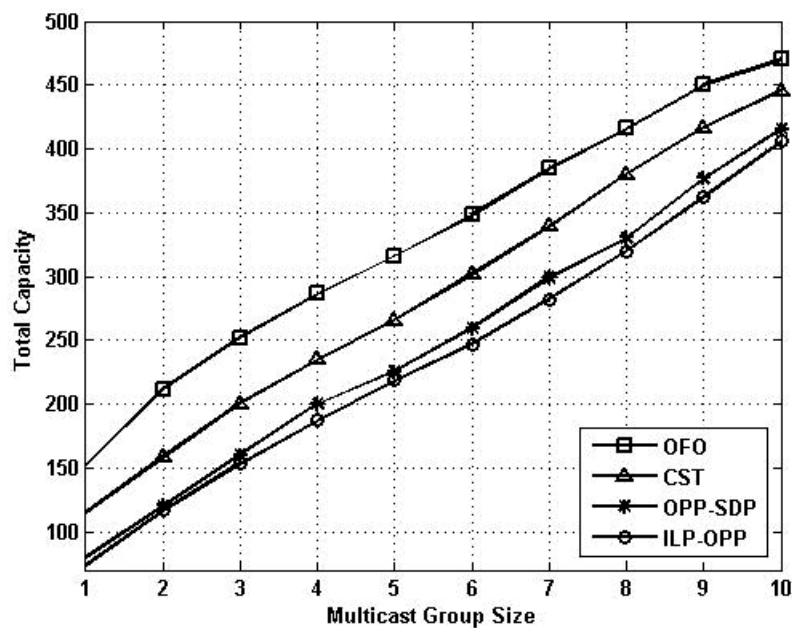
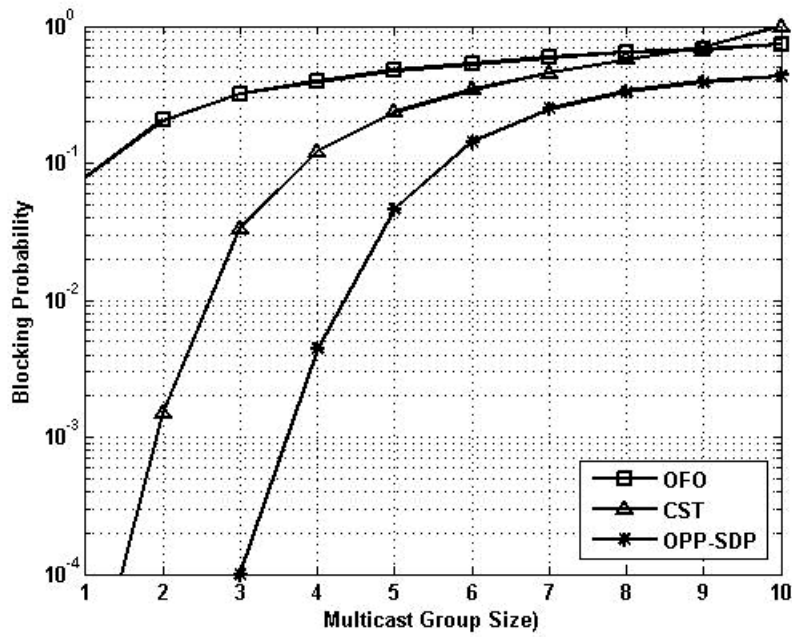
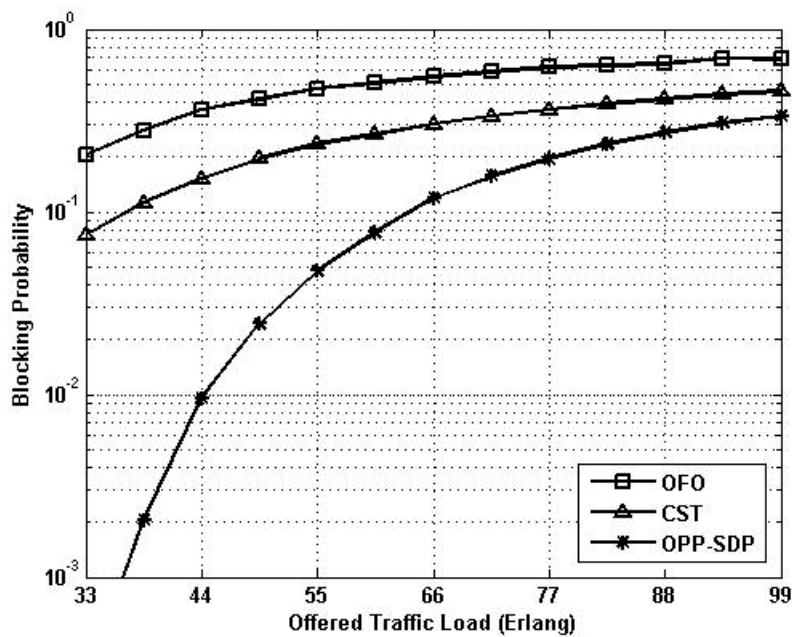


Figure 2-10: Capacity efficiency comparison for static multicast traffic protection for link failure recovery in COST239 network

For dynamic traffic protection, we also choose the COST239 network as the test network. Each link is assumed to have two fibers of 16 wavelengths per fiber, transmitting in opposite directions. The multicast session requests are assumed to arrive with a Poisson distribution and their holding time is negatively exponentially distributed. For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node. The total number of randomly generated multicast requests is 10^5 for each network traffic load in the simulation. The Steiner tree (ST) heuristic Algorithm [239] is applied for multicast tree routing.



(a)



(b)

Figure 2-11: Comparison of blocking performance for dynamic traffic in COST239 network: (a) the offered network traffic is fixed at 55 Erlang, and (b) the multicast group size is fixed at 5.

According to the results obtained in static traffic simulations, as show in **Figure 2-11**, the OPP approach also achieves the best blocking performance for dynamic traffic simulations. As such, the OPP approach is selected for performance comparison with our developed p -cycle approaches, which will be described in the next a few chapters.

2.7 Conclusions

This chapter reviews the current state of the research work of network resilience techniques in different layers, with special focus on multicast traffic protection approaches in the optical layer, due to the fact that the problem of multicast traffic protection has started to draw more and more research interests, because of the rapid growth of multicast applications.

Most of current optical multicast traffic protection approaches focus on single link failure recovery. They can be classified into four major categories: (i) tree-based protection approaches; (ii) ring-based protection approaches; (iii) path-based protection approaches; (iv) segment-based protection approaches. Among all the approaches, tree-based protection approaches are most-straightforward, but they were shown to be less efficient, and not suitable for sparse networks. Ring approaches are fast in recovery but the drawback is the inefficiency of resource unitization. Path/segment approaches are famous for their efficient resource utilization, but they are slow in failure recovery. The nature of complicated spare capacity sharing and complex restoration process makes the provisioning process too complicated, which is not desired by most network operators. Therefore, most protection approaches in the above four categories are either not cost-effective or slow in recovery speed. Thus, considerable efforts are required to propose novel multicast protection approaches, which are both cost-effective and fast in recovery speed.

Chapter 3. Link-Protecting p -Cycle Based Optical Multicast Protection Approach

3.1 Introduction

The link-protecting preconfigured protection cycle (p -cycle) based approach proposed by Grover [106] for unicast traffic protection exhibits fast restoration speed (like SDH/SONET rings), because p -cycles are pre-cross-connected. Compared with the ring based protection approaches, the link-protecting p -cycle based approach also offer mesh-like high efficiency, because they can protect both on-cycle and straddling links (spans). The features of ring-like restoration speed and mesh-like efficiency are preferred by network operators. The link protecting p -cycle based protection approach has been extensively studied for unicast traffic protection, but has never been applied to multicast traffic protection yet. The impacts of the network failures and the merits of link protecting p -cycle based protection approach motivate us to investigate its effectiveness in protecting optical multicast traffic, in comparison with existing multicast traffic protection approaches.

This chapter introduces the link-protecting p -cycle based approach for optical multicast traffic protection. It is organized as follows. Section 3.1 gives the background and motivation. Section 3.2 introduces the graphical model, assumptions and notations in this study. Section 3.3 elaborates on the protection mechanism of link protecting p -cycle based approach. Section 3.4 introduces the spare capacity optimization algorithm of p -cycle based link protection (SOPL). Section 3.5 presents the joint optimization algorithm of p -cycle based link protection (JOPL), while Section 3.6 explains the non-joint optimization algorithm of p -cycle based link protection (NJOPL). Section 3.7 presents the efficiency ratio based unity- p -cycle heuristic algorithm (ERH). Section 3.8 presents the dynamic p -cycle (DpC) algorithm.

Section 3.9 presents the link protecting p -cycle based protected working capacity envelope (PWCE) algorithm, and Section 3.10 presents the hybrid DpC and PWCE algorithm. Section 3.11 investigates their performance in static traffic environment. Section 3.12 evaluates their performance in dynamic traffic environment. Lastly, the conclusions are given in section 3.13.

3.2 Assumptions, definitions and notations

In this study, a network is modeled as a directed graph $G(N,E)$, where N is the set of nodes and E is the set of directed links (spans). $|X|$ is used to denote the total number of elements in a set of X (e.g., $|N|$ is the total number of nodes in the network). A directed link originating at node m and terminating at node n is denoted as link mn .

A multicast session Φ_i is denoted as $\{s_i, d_{i1}, d_{i2}, \dots, d_{ik}\}$, where s_i is the source node, $d_{i1}, d_{i2}, \dots, d_{ik}$ are the destination nodes, k is the multicast group size. For unicast, $k = 1$; for multicast, $1 < k \leq |N| - 1$; for broadcast, $k = |N| - 1$. In general, network traffic is unlikely to be symmetric in both directions between any two nodes. This is particularly true in the case of multicast traffic, where a source node sends data to multiple destination nodes. This implies that the number of working or protection wavelengths is not likely to be the same in both directions on a link. Therefore, without loss of generality, all light trees and p -cycles considered in our projects are *unidirectional*, i.e., they are *directed*. As shown in [120, 231, 240], one unit of capacity is defined as one wavelength on a link, and a unity p -cycle is defined as a directed p -cycle with one unit of capacity on every link in the p -cycle. If a cycle is selected for more than one time to protect multiple multicast trees, the cycle is said to have multiple copies. Given a network topology, the heuristic edge-digraph based cycle algorithm [68, 241] is applied to find all the simple cycles.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

To efficiently utilize the huge bandwidth offered by the optical multicast, the traffic of relevant higher layer applications are assumed to be groomed into one or more multicast sessions [242-245]. Every node in the network is also assumed to be equipped with full wavelength conversion capability and multicasting capability. The assumptions of full wavelength conversion capability and the multicast capability at every node are mainly to reduce the problem of complexity, so the focus is on the protection capability of the multicast protection approaches, without taking into consideration of wavelength conversion problem or sparse wavelength conversion problem and sparse splitting problem.

Next, the following general notations used in this study are introduced:

Sets

- Φ Set of multicast sessions, indexed by i .
- N Set of nodes, indexed by m or n .
- E Set of edges (links or spans), indexed by mn .
- T Set of trees routed, indexed by τ .
- C Set of unidirectional p -cycles, indexed by j .

Input parameters

- k Multicast group size
- c_{mn} Cost for a unit capacity on link mn (1 in this study).
- t_{mn} Total capacity constraint on link mn (max no. of wavelengths available on link mn)
- $\alpha_{j,mn}$ It is 1 if cycle j traverses link mn and 0 otherwise.
- w_{mn}^{max} Working capacity constraint on link mn . (max no. of working units on link mn).

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

$\beta_{j,mn}$ It is 1 if link mn can be protected by cycle j and 0 otherwise.

s Index for a source node.

d Index for a destination node.

Variables

f_j The total number of copies finally required for p -cycle j .

w_{mn} Number of working units on link mn .

v_{mn} Number of spare units required to be reserved on link mn to configure p -cycles.

In this study of p -cycle based spare capacity optimization (SOP) algorithms and heuristic algorithms, the optimal shortest path tree (OSPT) heuristic algorithm [215] and the Steiner tree (ST) heuristic algorithm [239] are applied for multicast tree routing. It should be noted that, in the SOP algorithms, w_{mn} are obtained by calculating the sum of working units of all multicast sessions on each link, after the routing. Hence, they are input parameters to the ILP formulations of the SOP algorithms. However, in the JOPL and the NJOPL algorithms, w_{mn} are variables in the ILP formulations. After all the multicast sessions are routed, the ILP-based SOP algorithms or the ERH algorithm is then applied to configuring p -cycles for protecting all the multicast sessions. Next, each design will be described in detail.

3.3 Protection mechanism of the link protecting p -cycle based approach

For link-protecting p -cycles, only the end nodes of the failed link handle the service recovery. All light paths traversing the failed link are rerouted around that link. A bidirectional link protecting p -cycle can provide one backup path against one on-cycle link failure and two backup paths against one straddling link failure [106]. A simple example is

shown in **Figure 3-1**, illustrating a link protecting unity- p -cycle indicated by the dashed line in (a) can protect one working unit in the opposite direction of the unity- p -cycle against any single on-cycle link failure shown in (b), and two working units (one in each direction) against any single straddling link failure shown in (c).

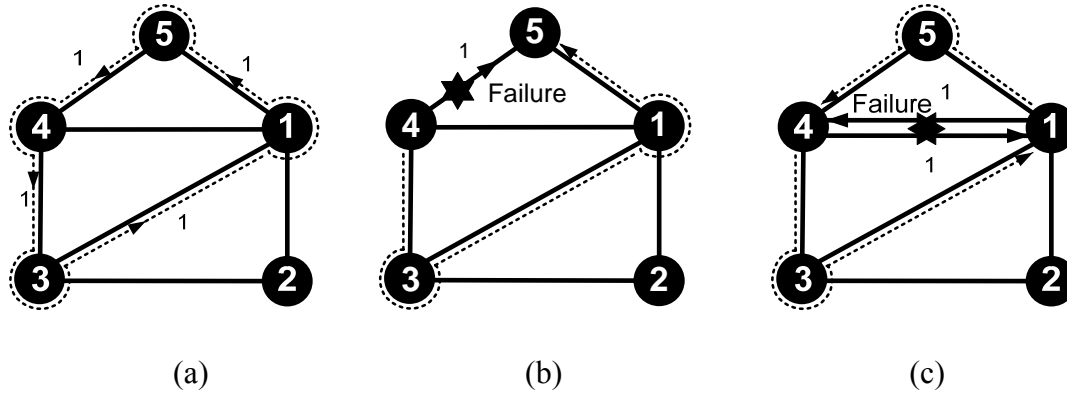


Figure 3-1: A simple example illustrating the link protecting p -cycle based approach

In this chapter, different algorithms of link-protecting p -cycle based approach of optical multicast traffic protection for single link failure recovery are presented. For static multicast traffic protection, ILP spare capacity optimization algorithm of p -cycle-based link protection (SOPL) [108] and the efficiency ratio based unity- p -cycle heuristic algorithm (ERH) [120], which were proposed for unicast traffic protection earlier, will be extended to multicast traffic protection first. In order to reduce the total network resource consumption, a joint optimization algorithm of p -cycle-based link protection (JOPL) and a non-joint optimization algorithm (NJOPL) are further proposed. For dynamic multicast traffic protection, we first consider applying the dynamic p -cycle (DpC) algorithm [132] and the p -cycle based protected working capacity envelope (PWCE) algorithm [135] proposed for unicast traffic protection to multicast traffic protection application [231]. The former is more efficient in the use of spare capacity, whereas the latter is much faster in the establishment of protected

multicast trees. In order to combine the merits of both algorithms, a hybrid DpC and PWCE design [231] for protecting multicast traffic is also proposed.

3.4 Spare capacity optimization algorithm of p -cycle based link protection (SOPL)

The ILP algorithm of spare capacity optimization of p -cycle-based link protection for unicast traffic protection in [246] is extended to multicast traffic protection. The ILP formulation reported in [246] is given below:

$$\text{Objectives: Minimize } \sum_{\forall mn \in E} c_{mn} v_{mn} \quad (3.1)$$

Constraints:

$$v_{mn} = \sum_{\forall j \in C} \alpha_{j,mn} f_j \quad \forall mn \in E \quad (3.2)$$

$$w_{mn} \leq \sum_{\forall j \in C} \beta_{j,mn} f_j \quad \forall mn \in E \quad (3.3)$$

$$w_{mn} + v_{mn} \leq t_{mn} \quad \forall mn \in E \quad (3.4)$$

The objective (3.1) is to minimize the spare capacity used for configuring the link-protecting p -cycles. Constraint (3.2) calculates the total spare capacity used by the selected candidate p -cycles on link mn . Constraint (3.3) guarantees all the working capacity of the multicast sessions is protected, while constraint (3.4) restricts the total capacity on each link.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

The variables in the ILP formulation of SOPL are v_{mn} and f_j . The approximate number of variables for ILP formulation of SOPL is $|E| + |C|$. The approximate number of constraints for ILP formulation of SOPL is $3|E|$. ($|E|$ is the number of edges. $|C|$ is the number of cycles. $|T|$ is the number of multicast sessions. $|E|$ and $|C|$ would increase with $|N|$ and the nodal degree.)

3.5 Joint optimization algorithm of p -cycle based link protection (JOPL)

In order to reduce the total capacity consumption, the design of joint optimization of p -cycle-based link protection (JOPL) is further studied. The JOPL algorithm minimizes the working capacity used for setting up the multicast trees and the spare capacity used for configuring the link-protecting p -cycles simultaneously, instead of optimizing the spare capacity only as in the SOP algorithms. The portion of setting up the primary multicast sessions in the ILP formulation of ILP-OPP in [204] is modified firstly, and then applied to our ILP formulation of the JOPL algorithm. More specifically, the constraints (3.6) – (3.9) are adapted from the ILP formulation in [204]. The additional notations used in the ILP formulations of JOPL are shown below:

Variables

$P_{sd,mn}^i$	It is 1 if the path from source s to destination d in multicast session i occupies link mn , and 0 otherwise
w_{mn}^i	It is 1 if multicast session i traverses link mn and 0 otherwise.

The ILP formulation of the JOPL algorithm is given below:

Objectives: **Minimize:**
$$\sum_{mn \in E} c_{mn} (w_{mn} + v_{mn}) \quad (3.5)$$

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach**Constraints:**

$$\sum_n P_{sd,sn}^i = 1 \quad \forall d, \forall i \quad (3.6)$$

$$\sum_n P_{sd,ns}^i = 0 \quad \forall d, \forall i \quad (3.7)$$

$$\sum_n P_{sd,dn}^i = 0 \quad \forall d, \forall i \quad (3.8)$$

$$\sum_n P_{sd,nd}^i = 1 \quad \forall d, \forall i \quad (3.9)$$

$$\sum_n P_{sd,nm}^i = \sum_n P_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i, \forall m \neq s, d \quad (3.10)$$

$$P_{sd,mn}^i \leq w_{mn}^i \quad \forall mn \in E, \forall d, \forall i \quad (3.11)$$

$$w_{mn} = \sum_{i=1}^{|T|} w_{mn}^i \quad \forall mn \in E \quad (3.12)$$

$$v_{mn} = \sum_{\forall j \in C} \alpha_{j,mn} f_j \quad \forall mn \in E \quad (3.13)$$

$$w_{mn} \leq \sum_{\forall j \in C} \beta_{j,mn} f_j \quad \forall mn \in E \quad (3.14)$$

$$w_{mn} + v_{mn} \leq t_{mn} \quad \forall mn \in E \quad (3.15)$$

The objective (3.5) is to minimize the total capacity. Constraints (3.6) – (3.11) are used to set up working multicast session i . Constraints (3.6) and (3.7) ensure that, for multicast session i , the source node has only 1 unit of outgoing flow and 0 unit of incoming flow. That means that no cycles are generated at the source and the destination nodes. Constraints (3.8) and (3.9) ensure that, for multicast session i , every destination node has 0 unit of outgoing flow and only 1 unit of incoming flow. Constraint (3.10) states that, for multicast session i , the incoming flow of any intermediate node is equal to its outgoing flow. Constraint (3.11) states that, for multicast session i , if any working path between the source and the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

destinations occupies link mn , one (and only one) of the wavelengths on link mn is reserved for the multicast session i . All the working paths within multicast session i can share that unique wavelength on link mn , because they carry the same information. This turns the light paths from the source to all the individual destinations into a single tree from the source to all the destinations. Constraint (3.12) calculates the sum of the working capacity on link mn required for all $|T|$ multicast sessions. Constraints (3.13) – (3.15) are used to determine the p -cycle allocation required to protect all $|T|$ multicast sessions. Constraint (3.13) calculates the total spare capacity used by the selected candidate p -cycles on link mn , while Constraint (3.14) guarantees all the working capacity of the multicast sessions is protected and Constraint (3.15) restricts the total capacity on each link in the given network topology. In mesh networks, for multicasting, a tree with no loops (known as simple tree) consumes less capacity than a tree with loops. In particular, a Steiner tree takes the minimum total working capacity to setup a multicast session. The capacity minimization objectives of the JOPL model enforce the working multicast sessions to be simple trees. In other words, loops or cycles would not be created under the capacity minimization objectives. In fact, this has been verified in the conducted simulations.

As there are $|E|$ spans, $|C|$ cycles and $|T|$ multicast sessions, the approximate number of variables for ILP formulation of the JOPL algorithm is $|E|[2+(1+k)|T|] + |C|$. The approximate number of constraints for ILP formulation of the JOPL algorithm is $4|E| + k|T|[4+|M|+|E|]$.

3.6 Non-joint optimization algorithm of p -cycle based link protection (NJOPL)

To investigate the effectiveness of the total capacity reduction of the p -cycle-based JOPL algorithm, a non-joint optimized algorithm of p -cycle-based link protection (NJOPL) of multicast sessions is also considered and analyzed. The NJOPL algorithm first minimizes the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

working capacity used for setting up the multicast sessions (This is to set-up the Steiner tree.), and then minimizes the spare capacity for configuring the p -cycles separately. The ILP formulation of the NJOPL design is given below, which consists of three steps.

Step 1:

Objectives: **Minimize:**
$$\sum_{\forall mn \in E} c_{mn} w_{mn} \quad (3.16)$$

Constraints:

(3.6)- (3.12) of the ILP formulation of the JOPL algorithm, and

$$w_{mn} < w_{mn}^{max} \quad \forall mn \in E \quad (3.17)$$

Step 2:

Objectives: **Minimize:**
$$\sum_{\forall mn \in E} c_{mn} v_{mn} \quad (3.18)$$

Constraints:

(3.13) - (3.15) of the ILP formulation of the JOPL algorithm

Step 3:

$$\text{Total capacity} = \sum_{\forall mn \in E} c_{mn} w_{mn} + \sum_{\forall mn \in E} c_{mn} v_{mn} \quad (3.19)$$

The objective of Step 1 is to minimize the working capacity used for setting up the multicast sessions. This is to set-up a Steiner tree. The constraints are the same as (3.6) - (3.12) of the ILP formulation of the JOPL algorithm. Constraint (3.17) is to restrict the maximum working capacity allowed on link mn . The outputs of the optimized results of the working capacity on

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

each link ($w_{mn} \forall mn \in E$) in Step 1 are part of the input parameters to the spare capacity optimization in Step 2. Step 2 of the NJOPL algorithm is the same as the SOPL algorithm, which is to minimize the spare capacity for configuring the p -cycles. Step 3 states that the total capacity is the sum of the optimized working capacity in Step 1 and the optimized spare capacity in Step 2.

As there are $|E|$ spans, $|C|$ cycles and $|T|$ multicast sessions, the approximate number of variables for ILP formulation of the NJOPL algorithm is $|E|[2+(1+k)|T|] + |C|$, which is the same as the JOPL algorithm. The approximate number of constraints for ILP formulation of the NJOPL algorithm is $5|E| + k|T|[4+|M|+|E|] + 1$.

3.7 Efficiency ratio based unity- p -cycle heuristic algorithm (ERH)

The above three ILP based optimization algorithms optimize the capacities required for the link-protecting p -cycle based multicast traffic protection approach, but they are slow in computational speed. In the case of unicast traffic protection, it has been shown that the performance of the efficiency ratio (ER) based unity- p -cycle heuristic algorithm (ERH) algorithm proposed in [120] is very close to that of the SOPL with much reduced computational time. The ERH algorithm can be also applied to multicast traffic protection [231, 232]. Its performance is compared with those of the other algorithms of the link protecting p -cycle based multicast traffic protection approach. The efficiency ratio (ER) of a unity- p -cycle is defined as the ratio of the number of working units (wavelengths) that are actually protected by it to the number of spare units required to be reserved for it [120].

$$ER(c_j) = \sum_{\forall mn \in E} \beta'_{j,mn} / \sum_{\forall mn \in E} \alpha_{j,mn} \quad (3.20)$$

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

$\alpha_{j,mn}$ is 1 if cycle j traverses link mn and 0 otherwise. $\beta'_{j,mn}$ is 1 if one unit of the unprotected capacity on link mn can be protected by cycle j and 0 otherwise.

The a priori efficiency (AE) in [7, 9] is defined to be the ratio of the total amount of working capacity, which the cycle has the potential to protect to the spare capacity of the cycle. The AE, which is determined by the topology, is to measure a cycle's capability in protecting working capacity. Its calculation is done before the routing. The AE can be used to pre-select the cycles.

The actual efficiency used in the capacitated iterative design algorithm (CIDA) [7] and the ER used in the ERH algorithm [8], which are determined by both the topology and the unprotected working capacity that actually can be protected [241], are defined to be the ratio of the working capacity that can actually be protected by the cycle over the spare capacity of the cycle. They give not only the measure of a cycle's capability to protect working capacity, but also an indication of a cycle's actual suitability for specific working capacity.

The flow chart of the ER -based unity- p cycle design heuristic algorithm is shown in **Figure 3-2**. Given a network topology, the heuristic edge-digraph based cycle algorithm [68, 241] is applied to find all the simple cycles. Next, given the traffic load, the multicast traffic is routed by using either the open shortest path tree (OSPT) heuristic algorithm [215] or the Steiner tree (ST) heuristic algorithm [239] and determine the working units on each link. The OSPT heuristic algorithm tries to minimize the end-to-end cost between the source and each destination using Dijkstra shortest path algorithm (SPA) and promote common arc-sharing among the end to end shortest paths to reduce the cost of using extra arcs. In contrast, the ST heuristic algorithm attempts to minimize the overall cost of the tree. After the routing, the ERH algorithm is applied to identify those most efficient p -cycles for protecting all the established multicast trees [231, 232]. Firstly, the ER of unity p -cycle of each candidate cycle

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

is calculated and the one with the maximum ER is chosen. Then, the working units on each unidirectional edge that can be protected by the selected cycle are removed. The whole process is iterated until all the working units are protected. Finally, the algorithm outputs the number of copies required for each p -cycle.

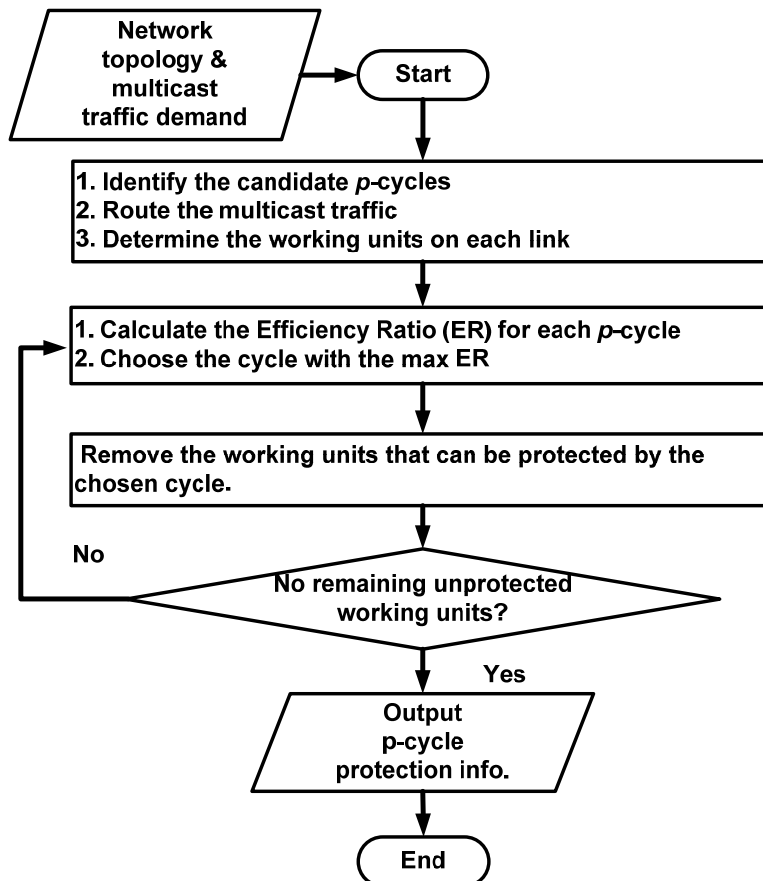
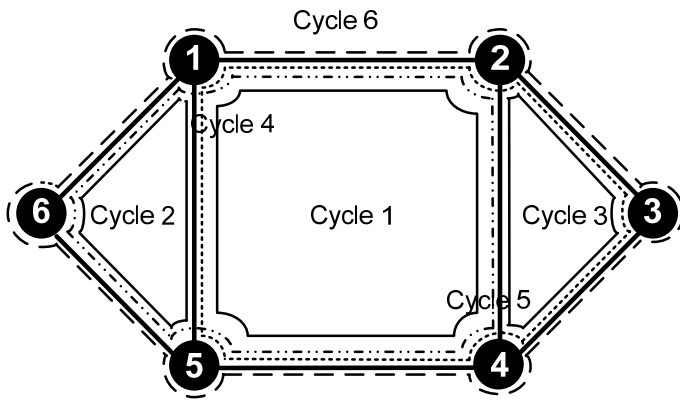


Figure 3-2: Flow chart of the efficiency ratio (ER) based unity- p -cycle heuristic algorithm

An example explaining the ERH algorithm for multicast traffic protection is given below. In the simple network topology consisting of 6 nodes and 8 links shown in **Figure 3-3**, there are 6 bi-directional cycles (each cycle has two unity- p -cycles: one is in clockwise direction, while the other in counter-clockwise direction.), which are shown in **Table 3-1**.

Figure 3-3: A simple network topology containing 6 p -cyclesTable 3-1: Identified p -cycles in the simple network topology shown in Figure 3-1

Cycle 1	$1 \leftrightarrow 2 \leftrightarrow 4 \leftrightarrow 5 \leftrightarrow 1$
Cycle 2	$6 \leftrightarrow 1 \leftrightarrow 5 \leftrightarrow 6$
Cycle 3	$2 \leftrightarrow 3 \leftrightarrow 4 \leftrightarrow 2$
Cycle 4	$6 \leftrightarrow 1 \leftrightarrow 2 \leftrightarrow 4 \leftrightarrow 5 \leftrightarrow 6$
Cycle 5	$1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4 \leftrightarrow 5 \leftrightarrow 1$
Cycle 6	$6 \leftrightarrow 1 \leftrightarrow 2 \leftrightarrow 3 \leftrightarrow 4 \leftrightarrow 5 \leftrightarrow 6$

Table 3-2: Test multicast sessions

Session no	Source	Destinations	Links involved in multicast Trees
1	1	{2,3,4,6}	{1→6, 1→2, 2→4, 2→3}
2	6	{1,4,5}	{6→1, 6→5, 5→4}
3	3	{2,5,6}	{3→2, 2→1, 1→6, 1→5}
4	4	{1,2}	{4→2, 2→1}
5	2	{1,3,4,5,6}	{2→3, 2→4, 2→1, 1→6, 1→5}
6	4	{1}	{4→5, 4→1}

Now, we have 6 multicast sessions, which are routed using the ST heuristic [23] in this simple network. These multicast sessions are shown in **Table 3-2**, where the last column indicates the links traversed by a multicast tree. After the wavelengths are assigned to the links that are traversed by the multicast trees, the sum of working units required on each directed link is obtained. As shown in **Figure 3-4 (a)**, the number on each direct link

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

indicates the sum of working units required to set up the 6 multicast sessions that are given in Table 3-2.

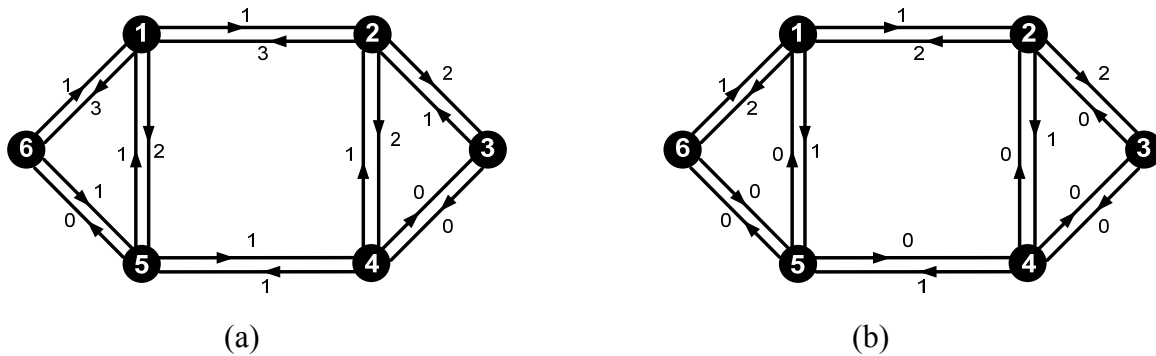


Figure 3-4: (a) Initial working units of all the multicast trees on each link, (b) remaining working units on each link

Table 3-3: The ER of all the identified unity- p -cycles in Table 3-1

Cycle no.	1	2	3	4	5	6
<i>ER</i> of the clockwise unity- p -cycle	1	1	0.667	1.4	1.2	1.5
<i>ER</i> of the counter clockwise unity- p -cycle	1	0.667	0.667	1.2	1.2	1.333

Next, the *ER* of each unit- p -cycle identified in the network topology is calculated and the one with the maximum *ER* is selected. For instance, cycle 6 has 6 spans. Theoretically, its clockwise unity- p -cycle can protect 10 working units (including one unit on each of the four straddling links $1 \rightarrow 5$, $5 \rightarrow 1$, $2 \rightarrow 4$ and $4 \rightarrow 2$, and one unit on each of the six on-cycle links: $1 \rightarrow 6$, $6 \rightarrow 5$, $5 \rightarrow 4$, $4 \rightarrow 3$, $3 \rightarrow 2$, and $2 \rightarrow 1$). However, there is no working capacity on link $4 \rightarrow 3$. Hence, it actually protects 9 working units in total, and its *ER* is $9/6=1.5$. In relation to Figure 3-4 (a), Table 3-3 shows the *ER* of all the identified unity- p -cycles. As shown in Table 3-3, the *ER* of the clockwise unity p -cycle of cycle 6 is the maximum among all the candidate cycles. It is selected first and the working units actually protected by it are removed.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

The remaining working units on each link are shown in **Figure 3-4 (b)**. After that, the next unity- p -cycle with the maximum ER based on the remaining working units on each link is identified. The process iterates until the working capacity on each link becomes zero. Finally, a set of p -cycles required to be configured to protect those six multicast sessions (shown in **Table 3-2**) is obtained and shown in **Table 3-4**.

Table 3-4: The set of p -cycles chosen by the ERH algorithm

Cycle no.	1	2	3	4	5	6
No. of copies required of the clockwise unity- p -cycle	1	0	0	1	0	1
No. of copies required of the counter clockwise unity- p -cycle	0	0	1	0	0	1

3.8 Dynamic p -cycle (DpC) algorithm

Link protecting p -cycles is also proposed to be applied to dynamic protection provisioning of multicast traffic for single link failure recovery, and the blocking performance is evaluated in comparison with other existing multicast protection algorithms [231, 234]. Three different link protecting p -cycle based multicast protection algorithms for dynamic multicast traffic protection are considered, namely the dynamic p -cycle (DpC) algorithm, the p -cycle based protected working capacity envelope (PWCE) algorithm, and the hybrid DpC and PWCE algorithm. The p -cycle-based multicast protection algorithms were shown to offer much better blocking performance, as compared with other existing multicast protection algorithms. The main reasons for the much better blocking performance are attributed to the facts that: (i) the selection of p -cycles is independent of the routing of the multicast light trees, (ii) there are no disjoint constraints between the selected p -cycles and the multicast light trees to be protected, (iii) the selected p -cycles are the most efficient p -cycles.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

Based on the ER -based unity- p -cycle heuristic algorithm [120], three protection strategies were proposed for dynamic provisioning of unicast traffic in [132]. Among the three protection strategies reported in [132], Strategy 3 achieves the best blocking performance with reasonable computational time for dynamic unicast traffic. Therefore, in this study, Strategy 3 in [132] is adopted as the dynamic p -cycle (DpC) design for dynamic provisioning of survivable multicast traffic [231]. The flow chart of the DpC design for dynamic provisioning of survivable multicast traffic is shown in **Figure 3-5**.

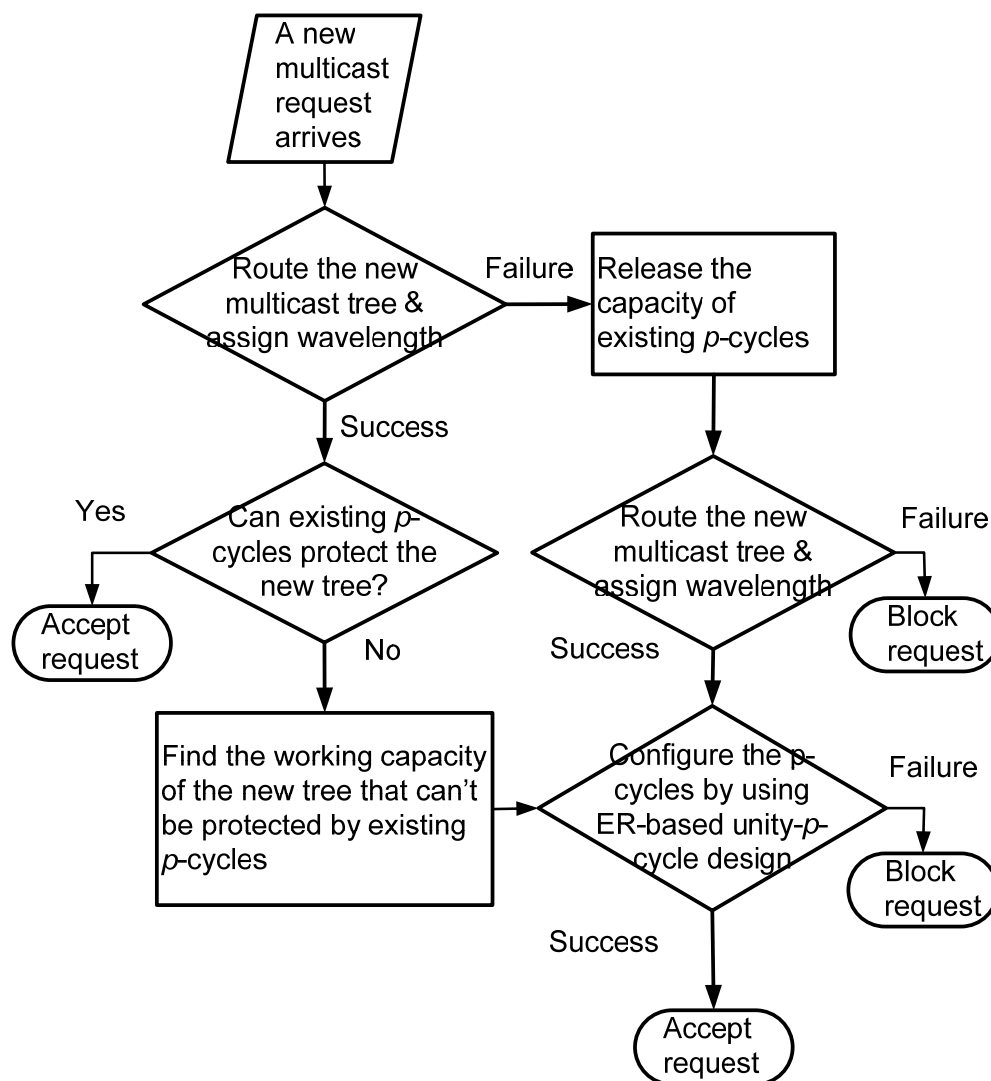


Figure 3-5: Flow chart of the Dynamic p -Cycle (DpC) algorithm for dynamic provisioning of multicast traffic

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

Upon the arrival of a new multicast request, the proposed model first tries to route the new multicast tree using either the OSPT heuristic algorithm or the ST heuristic algorithm and assign wavelengths to it. If the new multicast tree is successfully set up (The tree can be set up if there is a simple path with enough remaining free capacity from the source to each destination), the proposed model attempts to protect the new multicast tree by using the existing p -cycles. If the existing p -cycles cannot fully protect the whole new multicast tree but only part of the new multicast tree, additional new unity- p -cycles will be configured to protect the new multicast tree, if there is enough remaining free capacity for configuring cycles. If the routing of the new multicast tree is successful and all its working capacity can be protected by the existing p -cycles or by a combination of the existing p -cycles and newly configured p -cycles, the request is accepted; otherwise, it is blocked. On the other hand, if the new multicast tree cannot be set up within the remaining capacity of the network, all the existing p -cycles will be released for reconfiguration. As the old configuration of p -cycles may not fit the traffic, the purpose of the reconfiguration is to make the newly configured cycles to fit the current multicast traffic, and to accommodate the new incoming multicast request. After releasing the existing p -cycles, the proposed model attempts to route the new multicast tree, and reconfigure p -cycles to protect all the existing multicast trees as well as the new multicast tree. If this is successful, the new multicast request is accepted, otherwise it is blocked.

Upon successful setup of the new multicast request, the new multicast tree begins service. If a link in the network fails, the multicast trees traversing the failed link are rapidly switched to their corresponding pre-cross-connected p -cycles. The two adjacent nodes of the failed link handle the service restoration. The service recovery exhibits ring-like fast speed and takes about typically 30–80 ms [106, 247]. It is noted that a multicast tree will be tore down and its occupied capacity will be released upon the completion of the service of that multicast tree.

In the mean time, the corresponding p -cycles are also released if they no longer protect any multicast light trees.

3.9 Link protecting p -cycle based protected working capacity envelope (PWCE) algorithm

In [134], Grover introduced the concept of protected working capacity envelope (PWCE) for unicast traffic protection, which greatly simplifies the network management, whereas in [135-137], the performance of p -cycle based PWCE methods was evaluated for unicast traffic protection, which shows much faster computational speed, compared with the DpC algorithm. In this study, the link protecting p -cycle based PWCE model reported in [135] is extended to dynamic provisioning of survivable multicast sessions [231, 234].

Given the network topology, it first reserves some spare capacity on each edge to configure the p -cycles, in order to form an envelope of protected working capacities, by solving the ILP formulation below using the CPLEX 8.0 [248]. The remaining task is simply to route the dynamic multicast traffic in the pre-configured PWCE using either the OSPT heuristic algorithm or the ST heuristic algorithm. A multicast request is blocked if it cannot be routed in that envelope. As long as a light tree can be routed within this envelope, it is automatically protected, which greatly simplifies network management and reduces the processing complexity. Once the multicast request is accepted, the multicast tree is setup within the PWCE. When its service is over, the multicast tree is tore down and its working capacity is released. The additional notations used in the ILP formulation of the p -cycle based PWCE are shown below:

Input parameters:

H Hop limit for the selection of p -cycles

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

γ The maximal allowed variation of w_{mn}

Variables:

w_{max} The maximum constraint of w_{mn}

w_{min} The minimum constraint of w_{mn}

The ILP formulation reported in [135] is presented below:

$$\text{Objectives: Maximize } \sum_{mn \in E} w_{mn} \quad (3.21)$$

Constraints:

$$v_{mn} = \sum_{j \in C} \alpha_{j,mn} f_j \quad \forall mn \in E \quad (3.22)$$

$$w_{mn} \leq \sum_{j \in C} \beta_{j,mn} f_j \quad \forall mn \in E \quad (3.23)$$

$$w_{mn} + v_{mn} \leq t_{mn} \quad \forall mn \in E \quad (3.24)$$

$$w_{min} \leq w_{mn} \leq w_{max} \quad \forall mn \in E \quad (3.25)$$

$$\gamma = w_{max} - w_{min} \quad (3.26)$$

The objective (3.21) is to maximize the amount of protected working capacity envelope for a given network topology by selecting the most efficient candidates among all the identified p -cycles in the given network. Constraint (3.22) is to calculate the spare capacity required to be reserved in the network for the selected p -cycles. Constraint (3.23) states that the working capacity on all the links must be protected by the selected p -cycles, whereas constraint (3.24) states that the sum of the working capacity and the spare capacity on each edge must be no more than the total available capacity on each edge. Constraint (3.25) and constraint (3.26) restricts the variation of w_{mn} to control the shape of PWCE.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

The variables in the ILP formulation of SOPL are w_{mn} , v_{mn} and f_j . As there are $|E|$ links and $|C|$ cycles, the approximate number of variables for ILP formulation of p -cycle based PWCE is $2|E| + |C|$. The approximate number of constraints for ILP formulation of p -cycle based PWCE is $5|E|$.

The parameter γ ($\gamma = w_{max} - w_{min}$) is defined as the shape factor of the protected working capacity envelope, because it controls the shape of the envelope. The shape factor γ plays an important role in determining the working capacity that can be protected. Note that the shape factor γ can be varied from 0 to t_{mn} , where t_{mn} is the total available capacity on link mn . If $\gamma = 0$, the provisioned working capacities on all the links are forced to be equal, which implies the protected working capacity envelope is restricted to be flat. If $0 < \gamma < t_{mn}$, the degree of freedom for the variation of the envelope's shape increases with γ , which in turn affects the performance of the p -cycle based PWCE algorithm.

Table 3-5: Number of copies required for each unity- p -cycle in PWCE algorithm

Cycle no.	1	2	3	4	5	6
No. of copies required for the clockwise unity- p -cycle	0	0	4	4	0	2
No. of copies required for the counter clockwise unity- p -cycle	0	2	0	0	2	3

Next, the same simple network in **Figure 3-3** is used to illustrate this link protecting p -cycle based PWCE for multicast traffic protection. Assuming that each span has two fibers of 16 wavelengths per fiber, which are transmitting in opposite directions. As explained before, there are six cycles in the network of **Figure 3-3**. By solving the above ILP formulation, the

number of copies required for each cycle (which is shown in **Table 3-5**), the total provisioned working capacity (which is 174) and the total spare capacity required for p -cycle configuration (which is 78) can be obtained. The working capacity envelope (the working units provisioned on each directed link) and the spare capacity reserved on each directed link are shown in **Figure 3-6**. As long as a new multicast tree can be routed within this protected working capacity envelope, it is automatically protected.

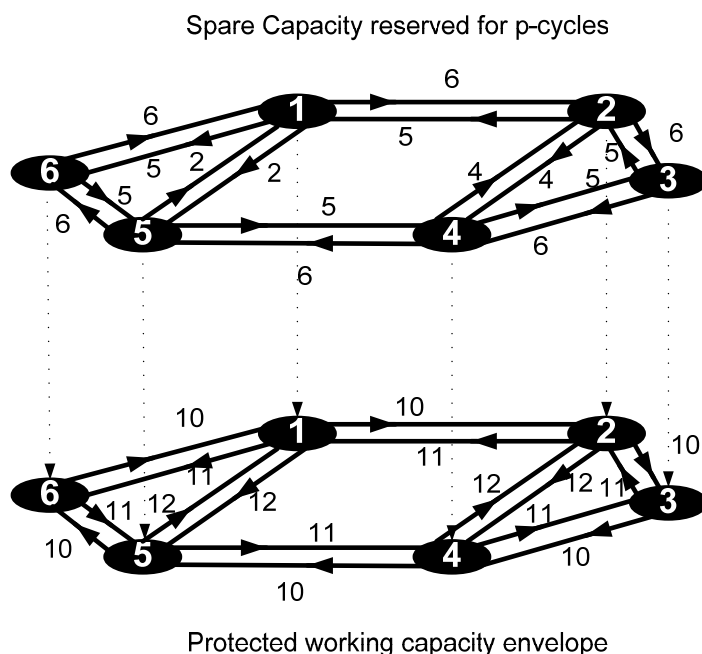


Figure 3-6: Illustration of the protected working capacity envelope and the spare capacity reserved for p -cycles for the simple network topology shown in Figure 3-3

3.10 Hybrid DpC and PWCE algorithm

In the performance evaluation section, in comparison with the existing multicast traffic protection algorithms, the DpC algorithm achieves the best blocking performance, whereas the p -cycle based PWCE algorithm offers the fastest computational speed for the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

establishment of protected multicast trees. In order to combine the merits of the two algorithms, a hybrid dynamic p -cycle and protected working capacity envelope (H-DpC-PWCE) algorithm is proposed for multicast traffic protection [231].

In the H-DpC-PWCE algorithm, a portion of the wavelength capacity on each link is assigned for the DpC protection mechanism, while the remaining capacity on each link is allocated for the p -cycle based PWCE protection mechanism. This way of partitioning the wavelength capacity can be viewed as dividing the optical layer into two sub-layers, which is shown in **Figure 3-7**, where each sub-layer is of identical capacity. Nevertheless, both sub-layers implement p -cycle protection mechanism. Hence, there are two sets of p -cycles operating in the mesh WDM network. The difference is that, within the PWCE sub-layer, a set of fixed optimal p -cycles is deployed. In contrast, the set of p -cycles in the DpC sub-layer is dynamically configured, adapting to the changing traffic. Hence, the protection mechanism is the same for both the DpC and PWCE sub-layers; the only difference is in the computation of the p -cycles to protect the incoming multicast requests in the two sub-layers.

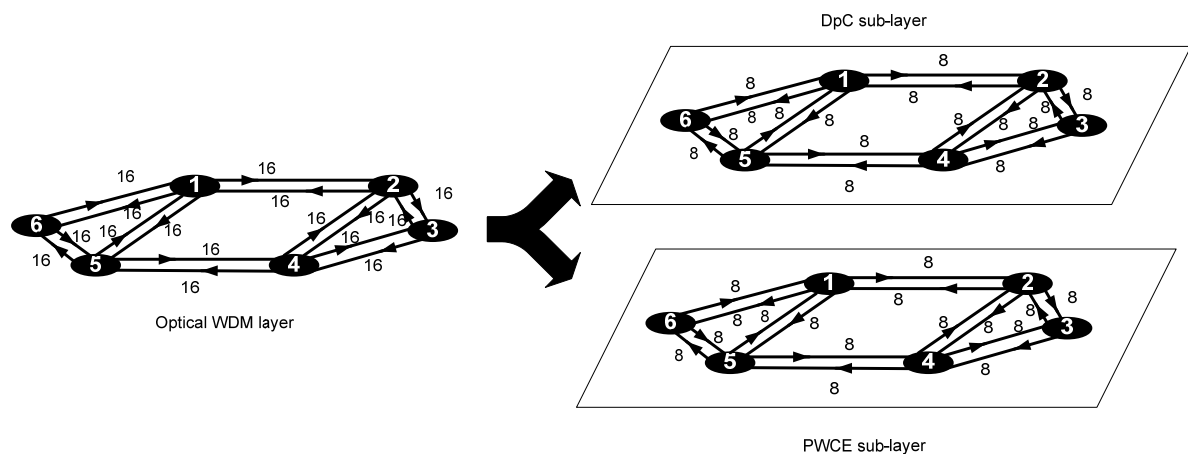


Figure 3-7: Partitioning the total deployed capacity into DpC and PWCE sub-layers

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

The flow chart of the H-DpC-PWCE algorithm is shown in **Figure 3-8**. In our simulations, we first determine the percentages of the wavelength capacity on each link assigned to PWCE sub-layer and DpC sub-layer. In our simulations, we assign half of the capacity to PWCE sub-layer, and the other half to DpC sub-layer. In practice, the capacity assigned to each sub-layer may be dynamically varied to accord with the changing traffic demand. If the traffic tends to be more uniformly distributed among the nodes, more capacity can be assigned to the PWCE sub-layer. On the other hand, if the traffic tends to be non-uniform and change unpredictably, more capacity may be assigned to the DpC sub-layer.

After the capacity of the PWCE sub-layer is determined, the proposed algorithm first reserves some spare capacity on each edge to configure the p -cycles, in order to form an envelope of protected working capacities within the PWCE sub-layer, according to the link-protecting p -cycle based PWCE algorithm described in **Section 3.9**.

When a new multicast request arrives, the proposed hybrid algorithm attempts to route it within the protected working capacity envelope in the PWCE sub-layer first. If this request cannot be accommodated within the PWCE sub-layer, it is then passed to the DpC sub-layer. Next, the hybrid algorithm tries to route the new multicast tree using remaining free capacity in the DpC sub-layer. If the new multicast tree is successfully set up, the proposed model attempts to protect the new multicast tree by using the existing p -cycles in the DpC sub-layer. If the existing p -cycles cannot fully protect the whole new multicast tree but only part of the new multicast tree, additional new unity- p -cycles will be configured in the DpC sub-layer to protect the new multicast tree, if there is enough remaining free capacity for configuring cycles. If the routing of the new multicast tree is successful and all its working capacity can be protected by the existing p -cycles or by a combination of the existing p -cycles and newly configured p -cycles, the request is accepted; otherwise, it is blocked. On the other hand, if the new multicast tree cannot be set up within the remaining capacity of the network, all the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

existing p -cycles in the DpC sub-layer will be released for reconfiguration. After releasing the existing p -cycles, the proposed model attempts to route the new multicast tree, and reconfigure p -cycles in the DpC sub-layer to protect all the existing multicast trees as well as the new multicast tree. If this is successful, the new multicast request is accepted, otherwise it is blocked.

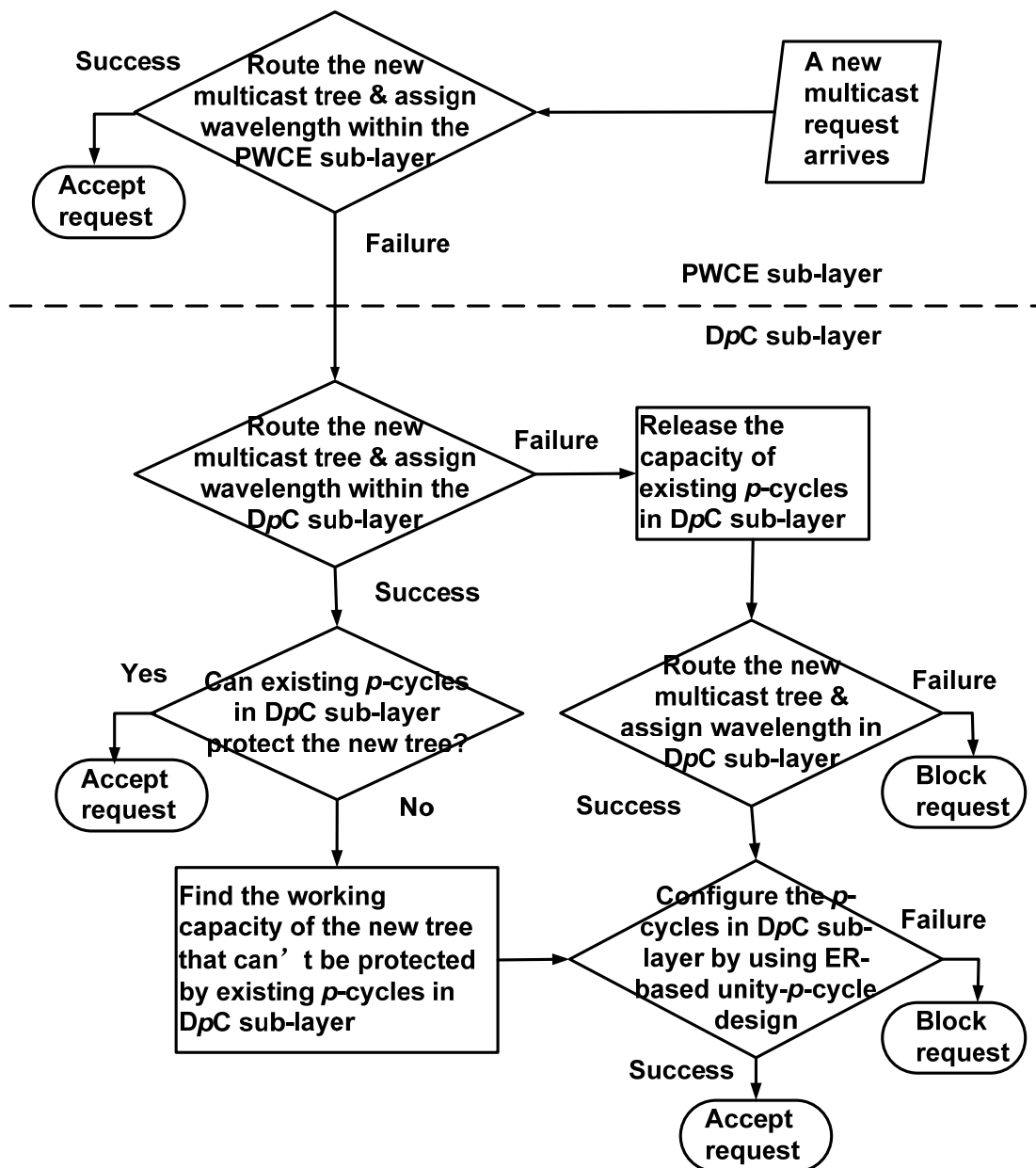


Figure 3-8: Flow chart of the H-DpC-PWCE algorithm

The key idea behind this hybrid algorithm is to combine the fast speed feature of the PWCE algorithm and the low blocking probability feature of the DpC algorithm. When the traffic load is light, most of the multicast requests could be set up quickly within the PWCE sub-layer, because the computational speed of the PWCE algorithm is the fastest. As the traffic load increases, the PWCE sub-layer will not be able to accommodate all the requests, and hence the blocking probability will increase. Accordingly, the DpC algorithm will configure a different set of p -cycles adaptively to accommodate the requests that cannot be set up in the PWCE sub-layer, according to the changing traffic.

In practical applications, one may consider to differentiate the multicast requests with different priorities. The PWCE sub-layer can be deployed to accommodate and protect higher priority requests, because the p -cycle based PWCE approach offers fast speed in the establishment of protected light trees; whereas the DpC sub-layer will be deployed to accommodate the lower priority requests.

3.11 Performance Evaluation for static traffic protection

To investigate the performance of the optical multicast protection schemes, we select the COST239 network (11 nodes and 26 links), the NSFNET network (14 nodes and 21 links) and the US backbone network (24 nodes and 43 links) as the test networks, whose average node degree (the average number of links connected to a node) are 4.727, 3 and 3.583 respectively, shown in **Figure 3-9**. The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM. One of the key criteria of static traffic protection is to minimize the total capacity (if the working capacity is fixed, the problem turns into spare capacity minimization). More wavelengths can accommodate more multicast trees. Therefore, the difference in the capacity efficiency of the algorithms can be easily observed. Hence, for performance evaluation of static traffic protection, in order to compare the difference of the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

total capacity efficiency among the algorithms, each link is assumed to have two fibers of 64 wavelengths per fiber, transmitting in opposite directions. For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node. All the ILP optimizations are solved by the ILOG CPLEX 8.0 [248].

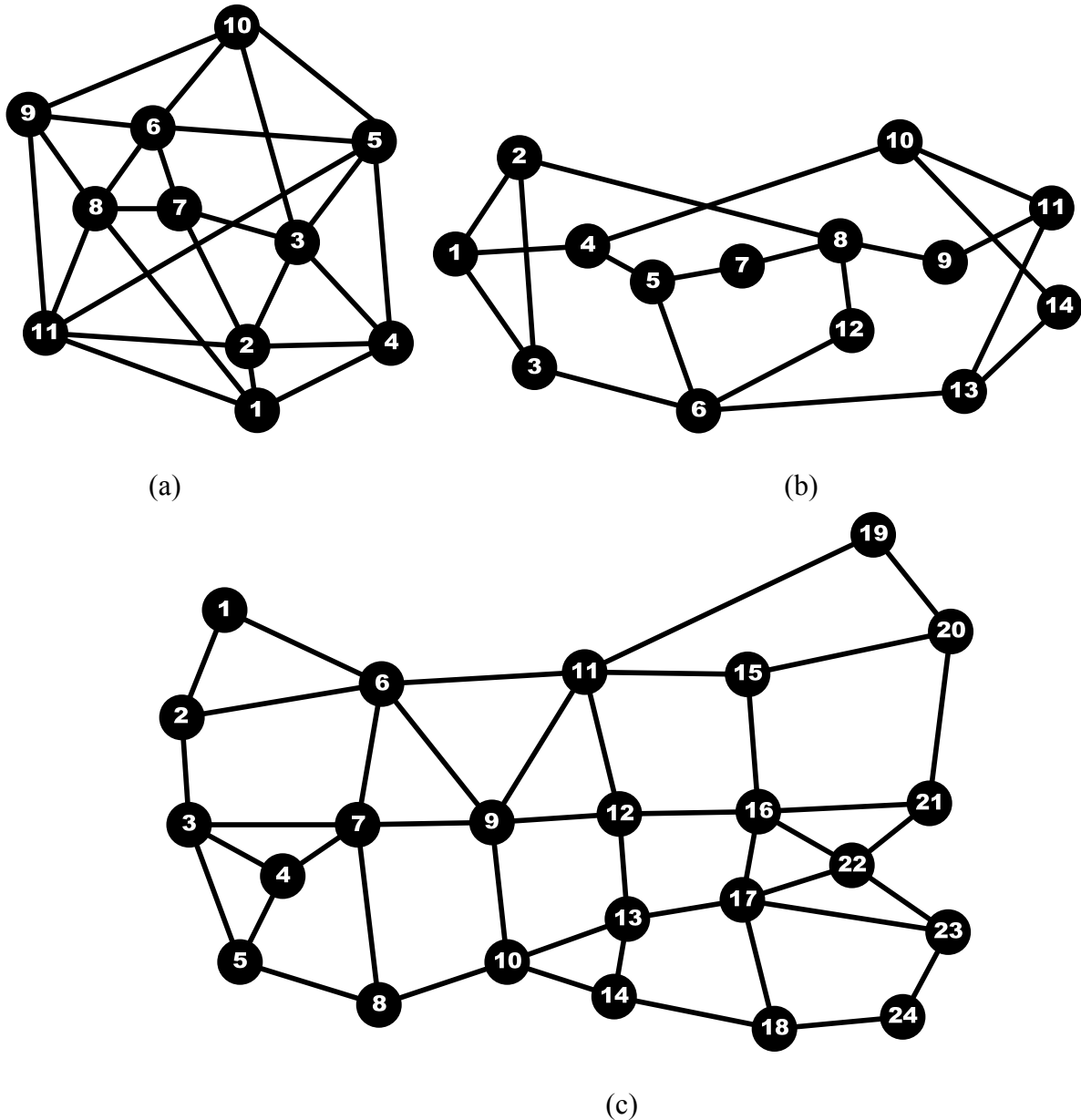


Figure 3-9: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network

Comparison of the average length of the primary working paths (ALPWP)

In this study, the average length of the primary working paths (ALPWP) is defined as the average value of the lengths of the paths connecting the source and the destinations in every routed primary working multicast trees.

For optical multicast routing, the total working capacity (or the total number of links traversed by the multicast trees) is desired to be minimized, so as to accommodate more multicast requests, and to save the scarce network wavelength capacity. However, although the total working cost is minimized, the average end-to-end cost (or the average length of the primary working paths) may not be minimized. In WDM mesh core networks, a fiber link may span thousands of kilometers, it would be desired that the optical signals traverse as few links as possible to reach the destinations, so as to reduce the number of EDFAs and regenerators required, and to reduce the noise and non-linear effects introduced by the EDFAs and fibers. Thus, the smaller the ALPWP, the better the BER performance. In **Table 3-6**, the ALPWP of the multicast trees routed by different designs in COST239 network is compared.

Table 3-6: Comparison of the ALPWP in COST239 network (k is the multicast group size)

k	1	2	3	4	5	6	7	8	9	10
OSPT	2.51	2.60	2.64	2.68	2.71	2.77	2.80	2.85	2.89	2.91
ST	2.51	2.57	2.70	2.73	2.77	2.80	2.89	2.98	2.97	3.10
JOPL	1.75	1.84	1.88	2.06	2.22	2.28	2.46	2.77	2.93	3.04
NJOPL	1.51	1.64	1.82	1.97	2.12	2.15	2.18	2.25	2.41	2.43

The results shown are the average value of 20 independent simulations. The OSPT and the ST are the heuristic routing algorithms used for p -cycle based spare capacity optimization algorithms, whereas the JOPL and the NJOPL utilize the ILP optimization for routing. It

should be noted that for the same set of multicast sessions, the working trees setup for p -cycle based spare capacity optimization algorithms and heuristic algorithms are all the same, because the same tree routing algorithm (the OSPT or the ST) is used. The reason why the ALPWP of the ST routing algorithm is longer than that of the OSPT routing algorithm (for $k \geq 3$) is that the former optimizes the overall cost of the tree, whereas the latter minimizes the end-to-end cost of for every source - destination pair. The working trees setup by the NJOPL algorithm are Steiner trees, whose working capacity is minimum; while the trees setup by the JOPL algorithm may not be Steiner trees, but the sum of the capacity reserved for the working trees and the capacity reserved for the p -cycles is minimum. As a consequence, the ALPWP of the JOPL algorithm is larger than that of the NJOPL algorithm.

Comparison of the capacity efficiency

In this subsection, only the results for the Steiner tree heuristic routing algorithm are shown, as it consume less working capacity than the open shortest path tree (OSPT) heuristic algorithm [231]. To investigate the effectiveness of the total capacity reduction of the JOPL algorithm, its performance is compared with that of the SOPL, the NJOPL and the ILP-OPP [204] algorithms. The OPP approach is selected for comparison, as it was reported to be the most efficient approach for multicast traffic protection [204].

Figure 3-10 , **Figure 3-11** and **Figure 3-12** show the performance comparison in terms of the total capacity and the spare capacity consumed in the COST239 network, the NSFNET network and the US backbone network, respectively. The results shown are the average value obtained from 20 simulation experiments. As the multicast group size increases, more links and nodes are traversed by each multicast tree and hence the working capacity required by multicast sessions would increase.

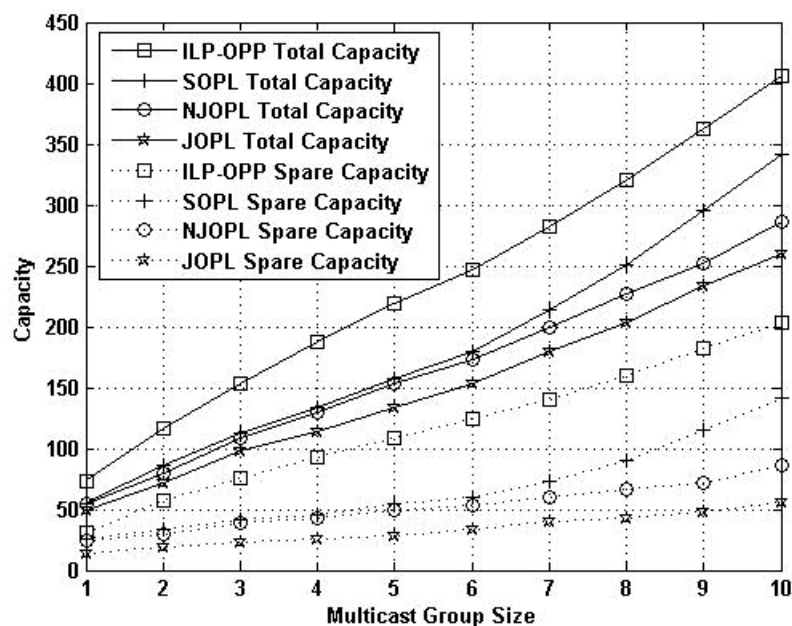
Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

Figure 3-10: Capacity comparison of optimized designs in COST239 network

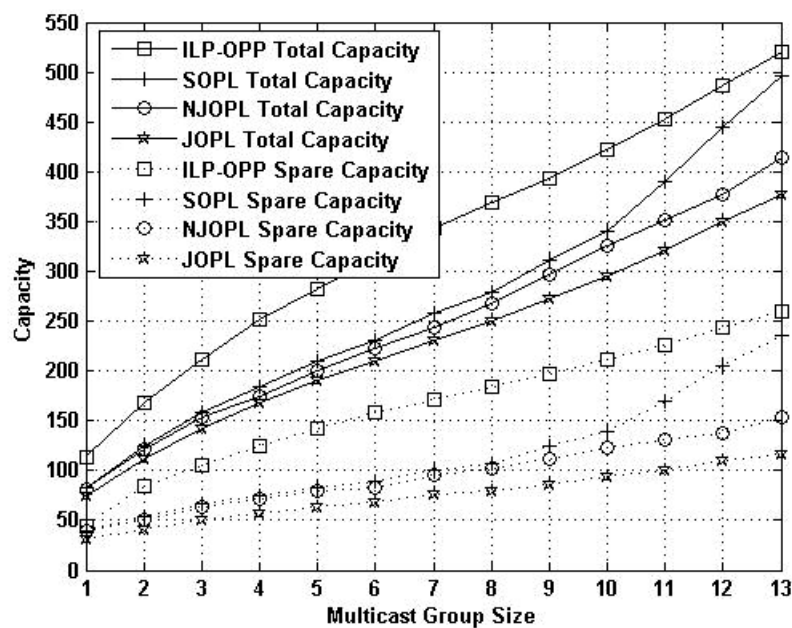


Figure 3-11: Capacity comparison of optimized designs in NSFNET network

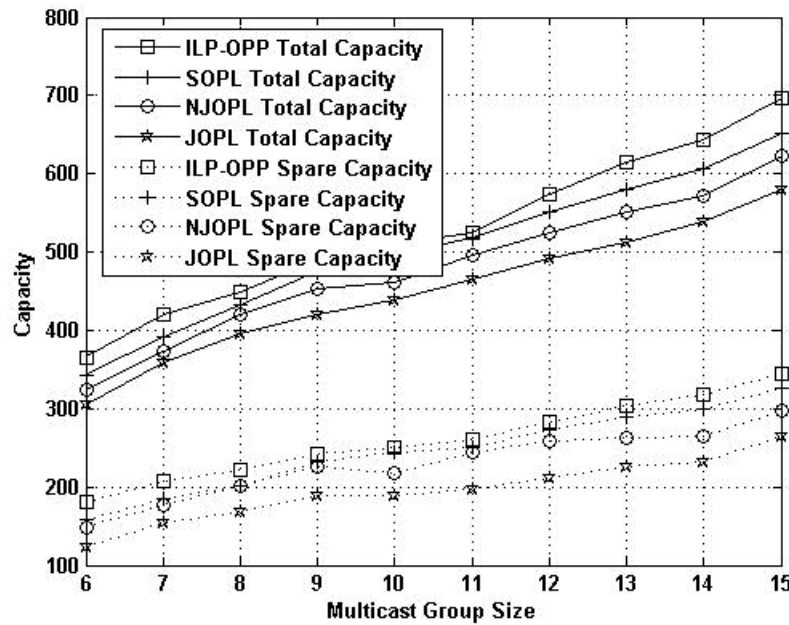


Figure 3-12: Capacity comparison of optimized designs in US backbone network

As expected, the total capacity consumed also increases with the multicast group size. For the total capacity consumption, the JOPL algorithm outperforms all other algorithm, particularly as the multicast group size increases. Compared with the NJOPL algorithm, the JOPL algorithm shows about 1% to 10% savings in total capacity consumption, which proves the advantage of the joint optimized design over the non-joint optimized design. This is because, in the JOPL algorithm, the multicast tree routing and the configuration of the p -cycles are solved simultaneously.

They must fit to each other, or in other words, the routing and wavelength assignment (RWA) of the multicast trees are chosen in conjunction with survivability considerations, so as to minimize the total capacity consumed. In the SOPL algorithm and the NJOPL algorithm, the multicast trees are routed before the spare capacity optimization of p -cycles. Hence, the p -cycle configuration is adapted to the multicast tree routing. Compared with the JOPL and NJOPL algorithms, the SOPL algorithm consumes more resources because the multicast tree

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

routing is done by the OSPT or the ST heuristic algorithm, which is not optimized. In the ILP-OPP algorithm, link disjoint path pairs can share capacity with other path pairs within the same multicast session [204]. However, the ILP-OPP algorithm does not consider sharing of the spare capacity among different multicast sessions [220]. In the proposed SOPL algorithm, there are no link-disjoint requirements between a cycle and a multicast tree, or between two multicast trees. The spare capacity of a p -cycle can be shared both within the same multicast session (intra-request sharing) and also among different multicast sessions (inter-request sharing). Hence, the SOPL algorithm performs better than the OPP. However, in unicast traffic protection, for the well known path-based protection technique – shared backup path protection algorithm (SBPP), spare capacity is shared among link-disjoint primary paths [79]. Due to the higher capacity sharing efficiency, the performance of the SBPP is superior to that of the p -cycle based link protection methods.

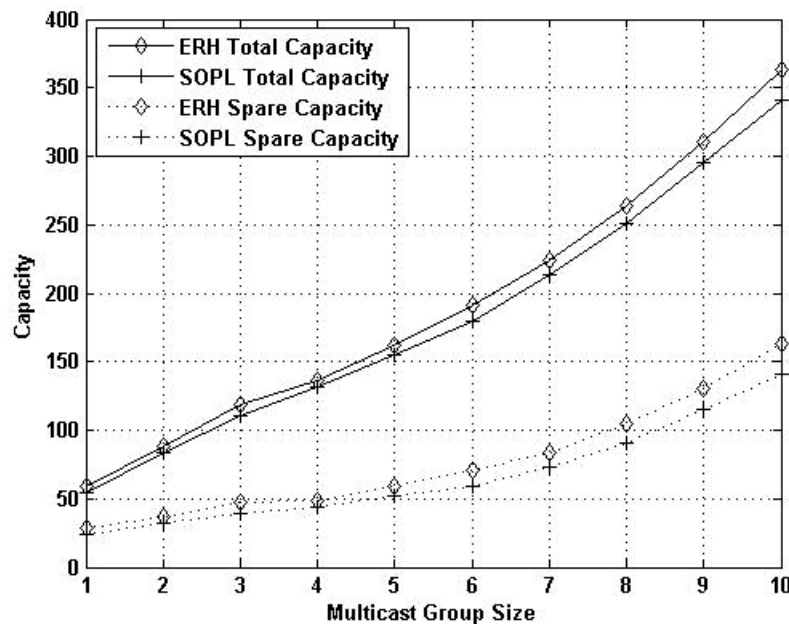


Figure 3-13: Capacity comparison of the SOPL and the ERH in COST239 network

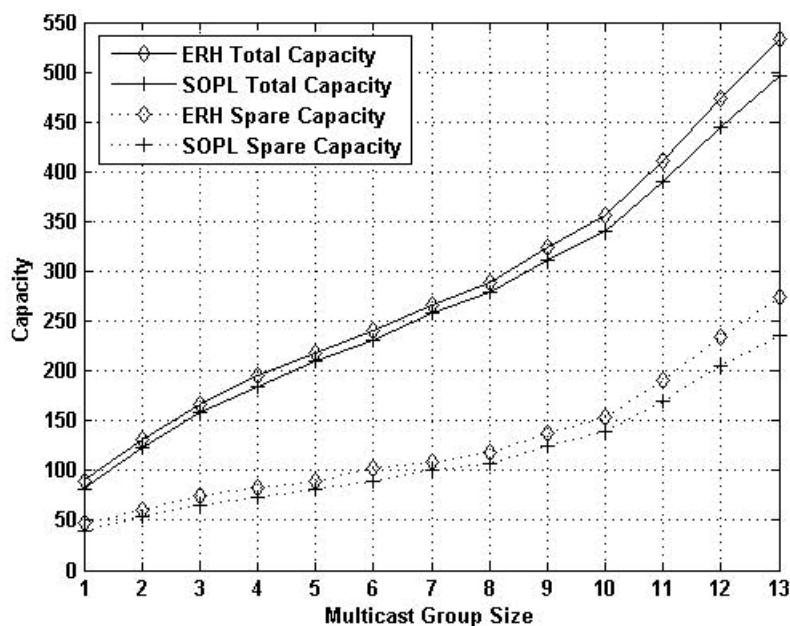


Figure 3-14: Capacity comparison of the SOPL and the ERH in NSFNET network

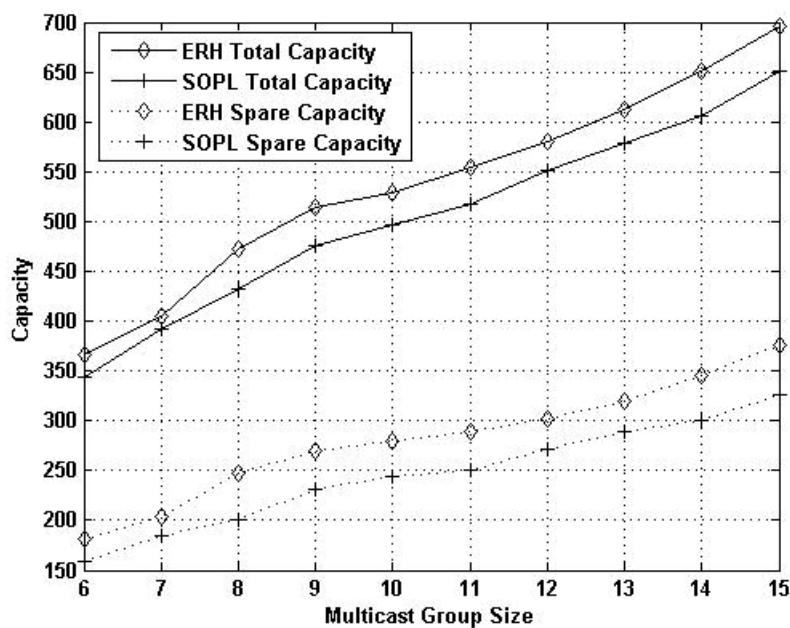


Figure 3-15: Capacity comparison of the SOPL and the ERH in US backbone network

Next, the performance of the ERH heuristic algorithm [120] is compared with that of the SOPL algorithm in COST239 network, NSFNET network and US backbone network. As

shown in **Figure 3-13**, **Figure 3-14** and **Figure 3-15**, the performance of the ERH heuristic algorithm is very close to that of the SOPL algorithm, with only about 1% to 5% increase in total capacity consumption and 2% to 10% increase in spare capacity consumption. The comparison of the total capacity required by SOPL and ERH (in three networks) are shown in **Figure 3-16** and **Figure 3-17**, respectively. As the number of nodes is different in three networks, we only provide comparison for multicast group size from 1 to 10. US backbone network has 24 nodes, while COST239 network and NSFNET network has only 11 nodes and 14 nodes, respectively. For the same multicast group size, a tree may traverse more links to reach the destinations in US backbone networks, which results in relatively higher working capacity and higher corresponding spare capacity required for p -cycle protection, compared with the COST239 network and the NSFNET network. Hence, the total capacity (for the same multicast group size) required by SOPL or ERH in US backbone network is much higher than those in the other two networks.

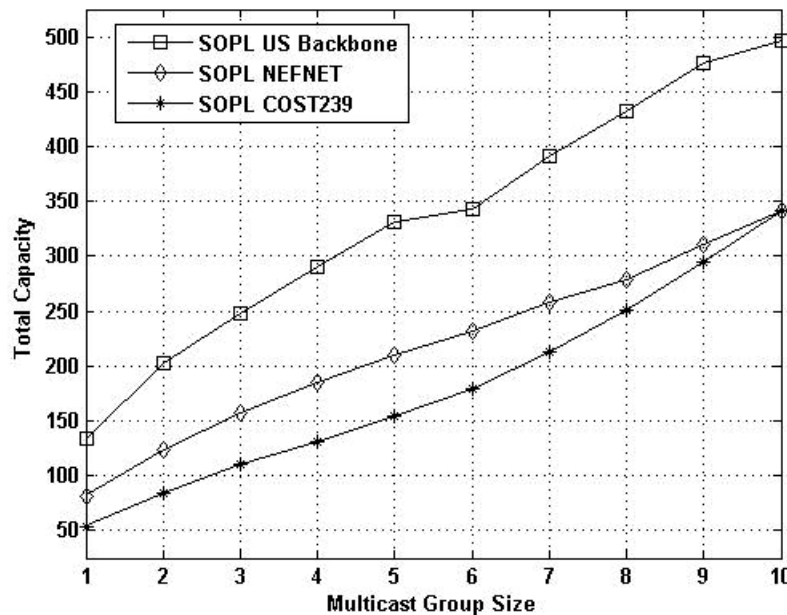


Figure 3-16: Comparison of total capacity required by SOPL in three networks

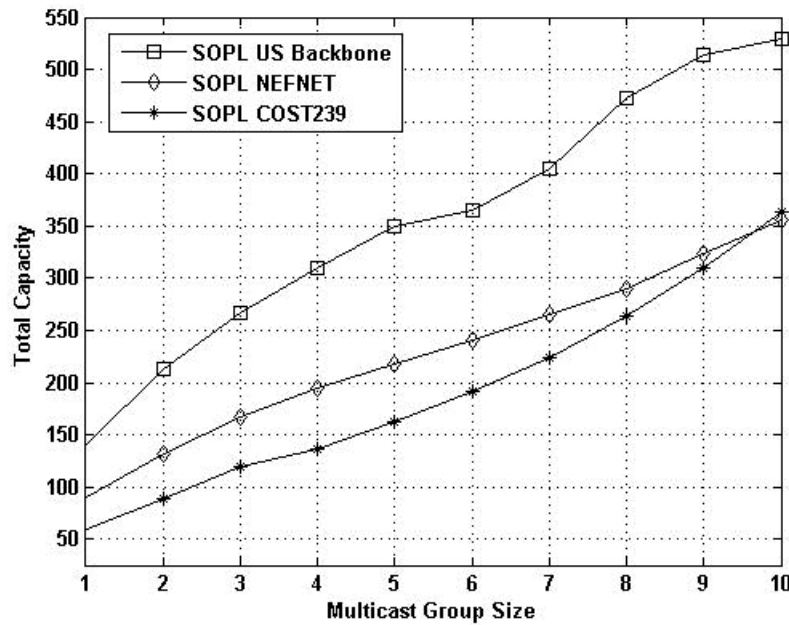


Figure 3-17: Comparison of total capacity required by ERH in three networks

Besides the capacity consumption, another important performance criterion is the computational time. **Table 3-7** compares the average total computational time consumed by the ERH heuristic algorithm with that of the optimized algorithms. As shown in **Table 3-7**, the ERH heuristic algorithm is the fastest as compared with other protection algorithms, and hence it is suitable to dynamic provisioning of survivable multicast sessions. Therefore, it is applied in the Dynamic p -Cycle (DpC) design in [234]. The ERH heuristic algorithm is much faster than the SOPL algorithm, so it is a fast approximation of the SOPL algorithm, while the SOPL algorithm serves as the bench mark for the ERH heuristic algorithm. The SOPL algorithm, whose total capacity consumption is comparable with the JOPL algorithm, is the fastest among all the ILP algorithms.

Table 3-7: Comparison of the average total computational time for setting up a multicast session in COST239 network ($k=5$)

Schemes	ERH	SOPL	NJOPL	ILP-OPP	JOPL
Time (ms)	5	15	930	1380	3310

Generally, besides the platform factor, the computational time also depends on the computational complexity of the algorithms. We can estimate the complexity of the ILP algorithms by counting the number of variables and the number of constraints, because the computational complexity increases with the number of variables and the number of constraints, which are compared in **Table 3-8**. $|N|$ is the number of nodes, $|E|$ is the number of edges, $|C|$ is the number of cycles, $|T|$ is the number of multicast sessions and k is the multicast group size. $|E|$ and $|C|$ would increase with $|N|$ and the nodal degree. Note that $|C|$ could be reduced considerably using p -cycle pre-selection strategies reported in [27], whereby the computational speed of p -cycle based algorithms would be significantly increased at the cost of consuming more spare capacity.

Table 3-8: Comparison of the number of variables and constraints in different ILP formulations

ILPs	Number of variables	Number of constraints
SOPL	$ E + C $	$3 E $
JOPL	$ E [2+(1+k) T] + C $	$4 E + k T [4+ N + E]$
NJOPL	$ E [2+(1+k) T] + C $	$5 E + k T [4+ N + E] + 1$
ILP-OPP	$ E \times (2k \times T + T + 1)$	$k \times T \times (8 + 3 E + 2 N) + 2 E $
p-cycle based PWCE	$2 E + C $	$5 E $

Because the performance of a network survivability scheme consists of both capacity consumption and computational time, there is no absolute best survivability scheme. For a particular network, if the top design objective is to achieve the least total capacity

consumption, the JOPL algorithm might be the suitable candidate. If the computational time is the primary concern, the ERH algorithm and SOPL algorithm are more suitable than the JOPL algorithm.

The study of network design with static traffic model is useful for network planning. In the static traffic model [249], light-tree requests are known in advance, so the primary light-tree and backup cycles or backup paths can be computed off-line either through ILP methods or heuristic methods to achieve optimal or sub-optimal solutions. However, demand is usually not static but changes dynamically. This means that working light-trees and also the backup cycles or backup paths will have to be established and torn down dynamically in accordance with the changing traffic demand. The ILP algorithms are time consuming and not scalable based on the current computational power and may not be suitable for on-line computation.

Therefore, dynamic service provisioning [250-254] with network survivability becomes a critical requirement for network planning and management. For dynamic traffic model, light-tree requests come and go dynamically and no knowledge of future arrivals is available at the time of provisioning current light-path requests.

3.12 Performance Evaluation for dynamic traffic protection

For dynamic traffic protection, the COST239 network, and the NSFNET network are selected as the test networks. The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM. One of the key criteria of dynamic traffic protection is the blocking probability. If the total number of available wavelengths is large, a network can support many multicast sessions simultaneously. Unless the traffic load is very high, there will not be any blockings or very few blockings. Besides, if the number of multicast requests in the network is huge (i.e., high traffic load), the amount of online calculation to route the multicast sessions and to configure the p -cycles is huge as well, which would cause the simulation time

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

to be extremely long. In contrast, if the available number of wavelengths is small, a limited number of multicast requests can be accepted, and blockings would occur. Without loss of the generality, in order to evaluate the blocking effect easily, the total number of available wavelengths on each link has to be reduced. Each link is assumed to have two fibers of 16 wavelengths per fiber, transmitting in opposite directions.

The multicast session requests are assumed to arrive with a Poisson distribution and their holding time is negatively exponentially distributed. For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node. Let λ be the arrival rate and μ be the average holding time of multicast sessions. Then, the total network traffic load is $\lambda\mu$. The total number of randomly generated multicast requests is 10^5 for each network traffic load in the simulation. For every incoming request, either if no candidate backup cycles/paths can protect the request, or if one or more links are out of capacity for either routing or protection, the current request is blocked.

When there is no free capacity on directed edge mn , its routing cost is infinity; however, when there is free capacity on directed edge mn , its routing cost is the reciprocal of the number of free wavelength units on directed edge mn . The more free wavelengths on directed edge mn , the lower its routing cost will be. The key idea behind this definition of the link routing cost is to balance the network traffic and to avoid congestions on crucial links. Because the Steiner tree problem is an NP-complete problem, in this study, the optimal shortest path tree (OSPT) heuristic algorithm [215] and the Steiner tree (ST) heuristic Algorithm [239] are applied for multicast tree routing. The OSPT heuristic algorithm tries to minimize the end-to-end cost between the source and each destination using Dijkstra shortest path algorithm (SPA) and promotes common arc-sharing among the end to end shortest paths

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

to reduce the cost of using extra arcs. In contrast, the ST heuristic algorithm attempts to minimize the overall cost of the tree.

As studied in [135], the shape factor γ can significantly affect provisioning of the protected working capacity in the p -cycle based PWCE approach. Before examining the blocking performance for multicast traffic, investigation on the effects of both the shape factor (γ) and the hop limit (H) of p -cycles on the total provisioned working capacity by link protecting p -cycle based PWCE in both the COST239 and the NSFNET networks is done firstly. For p -cycles, the length constraint of backup paths is restricted by the hop limit (H) of the p -cycles, which is the maximum limit of the p -cycle circumference (L). For link protecting p -cycles, the average length of the protection path is $L/2$ for straddling span failures, and $L-1$ for on-cycle span failures, respectively [27].

The optimized solutions are given in **Table 3-9** and **Table 3-10**, for the COST239 and the NSFNET networks, respectively. Because of the assumption that each link has two fibers of 16 wavelengths per fiber, transmitting in opposite directions, the total wavelength capacities are 832 ($16 \times 26 \times 2 = 832$) and 672 ($16 \times 21 \times 2 = 672$), for the COST239 and the NSFNET networks, respectively. As shown in **Table 3-9** and **Table 3-10**, when the hop limit increases, with the total capacity in the network being fixed, more working capacity can be protected, which implies that longer p -cycles tend to be more efficient. The shape factor (γ) also plays an important role in determining the total working capacity that can be protected. As each link is assumed to have two fibers of 16 wavelengths per fiber, transmitting in opposite directions, γ is varied from 0 to 16. The degree of freedom of the variation of shape of the envelope increases with γ . The larger the degree of freedom, the more total working capacity can be provisioned by the p -cycles. Similar to the results in [135], as γ grows, the total provisioned working capacity reaches a maximum for every hop limit of p -cycles. In both the

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

COST239 and the NSFNET networks, when there is no hop limit of p -cycles, the maximum of total provisioned working capacity emerges at $\gamma \geq 2$ and $\gamma \geq 3$, respectively.

Table 3-9: Effects of the shape factor (γ) and the hop limit (H) of p -cycles on the total provisioned working capacity in the p -cycle based PWCE in the COST239 network

$\gamma \backslash H$	5	6	7	8	9	10	11
0	520	572	624	624	624	624	624
1	571	620	640	649	657	664	672
2	603	629	642	649	658	668	682
3	607	628	642	652	659	668	682
≥ 4	608	629	642	652	659	668	682

Table 3-10: Effects of the shape factor (γ) and the hop limit (H) of p -cycles on the total provisioned working capacity in the p -cycle based PWCE in the NSFNET network

$\gamma \backslash H$	6	7	8	9	10	11	12	13	14
0	210	336	420	420	420	420	420	420	420
1	246	336	447	452	456	458	458	458	458
2	278	384	451	467	456	476	483	486	486
3	307	393	451	468	472	478	486	487	487
4	329	397	456	469	472	478	486	487	487
5	350	401	456	469	472	478	486	487	487
≥ 6	357	402	456	469	472	478	486	487	487

Simulations were carried to investigate the effects of the shape factor γ and hop limit H on the blocking probability for the dynamic protection provisioning of multicast sessions. γ is

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

varied from 0 to 4 in the COST239 network, and from 0 to 6, in the NSFNET network. The hop limit is varied from 5 to 11 in the COST239 network, and from 6 to 14 in the NSFNET network. However, the multicast group size (k) is fixed at 5, and the offered traffic is fixed to be 55E and 28E in the COST239 and the NSFNET networks, respectively.

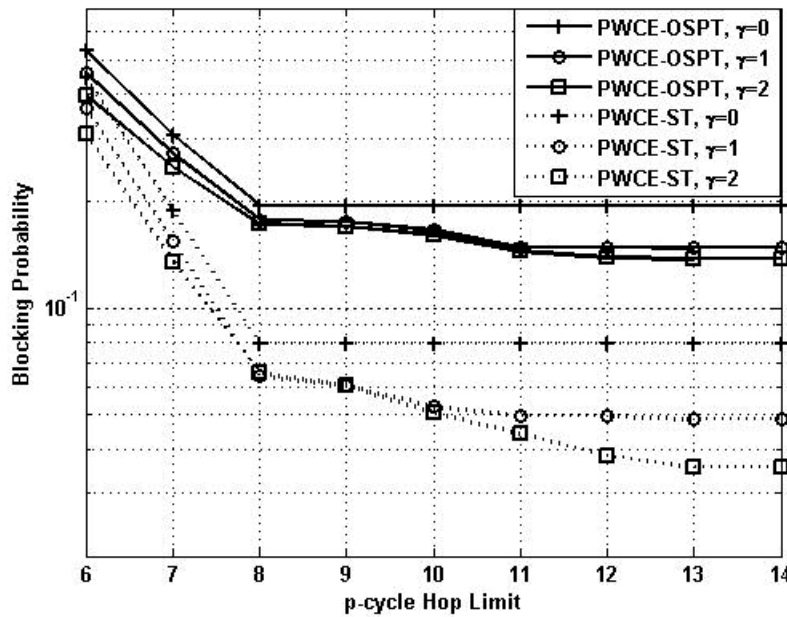
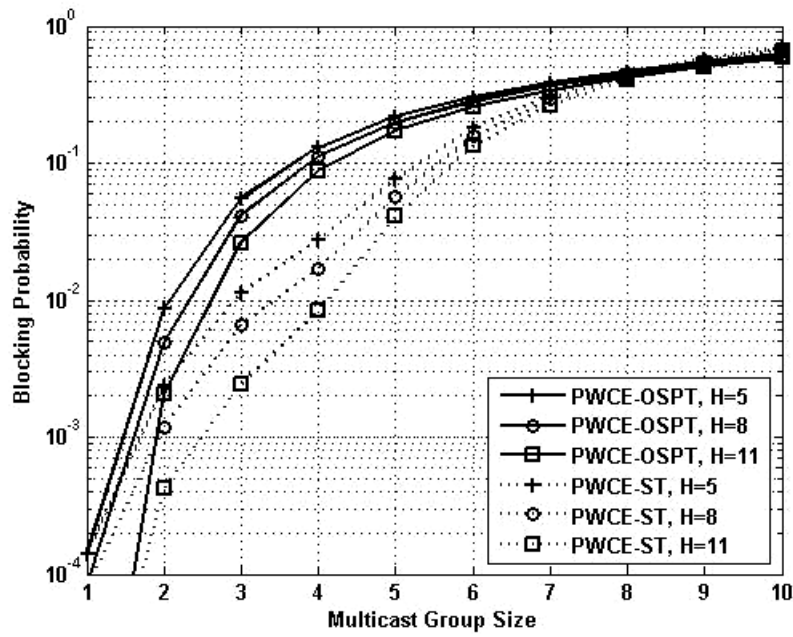
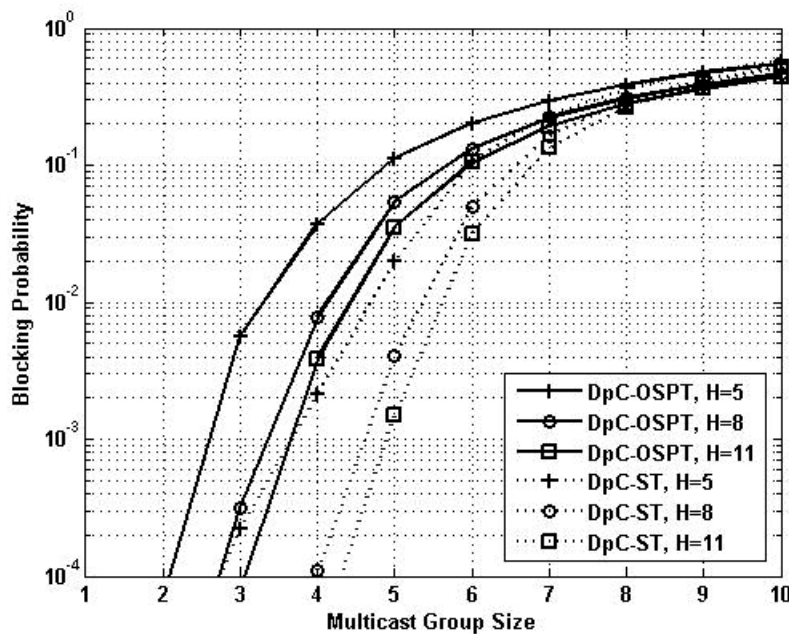


Figure 3-18: Effects of the shape factor and the hop limit on the blocking probability of p -cycle based PWCE in the NSFNET network

Only selected results for the NSFNET network were shown in **Figure 3-18** to conserve the space, because similar trends were observed for the COST239 network. Simulation results show that the blocking probability decreases with the increase of the hop limit. **Figure 3-18** also shows that the blocking performance of the protection algorithms is closely related to the routing policy. Dynamic multicast sessions routed by the ST heuristic algorithm experience lower blocking probability than those routed by the OSPT heuristic algorithm, because the ST heuristic algorithm computes near-optimal minimum cost trees, using less working capacity.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

(a)



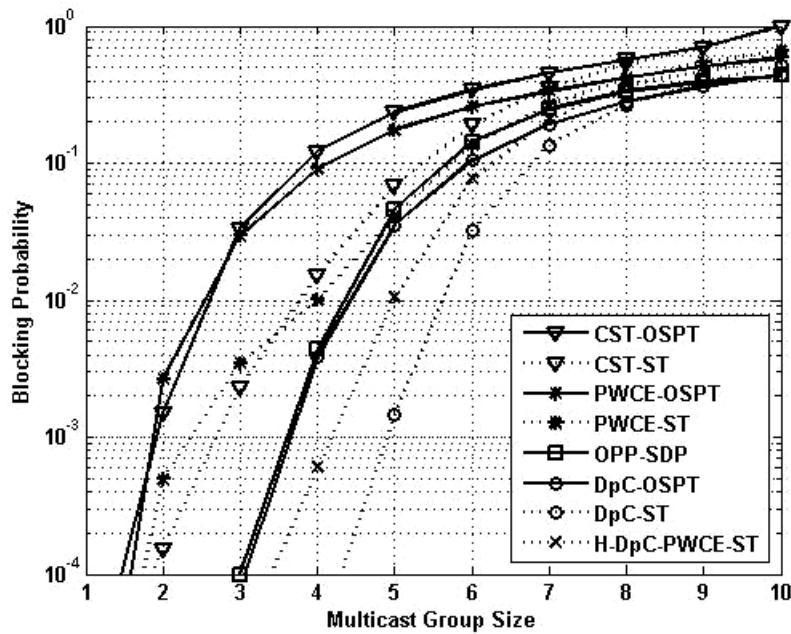
(b)

Figure 3-19: Effects of the hop limit on the blocking probability in p -cycle based multicast protection algorithms in the COST239 network (Offered traffic is fixed at 55E and γ is fixed at 4): (a) the p -cycle based PWCE, and (b) the dynamic p -cycle (DpC).

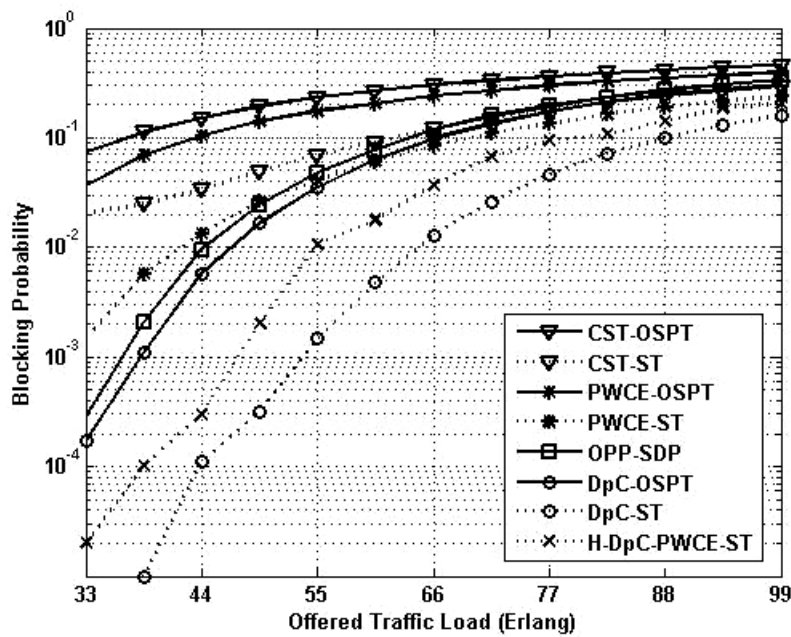
Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

As shown in **Table 3-9** and **Table 3-10**, the total provisioned working capacity in p -cycle based PWCE increases with γ until it reaches the maximum. Simulation results have shown that, for most of the cases, the blocking probability decreases, as the total provisioned working capacity increases (when γ increases).

Simulations were also carried out to investigate the effects of hop limits of p -cycles in both the COST239 network (the offered traffic is fixed at 55 E and γ is fixed at 4) and the NSFNET network (offered traffic is fixed at 28 E and γ is fixed at 6), for both the DpC and the p -cycle based PWCE algorithms. The hop limit was varied from 5 to 11 in COST239 network, and from 6 to 14 in the NSFNET network. Only selected results in the COST239 network are shown in **Figure 3-19** to conserve space, because similar trends were observed in the NSFNET network. As shown in **Figure 3-19**, for both the DpC and the p -cycle based PWCE algorithms, the blocking probability decreases as the hop limit increases. This is because, as the hop limit increases, longer and more efficient p -cycles are selected, which are able to protect more links. Although longer p -cycles require more spare capacity, the working capacity that can be protected per unit spare capacity is increased (or in other words, higher efficiency ratio (ER) [120] for longer p -cycles), which leads to lower blocking probability. Besides, the blocking probability increases, as multicast group size increases. This is because larger trees occupy more working capacity and also more spare capacity to protect. In other words, increase the multicast group size is logically equivalent to increase the network traffic. Again, as ST heuristic algorithm consumes less working capacity for routing multicast trees (because ST heuristic algorithm attempts to minimize the overall cost of the trees), compared with the OSPT heuristic algorithm, the overall blocking probability is lower for protection algorithms with ST routing algorithm.

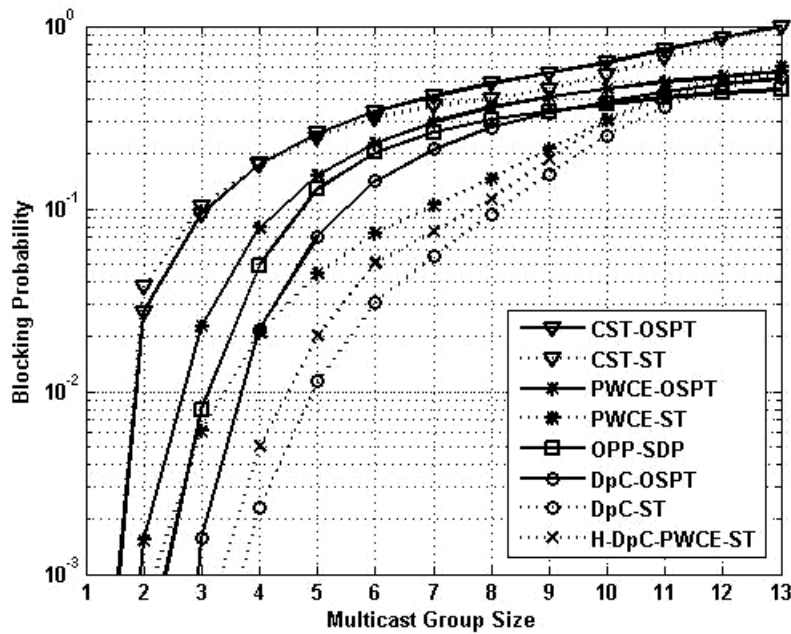


(a)

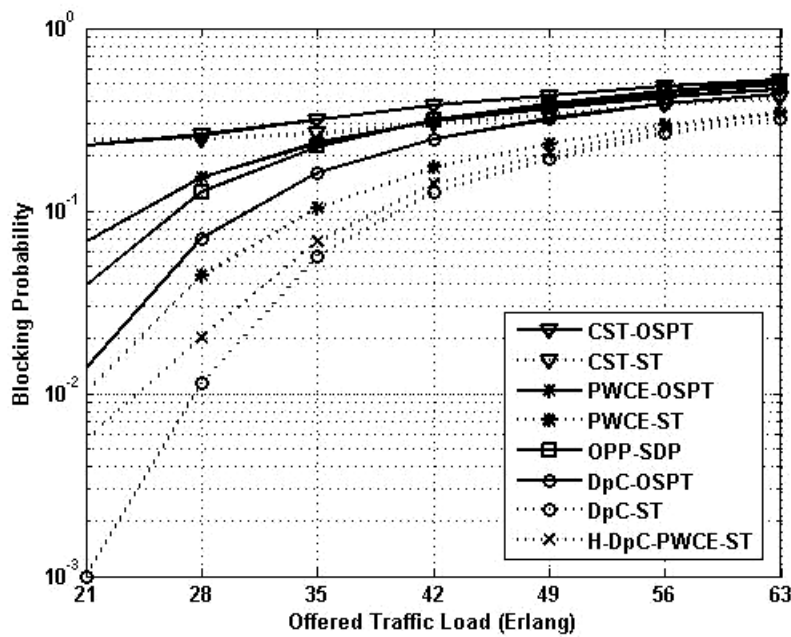


(b)

Figure 3-20: Comparison of blocking performance for various protection algorithms in the COST239 network: (a) the offered network traffic is fixed at 55 Erlang, and (b) the multicast group size is fixed at 5.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

(a)



(b)

Figure 3-21: Comparison of blocking performance for various protection algorithms in the NSFNET network: (a) the offered network traffic is fixed at 28 Erlang, (b) the multicast group size is fixed at 5.

The OPP-SDP algorithm [204] and also the cross sharing tree (CST) algorithm [202] were chosen for comparison with the p -cycle based algorithms. Among them, the OPP-SDP algorithm is reported as the most heuristic efficient technique for dynamic multicast traffic protection for link failure recovery, since it achieves the lowest blocking probability [204]. Note that the CST algorithm is much more efficient than the ADT algorithm, since it allows multiple link disjoint primary trees to share the backup spare capacity.

Figure 3-20 and **Figure 3-21** compare the blocking probability for various protection algorithms for the COST239 and the NSFNET networks, respectively. The hop limit for the p -cycle based protection approaches was not set for this study, in order to optimize the performance. For the p -cycle based PWCE, γ was set to be 2 and 3 for the COST239 and NSFNET networks, respectively.

As expected, the blocking probability increases with the multicast group size. That is because, for the same offered network traffic load, multicast traffic consumes more working wavelength capacity (and therefore higher network traffic) as well as more spare protection capacity, as the multicast group size increases. Also, as the offered traffic load increases, the blocking probability increases as well. As the total capacity on each link is limited, the number of successfully set-upped multicast sessions that the network can hold concurrently within a certain period of time is limited. As shown in **Figure 3-20** and **Figure 3-21**, the p -cycle based multicast protection algorithms (the DpC algorithm, the H- DpC -PWCE algorithm and the PWCE algorithm) achieve much better blocking performance than the existing OPP-SDP and the CST algorithms. The DpC algorithm yields the lowest blocking probability among all the protection algorithms, because it attempts to introduce new p -cycles or adjust the configuration of existing p -cycles, when each incoming request arrives, in order to adapt to the traffic changes. As the traffic load decreases or the multicast group size decreases, the advantage of the DpC algorithm over other protection algorithms gets larger.

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

Although the PWCE algorithm is the fastest among the three p -cycle based algorithms, it has the worst blocking performance among the three, because the set of p -cycles is fixed, which cannot adapt to the traffic changes. With the same routing algorithm, the blocking performance of the H-D p C-PWCE algorithm is better than that of the PWCE algorithm, but worse than that of the D p C algorithm. It will be shown that the H-D p C-PWCE algorithm has the moderate computational speed among the three shortly. The H-D p C-PWCE algorithm combines the fast speed feature of the PWCE algorithm and the low blocking probability of the D p C algorithm. With the layered structure, the H-D p C-PWCE algorithm is able to differentiate the services with different priorities. It is also identified that the blocking performance of the same protection algorithm is worse in NSFNET network, compared with that in COST239 network. This is because the lower nodal degree imposes more constraints on the routing of multicast trees and configuration of p -cycles.

This study has found that the main reasons for the much better blocking performance of the p -cycle based protection algorithms are attributed to the facts: (i) there are no disjoint constraints between the selected p -cycles and the multicast light trees to be protected; (ii) the selected p -cycles are the most efficient p -cycles. It is noted that the capacity efficiency of p -cycles comes from the protection of straddling spans in addition to the on-cycle spans [106]. Compared with the existing path and tree based protection approaches, the link-protecting p -cycle based protection approach provide the freedom of routings as well, since the routing of the multicast trees and the configuration of p -cycles can be separated. Besides the great simplification of network management pointed out earlier, the p -cycle based PWCE algorithm achieve comparable or even better performance than the OPP-SDP algorithm, when Steiner tree heuristic routing algorithm is applied and traffic load is relatively large.

It is noted that if the multicast group size is reduced to one, multicast traffic transforms to unicast traffic. Also, both OSPT and ST routing algorithms used in multicast routing become

the Dijkstra shortest path algorithm (SPA) used in unicast routing. The performance of the various protection algorithms were compared, when all traffic is unicast. To evaluate the blocking performance for the unicast case, the total traffic load was varied from 220E to 418 E in the COST239 network. Simulation results are shown in **Figure 3-22**.

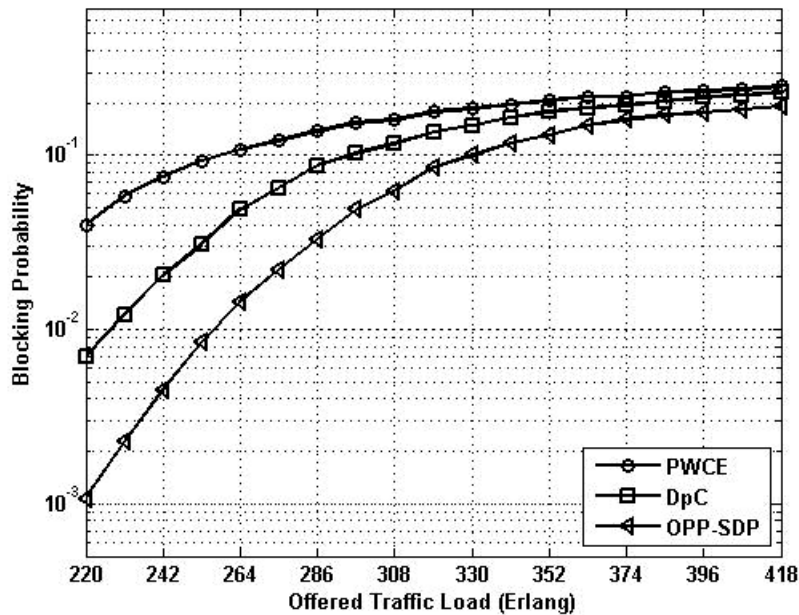


Figure 3-22: Comparison of blocking performance in the COST239 network for the unicast traffic case

It is found that in the unicast case, the OPP-SDP algorithm outperforms the p -cycle based protection algorithms, which is different from the multicast case. This conclusion is agreeable with our earlier work in [132, 135], where the shared backup path protection (SBPP) algorithm was shown to achieve better blocking performance than the p -cycles based protection algorithms for unicast traffic. It has been proven theoretically that p -cycles have the same lower bound ($1/(\bar{d}-1)$, where \bar{d} is the average nodal degree) on the redundancy as mesh based link protection approaches [107], but the lower limit is only achieved when Hamiltonian cycles are chosen for protection in the given network topology [107]. Hence, for

Chapter 3: Link-Protecting p -Cycle Based Optical Multicast Protection Approach

unicast traffic protection, the performance of p -cycle based link protection approaches can only approach mesh based protection approaches like SBPP, and never surpass. For multicast traffic protection, the key reason why OPP-SDP algorithm is inferior to DpC algorithm, is because, there is only intra-request spare capacity sharing in OPP-SDP, whereas DpC allows both intra-request spare capacity sharing and inter-request spare capacity sharing.

Table 3-11: Comparison of the average total computational time per multicast session for different multicast protection schemes in the COST239 network. (The offered network traffic $\lambda\mu$ is fixed at 55 Erlang, and the multicast group size k is fixed at 5.)

Schemes	CST	OPP-SDP	DpC	PWCE	H-PWCE-DpC
Time(ms)	53	23	18	5	9

The comparison of the average computational time for the establishment of a successful multicast light tree under different protection algorithms is shown in **Table 3-11**. The p -cycle based PWCE algorithm is the fastest, because it only requires to route the new request within the offline-computed PWCE. It should be noted that, after a link failure, the CST algorithm and the OPP-SDP algorithm require a complex signaling process to configure multiple nodes along the primary/protection trees/paths, so that either whole or partial traffic is switched to the backup tree/path through complicated reconfigurations [205]. Hence, they require a much longer restoration time. In contrast, for the p -cycle based algorithms, the p -cycles are preconfigured (i.e., pre-cross-connected), and only two end-nodes of the failed link perform the protection switching, thereby achieving fast restoration speed (typically 30-80 ms) [106, 247].

3.13 Conclusions

Several algorithms were proposed and investigated for link protecting p -cycle based multicast traffic protection approach, for both static traffic and dynamic traffic in optical mesh WDM networks. For static traffic, the newly proposed JOPL algorithm outperforms all other multicast traffic protection algorithms. The SOPL algorithm is the fastest in the computational speed among all the optimized designs and serves as the bench mark for the ERH algorithm for capacity efficiency; whereas the ERH algorithm offers fastest computational speed among all algorithms, and therefore was applied in DpC algorithm for dynamic traffic protection.

For dynamic provisioning of survivable multicast sessions, the simulation results showed that, although in unicast traffic protection, the blocking performance of link protecting p -cycle based protection algorithms is worse than the OPP-SDP algorithm, the link protecting p -cycle based algorithms achieve much better blocking performance than the existing multicast protection algorithms for multicast traffic protection. Among all multicast protection algorithms, the newly proposed DpC algorithm achieves the lowest blocking probability, whereas the p -cycle based PWCE scheme offers the fastest computational speed. Also, because the p -cycles are preconfigured, they offer fast restoration speed (typically 30-80 ms). The effects of the shape factor and the hop limit on the performance of p -cycle based PWCE algorithm for multicast traffic were studied as well. Simulation results showed that the blocking probability decreases when the hop limit increases. It also showed that, in general, the larger the shape factor γ , the lower the blocking probability.

Chapter 4. Tree-Protecting p -Cycle Based Multicast Protection Approach

4.1 Introduction

The two main types of network failures are link failures and node failures. Up to now, most research in the area of optical multicast traffic protection has been focused on link failure recovery, due to its predominance. In Chapter 3, the link-protecting p -cycle-based protection approach was extended from unicast traffic protection to multicast traffic protection. Although the proposed algorithms of the link-protecting p -cycle-based protection approach outperform the algorithms of the existing multicast traffic protection approaches for link failure recovery, they cannot cope with node failure recovery.

Although node failures are less frequent, the impact is more severe, since a single node failure is logically equivalent to several concurrent link failures. In the optical layer, the objective of the node failure recovery is to restore transit flows that pass through the failed node. The source flows and the sink flows cannot be restored by any protection algorithm. Both node failures and link failures are capricious in optical networks. It is difficult to predict when and where a failure will occur in a network. Without an efficient and fast recovery mechanism, a network failure can lead to severe disruption to network services and calamitous loss to end users.

In a network, it might be less cost-effective to implement dedicated protection approaches for separate link failure recovery and node failure recovery. Hence, a combined node and link failure recovery approach is desirable and very crucial to network survivability.

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

Some previous studies [36, 139, 144, 255] have addressed the problem of combined node and link failure recovery for unicast traffic protection. In the failure independent path-protecting (FIPP) p -cycle approach [36] and the flow p -cycle approach [139], the paths/segments have to be node-disjoint to share a copy of a p -cycle for combined node and link failure recovery. The node-encircling p -cycle (NEPC) approach [143] was reported for router failures in the IP layer. However, applying the NEPC approach in the WDM layer for combined node and link failure recovery is not so cost-effective [144].

To our best knowledge, little work has been done on combined node and link failure recovery for optical multicast traffic. Motivated by the significance of both the link failure recovery and node failure recovery to the optical multicast, the capability of combined node and link failure recovery of p -cycles is worthwhile and interesting to be proven in this study. Several p -cycle based optical multicast protection approaches for combined node and link failure recovery were developed. This chapter presents the proposed tree-protecting p -cycle based approach [229, 230, 232], which can provide combined node and link failure recovery.

This chapter is organized as follows. Section 4.1 gives the background and motivation of developing the tree-protecting p -cycle based multicast protection approach. Section 4.2 introduces some additional notations. Section 4.3 explains the protection mechanism of tree-protecting p -cycle based approach, whereas Section 4.4 discusses the spare capacity optimization algorithm of p -cycle based tree protection (SOPT), while Section 4.5 presents the efficiency score based heuristic algorithm of p -cycle based tree protection (ESHT). Section 4.6 elaborates the optimal path pair (OPP) based approach extended for combined node and link failure recovery. Section 4.7 investigates the proposed algorithms in static traffic environment, while Section 4.8 investigates the proposed algorithms in dynamic traffic environment. Lastly, the conclusions are given in section 4.9.

4.2 Additional notations

The general notations used in this study have been introduced in Section 3.2. Additional notations used in this chapter were introduced below:

Sets

D_{DTS} Set of disjoint tree sets (DTSs), indexed by \mathfrak{R}

Input parameters

$Y_{j,\mathfrak{R}-DTS}$ It is 1 if cycle j can protect DTS \mathfrak{R} ; 0 otherwise.

$Z_{\mathfrak{R}-DTS}^\tau$ It is 1 if DTS \mathfrak{R} contains tree τ ; 0 otherwise.

Variables

$f_{j,\mathfrak{R}-DTS}$ It is 1 if cycle j is selected for protecting DTS \mathfrak{R} ; 0 otherwise.

4.3 Protection mechanism of the tree-protecting p -cycle based approach

Similar to FIPP p -cycles [36] protecting light paths on an end-to-end basis, tree protecting p -cycles protect light trees on an end-to-end basis, instead of protecting each node and link [229, 230, 232]. For the case of link failure recovery, the same copy of a p -cycle (a unity p -cycle) can protect multiple mutually link-disjoint trees, as long as these trees are arc-disjoint with the cycle and their source and destination nodes are all on-cycle. For the case of

combined node and link failure recovery, in addition to satisfying the constraints on link failure recovery, trees that can share the same copy of a p -cycle should be mutually node-disjoint and they are also node-disjoint with the protection path provided by the cycle. Note that the node-disjoint constraints are applied to the intermediate nodes of the trees only. If a link/node in the network fails, the neighbor nodes of the failed link/node inform the source and the destination nodes of the trees affected, which will handle the service recovery then. The multicast traffic carried by the multicast trees traversing the failed link/node can be rapidly switched to their corresponding p -cycles, because p -cycles are preconfigured.

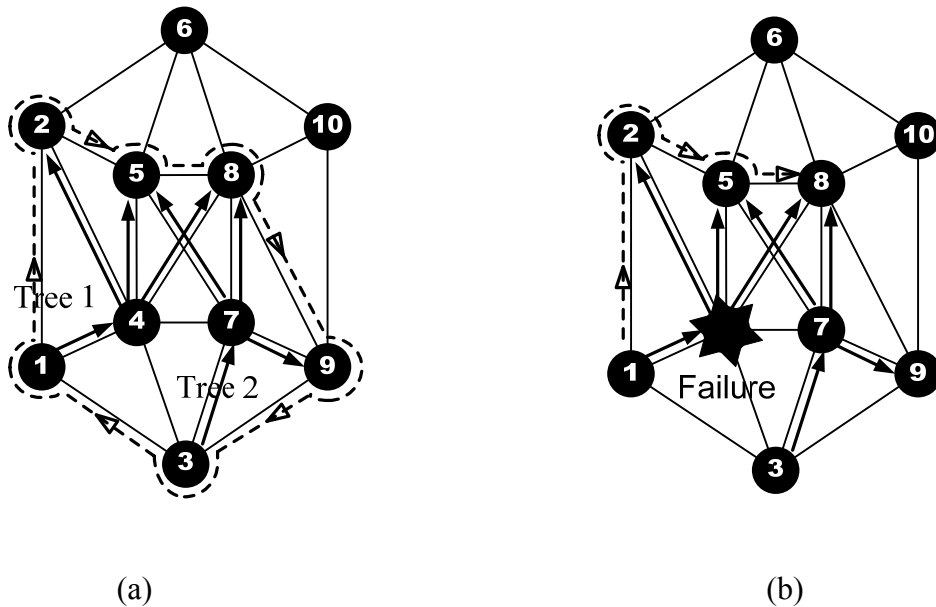


Figure 4-1: An example illustrating the tree-protecting p -cycle approach

An example shown in **Figure 4-1** illustrates that a unity tree-protecting p -cycle ($1 \rightarrow 2 \rightarrow 5 \rightarrow 8 \rightarrow 9 \rightarrow 3 \rightarrow 1$ shown in dashed line) protecting two multicast trees (tree 1 and tree 2 shown in solid lines for Φ_1 and Φ_2 : ($\Phi_1 = \{1, 2, 5, 8\}$ and $\Phi_2 = \{3, 5, 8, 9\}$)) for combined node and link failure recovery. Upon the failure of node 4 (or the failure of link $1 \rightarrow 4$, or link $4 \rightarrow 2$, or link $4 \rightarrow 5$, or link $4 \rightarrow 8$) of tree 1, the cycle provides a protection path $1 \rightarrow 2 \rightarrow 5 \rightarrow 8$, which

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

traverses all the three destination nodes of the tree 1. The similar process can be applied to failures on tree 2.

It should be noted that the proposed tree-protecting p -cycle based approach is different from the one ring for one multicast session (OFO) approach and the one ring for all multicast sessions (OFA) approach proposed in [214]. In the OFO approach, a ring is dedicated to protect a single multicast session. In the OFA approach, although only one ring is chosen for protecting all multicast sessions, this ring has to be large enough to cover all the nodes of all multicast sessions, e.g., Hamiltonian rings. In addition, as many copies of the ring as the number of the multicast sessions may be required, and each copy may be used to protect only one multicast session (effectively a dedicated 1:1 protection approach). Therefore, in both the OFO and the OFA approaches, the mutually-link-disjoint requirements among the multicast trees are not considered, and hence spare capacity cannot be efficiently utilized. In the proposed SOPT approach, a copy of a unity- p -cycle can be shared by multiple mutually disjoint trees, and hence the spare capacity is efficiently utilized.

Tree partition algorithm (TPA)

It may be difficult to find candidate p -cycles to protect large trees, especially in sparse networks, because of the disjoint constraints, and tree's source and destination nodes must be on-cycle [232]. To deal with this problem, a tree partition algorithm (TPA) [229] is developed. If and only if no cycle can be identified to protect a large multicast tree, it is then partitioned into several smaller sub-trees.

In the TPA algorithm, firstly, the disjointedness of the tree with each candidate cycle is checked. If they are not disjoint, the common intermediate nodes are recorded. After the check, for each intermediate node, its records are summed. The trouble node in a tree is

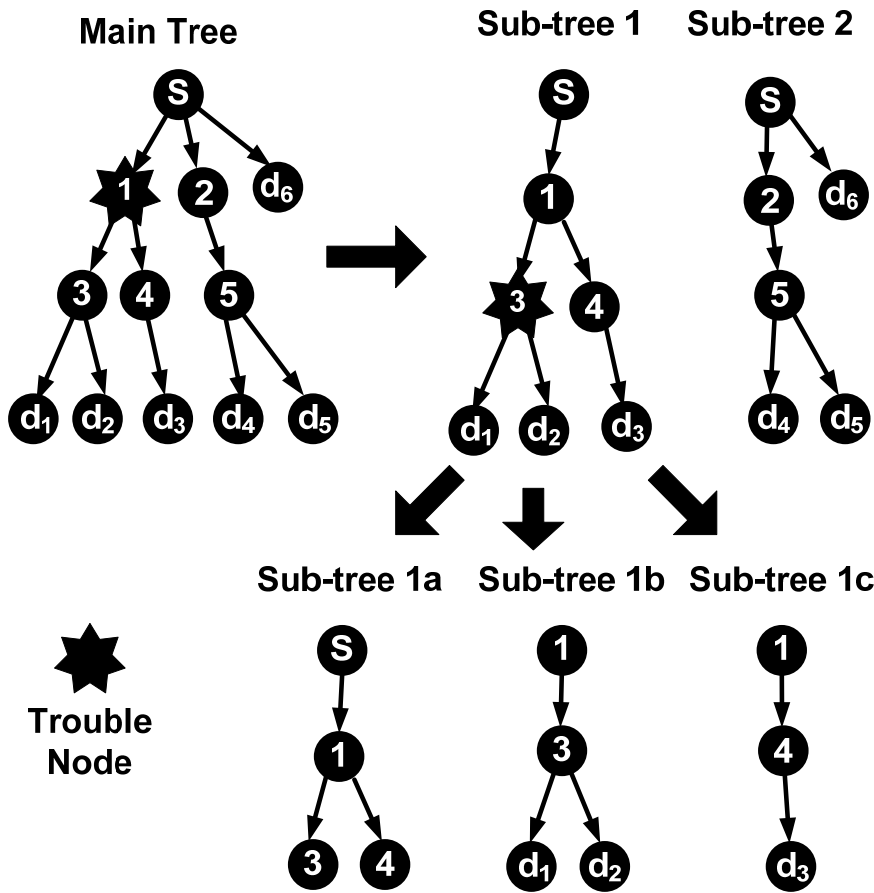
Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

defined as the intermediate node with the highest record. Next, the number of branches at the source node is identified.

Case 1: If there is more than one branch, firstly, the tree is partitioned into two sub-trees: one is the branch with the trouble node; the other one is formed by the rest of the branches. If a sub-tree is still cannot be protected by any one of the cycles, further partitioning this sub-tree into two portions is done in the same way, until all sub-trees can be protected.

Case 2: If there is only one outgoing link at the source node, this tree is partitioned into three sub-trees: the first one is formed by the stem from the source to its closest splitting node, and the outgoing links from the splitting node. Next, the tree branches, which originate from this splitting node, is partitioned into two sub-trees, treating this splitting node as the source node and following the same way as Case 1. After tree partitioning, the splitting node will appear in all the sub-trees, and each outgoing link from the splitting node will be present in the first sub-tree and also in one of the rest two sub-trees. This overlapping is to protect the tree against the splitting node failure. Notice that, there is no overlapping in the tree partition, if only the link failure recovery capability is required.

To illustrate the tree partition process, a simple example is shown in **Figure 4-2**. Assume that this tree in **Figure 4-2** is relatively large and it cannot be protected by any cycle, and assume that node 1 is identified as the trouble node out of the five intermediate nodes of the main tree. As the source nodal degree is greater than 1, the tree is partitioned into two sub-trees: sub-tree 1 and sub-tree 2. After first partition, suppose sub-tree 1 still cannot be protected. Assume node 3 is identified as the trouble node out of the three intermediate nodes of sub-tree 1. The source nodal degree of sub-tree 1 is only 1. Further partitioning of sub-tree 1 into 3 sub-trees is done according to case 2. Assuming that all sub-trees can be protected now, the TPA process terminates.



Main tree source:

 S

Main tree destinations:

 $\{d_1, d_2, d_3, d_4, d_5, d_6\}$

Main tree intermediate nodes:

 $\{1, 2, 3, 4, 5\}$ **Figure 4-2: A simple example of the tree partition algorithm (TPA)**

4.4 Spare capacity optimization algorithm of p -cycle based tree protection (SOPT)

Spare capacity optimization algorithm of p -cycle based tree protection (SOPT) algorithm is an ILP algorithm that optimizes the spare capacity required to configure the tree-protecting p -cycles [229]. In the SOPT algorithm, the candidate p -cycles in the network are identified first,

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

and then the multicast traffic is routed according to the Steiner Tree heuristic algorithm [239]. In this study, the concept of the disjoint route sets (DRS) approach [140] for p -cycle based path protection of unicast traffic is extended to the disjoint tree sets (DTS) approach. A disjoint tree set is defined as a set of multicast trees that are mutually link-disjoint (for link failure recovery) or node disjoint (for combined node and link failure recovery). The size of a DTS is the number of mutually disjoint trees inside this DTS. If a cycle can protect all the multicast trees in a DTS, this cycle is said to be able to protect this whole DTS.

In order to obtain the strictly optimal solution, all possible combinations [140] of DTSs identified from all the multicast trees need to be enumerated as the input to the proposed ILP model, which will be presented shortly. Generally, for M multicast trees, there could be C_M^2 possible combinations of DTSs of size 2, C_M^3 possible combinations of DTSs of size 3, and so on. In practice, there might be some multicast trees which are not mutually disjoint with any other trees, and such trees are referred to as DTSs of size 1. Hence, theoretically, there would be a total of $\sum_{i=1}^M C_M^i = 2^M - 1$ possible combinations of DTSs. This means that the optimization task becomes extremely hard, as the number of multicast sessions increases.

Ref [140] proposed a heuristic algorithm named “GenerateDRSs” to partially enumerate a subset of disjoint route sets. This algorithm is applied in this study to identify a promising subset of DTSs. $|DTS|$ is the number of DTSs. Given a group of M trees, this algorithm creates M DTS, one DTS for each tree by setting the tree itself as the first tree in that DTS. Then, for each DTS, the algorithm randomly selects another tree among all the remaining trees; if the selected tree is disjoint with all the trees inside that DTS, it is added to that DTS. This is iterated until all trees have been checked. Hence, one time execution of this heuristic algorithm would generate M random DTSs; X times execution would generate XM random DTSs. This subset of DTSs has a much smaller number of DTSs than the total number of all

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

possible DTSSs, and hence the ILP formulation of the SOPT algorithm becomes solvable when the number of multicast sessions is large.

Finally, the SOPT algorithm selects a set of most efficient p -cycles among the candidate cycles to protect all multicast sessions by the ILP optimization. Since only a subset of DTSSs and not all the DTSSs are considered, strictly speaking, the proposed SOPT design is not a truly optimized design. It can be classified as an ILP based heuristic design. The ILP formulation of the SOPT algorithm is given below:

$$\textbf{Objectives:} \quad \textbf{Minimize} \quad \sum_{mn \in E} c_{mn} v_{mn} \quad (4.1)$$

Constraints:

$$\sum_{\forall \mathfrak{R} \in D_{DTS}} \sum_{\forall j \in C} f_{j, \mathfrak{R}-DTS} Y_{j, \mathfrak{R}-DTS} Z_{\mathfrak{R}-DTS}^r \geq 1 \quad \forall \tau \in T \quad (4.2)$$

$$f_j = \sum_{\forall \mathfrak{R} \in D_{DTS}} f_{j, \mathfrak{R}-DTS} \quad \forall j \in C \quad (4.3)$$

$$v_{mn} = \sum_{\forall j \in C} \alpha_{j, mn} f_j \quad \forall mn \in E \quad (4.4)$$

$$w_{mn} + v_{mn} \leq t_{mn} \quad \forall mn \in E \quad (4.5)$$

The objective (4.1) is to minimize the total spare capacity required for configuring the p -cycles. Constraint (4.2) is to ensure that every multicast tree must be protected by at least one copy of a p -cycle. Constraint (4.3) is to calculate the total number of copies of p -cycle j required for protection. Constraint (4.4) is to determine the spare capacity allocation on each link reserved for configurations of p -cycles. Constraint (4.5) is to restrict the total capacity in each link.

The approximate number of variables for ILP formulation of the SOPT algorithm is $|E| + |C| \times |DTS| + |C|$. The approximate number of constraints for ILP formulation of the SOPT algorithm is $|T| + |C| + 2|E|$. ($|N|$ is the number of nodes. $|E|$ is the number of edges. $|C|$ is the number of cycles. $|T|$ is the number of multicast sessions. $|DTS|$ is the number of DTSS. $|E|$ and $|C|$ would increase with $|N|$ and the nodal degree.)

4.5 Efficiency score based heuristic algorithm of p -cycle based tree protection (ESHT)

4.5.1 ESHT for static traffic protection

The above ILP based SOPT algorithm selects an optimal subset of cycles among all the candidate cycles by capacity optimization. Since ILP based algorithm is not scalable to large networks with a large number of multicast sessions, an efficiency-score based heuristic algorithm of p -cycle based tree protection (ESHT), which can be viewed as a multicast version of the capacitated iterative design algorithm (CIDA) in [118] and the efficiency-ratio based unity- p -cycle heuristic algorithm (ERH) in [120, 231], is presented. Note that the CIDA algorithm and the ERH algorithm were independently developed for link protection under the context of unicast traffic.

An efficiency-score (ES) is introduced for cycle selection. The ES of unity p -cycle j is defined as the ratio of the sum of the working units of the largest set of unprotected mutually-disjoint trees that can be protected by unity p -cycle j to the sum of the spare units required by unity p -cycle j . Given a group of multicast trees, the largest set of mutually-disjoint trees is identified using a fast matrix algorithm (please see sub-section 4.5.3 for details). For each tree, the amount of other trees that are not mutually disjoint with it is recorded. A trouble tree is defined as the tree with the highest record. The trouble tree is identified by obtaining the

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

column sums of the matrix. It is then deleted from the matrix. The whole process iterates until the remaining trees are all mutually-disjoint. The set of remaining trees obtained is then the largest set of mutually-disjoint trees. The ES of unity p -cycle j can be calculated by equation (4.6).

$$ES(c_j) = \left(\sum_{\tau \in T_{md}(c_j)} W_{\tau} \right) / \sum_{\forall mn \in E} \alpha_{j,mn} \quad (4.6)$$

$T_{md}(c_j)$ The largest set of unprotected mutually node-disjoint trees that can be protected by cycle j . The trees inside this set are indexed by τ .

W_{τ} Sum of working units of tree τ .

$\alpha_{j,mn}$ It is 1 if cycle j traverses link mn and 0 otherwise.

For static traffic, given the network topology and the multicast traffic demand, the proposed ESHT algorithm first identifies all the candidate p -cycles using the heuristic edge-digraph based cycle algorithm [68] and route the multicast trees according to the Steiner tree heuristic algorithm [239]. If and only if no candidate cycles can protect a tree, it is partitioned into several sub-trees. Then, the largest set of unprotected mutually-disjoint trees that can be protected by each p -cycle is identified and its ES is calculated. The cycle with the highest ES is chosen and the trees that can be protected by it are marked. After that, check if there are remaining unprotected trees. If so, the next cycle with the highest updated ES is chosen to proceed. The above process is iterated until all multicast sessions are protected.

4.5.2 The matrix algorithm for identification of the disjoint tree sets

The matrix algorithm for identification of the disjoint tree sets, which serves the purpose of calculation of the efficiency score (ES) for cycle selection in the ESHT algorithm, is elaborated next. Let us consider an example of six candidate multicast trees (tree 1 to tree 6) and find the disjoint tree sets (DTSSs) among them. Matrix T_1 in (4.7) represents the relationship of disjointedness among the trees. The italic numbers outside the matrix are the indexes of the trees. The entry of the x^{th} row and the y^{th} column is 0 if tree x and tree y are mutually node disjoint, and 1 otherwise. A tree is always not disjoint with itself. Hence, the diagonal elements of matrix T are all equal to 1. For each tree, the amount of other trees that are not mutually disjoint with it, is recorded. The corresponding disjoint score matrix Ω_1 is obtained by calculating the column sum of T_1 , and is also given in equation (4.7). A trouble tree is defined as the tree with the highest score. In the disjoint score matrix Ω_1 , tree 2 has the highest score 4. It is identified as the trouble tree. Hence, tree 2 is removed from the matrix T_1 .

$$T_1 = \begin{matrix} & \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{matrix} \quad \Omega_1 = \begin{matrix} & \begin{matrix} 1 & \cancel{2} & 3 & 4 & 5 & 6 \end{matrix} \\ \begin{matrix} 1 \\ \cancel{2} \\ 3 \\ 4 \\ 5 \\ 6 \end{matrix} & \begin{bmatrix} 1 & \cancel{0} & 1 & 3 & 2 & 3 \end{bmatrix} \end{matrix} \quad (4.7)$$

A new matrix T_2 is obtained by eliminating the column and the row of tree 2 in T_1 and given in equation (4.8). The corresponding disjoint score matrix Ω_2 is also shown in equation (4.8).

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

$$\begin{array}{c}
 \begin{array}{ccccc}
 1 & 3 & 4 & 5 & 6
 \end{array} \\
 \mathbf{T}_2 = \begin{bmatrix}
 1 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 0 & 0 & 1 & 0 & 1 \\
 0 & 0 & 0 & 1 & 0 \\
 0 & 0 & 1 & 0 & 1
 \end{bmatrix} \begin{array}{c} 1 \\ 3 \\ 4 \\ 5 \\ 6 \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 \begin{array}{ccccc}
 1 & 3 & \cancel{4} & 5 & 6
 \end{array} \\
 \mathbf{\Omega}_2 = \begin{bmatrix}
 1 & 1 & \cancel{2} & 1 & 2
 \end{bmatrix}
 \end{array}
 \quad (4.8)$$

Now, both tree 4 and tree 6 have the highest score 2. Tree 4 is randomly chosen as the trouble tree and delete it from \mathbf{T}_2 . A new matrix \mathbf{T}_3 , and its corresponding disjoint score matrix $\mathbf{\Omega}_3$ are obtained then.

$$\begin{array}{c}
 \begin{array}{cccc}
 1 & 3 & 5 & 6
 \end{array} \\
 \mathbf{T}_3 = \begin{bmatrix}
 1 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 \\
 0 & 0 & 1 & 0 \\
 0 & 0 & 0 & 1
 \end{bmatrix} \begin{array}{c} 1 \\ 3 \\ 5 \\ 6 \end{array}
 \end{array}
 \quad
 \begin{array}{c}
 \begin{array}{cccc}
 1 & 3 & 5 & 6
 \end{array} \\
 \mathbf{\Omega}_3 = \begin{bmatrix}
 1 & 1 & 1 & 1
 \end{bmatrix}
 \end{array}
 \quad (4.9)$$

Now, all four trees have an equal disjoint score 1, which means they are mutually disjoint and can be grouped into one DTS, denoted as DTS_1 , which is the largest set of mutually-disjoint trees. Following the same procedure described above, the second largest DTS is obtained from the remaining ungrouped trees, i.e., tree 2 and tree 4. It is found that tree 2 and tree 4 are not mutually disjoint and hence are grouped into two separate DTSs. Therefore, 3 DTSs were found from the 6 multicast trees as follows:

$$\text{DTS}_1 = \{1 \ 3 \ 5 \ 6\}, \quad \text{DTS}_2 = \{4\}, \quad \text{and} \quad \text{DTS}_3 = \{2\}.$$

4.5.3 The p -cycle reconfiguration process in ESHT algorithm for dynamic multicast traffic

Since this ESHT algorithm is very fast as compared to its corresponding ILP based SOPT algorithm, it can be readily applied to dynamic multicast traffic. The flow chart of the p -cycle based reconfiguration process in the ESHT algorithm for dynamic multicast traffic is shown in **Figure 4-3**. As shown in **Figure 4-3**, upon the arrival of a new multicast request, the ESHT algorithm first tries to route the new multicast tree, according to the Steiner tree heuristic algorithm [239]. If the new multicast tree is successfully routed (the tree can be routed, if there is a simple path with enough remaining free capacity from the source to each destination), and if and only if no candidate cycle can protect this tree, it is partitioned into several sub-trees that can be protected, using the TPA algorithm. Then, the wavelengths are assigned to the sub-trees.

Case 1: if the new multicast session is successfully set up, the proposed model attempts to protect the new sub-trees, by using the existing cycles. If unsuccessful, additional new cycles will be configured, if there is enough remaining free capacity for configuring new cycles. If the routing of the new multicast tree is successful and all its sub-trees also can be protected by the existing cycles or by a combination of the existing cycles and newly configured cycles, the request is accepted; otherwise, it is blocked.

Case 2: if the new multicast tree cannot be set up within the remaining capacity of the network, all the existing cycles are released for reconfiguration. As the old configuration of p -cycles may not fit the traffic, the purpose of the reconfiguration is to make the newly configured cycles to fit the current multicast traffic, so as to accommodate the new incoming multicast request. After releasing the existing p -cycles, the proposed model attempts to route the new multicast tree and reconfigure cycles according to the ESHT design. If this is successful, the new multicast request is accepted; otherwise it is blocked.

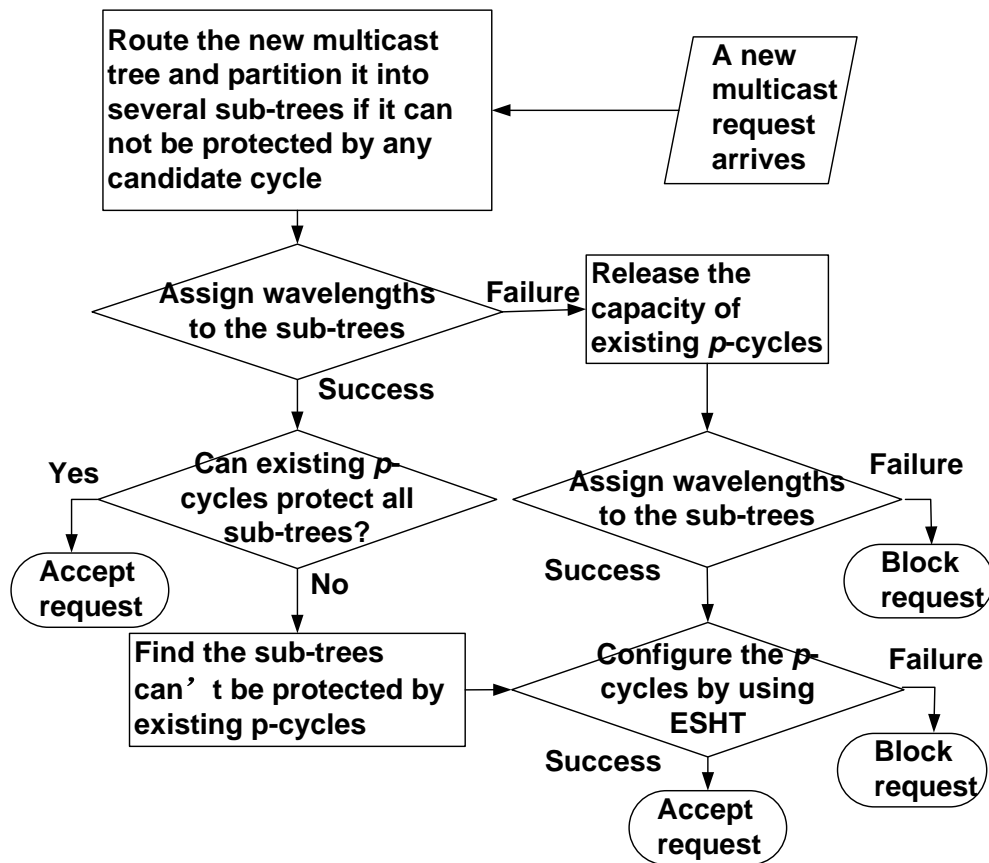


Figure 4-3: Flow chart of the p -cycle reconfiguration process in the ESH algorithm for dynamic multicast traffic

Upon successful setup of the new multicast request, the new multicast tree begins service. If a link/node in the network fails, the multicast trees traversing the failed link/node are rapidly switched to their corresponding pre-cross-connected p -cycles. As the p -cycles are preconfigured, the service recovery exhibits ring-like fast speed and takes about typically 30–80 ms [106, 247]. It is noted that a multicast tree will be tore down and its occupied capacity will be released upon the completion of the service of that multicast tree. In the mean time, the corresponding p -cycles are also released if they no longer protect any multicast light trees.

4.6 Optimal path pair (OPP) based approach

The OPP based approach was initially proposed for link failure recovery for unicast traffic in [204]. The basic idea supporting the optimal path pair approach is that for every multicast session, a link-disjoint path pair from the source to every destination node is sufficient to handle any link failure [204]. In this section, the application for combined node and link failure recovery is studied: a node-disjoint path pair from the source to every destination node is sufficient to handle combined node and link failure recovery; the working path and the backup path, which are node disjoint, will not fail simultaneously upon any single link/node failure. One source-destination pair can share the capacity with the other source-destination pairs within the same multicast session, because they actually carry the same information.

Table 4-1: The primary-backup path pairs for Φ_l ($\Phi_l = \{8, 1, 3, 4, 9\}$)

s-d Pair	Primary path	Node-disjoint backup path	Corresponding figure
(8,1)	$8 \rightarrow 4 \rightarrow 1$	$8 \rightarrow 9 \rightarrow 3 \rightarrow 1$	Figure 4-4 (a)
(8,3)	$8 \rightarrow 4 \rightarrow 3$	$8 \rightarrow 9 \rightarrow 3$	Figure 4-4 (b)
(8,4)	$8 \rightarrow 4$	$8 \rightarrow 9 \rightarrow 3 \rightarrow 1 \rightarrow 4$	Figure 4-4 (c)
(8,9)	$8 \rightarrow 4 \rightarrow 3 \rightarrow 9$	$8 \rightarrow 9$	Figure 4-4 (d)

Table 4-2: The final configured primary and backup links for Φ_l ($\Phi_l = \{8, 1, 3, 4, 9\}$)

Final primary links	$8 \rightarrow 4, 4 \rightarrow 1, 4 \rightarrow 3, 3 \rightarrow 9$
Final backup links	$8 \rightarrow 9, 9 \rightarrow 3, 3 \rightarrow 1, 1 \rightarrow 4$

An example illustrating the OPP based protection approach for Φ_l ($\Phi_l = \{8, 1, 3, 4, 9\}$) is shown in **Figure 4-4**. $\Phi_l = \{8, 1, 3, 4, 9\}$ has four destinations and therefore four source-destination pairs. The primary paths are shown in solid lines, whereas the backup paths are shown in dash lines. **Figure 4-4 (a)** shows the node-disjoint path pair for source-destination pair (8,1). **Figure 4-4 (b)** shows the node-disjoint path pair for source-destination pair (8,3).

Figure 4-4 (c) shows the node-disjoint path pair for source-destination pair (8,4). **Figure 4-4 (d)** shows the node-disjoint path pair for source-destination pair (8,9).

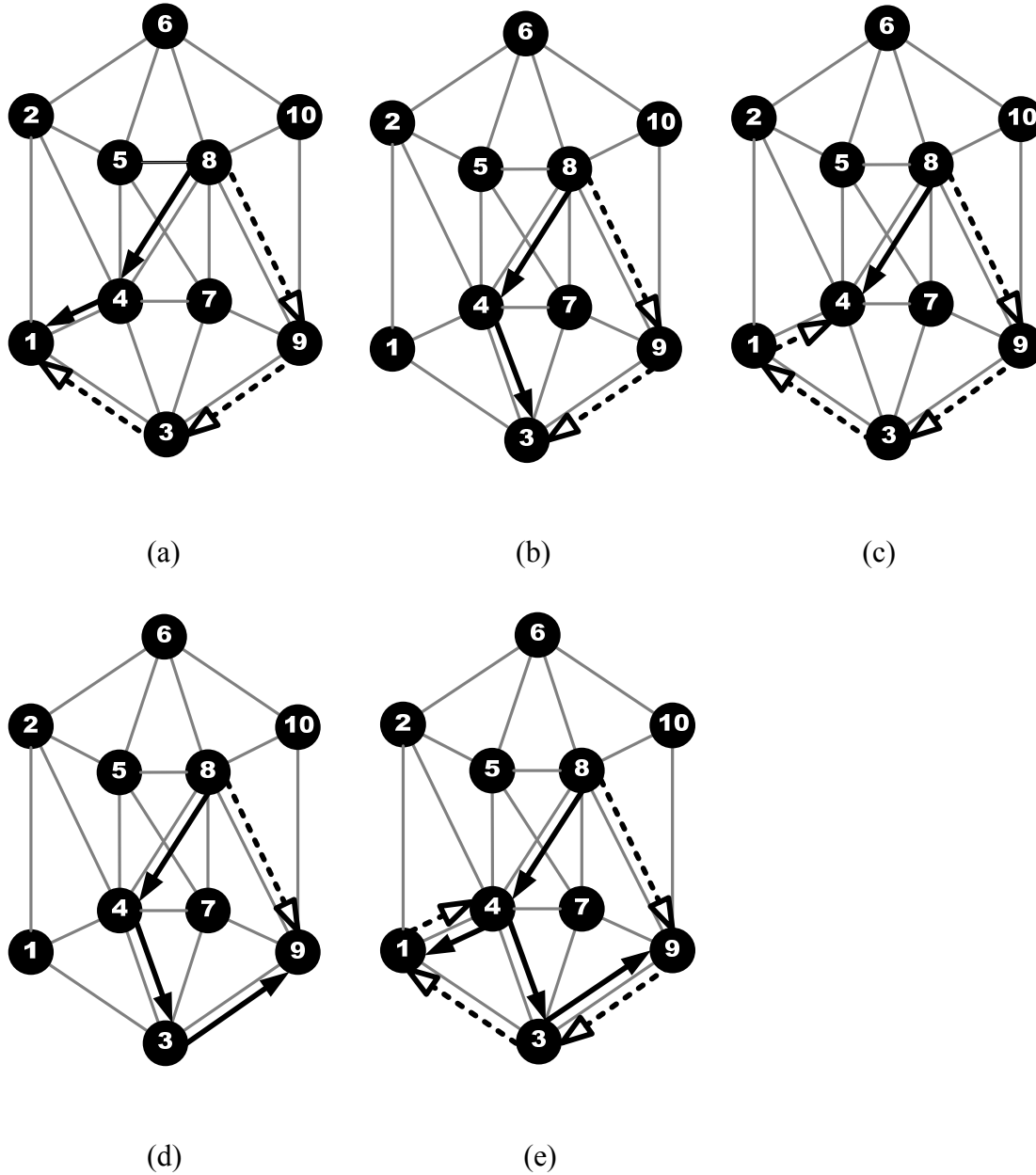


Figure 4-4: An example illustrating the OPP based protection approach

Because the path pairs can share capacity within the same multicast session, the total capacity required is reduced. The final configured primary and backup links for Φ_l are shown in **Figure 4-4 (e)** and **Table 4-2**. For instance, for source-destination pair (8,1), if

intermediate node 4 (or link $8 \rightarrow 4$ or link $4 \rightarrow 1$) fails, source-destination pair (8,1) will switch the transmission on the primary path ($8 \rightarrow 4 \rightarrow 1$) onto the backup path ($8 \rightarrow 9 \rightarrow 3 \rightarrow 1$).

4.6.1 Integer linear programming based optimal path pair algorithm (ILP-OPP)

The ILP formulation of the integer linear programming based optimal path pair algorithm (ILP-OPP) [204] is extended to combined node and link recovery, by modifying the link-disjoint constraints to node-disjoint constraints. Firstly, some additional notations used for the modified ILP formulation for ILP-OPP are introduced.

Variables

- $P_{sd,mn}^i$ It is 1 if the primary path from source s to destination d in multicast session i traverses link mn , and 0 otherwise.
- $B_{sd,mn}^i$ It is 1 if the backup path from source s to destination d in multicast session i traverses link mn , and 0 otherwise.
- $P_{sd,m}^i$ It is 1 if the primary path from source s to destination d in multicast session i traverses node m , and 0 otherwise.
- $B_{sd,m}^i$ It is 1 if the backup path from source s to destination d in multicast session i traverses node m , and 0 otherwise.
- u_{mn}^i It is 1 if the link mn is traversed by either primary path or the backup path in multicast session i and 0 otherwise.
- u_{mn} The total capacity on link mn

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

Next, the ILP formulation of ILP-OPP for combined node and link failure recovery is presented:

$$\text{Objectives: Minimize } \sum_{mn \in E} c_{mn} u_{mn} \quad (4.10)$$

Constraints:

$$\sum_n P_{sd,sn}^i = 1 \quad \forall d, \forall i \quad (4.11)$$

$$\sum_n P_{sd,ns}^i = 0 \quad \forall d, \forall i \quad (4.12)$$

$$\sum_n P_{sd,dn}^i = 0 \quad \forall d, \forall i \quad (4.13)$$

$$\sum_n P_{sd,nd}^i = 1 \quad \forall d, \forall i \quad (4.14)$$

$$\sum_n P_{sd,nm}^i = \sum_n P_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i, \forall m \neq s, d \quad (4.15)$$

$$\sum_n B_{sd,sn}^i = 1 \quad \forall d, \forall i \quad (4.16)$$

$$\sum_n B_{sd,ns}^i = 0 \quad \forall d, \forall i \quad (4.17)$$

$$\sum_n B_{sd,dn}^i = 0 \quad \forall d, \forall i \quad (4.18)$$

$$\sum_n B_{sd,nd}^i = 1 \quad \forall d, \forall i \quad (4.19)$$

$$\sum_n B_{sd,nm}^i = \sum_n B_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i, \forall m \neq s, d \quad (4.20)$$

$$P_{sd,m}^i \geq P_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i \quad (4.21)$$

$$P_{sd,n}^i \geq P_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i \quad (4.22)$$

$$B_{sd,m}^i \geq B_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i \quad (4.23)$$

$$B_{sd,n}^i \geq B_{sd,mn}^i \quad \forall mn \in E, \forall d, \forall i \quad (4.24)$$

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

$$P_{sd,m}^i + B_{sd,m}^i \leq 1 \quad \forall d, \forall i, \forall m \neq s, d \quad (4.25)$$

$$P_{sd,mn}^i \leq u_{mn}^i \leq 1 \quad \forall mn \in E, \forall d, \forall i \quad (4.26)$$

$$B_{sd,mn}^i \leq u_{mn}^i \leq 1 \quad \forall mn \in E, \forall d, \forall i \quad (4.27)$$

$$u_{mn} = \sum_{i=1}^{|T|} u_{mn}^i \quad \forall mn \in E \quad (4.28)$$

$$u_{mn} \leq t_{mn} \quad \forall mn \in E \quad (4.29)$$

The objective (4.10) is to minimize the total capacity. Constraints (4.11) to (4.15) are used to setup the primary paths in every multicast sessions. Constraints (4.11) and (4.12) ensure that, for multicast session i , the source node has only 1 unit of outgoing flow and 0 unit of incoming flow. Constraints (4.13) and (4.14) ensure that, for multicast session i , every destination node has 0 unit of outgoing flow and only 1 unit of incoming flow. Constraint (4.15) states that, for multicast session i , the incoming flow of any intermediate node is equal to its outgoing flow. Constraints (4.16) to (4.20) are used to setup the backup paths in every multicast sessions, following the same way of setting up the primary paths. Constraints (4.21) and (4.22) are used to identify the nodes along the primary paths from the source to every destination, in each multicast session. Constraints (4.23) and (4.24) are used to identify the nodes along the backup paths from the source to every destination, in each multicast session. Constraint (4.25) requires the primary path and backup path are node disjoint. The node disjoint constraint is applied to intermediate nodes only. Constraints (4.26) and (4.27) restrict that link cost to be counted (only once) if the link is used by either primary paths or backup paths in multicast sessions i . Constraint (4.28) calculates the sum of the total capacity on link mn required for all $|T|$ multicast sessions. Constraint (4.29) is to restrict the total capacity in

each link. Compared with the ILP formulation in [204], constraints (4.15), (4.20) to (4.29) are new in this section.

The approximate number of variables for ILP formulation of the proposed ILP-OPP algorithm is $2k \times |T| \times (|E| + |N|) + |E| \times (|T| + 1)$. The approximate number of constraints for ILP formulation of the proposed ILP-OPP algorithm is $k \times |T| \times (8 + 6|E| + 3|N|) + 2|E|$.

4.6.2 The OPP-SDP heuristic algorithm and the OPP-SDS heuristic algorithm

Based on the OPP concept, the OPP based shared disjoint path (OPP-SDP) heuristic algorithm and the OPP based shared disjoint segment heuristic algorithm (OPP-SDS) were proposed in [204]. The procedures of the OPP-SDP algorithm and the OPP-SDS algorithm are presented as follows [204]:

The OPP-SDP algorithm was shown to have the lowest blocking probability among all algorithms for dynamic traffic protection for link failure recovery [204]. When the OPP-SDP algorithm is applied to combined node and link failure recovery, the primary path has to be node-disjoint with the backup path. When the OPP-SDS algorithm is applied to combined node and link failure recovery, besides the node disjoint constraints between the primary segment and its backup segment, the upstream primary segment and its downstream segments have to be overlapped at least one link to provide node failure recovery. The OPP-SDP algorithm protects the path between every source and destination pair by computing a disjoint path pair with minimum cost. In order to minimize the cost, once a path pair is found, the cost of the arcs along that path pair is updated to be zero to increase the sharing of the new path pairs with the already-found ones within the same session. The path pairs within the same session are allowed for capacity sharing, because they actually carry the same information. Similar process is applied to the OPP-SDS algorithm.

Procedure of the OPP-SDP heuristic algorithm

- Step1:** When a multicast request arrives, identify all the source-destination pairs. For every source-destination pair, repeat steps 2 and 3.
- Step 2:** Find an optimal path pair between the current source-destination pair.
- Step 3:** Update cost = 0 for already found optimal path pairs

Procedure of the OPP-SDS heuristic algorithm

- Step1:** Create the primary tree using the Steiner tree heuristic algorithm.
- Step 2:** Identify the segments on the primary tree.
- Step 3:** For every primary segment, repeat steps 4 and 5.
- Step 4:** Find an optimal path pair between the end nodes of the segment.
- Step 5:** Update cost = 0 for already-found optimal path pairs

For a multicast request, if an optimal path pair (or segment pair) can be identified in the network for every source-destination pair and enough working capacity and spare capacity can be reserved for every source-destination path pair (or segment pair), the multicast request is accepted. Working capacity and spare capacity required by this multicast session are then assigned to it. In case of a link/node failure on working path (or segment) in the path pair (or segment pair), the adjacent nodes of the failed link/node will inform the source and destination node of that path pair (or segment pair). The source and destination will configure the backup path (segment) and switch the traffic onto the backup path (segment). After the service of a particular multicast session is over, its working capacity and spare capacity is then released.

4.7 Performance evaluation for static traffic protection

For performance evaluation for static traffic protection, the COST239 network (11 nodes and 26 links), the NSFNET network (14 nodes and 21 links) and the US backbone network (24 nodes and 43 links) are selected as the test networks (shown in **Figure 4-5**), whose average node degrees are 4.727, 3 and 3.583, respectively. The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM.

For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node. In this study of static multicast traffic protection, each link is assumed to have two fibers of 64 wavelengths per fiber, transmitting in opposite directions. For comparison, we extend the OPP approach [204] to the combined node and link failure recovery, because the OPP is reported to be the most efficient in [204]. For each multicast group size, 20 multicast sessions are randomly generated. For every multicast group size, 20 independent simulation experiments are performed to obtain the average value.

In the tree-protecting p -cycle based multicast protection approach, the splitting frequency is defined as the ratio of the number of trees being split to the total number of trees, by the TPA algorithm. **Table 4-3** shows the average splitting frequency of the tree-protecting p -cycle based multicast protection approach only in COST239 network to conserve the space, as similar results are observed for NSFNET network. As shown in **Table 4-3**, the splitting frequency increases with the multicast group size. For a multicast group size of 5, 2% of the trees need to be split.

Table 4-3: Average splitting frequency (SF) in the COST239 network

Group Size k	1	2	3	4	5	6	7	8	9	10
Split. Freq.	0	0	0	0.5%	2%	4.5%	11%	25.5%	56.5%	1

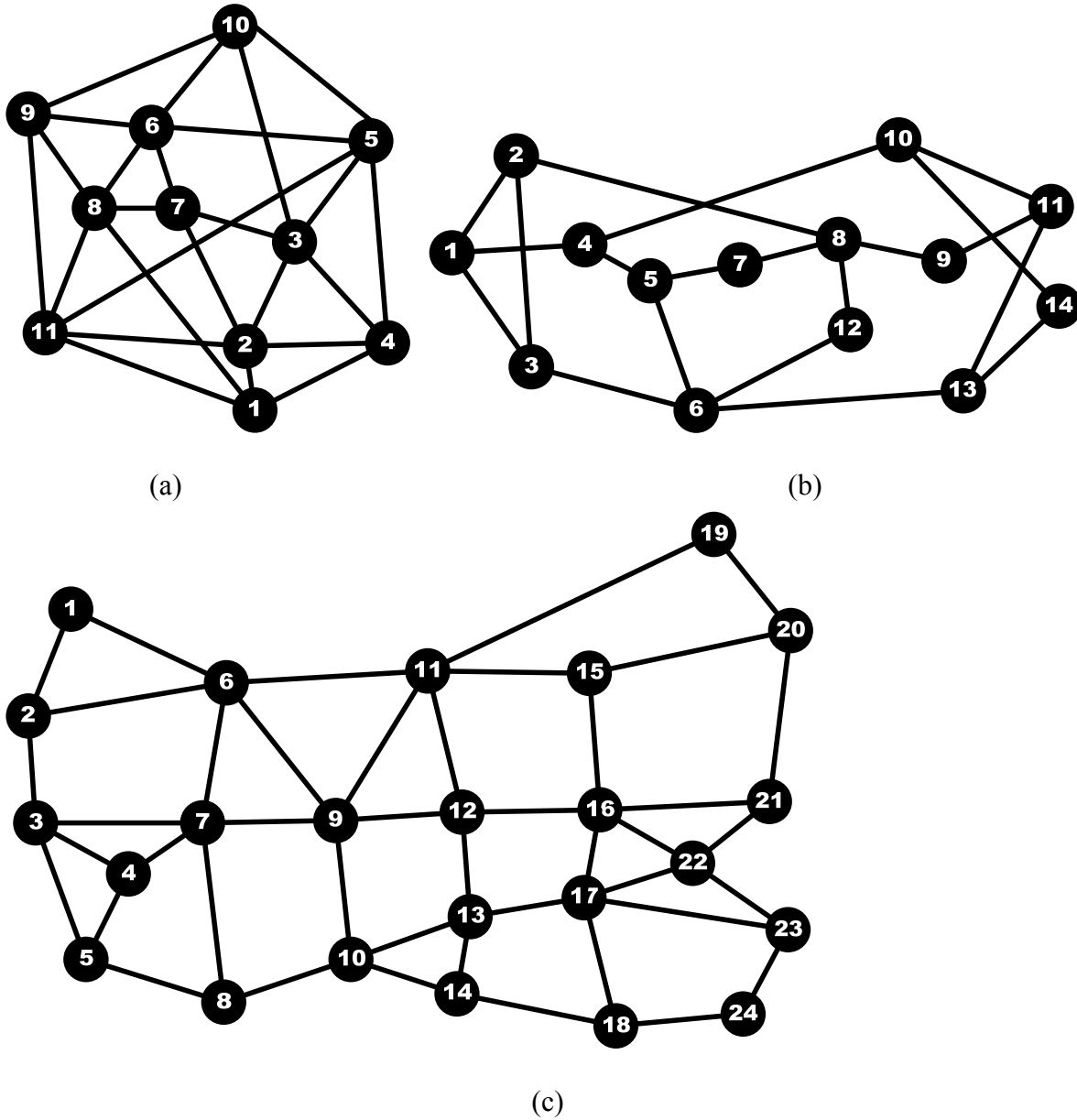


Figure 4-5: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network

The average total capacity (TC) required for the case of link failure recovery (LR) as well as for the case of combined node and link recovery (CNLR) in the COST239 network is compared in **Table 4-4**. The total capacity required by most protection algorithms would increase, if the node failure recovery capability is required on top of the link failure recovery capability. However, surprisingly, the extra capacity increased for node failure recovery is quite small (less than 14.1%).

Table 4-4: Total capacity comparison required by 20 random multicast sessions for link failure recovery (LR) and those for combined node and link recovery (CNLR) in COST239 network ($k = 5$)

Algorithms	TC_{LR}	TC_{CNLR}	PI	RE_{CNLR}
ESHT	233.1	248.5	6.6%	1.4126
SOPT	201.4	229.8	14.1%	1.2311
OPP-SDP	225.7	240.8	6.7%	1.0031
ILP-OPP	216.2	224.1	3.7%	1.0008

The percentage increase (PI) is defined to be the ratio of the difference of the total capacities in the CNLR case and the LR case to the total capacity in the LR case. The SOPT algorithm consumes the least total capacity for both the LR and the CNLR cases; whereas the PI of the total capacity for the ILP-OPP is the smallest. The average redundancy (RE) (which is defined as the average ratio of the spare capacity reserved to the working capacity [27]) for the CNLR case is shown in the 4th column. The RE can be calculated by equation (4.30):

$$RE = \frac{\sum_{\forall mn \in E} c_{mn} v_{mn}}{\sum_{\forall mn \in E} c_{mn} w_{mn}} \quad (4.30)$$

c_{mn} is the cost for a unit capacity on link mn (1 in this study). w_{mn} is the number of working units occupied by the multicast sessions on link mn . v_{mn} is the number of spare units required to be reserved on link mn to configure p -cycles.

Generally, heuristic algorithms have higher redundancy compared with their respective ILP bench marks. Among all algorithms, the ILP-OPP algorithm has the least redundancy (100.08%), while the ESHT has the highest redundancy (141.26%).

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

The comparison of the average total computational time (TI) for setting up a multicast session in COST239 network is shown in **Table 4-5**. Heuristic algorithms are faster than the corresponding ILP algorithms. For both the LR case and the CNLR case, the OPP-SDP heuristic algorithm is the fastest among all algorithms; whereas the ILP-OPP algorithm is the slowest. The computational speed of both the ESHT algorithm and the SOPT algorithm is slowed down by the disjointedness check and enumeration of DTSs.

Table 4-5: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in static traffic environment ($k = 5$)

Algorithms	ESHT	SOPT	OPP-SDP	ILP-OPP
$TI_{LR}(\text{ms})$	100	400	15	1430
$TI_{CNLR}(\text{ms})$	110	430	18	1500

Generally, besides the platform factor, the computational time also increases with the computational complexity of the algorithms. Two factors affecting the computational complexity of the ILP algorithms are the number of variables and constraints, which are compared in **Table 4-6**. $|E|$ and $|C|$ would increase with $|N|$ and the nodal degree. Note that $|C|$ could be reduced considerably using p -cycle pre-selection strategies reported in [27] whereby the computational speed of p -cycle based algorithms would be significantly increased at the cost of consuming more spare capacity.

Table 4-6: Comparison of the number of variables and constraints in different ILP algorithms

ILPs	Number of variables	Number of constraints
SOPT	$ E + C \times DTS + C $	$ T + C + 2 E $
ILP-OPP	$ 2k \times T \times (E + N) + E \times (T + 1) $	$k \times T \times (8 + 6 E + 3 N) + 2 E $

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

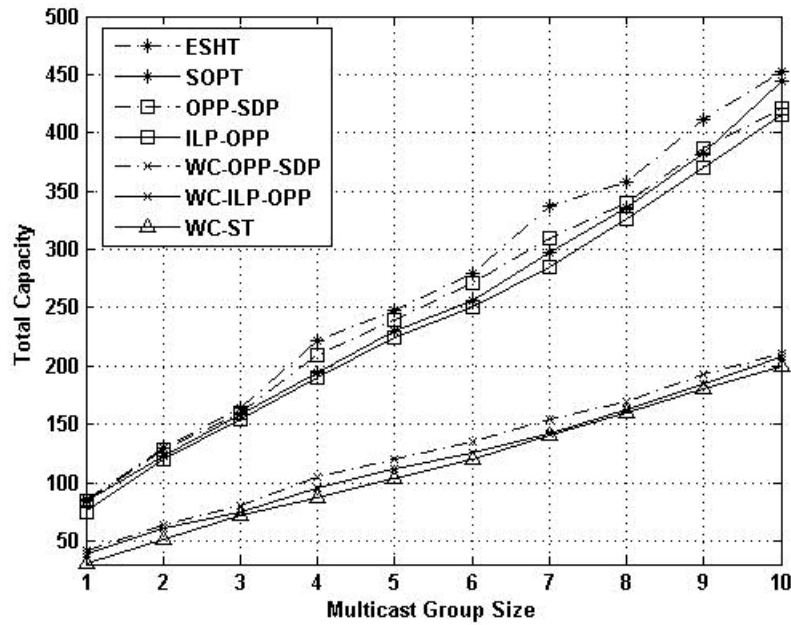
The capacity efficiency comparison for static multicast traffic protection for different ILP algorithms (in solid traces) and heuristic algorithms (in dash traces) in COST239 network, NSFNET network, and US backbone network is shown in **Figure 4-6**. The required working capacities, which are obtained using the Steiner tree heuristic algorithm [239], the ILP-OPP algorithm and the OPP-SDP heuristic algorithm, are also shown as traces marked as “WC-ST”, “WC-ILP-OPP”, and “WC-OPP-SDP” respectively, in all three sub-figures.

As the multicast group size increases, more links and nodes are traversed by each multicast tree and hence the working capacity required by multicast trees would increase. In all three test networks, Steiner tree heuristic algorithm consumes the least working capacity for routing multicast trees. In all the three test networks, the ILP-OPP achieves the best capacity efficiency among all algorithms. However, the OPP does not consider sharing of the spare capacity among different multicast sessions [220].

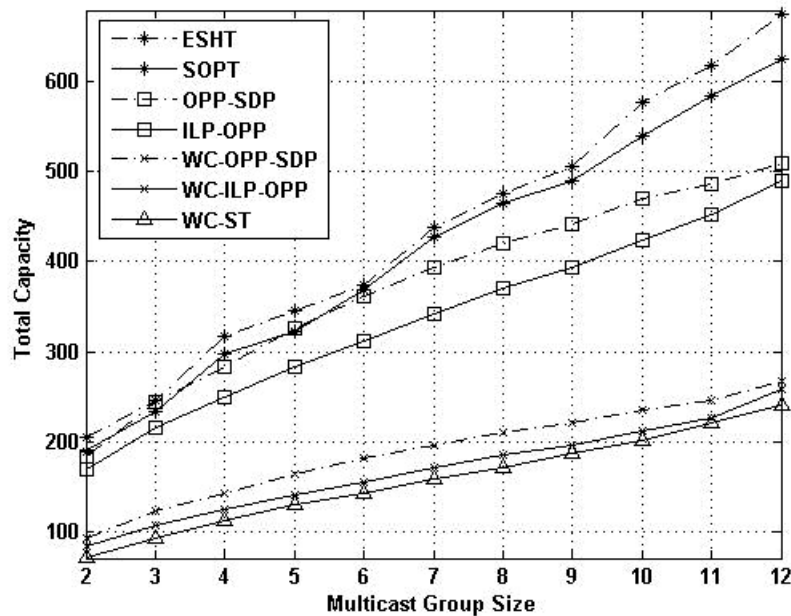
Although the tree-protecting p -cycle based approach allows inter-request spare capacity sharing, its efficiency is inferior to the OPP approach, because it is difficult to enumerate all the DTSs [229, 232]. Generally, for M multicast trees, there could be C_M^2 possible combinations of DTSs of size 2, C_M^3 possible combinations of DTSs of size 3, and so on. In practice, there might be some multicast trees which are not mutually disjoint with any other trees, and such trees are referred to as DTSs of size 1. Hence, theoretically, there would be a total of $\sum_{i=1}^M C_M^i = 2^M - 1$ possible combinations of DTSs. Besides, a large tree, which cannot be protected by a single cycle, have to be split into several smaller sub-trees. Nevertheless, splitting one tree into several sub-trees required overlapping at the splitting node for splitting node failure recovery, which further decreases the efficiency. Generally, the difference of capacity efficiency between the OPP based approach and the tree-protecting p -cycle based

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

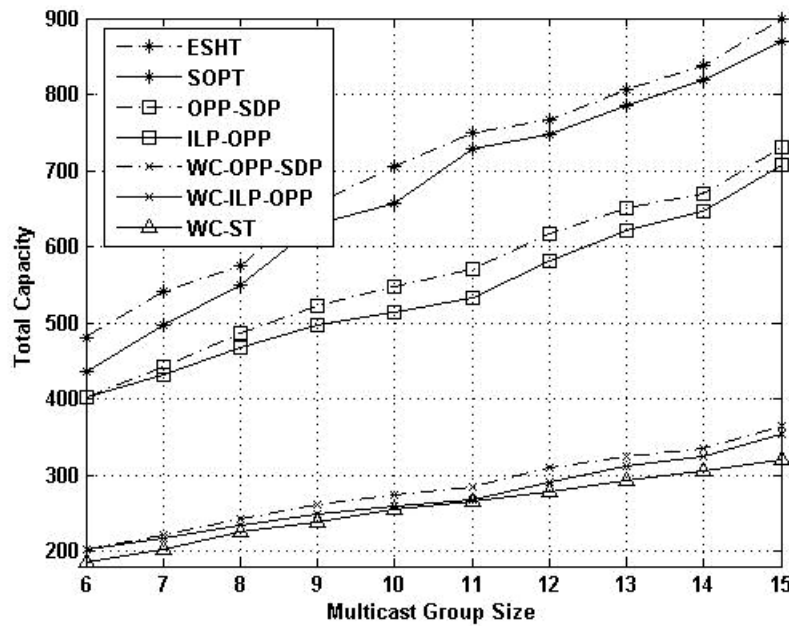
approach is small when the multicast group size is small, and gets larger as the multicast group size increases.



(a)



(b)



(c)

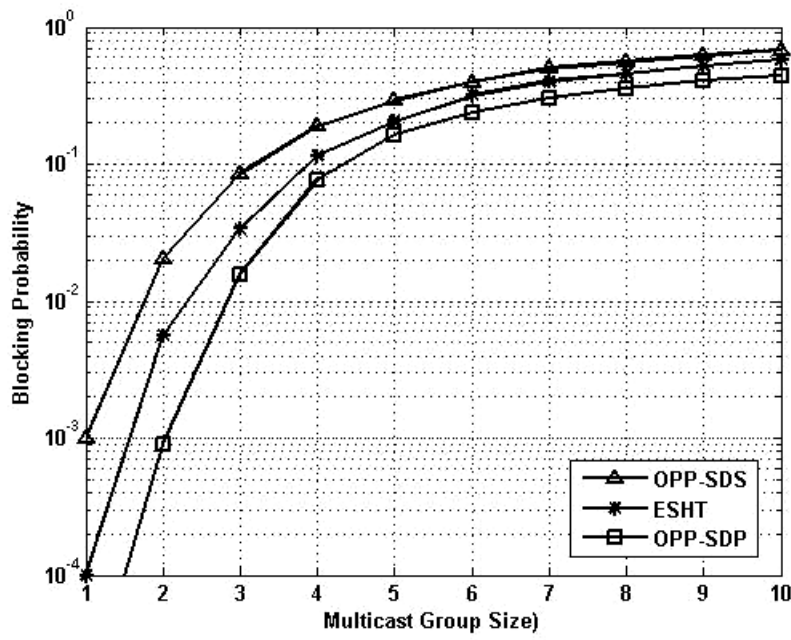
Figure 4-6: Capacity efficiency comparison for static multicast traffic protection for combined node and link failure recovery: (a) in COST239 network; (b) in NSFNET network; (c) in US backbone network.

As shown in **Figure 4-6**, the ILP algorithms achieve better results than their corresponding heuristic algorithms, but their differences are quite small. Results show that the capacity efficiency of the ESHT heuristic algorithm is close to that of the SOPT algorithm, while the capacity efficiency of the OPP-SDP algorithm is close to that of the ILP-OPP algorithm as well. The advantage of the ILP algorithms is that they solve all the variables simultaneously and can obtain the globally optimized solution (the selection of p -cycles in SOPT, or the routing of the paths pairs in ILP-OPP), according to both the optimization objectives and constraints. The heuristics can only get close to the global optimal point by iterative processing. Therefore, the ILP algorithms provide the theoretical optimal results, which serve as the bench marks (bounds) for the corresponding heuristic algorithms in each network, so that the effectiveness of the heuristic algorithms can be assessed. Note that the ESHT is much

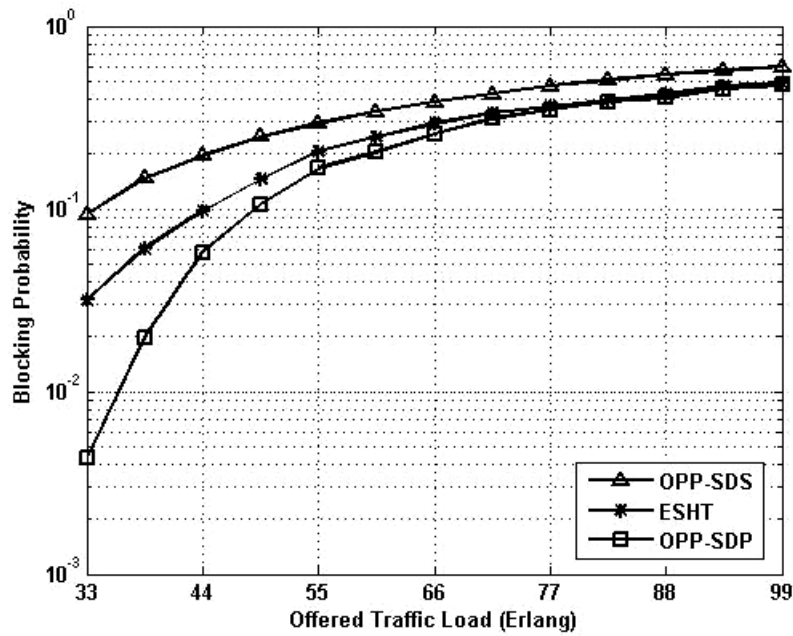
faster than the SOPT algorithm in computational speed and hence it is more suitable to be applied to dynamic traffic protection.

4.8 Performance evaluation for dynamic traffic protection

For dynamic traffic protection, the COST239 network, and the NSFNET network, US backbone network are selected as the test networks. The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM. Each link is assumed to have two fibers of 16 wavelengths per fiber, transmitting in opposite directions. The multicast session requests are assumed to arrive with a Poisson distribution and their holding time is negatively exponentially distributed. For every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node. Let λ be the arrival rate and μ be the average holding time of multicast sessions. Then total network traffic load is $\lambda\mu$. The total number of randomly generated multicast requests is 10^5 for each network traffic load in the simulation. For every incoming request, either if no candidate backup cycles/paths can protect the request, or if one or more links are out of capacity for either routing or protection, the current request is blocked. The OPP-SDP algorithm and the OPP-SDS algorithm [204] are selected for comparison. The OPP-SDP algorithm was reported to be the most efficient heuristic algorithm among all the existing heuristic algorithms for dynamic traffic protection against single link failure [204].

Chapter 4: Tree-Protecting p -Cycle Based Multicast Protection Approach

(a)



(b)

Figure 4-7: Blocking performance comparison in COST239 network for dynamic multicast traffic protection: (a) offered traffic is fixed at 55 Erlang, (b) the multicast group size (k) is fixed at 5.

Simulation results in **Figure 4-7** showed that, for blocking performance, the OPP-SDP algorithm is superior to the ESHT algorithm and the OPP-SDS algorithm. One of the reasons is because the tree partitions in the ESHT algorithm and segmentations in the OPP-SDS algorithm divide the working trees/paths into overlapped working domains for node failure recovery, which requires extra working capacity. The simulation results in NSFNET work and US backbone network are similar and therefore not shown.

The comparison of the average total computational time for setting up a multicast session in the COST 239 network for dynamic traffic protection is shown in **Table 4-7**. Similar to the results obtained in static traffic simulations, the OPP-SDP is the fastest for both the LR case and the CNLR case. The average total computational time for setting up a multicast session is longer for dynamic traffic protection, compared with those in static traffic protection, because of the network state update process (working/spare/total capacity matrixes update process, registry and release of trees/paths/cycles, etc), blocking check process and p -cycle reconfiguration process and so on.

Table 4-7: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in dynamic traffic environment ($k=5$, $\lambda\mu = 55$ Erlang)

Algorithms	OPP-SDP	ESHT
$TI_{LR}(\text{ms})$	23	319
$TI_{CNLR}(\text{ms})$	45	370

However, the OPP-SDP and the OPP-SDS require complicated signaling process to inform multiple relevant nodes to configure the backup paths, which results in long restoration time. Because resources along the protection paths are shared, cross-connects along the protection paths are not configured at the connection setup; instead they are only configured when a failure actually occurs. This introduces additional delays to signal at the intermediate nodes,

thus increasing restoration time significantly compared to those methods where protection paths are pre-configured (pre-fixed) for the intermediate nodes. In contrast, p -cycles offer much faster restoration speed, because p -cycles are pre-configured.

4.9 Conclusions

The extension of the p -cycle concept to tree protection enables p -cycles to protect the multicast traffic for combined node and link failure recovery. In this chapter, the tree-protecting p -cycle based multicast protection approach, including the spare capacity optimization algorithm of p -cycle based tree protection (SOPT) and the efficiency-score based heuristic algorithm of p -cycle based tree protection (ESHT), was presented. The ILP-optimal path pair (ILP-OPP) algorithm and the OPP-shared disjoint paths (OPP-SDP) heuristic algorithm and OPP-shared disjoint segments (OPP-SDS) heuristic algorithm proposed in [204] were extended for combined node and link failure recovery.

Simulation results show that, for static traffic protection, the capacity efficiency of the ESHT heuristic algorithm is close to that of its bench mark, the SOPT algorithm. However, the ESHT is much faster than the SOPT algorithm in computational speed and hence it is more suitable to be applied to dynamic traffic protection. For dynamic traffic protection, while the blocking performance of the ESHT is in between the OPP-SDP algorithm and the OPP-SDS algorithm. However, p -cycle based protection approaches offer much faster restoration speed, because p -cycles are pre-cross-connected.

Chapter 5. Node-and-Link Protecting p -Cycle Based Multicast Protection Approach

5.1 Introduction

As discussed in the last chapter, a combined node and link failure recovery approach is more cost-effective and very crucial to network survivability. The tree-protecting p -cycle based approach introduced in the last chapter provides a means for combined node and link failure recovery. The tree protecting p -cycle based approach protects multiple mutually disjoint trees (or sub-trees) on an end-to-end basis. The selected p -cycles are shared by multiple mutually disjoint trees. Therefore, both the ILP based SOPT algorithm and the ESHT heuristic algorithm have to consider mutually disjoint constraints. Besides, since only a subset of DTSs and not all the DTSs are considered, strictly speaking, the proposed SOPT algorithm is not a truly optimized design. The number of DTSs enumerated affects the performance of the tree-protecting p -cycle based approach as well.

Ref. [255] analyzed an ordinary p -cycle approach, in which, the node failures are restored using the flow p -cycle approach, whereas the link failures are restored through the conventional link-protecting p -cycle approach [106]. In this chapter, the node-and-link protecting p -cycle concept for multicast protection is introduced and investigated, which can be viewed as the multicast version of the ordinary p -cycle based protection approach proposed in [255] for unicast protection. The node-and-link protecting p -cycle based approach is shown to outperform other existing multicast protection approaches for combined node and link failure recovery.

This chapter is organized as follows. Section 5.1 gives the background and the motivation of developing the node-and-link protecting p -cycle based multicast protection approach. Section 5.2 introduces some additional notations used in this study. Section 5.3 explains the

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

protection mechanism of node-and-link protecting p -cycle based approach. Section 5.4 discusses the spare capacity optimization algorithm of node-and-link protecting p -cycle (SOPN), while Section 5.5 discusses the efficiency score based heuristic algorithm of node-and-link protecting p -cycle (ESHN). Section 5.6 investigates the proposed algorithms in static traffic environment. Section 5.7 investigates the proposed algorithms in dynamic traffic environment. The conclusions are given in section 5.8.

5.2 Additional notations

The general notations used in this study have been introduced in Section 3.2. Additional notations used in this chapter are introduced below:

Input parameters

w_m^τ	It is 1 if tree τ traverses node m ; and 0 otherwise.
$a_m^{j,\tau}$	It is 1 if cycle j can protect node m of tree τ , and 0 otherwise.

Variables

$f_m^{j,\tau}$	It is 1 if one copy of cycle j is selected for protecting node m of tree τ , and 0 otherwise.
----------------	--------------------------------------------------------------------------------------------------------

5.3 Protection mechanism of the node-and-link protecting p -cycle based approach

In this section, the protection mechanism of the node-and-link protecting p -cycle for multicast protection, which can be viewed as the multicast version of the ordinary p -cycle

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

based protection approach for unicast protection proposed in [255], is introduced. In this approach, the link failures are restored through the conventional link-protecting p -cycle principle [106, 120], whereas the node failures are restored by the flow p -cycles like principle [139]. This study has observed that an intermediate node of a tree can be protected by a cycle, as long as one of its upstream nodes and one level of its downstream nodes are on-cycle, besides its failure does not block the protection path provided by the cycle.

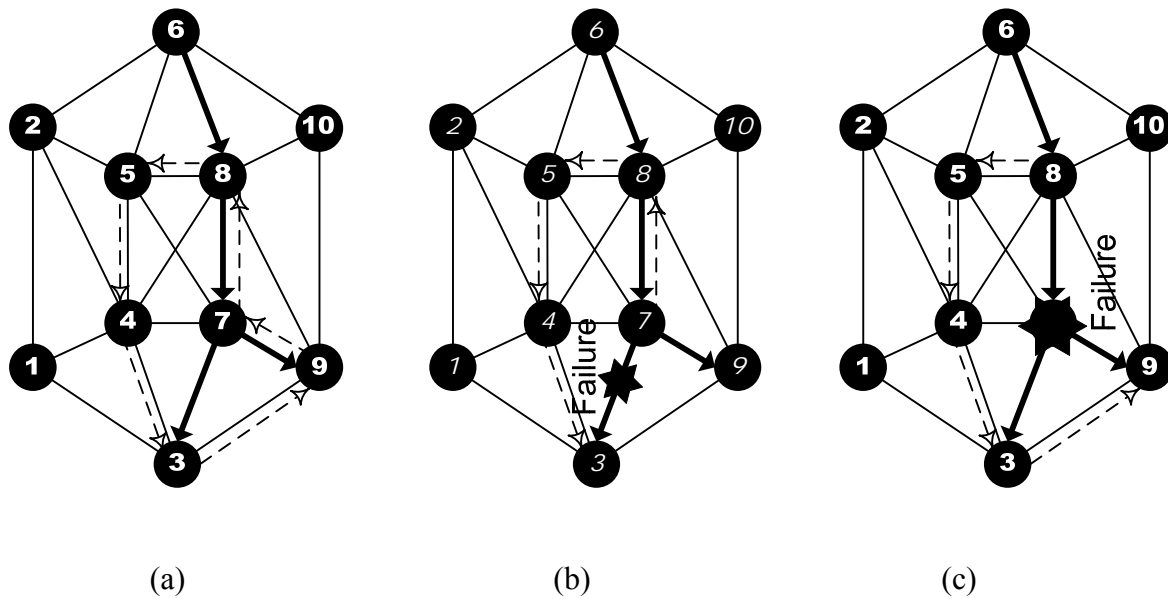


Figure 5-1: Illustration of the node-and-link protecting p -cycle approach: (a) a cycle and a tree; (b) link failure recovery; (c) node failure recovery.

The above constraints enable a p -cycle to recover an intermediate node failure by rerouting the traffic from one of this node's upstream nodes to one level of this node's downstream nodes, so that this node's downstream destination nodes can still receive the information from the source. Hence, the node-and-link protecting p -cycles are able to protect the nodes on the portions of the trees that “flow” across the cycles.

The example in **Figure 5-1** illustrates the node-and-link protecting p -cycle approach. In this approach, one copy of a p -cycle can be shared for the (on-cycle/straddling) link failure

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

recovery (as illustrated in **Figure 5-1 (b)**), and intermediate node failure recovery (as illustrated in **Figure 5-1 (c)**), in order to maximize the efficiency. As shown in **Figure 5-1 (a)**, Tree 1 routed for a multicast request Φ_1 ($\Phi_1 = \{6, 3, 9\}$) has two intermediate nodes (nodes 7 and 8). Let us take intermediate node 7 as an instance to illustrate node failure recovery. Node 7 has two upstream nodes (nodes 8 and 6), and one level of downstream nodes (nodes 3 and 9), which are destination nodes as well.

If node 7 fails, both destination nodes 3 and 9 are affected. Hence, the objective of failure recovery of node 7 is to find a cycle which can restore traffic from the source node to destination nodes 3 and 9. Therefore, for protecting node 7, we have 2 options of cycles: (i) cycles traversing the source node, as well as nodes 3 and 9 ; (ii) cycles traversing node 8, as well as nodes 3 and 9 (e.g., cycle 1: $8 \rightarrow 5 \rightarrow 4 \rightarrow 3 \rightarrow 9 \rightarrow 7 \rightarrow 8$ shown in the dashed line in **Figure 5-1 (a)**). Both two options provide backup paths for protection against the failure of node 7. For instance, as shown in **Figure 5-1 (c)**, after the failure of node 7, cycle 1 reroutes the traffic from the source node to destination nodes 3 and 9 via the protection path ($8 \rightarrow 5 \rightarrow 4 \rightarrow 3 \rightarrow 9$).

For link failure recovery, a unity- p -cycle can be shared by one working unit on any on-cycle link in opposite direction and two working units in both directions on any straddling link. As long as the working capacity on each link is protected, all the multicast trees are protected against any single link failure. For node failure recovery, as a single failure at any time is assumed, different nodes can share a copy of cycle for protection. However, for a specific common component (link/node) of multiple trees, the number of copies required for a particular cycle is determined by the number of trees traversing it, because the failure of this common component would affect multiple trees.

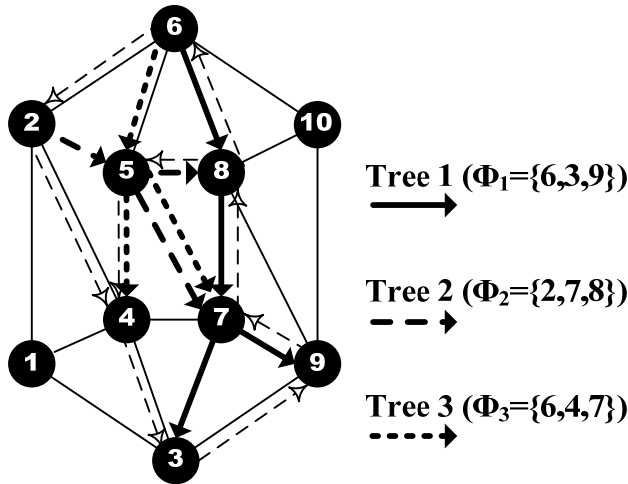


Figure 5-2: An example illustrating that the no. of copies required for a particular cycle should satisfy the largest node-failure-specific simultaneous use

As shown in **Figure 5-2**, tree 1 for Φ_1 ($\Phi_1 = \{6, 3, 9\}$) has two intermediate nodes (nodes 7 and 8). Tree 2 for Φ_2 ($\Phi_2 = \{2, 7, 8\}$) has one intermediate node (nodes 5). Tree 3 for Φ_3 ($\Phi_3 = \{6, 4, 7\}$) has one intermediate node (node 5). Cycle 2 (8→6→2→4→3→9→7→8) can protect those three intermediate nodes (nodes 5, 7, 8). As shown in **Figure 5-2**, node 5 is a common intermediate node of Tree 2 and Tree 3. Failure of node 5 affects both Tree 2 and Tree 3. Hence, two copies of cycle 2 are required to recover Tree 2 and Tree 3 should node 5 fail. Nodes 7 and 8 are intermediate nodes of Tree 1 only, hence only one copy of cycle 2 is required for protecting Tree 1 should node 7 or node 8 fail. Since a single node failure at any time is assumed, the number of copies of a particular p -cycle required should satisfy largest node-failure-specific simultaneous use. It only requires 2 copies of cycle 2 in total, instead of 3 copies for 3 trees in total, to protect those three trees should any one of the nodes 5, 7 and 8 fail. The spare capacity reserved is significantly reduced by allowing multiple intermediate nodes to share a p -cycle.

The protection mechanisms of node-and-link protecting p -cycles and tree-protecting p -cycles are different. The node-and-link protecting p -cycles protect all individual nodes (on

the flows) and links, so as to achieve combined node and link failure recovery for multicast trees. The p -cycles are shared by nodes or links. For link failure recovery, the end nodes of the link are responsible for protection switching. For node failure recovery, one of the upstream nodes and one level of the downstream nodes are responsible for the protection switching. If all the nodes and links of all multicast trees are protected, these multicast trees are protected for combined node and link failure recovery.

Tree protecting p -cycles protect the multiple mutually disjoint trees (or sub-trees) on end-to-end basis. In this approach, a p -cycle can be shared by multiple mutually disjoint trees. For both the node failure recovery and link failure recovery, the end nodes of the trees (or sub-trees) are responsible for the protection switching.

5.4 Spare capacity optimization algorithm of the node-and-link protecting p -cycle (SOPN)

The ILP formulation in [255] is extended to optical multicast traffic protection and being named as the spare capacity optimization algorithm of node-and-link protecting p -cycle (SOPN), which minimizes the spare capacity required to configure the node-and-link protecting p -cycles. In the SOPN algorithm, after identifying the candidate p -cycles and routing the multicast traffic, $a_m^{j,\tau}$, w_m^τ , w_{mn} , $\alpha_{j,mn}$, and $\beta_{j,mn}$ are obtained as the input parameters, using the proposed multicast protection mechanism presented above, and a subset of p -cycles is selected by ILP optimization, such that all link working capacity and node transit working capacity are protected, and the spare capacity required is minimized as well. Next, the ILP formulation of the SOPN design is presented:

$$\text{Objectives: Minimize } \sum_{mn \in E} c_{mn} v_{mn} \quad (5.1)$$

Constraints:

$$\sum_{j \in C} f_m^{j,\tau} a_m^{j,\tau} = w_m^\tau \quad \forall \tau \in T, \forall m \neq s, d \quad (5.2)$$

$$f_j \geq \sum_{\tau \in T} f_m^{j,\tau} \quad \forall j \in C, \forall m \neq s, d \quad (5.3)$$

$$w_{mn} \leq \sum_{j \in C} \beta_{j,mn} f_j \quad \forall mn \in E \quad (5.4)$$

$$v_{mn} = \sum_{j \in C} \alpha_{j,mn} f_j \quad \forall mn \in E \quad (5.5)$$

$$w_{mn} + v_{mn} \leq t_{mn} \quad \forall mn \in E \quad (5.6)$$

The objective (5.1) is to minimize the spare capacity required for configuration of the node-and-link protecting p -cycles. Constraint (5.2) ensures 100% (intermediate) node failure restorability. Constraint (5.3) determines the maximum number of copies required for node failure recovery by cycle j , whereas Constraint (5.4) guarantees 100% single link failure recovery. Constraint (5.5) calculates the total spare capacity used by the selected candidate p -cycles on link mn . Constraint (5.6) is to restrict the total capacity on each link.

5.5 Efficiency score based heuristic algorithm of the node-and-link protecting p -cycle (ESHN)

The above ILP based SOPN design selects an optimal subset of candidate cycles by capacity optimization. Since ILP-based design is not scalable to large networks with a large number of multicast sessions, an efficiency score based heuristic algorithm of node-and-link

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

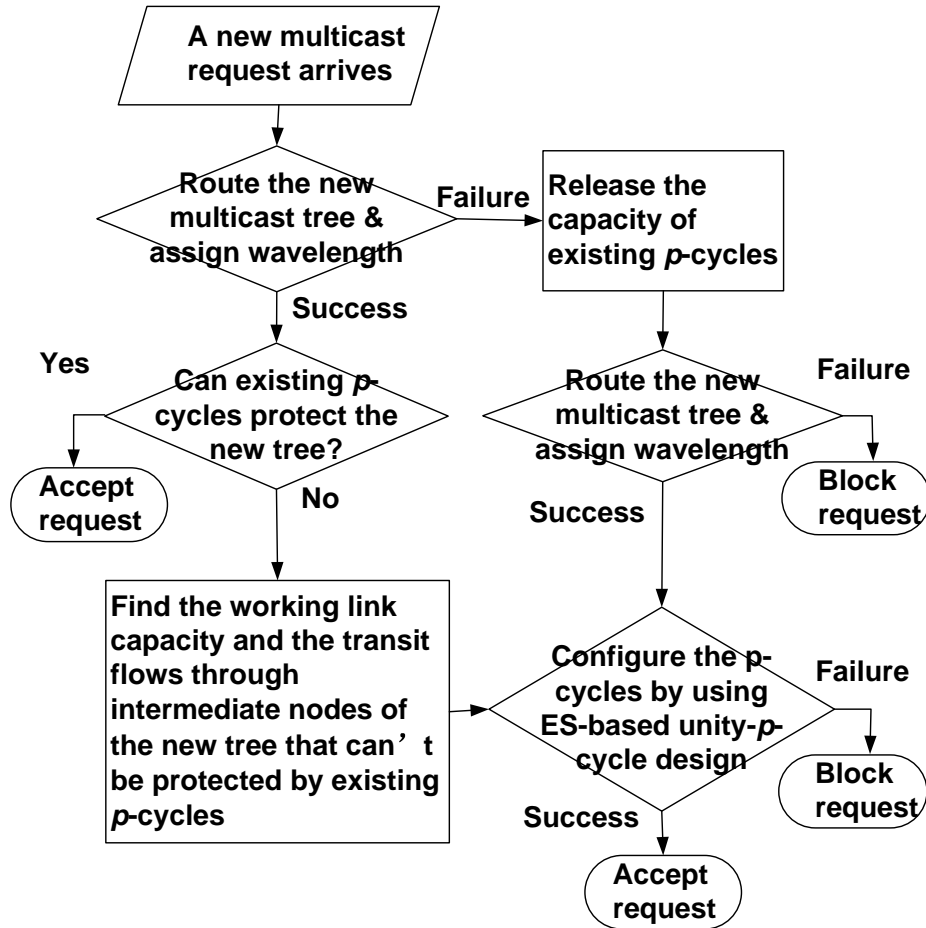
protecting p -cycle design (ESHN), which can be viewed as a multicast version of the capacitated iterative design algorithm (CIDA) in [118] and the efficiency-ratio based unity- p -cycle heuristic algorithm (ERH) in [120], are considered. Note that both the CIDA and the ERH were independently developed for dealing with link failures in the context of unicast traffic, whereas the ESHN is developed for multicast traffic protection and can be applied for link failure recovery or node failure recovery or both.

Similar to ESHT, an efficiency-score (ES) is introduced for measuring the efficiency of a cycle for combined node and link failure recovery. The ES of unity p -cycle j , which can be calculated by (5.7), is uniquely defined as the ratio of the sum of largest amount of unprotected link working capacity ($W_{j,L}$) and unprotected node transit capacity ($W_{j,N}$) that unity- p -cycle j can protect to the sum of spare capacity required by unity- p -cycle j ($\sum_{\forall mn \in E} \alpha_{j,mn}$). $W_{j,L}$ is calculated by the link protecting p -cycle principle: a unity- p -cycle can protect one working unit on any on-cycle link in opposite direction and two working units in both directions on any straddling link. $W_{j,N}$ is calculated by the flow p -cycle principle: the amount of unprotected node transit capacity can be protected by a unity- p -cycle is maximized by randomly picking the nodes that this unity- p -cycle can protect, with the constraint that no common node of multiple trees is allowed.

$$ES(c_j) = \left[W_{j,L} + W_{j,N} \right] / \sum_{\forall mn \in E} \alpha_{j,mn} \quad (5.7)$$

$W_{j,L}$ The largest amount of unprotected link working capacity that unity- p -cycle j can protect.

$W_{j,N}$ The largest amount of unprotected node transit capacity that unity- p -cycle j can protect.

$\alpha_{j,mn}$ It is 1 if cycle j traverses link mn and 0 otherwise.**Figure 5-3: Flow chart of the ESHN algorithm for dynamic multicast traffic**

For static traffic, given a network topology, the ESHN algorithm identifies all the candidate cycles using the heuristic edge-digraph based cycle algorithm [68, 241] and routes all the multicast traffic, according to the Steiner tree (ST) heuristic algorithm [239] first. Then, the ES for each unity- p -cycle is calculated and the one with the maximum ES is selected. The unprotected capacity on each link and also the unprotected transit flows passing through each node are then updated. Then, the next candidate cycle with the maximum ES is searched. The whole process iterates until all the working units on every link and all the transit flows

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

through all the nodes are protected. Finally, the algorithm outputs the number of copies required for each p -cycle.

The ESHN algorithm can also be applied to dynamic multicast traffic protection. The flow chart of p -cycle reconfiguration process of the ESHN algorithm for dynamic multicast traffic protection is presented in **Figure 5-3**. The process presented is similar to the dynamic p -cycle (DpC) algorithm in [231], but we here also consider the node failure recovery in the ESHN.

Upon the arrival of a new multicast request, the proposed model first tries to route the new multicast tree using the ST heuristic algorithm [239] and assign wavelengths to it. If the new multicast tree is successfully set up (The tree can be set up if there is a simple path with enough remaining free capacity from the source to each destination), the proposed model attempts to protect the new multicast tree by using the existing p -cycles. If the existing p -cycles cannot fully protect the whole new multicast tree (its link working capacity and node transit capacity) but only part of the new multicast tree, additional new unity- p -cycles will be configured to protect the unprotected link working capacity and node transit capacity, if there is enough remaining free capacity for configuring cycles. If the routing of the new multicast tree is successful and all its link working capacity and node transit capacity can be protected by the existing p -cycles or by a combination of the existing p -cycles and newly configured p -cycles, the request is accepted; otherwise, it is blocked. On the other hand, if the new multicast tree cannot be set up within the remaining capacity of the network, all the existing p -cycles will be released for reconfiguration. As the old configuration of p -cycles may not fit the traffic, the purpose of the reconfiguration is to make the newly configured cycles to fit the current multicast traffic, so as to accommodate the new incoming multicast request. After releasing the existing p -cycles, the proposed model attempts to route the new multicast tree, and reconfigure p -cycles to protect all the existing multicast trees as well as the new multicast tree. If this is successful, the new multicast request is accepted, otherwise it is blocked.

Upon successful setup of the new multicast request, the new multicast tree begins service. If a link or a node in the network fails, the multicast trees traversing the failed link or the failed node are rapidly switched to their corresponding pre-cross-connected p -cycles. Because the p -cycles are pre-configured, the service recovery exhibits ring-like fast speed and takes about typically 30–80 ms [106, 247]. It is noted that a multicast tree will be tore down and its occupied capacity will be released upon the completion of the service of that multicast tree. In the mean time, the corresponding p -cycles are also released if they no longer protect any multicast light trees.

5.6 Performance evaluation for static traffic protection

For performance evaluation, we select the COST239 network (11 nodes and 26 links), the NSFNET network (14 nodes and 21 links) and the US backbone network (24 nodes and 43 links) are selected as the test networks (shown in **Figure 5-4**), whose average node degrees are 4.727, 3 and 3.583, respectively.

The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM. In this study, for every multicast session, the source node is randomly selected among all the nodes, and the set of destination nodes is also randomly selected among all the nodes excluding the source node, following uniform distribution. For static traffic protection, each link is assumed to have two fibers of 64 wavelengths per fiber, transmitting in opposite directions. For every multicast group size, 20 independent simulation experiments are performed and the average value is obtained. For each simulation experiment, 20 multicast sessions were generated.

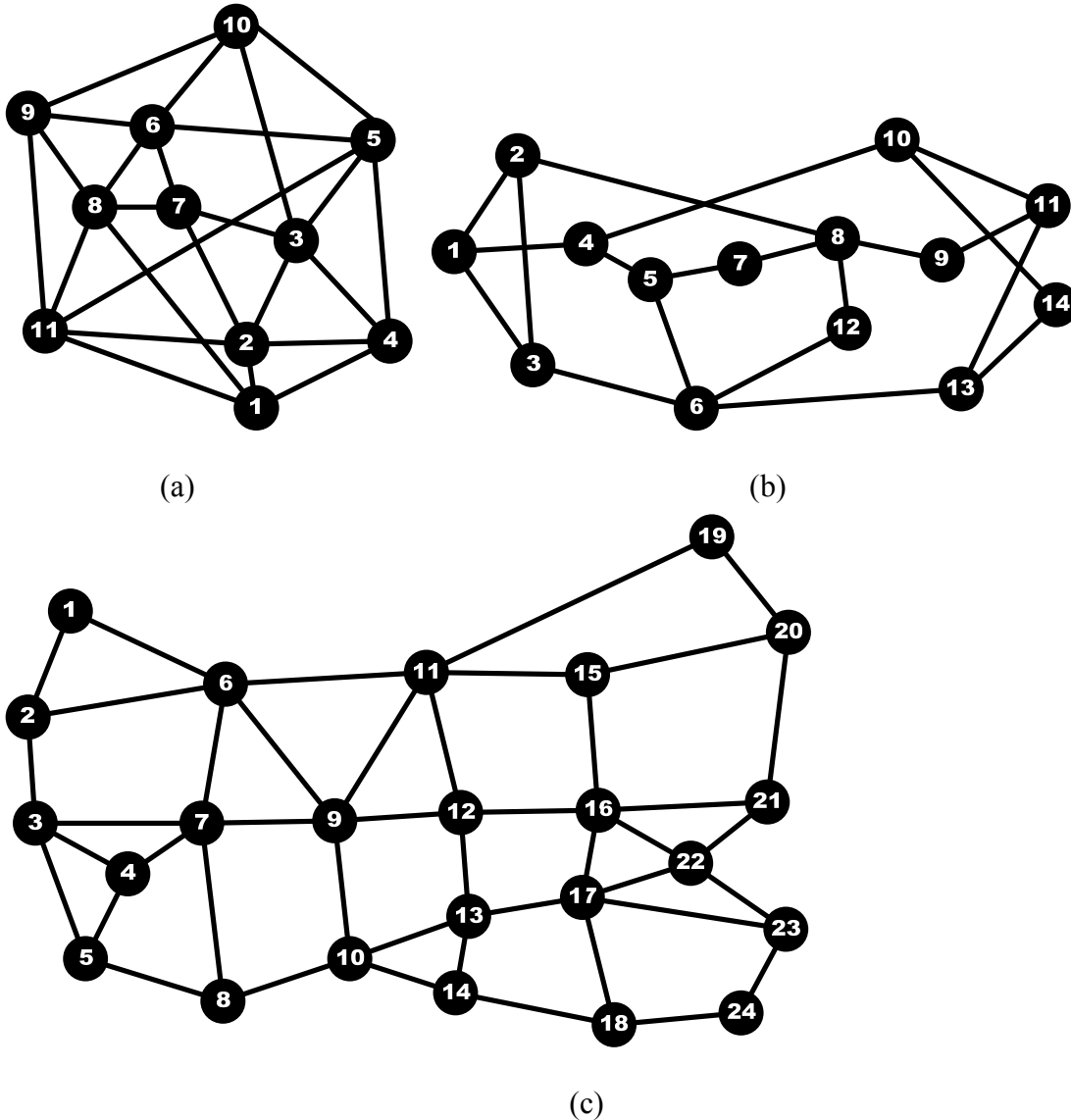


Figure 5-4: Test networks: (a) COST239 network; (b) NSFNET network; (c) US backbone network

Firstly, the cycle hop limit (H) effect on the required average total capacity of the four p -cycle based algorithms in the COST239 network is examined. The results are shown in **Table 5-1**. As the H increases, longer and more efficient cycles are selected and hence the required total capacity is reduced. The average total capacity (TC) required for the case of link failure recovery (LR) as well as for the case of combined node and link recovery (CNLR) in the COST239 network is compared in **Table 5-2**.

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach**Table 5-1: The cycle hop limit (H) effect on the required total capacity for four p -cycle based algorithms in the COST239 network (multicast group size $k = 5$)**

H	5	6	7	8	9	10	All
ESHT	279.6	267.2	259.2	255.2	252.1	249.4	248.5
SOPT	261.7	250.2	243.3	236.7	233.1	230.3	229.8
ESHN	218.3	203.6	199.4	195.8	193.1	191.6	190.6
SOPN	198.3	182.3	176.7	175.1	174.7	173.2	173.1

Table 5-2: Comparison between the average total capacity (TC) required by 20 random multicast sessions for link failure recovery (LR) and those for combined node and link recovery (CNLR) in COST239 network ($k=5$)

Algorithms	TC_{LR}	TC_{CNLR}	PI	RE_{CNLR}
ESHT	233.1	248.5	6.6%	1.4126
SOPT	201.4	229.8	14.1%	1.2311
OPP-SDP	225.7	240.8	6.7%	1.0031
ILP-OPP	216.2	224.1	3.7%	1.0008
ESHN	162.4	190.6	17.4%	0.8505
SOPN	155.2	173.1	11.5%	0.6806

The total capacity required by most protection algorithms would increase if the node failure recovery capability is required on top of the link failure recovery capability. However, surprisingly, the extra capacity increased for node failure recovery is quite small (less than 17.4%). The percentage increase (PI) is defined to be the ratio of the difference of the total capacities in the CNLR case and the LR case to the total capacity in the LR case. The SOPN consumes the least total capacity for both the LR and the CNLR cases; whereas the PI of the total capacity for the ILP-OPP is the smallest. The average redundancy (RE) (which is

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

defined as the average ratio of the spare capacity reserved to the working capacity [27]) for the CNLR case is shown in the 4th column. The RE can be calculated by (5.8):

$$RE = \frac{\sum_{\forall mn \in E} c_{mn} v_{mn}}{\sum_{\forall mn \in E} c_{mn} w_{mn}} \quad (5.8)$$

c_{mn} is the cost for a unit capacity on link mn (1 in this study). w_{mn} is the number of working units occupied by the multicast sessions on link mn , and v_{mn} is the number of spare units required to be reserved on link mn to configure p -cycles.

Generally, heuristic algorithms have higher redundancy compared with their respective ILP bench marks. Among all algorithms, the SOPN has the least redundancy (68.06%), while the ESHT has the highest redundancy (141.26%).

The comparison of the average total computational time (TI) for setting up a multicast session in COST239 network is shown in **Table 5-3**. For the LR case, the node-and-link protecting p -cycle based approach is essentially the link-protecting p -cycle based approach: the ESHN and the SOPN correspond to the efficiency-ratio based unity- p -cycle heuristic algorithm (ERH) [120, 231] and the spare capacity optimization algorithm of p -cycle based link protection (SOPL) [232]. The ESHN is the fastest among all the algorithms. For the CNLR case, the OPP-SDP is the fastest. The computational speed of the ESHN is slowed down in the CNLR case by the process of maximizing the node transit capacity that can be protected by each unity- p -cycle. The SOPN is also slowed down, because spare capacity required for node failure recovery is minimized by considering largest node-failure-specific

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

simultaneous use. Heuristic algorithms are also shown to be faster than the corresponding ILP algorithms.

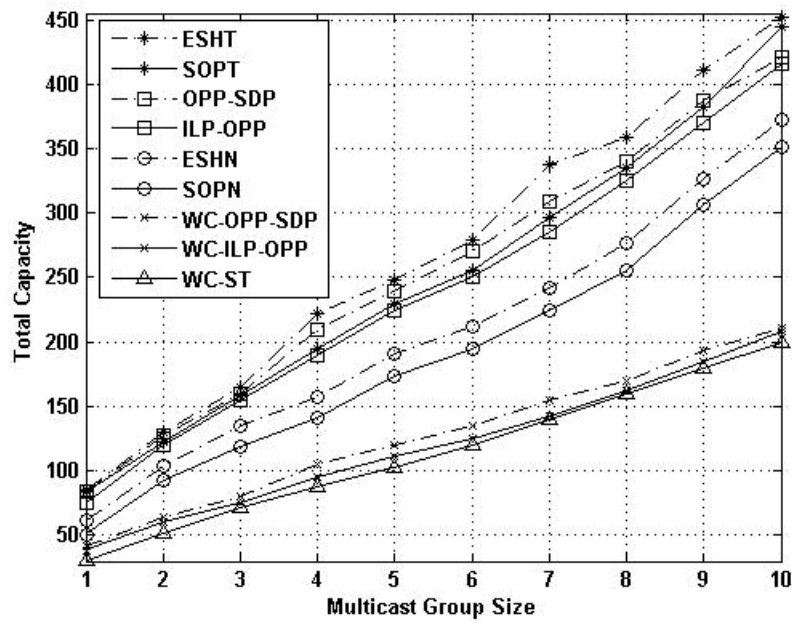
Table 5-3: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in static traffic environment (multicast group size = 5)

Algorithms	ESHT	SOPT	OPP-SDP	ILP-OPP	ESHN	SOPN
$TI_{LR}(\text{ms})$	100	400	15	1430	6	25
$TI_{CNLR}(\text{ms})$	110	430	18	1500	750	1120

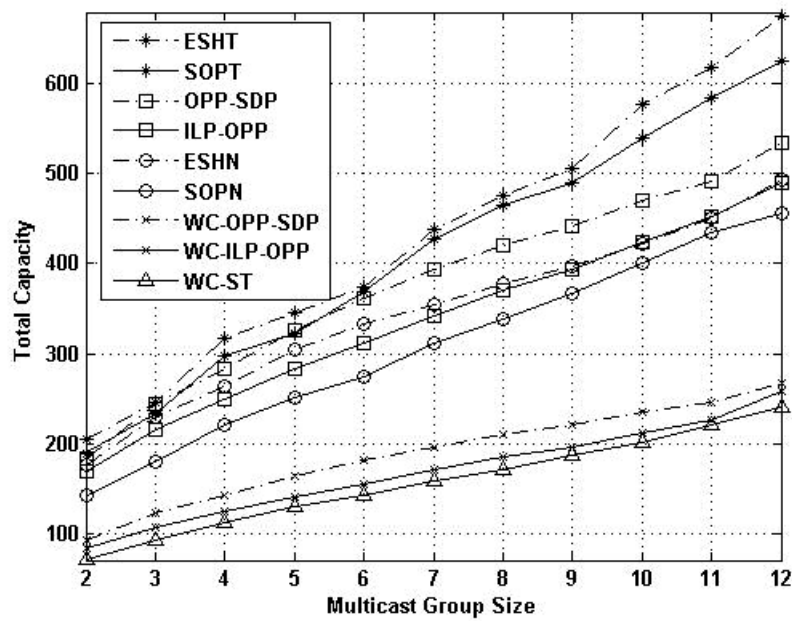
Table 5-4: Comparison of the number of variables and constraints in different ILP algorithms

ILPs	Number of variables	Number of constraints
SOPT	$ E + C \times DTS + C $	$ T + C + 2 E $
SOPN	$ E + C \times T \times N + C $	$ N \times (T + C) + 3 E $
ILP-OPP	$ 2k \times T \times (E + N) + E \times (T + 1) $	$k \times T \times (8 + 6 E + 3 N) + 2 E $

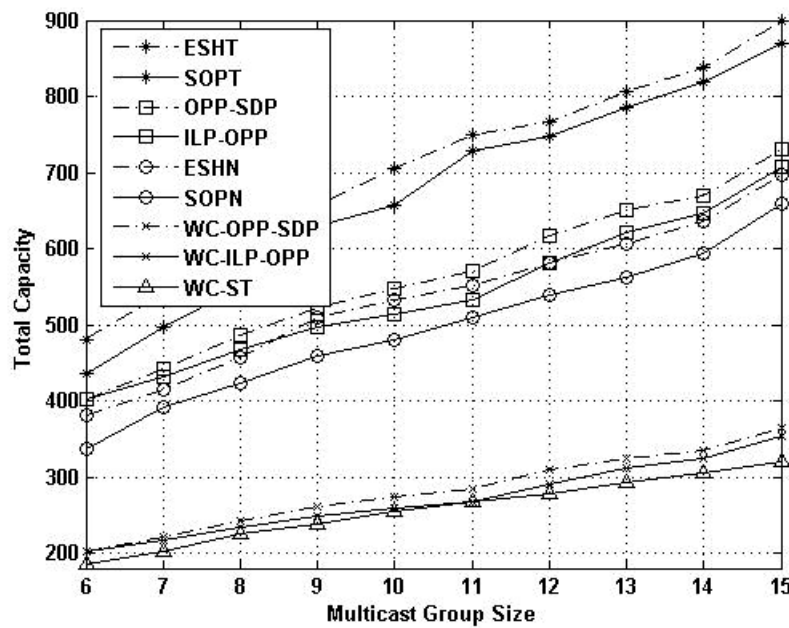
Generally, besides the platform factor, the computational time also increases with the computational complexity of the algorithms. Two factors affecting the computational complexity of the ILP algorithms are the number of variables and constraints, which are compared in **Table 5-4**. $|N|$ is the number of nodes. $|E|$ is the number of edges. $|C|$ is the number of cycles. $|T|$ is the number of multicast sessions. $|DTS|$ is the number of DTSs. k is the multicast group size. $|E|$ and $|C|$ would increase with $|N|$ and the nodal degree. Note that $|C|$ could be reduced considerably using p -cycle pre-selection strategies reported in [27], whereby the computational speed of p -cycle based algorithms would be significantly increased at the cost of consuming more spare capacity.

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

(a)



(b)



(c)

Figure 5-5: Total capacity comparison for static multicast traffic protection: ILP algorithms (solid traces) vs. heuristic algorithms (dash traces): (a) in the COST239 network; (b) in the NSFNET network; (c) in the US backbone network.

Figure 5-5 (a), (b) and (c) show the required total capacity versus the multicast group size for different ILP algorithms (in solid traces) and heuristic algorithms (in dash traces) in the COST239, NSFNET and US backbone networks, respectively. The required working capacities, which are obtained using the Steiner tree heuristic algorithm [239], the ILP-OPP algorithm and the OPP-SDP heuristic algorithm, are also shown as traces marked as “WC-ST”, “WC-ILP-OPP”, and “WC-OPP-SDP” respectively, in all three sub-figures. As the multicast group size increases, more links and nodes are traversed by each multicast tree and hence the working capacity required by multicast trees would increase. In all the three test networks, the SOPN achieves the best capacity efficiency among all algorithms. This is because, for node failure recovery, the optimization in the SOPN chooses the least copies of each cycle just enough to satisfy the failure-specific simultaneous use for copies of each cycle; for link failure recovery, the spare capacity is shared among different multicast sessions.

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

However, the OPP does not consider sharing of the spare capacity among different multicast sessions [220]. The efficiency of tree-protecting p -cycle based approach is inferior to the rest, because it is difficult to enumerate all the DTSs [229, 232]. Besides, splitting one tree into several sub-trees require overlapping at the splitting node for splitting node failure recovery, which further decreases the efficiency. As shown in **Figure 5-5**, the ILP algorithms achieve better results than their corresponding heuristic methods, but their differences are quite small.

The advantage of the ILP algorithms is that they solve all the variables simultaneously and can obtain the globally optimized solution (the selection of p -cycles for the SOPN and the SOPT, or the routing of the paths pairs for the ILP-OPP), according to both the optimization objectives and constraints. However, the ILP algorithms may be very time consuming, as the network size and the number of multicast session increase, and hence they are generally not suitable for dynamic traffic. Heuristic algorithms can only look for a locally optimized point (the most efficient cycle for the ESHN and the ESHT, or the minimum cost path pair for the first source-destination pair of the first multicast session for the OPP-SDP), based on the limited number of initial input parameters, at the beginning. Then, the results of locally optimized variables of the previous iteration would be the input parameters to the next iteration of local optimization, so as to find the next locally optimized point (after the network capacity matrixes, cost matrixes, and so on, are updated, the next most efficient cycle for the ESHN and the ESHT, or the minimum cost path pair for the next source-destination pair for the OPP-SDP). In other words, the heuristics can only get close to the global optimal point by iterative processing. Therefore, the significant drawback is their “greedy” nature: they always look for the nearest local optimal point and therefore their results are not globally optimized. The larger the network and the more the variables, the more difficult for the heuristic algorithms to get close to the global optimal point, and

therefore the larger the gap would be between the ILP algorithms and the corresponding heuristic algorithms.

Therefore, the ILP algorithms provide the theoretical optimal results, which serve as the bench marks (bounds) for the corresponding heuristic algorithms in each network so that the effectiveness of the heuristic algorithms can be assessed. However, heuristic algorithms are faster and more scalable, which are more suitable for dynamic traffic.

5.7 Performance evaluation for dynamic traffic protection

In this study of dynamic traffic protection, the COST239, NSFNET and US backbone networks are selected as the test networks. The computing platform is an Intel Quad-Core CPU (2.66 GHz) PC with 4G RAM. If the total number of available wavelengths is large, a network can support many multicast sessions simultaneously. Unless the traffic load is very high, there will not be any blockings or very few blockings. In order to evaluate the blocking effect easily, the total number of available wavelengths on each link is reduced to be 16. The total number of randomly generated multicast requests is 10^5 for each network traffic load. For every incoming request, either if no candidate backup cycles/paths can protect the request, or if one or more links are out of capacity for either routing or protection, the current request is blocked.

Traffic requests are assumed to arrive to the overall network from a Poisson process with an average arrival rate λ and have exponentially distributed holding times with a mean value μ . Hence, the network offered traffic is $\lambda\mu$. The total network traffic is a combination of unicast and multicast traffic. Let R be the probability that a traffic request is a multicast request, which can be considered as the percentage of the multicast requests to the total requests. Multicast requests are assumed to be of random multicast group size, following a

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

truncated geometric distribution [256] with parameter q . The probability of a multicast request with group size k is given by (5.9):

$$P(x = k) = \left[(1-q)q^{k-1} \right] / \left[(q - q^{N-1}) \right], 2 \leq k \leq N-1 \quad (5.9)$$

The average multicast group size for a multicast request can be calculated by (5.10):

$$E(x) = \left[2q - q^2 - Nq^{N-1} + (N-1)q^N \right] / \left[(1-q)(q - q^{N-1}) \right] \quad (5.10)$$

Proof:

$$\begin{aligned} E(x) &= \sum_{k=2}^{N-1} P(x = k) \times k = \sum_{k=2}^{N-1} \frac{(1-q)q^{k-1}}{q - q^{N-1}} \times k \\ &= \frac{1-q}{q - q^{N-1}} \sum_{k=2}^{N-1} kq^{k-1} = \frac{1-q}{q - q^{N-1}} \sum_{k=2}^{N-1} (q^k)' = \frac{1-q}{q - q^{N-1}} \left(\sum_{k=2}^{N-1} q^k \right)' \\ &= \frac{2q - q^2 - Nq^{N-1} + (N-1)q^N}{(1-q)(q - q^{N-1})} \end{aligned}$$

The effective multicast traffic load ρ_1 , effective unicast traffic load ρ_2 , and effective total traffic load ρ are defined as follows:

$$\rho_1 = \lambda \mu RE(x) \quad (5.11)$$

$$\rho_2 = \lambda \mu (1 - R) \quad (5.12)$$

$$\rho = \lambda \mu [RE(x) + (1 - R)] \quad (5.13)$$

Both the effective multicast traffic load and the total traffic load take into account the average multicast group size $E(x)$. Let $r = \rho_1 / \rho$ be the multicast traffic parameter, which is

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

defined as the ratio of the effective multicast traffic load to the effective total traffic load. r can be calculated by (5.14):

$$r = \rho_{1N} / \rho_N = \frac{N\lambda RE(x)}{N\lambda RE(x) + N\lambda(1-R)} = \frac{R \bullet E(x)}{R[E(x)-1] + 1} \quad (5.14)$$

$$R = \frac{r}{(1-r)E(x) + r} \quad (5.15)$$

As shown in the **Figure 5-6**, r increases with both R and $E(x)$.

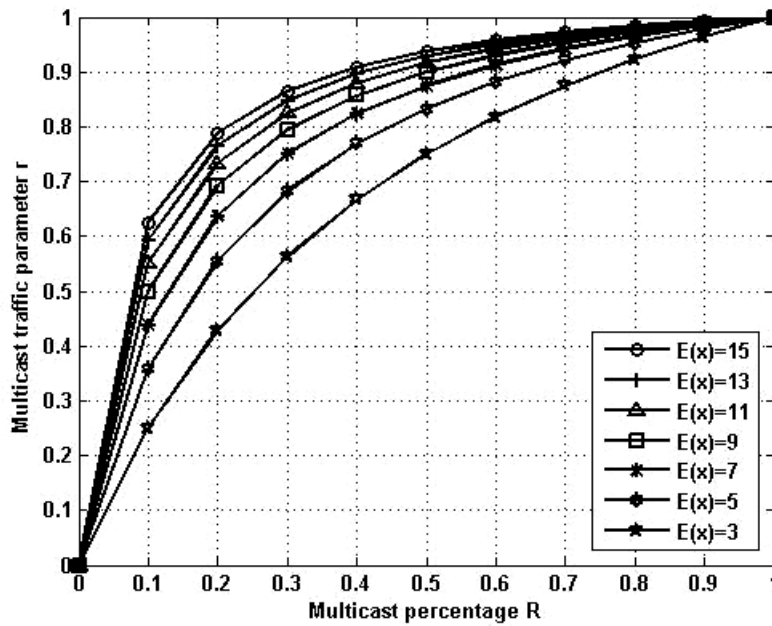
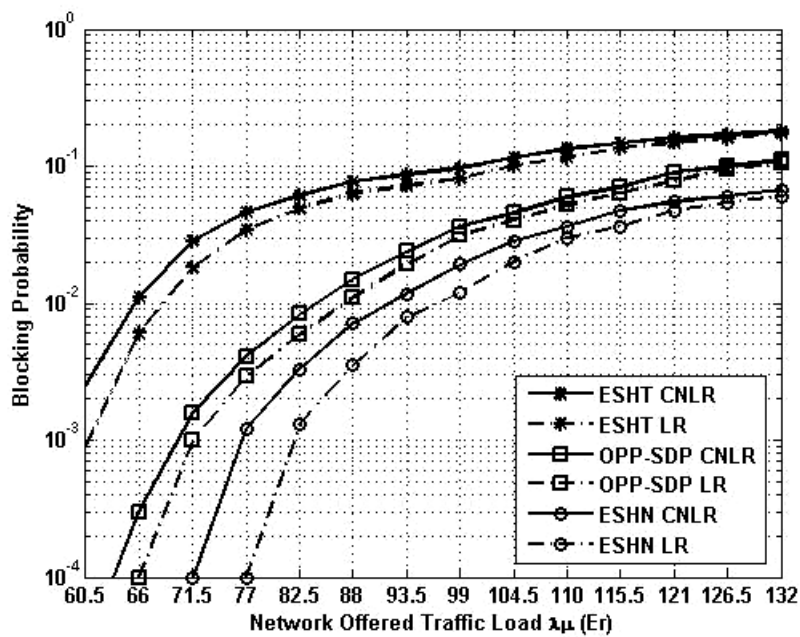
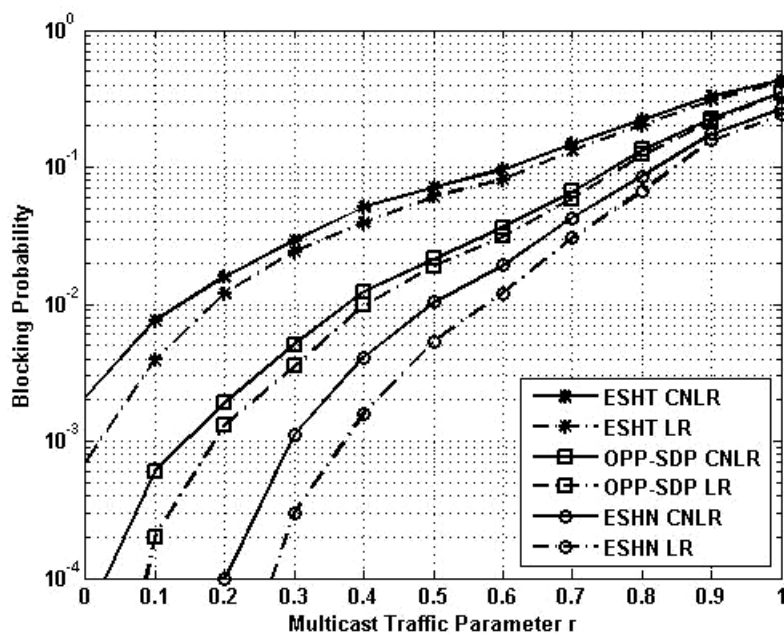


Figure 5-6: Multicast traffic parameter r vs. multicast percentage R with different average multicast group size $E(x)$



(a)



(b)

Figure 5-7: Blocking performance comparison in COST239 network for dynamic multicast traffic protection (the average multicast group size $E(x)$ is 5): (a) r is fixed at 0.6, (b) the network offered traffic load $\lambda\mu$ is fixed at 99 Erlang.

Simulation results for the COST239 network in **Figure 5-7 (a) and (b)** (results for the CNLR case are shown in solid traces; whereas the results for the LR case are shown in dash

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

traces.) show that, the blocking probability increases with the network offered traffic load and the multicast traffic parameter r , respectively. This is because, as the network offered traffic load increases, there are more demands within the same period of time. As the multicast traffic parameter r increases, there is more multicast traffic, which consumes more capacity than unicast traffic. (Unicast traffic is equivalent to multicast traffic with multicast group size equal to one. The larger the multicast group size, the more capacity is consumed). Similar trends have been observed in the NSFNET and US backbone networks. Hence, it is advised that, when r is high, the network offered traffic load should be controlled to be moderate, in order to keep a low blocking performance. As expected, compared with the results in the LR case, the blocking probabilities for the CNLR case are higher for all the algorithms, because more spare capacity is required for additional node failure recovery capability, on top of the link failure recovery capability. However, the difference between the blocking performance traces of the CNLR case and the LR case is not large, as it has been proven in the simulations for static traffic that, the extra capacity increased for node failure recovery is quite small (less than 17.4%). Thus, network operator can provide three classes of protection for multicast services: (1) without protection; (2) with link failure recovery; (3) with combined node and link failure recovery. The higher the class of protection, the more cost, and therefore more fees would be charged to multicast service content providers.

In the three test networks, for both the CNLR and the LR cases, the simulation results show that the ESHN outperforms the rest of the heuristic algorithms. This is agreeable with the results obtained in the simulations for static traffic. This is because the node-and-link protecting p -cycle based approach considers both inter-request spare capacity sharing and intra-request spare capacity sharing. However, the OPP-based approach only considers intra-request spare capacity sharing. Generally, more capacity-efficient protection approaches achieve better blocking performance.

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

The simulation results also show that the blocking performance of the ESHN and the OPP-SDP are superior to that of the ESHT. One of the reasons is because that, the tree partitions in the ESHT divide the working trees into overlapped working domains for node failure recovery, which requires extra spare capacity. Another reason is that because it is difficult to enumerate all the DTSs [229, 232].

Table 5-5: Comparison of the average total computational time (TI) for setting up a multicast session in COST239 network for the LR case and for the CNLR case in dynamic traffic environment ($E(x)=5$, $r=0.6$, $\lambda\mu = 60.5$ Erlang)

Algorithms	OPP-SDP	ESHT	ESHN
$TI_{LR}(\text{ms})$	26	329	18
$TI_{CNLR}(\text{ms})$	47	380	1550

The comparison of the average total computational time for setting up a multicast session in the COST 239 network for dynamic traffic protection is shown in **Table 5-5**. Similar to the results obtained in static traffic simulations, the ESHN is the fastest for the LR case, whereas the OPP-SDP is the fastest for the CNLR case. The average total computational time for setting up a multicast session is longer for dynamic traffic protection, compared with those in static traffic protection, because of the network state update process (working/spare/total capacity matrixes update process, registry and release of trees/paths/cycles, etc), blocking check process and p -cycle reconfiguration process and so on.

Besides the capacity consumption and computational time, another important performance criterion is the restoration speed. p -cycle based protection approaches offer much faster restoration speed, because p -cycles are fully preconfigured with preplanned spare capacity, where only on-cycle end nodes of protection entity (link, segment-flow, path or tree) handle the switching after the failure [27, 36, 139, 229]. No switching and configuration processes

are required at the intermediate nodes. In contrast, path-based approaches require a complicated two way signaling process (e.g., following the RSVP-TE protocol, which consists of a PATH message and a RESV message to inform multiple relevant nodes to configure the backup paths) and cross-connection process, which results in much longer restoration time [139].

5.8 Conclusions

In this chapter, the node-and-link protecting p -cycle based approach was proposed. Its performance was investigated and evaluated, in comparison to the tree-protecting p -cycle based approach and the OPP based approach. The node-and-link protecting p -cycle based approach protects individual nodes (on the flows) and links. The selected p -cycles are shared by nodes and links. The tree protecting p -cycle based approach protects multiple mutually disjoint trees (or sub-trees) on an end-to-end basis. The selected p -cycles are shared by multiple mutually disjoint trees.

The OPP based approach is selected for performance evaluation and comparison, because it was reported to be most efficient among the existing approaches [204]. The OPP based approach protects the paths from the source to every destination in each multicast session. Both the node-and-link protecting p -cycle based approach and the tree protecting p -cycle based approach consider inter-request and intra-request capacity sharing. However, the OPP-based approach only considers intra-request capacity sharing.

Besides, p -cycle based protection approaches offer much faster restoration speed, because p -cycles are fully preconfigured. Simulation results show that the SOPN algorithm achieves the best capacity efficiency in static traffic. For dynamic traffic simulations conducted, the

Chapter 5: Node and Link Protecting p -Cycle Based Multicast Protection Approach

ESHN algorithm outperforms the rest of the approaches. Besides, p -cycle based protection approaches offer much faster restoration speed, because p -cycles are fully preconfigured.

Chapter 6. Conclusions and Future Work

6.1 Conclusions

WDM networks transport huge amount of unicast/multicast traffic, in order to meet exponentially increasing demand. As network failures are capricious, without an efficient and fast recovery mechanism, a network failure can cause huge data loss and therefore lead to severe disruption to network services and calamitous loss to end users. Hence, failure resilience is crucial to WDM networks, especially for multicast traffic, as multicast traffic suffers even more in a network failure, compared with the unicast traffic.

The optical network resilience consists of four steps: (i) fault detection; (ii) fault localization; (iii) fault notification; (iv) fault mitigation [97]. Fault detection should be handled at the layer closest to the failure; for optical networks, this is the physical layer. Fault localization requires communication between nodes to determine where the failure has occurred. Once a failure has been detected and localized, the node(s) responsible for fault mitigation must be notified and repair procedures should be initiated. Fault mitigation is typically done by using protection and restoration approaches.

This thesis focused on the investigation of optical multicast traffic protection approaches for WDM mesh networks, in particular, the pre-configured protection cycle (p -cycle) based approaches, because the p -cycle based approaches can provide protection with ring-like fast speed and mesh-like high capacity efficiency. p -cycles based protection approaches have been intensively studied for unicast traffic protection, but have not been investigated for multicast traffic protection yet. The p -cycles make use of the ring protection switching function (originally developed and used in SONET/SDH rings) to perform fast protection switching, but goes beyond the ring functionality.

In Chapter 3, the link-protecting p -cycle based protection approach was analyzed for multicast traffic protection for link failure recovery. Link protecting p -cycles provide both ring like restoration speed (because upon a link failure, only the end nodes of the failed link handle the protection switching) and mesh like efficiency (because link protecting p -cycles protect both on-cycle links and straddling links, compared with rings). Besides applying link protecting p -cycle based protection algorithms previously proposed for unicast traffic protection (such as the SOPL algorithm and the ERH algorithm for static multicast traffic protection, p -cycle based PWCE algorithm and the DpC algorithm for dynamic multicast traffic protection), new link protecting p -cycle based protection algorithms were also proposed for multicast traffic protection (such as the JOPL algorithm, the NJOPL algorithm for static multicast traffic protection, and the hybrid DpC and PWCE algorithm for dynamic multicast traffic protection). In the simulations conducted, the link protecting p -cycle based protection approach was shown to outperform other existing multicast traffic protection approaches for link failure recovery, in terms of capacity efficiency in static traffic environment and blocking performance for dynamic traffic environment.

In Chapter 4, motivated by the serious impact of node failures, the tree-protecting p -cycle based multicast traffic protection approach (the SOPT algorithm and ESHT algorithm) was proposed and examined for combined node and link failure recovery. The advantage of tree-protecting p -cycle based approach over link protecting p -cycle based approach is the ability of the node failure recovery. Tree protecting p -cycles protect light trees (or sub-trees) on an end-to-end basis. For the case of link failure recovery, the same copy of a p -cycle can protect multiple mutually link-disjoint trees, as long as these trees are arc-disjoint with the cycle and their source and destination nodes are all on-cycle. For the case of combined node and link failure recovery, in addition to satisfying the constraints on link failure recovery, trees sharing the same copy of a p -cycle have to be mutually node-disjoint, and node-disjoint with

the protection path provided by the cycle. For both the node failure recovery and link failure recovery, the end nodes of the trees (or sub-trees) are responsible for the protection switching. Tree-protecting p -cycle based approach retains the ring-like fast restoration speed, because p -cycles are pre-configured, and only the end nodes of the trees handle the protection switching upon a link/node failure. However, the capacity efficiency of the tree-protecting p -cycle based approach is limited by the difficulty of enumerating all possible disjoint tree sets (DTS) and so on.

In Chapter 5, to improve the performance for combined node and link failure recovery, the node-and-link protecting p -cycle based protection approach (the SOPN algorithm and the ESHN algorithm) was proposed. In contrast to the tree protecting p -cycle based approach, the node-and-link protecting p -cycle based protection approach protects individual nodes and links of the multicast trees. The link failures are restored through the conventional link-protecting p -cycle principle, whereas the node failures are restored by the flow p -cycles like principle. Hence, the node and link protecting p -cycles are able to protect on-cycle/straddling links and the nodes on the portions of the trees that “flow” across the cycles. The node-and-link protecting p -cycle based approach retains the ring-like fast restoration speed, because p -cycles are pre-configured, and only the end nodes of failed link handle the protection switching upon a link failure, or end nodes of the flows handle the protection switching upon a node failure. This study showed that node-and-link protecting p -cycle based protection approach is superior to the existing multicast protection approaches, in terms of capacity efficiency in static traffic environment and blocking performance for dynamic traffic environment, for combined node and link failure recovery.

Through the studies of multicast traffic protection, it was proven that, similar to the unicast traffic protection case, p -cycle based approaches are also very promising for optical multicast traffic protection, in terms of capacity efficiency, blocking performance and recovery speed.

The proposed p -cycle based protection approaches can prevent severe disruptions to optical multicast traffic and calamitous loss to end users. The work on optical multicast protection presented in this thesis can be classified into another new category: p -cycle based multicast protection approaches [229-234]. It is believed that this work is of significance of preventing catastrophic loss to network operators and users, as the p -cycles were extended to multicast protection for the first time.

6.2 Suggestions for future work

The future work can be explored in the following four topics: (i) the first topic is to consider sparse wavelength conversion and sparse splitting in our current work; (ii) the second topic is the traffic protection in IP/WDM networks, considering joint optimization of routing, grooming, and protection; (iii) the third topic is the theoretical analysis of blocking probability and availability of optical multicast traffic protection; (iv) the fourth topic is in the direction of survivable network designs of wavelength division multiplexing – passive optical networks (WDM-PONs).

In the current study, every node in the network is assumed to be equipped with full wavelength conversion capability and multicasting capability. The assumptions of full wavelength conversion capability and the splitting capability at every node are mainly to reduce the problem complexity, so that study could be focused on the multicast traffic protection, without taking into consideration of sparse wavelength conversion problem and sparse splitting problem. In the future work, if sparse wavelength conversion and sparse splitting are considered, adding more constraints into the algorithms is necessary. The total capacity (static traffic) required and the number of blockings (dynamic traffic) would

increase. Current results could serve as a lower bound for the future work considering sparse wavelength conversion (or without wavelength conversion) and sparse splitting.

The trend of network revolution is moving towards IP/WDM networks [243, 244, 257-259]. We believe that research in traffic protection in IP/WDM networks [251, 260, 261] is worthwhile. In the current study, to efficiently utilize the huge bandwidth offered by optical multicast, the traffic of relevant higher layer applications is assumed to be groomed into one or more multicast sessions. This assumption provides ease for us to focus on multicast traffic protection in the current study. Nevertheless, future work can be focused on the problem of joint optimization of grooming, routing and protection. Performance comparison can be done to check the advantages and disadvantages of protection in the IP layer and protection in the WDM layer.

For provisioning dynamic traffic, the simulation-based performance evaluation has the weakness of the lack of generality of the results. Statements for the simulations scenarios can only be made in the test networks considered. A rigorous theoretical analysis (similar to Kaufman analysis [262-264]) and mathematical models of the blocking probability are recommended for optical multicast and optical multicast traffic protection, in comparison to previous simulation-based performance evaluation. Besides the mathematical models of the blocking probability, the analysis on the availability of optical multicast and optical multicast protection has been rarely studied. It is believed that survivable network designs for optical multicast with availability constraints are worthwhile.

The hierarchical structure of a current WDM network consists of the backbone network, the metropolitan area network and the access network. Recently, the WDM-PON [265-267] has been actively researched as a potential technology for the next generation access networks. As a WDM-PON [268-276] carries huge data, a network failure could also cause huge loss to

Chapter 6: Conclusions and Future Work

the end customers. Fast and efficient protection approaches or survivable structure designs are crucial to the development of the WDM-PON as well.

References

- [1] Internet World Statistics, <http://www.internetworldstats.com/>.
- [2] T. J. Walsh and D. R. Kuhn, "Challenges in securing voice over IP," *IEEE Security & Privacy Magazine*, vol. 3, no. 3, pp. 44-49, 2005.
- [3] J. D. Weisz, S. Kiesler, H. Zhang, Y. Ren, R. E. Kraut, and J. A. K. Konstan, "Watching together: integrating text chat with video," in Proc. *SIGCHI'07*, San Jose, California, USA pp. 877 - 886, 2007.
- [4] A. N. Bonnie, J. S. Diane, G. Michelle, and S. Luke, "Why we blog," *ACM Commun.*, vol. 47, no. 12, pp. 41-46, 2004.
- [5] F. Thouin and M. Coates, "Video-on-demand networks: design approaches and future challenges," *IEEE Network*, vol. 21, no. 2, pp. 42-48, 2007.
- [6] N. F. Huang and H. I. Liu "Wavelength division multiplexing-based video-on-demand systems," *IEEE/OSA J. Lightw. Technol.*, vol. 17, no. 2, pp. 155-164, 1999.
- [7] E. Carmen, "Video conferencing as a technology to support group work: a review of its failures," in Proc. *CCSCW'88*, Portland, Oregon, United States, pp. 13 - 24, 1988.
- [8] M. J. Rosenberg, *E-learning: Strategies for Delivering Knowledge in the Digital Age*: McGraw-Hill Professional, 2001.
- [9] T. Anderson, *E-learning in the 21st Century: A Framework for Research and Practice*: Routledge, 2003.
- [10] R. Kishimoto and I. Yamashita, "HDTV communication systems in broadband communication networks," *IEEE Commun. Mag.*, vol. 29, no. 8, pp. 28-35, 1991.
- [11] H. Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier*, 2000.
- [12] W. Cai, P. Xavier, S. J. Turner, and B.-S. Lee, "A scalable architecture for supporting interactive games on the internet," in Proc. *PADS'02*, Washington, DC, USA, pp. 54-61, 2002.
- [13] A. Hiltgen, T. Kramp, and T. Weigold, "Secure Internet banking authentication," *IEEE Security Privacy*, vol. 4, no. 2, pp. 21-29, 2006.
- [14] M. C. McChesney, "Banking in cyberspace: an investment in itself," *IEEE Spectr.*, vol. 34, no. 2, pp. 54-59, 1997.
- [15] H. Anderson, "Money and the Internet: a strange new relationship," *IEEE Spectr.*, vol. 34, no. 2, pp. 74-76, 1997.
- [16] P. Lipinski and J. Korczak, "Early warning in online stock trading systems," in Proc. *ISDA'05*, Wroclaw, Poland, pp. 538 - 543, 2005.
- [17] M. N. Huhns and J. M. Vidal, "Online auctions," *IEEE Internet Comput.*, vol. 3, no. 3, pp. 103-105, 1999.
- [18] T. Murata, "Visualizing the structure of Web communities based on data acquired from a search engine," *IEEE Trans. Ind. Electron.*, vol. 50, no. 5, pp. 860-866, 2003.
- [19] L. Introna and H. Nissenbaum, "Defining the Web: the politics of search engines," *Computer*, vol. 33, no. 1, pp. 54-62, 2000.
- [20] J. Feldman, "File sharing madness," *Network Magazine*, vol. 19, no. 11, pp. 41-2, 2004.
- [21] L. Kwei-jay, "E-Commerce Technology: Back to a Prominent Future," *IEEE Internet Comput.*, vol. 12, no. 1, pp. 60-65, 2008.

-
- [22] D. A. Hantula, D. D. Brockman, and C. L. Smith, "Online Shopping as Foraging: The Effects of Increasing Delays on Purchasing and Patch Residence," *IEEE Trans. Prof. Commun.*, vol. 51, no. 2, pp. 147-154, 2008.
 - [23] M. Limayem, M. Khalifa, and A. Frini, "What makes consumers buy from Internet? A longitudinal study of online shopping," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 30, no. 4, pp. 421-432, 2000.
 - [24] S. K. Mun and J. W. Turner, "Telemedicine: Emerging e-medicine," *Annual Review of Biomedical Engineering*, vol. 1, pp. 589-610, 1999.
 - [25] L. G. Roberts, "Beyond Moore's law: Internet growth trends," *Computer*, vol. 33, no. 1, pp. 117-119, 2000.
 - [26] D. Crawford, "Fiber optic cable dig-ups : causes and cures," *Network reliability: a report to the nation - compendium of technical papers, national engineering consortium, Chicago*, 1993.
 - [27] W. D. Grover, *Mesh-Based Survivable Networks - Options and Strategies for Optical, MPLS, SONET, and ATM Networking*: Prentice Hall, 2004.
 - [28] M. R. Wilson, "The quantitative impact of survivable network architectures on service availability," *IEEE Commun. Mag.*, vol. 36, no. 5, pp. 122-126, 1998.
 - [29] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, I - Protection," in Proc. *INFOCOM'99*, New York, NY, USA, p. 5420, 1999.
 - [30] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks. II. Restoration," in Proc. *ICC'99*, Vancouver, BC, Canada, vol. 3, pp. 2023-2030, 1999.
 - [31] J. Doucette and W. D. Grover, "Comparison of mesh protection and restoration schemes and the dependency on graph connectivity," in Proc. *DRCN'01*, Budapest, Hungary, pp. 121-128, 2001.
 - [32] S. Ramamurthy, L. Sahasrabudhe, and B. Mukherjee, "Survivable WDM mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 4, pp. 870-883, 2003.
 - [33] D. Johnson, "Survivability strategies for broadband networks," in Proc. *GLOBECOM '96*, London, UK, vol. 1, pp. 452-456 vol.1, 1996.
 - [34] T. H. Wu, "Emerging technologies for fiber network survivability," *IEEE Commun. Mag.*, vol. 33, no. 2, pp. 58-59, 62-74, 1995.
 - [35] M. Guido, P. Achille, D. P. Simone, and M. Martinelli, "Optical network survivability: protection techniques in the WDM layer," *Photonic Netw. Commu.*, vol. 4, no. 3, 2002.
 - [36] A. Kodian and W. D. Grover, "Failure-independent path-protecting p-cycles: efficient and simple fully preconnected optical-path protection," *IEEE/OSA J. Lightw. Technol.*, vol. 23, no. 10, pp. 3241-3259, 2005.
 - [37] L. Sahasrabudhe, S. Ramamurthy, and B. Mukherjee, "Fault management in IP-over-WDM networks: WDM protection versus IP restoration," *IEEE J. Sel. Areas. Commun.*, vol. 20, no. 1, pp. 21-33, 2002.
 - [38] C. Metz, "IP protection and restoration," *IEEE Internet Comput.*, vol. 4, no. 2, pp. 97-102, 2000.
 - [39] G. M. Bernstein, J. Yates, and D. Saha, "IP-centric control and management of optical transport networks," *IEEE Commun. Mag.*, vol. 38, no. 10, pp. 161-167, 2000.
 - [40] J. Zhao, L. Lei, Y. Ji, and D. Xu, "Integrated multilayer survivability strategy with inter-layer signaling," in Proc. *ICCT'03*, Beijing, PRC, vol. 1, pp. 612-616 vol.1, 2003.
 - [41] S. De Maesschalck, D. Colle, A. Groebbens, C. Develder, A. Lievens, P. Lagasse, M. Pickavet, P. Demeester, F. Saluta, and M. Quagliatti, "Intelligent optical networking for multilayer survivability," *IEEE Commun. Mag.*, vol. 40, no. 1, pp. 42-49, 2002.
-

-
- [42] G. D. Morley and W. D. Grover, "Current approaches in the design of ring-based optical networks," in Proc. *CCECE'99*, Edmonton, Alta., Canada, vol. 1, pp. 220-225 vol.1, 1999.
 - [43] O. Gerstel and R. Ramaswami, "Optical layer survivability: a post-bubble perspective," *IEEE Commun. Mag.*, vol. 41, no. 9, pp. 51-53, 2003.
 - [44] M. S. Kiaei, C. Assi, and B. Jaumard, "A survey on the p-cycle protection method," *Commun. Surveys Tuts.*, vol. 11, no. 3, pp. 53-70, 2009.
 - [45] J. Drake, "A review of the four major SONET/SDH rings," in Proc. *ICC'93*, Geneva, Switzerland, vol. 2, pp. 878-884 vol.2, 1993.
 - [46] J. Zheng and H. T. Mouftah, "Optical WDM networks - concepts and design principles," *IEEE Press*, 2004.
 - [47] G. Frosini and B. Lazzerini, "Ring-protection mechanisms: general properties and significant implementations," *IET J Comput Digit Tech*, vol. 132, no. 4, pp. 203-210, 1985.
 - [48] L. Velasco, S. Spadaro, J. Comellas, and G. Junyent, "Introducing OMS protection in GMPLS-based optical ring networks," *Comput. Netw.*, vol. 52, no. 10, pp. 1975-87, 2008.
 - [49] T. Tsuboi, M. Natori, and S. Mitachi, "Single-fiber optical protection ring architecture suitable for asymmetric traffic," in Proc. *GLOBECOM '03*, San Francisco, CA, USA, vol. vol.7, pp. 4044-8, 2003.
 - [50] M. J. Li, D. J. Tebben, M. J. Soulliere, S. Hilbert, M. Zhao, I. Lelic, D. G. Hoefer, M. Gauland, V. Kaliniouk, L. Guiziou, J. M. Jouanno, and R. E. Wagner, "Transparent two-fiber optical channel shared protection ring," *Fiber and Integrated Optics*, vol. 22, no. 6, pp. 385-404, 2003.
 - [51] D. Forbes, G. Cannel, E. Pittuck, and N. Baker, "Optical shared protection ring performance," in Proc. *ECOC '99*, Nice, France, vol. vol.2, pp. 52-3, 1999.
 - [52] D. Uehara, K. Asahi, Y. Nakabayashi, M. Yamashita, C. Konishi, and S. Fujita, "Highly reliable and economical WDM ring with optical self-healing and 1:N wavelength protection," in Proc. *ECOC'97*, Edinburgh, U.K, vol. vol.4, pp. 65-8, 1997.
 - [53] M. J. Li, M. J. Soulliere, D. J. Tebben, L. Nederlof, M. D. Vaughn, and R. E. Wagner, "Transparent optical protection ring architectures and applications," *IEEE/OSA J. Lightw. Technol.*, vol. 23, no. 10, pp. 3388-403, 2005.
 - [54] M. J. Li, "Optical protection ring architectures and applications," in Proc. *SPIE*, USA, vol. 4872, pp. 266-80, 2002.
 - [55] G. P. Doyle, "Fiber distributed data interface in naval applications," *Sea Technology*, vol. 36, no. 8, pp. 63-65, 1995.
 - [56] R. Jain, "Error characteristics of fiber distributed data interface (FDDI)," *IEEE Trans. Commun.*, vol. 38, no. 8, pp. 1244-1252, 1990.
 - [57] S. P. Joshi, "High-performance networks: a focus on the fiber distributed data interface (FDDI) standard," *IEEE Micro*, vol. 6, no. 3, pp. 8-14, 1986.
 - [58] W. E. Burr and F. E. Ross, "Fiber distributed data interface: a proposal for a standard 100 Mbit/s fiber optic token ring network," in Proc. *FOC/LAN 84*, Las Vegas, NV, USA pp. 254-257, 1984.
 - [59] L. Zong, Y. Li, H. Zhang, Y. Chu, and Y. Guo, "A novel OADM structure for two-fiber unidirectional optical path protection switching ring networks," in Proc. *SPIE*, USA, vol. 4225, pp. 1-5, 2000.
-

-
- [60] C. K. Weng and W. I. Way, "A single-fiber optical unidirectional path-switched-ring network using double-sideband-suppressed carrier modulation technique," *IEEE Photon. Technol. Lett.*, vol. 18, no. 21, pp. 2236-8, 2006.
 - [61] R. B. Billah, W. Bin, and A. S. Awwal, "Efficient traffic grooming in synchronous optical network/wavelength-division multiplexing bidirectional line-switched ring networks," *Opt. Eng.*, vol. 43, no. 5, pp. 1101-14, 2004.
 - [62] I. Rados, P. Turalija, and T. Sunaric, "Availability model of bidirectional line switched ring," in Proc. *ICTON'01*, Cracow, Poland, pp. 312-16, 2001.
 - [63] A. Fumagalli, M. Tacca, and I. Cerutti, "Minimizing the number of optical crossconnect ports in mesh networks based on bidirectional line-switched WDM self-healing ring protection," in Proc. *ICCCN'99*, Boston, MA, USA pp. 398-403, 1999.
 - [64] X. Fang, R. Iraschko, and R. Sharma, "All-optical four-fiber bidirectional line-switched ring," *IEEE/OSA J. Lightw. Technol.*, vol. 17, no. 8, pp. 1302-1308, 1999.
 - [65] W. D. Grover and R. Martens, "Optimized design of ring-mesh hybrid networks," in Proc. *DRCN 2000*, Munich, Germany, pp. 291-297, 2000.
 - [66] D. Cavendish, "Evolution of optical transport technologies: from SONET/SDH to WDM," *IEEE Commun. Mag.*, vol. 38, no. 6, pp. 164-172, 2000.
 - [67] O. Gerstel, P. Lin, and G. Sasaki, "Combined WDM and SONET network design," in Proc. *INFOCOM'99*, New York, USA, vol. 2, pp. 734-743 vol.2, 1999.
 - [68] H. Hwang, S. Ahn, Y. Yoo, and C. S. Kim, "Multiple shared backup cycles for survivable optical mesh networks," in Proc. *ICCCN'01*, Scottsdale, Arizona, USA, pp. 284-289, 2001.
 - [69] B. Mukherjee, *Optical WDM Networks*: Springer Science+Business Media, Inc., 2006.
 - [70] C. Ou and B. Mukherjee, *Survivable optical WDM networks*: Springer Science+Business Media, Inc., 2005.
 - [71] L. Zhou, M. Held, and U. Sennhauser, "Connection availability analysis of shared backup path-protected mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 25, no. 5, pp. 1111-19, 2007.
 - [72] H. Luo, H. Yu, and L. Li, "A heuristic algorithm for shared segment protection in mesh WDM networks with limited backup path/segments length," *Computer Commun.*, vol. 29, no. 16, pp. 3197-3213, 2006.
 - [73] D. A. A. Mello, D. A. Schupke, and H. Waldman, "A matrix-based analytical approach to connection unavailability estimation in shared backup path protection," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 844-846, 2005.
 - [74] J. Doucette, M. Cloqueur, and W. D. Grover, "On the availability and capacity requirements of shared backup path-protected mesh networks," *Opt. Netw. Mag.*, vol. 4, no. 6, pp. 29-44, 2003.
 - [75] P. H. Ho, J. Tapolcai, and A. Haque, "Spare capacity reprovisioning for shared backup path protection in dynamic generalized multi-protocol label switched networks," *IEEE Trans. Reliab.*, vol. 57, no. 4, pp. 551-63, 2008.
 - [76] S. Wang and L. Li, "Impairment aware optimal diverse routing for survivable optical networks," *Photonic Netw. Commu.*, vol. 13, no. 2, pp. 139-54, 2007.
 - [77] R. Bhandari, "Optimal diverse routing in telecommunication fiber networks," in Proc. *INFOCOM '94*, Toronto, Ont., Canada vol. vol.3, pp. 1498-508, 1994.
 - [78] D. Medhi, "Diverse routing for survivability in a fiber-based sparse network," in Proc. *ICC'91*, Denver, CO, USA, pp. 672-6, 1991.
 - [79] G. X. Shen and W. D. Grover, "Survey and performance comparison of dynamic provisioning methods for optical shared backup path protection," in Proc. *BROADNETS'05*, Boston, Massachusetts, USA, pp. 1310-1319, 2005.
-

-
- [80] N. N. Hoang, D. Habibi, V. P. Quoc, and L. Kungmeng, "A shared backup path protection scheme for optical mesh networks," in Proc. *APCC'05*, Perth, Australia, pp. 309-313, 2005.
 - [81] R. Martinez, R. Munoz, and R. Casellas, "Experimental evaluation of the backup sharing aggressiveness for dynamic shared path protection in GMPLS transparent optical networks," in Proc. *ICTON'08*, Athens, Greece vol. vol.3, pp. 27-30, 2008.
 - [82] D. Habibi, V. Q. Phung, and H. N. Nguyen, "Minimizing the number of constraints for Shared Backup Path Protection (SBPP) in Shared Risk Link Group (SRLG) optical mesh networks," in Proc. *ICON'07*, Adelaide, SA, Australia pp. 246-251, 2007.
 - [83] Q. Guo, P. H. Ho, A. Haque, and H. T. Mouftah, "Availability-constrained Shared Backup Path Protection (SBPP) for GMPLS-based spare capacity reprovisioning," in Proc. *ICC'07*, Glasgow, UK, pp. 2186-2191, 2007.
 - [84] N. Mallick, "Protection capacity savings due to end-to-end shared backup path restoration in optical mesh networks," in Proc. *OFC'06*, Anaheim, CA, USA p. 6 pp., 2006.
 - [85] B. Jaumard and D. L. Truong, "Backup path re-optimizations for shared path protection in multi-domain networks," in Proc. *GLOBECOM'06*, San Francisco, CA, USA, p. 6 pp., 2006.
 - [86] B. G. Jozsa, D. Orincsay, and A. Kern, "Surviving multiple network failures using shared backup path protection," in Proc. *ISCC'03*, Kemer-Antalya, Turkey vol. vol.2, pp. 1333-40, 2003.
 - [87] C. Ou, B. Mukherjee, and H. Zang, "Sub-path protection for scalability and fast recovery in WDM mesh networks," in Proc. *OFC'02*, Anaheim, California, USA, pp. 495-496, 2002.
 - [88] D. Xu, Y. Xiong, and C. Qiao, "Novel algorithms for shared segment protection," *IEEE J. Sel. Areas. Commun.*, vol. 21, no. 8, pp. 1320-1331, 2003.
 - [89] J. Tapolcai, P. H. Ho, D. Verchere, T. Cinkler, and A. Haque, "A new shared segment protection method for survivable networks with guaranteed recovery time," *IEEE Trans. Reliab.*, vol. 57, no. 2, pp. 272-282, 2008.
 - [90] D. L. Truong and B. Jaumard, "Using topology aggregation for efficient shared segment protection solutions in multi-domain networks," *IEEE J. Sel. Areas. Commun.*, vol. 25, no. 9, pp. 96-107, 2007.
 - [91] P. H. Ho and H. T. Mouftah, "A novel survivable routing algorithm for shared segment protection in mesh WDM networks with partial wavelength conversion," *IEEE J. Sel. Areas. Commun.*, vol. 22, no. 8, pp. 1548-1560, 2004.
 - [92] P. H. Ho and H. T. Mouftah, "A framework for service-guaranteed shared protection in WDM mesh networks," *IEEE Commun. Mag.*, vol. 40, no. 2, pp. 97-103, 2002.
 - [93] A. Banerjee, L. Drake, L. Lang, B. Turner, D. Awduche, L. Berger, K. Kompella, and Y. Rekhter, "Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques," *IEEE Commun. Mag.*, vol. 39, no. 7, pp. 144-151, 2001.
 - [94] A. Banerjee, J. Drake, J. P. Lang, B. Turner, K. Kompella, and Y. Rekhter, "Generalized multiprotocol label switching: an overview of routing and management enhancements," *IEEE Commun. Mag.*, vol. 39, no. 1, pp. 144-150, 2001.
 - [95] T. D. Nadeau and H. Rakotoranto, "GMPLS operations and management: today's challenges and solutions for tomorrow," *IEEE Commun. Mag.*, vol. 43, no. 7, pp. 68-74, 2005.
-

-
- [96] J. Perello, E. Escalona, S. Spadaro, J. Cornelias, and G. Junyent, "Resource discovery in ASON/GMPLS Transport Networks," *IEEE Commun. Mag.*, vol. 45, no. 10, pp. 86-92, 2007.
 - [97] J. P. Lang and J. Drake, "Mesh network resiliency using GMPLS," *Proc. IEEE*, vol. 90, no. 9, pp. 1559-1564, 2002.
 - [98] J. T. Park, "Resilience in GMPLS path management: model and mechanism," *IEEE Commun. Mag.*, vol. 42, no. 7, pp. 128-135, 2004.
 - [99] D. Leung and W. D. Grover, "Restorable mesh network design under demand uncertainty: toward future proofed transport investments," in *Proc. OFC'04*, Anaheim, California, USA, vol. 2, p. 3, 2004.
 - [100] M. Clouqueur and W. D. Grover, "Mesh-restorable networks with complete dual failure restorability and with selectively enhanced dual-failure restorability properties," in *Proc. OptiComm 2002*, Boston, MA, USA, pp. 1-11, 2002.
 - [101] S. S. Lumetta and M. Medard, "Towards a deeper understanding of link restoration algorithms for mesh networks," in *Proc. INFOCOM'01*, Anchorage, Alaska, USA, vol. 1, pp. 367-375 vol.1, 2001.
 - [102] B. D. Venables, W. D. Grover, and M. H. MacGregor, "Two strategies for spare capacity placement in mesh restorable networks," in *Proc. ICC'93*, Geneva, Switzerland, vol. 1, pp. 267-271, 1993.
 - [103] G. Li, D. Wang, C. Kalmanek, and R. Doverspike, "Efficient distributed restoration path selection for shared mesh restoration," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 761-771, 2003.
 - [104] R. R. Iraschko and W. D. Grover, "A highly efficient path-restoration protocol for management of optical network transport integrity," *IEEE J. Sel. Areas. Commun.*, vol. 18, no. 5, pp. 779-794, 2000.
 - [105] R. R. Iraschko, M. H. MacGregor, and W. D. Grover, "Optimal capacity placement for path restoration in mesh survivable networks," in *Proc. ICC' 96*, Dallas, TX, USA vol. 3, pp. 1568-1574 vol.3, 1996.
 - [106] W. D. Grover and D. Stamatelakis, "Cycle-oriented distributed preconfiguration: ring-like speed with mesh-like capacity for self-planning network restoration," in *Proc. ICC'98*, Atlanta, Georgia, USA, vol. 1, pp. 537-543 vol.1, 1998.
 - [107] D. Stamatelakis and W. D. Grover, "Theoretical underpinnings for the efficiency of restorable networks using preconfigured cycles ("p-cycles")," *IEEE Trans. Commun.*, vol. 48, no. 8, pp. 1262-1265, 2000.
 - [108] D. A. Schupke, C. G. Gruber, and A. Autenrieth, "Optimal configuration of p-cycles in WDM networks," in *Proc. ICC'02*, New York, USA, vol. 5, pp. 2761-2765, vol.5, 2002.
 - [109] D. A. Schupke, "On Hamiltonian cycles as optimal p-cycles," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 360-362, 2005.
 - [110] H. Zhang and O. Yang, "Finding protection cycles in DWDM networks," in *Proc. ICC'02*, New York, USA, vol. 5, pp. 2756-2760 vol.5, 2002.
 - [111] M. Prabhaker and D. Narsingh, "On algorithms for enumerating all circuits of a graph," *SIAM Journal on Computing*, vol. 5, no. 1, pp. 90-99, 1976.
 - [112] D. B. Johnson, "Finding all the elementary circuits of a directed graph," *SIAM Journal on Computing*, vol. 4, no. 1, pp. 77-84, 1975.
 - [113] Prabhaker Mateti and N. Deo, "On algorithms for enumerating all circuits of a graph," *SIAM Journal on Computing*, vol. 5, no. 1, pp. 90-99, 1976.
-

-
- [114] B. Wu, K. L. Yeung, and S. Xu, "ILP formulation for p-cycle construction based on flow conservation," in Proc. *GLOBECOM '07*, Washington, DC, USA, pp. 2310-2314, 2007.
 - [115] B. Wu, K. L. Yeung, K. S. Lui, and S. Xu, "A new ILP-based p-cycle construction algorithm without candidate cycle enumeration," in Proc. *ICC '07*, Glasgow, Scotland, UK, pp. 2236-2241, 2007.
 - [116] K. Lo, H. Daryoush, A. Rasan, P. Quoc Viet, N. Hoang Nghia, and K. ByungKyu, "A hybrid p-cycle search algorithm for protection in WDM mesh networks," in Proc. *ICON '06*, Singapore, vol. 2, pp. 1-6, 2006.
 - [117] K. Lo, D. Habibi, A. Rasan, Q. V. Phung, and H. N. Nguyen, "Heuristic p-cycle selection design in survivable WDM mesh networks," in Proc. *ICON '06*, Singapore, vol. 2, pp. 1-6, 2006.
 - [118] J. Doucette, D. He, W. D. Grover, and O. Yang, "Algorithmic approaches for efficient enumeration of candidate p-cycles and capacitated p-cycle network design," in Proc. *DRCN'03*, Banff, Alberta, Canada pp. 212-220, 2003.
 - [119] W. D. Grover and D. Stamatelakis, "Bridging the ring-mesh dichotomy with p-cycles," in Proc. *DRCN'00*, Munich, Germany, pp. 92-104, 2000.
 - [120] Z. R. Zhang, W. D. Zhong, and B. Mukherjee, "A heuristic method for design of survivable WDM networks with p-cycles," *IEEE Commun. Lett.*, vol. 8, no. 7, pp. 467-469, 2004.
 - [121] W. D. Grover and J. Doucette, "Advances in optical network design with p-cycles: joint optimization and pre-selection of candidate p-cycles," in Proc. *IEEE/LEOS Summer Topical Meetings'02*, Quebec, Canada, pp. WA2-49-WA2-50, 2002.
 - [122] H. N. Nguyen, D. Habibi, V. Q. Phung, S. Lachowicz, L. Kungmeng, and B. Kang, "Joint optimization in capacity design of networks with p-cycle using the fundamental cycle set," in Proc. *GLOBECOM '06*, San Francisco, CA, USA, pp. QRP02-QRP05, 2006.
 - [123] Z. Xie, J. Xing, L. Wu, and Y. Ji, "Shared p-cycles design for dual link failure restorability in optical WDM networks," *J. China Univ. Posts Tele.*, vol. 14, no. 3, pp. 74-78, 2007.
 - [124] W. Li, J. Doucette, and M. Zuo, "p-cycle network design for specified minimum dual-failure restorability," in Proc. *ICC '07*, Glasgow, Scotland, UK, pp. 2204-2210, 2007.
 - [125] M. Greene, T. Li, and B. Wang, "Improving dual-failure performance in WDM optical networks using p-cycle based protection with minimized wavelength conversion costs," *Proceedings of SPIE*, vol. 6022, no. 602229, pp. 1-12, 2005.
 - [126] D. A. Schupke, W. D. Grover, and M. Clouqueur, "Strategies for enhanced dual failure restorability with static or reconfigurable p-cycle networks," in Proc. *ICC'04*, Paris, France, vol. 3, pp. 1628-1633, 2004.
 - [127] D. A. Schupke, "Multiple failure survivability in WDM networks with p-cycles," in Proc. *ISCAS'03*, Bangkok, Thailand, vol. 3, pp. III-866-III-869 vol.3, 2003.
 - [128] H. Wang and H. T. Mouftah, "p-cycles in multi-failure network survivability," in Proc. *ICTON'05*, Barcelona, Spain, vol. 1, pp. 381-384 Vol. 1, 2005.
 - [129] L. Chang and R. Lu, "p-cycle design in survivable WDM networks with shared risk link groups (SRLGs)," *Photonic Netw. Commu.*, vol. 11, no. 3, pp. 301-311, 2006.
 - [130] C. C. Sue, S. Min-Shao, and H. Chin-Yu, "Dependable WDM networks with reconfigurable edge-disjoint p-cycles," in Proc. *ITRE'05*, Hsinchu, Taiwan, PRC, pp. 126-130, 2005.
-

-
- [131] W. He, F. Jing, and A. K. Somani, "A p-cycle based survivable design for dynamic traffic in WDM networks," in Proc. *GLOBECOM'05*, St. Louis, Missouri, USA, vol. 4, p. 5, 2005.
 - [132] W. D. Zhong and Z. R. Zhang, "p-cycles-based dynamic protection provisioning in optical WDM networks," *IEICE Trans. Commun.*, vol. E88-B, no. 5, pp. 1921-1926, 2005.
 - [133] L. Ruan and F. Tang, "Dynamic establishment of restorable connections using p-cycle protection in WDM networks," in Proc. *BROADNETS'05* Boston, MA, USA pp. 137-144 Vol. 1, 2005.
 - [134] W. D. Grover, "The protected working capacity envelope concept: an alternate paradigm for automated service provisioning," *IEEE Commun. Mag.*, vol. 42, no. 1, pp. 62-69, 2004.
 - [135] Z. R. Zhang, W. D. Zhong, and S. K. Bose, "Dynamically survivable WDM network design with p-cycle-based PWCE," *IEEE Commun. Lett.*, vol. 9, no. 8, pp. 756-758, 2005.
 - [136] G. X. Shen and W. D. Grover, "Design and performance of protected working capacity envelopes based on p-cycles for dynamic provisioning of survivable services," *J. Opti. Netw.*, vol. 4, no. 7, pp. 361-390, 2005.
 - [137] G. X. Shen and W. D. Grover, "Automatic lightpath service provisioning with an adaptive protected working capacity envelope based on p-cycles," in Proc. *DRCN'05*, Island of Ischia, Italy, p. 9, 2005.
 - [138] R. He, K. C. Chua, and G. Mohan, "Protected working lightpath envelope: a new paradigm for dynamic survivable routing," in Proc. *ICCCN '07*, Honolulu, Hawaii, USA, pp. 291-296, 2007.
 - [139] G. X. Shen and W. D. Grover, "Extending the p-cycle concept to path segment protection for span and node failure recovery," *IEEE J. Sel. Areas. Commun.*, vol. 21, no. 8, pp. 1306-1319, 2003.
 - [140] A. Kodian, W. D. Grover, and J. Doucette, "A disjoint route-sets approach to design of path-protecting p-cycle networks," in Proc. *DRCN'05*, Island of Ischia, Italy, p. 8, 2005.
 - [141] D. Baloukov, W. D. Grover, and A. Kodian, "Toward jointly optimized design of failure-independent path-protecting p-cycle networks," *J. Opti. Netw.*, vol. 7, no. 1, pp. 62-79, 2008.
 - [142] C. Ge, N. Bai, X. Sun, and M. Zhang, "Iterative joint design approach for failure-independent path-protecting p-cycle networks," *J. Opti. Netw.*, vol. 6, no. 12, pp. 1329-1339, 2007.
 - [143] D. Stamatelakis and W. D. Grover, "IP layer restoration and network planning based on virtual protection cycles," *IEEE J. Sel. Areas. Commun.*, vol. 18, no. 10, pp. 1938-1949, 2000.
 - [144] J. Doucette, P. A. Giese, and W. D. Grover, "Combined node and span protection strategies with node-encircling p-cycles," in Proc. *DRCN'05*, Island of Ischia, Italy, p. 9, 2005.
 - [145] J. Doucette, W. D. Grover, and P. A. Giese, "Physical-layer p-cycles adapted for router-level node protection: a multi-layer design and operation strategy," *IEEE J. Sel. Areas. Commun.*, vol. 25, no. 5, pp. 963-973, 2007.
 - [146] M. Clouqueur and W. D. Grover, "Availability analysis of span-restorable mesh networks," *IEEE J. Sel. Areas. Commun.*, vol. 20, no. 4, pp. 810-821, 2002.
 - [147] L. Zhou, M. Held, and U. Sennhauser, "Connection availability analysis of span-restorable mesh networks," *Photonic Netw. Commu.*, vol. 14, no. 2, pp. 135-148, 2007.
-

-
- [148] M. L. Shooman, *Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design*. New York: John Wiley & Sons Inc., 2002.
 - [149] D. A. Schupke, "The tradeoff between the number of deployed p-cycles and the survivability to dual fiber duct failures," in Proc. *ICC'03*, Anchorage, Alaska, USA, vol. 2, pp. 1428-1432, 2003.
 - [150] D. S. Mukherjee, C. Assi, and A. Agarwal, "An alternative approach for enhanced availability analysis and design methods in p-cycle-based networks," *IEEE J. Sel. Areas. Commun.*, vol. 24, no. 12, pp. 23-34, 2006.
 - [151] P. Cholda and A. Jaiszczyk, "Reliability assessment of optical p-cycles," *IEEE/ACM Trans. Netw.*, vol. 15, no. 6, pp. 1-14, 2007.
 - [152] P. Cholda and A. Jaiszczyk, "Reliability assessment of rings and p-cycles in DWDM networks," in Proc. *NGIN'05*, Rome, Italy, pp. 364-371, 2005.
 - [153] P. Cholda and A. Jaiszczyk, "Reliability assessment of p-cycles," in Proc. *GLOBECOM'05*, St. Louis, MO, USA, vol. 1, p. 5, 2005.
 - [154] W. D. Grover, "High availability path design in ring-based optical networks," *IEEE/ACM Trans. Netw.*, vol. 7, no. 4, pp. 558-574, 1999.
 - [155] A. Ranjbar and C. Assi, "Availability-aware design in FIPP p-cycles protected mesh networks," in Proc. *ONDM'08*, Catalonia, Spain, pp. 1-6, 2008.
 - [156] R. Beverly and K. C. Claffy, "Wide-area IP multicast traffic characterization," *IEEE Network*, vol. 17, no. 1, pp. 8-15, 2003.
 - [157] C. Diot, B. N. Levine, B. Lyles, H. Kassem, and D. Balensiefen, "Deployment issues for the IP multicast service and architecture," *IEEE Network*, vol. 14, no. 1, pp. 78-88, 2000.
 - [158] C. Metz, "Reliable multicast: when many must absolutely positively receive it," *IEEE Internet Comput.*, vol. 2, no. 4, pp. 9-13, 1998.
 - [159] D. N. Yang, W. Liao, and C. J. Kao, "Source filtering in IP multicast routing," *IEEE Trans. Broadcast.*, vol. 52, no. 4, pp. 529-542, 2006.
 - [160] A. Ganjam and H. Zhang, "Internet multicast video delivery," *Proc. IEEE*, vol. 93, no. 1, pp. 159-170, 2005.
 - [161] K. Hastings and N. Nechita, "Challenges and opportunities of delivering IP-based residential television services," *IEEE Commun. Mag.*, vol. 38, no. 11, pp. 86-92, 2000.
 - [162] Y. Peng, W. Hu, W. Sun, X. Wang, and Y. Jin, "Impairment constraint multicasting in translucent WDM networks: architecture, network design and multicasting routing," *Photonic Netw. Commu.*, vol. 13, no. 1, pp. 93-102, 2007.
 - [163] S. Sankaranarayanan and S. Subramaniam, "Comprehensive performance modeling and analysis of multicasting in optical networks," *IEEE J. Sel. Areas. Commun.*, vol. 21, no. 9, pp. 1399-1413, 2003.
 - [164] G. N. Rouskas, "Optical layer multicast: rationale, building blocks, and challenges," *IEEE Network*, vol. 17, no. 1, pp. 60-65, 2003.
 - [165] A. Ding and G. S. Poo, "A survey of optical multicast over WDM networks," *Computer Commun.*, vol. 26, no. 2, pp. 193-200, 2003.
 - [166] T. Wen-Yu and K. Sy-Yen, "All-optical multicasting on wavelength-routed WDM networks with partial replication," in Proc. *ICIN'01*, Los Alamitos, CA, USA, pp. 813-18, 2001.
 - [167] L. H. Sahasrabudhe and B. Mukherjee, "Light trees: optical multicasting for improved performance in wavelength routed networks," *IEEE Commun. Mag.*, vol. 37, no. 2, pp. 67-73, 1999.
 - [168] X. Liu, H. Wang, and Y. Ji, "Serial multicast mode in all-optical networks," *IEEE Photon. Technol. Lett.*, vol. 18, no. 22, pp. 2416-2418, 2006.
-

-
- [169] C. F. Lam, M. Boroditsky, M. D. Feuer, N. J. Frigo, B. Desai, and J. Kang, "Demonstration of programmable optical multicasting in a regional/metro area network," *IEEE Photon. Technol. Lett.*, vol. 13, no. 11, pp. 1236-1238, 2001.
 - [170] W. S. Hu and Q. J. Zeng, "Multicasting optical cross connects employing splitter-and-delivery switch," *IEEE Photon. Technol. Lett.*, vol. 10, no. 7, pp. 970-972, 1998.
 - [171] M. Rajkumar, X. Zhang, and C. Qiao, "Benefits of multicasting in all-optical networks," *Proc. SPIE, All-Optical Networking: Architecture, Control, and Management Issues*, vol. 3531, pp. 209-220, 1998.
 - [172] L. Z. Granville, D. M. da Rosa, A. Panisson, C. Melchior, M. J. B. Almeida, and L. M. R. Tarouco, "Managing computer networks using peer-to-peer technologies," *IEEE Commun. Mag.*, vol. 43, no. 10, pp. 62-68, 2005.
 - [173] S. Sen and W. Jia, "Analyzing peer-to-peer traffic across large networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 2, pp. 219-232, 2004.
 - [174] Y. Yang, J. Wang, and C. Qiao, "Nonblocking WDM multicast switching networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 12, pp. 1274-1287, 2000.
 - [175] W. Zhuoran, N. Chi, and S. Yu, "Characterization of 1 by N broadcast and 2 by N multicast packet switching using active-vertical-coupler-based optical crosspoint switch," *IEEE/OSA J. Lightw. Technol.*, vol. 24, no. 8, pp. 2978-2985, 2006.
 - [176] Z. Wang, N. Chi, and S. Yu, "2-to-4 optical multicast using active vertical coupler optical crosspoint switch matrix," *IEEE Photon. Technol. Lett.*, vol. 18, no. 1, pp. 286-288, 2006.
 - [177] K. O. S. Yoshima, N. Wada, F. Kubota, K. Kitayama, "Multicast-capable optical code label switching and its experimental demonstration," *IEEE/OSA J. Lightw. Technol.*, vol. Vol. 24, no. No. 2, pp. pp. 713-722, 2006.
 - [178] H. S. Chung, S. H. Chang, S. S. Lee, and K. Kim, "Experimental demonstration of optical multicast using WSS based multi-degree ROADMs," in *Proc. OFC'08*, San Diego, California, USA, pp. 1-3, 2008.
 - [179] M. Ali and J. S. Deogun, "Cost-effective implementation of multicasting in wavelength-routed networks," *IEEE/OSA J. Lightw. Technol.*, vol. 18, no. 12, pp. 1628-1638, 2000.
 - [180] S.-C. Lee, R. Varrazza, O. Ansell, and S. Yu, "Highly flexible 4 by 4 optical crosspoint packet switch matrix for optical multicast operations," *IEEE Photon. Technol. Lett.*, vol. 17, no. 4, pp. 911-913, 2005.
 - [181] N. K. Singhal, L. H. Sahasrabudhe, and B. Mukherjee, "Optimal multicasting of multiple light-trees of different bandwidth granularities in a WDM mesh network with sparse splitting capabilities," *IEEE/ACM Trans. Netw.*, vol. 14, no. 5, pp. 1104-1117, 2006.
 - [182] J.P. Wang, X.T. Qi, and B. Chen, "Wavelength assignment for multicast in all-optical WDM networks with splitting constraints," *IEEE/ACM Trans. Netw.*, vol. 14, no. 1, pp. 169-182, 2006.
 - [183] M. Ali, "Optimization of splitting node placement in wavelength-routed optical networks," *IEEE J. Select. Areas Commun.*, vol. 20, no. 8, pp. 1571-1579, 2002.
 - [184] X. Zhang, J. Y. Wei, and C. Qiao, "Constrained multicast routing in WDM networks with sparse light splitting," *IEEE/OSA J. Lightw. Technol.*, vol. 18, no. 12, pp. 1917-1927, 2000.
 - [185] X. H. Jia, D. Z. Du, X. D. Hu, M. K. Lee, Lee, and J. Gu, "Optimization of wavelength assignment for QoS multicast in WDM networks," *IEEE Trans. Commun.*, vol. 49, no. 2, pp. 341-350, 2001.
-

-
- [186] G. Sahin and M. Azizoglu, "Multicast routing and wavelength assignment in wide-area networks," in Proc. *SPIE*, Boston, MA, USA, vol. 3531, pp. 196-208, 1998.
 - [187] A. M. Hamad and A. E. Kamal, "A survey of multicasting protocols for broadcast-and-select single-hop networks," *IEEE Network*, vol. 16, no. 4, pp. 36-48, 2002.
 - [188] S. Ramesh, G. N. Rouskas, and H. G. Perros, "Computing blocking probabilities in multiclass wavelength-routing networks with multicast calls," *IEEE J. Sel. Areas. Commun.*, vol. 20, no. 1, pp. 89-96, 2002.
 - [189] A. E. Kamal and A. K. Al-Yatama, "Blocking probabilities in circuit-switched wavelength division multiplexing networks under multicast service," *Performance Evaluation*, vol. 47, no. 1, pp. 43-71, 2002.
 - [190] S.G. Yan, M. Ali, and J. deogun, "Route optimization of multicast sessions in sparse light-splitting optical networks," in Proc. *GLOBECOM'01*, San Antonio, TX, USA, vol. 4, pp. 2134-2138, 2001.
 - [191] I. S. Hwang and T. C. Lin, "Performance assessment of multicast node placement for multicast routing in WDM networks with sparse light splitting," *Photonic Netw. Commu.*, vol. 16, no. 2, pp. 107-116, 2008.
 - [192] X. Wang, S. Wang, and L. M. Li, "A novel efficient multicast routing algorithm in sparse splitting optical networks," *Photonic Netw. Commu.*, vol. 14, no. 3, pp. 287-295, 2007.
 - [193] W. Y. Tseng and S.-Y. Kuo, "All-optical multicasting on wavelength-routed WDM networks with partial replication," in Proc. *ICIN'01*, Los Alamitos, CA, USA, pp. 813-18, 2001.
 - [194] B. Chen and J. Wang, "Efficient routing and wavelength assignment for multicast in WDM networks," *IEEE J. Sel. Areas. Commun.*, vol. 20, no. 1, pp. 97-109, 2002.
 - [195] G. S. Poo and Y. Zhou, "A new multicast wavelength assignment algorithm in wavelength-routed WDM networks," *IEEE J. Sel. Areas. Commun.*, vol. 24, no. 4, pp. 2-12, 2006.
 - [196] Y. Zhou and G. S. Poo, "Multi-wavelength multicast wavelength assignment algorithm for limited wavelength conversion in wavelength-division multiplexing networks," *IET Commun.*, vol. 1, no. 4, pp. 776-783, 2007.
 - [197] N. Sreenath, C. S. R. Murthy, and G. Mohan, "Virtual source based multicast routing in WDM optical networks," *Photonic Netw. Commu.*, vol. 3, no. 3, pp. 213-226, 2001.
 - [198] R. Libeskind-Hadas and R. Melhem, "Multicast routing and wavelength assignment in multihop optical networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 5, pp. 621-629, 2002.
 - [199] Y. Wang and Y. Yang, "Multicasting in a class of multicast-capable WDM networks," *IEEE/OSA J. Lightw. Technol.*, vol. 20, no. 3, pp. 350-359, 2002.
 - [200] M. Ali, "Optimization of splitting node placement in wavelength-routed optical networks," *IEEE J. Sel. Areas. Commun.*, vol. 20, no. 8, pp. 1571-1579, 2002.
 - [201] R. K. Pankaj and R. G. Gallager, "Wavelength requirements of all-optical networks," *IEEE/ACM Trans. Netw.*, vol. 3, no. 3, pp. 269-280, 1995.
 - [202] N. K. Singhal, C. Ou, and B. Mukherjee, "Cross-sharing vs. self-sharing trees for protecting multicast sessions in mesh networks," *Comput. Netw.*, vol. 50, no. 2, pp. 200-206, 2006.
 - [203] N. K. Singhal, C. Ou, and B. Mukherjee, "Shared protection for multicast sessions in mesh networks," in Proc. *OFC'05*, Anaheim, CA, USA, vol. 2, p. 3, 2005.
 - [204] N. K. Singhal, L. H. Sahasrabudhe, and B. Mukherjee, "Provisioning of survivable multicast sessions against single link failures in optical WDM mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 11, pp. 2587-2594, 2003.
-

-
- [205] N. K. Singhal and B. Mukherjee, "Protecting multicast sessions in WDM optical mesh networks," *IEEE/OSA J. Lightw. Technol.*, vol. 21, no. 4, pp. 884-892, 2003.
 - [206] A. Fei, J. Cui, M. Gerla, and D. Cavendish, "A "dual-tree" scheme for fault-tolerant multicast," in Proc. *ICC'01*, New York, USA, vol. 3, pp. 690-694, vol.3, 2001.
 - [207] M. Medard, S.G. Finn, R.A. Barry, and R. G. Gallager, "Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs," *IEEE/ACM Trans. Netw.*, vol. 7, no. 5, pp. 641-652, 1999.
 - [208] Y. Li, Y. Jin, L. Li, and L. M. Li, "On finding the multicast protection tree considering SRLG in WDM optical networks," *ETRI Journal*, no. 28, pp. 517-520 2006.
 - [209] M. Yang, J. P. Wang, X. T. Qi, and Y. T. Jiang, "On finding the best partial multicast protection tree under dual-homing architecture," in Proc. *HPSR'05*, HongKong, PRC, pp. 128-132, 2005.
 - [210] W. Zhang, G. Xue, J. Tang, and K. Thulasiraman, "Faster algorithms for construction of recovery trees enhancing QoP and QoS," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 642-655, 2008.
 - [211] G. W. Xie, W. Q. Sun, Y. H. Jin, W. Guo, and W. S. Hu, "Optimal multicast protection with differentiated leaf availability guarantee in optical mesh networks," in Proc. *SPIE*, vol. 6354, pp. 63541I1-63541I9, 2006.
 - [212] A. Khalil, A. Hadjiantonis, G. Ellinas, and M. Ali, "Dynamic provisioning of survivable heterogeneous multicast and unicast traffic in WDM networks," in Proc. *ICC'06*, Istanbul, Turkey, vol. 6, pp. 2465-2470, 2006.
 - [213] T. Rahman and G. Ellinas, "Protection of multicast sessions in WDM mesh optical networks," in Proc. *OFC'05*, Anaheim, CA, USA, vol. 2, p. 3, 2005.
 - [214] P. Leelarusmee, C. Boworntummarat, and L. Wuttisittikulkij, "Design and analysis of five protection schemes for preplanned recovery in multicast WDM networks," in Proc. *SAWWC'04*, Princeton, NJ, USA, pp. 167-170, 2004.
 - [215] A. Khalil, A. Hadjiantonis, G. Ellinas, and M. A. Ali, "Pre-planned multicast protection approaches in WDM mesh networks," in Proc. *ECOC'05*, Glasgow, UK, pp. 25-26 vol.1, 2005.
 - [216] I. S. Hwang, R. Y. Cheng, and W. D. Tseng, "A novel dynamic multiple ring-based local restoration for point-to-multipoint multicast traffic in WDM mesh networks," *Photonic Netw. Commu.*, vol. 14, no. 1, pp. 23-33, 2007.
 - [217] H. B. Luo, H. F. Yu, L. M. Li, and S. Wang, "On protecting dynamic multicast sessions in survivable mesh WDM networks," in Proc. *OFC'06*, Anaheim, California. USA, p. 3, 2006.
 - [218] N. K. Singhal and B. Mukhejee, "Dynamic provisioning of survivable multicast sessions in optical WDM mesh networks," in Proc. *OFC'03*, vol. 1, pp. 207-209, 2003.
 - [219] X. Wang, S. Wang, L. M. Li, and Y. J. Song, "Dynamic multicast protection algorithms for reducing residual links in WDM mesh networks," in Proc. *ISCC'07*, pp. 275-281, 2007.
 - [220] H. Luo, L. M. Li, H. Yu, and S. Wang, "Achieving shared protection for dynamic multicast sessions in survivable mesh WDM networks," *IEEE J. Sel. Areas. Commun.*, vol. 25, no. 9, pp. 83-95, 2007.
 - [221] L. Liao, L. M. Li, and S. Wang, "Multicast protection scheme in survivable WDM optical networks," *J. Netw. Comput. Appl.*, vol. 31, no. 3, pp. 303-316, 2008.
-

-
- [222] H. B. Luo, L. M. Li, H. F. Yu, and S. Wang, "Cost reduction for provisioning survivable multicast sessions in WDM mesh networks," *IEEE Commun. Lett.*, vol. 10, no. 10, pp. 725-727, 2006.
 - [223] X. Wang, S. Wang, L. M. Li, and Y. Song, "Achieving resource reduction for protecting multicast sessions in WDM mesh networks" *Photonic Netw. Commu.*, vol. 15, no. 2, pp. 131-140, 2008.
 - [224] C. S. Wu, S. W. Lee, and Y. T. Hou, "Backup VP preplanning strategies for survivable multicast ATM networks," in Proc. *ICC'97*, Montreal, Quebec, Canada, vol. 1, pp. 267-271, 1997.
 - [225] C. Lu, H. Luo, S. Wang, and L. M. Li, "A novel shared segment protection algorithm for multicast sessions in mesh WDM networks," *ETRI Journal*, vol. 28, pp. 329-336, 2006.
 - [226] C. Lu, X. Y. Nie, S. Wang, and L. M. Li, "Adaptive segment protection algorithm of multicast on WDM networks against single link failure," in Proc. *SPIE* vol. 6022, pp. 60222C-1 to C-11, 2005.
 - [227] C. Lu, H. Luo, S. Wang, and L. M. Li, "A novel shared segment protection algorithm for multicast sessions in mesh WDM networks," *ETRI Journal*, vol. 28, no. 3, pp. 329-336, 2006.
 - [228] J. Li, H. Zhang, B. Zhou, and Y. Guo, "A novel fast multicast algorithm with enhanced survivability in WDM optical networks," *Photonic Netw. Commu.*, vol. 8, no. 2, pp. 329-336, 2004.
 - [229] F. Zhang and W. D. Zhong, "p-cycle based tree protection of optical multicast traffic for combined link and node failure recovery in WDM mesh networks," *IEEE Commun. Lett.*, vol. 13, no. 1, pp. 40 - 42, 2009.
 - [230] F. Zhang and W. D. Zhong, "A heuristic algorithm of p-cycle based tree protection of optical multicast traffic in WDM mesh networks," in Proc. *OECC 2008*, Sydney, Australia, 2008.
 - [231] F. Zhang and W. D. Zhong, "Performance evaluation of p-cycle based protection methods for provisioning of dynamic multicast sessions in mesh WDM networks," *Photonic Netw. Commu.*, vol. 16, no. 2, pp. 127-138, 2008.
 - [232] F. Zhang, W. D. Zhong, and Y. H. Jin, "Optimizations of p-cycle-based protection of optical multicast sessions," *IEEE/OSA J. Lightw. Technol.*, vol. 26, no. 19, pp. 3298 - 3306, 2008.
 - [233] W. D. Zhong, F. Zhang, and Y. H. Jin, "Optimized designs of p-cycles for survivable multicast sessions in optical WDM networks," in Proc. *ChinaCom '07, Paper OCN03.1*, Shanghai, China, 2007.
 - [234] F. Zhang and W. D. Zhong, "Applying p-cycles in dynamic provisioning of survivable multicast sessions in optical WDM networks," in Proc. *OFC 2007*, Anaheim, California, USA, Paper JWA74, 2007.
 - [235] C. Boworntummarat, L. Wuttisittikulkij, and S. Segkhoonthod, "Light-tree based protection strategies for multicast traffic in transport WDM mesh networks with multifiber systems," in Proc. *ICC'04*, Paris, France, vol. 3, pp. 1791-1795, 2004.
 - [236] M. Medard, S. Finn, and R. Barry, "Automatic protection switching for multicasting in optical mesh networks," in Proc. *OFC'97*, Dallas, TX, USA, pp. 314-315, 1997.
 - [237] J. B. Slevinsky, W. D. Grover, and M. H. MacGregor, "An algorithm for survivable network design employing multiple self-healing rings," in Proc. *GLOBECOM '93*, Houston, TX, USA, pp. 1568-1573 vol.3, 1993.
-

-
- [238] Guido Maier, Achille Pattavina, S. D. Patre, and M. Martinelli, "Optical network survivability: protection techniques in the WDM layer " *Photonic Netw. Commu.*, vol. 4, no. 3, pp. 251-269, 2002.
 - [239] J. R. Evans and E. Minieka, *Optimization Algorithms for Networks and Graphs*: Marcel Dekker, Inc., 1992.
 - [240] F. Zhang and W. D. Zhong, "A novel path-protecting p-cycle heuristic algorithm," in Proc. *ICTON'06*, Nottingham, UK, vol. 3, pp. 203-206, We.B3.5, 2006.
 - [241] Z. R. Zhang, "Design and analysis of p-cycle-based survivable optical networks," PhD Thesis, Nanyang Technological University (Singapore), 2005.
 - [242] B. Chen, W. D. Zhong, and S. K. Bose, "Applying saturated cut method for dynamic traffic grooming in IP/MPLS over WDM networks," *IEEE Commun. Lett.*, vol. 10, no. 2, pp. 117-119, 2006.
 - [243] B. Chen, S. K. Bose, and W. D. Zhong, "Priority enabled dynamic traffic grooming," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 366-368, 2005.
 - [244] B. Chen, W. D. Zhong, and S. K. Bose, "A path inflation control strategy for dynamic traffic grooming in IP/MPLS over WDM network," *IEEE Commun. Lett.*, vol. 8, no. 11, pp. 680-682, 2004.
 - [245] Z. Keyao and B. Mukherjee, "A review of traffic grooming in WDM optical networks: architectures and challenges," *Opt. Netw. Mag.*, vol. 4, no. 2, pp. 55-64, 2003.
 - [246] D. A. Schupke, C. G. Gruber, and A. Autenrieth, "Optimal configuration of p-cycles in WDM networks," in Proc. *ICC'02*, New York, USA, vol. 5, pp. 2761-2765 vol.5, 2002.
 - [247] T. Y. Chow, F. Chudak, and A. M. Ffrench, "Fast optical Layer mesh protection using pre-cross-connected trails," *IEEE/ACM Trans. Netw.*, vol. 12, no. 3, pp. 539-548, 2004.
 - [248] ILOG CPLEX 8.0 Reference Manual, http://web.njit.edu/all_topics/Prog_Lang_Docs/cplex80/doc/refman/onlinedoc/.
 - [249] S. Bregni, U. Janigro, and A. Pattavina, "Optimal allocation of limited optical-layer resources in WDM networks under static traffic demand," *Photonic Netw. Commu.*, vol. 5, no. 1, pp. 33-40, 2003.
 - [250] R. Ramamurthy, Z. Bogdanowicz, S. Samieian, D. Saha, B. Rajagopalan, S. Sengupta, S. Chaudhuri, and K. Bala, "Capacity performance of dynamic provisioning in optical networks," *IEEE/OSA J. Lightw. Technol.*, vol. 19, no. 1, pp. 40-48, 2001.
 - [251] Z. Qin and G. Mohan, "Protection approaches for dynamic traffic in IP/MPLS-over-WDM networks," *IEEE Commun. Mag.*, vol. 41, no. 5, pp. S24-S29, 2003.
 - [252] S. Sengupta and R. Ramamurthy, "From network design to dynamic provisioning and restoration in optical cross-connect mesh networks: an architectural and algorithmic overview," *IEEE Network*, vol. 15, no. 4, pp. 46-54, 2001.
 - [253] H. N. Son, X. Jiang, V. T. Le, and H. Susumu, "Ant-based survivable routing in dynamic WDM networks with shared backup paths," *J. Supercomp.*, vol. 36, no. 3, pp. 297-307, 2006.
 - [254] Y. Wang, Q. Zeng, and H. Zhao, "Dynamic survivability in WDM mesh networks under dynamic traffic," *Photonic Netw. Commu.*, vol. 6, no. 1, pp. 5-24, 2003.
 - [255] D. P. Onguetou and W. D. Grover, "A new insight and approach to node failure protection with ordinary p-cycles," in Proc. *ICC '08*, Beijing, China, pp. 5145-5149, 2008.
 - [256] W. D. Zhong, Y. Onozato, and J. Kaniyil, "A copy network with shared buffers for large-scale multicast ATM switching," *IEEE/ACM Trans. Netw.*, vol. 1, no. 2, pp. 157-165, 1993.
-

-
- [257] N. Ghani, S. Dixit, and T.-S. Wang, "On IP-over-WDM integration," *IEEE Commun. Mag.*, vol. 38, no. 3, pp. 72-84, 2000.
 - [258] X. Niu, W.D. Zhong, G. Shen, and T. H. Cheng, "Connection establishment of label switched paths in IP/MPLS over optical networks " *Photonic Netw. Commu.*, vol. 6, no. 1, pp. 33-41, 2004.
 - [259] W.D. Zhong, X. Niu, B. Chen, and S. K. Bose, "Performance comparison of overlay and peer models in IP/MPLS over optical networks " *Photonic Netw. Commu.*, vol. 9, no. 1, pp. 121-131, 2005.
 - [260] Y. Ye, S. Dixit, and M. Ali, "On joint protection/restoration in IP-centric DWDM based optical transport networks," *IEEE Commun. Mag.*, vol. 38, no. 6, pp. 174-183, 2000.
 - [261] N. S. C. Correia and M. C. R. Medeiros, "Protection schemes for IP-over-WDM networks: throughput and recovery time comparison " *Photonic Netw. Commu.*, vol. 11, no. 2, pp. 127-149, 2006.
 - [262] J. S. Kaufman and K. M. Rege, "Blocking in a shared resource environment with batched Poisson arrival processes," *Performance Evaluation*, vol. 24, no. 4, pp. 249-263, 1996.
 - [263] J. S. Kaufman, "Blocking in a completely shared resource environment with state dependent resource and residency requirements," in Proc. *INFOCOM '92*, Florence, Italy pp. 2224-2232 vol.3, 1992.
 - [264] J. Kaufman, "Blocking in a shared resource environment," *IEEE Trans. Commun.*, vol. 29, no. 10, pp. 1474-1481, 1981.
 - [265] K. Grobe and J. P. Elbers, "PON in adolescence: from TDMA to WDM-PON," *IEEE Commun. Mag.*, vol. 46, no. 1, pp. 26-34, 2008.
 - [266] C. H. Lee, W. V. Sorin, and B. Y. Kim, "Fiber to the home using a PON infrastructure," *IEEE/OSA J. Lightw. Technol.*, vol. 24, no. 12, pp. 4568-4583, 2006.
 - [267] X. F. Sun, C. K. Chan, and L. K. Chen, "A survivable WDM-PON architecture with centralized alternate-path protection switching for traffic restoration," *IEEE Photon. Technol. Lett.*, vol. 18, no. 4, pp. 631-633, 2006.
 - [268] Z. Xu, Y. J. Wen, W. D. Zhong, T. H. Cheng, X. Cheng, Y. Wang, and Y. K. Yeo, "10 Gb/s WDM-PON based on FP-LDs injection locked by downlink optical carrier," *Opt. Commun.*, vol. 281, no. 20, pp. 5213-17, 2008.
 - [269] X. Cheng, Y. J. Wen, Z. Xu, Y. Wang, and Y.-K. Yeo, "Survivable WDM-PON with self-protection and in-service fault localization capabilities," *Opt. Commun.*, vol. 281, no. 18, pp. 4606-11, 2008.
 - [270] Z. Xu, Y. J. Wen, W. D. Zhong, C.-J. Chae, X.-F. Cheng, Y. Wang, C. Lu, and J. Shankar, "High-speed WDM-PON using CW injection-locked Fabry-Perot laser diodes," *Opt. Express*, vol. 15, no. 6, pp. 2953-2962, 2007.
 - [271] Z. Xu, Y. J. Wen, W. D. Zhong, M. Attygalle, X. F. Cheng, Y. Wang, and C. Lu, "Carrier-reuse WDM-PON using a shared delay interferometer for separating carriers and subcarriers," *IEEE Photon. Technol. Lett.*, vol. 19, no. 11, pp. 837-9, 2007.
 - [272] Y. Zhang, N. Deng, C. K. Chan, and L. K. Chen, "A multicast WDM-PON architecture using DPSK/NRZ orthogonal modulation," *IEEE Photon. Technol. Lett.*, vol. 20, no. 17, pp. 1479-81, 2008.
 - [273] S. Yikai, T. Yue, E. Wong, N. Nadarajah, and C. C. K. Chan, "All-optical virtual private network in passive optical networks," *Laser & Photonics Reviews*, vol. 2, no. 6, pp. 460-79, 2008.
-

- [274] N. Deng, C.-K. Chan, L.-K. Chen, and C. Lin, "A WDM passive optical network with centralized light sources and multicast overlay," *IEEE Photon. Technol. Lett.*, vol. 20, no. 2, pp. 114-16, 2008.
- [275] N. R. Dono, P. E. Green, Jr., K. Liu, R. Ramaswami, and F. F. K. Tong, "A wavelength division multiple access network for computer communication," *IEEE J. Select. Areas Commun.*, vol. 8, no. 6, pp. 983-94, 1990.
- [276] C. C. K. Chan, L.-K. Chen, and C. Lin, "Novel network architectures for survivable WDM passive optical networks," in Proc. *ECOC'08*, Brussels, Belgium, pp. 1 - 4, 2008.

Author's Publications

Journal publications

- [1] **F. Zhang** and W. D. Zhong, "Performance evaluation of p -cycle based protection methods for provisioning of dynamic multicast sessions in mesh WDM networks," *Photonic Netw. Commu.*, vol. 16, no. 2, pp. 127-138, 2008. (related to Chapter 3)
- [2] **F. Zhang**, W. D. Zhong, and Y. H. Jin, "Optimizations of p -cycle-based protection of optical multicast sessions," *IEEE/OSA J. Lightw. Technol.*, vol. 26, no. 19, pp. 3298 – 3306, 2008. (related to Chapter 3 and Chapter 4)
- [3] **F. Zhang** and W. D. Zhong, " p -cycle based tree protection of optical multicast traffic for combined node and link failure recovery in WDM mesh networks," *IEEE Commu. Lett.*, vol. 13, no. 1, pp. 40-42, 2009. (related to Chapter 4)
- [4] **F. Zhang**, and W. D. Zhong, "Performance evaluation of optical multicast protection approaches for combined node and link failure recovery," *IEEE/OSA J. Lightw. Technol.*, vol. 27, no. 18, pp. 4017-4028, 2009. (related to Chapter 5)
- [5] **F. Zhang**, W. D. Zhong, and T. K. Wong, "Extending p -cycles to source failure recovery on top of combined node and link failure recovery for optical multicast sessions," to be submitted to *IEEE/OSA J. Lightw. Technol.*, 2009. (related to Chapter 5)
- [6] W. D. Zhong, **F. Zhang**, Z. Xu, Y. Gu, T. H. Cheng, M. Craig, and A. Ivan, "Multicast/broadcast-capable carrier-reuse architecture for WDM-PONs," submitted to *IEEE J. Select. Areas Commun.*, 2009.

Conference publications

- [1] **F. Zhang** and W. D. Zhong, "Applying p -cycles in dynamic provisioning of survivable multicast sessions in optical WDM networks," in Proc. *OFC '07*, Anaheim, California, USA, Paper JWA74, 2007. (related to Chapter 3)
- [2] W. D. Zhong, **F. Zhang**, and Y. H. Jin, "Optimized designs of p -cycles for survivable multicast sessions in optical WDM networks," in Proc. *ChinaCom '07*, Invited paper, Paper OCN03.1, Shanghai, China, 2007. (related to Chapter 3)
- [3] **F. Zhang** and W. D. Zhong, "A heuristic algorithm of p -cycle based tree protection of optical multicast traffic in WDM mesh networks," in Proc. *OECC '08*, Sydney, Australia, 2008. (related to Chapter 4)
- [4] **F. Zhang** and W. D. Zhong, "A novel path-protecting p -cycle heuristic algorithm," in Proc. *ICTON 2006*, Nottingham, UK, vol. 3, pp. 203-206, We.B3.5, 2006. (related to Chapter 2)
- [5] **F. Zhang** and W. D. Zhong, "Optimized design of node-and-link protecting p -cycle with restorability constraints for optical multicast traffic protection," in Proc. *OECC'09, IEEE OECC'09 Best Student Paper*, Paper ThN5, HK, P.R.C., 2009. (related to Chapter 5)
- [6] Y. Gu, W. D. Zhong, **F. Zhang**, Z. Xu, and C. Michie, "A carrier-reuse WDM-PON architecture with multicast/broadcast capability," accepted for publication in *ICICS'09*, Macau, P. R. C., 2009.

- [7] W. D. Zhong, **F. Zhang**, and Z. Xu, "WDM-PON: a promising candidate for the future access network of intelligent buildings," accepted for publication in *IBASH'09*, Invited paper, Taiwan, P.R.C., 2009.