Next Generation Reliable Transport Networks

Zhang, Jiang; Dittmann, Lars

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

Next Generation Reliable Transport Networks

Jiang Zhang

June 2011

Networks Technology & Service Platforms
Department of Photonics Engineering
Technical University of Denmark
2800 Kgs. Lyngby
DENMARK

To my dear parents.

Abstract

This thesis focuses the efforts on ensuring the reliability of transport networks and takes advantages and experiences from the transport networks into the networks for particular purposes.

Firstly, the challenges of providing reliable multicast services on Multipath Label Switching-Transport Profile (MPLS-TP) ring networks are addressed. Through the proposed protection structure and protection switching schemes, the recovery mechanism is enhanced in terms of recovery label consumption, operation simplicity and fine traffic engineering granularity. Furthermore, the extensions for existing and proposed protection schemes on the interconnected-ring structure are presented, which not only fulfill the requirements suggested by ITU and IETF organizations, but also increase the scalability and applicability of the transport ring networks.

Secondly, avionic transport networks are investigated, aiming at enabling the full exploitation of key optical networking technologies in future aircrafts. A three-layered optical transport networks over a ring topology is suggested, as it can provide full reconfiguration flexibility and support a wide range of avionic applications. According to different levels of criticality and security, there are certain physical or logical segregation requirements between the avionic systems. Such segregations can be implemented on the proposed avionic networks with different hierarchies. In order to fulfill the segregation requirements, a tailored heuristic approach for solving the wavelength and fiber assignment problem is proposed and implemented for avionic optical transport networks. Simulation results give out resource consumptions and prove the efficiency of the proposed mechanisms.

Finally, a Home Environment Service Knowledge Management sys-

tem is proposed. Through ontology technologies, a knowledge base is constructed to represent the whole information of a home environment. By applying the reasoner tool, the proposed system manages to keep the consistency in a home environment and helps all software configure and update procedures across multiple vendors.

Resumé

Denne afhandling fokuserer på at sikre pålideligheden af transportnetværk og bringer fordele og erfaringer fra transportnetværk ind i netværk til særlige formål, hvilket muliggør ny udvikling af forskellige typer af netværk.

I første del af afhandlingen er udfordringerne ved at levere pålidelige multicasttjenester på Multipath Label Switching-Transport Profile (MPLS-TP) ringnetværk beskrevet. Gennem den foreslåede beskyttelsesstruktur og foreslåede omstillingssystem er gendannelsesmekanismen forbedret hvad angår labelforbrug til gendannelse, operationsenkelhed og traffikstyring. Ydermere opfylder den foreslåede beskyttelsesstruktur i den sammenkoblede ringstruktur ikke kun kravene foreslået af ITU- og IETF-organisationerne, men øger også skalerbarheden og anvendeligheden af de undersøgte transportringnetværk.

I anden del er det flyelektroniske transportnetværk undersøgt, med henblik på at muliggøre den fulde udnyttelse af nøgleteknologier inden for optiske netværk i fremtidige flyvemaskiner. Et tre-lags optisk transportnetværk baseret på en ringtopologi er foreslået, og det kan levere fuld rekonfigurationsfleksibilitet og understøtte en lang række flyelektroniske enheder. På grund af de kritiske sikkerhedskrav i flyelektronik kan adskillelse ske i flere hierarkier. Baseret på sådanne isolationskrav, er en skræddersyet heuristisk fremgangsmåde til løsning af bølgelængde- og fibertildelingsproblemer foreslået og implementeret til anvendelse i flyelektroniske optiske transportnetværk. Simulationsresultater giver eksempler på ressourceforbrug og viser effektiviteten af de foreslåede mekanismer.

I tredje del er et Home Environment Service Knowledge Managementsytem foreslået til håndtering af information i et hjemmemiljø og

til at hjælpe med softwarekonfiguration og -opdateringsprocedurer på tværs af udbydere.

Acknowledgements

The way of achieving the Ph.D is full of challenges and hard work. The credit for this thesis goes to the people who give me endless encouragement and support.

I would like to thank my main supervisor, Professor. Lars Dittman. Without him I would not have had the opportunity to experience the journey of research and innovation. His profession, confidence and optimism always guide me through the hard period.

I am also deeply grateful to my co-supervisor Professor. Michael S. Berger for his continued inspiration, encouragement and especially the extreme patience to understand what I meant to express. Lots of the sparks of my innovations are come from such discussions. My work can always get improved from his practical suggestions.

My thanks also go to all my colleges and friends at DTU Fotonik: Dr Villy B. Iversen, Dr. Lars Staalhagen, Dr. Sarah Ruepp, Dr. Anna V. Manolova, Dr. Jóse Soler, Dr. Henrik Wessing, Dr. Ying Yan, Dr. Anders Clausen, Dr. Christophe Peucheret, Dr. Hao Yu, Rong Fu, Lukasz Brewka, Ana Rosselló-Busquet, Anders Rasmussen, Thang Tien Pham, JiaYuan Wang, Anna Zakrzewska and Yi An for their help and assistance on reviewing this thesis, and more important for the joy they have brought to my life and the warm they have made in my heart.

Finally, I would like to thank my parents, GuoJian Zhang and DongNing Jiang. There is no word I can use to express my love. I would also like to thank HongPo. He is always there for me with his love and support.

Ph.D. Publications

The following publications have been made throughout this Ph.D project.

[1] **J. Zhang**, R. Fu, H. Yu, S. Ruepp, M. S. Berger, and L. Dittmann, "Two novel tunnel-based ring protection switching for MPLS-TP multicast services," in *IEEE 18th International Conference on Telecommunications (ICT)*, 2011

[2] **J. Zhang**, A. Yi, M. S. Berger, C. Peucheret, and A. Clausen, "Developing a generic optical avionic network," in *IEEE 18th International Conference on Telecommunications (ICT)*, 2011

[3] **J. Zhang**, A. Rosselló-Busquet, J. Soler, M. S. Berger, and L. Dittmann, "Home environment service knowledge management system," in *IEEE 11th International Conference on Telecommunications (ConTEL 2011)*, 2011

[4] **J. Zhang**, M. S. Berger, and S. Ruepp, "Flow-based end-to-end OAM functions for the multicast service on the MPLS-TP ring network," in *IEEE International Conference on Communications (ICC)*, 2010

[5] A. Rasmussen, **J. Zhang**, H. Yu, R. Fu, S. Ruepp, H. Wessing, and M. S. Berger, "High capacity carrier Ethernet transport networks," in *4th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CISST'10)*, 2010

[6] S. Ruepp, H. Wessing, **J. Zhang**, A. Manolova, A. Rasmussen, L. Dittmann, and M. S. Berger, "Providing resilience for carrier Ethernet multicast traffic," in *4th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CISST'10)*, 2010

[7] M. Barkauskaite, **J. Zhang**, H. Wessing, M. S. Berger, and S. Ruepp, "Modeling of reliable multicasting services," in *OPNETWORK 2010*, 2010

[8] **J. Zhang**, M. S. Berger, and S. Ruepp, "Resilient MPLS-TP multicast service based on an interconnected-ring structure," in *OPNETWORK 2010*, 2010

[9] S. Ruepp, H. Wessing, **J. Zhang**, A. V. Manolova, A. Rasmussen, L. Dittmann, and M. S. Berger, "Evaluating multicast resilience in carrier Ethernet," *WSEAS Transactions on Circuits and Systems*, vol. 9, pp. 101–110, 2010

[10] A. Rasmussen, **J. Zhang**, H. Yu, R. Fu, S. Ruepp, H. Wessing, and M. S. Berger, "Towards 100 gigabit carrier Ethernet transport networks," *WSEAS Transactions on Circuits and Systems*, vol. 9, pp. 153–164, 2010

[11] R. Fu, **J. Zhang**, and M. S. Berger, "Enhanced BRPC routing procedure for PCE based inter-domain routing," in *International conference on Communictions (ICCOM'10)*, 2010

[12] **J. Zhang**, S. Ruepp, M. S. Berger, and H. Wessing, "Protection for MPLS-TP multicast services," in *IEEE Design of Reliable Communication Networks (DRCN 2009)*, 2009

[13] N. Ploskas, M. S. Berger, **J. Zhang**, and L. Dittmann, "Ontology for software configuration management : A knowledge management framework for software configuration management," in *3rd International Conference on Software and Data Technologies (ICSOFT*

2008), 2008

[14] N. Ploskas, M. S. Berger, **J. Zhang**, and G.-J. Wintterle, "A knowledge management framework for software configuration management," in *32nd Annual IEEE International Computer Software and Applications (COMPSAC 08)*, 2008

The publications which are under reviewed:

[15] **J. Zhang**, Y. An, M. S. Berger, V. B. Iversen, and L. Dittmann, "Solving fiber partition constraints in MC-RWA of WDM ring networks," *IEEE Communications Letters*

[16] **J. Zhang**, Y. An, M. S. Berger, and A. T. Clausen, "Wavelength and fiber assignment problems on avionic networks," in *Avionics, Fiber-Optics and Photonics Technology Conference 2011*, 2011

[17] **J. Zhang**, J. Wang, A. Zakrzewska, A. Rasmussen, A. Manolova, H. Yu, Y. Yan, S. Ruepp, and M. S. Berger, "Protection schemes on interconnected-ring topology for MPLS-TP multicast services," *IET*

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Introduction

Network infrastructures have become increasingly critical for our society, and networked services have kept on blooming and become more and more demanding. Decades ago, it was hard to imagine that person's lives and businesses would greatly rely on Internet applications. The applications, such as web services, Voice over IP, NetBank, online stock trading, play important roles on our daily life. However, due to such great dependence, failures in the networks can result in serious loss to users. Considering such importance, network reliability is one of the major concerns of network carriers.

However, providing high-degree reliability to networks is challenging, especially for the next generation networks. Nowadays the network applications, such as IPTV and online trading, are more and more sensitive to the quality of the networks. Even a small degradation can cause bad consequences to the end users. In addition as the networks keep expanding both in horizontal and vertical ways, the network systems become more complex than before. A great deal of network equipments of different types and from various vendors are running different protocols and have diverse levels of reliabilities. All those facts show the importance and difficulty to build up reliable networks. This thesis focuses on addressing the challenges to investigate different approaches to provide reliable transport networks and network transmission services.

During the network evolution, all the research efforts are not only

striding in the large-scale terrestrial transport networks, but also in some networks serving for particular purposes, such as the networks inside devices or the networks for special areas. The experiences gained from the terrestrial transport networks are well exploited and evaluated in the networks with particular characteristics, enabling the state-of-art developments on different types of networks. This thesis contains the research work on two specific networks, aircraft networks and home networks.

1.1.1 Motivation

The research work of this thesis is driven by three projects.

- High quality IP network for IPTV and VoIP (HIPT)

  Since the ending of the network boom several years ago, the declining ability to gain profits from the Internet forces all the network carriers and services providers to look for the next big break. Among the packet-based services, there is a wide agreement that IP Television (IPTV) broadcast services and Voice over IP (VoIP) services will become the new dominant telecom services in the following years. Founded by the Danish Advanced Technology Foundation, the HIPT project aims at investigating this promising issue. The main object of the HIPT project is to investigate and improve transport networks for packet-based multicast services, through developing the functionalities required by the increasing demands, in terms of control plane, traffic management, resiliency and advanced Operation, Administration and Maintenance (OAM) functions. The research work carried out in this thesis involves providing reliable multicast services on Multipath Label Switching - Transport Profile (MPLS-TP) transport networks. Based on the mature MPLS technology, the MPLS-TP is a joint ITU-IETF effort to provide packet-transport network services in a simple, cost-effective and highly reliable way. Ring structure has been chosen as the studied network topology, due to its natural ability to provide simple and efficient multicast solutions and the strong survivability characteristic. Within MPLS-TP ring transport networks, the employed approaches to ensure reliability include the OAM functions and different protection switching strategies. The HIPT project is the starting point of the resilience

studies of this thesis. The research efforts on investigating the reliability related MPLS technologies and the state-of-art ITU and IETF standards have been going through all three-year studies. The latest and important achievements are presented in this thesis.

- Developing Aircraft Photonic Networks (DAPHNE)

  The DAPHNE project is a three-year European Commission research project staring from July 2009. The objective of the project is to enable the use of integrated modular photonic networks on aircraft. Bring benefits of photonics to aircraft data communications by the implementation of a highly integrated optical infrastructure capable of supporting multiple aircraft networks over a lighter and more modular physical layer, thereby improving performance (connectivity, flexibility, bandwidth and channel count) and aircraft cost-of-ownership compared with today's diverse electrical data communications infrastructure [19]. The work presented in this thesis relates to the design of a reliable avionic transport network.

- Software COnfiguration Management framework for Networked serviCes environments and architectures incorporating ambient intelligence features (COMANCHE)

  The European Commission funded COMANCHE project started from July 2005 and finished three years later in July 2008. This project aims to develop a scalable network framework for software configuration management in a home environment, which provides consistent, secure, low-cost software configuration services across the multivendor environment to maintain the whole information of home environment and help all the configuration and update procedures. The research work presented in this thesis combines the work carried out in the COMANCHE project and the subsequent work after the COMANCHE project, which gains experiences from the COMANCHE project and proposes a home environment service knowledge management system.

1.1.2 Structure of Thesis

Chapter 2 introduces the concept of the transport network and its technologies. Some particular issues such as recovery schemes, ring protections and OAM functions are well described as background information for the studies in the later chapters. Chapter 3 and Chapter 4 present the research work on MPLS-TP ring protections. Chapter 3 investigates reliable MPLS-TP multicast services on single-ring networks. Two novel ring protection schemes are proposed based on the experiences of the latest protection schemes documented in ITU and IETF's draft standards. In Chapter 4 the proposed protection schemes and one of IETF standardized protection schemes are extended onto interconnected-ring networks. The design and implementation of the interconnection points of rings are well investigated in term of multicast services, protection operations and OAM functions. Chapter 5 and 6 present the research efforts which have been focused on avionic transport networks. Chapter 5 proposes a generic avionic network with three network layers and based on ring structure. It is characteristic in the sense that it has flexible configuration among different network layers and has a great ability to support a broad range of avionic systems. Three different proposed survivability scenarios ensure the network reliability in different level of security and costs. Chapter 6 presents the studies on the network optimization problem which stems from the isolation requirements of different avionic systems with different security levels. The research work on home environment networks is given in Chapter 7. A home environment service knowledge management system is proposed, which can manage whole information of a home environment and help all software configure and update procedures across multivendor environments. Conclusions and outlooks of the research work presented in this thesis are given in Chapter 8.

1.1.3 Chapters Based on Publications

This Ph.D study resulted in 17 peer-reviewed journal and conference contributions [1–17]. The research work presented in this thesis is mainly based on those publications. This section provides a map which links different chapters of this thesis to the respective research papers. The map is shown in Table 1.1.

Chapter	Paper	Author number
3	Combination of [1] and [7]	First and Second
4	Combination of [4], [8], [12] and [17]	First, First, First,First and First
5	Based on [2]	First
6	Combination of [15] and [16]	First and First
7	Combination of [3], [13] and [14]	First,Third and Third

Table 1.1: Chapters of thesis based on research papers.

Chapter 2

Reliable Transport Networks Background

2.1 Transport Networks and Their Requirments

There are a number of different purposes to deploy a telecommunication network. When this network is used as a transport network, the main purpose is to provide a reliable link for information transmission. To develop a qualified transport network, several characteristics should be considered. As a transport network, rather than the transport layer of a specific network, it should support traffic originated from a wide range of services. In other words, client independency or transmission transparency provides better adaptability. It should also provide Quality of Service (QoS) to ensure transmission performance according to different levels of agreements. Protection and management mechanism are two other important features for a transport network to increase network robustness. Additionally, from the economic point of view, transport network should balance the traffic and make the physical media used more efficiently. Lower Capital Expenditures (CAPEX) and Operating Expenditures (OPEX) also bring more profits.

In the recommendation "Generic functional architecture of transport networks" [20] published by Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) in Mar 2000,

it provides a technology-independent standardization for transport networks by describing a functional architecture of transport networks. All the components, functions and mechanisms introduced in [20] are designed to fulfill the requirements of transport networks.

2.2 Transport Network Technologies

Traditional telecommunication technologies, such as Synchronous Digital Hierarchy (SDH) and Asynchronous Transfer Mode (ATM), are widely used as solutions to deploy transport networks due to their great carrier grade quality. However those technologies, especially the SDH, were originally designed for transmitting circuit-based services, which are no longer suitable and efficient for the increasingly demanded packet-based services, such as Voice over IP (VoIP) and IP Television (IPTV) services. Multiprotocol Label Switching - Transport Profile (MPLS-TP) and Provider Backbone Bridge Traffic Engineering (PBB-TE) technologies are two promising alternatives for network carriers to meet the challenges. Both of them are based on mature technologies. They aim at deploying the hybrid packet-based and circuit-based transport networks in a simple and cost-efficient way and at the same time keeping the same high level of reliability set by the SDH and the ATM technologies.

2.2.1 MPLS-TP Technology

MPLS-TP is an ITU and IETF joint effort which is based on the mature MPLS packet technology. The MPLS technology was first standardized by IETF to provide a effective way to transport network layer packets [21]. ITU investigated and standardized the MPLS technology following the transport network structure requirements defined by ITU [20]. ITU also suggested another adapted MPLS technology, Transport MPLS (T-MPLS) [22–25], which removes some unnecessary properties of MPLS and makes it more suitable for being a transport network technology. Now ITU and IETF work together on MPLS-TP, which aims at supporting the capabilities and functionalities needed for packet-transport network services and operations through combing the packet experience of MPLS with the operational experience and practices of existing transport networks [26].

Unlike the traditional routing scheme, one of the most favorable features of MPLS-TP is that the MPLS-TP router forwards packets based on labels. In the traditional IP routing scheme, each router makes an independent forwarding decision based on the destination address of the incoming packet. Every router along the transmission path performs the same forwarding decision process. Actually, such same process could be simplified and be done only once. In an MPLS-TP network, this function is allocated in the ingress node, which is the first router where the user traffic enters the MPLS-TP network. Based on some preconfigured criteria, such as destination address or the combinations of different conditions, the incoming user traffic is divided into different Forwarding Equivalence Classes (FECs). Insofar as the forwarding decision is concerned, the packets, which belong to a particular FEC and travel from a particular node, do not need to be distinguished again and will follow the same transmission path. Therefore, for each FEC a label is assigned based on the FEC-to-NHLFE Map. NHLFE stands for Next Hop Label Forwarding Entry, which includes the information of the packet's next hop, the operation to perform on the packet's label and the outgoing label. According to the NHLFE information, packets are labeled and sent out from the ingress node. When a labeled packet arrives at the next MPLS-TP router (which usually is called Label Switching Router (LSR)), the incoming label is used as an index to check the forwarding table to find the NHLFE information. Using the NHLFE information, the incoming label is swapped into the new outgoing label and the packet is forwarded to the next hop. After a series of label swapping actions, the packet is delivered to the egress node, which is the last MPLS-TP router before the packet goes out of the MPLS-TP network domain. The label information in each LSR is configured before the traffic transmission. There are two ways to configure the labels, by manual configuration or by Label Distribution Protocols. The label swapping path is called Label Switched Path (LSP). Because of the label preconfigured feature, the LSP can be controlled and the MPLS-TP network is thus called connection-oriented network. The process of the transmission of MPLS-TP is illustrated in Figure 2.1.

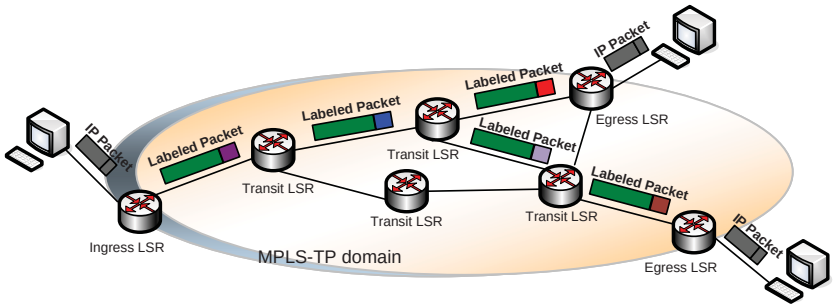


Figure 2.1: MPLS-TP traffic transmission.

2.2.2 PBB-TE Technology

The Ethernet has been developed as a Local Area Network (LAN) protocol since the early 1970s. Based on early Ethernet technologies, IEEE (Institute of Electrical and Electronics Engineers) developed and standardized Ethernet technologies in IEEE Std 802.3 LAN standard, which is issued in 1985. As the Ethernet evolves, a number of horizontal enhancements are adopted. Such horizontal enhancements expand LAN's service area and make LAN technologies to be used in Metropolitan Area Networks(MAN). Also more functions are added, such as Virtual LAN (VLAN), traffic management, etc. These enhancements are standardized in IEEE Std 802.1 series standards.

IEEE Std 802.1D [27] specifies Media Access Control (MAC) bridges which mainly implement the interconnection of separate IEEE 802 LANs. IEEE Std 802.1Q [28] provides Virtual LAN Services. Service provider networks are separated from customer networks in IEEE Std 802.1ad [29]. In order to distinguish the service VLAN and customer VLAN, two new tags, S-VLAN tag and C-VLAN tag, are introduced. Such strategy is usually called Q-in-Q mechanism. IEEE Std 802.1ag [30] proposes Connectivity Fault Management to detect, verify and isolate the connectivity failures in a VLAN. IEEE Std 802.1ah [31] further isolates the customer addresses and VLANs from provider backbone addresses and VLANs. It provides a method to interconnect independent

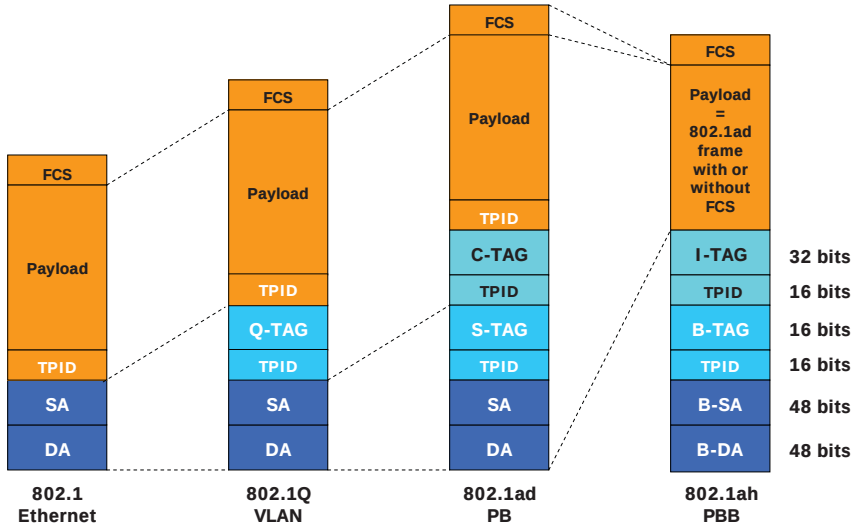


Figure 2.2: Evolvement of Ethernet towards transport networks in terms of tag changes [18].

provider bridged networks to offer much more service instances. Such strategy is usually called MAC-in-MAC mechanism. This evolution can be demonstrated by the evolvement of tags introduced, which is shown in Figure 2.2.

PBB-TE is a new effort from IEEE which is standardized in IEEE Std 802.1Qay [32]. It provides a packet-switched connection-oriented Ethernet technology for carrier grade transport networks, which is based on a few modifications of IEEE Std 802.1ah and IEEE Std 802.1ag standard. PBB-TE adopts an external management plane for determining and deploying the traffic paths crossing the Carrier Ethernet networks. The management plane helps network operators to implement traffic engineering and network management over the paths. Each path is identified by the combination of the Backbone Source MAC Address (B-SA), Backbone Destination MAC Address (B-DA) and Backbone VLAN Identifier (B-VID). The B-VID is used to distinguish different paths to the same destination. PBB-TE provides network services to network

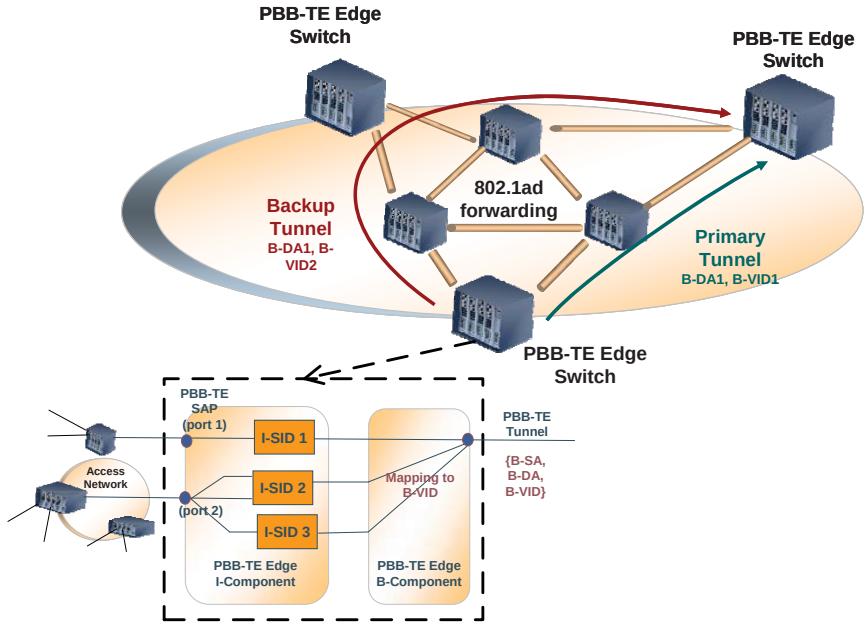


Figure 2.3: PBB-TE traffic transmission.

users. The network service is identified by Service Instance Identifier (I-SID). Each service is associated with a preconfigured network path. The combination of B-DA and B-VID is used to forward frames. The B-DA and B-SA are globally unique, which greatly reduces the complicated network operations of exchanging network addresses. A more detailed transmission model is illustrated in Figure 2.3. PBB-TE disables the spanning tree protocol and the address learning process. The filtering information of the forwarding table is preset by the management system. The static forwarding database avoids complex signalling and provides more efficient network resource utilization. If a frame is an unknown frame for a bridge, PBB-TE discards the frame instead of flooding it, which prevents from unexpected network traffic.

2.3 Building up Reliability in Transport Networks

It is critical to deliver reliable network services with strict service level agreements to end customers. Survivability is the network's ability to recover traffic delivery following a failure or a degradation. It is such a complex issue that involves many parts of the networks, different network layers and lots of recovery strategies. Within the scope of this thesis, a general overview and some recovery schemes are introduced as background information for the research work presented in the next several chapters.

A resilient network is required to detect facility or node degradation or failure and perform recovery operations in a time sensitive way with certain levels of service level agreements. The network can be affected by many kinds of failures, such as physical link cut, device failure, system configuration bug and so on. The degradation usually is observed by packet loss or delay measurement. The failure and degradation could be detected by upper layer applications or reported by lower layers. Transport networks normally get help from some automatically maintenance functions, such as Operation, Administration, and Maintenance (OAM) functions to monitor the state of the networks. Upon the detection of the failures, proper recovery operations are triggered. There are many types of recovery schemes, some examples are introduced in the following subsection.

2.3.1 Recovery Schemes

Protection

In the protection scheme, the resources are pre-allocated for reestablishing traffic deliveries. Linear protection is the most common mechanism when deploying a protection recovery scheme. It has the simplest form where there is a dedicated recovery entity for each working entity, whereas in the most complex mode, m recovery resources need to be shared by n working entities.

- 1+1 Protection

In 1+1 protection, the traffic is fed both on working and protection paths. The selector on the receiver node is simply configured to choose the better signals.

- 1:1 Protection

  In 1:1 protection, one protection resource is configured for one working entity. Under failure free situations, only the working entity is in charge of transmitting the traffic, while the traffic is switched onto the protection entity after the detection of a failure or degradation.

- 1:n and m:n Protection

  In a more general case, 1:n protection, one protection entity is allocated for n working entities. The protected n entities are prioritized when there are no sufficient protection resources. The most complex protection, m:n protection, protects m working entities on n protection entities.

Restoration

Restoration is different from protection in the sense of the provision of recovery resources. The recovery resources are only allocated at the time of need. Restoration represents a more efficient way of using network resource. However, there is no guarantee that enough resources are available to recover the traffic when a failure or degradation happens. Furthermore, the extra computation time delays the whole recovery actions.

2.3.2 Ring Topology Protection

Some tailored protection schemes may be required for different network topologies if the optimized mechanisms perform significantly better than the generic mechanism in the same topology. Ring protection is a good example of such topology-aware protection schemes.

Quite different from protection schemes used for mesh topology networks, ring protection schemes take advantages of the characteristics of ring. For instance, ring has two directions on all of the links. All the entities in clockwise direction can be configured as working entities and

the ones in counter-clockwise direction can be configured as protection entities. Furthermore, ring can always survive from one cut and still keep every node along the ring connected.

The number of recovery elements and the amount of OAM functions are all promisingly reduced. Furthermore, most of the deployed Synchronous Optical Networking (SONET)/SDH networks are based on ring structure. Designing transport network services on the same network topology with SONET/SDH legacy networks will significantly reduce both CAPEX and OPEX.

2.3.3 OAM Functions

OAM is an important and fundamental functionality in transport networks as it helps transport network operators to monitor the network infrastructure and helps transport service providers to monitor the transport services with diverse service level agreements. Through automatically detecting failures and service degradations, the network operational complexity is greatly reduced. The network survivability is also enhanced by the OAM's ability to efficiently trigger the recovery schemes even before end users report the problems. The OAM functions provide a management structure and a comprehensive set of tools to the network carriers. In the following subsections, the functional elements and the structure of the OAM are introduced, and also some particular methods which will be used in the scope of this thesis are described.

The OAM Structure and Functional Elements

The OAM operates in the context of Maintenance Entities (MEs) which represent the relationship between two Maintenance Entity Group (MEG) End Points (MEPs). The MEP is an OAM mechanism entity which cooperates with other MEPs in the same MEG to implement the maintenance and monitoring functions on ME. One or more MEs that belong to the same transport path and are maintained and monitored as a group, construct a MEG. Between MEPs, there are zero or more intermediate points, called MEG Intermediate Points (MIPs), which cooperate with associated MEPs to perform certain types of OAM functions. Figure 2.4 shows an example of a MEG consisting of two MEs and three MEPs.

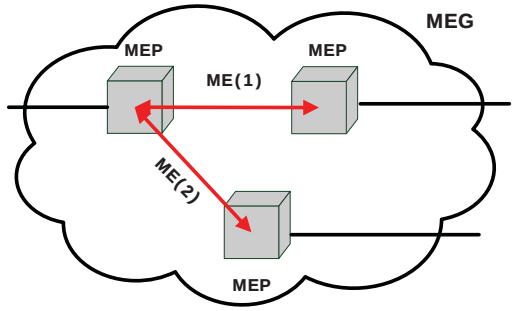


Figure 2.4: Structure and functional components of OAM.

Continuity Check (CC) and Connectivity Verification (CV) Methods

The CC function is used to detect the defects which are associated with status of connectivity. And the CV function is to detect an unexpected connectivity defect between two MEGs, as well as unexpected connectivity within the MEG with an unexpected MEP [33].

MEP periodically sends Continuity Check and Connectivity Verification (CC-V) packets with CC and CV information to its peer MEPs. The CC and CV information mainly include MEG ID, MEP ID and transmission period. When receiving a CC-V packet, the MEP checks the CC and CV information and reports the status of unexpected information.

- CC-V Transmission

  The CC-V packets are periodically transmitted to peer MEPs in the same MEG, which is shown in Figure 2.5. The transmission period is a predefined parameter and is encoded in the Period field of a CC-V packet. There are three main types of applications, and each one has different requirements for the CC-V transmission period. For fault management, the default transmission period is 1 second. For Performance Monitoring, the default transmission period is 100 milliseconds. For Protection Switching, the default transmission period is 3.33 milliseconds. According to demands,

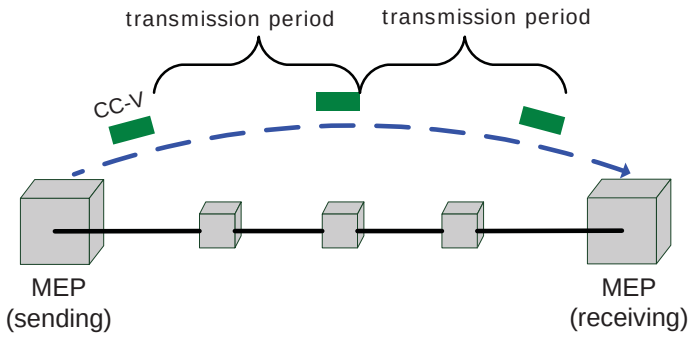


Figure 2.5: CC-V packet transmission.

CC-V transmission period could also be configured to one of the other four values, 10ms, 10s, 1min and 10min.

- CC-V Reception

  If a MEP has not received any CC-V packets from a given peer MEP during the last 3.5*CC-V transmission period, the loss of continuity (LOC) defect is detected, which indicates that the continuity is lost between this given pair of MEPs. The situation is shown in the Figure 2.6.(a).

  Upon receiving a CC-V packet, the MEP checks the CV information carried by CC-V packet. If the MEG ID carried by CC-V packet is not identical with the MEG ID of the receiving MEP, then the Mismerge defect is detected. This indicates there is some unexpected connectivity between the pair of MEPs. If the MEG ID is right, but the MEP ID carried by CC-V packet equals to the MEP ID of the receiving MEP, or is not in the list of the expected MEPs on peer MEPs, then the Unexpected MEP defect is detected. This means an unexpected MEP connectivity within MEG, which is shown in Figure 2.6.(b). If MEG ID and MEP ID are correct, but the value of the Period field is not the same as the configured CC-V transmission period of the receiving MEP, then the Unexpected Period defect is detected, which indicates that the

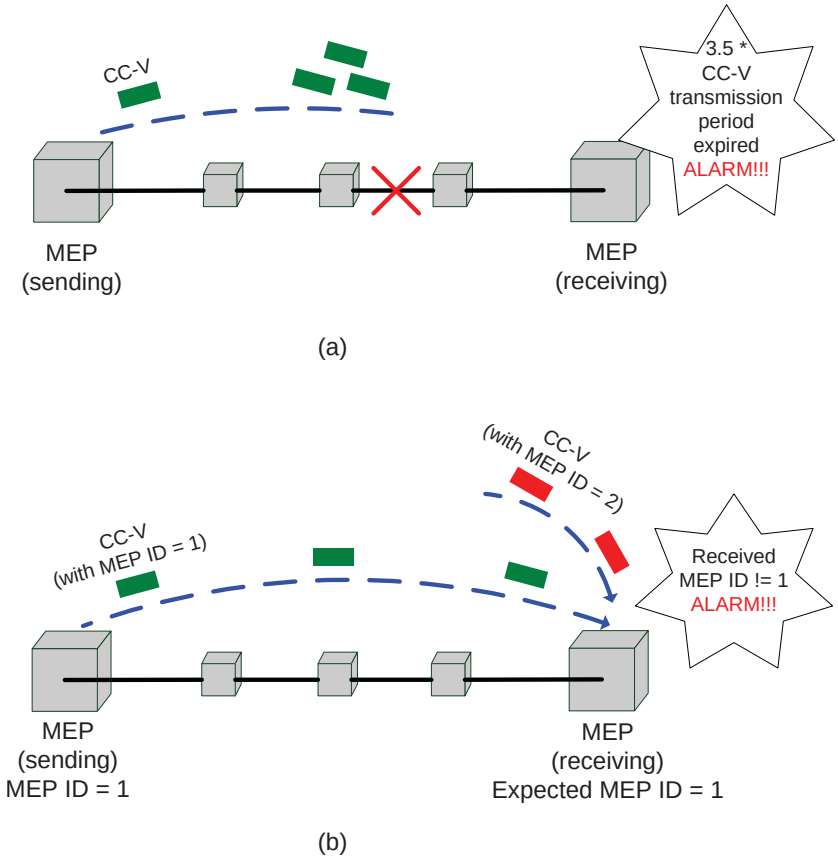


Figure 2.6: The defects detected by the CC-V reception.

two MEPs use different CC-V transmission rates.

Remote Defect Indication (RDI) Methods

The RDI method is capable of performing single-ended fault management and contributing to far-end performance monitoring. RDI information is used to inform the peer MEPs the sending MEP's condition of encountering a signal fail. The RDI information is piggy-backed onto the CC-V packet.

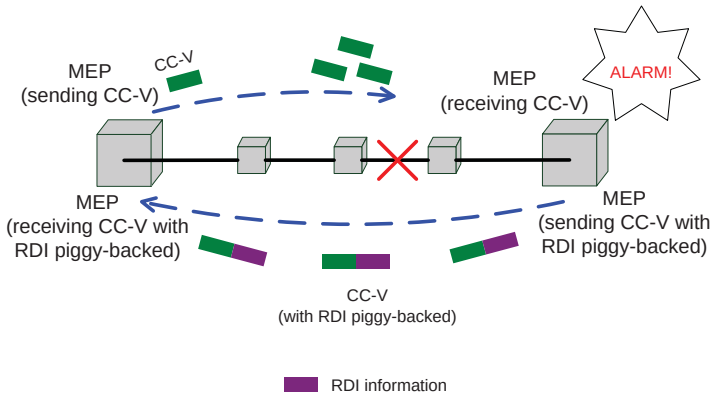


Figure 2.7: RDI information transmission.

- RDI Information Transmission

  When detecting a signal fail condition, the MEP puts the RDI information to the periodically transmitted CC-V packets until the signal fail condition is cleared.

- RDI Information Reception

  When receiving a CC-V packet with RDI information, the MEP knows that the sending MEP encounters a signal fail condition. Figure 2.7 shows the CC-V packet with RDI information when the loss of continuity (LOC) defect is detected by far-end MEP.

2.4 Summary

In this chapter transport networks and their requirements are introduced. Two mainly adopted packet-based transmission technologies, MPLS-TP and PBB-TE, are described. They aim at achieving the high benchmarks set by traditional transport technologies and at the same time keeping the operation simple and the cost at a profit level.

Among various transport network requirements, reliability is one of the most important and complex concerns faced by all network car-

riers. Many recovery schemes, such as protection and restoration are deployed to ensure the transport services to meet certain service level agreements. Based on ring structure, some tailed protection schemes are investigated, aiming at achieving better performance in terms of the amount of involved protection entities, the operation complexity, the resource consumption and so on. OAM is another functionality employed in transport networks, which monitors the network infrastructure and the quality of the provided transport services. With the help of OAM, the reliability of transport networks is further enhanced.

Chapter 3

Protection Schemes on Single-Ring Topology for MPLS-TP Multicast Services

3.1 Introduction

The challenges of ensuring the reliability of the MPLS-TP multicast services on single-ring network are addressed in this chapter. Based on the investigations and the comparisons of the schemes suggested by ITU and IETF for MPLS-TP ring protection, two novel MPLS-TP ring protection schemes are proposed, Sub-Path Maintenance Entity based Wrapping (SPME-based Wrapping) protection scheme and Sub-Path Maintenance Entity based Ring Optimized Multicast Wrapping (SPME-based ROM-Wrapping) protection scheme. Both of them are aiming at retaining the advantages of the existing MPLS-TP ring protections and avoiding their limitations. The requirements of designing an efficient and reliable MPLS-TP ring protection strategy, for instance with respect to label consumption, bandwidth utilization and operation complexity are well studied.

The remainder of this chapter is structured as follows. Section 3.2 overviews the related work for MPLS-TP ring protections. In Sec-

tion 3.3, the studies on the ROM-Wrapping and the SPME-based Steering protection schemes are presented. The advantages and limitations are concluded. Section 3.4 introduces the proposed SPME-based Wrapping protection scheme and Section 3.5 describes the proposed SPME-based ROM-Wrapping protection scheme. Section 3.7 summaries the chapter.

3.2 Related Work

There have been many concrete research work on MPLS-TP multicast ring protections taken by IETF and ITU. For example, the draft standards [34, 35] were proposed by IETF. In both of these draft standards, protection paths are preconfigured for all working Label Switching Paths (LSPs). When there is a failure detected by Operation, Administration and Maintenance (OAM) function, the Automatic Protection Switching (APS) protocol is used to coordinate the protection switching actions between the ring nodes [34]. However, such mechanisms greatly rely on the accurate performance of the APS messages. It also requires high intelligent function settings for each node to distinguish error-affected LSPs and trigger proper protection switching.

In another IETF's draft standard [36], APS protocol is not adopted, and OAM function is used both for failure detection and protection trigger, which significantly simplifies signaling for protection switching. Two protection switching schemes are proposed in [36], the ROM-Wrapping and the SPME-based Steering for point-to-multipoint (p2mp) paths. The ROM-Wrapping is an improved scheme based on the traditional wrapping protection switching, aiming at reducing bandwidth waste and removing the distinction between link failures and node failures. The SPME-based Steering is the second protection scheme proposed by [36]. It introduces tunnels to protection configurations and protection switching operations. The protection resource utilization is improved through sharing protection tunnels by many working LSPs. Both of these schemes present valuable methods for ensuring reliable MPLS-TP multicast services based on ring structures. However, there are still some limitations, which make them not fulfill some of the MPLS-TP ring protection requirements stated in [26], for instance the label consumption.

This chapter investigates both of these protection schemes, and proposes a SPME-based Wrapping protection scheme and a SPME-based ROM-Wrapping protection scheme for MPLS-TP multicast services, which retain the advantages of the previous schemes and at the same time, avoid the limitations.

3.3 Investigation on the ROM-Wrapping and the SPME-Based Steering Protection Schemes

3.3.1 The ROM-Wrapping Protection Scheme

The ROM-Wrapping protecion scheme operates almost the same as the traditional wrapping, but with one difference - rather than configuring the recovery LSP between the end nodes of a failed link (link protection mode) or between the upstream and downstream node of a failed node (node protection mode), the ROM-Wrapping configures a recovery p2mp LSP from the upstream (with respect to the failure) node and all the egress nodes (for the particular LSP) downstream from the failure [36]. Instead of re-joining the working path, the configured protection path indicates all the egress nodes. In Figure 3.1, a link failure is assumed on the link from node C to node D. Figure 3.1.(a) and Figure 3.1.(b) illustrate the difference between the traditional wrapping and the ROM-Wrapping.

It is clear from Figure 3.1 that overlapping paths between the working path and the protection path in the traditional wrapping case are avoided by the ROM-Wrapping and resource utilization is improved. The traditional wrapping protection scheme needs to be set as link failure mode or node failure mode, since this configuration affects where the re-join point is. If link failure mode is applied, the re-join point will be the downstream node regarding to the failure (node D). If node failure mode is configured, the protection path will re-join the working path at the following node of the failure (node E). This mechanism sometimes causes problems. For example, in Figure 3.1.(a), if node failure mode is applied, the protection path will re-join at node E, even the failure is a link failure. If node D is an egress node, then it will not receive any traffic, even node D does not incur any failures. The ROM-Wrapping pro-

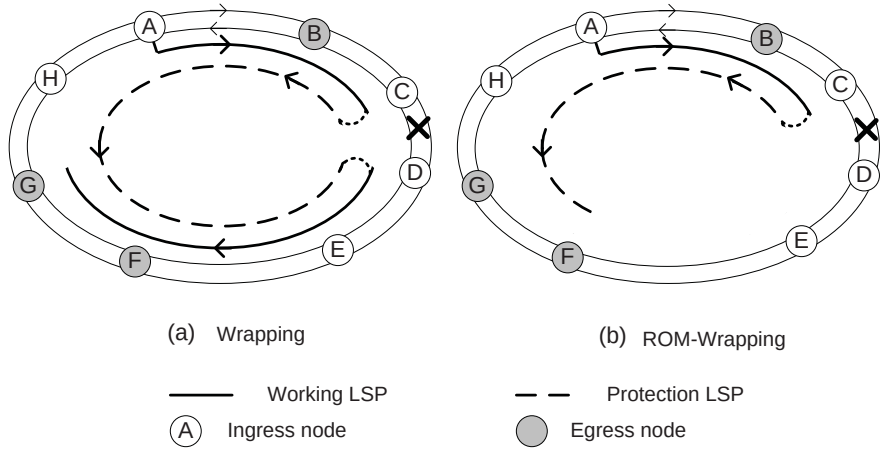


Figure 3.1: Operations of the Wrapping and the ROM-Wrapping protection schemes.

tection scheme avoids distinguishing node and link failures, and works correctly for both situations. However, there are still some limitations on the ROM-Wrapping. When using the ROM-Wrapping, each working LSP has to be configured with its own protection LSP, since a protection LSP needs to indicate all the egress nodes for this working LSP and normally different working LSPs have different egress nodes. Furthermore, regarding to different failures of one particular working LSP, different protection paths need to be configured individually, due to each protection LSP ending at different locations based on where the failure happens. Such pre-configuration consumes a lot of MPLS-TP labels, which weakens the optimization criteria of minimizing the number of labels required in [26].

3.3.2 The SPME-based Steering Protection Scheme

The SPME-based Steering is the second protection scheme proposed by [36]. The SPME construct can be defined between any two Label Switch Routers (LSRs) of a MPLS-TP LSP [36]. It works as a tunnel and is implemented by pushing SPME label into the packet label stack.

Two SPMEs in opposite directions are configured for each node locating on the ring. The SPME in the clockwise direction is designed as the working SPME and the SPME in the counter-clockwise direction as the protection SPME. All the LSPs coming from the same ingress node are aggregated together in SPME and the traffic is delivered on both SPMEs configured for this ingress nodes. Each node except the ingress node is configured as egress node along SPMEs. The traffic is forwarded along both SPMEs and is dropped at each node except the ingress node (by dropping it means a copy of the traffic is left at the node). At each node, the underlying label (below the SPME label) is examined and used to distinguish whether this node is a destination node or not. Each node originally accepts the traffic from the working SPME. If the traffic from the working SPME is cut off by some failures, the node switches its selector bridge to receive the traffic from the protection SPME. Figure 3.2 illustrates the operation of the SPME-based Steering. Figure 3.2.(a) shows the traffic delivery under failure free conditions and Figure 3.2.(b) shows the SPME-based Steering operations when the link from node C to node D incurs a failure. The swapping of label stack is listed in Figure 3.2.(a), which stay the same when the failure happens. The content of the label stack follows the rule defined in [36]. Each level is separated by the "|" character and the bottom is denoted by the string "BOS". The Px(y) indicates the label for LSR-X to transmit to LSR-Y over the SPME. The string "LI" denotes the label of an ingress for a LSP, and the string "LE" denotes the label of the egress for a LSP [36]. For instance, the packet enters ring from ingress node A with label stack [LI|BOS]. LI is the incoming label in the ingress node A for a particular LSP. Two SPME labels are pushed into label stack of this packet, when it is delivered by working and protection SPMEs. PA1(H) denotes that the packet need to be sent from node A to the final egress node H. The number "1" indicates this SPME is the working SPME in the clockwise direction. PA2(B) indicates that the packet needs to be delivered from node A to node B. Node B is the final egress node. The number "2" points out that this SPME is the protection SPME in the counter-clockwise direction.

The advantages of applying the SPME-based Steering are that the protection resource can be shared by many LSPs and label consumption is significantly reduced. However, this scheme concurrently sends

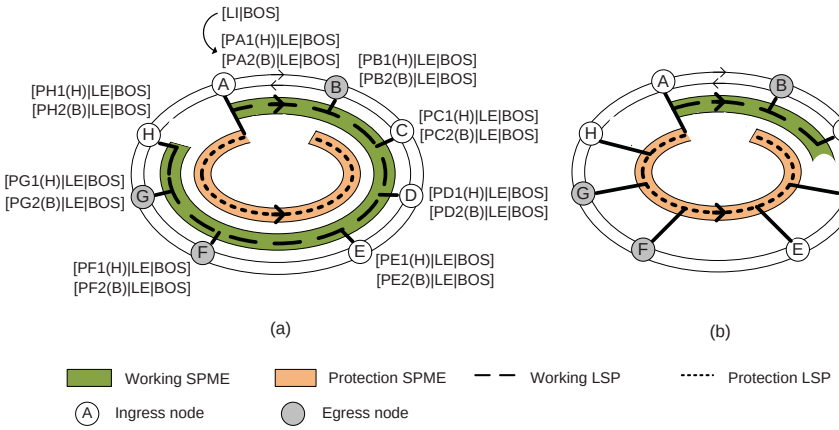


Figure 3.2: Operation of the SPME-based Steering.

the traffic on both working and protection paths, consequently increasing the traffic load and power consumption. Another limitation that should be noticed is that since all the LSPs from the same ingress node are aggregated, in such a way, traffic engineering, such as per hop behavior, can only be implemented for tunnels, rather than for each LSP. In other words, the SPME-based Steering method builds a "broadcast" tunnel from an ingress node to the rest of the nodes locating on the ring. Setting up a tunnel in part of networks indeed can increase management efficiency and simplify network operation. But establishing a tunnel crossing the entire ring network and losing the control of each LSP inside the tunnel within entire ring network scope bring a limitation, especially for large scale ring networks. Furthermore, it can be seen in Figure 3.2 that each node uses the same label (LE), the outgoing label of the ingress node, to identify this LSP. The label LE is significant on the entire ring network, rather than only on a single link, which happens to be the main reason that how a finer granularity traffic engineering can be applied for each LSP on a link.

3.4 The Proposed SPME-based Wrapping Protection Scheme

In order to introduce 1:1 protection switching method into SPME-based Steering, the SPME-based Wrapping protection scheme is proposed [1]. Taking advantages of 1:1 protection switching, bandwidth utilizations and power consumptions are decreased. In the meantime the operation complexity does not increase much, since the switching is based on tunnels instead of on each LSP.

Like SPME-based Steering, two opposite directional SPMEs are configured for each node on the ring with any subset nodes on the ring configured as egress node, and the SPME in the clockwise direction is designed as the working SPME and the SPME in the counter-clockwise direction as the protection SPME. Instead of concurrently sending the traffic on both SPMEs, the traffic is only sent along the working SPME under failure free situation. The OAM function is used between neighboring nodes to monitor network continuity and report failures. The node that receives failure report and locates on the upstream of the failure in the clockwise direction is in charge of triggering protection switching. After the protection switching has been triggered in a particular node, all the traffic in the working SPME is switched to the protection SPME configured for this node. Figure 3.3 illustrates the traffic delivery under failure free situation (a) and protection switching situation (b). The label assignment and swapping in the label stack follows the rule of the SPME-based Steering. In order to avoid receiving multiple packet copies, the switched bridge only accepts packets from the clockwise direction unless the traffic in the clockwise direction is affected by failures. The underlying label is examined by each node to distinguish whether this node is a destination or not.

3.5 The Proposed SPME-based ROM-Wrapping Protection Scheme

The proposed SPME-based ROM-Wrapping protection scheme is designed based on the ROM-Wrapping protection scheme. In order to reduce the complexity of pre-configuring the protection paths and the

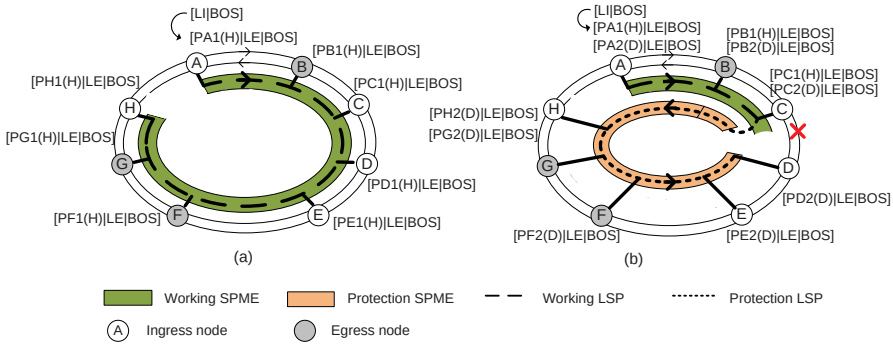


Figure 3.3: Operation of the SPME-based Wrapping.

label consumption of setting up protection paths, the idea of the tunnel is adopted to establish protection tunnels, which are shared by working LSPs. As to protection situation, the proposed Reverse Label Table Checking (RLTC) method and the introduced Virtual Entry (VE) in label tables are able to maintain the identities of different LSPs and keep label significant on each single link, providing network carriers fully control on each particular LSP and eliminating the limitations on the traffic engineering, arose from building tunnels. Thus network carriers have ability to deploy finer granularity traffic engineering. Additionally, a symbol named Protection Receive Symbol (PRS) is proposed to avoid multiple copies received by the egress nodes.

Under failure free situation, traffic is delivered individually by the working LSP in the clockwise direction. Packets along a particular LSP are only dropped to the egress nodes of this LSP. In order to set up SPME-based ROM-Wrapping protection scheme, for each node, one SPME is configured, which is in the counter-clockwise direction and used as protection SPME. The OAM function is applied between neighboring nodes to monitor network continuity and report failures. When a failure is detected by a node and the protection switching is triggered by this node, all the LSPs (regardless from which ingress node those LSPs come) passing through this node will be switched onto the protection SPME configured for this node. The protection switching operation

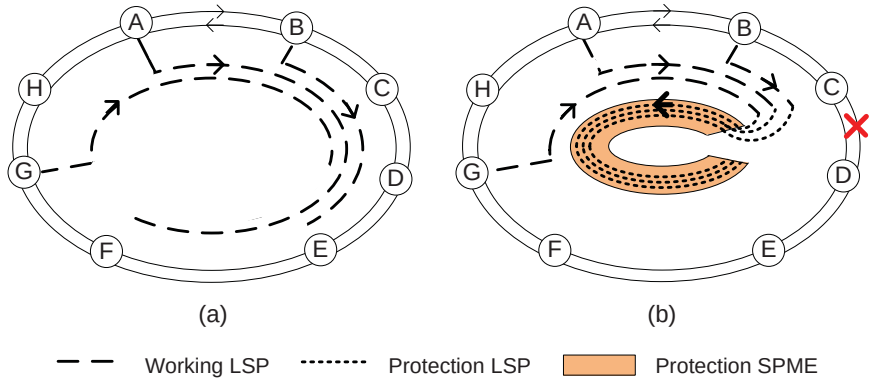


Figure 3.4: Operation of the proposed SPME-based ROM-Wrapping protection scheme.

is illustrated in Figure 3.4. Figure 3.4.(a) shows the traffic delivery of three LSPs from different ingress nodes under an failure free condition. Figure 3.4.(b) demonstrates the protection switching after the failure of the link from node C to node D is detected. All LSPs are switched onto the protection SPME configured for node C.

The protection SPME tunnel is realized by operating label stack in the way that protection SPME labels are pushed into the label stacks of all the packets entering the protection SPMEs. Protection SPME labels are swapped along the protection SPME. For node C in Figure 3.4, the swapping of protection SPME labels is: PC(D)-PB(D)-PA(D)-PH(D)-PG(D)-PF(D)-PE(D)-PD(D). Inside protection SPME, all protected LSPs are distinguishable. They can be recognized by the underlying labels. How to maintain the identities of all LSPs is implemented by the LSP path retrieve, which is explained in the next paragraph. Through distinguishing LSPs, packets along the protection SPME are only dropped at the corresponding egress nodes of different LSPs.

In order to keep the identities of the LSPs inside protection SPME, LSP paths are retrieved by using the proposed RLTC method. The RLTC is operated after protection SPME label is popped out and before protection SPME label is swapped. During normal LSP label swapping,

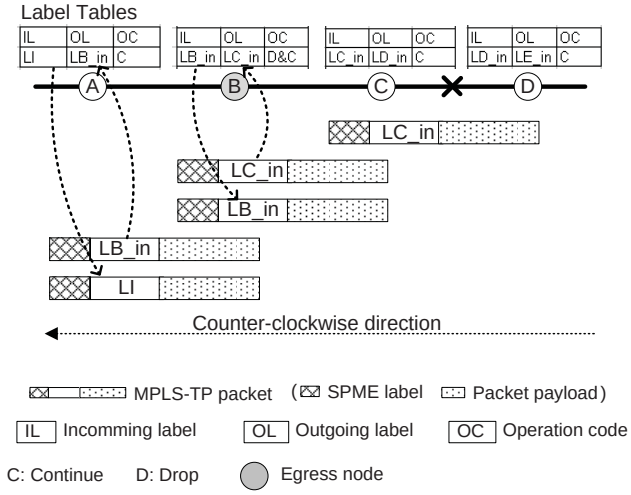


Figure 3.5: Reverse Label Table Checking (RLTC) and the corresponding label swapping.

the label of an incoming packet is used to check Incoming Label (IL) column of the label table. In RLTC method, the label of an incoming packet is used to check the Outgoing Label (OL) column of the label table and the corresponding item of the IL will be swapped into the label field of the packet before the packet is sent out. Figure 3.5 shows the operation of the RLTC method. By applying the RLTC, LSP path inside protection SPME is retrieved in the counter-clockwise direction based on the information stored in the label tables of the working LSP path in the clockwise direction. The information in the label table of the working LSP helps nodes distinguish particular LSP inside the protection SPME. Based on the operation code in the working LSPs' label tables, for instance "drop", "continue", "drop and continue", the node can decide whether to accept packets from protection SPME or not.

The VE, Virtual Entry, is introduced and stored in certain nodes' working LSP label table to make sure the RLTC method work correctly. Figure 3.6 explains why the VE in label table is needed. In Figure 3.6.(a), the information for presenting a particular working LSP is illustrated, which is stored in each node on the ring. Assuming a

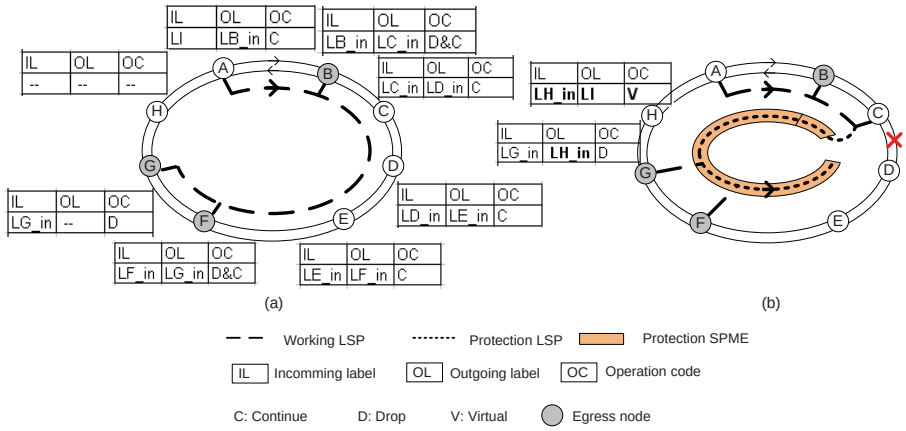


Figure 3.6: Adds Virtual Entries into the label tables of the working LSP.

failure is incurred on the link from node C to node D, the traffic is switched onto the protection SPME and the RLTC is applied. When traffic reaches node H in the counter-clockwise direction, the RLTC will not work correctly, since node H originally is not part of this working LSP and consequently has no information about this working LSP. Figure 3.6.(b) shows the way of introducing VEs in the label tables to solve the problem (only the changes in label tables are shown in Figure 3.6.(b)). Node H uses a VE in its label table to retrieve the working LSP. Actually VEs connect the tail of a working LSP to the head of a working LSP, making the RLTC continue retrieving working LSP cross the break between the start and the end of a working LSP. The operation code of the VEs is set to "virtual", which distinguishes themselves from the other operation codes. The "virtual" operation code only forwards packets in the counter-clockwise direction. In theory, the last node along working LSP will delete all the packets of this LSP. In case for some unknown reasons that some packets do come to a node in the clockwise direction and check VEs in label table, the corresponding operation code, "virtual", will cause packet deletion to prevent looping.

In order to avoid multiple copies of packets received by egress nodes, a PRS symbol is proposed, which is maintained in each packet's pro-

tection SPME label. Only after the operation code is equal to "D" in label table, can the PRS be set to "accepted", before that the PRS stay as "unaccepted". Along the protection SPME, packets can only be accepted with the PRS set as "accepted". Beacuse there are some overlaps between the working LSPs and the protection SPME, and packets which have already been accepted from the working LSPs should not be accepted again from the protection SPME. Only until packets have arrived the tail of the normal working LSP (the operation code is set as "D"), packets can be accepted by egress nodes.

3.6 The Comparisons between the ROM-Wrapping and the SPME-based ROM-Wrapping

In this section, a comparison between the proposed SPME-based ROM-Wrapping protection scheme and the ROM-Wrapping protection scheme is discussed in several resilience related aspects, showing the advantages brought by the SPME-based ROM-Wrapping scheme.

3.6.1 The Multicast Services under Failure free Situation

Same as the ROM-Wrapping, the SPME-based ROM-Wrapping has not changed the way of delivering multicast traffic under the failure free situation, which keeps great consistency with traditional MPLS-TP multicast services.

3.6.2 Distinguish between Link and Node Failures

Compared to the traditional wrapping scheme, one of the advantages of the ROM-Wrapping is that there is no need to distinguish link and node failures. The protection actions for a link failure will not fail just because the system is configured as node protection, or the other way around. SPME-based ROM-Wrapping has been able to maintain this advantage.

3.6.3 Saving Protection Label Consumption

One of the advantages of the SPME-based ROM-Wrapping, compared to the ROM-Wrapping, is that it greatly reduces the protection label consumption. For each working LSP, the ROM-Wrapping needs to configure an individual protection LSP. With respect to different failures, different protection paths need to be configured. All those pre-configured paths implies one thing: a great amount of labels are needed. The protection label configurations of the multicast traffic illustrated in Figure 3.1 are listed in the following two tables as an example. Table 3.1 lists all the labels that are needed by the ROM-Wrapping protection scheme for this particular multicast traffic, and compared with it, the labels needed by the SPME-based ROM-Wrapping are listed in Table 3.2. It needs to be noted that the second part of Table 3.2 lists the labels configured for the protection SPMEs, which are shared by all the multicast traffic passing through the links. It is clear that SPME-based ROM-Wrapping can save a lot of label resources by sharing the protection SPME tunnels and reusing the working LSP's labels. The advantage will become even more obvious when the network load is heavy. Since the label consumption is a big concern in MPLS-TP requirements [26], the SPME-based ROM-Wrapping protection scheme provides a valuable alternative to provide protection for MPLS-TP multicast services.

3.6.4 Protection Tunnel and LSP Identity

The operations of the protection switching and OAM functions become much easier in the SPME-based ROM-Wrapping protection scheme, given that the protection switching and OAM functions are operated based on the protection tunnels. However, the RLTC method manages to keep LSP identifiable on each single link, which provides network carriers the full control on each particular LSP and a way to deploy finer granularity traffic engineering.

3.6.5 Protection Hop Count and Protection Bandwidth

In the SPME-based ROM-Wrapping, the protection traffic travels along the protection SPME tunnel and ends at the end of the protection SPME. In other words, all the protection traffic is transmitted all the

	Label consumption of the ROM-Wrapping for a particular multicast traffic
Protected LSP:	B_in >C_in >D_in >E_in >F_in >G_in
A's Backup:	A_H_in >A_G_in >A_F_in >A_E_in >A_D_in > A_C_in >A_B_in
B's Backup:	B_A_in >B_H_in >B_G_in >B_F_in
C's Backup:	C_B_in >C_A_in >C_H_in >C_G_in >C_F_in
D's Backup:	D_C_in >D_B_in >D_A_in >D_H_in >D_G_in > D_F_in
E's Backup:	E_D_in >E_C_in >D_B_in >D_A_in >D_H_in > E_G_in >E_F_in
F's Backup:	F_E_in >F_D_in >F_C_in >F_B_in >F_A_in > F_H_in >F_G_in

Table 3.1: All the labels needed for protecting a specific multicast traffic by the ROM-Wrapping protection scheme.

way around the ring. On the first thought, it seems to use a lot more protection bandwidth for each traffic. While the protection traffic under the ROM-Wrapping scheme also travels most part of the ring. Among all the failure situations, the maximum hop counts it can save (comparing to travel the entire ring) is the largest hop distance between the egress nodes. Since the traffic dealt with has multiple egress nodes on a single ring, the advantage on the protection bandwidth of the ROM-Wrapping is not that overwhelming, not to mention the less label consumption and the configuration simplicity brought by the SPME-based ROM-Wrapping.

The most concerned parameter of a protection scheme is the protection switching time, which is highly related to the hop counts traveled by the protection traffic. Even though the SPME-based ROM-Wrapping uses a little more protection bandwidth, the hop counts made by the protection traffic before the egress nodes receive the traffic are the same as the ROM-Wrapping. Same as the ROM-Wrapping, the SPME-based ROM-Wrapping delivers the protection traffic in the counter-clockwise direction. Because the SPME-based ROM-Wrapping reuses the information of the working label tables, the egress node accepts the traffic as soon as it receives the traffic from the protection SPME. Thus the

	Label consumption of the SPME-based ROM-Wrapping for a particular multicast traffic
Protected LSP:	B_in >C_in >D_in >E_in >F_in >G_in ″H_in″>A_in
	″″: virtual entry

	Label consumption of the SPME-based ROM-Wrapping for shared protection SPMEs
A's P-SPME:	PA(B)>PH(B) >PG(B) >PF(B) >PE(B) > PD(B) >PC(B) >PB(B)
B's P-SPME:	PB(C)>PA(C) >PH(C) >PG(C) >PF(C) > PE(C) >PD(C) >PC(C)
C's P-SPME:	PC(D)>PB(D)>PA(D) >PH(D) >PG(D) > PF(D) >PE(D) >PD(D)
D's P-SPME:	PD(E)>PC(E)>PB(E)>PA(E) >PH(E) > PG(E) >PF(E) >PE(E)
E's P-SPME:	PE(F)>PD(F)>PC(F)>PB(F)>PA(F) > PH(F) >PG(F) >PF(F)
F's P-SPME:	PF(G)>PE(G)>PD(G)>PC(G)>PB(G)> PA(G) >PH(G) >PG(G)
H's P-SPME:	PH(A)>PG(A)>PF(A)>PE(A)>PD(A)> PC(A)>PB(A)>PA(A)

Table 3.2: All the labels needed for protecting a specific multicast traffic by the SPME-based ROM-Wrapping protection scheme and the protection labels shared by all multicast LSPs.

protection hop counts before the traffic is recovered by the egress nodes are the same under the two protection schemes.

3.7 Summary

As the result of investigation and comparison between the schemes introduced by the IETF and ITU for MPLS-TP multicast ring protections, this chapter proposes two MPLS-TP ring protections to provide resilience for MPLS-TP multicast services: the SPME-based Wrapping and the SPME-based ROM-Wrapping protection schemes. The SPME-based Wrapping implements a wrapping between a shared working tunnel and a shared protection tunnel. LSPs are aggregated into tunnels, and thus the operations for providing multicast services and protection switching are greatly simplified. However the traffic engineering based on LSPs is hardly achieved. The proposed SPME-based ROM-Wrapping protection scheme is implemented without changing or disturbing any traditional MPLS-TP ring multicast service operations. The protection scheme operates the same for both link failures and node failures. In order to reduce complicated protection pre-configurations, shared protection tunnels are built to deliver the switched traffic. In the meantime, LSP identities are maintained under protection situation by operating the RLTC method, helping network carriers control each particular LSP to deploy finer granularity traffic engineering. In order to configure protection paths, a great amount of labels are needed in the ROM-Wrapping protection scheme, which disobeys the requirements of reducing label consumptions when providing ring protection. The protection label consumption is greatly reduced in the SPME-based ROM-Wrapping protection scheme by using SPME tunnels and the RLTC method. Compared to the ROM-Wrapping protection scheme, the SPME-based ROM-Wrapping uses a little more protection bandwidth, but the hop count before the protection traffic is received by each egress node (one of the important factors affect protection switching time) remain the same.

All the strategies introduced in this chapter are implemented in a single-ring structure. However in more realistic environments, the rings are interconnected with each other. For instance, within metro area, normally the networks are composed by a main Metro-core ring and several Metro-Access rings attached. With more general sense, the in-

troduced protection strategies in this chapter should be extended into interconnected-ring structures. And such requirements are also stated in MPLS-TP requirements [26]: MPLS-TP must include recovery mechanisms that operate in any single ring supported in MPLS-TP, and continue to operate within the single rings even when the rings are interconnected. More detailed explanations and implementations are expressed in the next chapter.

Chapter 4

Protection Schemes on Interconnected-Ring Topology for MPLS-TP Multicast Services

4.1 Introduction

This chapter investigates the issue of implementing protection schemes for MPLS-TP multicast services on interconnected-ring topology. The studied ring protection schemes consist of the Sub-Path Maintenance Entity based Steering (SPME-based Steering) protection scheme and the Sub-Path Maintenance Entity based Ring Optimized Multicast Wrapping (SPME-based ROM-Wrapping) protection scheme. The SPME-based Steering protection scheme is proposed in [36–38] and its strategy has been discussed in Chapter 3. However, the proposal for the SPME-based Steering protection scheme only describes how to apply it on a single-ring structure and the implementation on interconnected-ring networks is suggested as a future work. This chapter extends the SPME-based Steering protection scheme onto interconnected-ring networks and presents a detailed implementation. The SPME-base ROM-Wrapping protection scheme proposed in Chapter 3 is further studied and extended onto interconnected-ring networks.

The rest of this chapter is organized as follows. In Section 4.2, a general interconnected-ring structure is introduced for the studies. Section 4.3 describes the multicast service, OAM functions and protection switching in the SPME-based Steering protection scheme on the interconnected-ring network. Section 4.4 introduces the strategies in the SPME-based ROM-Wrapping protection scheme on the interconnected-ring network. A comparison between these two protection schemes is presented in Section 4.5. Section 4.6 summaries the chapter.

4.2 Interconnected-Ring Structures

Metro area networks consist of many rings. Typically, access rings attach to a core ring. There are two common methods to interconnect rings, dual-node interconnection and single-node interconnection. When applying dual-node interconnection, the interconnected rings are connected by two nodes, whereas single-node interconnection connects two rings via only one node. Dual-node interconnection provides a 1:1 or 1+1 alike protection for the interconnection nodes and links. From a reliability's point of view the single-node interconnection has no ability to recover from failures on interconnection points. Therefore, the dual-node interconnection method is adopted in this chapter to connect rings. Figure 4.1 illustrates a general interconnected-ring structure which is used for the studies in this chapter. The structure includes 5 rings, indexed from Ring 1 to Ring 5.

The interconnection nodes are denoted with "IN" as the beginning of the name. There are four interconnection nodes between two interconnected rings, two on each side. Typically, the interconnection nodes on the upstream ring are in charge of delivering and protecting the traffic flows traveling from one ring to another. For instance, IN211 and IN212 are in charge of delivering and protecting the traffic flows from Ring 2 to Ring 1. Three integer numbers are used to denote an interconnection node. The first number indicates which ring this interconnection node locates. The second number represents which ring this interconnection node connects to. The third number is a sequence number indicating this interconnection node is the first or second interconnection node in the clockwise direction. IN122 and IN121 do the same job for the traffic flows from Ring 1 to Ring 2. The cooperation between interconnection

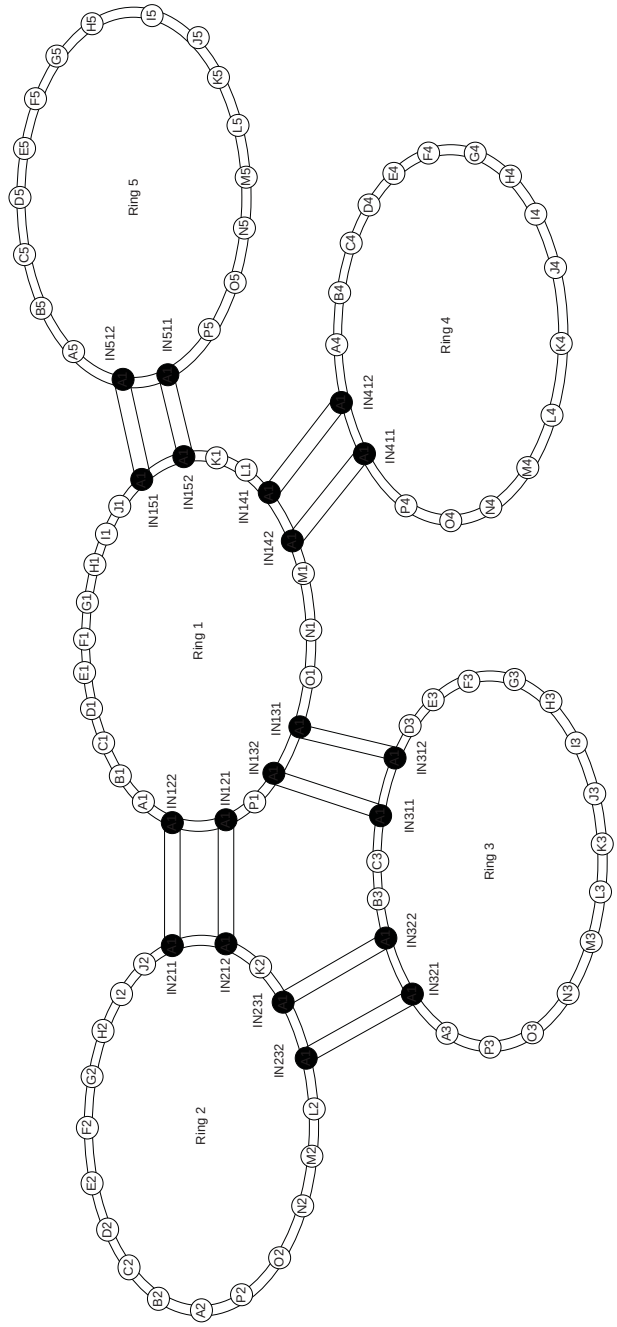


Figure 4.1: A general interconnected-ring structure generated for the studies.

nodes is different from one protection scheme to another. More details are described in the related sections.

Besides interconnection nodes, there are sixteen nodes located on each ring. The number sixteen is stated in [26] to be the number that must be supported in a ring in order to support the upgrade of existing Time-Division Multiplexing (TDM) rings to MPLS-TP.

4.3 SPME-based Steering on Interconnected-Ring Networks

The strategies of the SPME-based Steering protection scheme on the single-ring network have been explained in Chapter 3, including SPME configuration, multicast traffic delivery, OAM functions and protection switching. In order to maintain consistency, the functions from the SPME-based Steering protection scheme on a local ring proposed in [37, 38] and described in Chapter 3 are kept as many as possible. Changes are only made due to the need for interconnection purpose. The new proposed functions of traffic delivery, OAM and protection switching are mainly related to interconnection nodes.

In standard [37], the SPME labeling is realized by pushing an extra SPME label into label stacks and swapping SPME labels when packets are delivered inside the SPME tunnel. This method has been described and adopted by Chapter 3. In this chapter, another method, the context labeling method is adopted to realize SPMEs, which is used in [38]. The concept of context labeling is originally defined in [39]. A context-identifying label indicates a context label space that is used to interpret the context-specific labels (underlying the context-identifying label) for a specific tunnel. The SPME label is designed as a context-identifying label and point to a label information base (LIB). At each hop, the node looks up the context-specific label (particular Lable Switched Path(LSP) label) in the forwarding table, which is stored in a particular LIB indicated by the context-indentifying label(SPME label). Through the context-specific label, the forwarding function of the node decides the action taken for a packet. More detailed explanations and examples can be found in [38, 39].

4.3.1 Multicast Services of the SPME-based Steering Protection Scheme on Interconnected-Ring networks

Following the basic rules of the SPME-based Steering, all the traffic flows entering the interconnected-ring networks from the same ingress node are aggregated together. For these traffic flows, the ring from where the traffic flows first enter the interconnected-ring network is referred to as the source ring and all the other rings are referred to as the downstream rings. On the source ring, two point-to-multipoint (p2mp) SPMEs in the opposite direction are configured for a ingress node. The SPME in the clockwise direction is used as the working SPME and the protection SPME is in the counter-clockwise direction. Traffic is delivered on both SPMEs. The same working SPME context label (or protection SPME context label) is used for all the traffic from the same ingress node. Each particular LSP uses its own context-specific label.

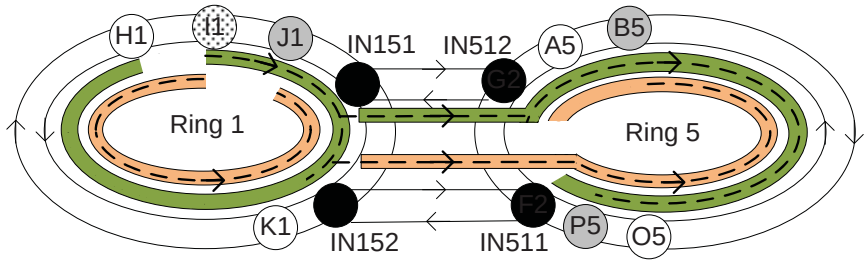
Through both interconnection nodes, the traffic is delivered into the downstream rings. For downstream rings, the ring in the upstream direction is considered the upstream ring. Two p2mp SPMEs are configured from the interconnection nodes of the upstream ring all the way around the downstream ring in opposite directions. The working SPME is in the clockwise direction and the protection SPME is in the counter-clockwise direction. Traffic is transmitted on both SPMEs on the downstream ring. The first interconnection node of the upstream ring in the clockwise direction is configured as the working interconnection node and the other one is used as the protection interconnection node. The context-identifying label of the SPMEs designated for the downstream rings can be configured as a different value from the one used in the upstream ring. For simplicity, the same working (protection) context-identifying label for the working (protection) SPME are configured for a particular ingress node on the whole interconnected-ring network.

Figure 4.2 illustrates two multicast traffic examples. Since all interconnection nodes on the interconnected-ring network operate following the same principle, in the following figures, only one interconnection part of the ring network is presented. In Figure 4.2(a), multicast traffic flow M_1 enters the interconnected-ring network from node I1 located on Ring 1. Node J1, B5 and P5 are the destinations of M_1. Ring 1 is the source ring for M_1 and also the upstream ring for Ring 5. Node IN151 is

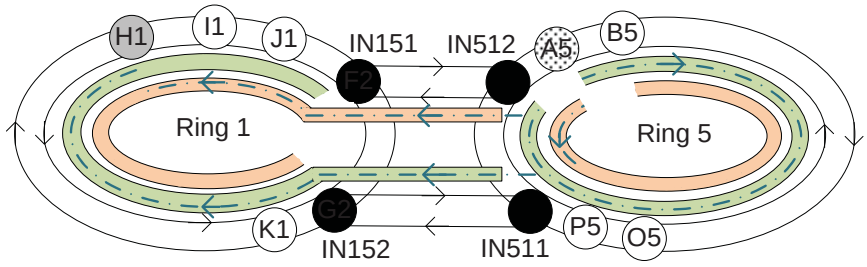
the first one between two interconnection nodes (IN151, IN152) located along Ring 1 in the clockwise direction, thus node IN151 is configured as the working interconnection node for downstream Ring 5. The working SPME designated for downstream Ring 5 starts from node IN151 and passes node IN512, node A5 and ends at node IN511. Node IN152 is configured as the protection interconnection node for downstream Ring 5. The protection SPME for downstream Ring 5 starts from node IN152 and ends at node IN512. The traffic of M_1 is delivered from Ring 1 to Ring 5, interconnection nodes IN151 and IN152 between Ring 1 and Ring 5 operate interconnection functions. Multicast traffic flow M_2 travels from Ring 5 to Ring 1. Node IN511 and IN512 are the interconnection nodes which perform interconnection functions for the traffic delivered from Ring 5 to Ring 1. The operation is shown in Figure 4.2(b). All the configuration of SPMEs follows the same rule as described in case shown in Figure 4.2(a). One thing needs to be noted that node IN511 is the one configured as the working interconnection node, not node IN512.

The interconnection nodes play two logic roles in the interconnected-ring network, a normal node sitting on the ring and a logic ingress node to deliver the multicast traffic into the interconnected downstream ring. Inside interconnection nodes the forwarding functions of these two logic roles operate separately. The two forwarding functions are denoted as normal node forwarding function (NN_FF) and logic ingress node forwarding function (LIN_FF). Figure 4.3 illustrates the locations of the function blocks and also the data stream between the blocks.

The NN_FF of an interconnection node is executed first and is same as a normal node's forwarding function: identifying the context LIB and looking up the underlying context-specific label in the forwarding table, which is stored in identified LIB. The NN_FF passes all the received packets to the LIN_FF. Based on the information stored in a proposed Interconnection Nodes Functional Table (INFT), the LIN_FF decides whether a particular LSP should be delivered into interconnected downstream ring or not. Similar to the forwarding table, the INFT is stored in a specific LIB, which is indicated by the working (protection) SPME label. Table 4.1 illustrates the elements and contents of the INFTs on node IN151 and IN152 for the working and protection SPMEs used by multicast traffic M_1, when the working SPME for ingress node I_1 is configured with W_SPME_IngressI1 as the context-identifying la-



(a) multicast traffic flow M_1



(b) multicast traffic flow M_2

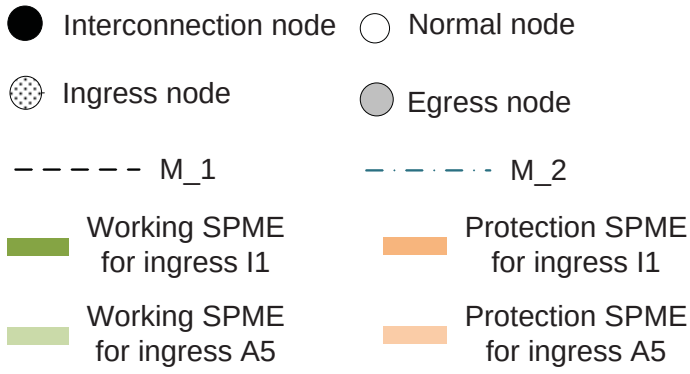


Figure 4.2: Configurations of the working and protection SPMEs on the interconnected-ring structure.

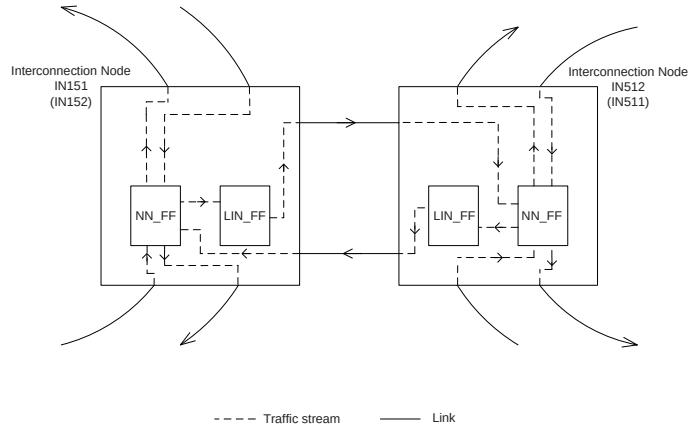


Figure 4.3: Forwarding funtion blocks and data stream inside interconnection nodes in the SPME-based Steering protection scheme.

bel and the protection SPME is configured with P_SPME_IngressI1. As the same, the working SPME for ingress node A_5 is configured with W_SPME_IngressA5 as the context-identifying label and the protection SPME is configured with P_SPME_IngressA5. Table 4.2 illustrates the contents on node IN511 and IN512 used by multicast traffic M_2.

After receiving packets from NN_FF, LIN_FF locates the same LIB pointed by context-identifying label and uses the underlying context-specific label as index to check the INFT. If there is no traffic request on the interconnected downstream ring from this traffic flow, the Function Enabled element of the INFT is set to False. If the Function Enabled element is marked as True, then the packets will be delivered into the interconnected downstream ring. The outgoing label listed under the Outgoing Label element will be used to swap the context-specific label. Packets will be transmitted on both downstream SPMEs (working and protection) configured for the ingress node from where the packets enter the network. As mentioned before, within the whole network one context-indentifying label is used for all the working SPMEs configured for a certain ingress node and one for all the protection SPMEs. Therefore, when the packets are delivered into downstream ring, they have the same working or protection context-indentifying labels as the ones

LIB: W_SPME_IngressI1

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN151:	J1_IN151_W	True	IN151_IN512_W
IN152:	IN151_IN152_W	True	IN152_IN511_P

(a)

LIB: P-SPME_IngressI1

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN152:	K1_IN152_P	False	IN152_IN511_P
IN151:	IN152_IN151_P	False	IN151_IN512_W

(b)

Table 4.1: Elements and contents of the INFTs on node IN151 and IN152 for working and protection SPME used by multicast traffic M_1

LIB: W_SPME_IngressA5

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN511:	P5_IN511_W	True	IN511_IN152_W
IN512:	IN511_IN512_W	True	IN512_IN151_P

(a)

LIB: P-SPME_IngressA5

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN512:	A5_IN512_P	False	IN512_IN151_P
IN511:	IN512_IN511_P	False	IN511_IN152_W

(b)

Table 4.2: Elements and contents of the INFTs on node IN151 and IN152 for working and protection SPME used by multicast traffic M_2

used in the upstream ring.

Under failure free situation, the NN_FFs of both working and protection interconnection nodes accept packets from the working SPME. The working interconnection node feeds the traffic into the working SPME on the downstream ring, whereas the protection interconnection node feeds the traffic into the protection SPME on the downstream ring. It is worth mentioning that, even though the protection interconnection nodes receive the traffic from the working SPME, the packets that are transmitted on the downstream ring's protection SPME still use the context-identifying label configured for the protection SPME. When there is a loss of continuity on the working SPME on the upstream ring, both working and protection interconnection nodes select the traffic from the protection SPME. However, the working interconnection node still transmits the traffic into the downstream ring by the working SPME and by doing this, the downstream ring will not be affected by the upstream ring's failure.

4.3.2 OAM Functions of the SPME-based Steering Protection Scheme on Interconnected-Ring Networks

The Continuity Check (CC) method of OAM functions is adopted to trigger the protection switching. For a given ingress node, the CC OAM function is operated on all working and protection SPMEs configured for this ingress node. If a node cannot receive any Continuity Check and Connectivity verification (CC-V) packet on the working SPME within 3.5 continuous CC-V transmission periods, a loss of continuity failure is assumed. Error-affected nodes trigger protection switching to read packets from the protection SPME. The ingress node is in charge of generating CC-V packets for both working and protection SPMEs on the source ring. All the CC-V packets transmitted on the downstream ring's working (protection) SPME are issued by the upstream ring's working (protection) interconnection node. The OAM function of the interconnection node is divided into two logic functions, the interconnection node's normal node OAM function (NN_OAM) and the interconnection node's logic ingress node OAM function (LIN_OAM). These two functions operate independently. The NN_OAM function checks

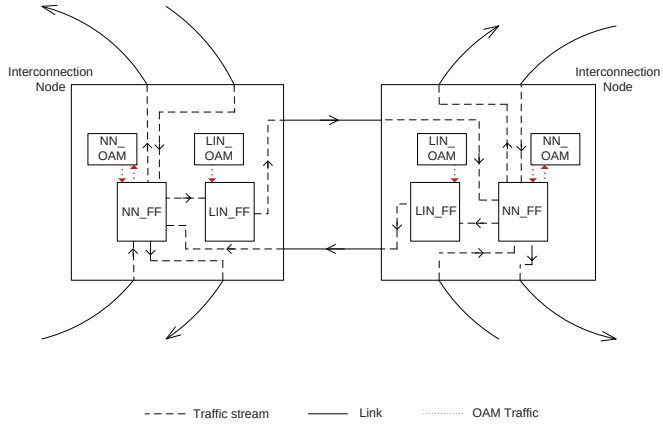


Figure 4.4: OAM funtion blocks inside interconnection nodes in the SPME-based Steering protection scheme.

the continuity of the working SPME on the local ring in order to perform protection switching to ensure a continuous traffic delivery into the downstream ring. The LIN_OAM function generates CC-V packets into the downstream ring's SPMEs. Figure 4.4 presents a complete node structure with respect to the forwarding and OAM functions.

4.3.3 Protection Switching of the SPME-based Steering Protection Scheme under the Interconnection Node and Link Failures

Figure 4.5 illustrates five types of interconnection node and link failures. In this work, only single failure is considered. Error 1 and Error 2 cause protection switching on Ring 5. Between these two failures, there is no need to distinguish the error types or locations. The nodes on Ring 5 just switch their selectors to read the traffic from the protection SPME when they stop receiving CC-V packets from working SPME. Error 3, 4 and 5 do not affect the working SPME on Ring 5, thus they do not trigger the protection switching on any node on Ring 5.

Figure 4.6 shows the protection operation under the failure on the working interconnection node on the upstream ring. The protection

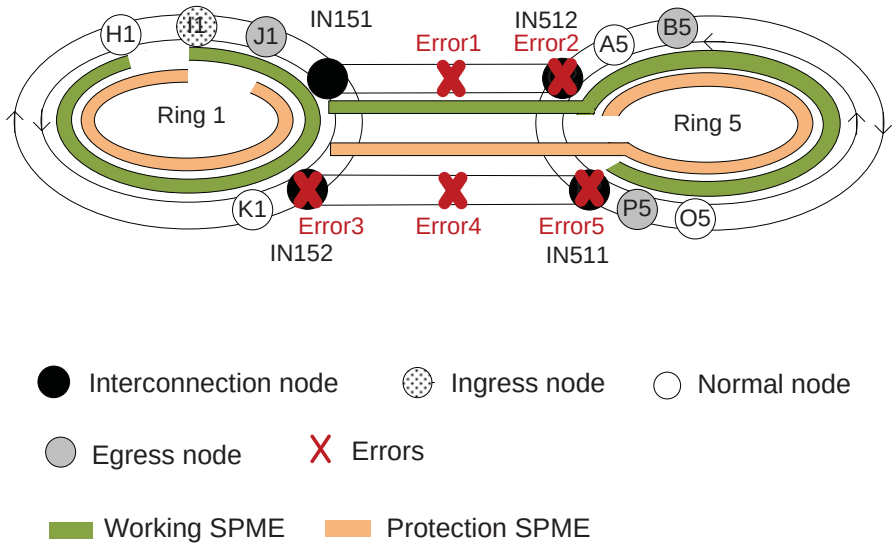


Figure 4.5: Protection switching of the SPME-based Steering protection scheme under interconnection node and link failures (Error 1-5).

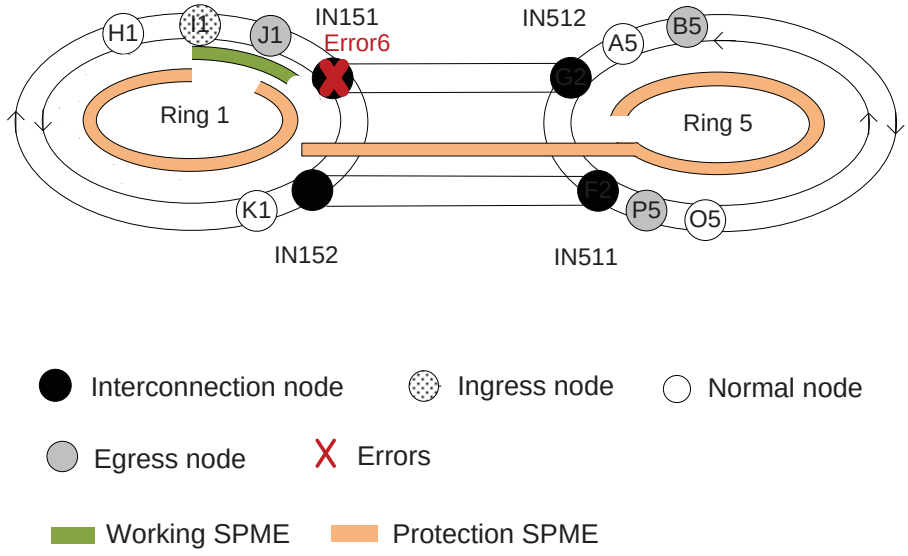


Figure 4.6: Protection switching of the SPME-based Steering protection scheme under interconnection node and link failures (Error 6).

LIB: P-SPME_IngressI1

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN152:	K1_IN152_P	~~False~~ True	IN152_IN511_P

Table 4.3: Changes of the INFT elements under working interconnetion node failure (Error 6).

interconnection node (IN152) first accepts the traffic from protection SPME on the upstream ring and then change the Function Enabled element to True on all the LSP from Ring 1 to Ring 5. The changes are shown in Table 4.3. All the nodes on the downstream ring switches the selector to accept the traffic from ingress node I1 from protection SPME.

The protection procedure under the failure of the link between inter-

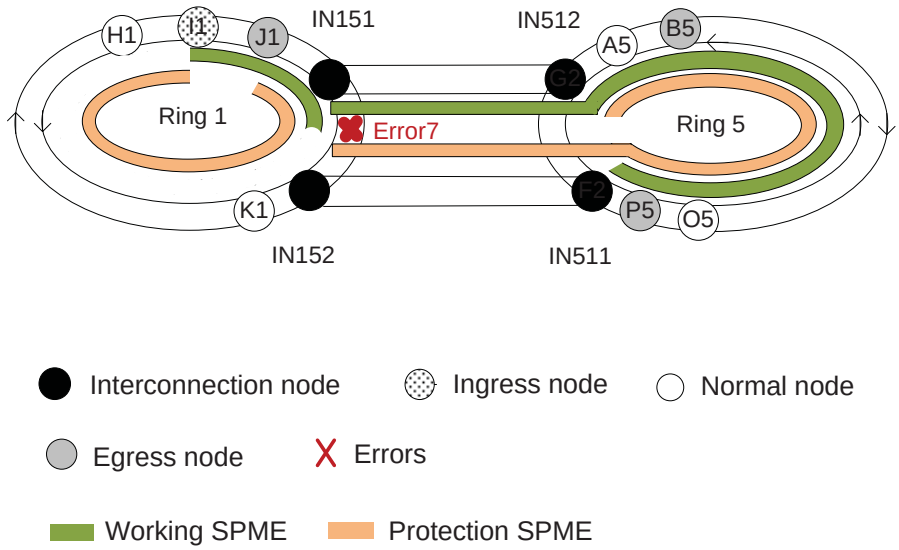


Figure 4.7: Protection switching of the SPME-based Steering protection scheme under the interconnection node and link failures (Error 7).

connection nodes on the upstream ring is shown in Figure 4.7. This failure does not affect the working interconnection node IN151 and working SPME in Ring 5. The protection interconnection node IN152 switches to accept the traffic from protection SPME on the upstream ring and then change the Function Enabled element to True for all LSPs from Ring 1 to Ring 5, which is the same as shown in Table 4.3.

4.4 SPME-based ROM-Wrapping on Interconnected-Ring Networks

This section continues the discussion about the proposed SPME-based ROM-Wrapping protection scheme and explains how it is applied on interconnected-ring networks. The functions of the SPME-based ROM-Wrapping protection scheme for a single-ring network, introduced in Chapter 3, are applied on each local ring of the interconnected-ring network. In this section the functionalities and strategies required to

interconnect rings are focused.

4.4.1 Multicast Services of the SPME-based ROM-Wrapping Protection Scheme on Interconnected-Ring Networks

The multicast services protected by the SPME-based ROM-Wrapping protection scheme are LSP based multicast services. In other words, all working LSPs are independently pre-configured and there is no aggregation among any working LSPs. Only protection SPMEs are configured for protection switching reasons. Traffic flows enter the downstream ring through the interconnection node located on the upstream ring. Since SPME-based ROM-Wrapping protection scheme is designed based on 1:N linear protection, only working interconnection node is enabled to transmit traffic flows into the downstream ring under failure free condition. The protection interconnection node is switched on until a failure happens. The first interconnection node along the upstream ring in the clockwise direction is configured as the working interconnection node and the second one is configured as the protection interconnection node.

The multicast traffic examples used in Section 4.3, M_1 and M_2 are reused in this section, and the multicast traffic transmissions of the SPME-based ROM-Wrapping are illustrated in Figure 4.8. M_1 enters the interconnected-ring network from node I1 (ingress node). Besides node J1, B5 and P5, node IN151 and IN152 are also configured as egress node for M_1, to make sure the interconnection nodes IN151 and IN152 get M_1 traffic to feed Ring 5. Under failure free situation, M_1 is delivered through the working interconnection node IN151 into the downstream ring Ring 5. The protection interconnection node IN152 is switched on to deliver M_1 traffic after the protection switching is triggered by a failure. M_2 enters the networks from node A5 (ingress node). Node IN511 is configured as the working interconnection node for the traffic from Ring 5 to Ring 1. Besides node H1, node IN511 and IN512 are also configured as egress nodes for M_2. Through node IN511, M_2 is delivered into Ring 1 under failure free situation.

Similar to the SPME-based Steering protection scheme, interconnection nodes play two logic roles in the SPME-based ROM-Wrapping protection scheme: a normal node on the local ring and a logic ingress

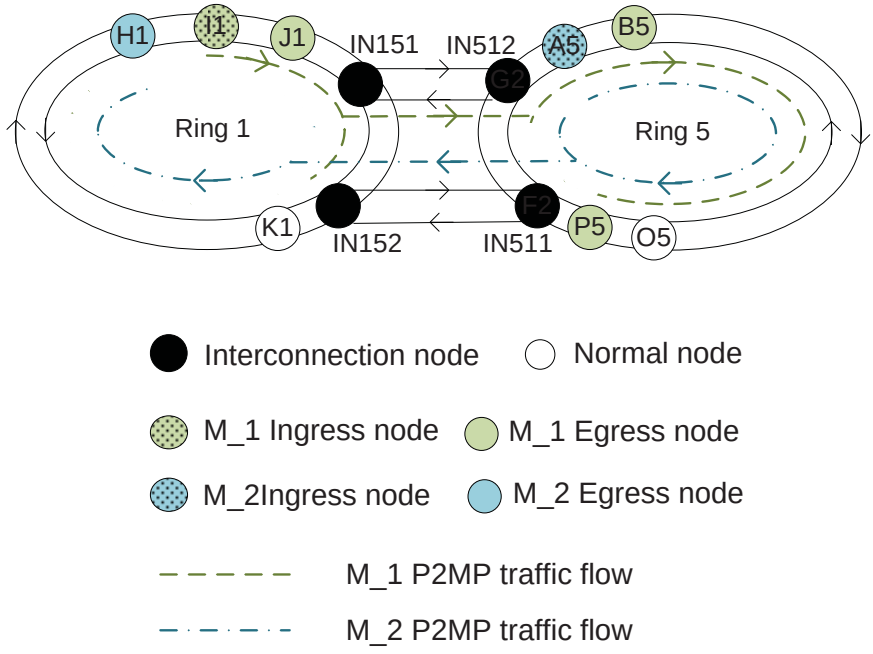


Figure 4.8: Multicast Services of the SPME-based ROM-Wrapping for multicast traffic M_1 and M_2 on interconnected-ring networks.

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN151:	M_1_J1_IN151	True	M_1_IN151_IN512
IN512:	M_1_IN151_IN512	—	M_1_IN511_IN512
IN152:	M_1_IN151_IN152	False	M_1_IN152_IN511
IN511:	M_1_IN152_IN511	—	M_1_IN511_IN512

Table 4.4: Elements and contents of the INFTs of the SPME-based ROM-Wrapping protection scheme for multicast traffic M_1.

node for the downstream ring. The forwarding functions are also divided into NN_FF and LIN_FF functions. However, due to difference in the protection strategy, in the SPME-based ROM-Wrapping protection scheme the cooperation between the forwarding functions of the interconnection nodes are quite different from the SPME-based Steering protection scheme. As shown in Figure 4.3, when traffic is transmitted from Ring 1 to Ring 5 under the SPME-based Steering protection scheme, the LIN_FF of node IN512 and node IN511 on the downstream Ring 5 are not used. However, in the SPME-based ROM-Wrapping protection scheme, the LIN_FF of node IN512 on the downstream Ring 5 needs to cooperate with the LIN_FF of node IN151 on the upstream Ring 1, when transmitting the traffic from Ring 1 to Ring 5. Figure 4.9 illustrates the locations of the forwarding function blocks and the data streams between the blocks. The multicast M_1 represents the traffic from Ring 1 to Ring 5 and the multicast M_2 represents the traffic from Ring 5 to Ring 1.

The SPME-based ROM-Wrapping protection scheme does not adopt the context label method, thus all forwarding tables and INFTs (interconnection nodes functional table) are not interpreted in different context label spaces. Example entries of INFTs for multicast traffic M_1 and M_2 are listed in Table 4.4 and Table 4.5.

The NN_FF of the interconnection node on the upstream ring passes all received packets to the LIN_FF on the same node. The LIN_FF uses the incoming label as index to check the INFT. If the Function Enabled element is marked as True, then the packet is delivered into the LIN_FF of the interconnection node on the downstream ring. If it is

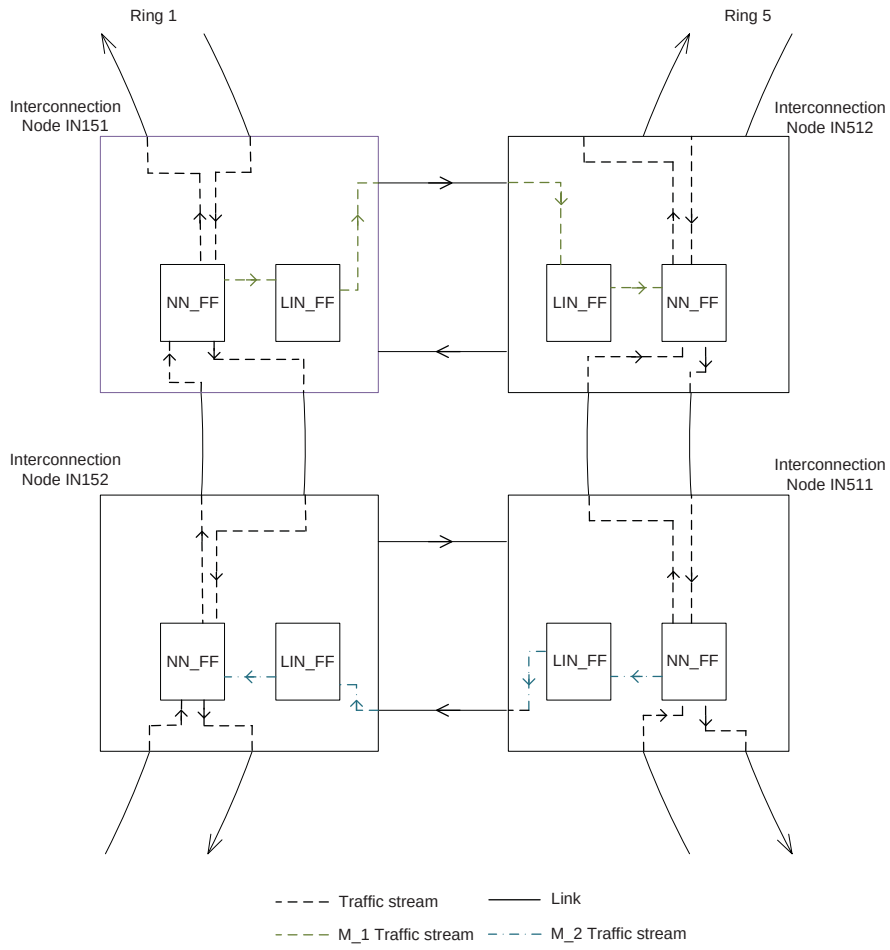


Figure 4.9: Forwarding funtion blocks and data stream inside interconnection nodes in the SPME-based ROM-Wrapping protection scheme.

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN511:	M_2_P5_IN511	True	M_2_IN511_IN152
IN152:	M_2_IN511_IN152	—	M_2_IN151_IN152
IN512:	M_2_IN511_IN512	False	M_2_IN512_IN151
IN151:	M_2_IN512_IN151	—	M_2_IN151_IN152

Table 4.5: Elements and contents of the INFTs of the SPME-based ROM-Wrapping protection scheme for multicast traffic M_2.

Forwarding Table

	Incomming Label	Outgoing Label	Operation Code
IN151:	M_1_J1_IN151	M_1_IN151_IN152	D&C
IN152:	M_1_IN151_IN152	M_1_IN152_K1	D
K1:	M_1_IN152_K1	M_1_K1_L1	V
IN512:	M_1_IN511_IN512	M_1_IN512_A5	C
A5:	M_1_IN512_A5	M_1_A5_B5	C
IN511:	M_1_P5_IN511	M_1_IN511_IN512	V

∗D:drop; C:continue; V:virtual.

Table 4.6: Forwarding table example of the SPME-based ROM-Wrapping protection scheme for multicast traffic M_1.

False, then the packet is deleted. The Function Enabled element is set as False, if there is no traffic request on the interconnected downstream ring from this traffic flow. Under failure free situation, this element is set to False on the protection interconnection node on the upstream ring. The outgoing label, listed under the Outgoing Label element, is used to swap the labels.

After the LIN_FF of the interconnection node on the downstream ring receives the packet, it uses the incoming label as index to check the INFT and swaps the label. The LIN_FF further passes the packet to the NN_FF on the same node. The NN_FF uses the incoming label as index to check the forwarding table, swaps the labels and injects the packet into the downstream ring link. Parts of the forwarding tables for traffic M_1 and M_2 are listed in Table 4.6 and Table 4.7.

Forwarding Table

	Incomming Label	Outgoing Label	Operation Code
IN511:	M_2_P5_IN511	M_2_IN511_IN512	D&C
IN512:	M_2_IN511_IN512	M_2_IN512_A5	D
A5:	M_2_IN512_A5	M_2_A5_B5	C
IN152:	M_2_IN151_IN152	M_2_IN152_K1	C
H1:	M_2_G1_H1	M_2_H1_I1	D
IN151:	M_2_J1_IN151	M_2_IN151_IN152	V

∗D:drop; C:continue; V:virtual.

Table 4.7: Forwarding table example of the SPME-based ROM-Wrapping protection scheme for multicast traffic M_2.

4.4.2 OAM Functions and Configured Protection SPMEs of the SPME-based ROM-Wrapping Protection Scheme on Interconnected-Ring Networks

The OAM functions of the SPME-based ROM-Wrapping also consist of two logic functions, the normal node OAM function (NN_OAM) and logic ingress node OAM function (LIN_OAM). The locations of the OAM function blocks inside the nodes structure are shown in Figure 4.10. Only the OAM functions used for the purpose of protecting traffic from Ring 1 to Ring 5 are illustrated.

The protection SPMEs are configured inside each local ring, similar to a single-ring case introduced in Section 3.5 of Chapter 3: for each node, one protection SPME is configured, which is in the counter-clockwise direction. The protection switching is triggered by the CC and Remote Defect Indication (RDI) OAM methods, which are operated between any two adjacent nodes on the ring. The NN_OAM functions of the interconnection nodes attend the local ring CC and RDI methods with their neighbors to ensure the interconnection nodes can get the traffic from the local ring. If the NN_OAM functions of the interconnection nodes find a failure, they switch all the LSPs onto the protection SPME configured for the error-affected Interconnection node on the local ring.

The LIN_OAM function of the working interconnection node on the upstream ring operates the CC and RDI methods with the LIN_OAM

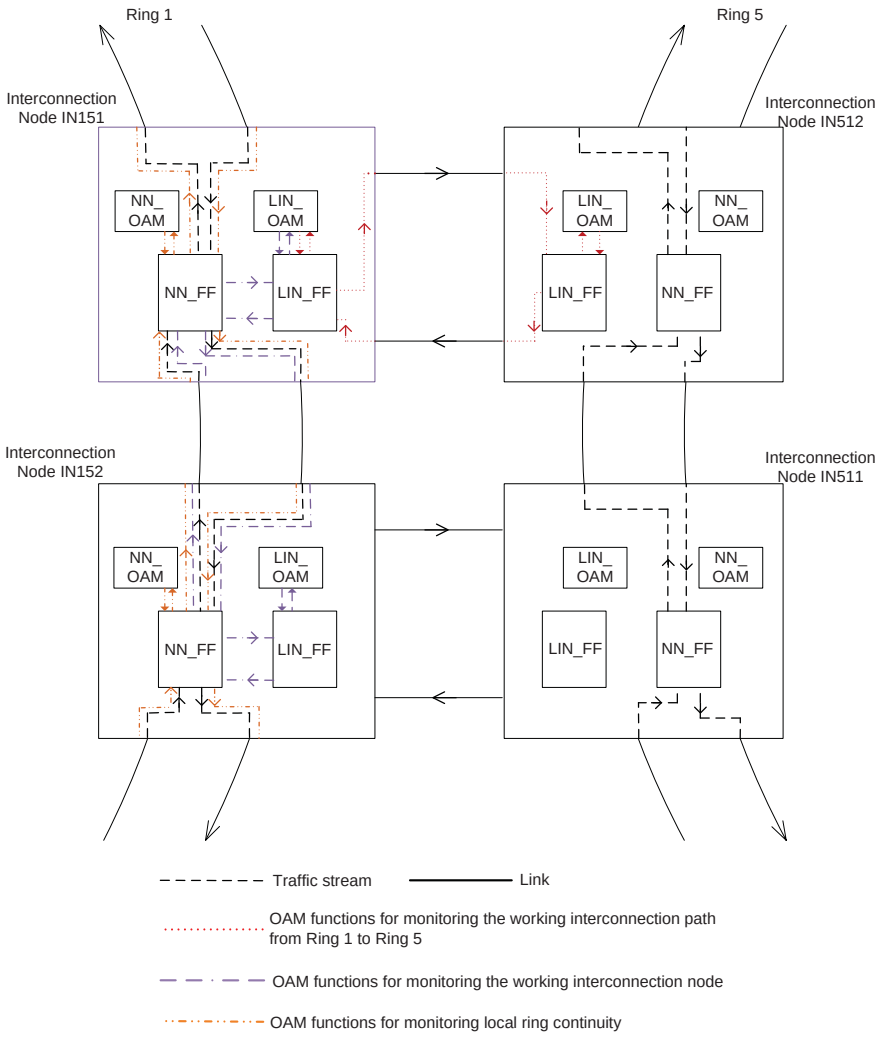


Figure 4.10: OAM functions of the SPME-based ROM-Wrapping for traffic from Ring 1 to Ring 5 on the interconnected-ring network.

function of the connected interconnection node on the downstream ring to ensure the reliability on the working path between the two rings. Figure 4.10 illustrates how the continuity between Ring 1 and Ring 5 are monitored. According to the operation of the OAM function for monitoring the working interconnection path from Ring 1 to Ring 5, node IN151 can be informed about the loss of continuity that may arise from the failure of the link between node IN151 and node IN512, or failure of node IN512. Based on the failure detection, node IN151 sends an message to inform node IN152 to start to transmit the traffic into the downstream ring. In order to start transmitting the received traffic, node IN152 sets the "Function Enabled" elements to True on all the entries which are configured for the traffic from Ring 1 to Ring 5. Node IN151 itself sets the "Function Enabled" elements to False on all the entries, which are configured for traffic from Ring 1 to Ring 5 and stops the transmission.

Since the SPME-based ROM-Wrapping protection scheme employs 1:1 linear protection between the working interconnection node and the protection interconnection node, the LIN_OAM function of the protection interconnection node on the upstream ring is in charge of monitoring the state of the working interconnection node on the upstream ring. Through this OAM function, node IN152 can detect a loss of continuity, which may arise from the failure of the link between node IN151 and node IN152, or failure of node IN151. Node IN152 replaces node IN151 to start to transmit the traffic into Ring 5. All the "Function Enabled" elements on node IN152 for the traffic from Ring1 to Ring 5 are changed to True. In order to avoid duplicated traffic, node IN152 informs node IN151 to stop transmitting the traffic into the downstream ring. All the "Function Enabled" elements on node IN151 for the traffic from Ring1 to Ring 5 are changed to False. The information message is sent all the way around the ring to make sure that node IN151 receives it successfully.

Interconnection Nodes Funtional Table

	Incomming Label	Function Enabled	Outgoing Label
IN151:	M_1_J1_IN151	~~True~~ False	M_1_IN151_IN512
	M_3_J1_IN512	~~True~~ False	M_3_IN151_IN512
IN152:	M_1_IN151_IN152	~~False~~ True	M_1_IN152_IN511
	M_3_IN151_IN152	~~False~~ True	M_3_IN152_IN511
IN511:	M_1_IN152_IN511	–	M_1_IN511_IN512
	M_3_IN152_IN511	–	M_3_IN511_IN512

Table 4.8: Contents of the INFTs under the interconnection failure.

4.4.3 Protection Switching of the SPME-based ROM-Wrapping Protection Scheme under the Interconnection Node and Link Failures

In this subsection, the protection switching for the interconnection link and node failures is further discussed. More details of the changes in the INFTs and the operation of the RLTC are explained based on examples.

Figure 4.11 illustrates the protection switching operations after node IN151 detects there is a loss of continuity. The failure may be caused by the failure of the link between node IN151 and node IN512, or failure of node IN512. In order to describe the protection switching more clearly, another multicast traffic M_3 is introduced, which also travels from Ring 1 to Ring 5. Because of the detected failure, node IN152 starts to transmit the traffic into Ring 5. Node IN151 changes M_1 and M_3's "Function Enabled" elements on the INFT to False to stop transmitting M_1 and M_3 from this link. Node IN152 changes M_1 and M_3's "Function Enabled" elements on the INFT to True to start the transmission. The changes of the INFTs are shown in Table 4.8. Since the traffic is entering Ring 5 from the protection interconnection link, node IN511 transmits it on the protection SPME configured for node IN511. The contents in the forwarding table used for the proposed Reverse Label Table Checking (RLTC) method (Section 3.5 of Chapter3) are listed in Table 4.9.

The operation of the protection switching triggered by node IN152 due to loss of continuity from IN151 is illustrated in Figure 4.12. Protection interconnection node IN152 receives traffic from the protection

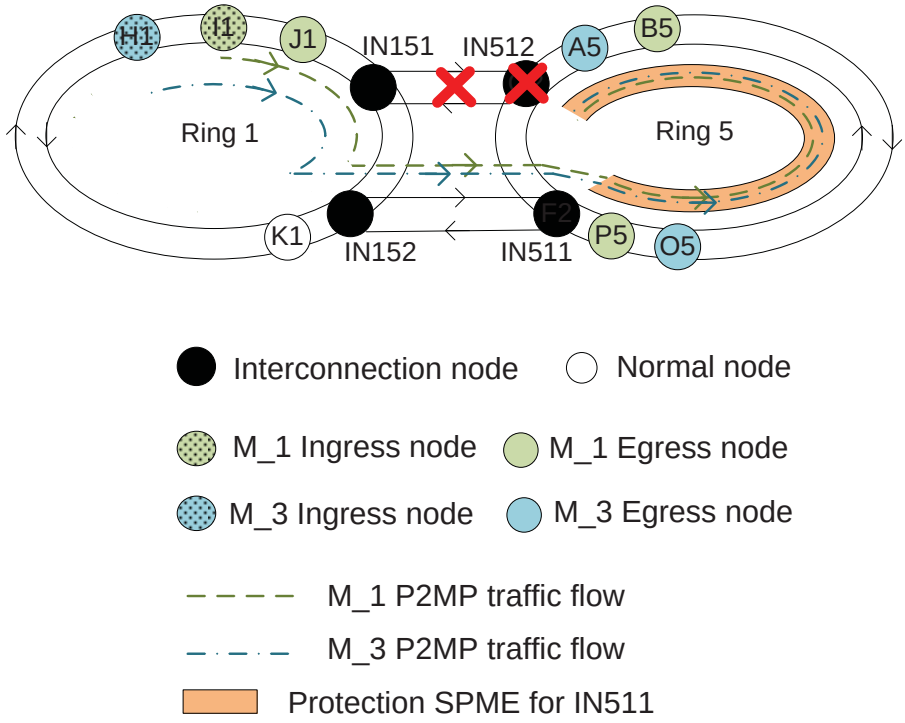


Figure 4.11: Protection switching of the SPME-based ROM-Wrapping protection scheme under the interconnection link failure and interconnection node failure on the downstream ring.

Forwarding Table

	Incomming Label	Outgoing Label	Operation Code
I1:	M_3_H1_I1	M_3_I1_J1	C
J1:	M_1_I1_J1	M_1_J1_IN151	D&C
	M_3_I1_J1	M_3_J1_IN151	C
IN151:	M_1_J1_IN151	M_1_IN151_IN152	D&C
	M_3_J1_IN151	M_3_IN151_IN152	D&C
IN152:	M_1_IN151_IN152	M_1_IN152_K1	D
	M_3_IN151_IN152	M_3_IN152_K1	D
K1:	M_1_IN152_K1	M_1_K1_L1	V
	M_3_IN152_K1	M_3_K1_L1	V
IN512:	M_1_IN511_IN512	M_1_IN512_A5	C
	M_3_IN511_IN512	M_3_IN512_A5	C
A5:	M_1_IN512_A5	M_1_A5_B5	C
	M_3_IN512_A5	M_3_A5_B5	D&C
B5:	M_1_A5_B5	M_1_B5_C5	D&C
	M_3_A5_B5	M_3_B5_C5	C
O5:	M_1_N5_O5	M_1_O5_P5	C
	M_3_N5_O5	M_3_O5_P5	D
P5:	M_1_O5_P5	M_1_P5_IN511	D
	M_3_O5_P5	M_3_P5_IN511	V
IN511:	M_1_P5_IN511	M_1_IN511_IN512	V
	M_3_P5_IN511	M_3_IN511_IN512	V

Table 4.9: Contents of the forwarding tables used for the interconnection failure.

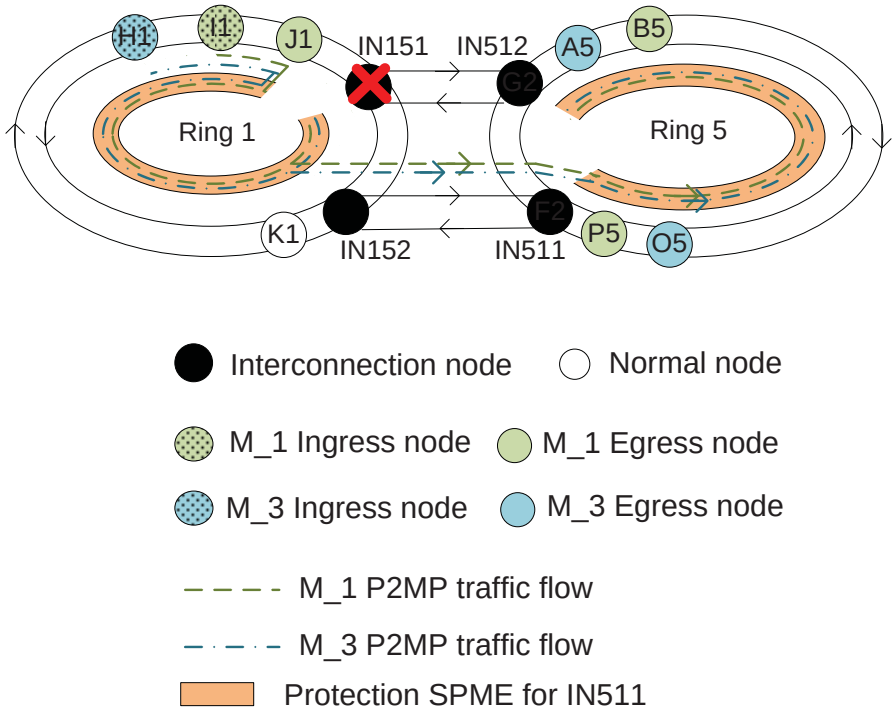


Figure 4.12: Protection switching of the SPME-based ROM-Wrapping protection scheme under the interconnection node failure on the upstream ring.

SPME on Ring 1 and starts to feed the traffic into Ring 5. The remaining of the protection procedures under this failure are the same as the one illustrated in Figure 4.11. The changes of the configurations are already listed in Table 4.8 and Table 4.9.

4.5 The Comparisons between the SPME-based Steering and the SPME-based ROM-Wrapping on Interconnected-Ring Networks

In this section, a comparison between the SPME-based Steering and the SPME-based ROM-Wrapping protection scheme for the interconnected-ring network is presented. All considered aspects are highly related to the network performance. Two multicast traffic, M_4 and M_5, are introduced as examples to show the differences between these two protection schemes.

4.5.1 Bandwidth used for Delivering Multicast Services under Failure Free Situation

The SPME-based ROM-Wrapping provides an LSP based multicast services, which means for each multicast request there is an independent configured LSP and no aggregation among any working LSPs. The traffic is sent exactly to each egress node. Figure 4.13 illustrates the traffic delivery of the multicast traffic M_4 and M_5 under the SPME-based ROM-Wrapping protection scheme. Due to applying the context labeling method to realize SPMEs, the SPME-based Steering also individually deals with each multicast traffic flow, even though all the flows are transmitted inside the SPME tunnels. The multicast traffic stops at the egress node at the farthest end which labeled by the context-identifying label. Figure 4.14 shows the traffic delivery of the multicast traffic M_4 and M_5 under the SPME-based Steering protection scheme. From Figure 4.13 and Figure 4.14 it is clear that the SPME-based ROM-Wrapping and the SPME-based Steering protection scheme require the same bandwidth for the working paths.

However, the SPME-based Steering works in the manner of 1+1 protection scheme. The multicast traffic is transmitted on both working and protection SPME tunnels. On the other hand, the SPME-based ROM-Wrapping adopts 1:1 protection scheme, and the traffic is only transmitted on the working LSPs under failure free situation. It is clear that under failure free situation, the networks using the SPME-based ROM-Wrapping protection scheme will have less traffic burden and less power

consumption than using the SPME-based Steering protection scheme. Furthermore, the reserved protection resource of the SPME-based ROM-Wrapping protection scheme can also be used for extra traffic transmission to enhance the efficiency of network resources [40].

Figure 4.13: Multicast traffic M_4 and M_5 under the SPME-based ROM-Wrapping protection scheme.

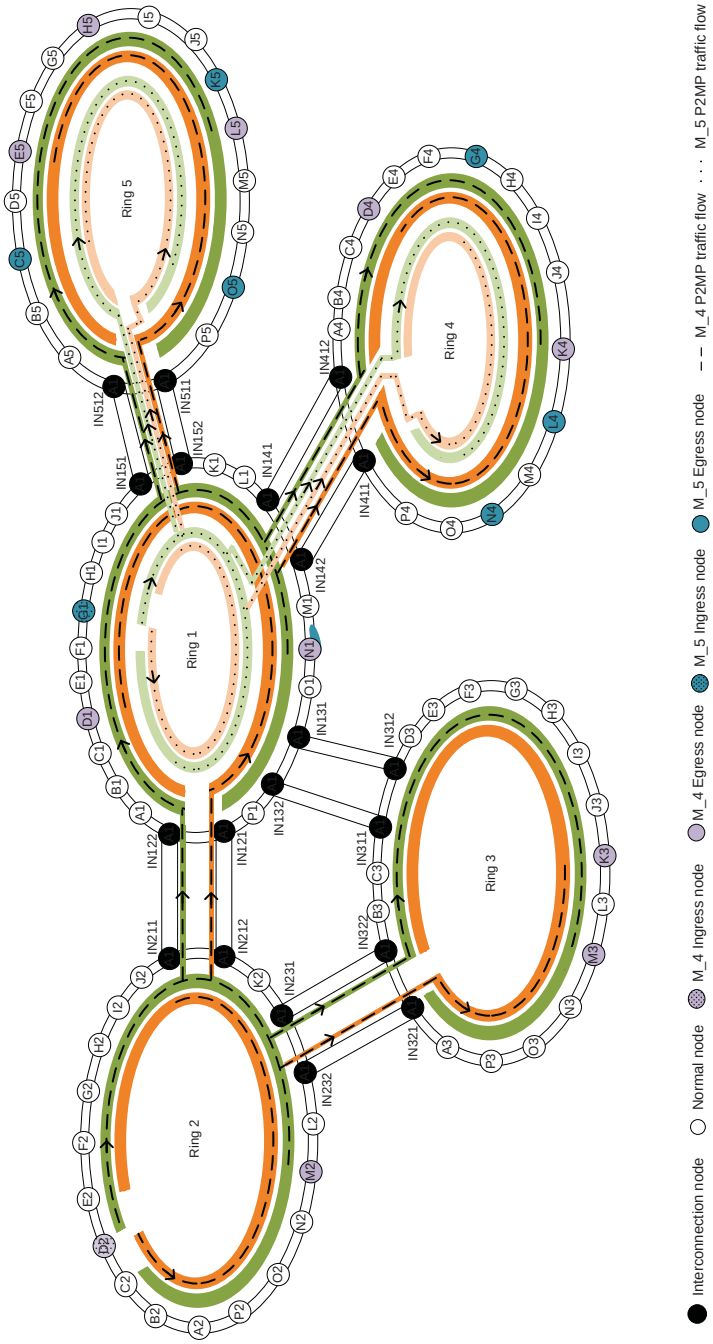


Figure 4.14: Multicast traffic M_4 and M_5 under the SPME-based Steering protection scheme.

4.5.2 Bandwidth used for Protection

The protection SPMEs of the SPME-based ROM-Wrapping are configured between any two adjacent nodes all the way around the local ring. For each node pair the configured protection SPME is independent. However, when a single error is considered on one of the ring at a time, the protection resources can be reserved in a Shared Explicit style [41], which means that the protection SPMEs can share the same resources. For example, it is assumed that the multicast traffic M_4 and M_5 require M units bandwidth on the link along the working LSP respectively. Then the bandwidth needed for protection is equal to 2M units on all the links in the counter-clockwise direction on local Ring 1, Ring 4 and Ring 5. The needed protection bandwidth is equal to M units on all the links in the counter-clockwise direction on Ring 2 and Ring 3. Figure 4.15 shows the protection switching procedure under a failure on Ring 1. The used protection SPME and required protection traffic on Ring 1 are illustrated.

The protection SPMEs of the SPME-based Steering cover all the nodes on the interconnected-ring network. However, due to using the context labeling method, for a multicast traffic, requiring M units bandwidth on the working LSP, the required bandwidth for protection are M units for each link on the protection path. Figure 4.16 illustrates the protection switching procedure under the same failure as shown in Figure 4.15. After comparison, it can be seen that on local ring the SPME-based Steering requires less protection bandwidth than the SPME-based ROM-Wrapping.

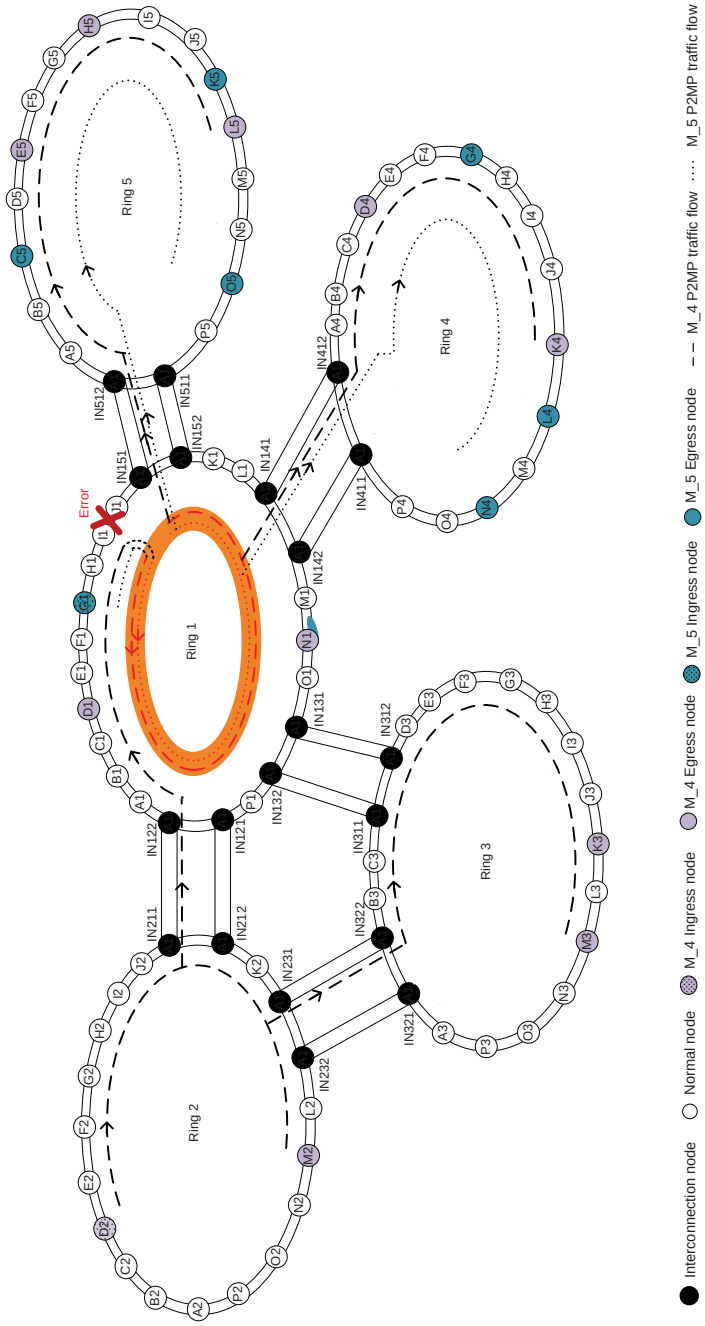


Figure 4.15: Protection switching of the SPME-based ROM-Wrapping protection scheme under a failure.

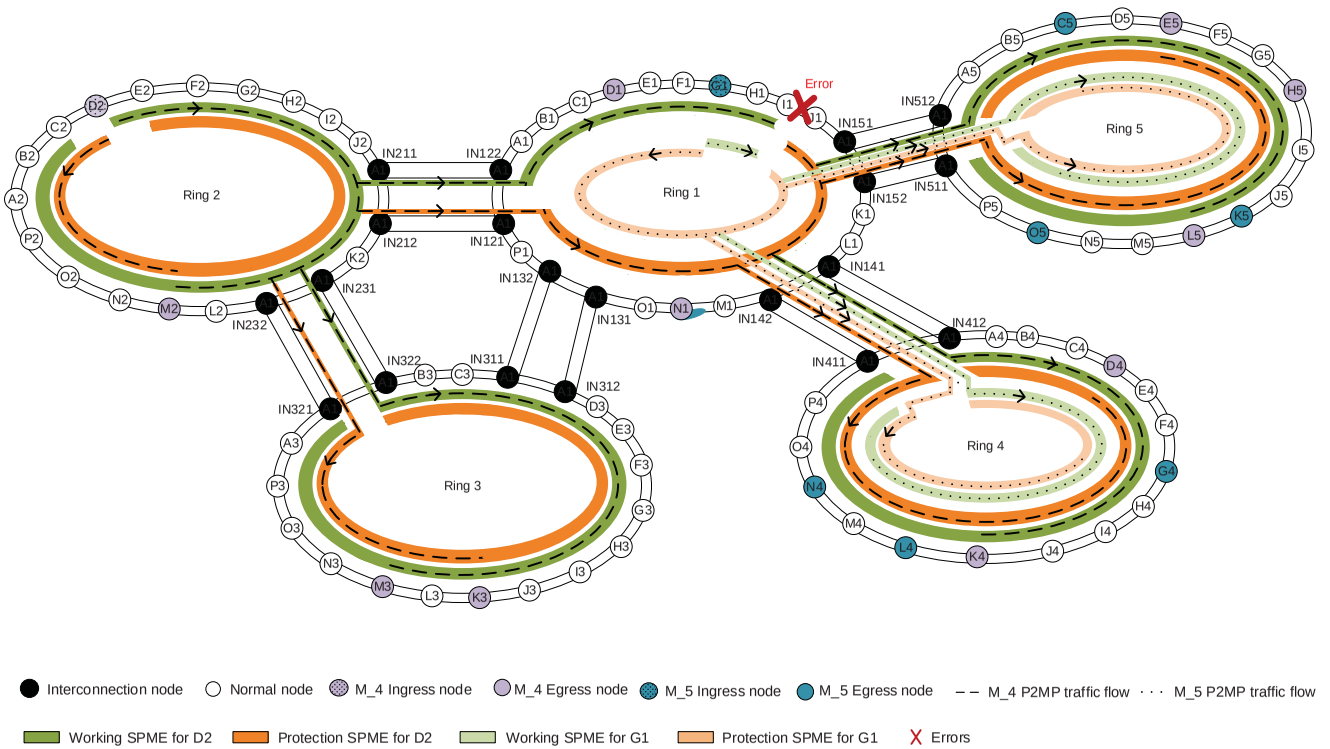


Figure 4.16: Protection switching of the SPME-based Steering protection scheme under a failure.

4.5.3 Number of the OAM Entities needed for Protection

In the SPME-based Steering protection scheme, the OAM functions are operated on both working and protection SPMEs. The egress nodes need to switch their selectors to read the traffic from the protection SPME when they stop receiving CC-V packets from the working SPME. For example, in Figure 4.16, egress node D1 of M_4 needs to monitor the CC-V packets from working SPME for D2 and protection SPME for D2. According to the design of the SPME-based Steering, on the source ring working and protection SPMEs are configured for each ingress node. This means that each egress node on the source ring needs to set up independent OAM entities for SPMEs configured for different ingress nodes. On a downstream ring, even all the working SPMEs (protection SPMEs) start from the same working interconnected node (protection interconnected node) on the upstream ring, they still need to be configured independently for different original ingress nodes in order to keep the consistency on different context label spaces. Thus each egress node on the downstream ring still needs to set up independent OAM entities for the SPMEs configured for different ingress nodes. For example, node N1 is the egress node both for the multicast traffic from ingress node D2 and ingress node G1. Therefore, there are separated OAM entities configured for the SPMEs for ingress D2 and the SPMEs for ingress G1.

In the SPME-based ROM-Wrapping protection scheme, the OAM functions are operated between adjacent nodes on all local rings. Besides interconnection nodes, normal nodes maintain two OAM entities at a time, one with the node on the left hand side and the other one with the node on the right hand side. If a node detects a failure occurring on the following link, it switches all the traffic onto the protection SPME no matter which ingress node the traffic is from. For instance, the OAM functions are operated between node I1 and node J1 under the SPME-based ROM-Wrapping protection scheme shown in Figure 4.15. When there is a failure between node I1 and node J1, node I1 switches all the traffic passing through node I1 to the protection SPME configured for node I1. Compared to the SPME-based Steering, the SPME-based ROM-Wrapping needs less number of OAM entities for the protection of the traffic on the entire interconnected-ring network. However, under the SPME-based ROM-Wrapping, the protection between the intercon-

nection nodes is the 1:1 protection scheme, thus there are extra OAM functions needed to switch the protection interconnection node on in case the working interconnection node is broken. But, for all the 1:1 protection schemes, such OAM functions between the protected entities pair cannot be avoided.

4.6 Summary

In this chapter, how to implement the SPME-based Steering protection scheme and the SPME-based ROM-Wrapping protection scheme on the MPLS-TP interconnected-ring network is discussed. The main focus is on introducing the implementation of the interconnection parts between the rings. Based on different protection schemes, the interconnection nodes apply different strategies to transmit the multicast traffic into different rings. The bandwidth required for delivering the multicast traffic is the same under both the SPME-based ROM-Wrapping and the SPME-based Steering protection scheme. In the SPME-based Steering protection scheme, if there is a failure on the working interconnection node or path and the traffic stops transmitting from the working SPME, then all the nodes on the downstream simply select the traffic from the protection SPME. In the SPME-based ROM-Wrapping protection scheme, if there is a failure on the interconnection node on the upstream ring or failure on the working interconnection path, the protection interconnection node on the upstream ring is switched on and starts to transmitting the traffic into the downstream ring along the protection SPME which is configured for the connected interconnection node on the downstream ring. If there is a failure detected by the node along the local ring, all the traffic passing through this node is switched onto the protection SPME configured for this node. On each local ring, the SPME-based Steering protection scheme requires less protection bandwidth than the SPME-based ROM-Wrapping protection scheme. The SPME-based Steering protection scheme employs the 1+1 protection method. Under failure free situation, it brings much more traffic burden and consumes more power than the SPME-based ROM-Wrapping protection scheme which adopts 1:1 protection method. Furthermore, the reserved protection bandwidth of the SPME-based ROM-Wrapping protection scheme can be used for extra traffic transmission to increase the

resource efficiency. Under the SPME-based Steering protection scheme, egress node needs to maintain independent OAM entities for the working and protection SPMEs configured for different ingress nodes, whereas under the SPME-based ROM-Wrapping protection scheme, each node (except interconnection nodes) only needs to maintain two OAM entities with its neighbors for all the traffic passing through this node. Compared to the SPME-based Steering protection scheme, the SPME-based ROM-Wrapping protection scheme needs fewer number of OAM entities for the protection of the traffic on the entire interconnected-ring network.

Chapter 5

Developing Aircraft Photonic Networks

5.1 Introduction

The rapid growth of the data traffic in terrestrial networks stimulated the continuous development of network and communication technologies. In particular, optical communication networks are well adapted to fulfill the ever increasing demand for speed and capacity. However it is hard to believe the fact that the on-board aircraft systems of the modern aircrafts, usually considered using the advanced technologies, are actually behind the state-of-the-art. To be more specific, the increasing demands, such as the aircraft safety, the in-flight entertainment system and the improved pilots' situational awareness, have not only resulted in a dramatic increase in aircraft cost, but also in the size and complexity of the existing aircraft systems. Furthermore, most of the on-board aircraft systems are separately implemented based on copper cable link networks. The increasing systems make the avionic system as opposed to the airframe has being the most expensive element of the aircraft, which is 60% of the typical aircraft "flyaway cost" by the end of the 1990's [19]. You would not even mention the problem of electromagnetic interference which arises from the growing complexity of aircraft on-board networks. Therefore the task to improve or redesign the current aircraft system networks to satisfy the future aircraft requirements has great meaning.

The Developing Aircraft Photonic Networks (DAPHNE) project starts from July 2010, which is a three-year European Commission research project. The primary objective of DAPHNE is to enable the full exploitation of key terrestrial optical networking technology, with its associated performance developments and advantages, in future European aircraft and systems. The project will adopt key components and network technologies from commercial markets and develop and validate future aircraft networks to take European aircraft systems capability well beyond current state-of-the-art and be suitable as a platform for future developments [19].

Optical fiber provides vast bandwidth compared to traditional copper cable, which can simply satisfies bandwidth requirements for aircraft system. The size and weight of fiber links have far more advantages over copper cable links. Electromagnetic interference immunity of fiber optics interconnect is another important reason to drive fiber system on aircraft. From security aspect, existing avionic system data can be monitored for malicious purposes. However for fiber networks it is impossible to eavesdrop or tap into signals. The fiber optics technology also provides the ability to segregate communication channels in a hierarchical way: fibers in different parts of the aircraft, ribbon fibers, wavelength segregation and time segregation. Avionic systems with different security levels (often referred to as Design Assurance Levels, DALs) can flexibly be arranged in channels with different segregation levels.

Although optics networks have numerous advantages compared to traditional copper wired networks, it still requires thorough research work to adapt terrestrial fiber optical network technologies into aircraft system networks, since lots of major differences exist between them. For example, the length of avionic system link is much shorter than that of terrestrial networks, and the longest one is usually about 100 m. Protocols designed for long distance optical networks should be revised before applying to avionic systems. Avionic systems require components to operate under considerably harsh environment conditions, which include huge operating temperature rage, shock and vibration, resistance to a range of contaminants and so on. The problem is to adapt and verify terrestrial network component to fulfill those environment requirements. In addition to environment requirements, terrestrial network components need to pass higher quality performance tests, such as smaller

wavelength drift over temperature, which are important for the safety reason.

It is believed that the objectives of the DAPHNE project can be attained through the research work in four aspects: Adapting optical network technologies for aircraft platforms; defining a modular infrastructure for aircraft fiber optical networks; developing existing photonic component technology for aircraft environments; disseminating project results to aircraft industry to ensure effective uptake.

The work presented in this thesis relates to designing the avionic transport networks. It involves two main parts which are introduced in this chapter and next chapter (Chapter 6) respectively. First part proposes a generic optical network design for future avionic systems. A three-layered network structure over a ring optical network topology is suggested, as it can provide full reconfiguration flexibility and support a wide range of avionic applications. Segregation can be made on different hierarchies according to system criticality and security requirements. Two network configurations are presented, focusing on how to support different network services by such a network. Finally, three redundancy scenarios are discussed and compared.

Second part of the work considers traffic fiber partition constraint when solving the multicast routing and wavelength assignment (MC-RWA) problem on WDM ring networks. A traffic fiber partition constraints aware - maximum loaded link perturbation (TFP-MLLP) scheme is proposed, aiming at increasing the efficiency of searching during simulated annealing process. Additionally, the proposed strategies can give out optimal fiber assignment solutions with different limitations on the amount of wavelengths that can be accommodated in one single fiber. All algorithms are evaluated on networks of different sizes with randomly generated traffic requests. Numerical results show the performance of the proposed strategies.

5.2 Developing A Generic Optical Avionic Network

Existing aircraft data networks are based on copper conductors. With the goal of improving the aircraft safety and the comfort of passengers and crews, many technological advances have been continuously

deployed in avionic data networks so that they can improve the capability and functionality of on-board systems. These networks have consequently become larger, heavier and more expensive. This trend is expected to continue [42]. The mass of a state-of-art coaxial cable for avionic systems is from 40 to 100 g/m. In contrast, a simplex optical aerospace cable has only maximum 5 g/m mass [43]. Transmitting the signal with one cable over the same distance, at least 10 fold weight reduction can be achieved by switching to optical fibres. Fibre optics ribbon cables can provide even more benefit: a 12 way optical ribbon cable weights 10 g/m [43]. Hence a 6 fold increased weight reduction can be achieved by replacing simplex optical cables with optical ribbon cables. Compared to copper cables, optical fibres also have advantages with respect to attenuation.

Furthermore, optical fibres provide much more capacity than copper cables. The Bit rate-distance product (BL), a commonly used figure for communication systems, is in the order of Mbit/s-km within coaxial cables, while in optical systems it is in the order of Gbit/s-km in multimode fibres (MMFs) [44] and it has exceeded Pbit/s-km in single mode fibres (SMFs) [45]. Fibre optics also offers other benefits, for instance with respect to electromagnetic compatibility.

The networks in present avionic systems are mainly deployed according to point-to-point and bus topologies [46]. Replacing copper cables with optical fibres as the transmission media in existing network structures might not provide much benefit since it will require massive optical-electrical-optical (OEO) conversion. Therefore, new avionic networks need to be designed to support the applications while reducing the number of permanent links.

A generic network for avionic systems is proposed, providing reliable services. The utilisation of the fibre switching and the wavelength division multiplexing (WDM) technique in optical communications provides flexibility of scaling, re-configuration and data isolation. The advantages of this generic network proposal are: the scalability to different network sizes; the adaptability to different capacity demands; the upgrade capability for future requirements.

The remaining part of this chapter is organised as follows. Section 5.2.1 describes the physical layer topology and the structure of the proposed generic network. It briefly covers the optical components that

can be used in this network. Two network configurations are described in Section 5.2.2, both of which are detailed with respects to the services they can potentially support. The redundancy scheme is also described in this section. Finally Section 5.2.3 summarizes this chapter.

5.2.1 The Proposed Avionic Network

Current on-board networks essentially support a single application satisfying a given design assurance level. Each application will therefore rely on its own network, resulting in a proliferation of distinct network physical infrastructures. Simply replacing copper cables on board with optical fibres will not solve the space, weight and energy consumption challenges, since all the electrical transceivers will also require or need to be replaced by optical components that are not necessarily lighter. Cost benefits may also be marginal since optical components are generally more expensive due to lower integration level compared to electronics.

In order to address these challenges, a layered transport network with ring structure to support conventional avionic systems is designed. Our generic network mainly focuses on supporting in-cabin systems, which normally accommodate a number of bandwidth demanding applications. The proposed network is characteristic in the sense that it provides a generic transport network through flexible configuration among different network layers and has a great ability to support a diversity of avionic systems. Reliability is another key feature of this network.

Figure 5.1 shows the topology of the physical links between nodes in the proposed optical avionic network. An optical ring structure was used in this network, connecting a head-end server node (HESN) with service nodes (SNs). The HESN provides connection between a central computer and SNs. It may be shared by many systems. Each system serves a specific purpose but may provide a number of applications, for example health monitoring system or in-flight entertainment (IFE) system. In such a system, information is distributed to and/or collected from many destinations or sources at different locations in the aeroplane. These destinations are called members in this chapter. For instance, sensors and video cameras are members of the health monitoring system, and seat groups (SGs) are members of the IFE system. The SNs scattered in the aeroplane are designed to connect the members of a system

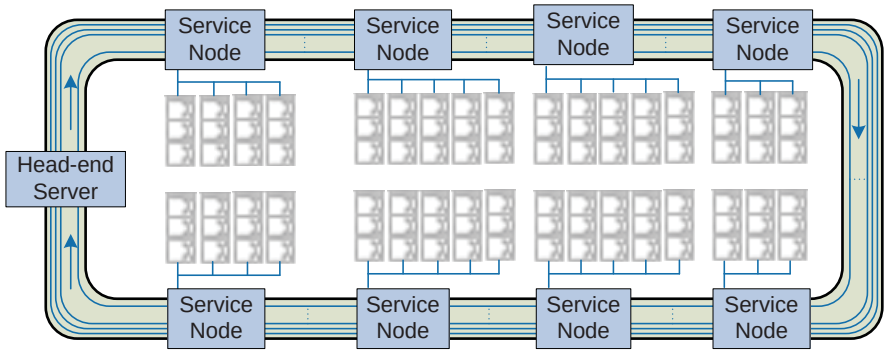


Figure 5.1: Physical topology of the proposed generic optical avionic network, illustrated here in the case of an in-flight entertainment system with some seat groups connected to service nodes.

together. However, members of different systems should not interfere with each other at the same SN.

Ring structures are often used in terrestrial networks. In order to realise point-to-point service, the traffic is delivered along the ring. For point-to-multipoint service, the "drop and continue" method is used. Such simplicity reduces the possibility of connection faults and avoids complicated connections among intermediate routers, which fits the safety concern of the flight system design. Furthermore, a ring structure naturally supports connection survivability. If the physical connection in one direction breaks, the traffic can be delivered in the other direction. The connection is therefore recovered.

In this generic network, several fibre ribbon cables are used to build the physical ring network. The clockwise direction ring is defined as service path, and the counter-clockwise direction ring is used for redundancy. The communication is designed as unidirectional. Some fibres in the ribbon serve the clockwise direction communication while the others serve the counter-clockwise direction.

In terrestrial deployments, layered networks are mostly used, since they provide point-to-point logic connections while in practice fewer cables are physically deployed. The proposed avionic network is designed as a layered network with hierarchical switching ability. Figure 5.2 de-

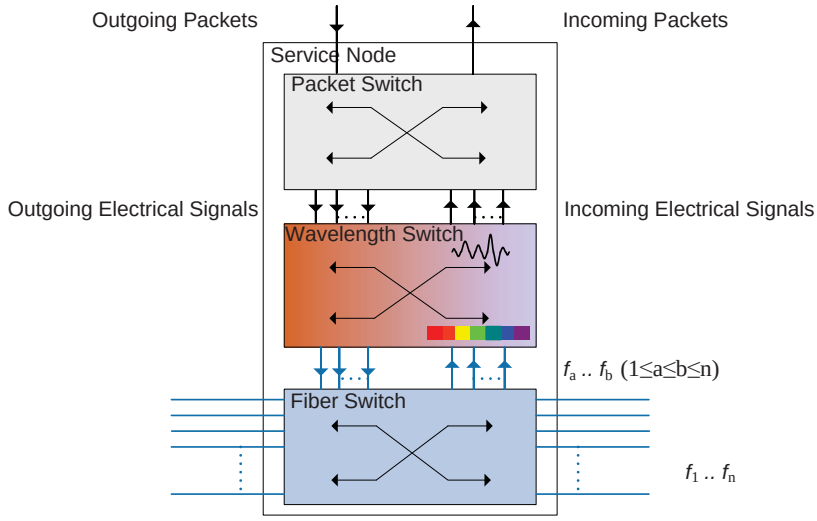


Figure 5.2: Layered optical network structure implemented at the service nodes.

picts the implementation of a SN. The three layers used in this implementation are fibre switching layer, wavelength switching layer and packet switching layer.

Thanks to the switching functions of these three layers, the proposed avionic network can provide a generic network with flexible configurations. According to criticality and security, the flight systems can be segregated at either fibre level or wavelength level, or just by using different logical paths, in another words, at the packet switching level. For bandwidth requirement concerns, the traffic from different flight systems can be delivered on the same wavelength or one wavelength can be dedicated to a specific system. For high bandwidth requirements, one or more fibres can be assigned to meet the demand of a particular system. For some systems, all three layers switching functions might not be necessary at the same time. Consequently, one or two of them can be skipped. For example, a sensor can be directly connected to the SN by a dedicated fibre to deliver analogue signals. By incorporating the packet switching layer, many flight system interfaces can be implemented and

many transport protocols can be supported by the network. The proposed avionic network can indeed provide a generic transport network and integrate diverse flight systems.

1. *Fibre switching layer*

   In terrestrial networks, the growing demand triggered the development of many technologies, for example WDM. WDM enables smooth capacity increase while avoiding the costly deployment of new fibres. In our generic network, not only is WDM used as an important physical layer technology, but a number of fibres are also employed in the form of optical ribbon cables, to provide a number of advantages:

   - First of all, considering cable packaging, applying a few more fibres in the ring network will not bring huge difference on the weight and the associated fuel consumption. However the total capacity is hence increased.
   - One or a few fibres can be dedicated to a specific application or a system. In this way, data transmission of, for instance, the flight control system will not share the same fibre as the entertainment system, which is less critical. Thus isolation can be achieved.
   - Reconfiguring is possible at the fibre layer.
   - Some fibres can be used for protection switching purpose.
   - Some fibres can be deployed in the physical ring as resources for future upgrading purpose, which makes upgrading of the network easier and cheaper.

2. *Wavelength switching layer*

   The purpose of the wavelength switching layer is, similarly to terrestrial networks, to fully exploit the capacity of the optical fibres deployed in the fibre switching layer. It can also serve as the mean of application/system segregation to realise different types of services, which are described in more details in Section 5.2.2. In this layer, optical add-drop multiplexers (OADMs) are used to drop the wavelengths containing the data that will be sent to the

packet switching layer, as well as to add data from the upper layer into the information streams.

3. *Packet switching layer*

   After the signals are converted from the optical to the electrical domain, the traffic can be switched based on packets. A pair of transmitter and receiver buffers is assigned to each supported flight system. Each flight system reads incoming packets from its own receiver buffer and puts outgoing packets into its transmitter buffer. The packet switching layer is illustrated in Figure 5.3 The idea of the proposed avionic network is to deliver and receive packets only to and from the system they belong to. How to deal with the packets, such as discard or accept, is the task of different connected flight systems. The supported flight system can be an internet service based on Ethernet protocol, an avionic system using the AFDX [47] protocol, or an avionic system with the CANBUS [46] protocol. There are two ways to distinguish packets from different flight systems. First, if one or several wavelengths are assigned to a specific flight system, then packets recovered from those wavelengths can be directly inserted into the corresponding buffer. Second, if a wavelength carries packets from various flight systems, a system identification label can be added in front of each packet before it is sent out. The packet switching layer will separate packets according to this label.

5.2.2 The Proposed Avionic Network Services

The following two sections illustrate two specific configurations of the proposed avionic networks, which support point-to-point and point-to-multipoint services. The point-to-point service and point-to-multipoint services are the basic standard services provided by transport networks. Many systems can directly use these two services to obtain connectivity among system members. The IFE system will be taken as an example. In general, two different types of IFE system philosophies exist regarding the location of the content for on demand video and audio. The data can be stored either on a central computer (server based content) or on in-seat displays (local content). In the first case, the video or audio will be delivered to particular seats according to demands. In such case

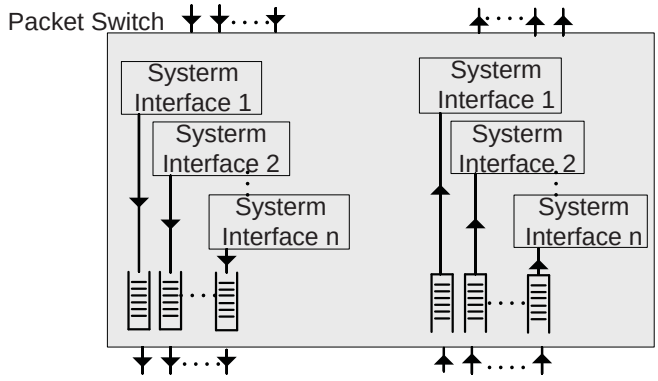


Figure 5.3: Internal structure of the packet switching layer of a service node.

the point-to-point service suits well for providing the connectivity and delivering the information to the right location. In the latter case, all the video and audio information will be delivered to and stored in each seat hard disk. Therefore, the point-to-multipoint service becomes a better choice for providing a simple and efficient connectivity solution.

For simplicity reasons, details of the fibre switching layer have been omitted in what follows. The fibre used for carrying the traffic can be assumed as switched and chosen.

The proposed avionic network with wavelength dedicated to node

This section introduces the first proposed network configuration, which is mainly designed for point-to-point services. Point-to-multipoint services are then implemented upon multiple point-to-point services. In order to illustrate how the services are delivered, an example of how to deliver Ethernet service to and from a group of SGs, is presented in Figure 5.4. To be more specific, the point-to-point service refers here to the connectivity provided from the HESN to a particular SN. The basic idea is that several dedicated wavelengths are assigned for a particular SN. From the HESN to the SN, those dedicated wavelengths carry downlink traffic, and they carry uplink traffic from the SN to the HESN. Figure 5.4

depicts the internal structure of SN K. Wavelengths λ_k to λ_{k+m} are assigned to this particular SN. Therefore only traffic carried by λ_k to λ_{k+m} is converted into electronic signals at SN K, while other wavelengths just bypass this node. Since $\lambda_k$to λ_{k+m} are assigned to SN K, traffic for all the systems connecting to SN K are carried by those wavelengths. In order to distinguish packets of different systems, a system identification label is added in front of each packet. SN K uses those system identification labels to separate packets and store them into the corresponding receiver buffers. Each SG connects to SN K through an Ethernet service interface, which reads packets from its own receiver buffer and delivers them to each SG. The Ethernet service interface can be implemented by an off-shelf Ethernet switch. If SGs want to send information back to the HESN, the packets will be put into the corresponding transmitter buffer through the Ethernet service interface. From all the transmitter buffers, the traffic is converted into optical signals and carried by λ_k to λ_{k+m} again. Eventually all the wavelengths are combined and delivered further.

To serve the systems that have multiple members requiring the same information, packets will be duplicated and separately sent by point-to-point services in order to emulate the point-to-multipoint service.

For more advanced configurations, each wavelength, which is dedicated to a node, can also be configured to carry the information for some specific systems or even only for one particular system. By doing this, the traffic from different systems can be segregated at the wavelength level.

The proposed avionic network with wavelength dedicated to system

This section introduces the second proposed network configuration mainly designed for point-to-multipoint services, with point-to-point service as a special case. Delivering an Ethernet service to and from several groups of SGs is used as an example. Figure 5.5 depicts the internal structure of one SN that connects to a group of SGs requiring the Ethernet service. The point-to-multipoint service provides a particular system with the connectivity between the HESN and some SNs, which have connected members of this system. For different systems, individual point-to-multipoint services can be configured. Two particular groups

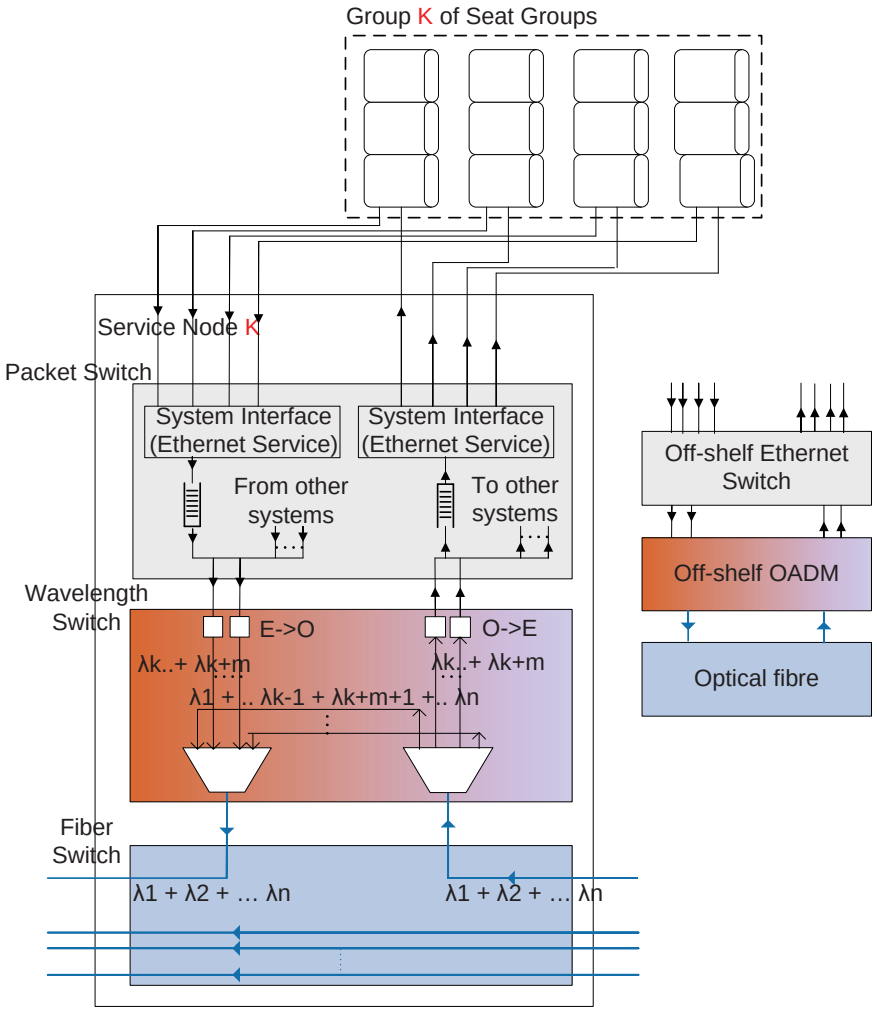


Figure 5.4: The proposed avionic network with λ dedicated to node.

of wavelengths are assigned for a specific system for downstream and upstream traffic. If a SN has a connected member belonging to this specific system, these two groups of wavelengths are configured to be received by this SN. Otherwise these two groups will bypass this SN. Figure 5.5 illustrates the implementation of a SN that is configured as such for an Ethernet service system. λ_1 to λ_n are assigned to downstream multicast traffic delivery and λ_{n+1} to λ_{n+m} are assigned to upstream traffic delivery. Since the traffic in λ_1 to λ_n is dedicated to the Ethernet service, packets carried by λ_1 to λ_n are not labelled with system identification labels and are directly inserted into the corresponding receiver buffer. Through the Ethernet service interface, packets can be sent to each SG from this receiver buffer. In order to provide more advanced configurations, each wavelength between λ_1 to λ_n can be configured to represent different channels of this system. Therefore, there can be a separate receiver buffer for each wavelength. The traffic carried by λ_{n+1} to λ_{n+m} contains upstream information from all the previously passed SNs that are related to the Ethernet Service system. In this SN, the upstream information of this SN will be combined with all the previous information and carried by λ_{n+1} to λ_{n+m} again.

When the system has only one member, then only one SN will be configured to receive the assigned wavelengths, which can be considered as a special case of implementation of a point-to-point service.

Network Redundancy

Due to safety concerns, providing redundancy in the network is one of the most important functions. In this chapter, three redundancy scenarios have been proposed and the illustrations are based on the first proposed network configuration (see Section 5.2.2 with wavelength dedicated to node). The first scenario provides complete physical redundancy. The network is completely duplicated by two sets of SNs and the opposite direction is used to carry redundant traffic. The structure is illustrated in Figure 5.6. The difference between this scenario and the other scenarios in this chapter is that the isolated physical redundancy does not introduce any logical function, such as traffic selection, into the SN, and it allows the network to survive from the complete failure of one SN. However each SG needs some level of intelligence to distinguish and select from duplicated packets.

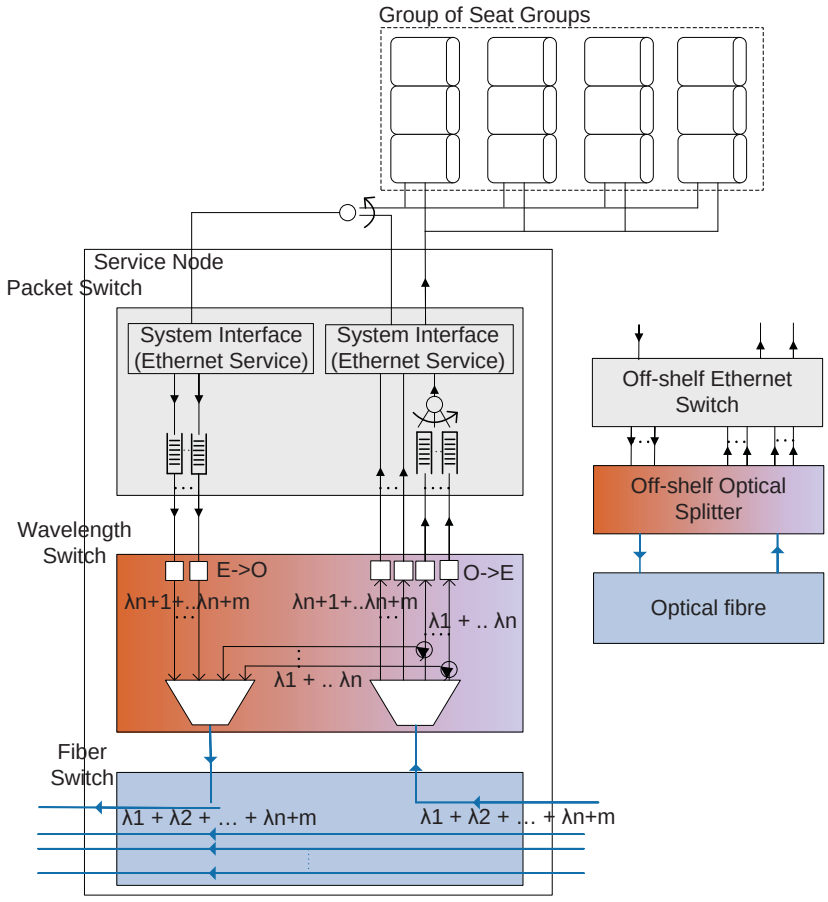


Figure 5.5: The proposed avionic network with λ dedicated to system.

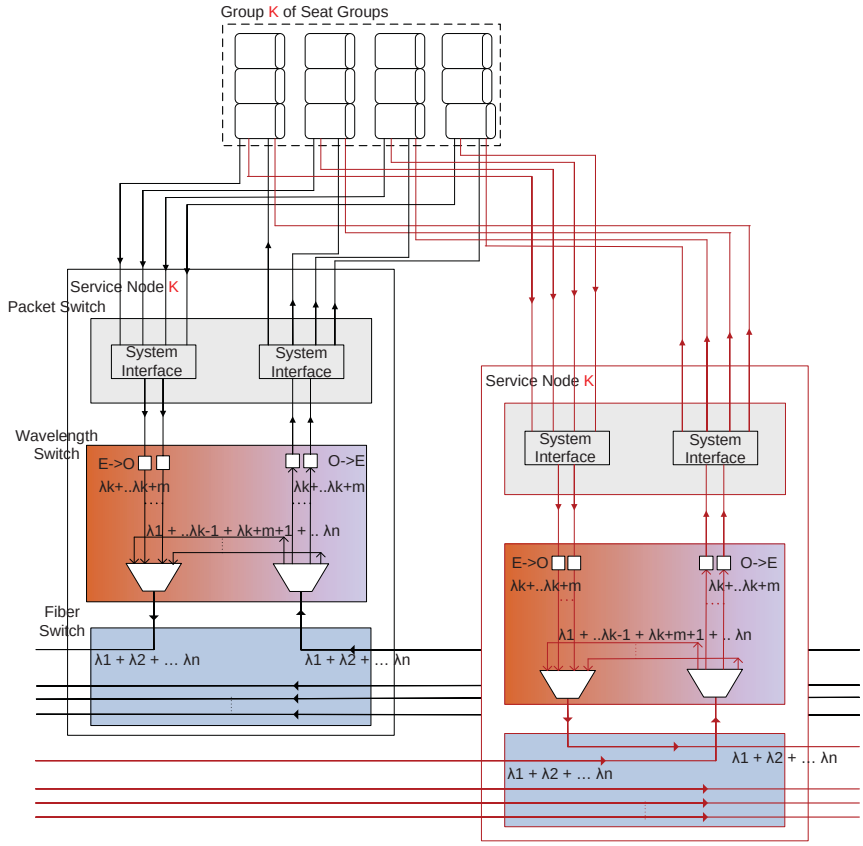


Figure 5.6: Redundancy scenario 1 of the proposed generic optical avionic network.

The second scenario implements the redundancy inside the same SN, which is shown in Figure 5.7. Each optical or electrical component is duplicated and located next to each other. This scenario is similar to scenario 1. However the redundancy is not physically isolated, as the components are in the same SN. It can save space on board, but the SN's failure caused by, for instance, physical damage may influence both working and redundant paths. The redundancy of the packet switching layer can be implemented in different ways. For example, the system interface does not need to be duplicated, if the supported system has its own redundancy traffic management, as in AFDX [47]. Both signals are sent to the unique interface of the supported system and the traffic is selected by the supported system. In case the supported system has no ability to deal with the duplicated traffic, the system interface has to be duplicated and the traffic will be selected by SGs, as shown in Figure 5.7.

In the third scenario shown in Fiugre 5.8, only electrical components have been duplicated. Active components are more likely to incur failures than passive components. Therefore duplicating only active components provides a reasonable low-cost solution. This scenario also introduces a traffic selector, which selects the traffic from the redundant signals. The selected traffic is sent to SGs or wavelength switching layer. The traffic selector relieves the selection task from each SG. However, in the mean time, additional components are introduced, and they also need to be protected.

The security level decreases from scenario 1 to scenario 3, as the system becomes cheaper. According to real requirements, network designers can choose the best solution among those three scenarios.

5.2.3 Summary

This chapter has proposed an optical avionic network, which is designed as a generic transport network that can support a wide range of systems. The proposed transport network has three switching layers and is based on a ring structure. The three switching layers are fibre switching layer, wavelength switching layer and packet switching layer. They provide different degrees of configuration and offer great flexibility to segregate and deploy diverse systems according to their security and bandwidth

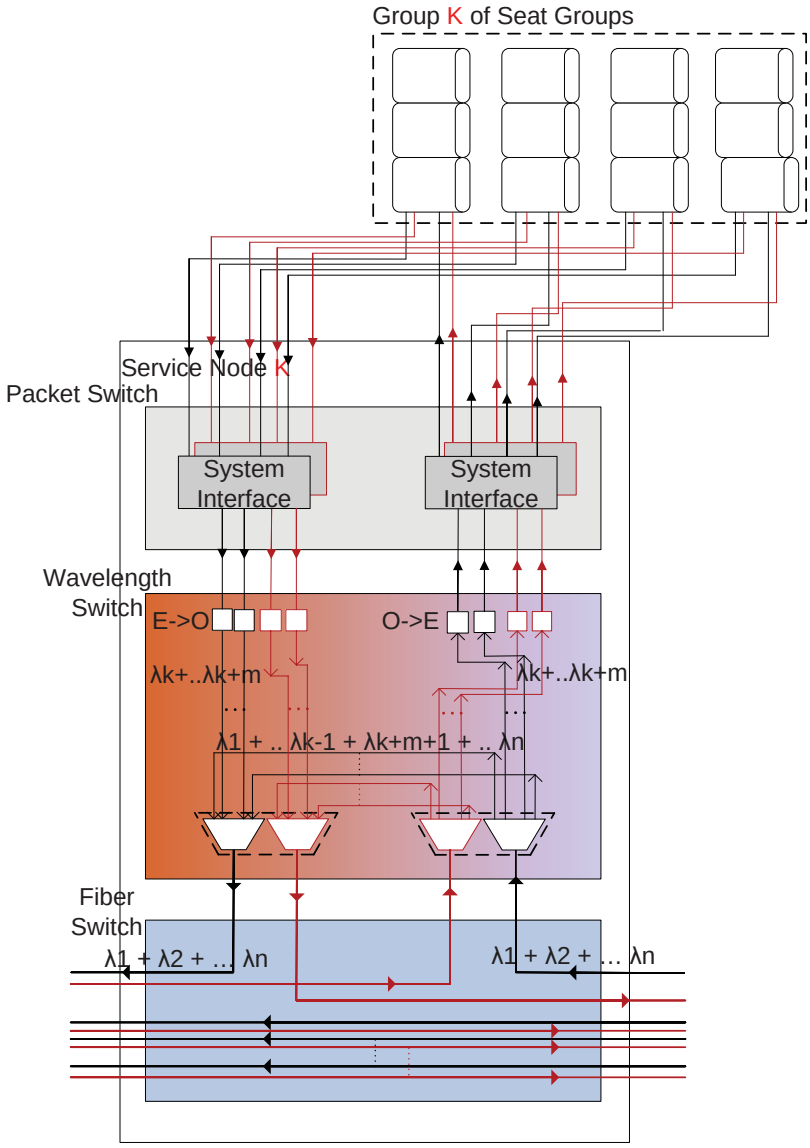


Figure 5.7: Redundancy scenario 2 of the proposed generic optical avionic network.

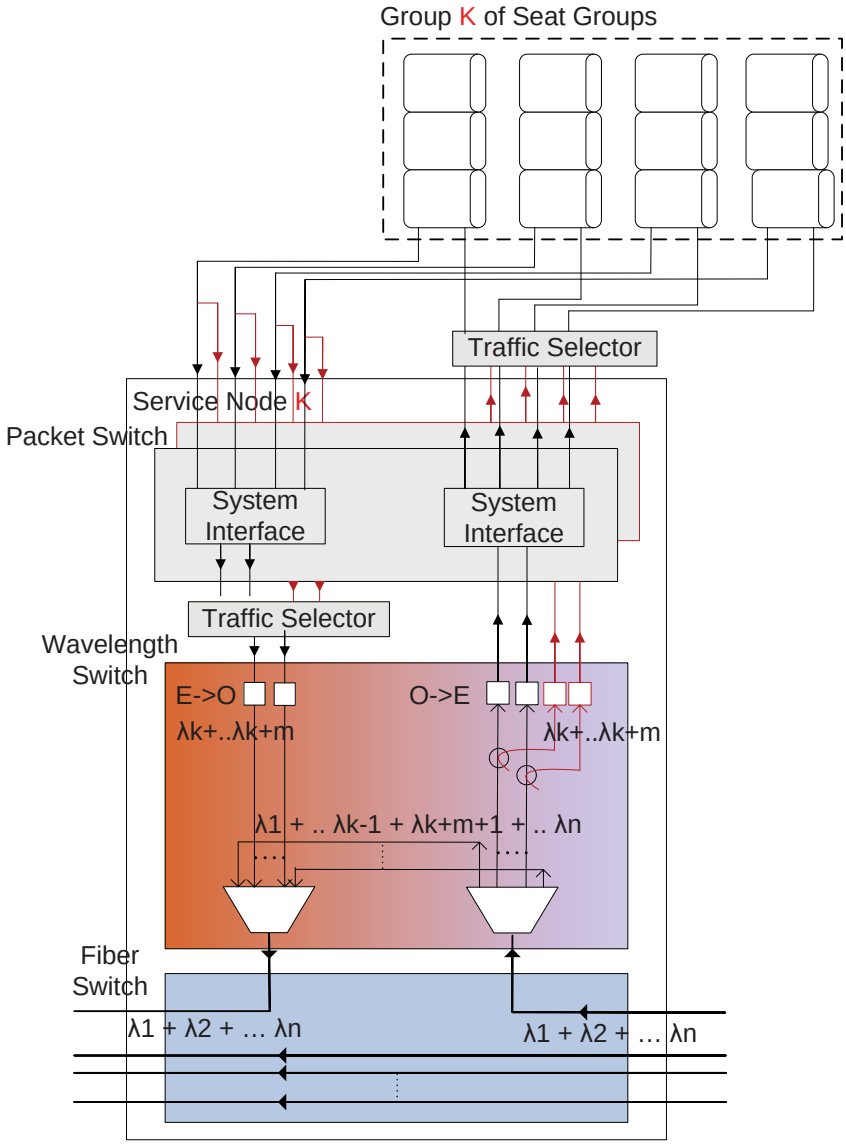


Figure 5.8: Redundancy scenario 3 of the proposed generic optical avionic network.

requirements. Furthermore, the ring supports redundancy schemes to ensure the reliability of the proposed avionic optical network. The point-to-point and point-to-multipoint services implemented on the proposed network configurations can be used as standard services to support specific systems or as examples of flexible network configurations.

Chapter 6

Network Optimization on Avionic WDM Ring Networks

6.1 Introduction

Wavelength division multiplexing (WDM) transmission technology provides large-bandwidth optical networks. However, compared to rapidly increasing bandwidth requirements, wavelengths and fibers still seem to be precious resources. Without wavelength conversion, the same wavelength should be assigned to a given traffic request all the way along the traffic route. The wavelength-continuity (WC) constraint regulates that the same wavelength cannot be assigned to any two traffic routes both of which share a given common link. Due to practical limitations on the amount of wavelengths available in one fiber, a wise strategy for route configuration, wavelength assignment and fiber assignment has a crucial impact on increasing the efficiency of WDM networks. In this chapter, a set of optimization solutions to deploy WDM ring networks on the aircraft for multicast services is provided.

Regarding multicast traffic requests, such optimization problem is often referred to as multicast routing and wavelength assignment (MC-RWA) problem. Based on different types of traffic requests, static or dynamic, the objectives of the MC-RWA problem are different. For

dynamic traffic type, the MC-RWA tries to assign each incoming traffic request a proper wavelength in order to decrease the traffic blocking probability. While for static traffic, which is determined in advance, the MC-RWA aims to reduce the total number of used wavelengths. Since most of the traffic requests from the avionic systems are predictable, only static traffic requests are considered in this chapter.

There are many research work preformed to investigate MC-RWA problem [48–50], where some [51–54] specially focus on WDM ring networks. The MC-RWA problem based on WDM ring network without wavelength conversion and with static traffic has been proven as NP-hard [51]. To solve the problem, some papers formulate the problem with integer programming and study the linear programming relaxation and then solve it with standard or proposed exact solutions [52]. Other literatures concentrated on the development of heuristic algorithms [50,51,53]. The Simulated Annealing (SA) approach is adopted in this work, which is one of the most widely used heuristic algorithms for solving optimal problems and also has been reported to give efficient performance on a wide range of standard optimal combination problems [55].

Most MC-RWA optimization solutions only consider WC constraints to decide whether or not a same wavelength can be assigned to different routes. However, in practical environment, for safety reasons, certain traffic requests are required to be physically separated from others in different fibers due to various system security levels or system importance diversities. On the aircraft, such security characteristics are controlled by the Design Assurance Level (DAL), a measurement to assess the impact of a failure condition within a system. In order to ensure the safe operation of an aircraft, all functions, systems and items should be developed according to different standardized DAL assigned to them [56]. It is also reasonable that systems with higher DAL level should be implemented and deployed separately from the one with lower DAL level, and systems with similar DAL level could be integrated in some ways.

With systems' different DAL levels, it is clear that the two traffic routes cannot be assigned the same wavelength if the two systems are required to be physically partitioned with each other, even though they may not share a common link. However, only considering the DALs when solving MC-RWA problems is not that difficult. As long as the MC-RWA problems are only solved among the systems with the DALs

which do not need to be partitioned, then the problems makes no difference. What is really interesting is that if system is declared need to be partitioned with some other systems independently, then how to solve the MC-RWA problems and how the total number of used wavelengths and fibers are affected.

Such special constraint is taken into account in this chapter when solving the MC-RWA problem and is referred to as traffic fiber partition (TFP) constraint. It is assumed that two wavelengths in different fibers are considered different even if they may have the same color. Thus all wavelengths in all fibers are assumed to be different. It is clear that if two routes are assigned with the same wavelength, then they will be delivered in the same fiber. Therefore, the TFP constraint is first examined in the wavelength assignment stage. Since two wavelengths may be assigned to routes which need to be partitioned into two fibers, these two wavelengths need to accommodate in different fibers, so that the second step must be solved in fiber assignment stage. The simulated annealing (SA) approach was adopted and a proposed perturbation mechanism was introduced to further solve the problems.

In order to keep generality it is assumed that the studied multicast traffic requests only locate on parts of the ring, and actual traffic routes will be calculated based on the locations of the source and destinations. It is further assumed that the ring is constructed by multiple bidirectional fibers and the same wavelength cannot be used on different directions on the same edge.

6.2 Problem Formulation

It is assumed a ring network $G(V, E)$ has n nodes. Let $V = \{0, 1, ...n-1\}$ be the set of nodes, indexed from 0 to $n-1$ in the clockwise direction, $E = \{(0,1), (1,2), ..., (n-2, n-1), (n-1, 0)\}$ be the set of undirected links, indexed from 0 to $n-1$. It is also assumed that there are r multicast groups $M_i = (s_i, D_i)$, where $D_i = \left\{ d_i^0, d_i^1, ..., d_i^{k_i} \right\}$,s_i is the source and $d_i^0, d_i^1, ..., d_i^{k_i}$ are the destinations, $i = 0, 1, ...r-1$,$k_i \in \{0, 1, ..., n-1\}$. It is further assumed that $d_i^0 < d_i^1 < ... < d_i^{k_i}$ and $s_i = d_i^l$, for some l, $0 \leq l \leq k_i$. The route of M_i is represented by R_i, $i = 0, 1, ..., r-1$.

There are three possible types of methods to route the multicast M_i, which are illustrated in Figure 6.1 [51].

1. A clockwise direction path from s_i to d_i^{l-1} ($d_i^{k_i}$ if $l = 0$)
2. A counter-clockwise direction path from s_i to d_i^{l+1} (d_i^0 if $l = k_i$)
3. Two paths from s_i: a clockwise direction path from s_i to $d_i^q, 0 \leq q \leq k_i, q \neq l$, and a counter-clockwise direction path from s_i to d_i^{q+1} (d_i^0 if $q = k_i$)

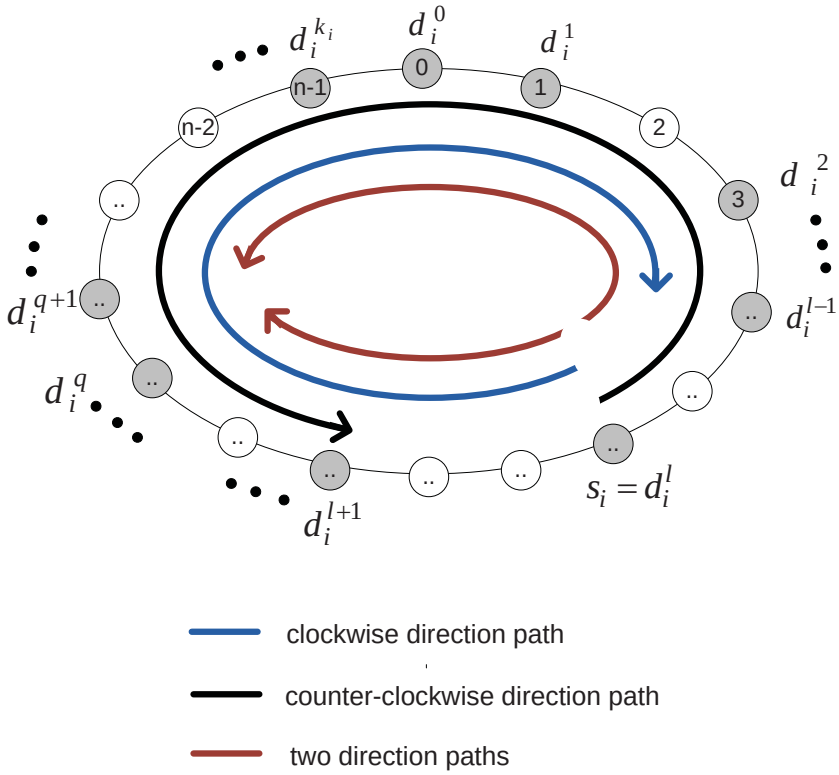


Figure 6.1: Three possible paths of a multicast route on the ring.

Since it is assumed that the same wavelength cannot be used on different directions on the same link, then only how routes locate along the ring will affect the number of used wavelengths, no matter how the traffic is delivered, in clockwise direction, counter-clockwise direction or both. Therefore, the route for multicast traffic, no matter which type of route methods are used, can be considered as a line which occupies a set of continuous links and lies along the ring. This line or route R_i can be represented by the pair of end points $(d_i^m, d_i^{m-1}), d_i^m, d_i^{m-1} \in D_i$, and if $d_i^m = d_i^0, d_i^{m-1} = d_i^{k_i}$. The d_i^m can be considered as the starting point of the line in clockwise direction, and d_i^{m-1} as the ending point.

The overlapping status of two given routes is recorded by a $r \times r$ matrix $O = (o_{ij})$, $i, j = 0, 1, ..., r-1$. $o_{ij} = o_{ji} = 1$, if R_i and R_j do not share links and $o_{ij} = o_{ji} = 0$, otherwise. Regarding a certain link e, $RE(e)$ represents the set of routes which pass link e. The requirements of the TFP constraint are stored in another $r \times r$ matrix $P = (p_{ij})$, $i, j = 0, 1, ..., r-1$ where $p_{ij} = p_{ji} = 0$ if M_i and M_j need to be segregated on different fibers and $p_{ij} = p_{ji} = 1$, otherwise. Regarding a specific traffic request M_i, $MP(M_i)$represents the set of traffic requests which need to be partitioned with M_i. Let $x_w = 1$, if wavelength $w \in \{0, 1, ..., W\}$ is assigned to any route in any fiber. It is assumed that each fiber can maximally accommodate MAX_W wavelengths. It should be noticed that two wavelengths on separated fibers will be identified by two different w even if they have the same frequency. $y_f = 1$ denotes that fiber $f \in \{0, 1, ..., F\}$ is used.

Based on the given groups of multicast traffic $\{M_i = (s_i, D_i)\}$ and taking the WC constraint O and the TFP constraint P into account, the optimization problem is to search path solution for multicast route M_i, wavelength assignment for each R_i and fiber assignment for each w, in order to minimize the number of used wavelengths and fibers.

$$\text{Objective: } \min \sum_{w \in W} x_w \text{ and } \min \sum_{f \in F} y_f$$

$$\sum_{w \in W} g_w^{R_i} = 1, i \in \{0, 1, ..., r-1\}, g_w^{R_i} \in \{0, 1\} \tag{6.1}$$

$$\sum_{R_i \in RE(e)} g_w^{R_i} \leq x_w, w \in W, e \in E, x_w \in \{0, 1\}, g_w^{R_i} \in \{0, 1\} \tag{6.2}$$

$$\sum_{f \in F} h_f^w = 1, w \in W \tag{6.3}$$

$$\sum_{w \in W} h_f^w \leq MAX\_W, f \in F \tag{6.4}$$

$$\begin{gathered} \sum_{M_j \in \{MP(M_i), M_i\}} t_f^{M_j} \geq 2, \\ i, j \in \{0, 1, ..., r-1\}, \\ f \in F, t_f^{M_j} \in \{0, 1\} \end{gathered} \tag{6.5}$$

$g_w^{R_i} = 1$ if R_i is assigned with wavelength w and $g_w^{R_i} = 0$, otherwise. Constraint 6.1 ensures each multicast route is assigned one and only one wavelength. Constraint 6.2 makes sure wavelength w is assigned to at most one route on each link. Constrain 6.3 dictates each wavelength accommodates in one and only one fiber, and maximally MAX_W wavelengths can be accommodated in one fiber which regulated by constraint 6.4. $t_f^{M_j} = 1$, if the wavelength assigned to M_j is accommodated in fiber f, or in other words, if traffic M_j is delivered in fiber f, $t_f^{M_j} = 0$ otherwise. Constraint 6.5 makes sure there are at least two fibers available to deliver certain traffic and the other traffic which has to be segregated from it.

6.3 Route Selection

The routes for multicast requests are selected based on the maximal-gap routing algorithm. The basic idea is to choose the routes with minimum number of used edges [51]. It is described previously that route R_i can be represented by the pair of the end points $(d_i^m, d_i^{m-1}), (if\ d_i^m = d_i^0, d_i^{m-1} = d_i^{k_i})$. Therefore the gap (empty space along the ring between two end points of the route) can be represented by $(d_i^{m-1}, d_i^m), (if\ d_i^{m-1} = d_i^{k_i}, d_i^m = d_i^0)$. d_i^{m-1} is considered as the staring point of the gap in clockwise direction, and d_i^m as the ending point. The length of a gap is denoted by $length(d_i^{m-1}, d_i^m)$. The route will be selected for $max\left\{length(d_i^{m-1}, d_i^m)\right\}$.

6.4 Wavelength Assignment with TFP constraints

The wavelength assignment problem can be solved by three methods. The first one is based on iteratively combining maximal matching sets. The second method is achieved by iteratively finding maximum cliques. The third method is to find minimum coloring. More details are listed below:

- **Method Based On Maximum Matching**

  If $G = (V, E)$ is a graph and $E_1 \subseteq E$, then E_1 is called a *matching* if E_1 is edge-independent. A matching in a graph is said to be *maximum* if it is maximum edge-independent [57]. The wavelength assignment problem can be transformed into solving maximal matching in a introduced graph $G_w(V, E)$, where each vertex corresponds to a route R_i and each edge represents that the two linked routes can be assigned the same wavelength. Every time after the maximum matching is found in $G_w(V, E)$, the two routes (eg. R_a, R_b) linked by the matching are grouped together and become a new vertex (R_{ab}) in a temp graph $G'_w(V, E)$. Only the edges in $G_w(V, E)$ which link a vertex with both R_a, R_b are remained in $G'_w(V, E)$. After grouping all the matching involved routes, then $G_w(V, E) = G'_w(V, E)$. The iteration will finish when there is no more matching can be found. The number of final vertices in $G_w(V, E)$ is the number of used wavelengths. The elements in each vertex are the routes that can share the same wavelength.

- **Method Based On Maximum Clique**

  In a graph $G = (V, E)$, a clique is a subset of vertices in which every two vertices in the subset are connected by an edge. The wavelength assignment problem can also be transformed into iteratively finding maximum clique in a introduced graph $G_w(V, E)$, where each vertex corresponds to a route R_i and each edge represents that the two linked routes can be assigned the same wavelength. A temporary graph $G'_w(V, E)$ is introduced to store the intermediate stage. At the initial stage, $G'_w(V, E)$ is set equal to $G_w(V, E)$. The result of maximum clique in $G'_w(V, E)$ is stored in a

result graph $G_c(V_c, E_c)$, in which V_c is the vertex set containing all the vertices of the found maximum clique. Based on the maximum clique result, $G'_w(V, E)$ is changed to delete all the vertices included in V_c and all the edges linking those vertices included in V_c. Then the changed $G'_w(V, E)$ is ready for next round of finding maximum clique. Within each iteration, the vertices of $G_c(V_c, E_c)$ are the routes, which will be assigned the same wavelength. The iteration ends when there is no vertex left in $G'_w(V, E)$. The Bron-Kerbosch algorithm is adopted to solve the maximum clique problem [58].

- **Method Based On Coloring**

  The idea of coloring the vertices of a graph, so that no two adjacent vertices have the same color [57], can also help to solve the wavelength assignment problem. A simple sequential coloring approach documented in [59,60] is adopted. The vertices of the graph G are colored in creasing order of vertex degree. Firstly, vertex with the least degree is colored with say, color 1. Then find the maximal independent set of vertices that are not adjacent to this vertex. All the vertices in the maximal independent set are colored with the same color, color 1. Secondly, all the colored vertices and its incident edges are removed from G. The degrees of remaining vertices are recalculated. The process is then repeated with color 2, then color 3, and so on, until all vertices are colored.

  Since the independent set corresponds to a clique in the complement graph, the maximal clique in the complement graph for certain vertex in non-increasing order of degrees can be calculated, instead of finding the maximal independent set for certain vertex in increasing order of degrees. By doing so, the way to construct the graph and most of the programs (developed for method based on clique) can be reused.

  The introduced graph $G_w(V, E)$ is same as the one used in the previous methods, where each vertex corresponds to a route R_i and each edge represents that the two linked routes can be assigned the same wavelength. A list of vertex degrees are maintained in $\{DEG_i, i = 0, 1, ..., r-1\}$. A temporary graph $G'_w(V, E)$ is introduced to store the intermediate stage. At the initial stage, $G'_w(V, E)$ is set equal to $G_w(V, E)$. The vertex v_m with maximal

($max\{DEG_i\}$) degree is selected. The maximal clique among all the vertices which connect to vertex v_m is calculated. The result is stored in a result graph $G_c(V_c, E_c)$. Vertex v_m and all the vertices of $G_c(V_c, E_c)$ are the routes, which will be assigned the same wavelength. After that, vertex v_m and the vertices of $G_c(V_c, E_c)$ and all its incident edges are removed from $G'_w(V, E)$. The degree list $\{DEG_i\}$ is recalculated. Then the changed $G'_w(V, E)$ is ready for next round of process. The iteration ends when there is no vertex left in $G'_w(V, E)$.

When constructing $G_w(V, E)$, the WC and TFP constraints are considered sequentially. Step 1 draws an edge between two vertexes (R_i, R_j), only when they are not sharing the same link of the ring ($o_{ij} = o_{ji} = 1$). In step 2, the TFP constraint is considered. If two traffic requests have to be partitioned into two fibers, then these two routes cannot be assigned to the same wavelength, no matter whether they overlap with each other or not. Therefore the established edges from step 1 will be examined, and any edge between two vertexes (R_i, R_j) will be deleted if ($p_{ij} = p_{ji} = 0$). In such a way, the possibility of combining these two routes is terminated. In other words, the two routes will not be assigned the same wavelength.

6.5 Fiber Assignment with the Limitation of Wavelengths in One Fiber

In the fiber assignment stage only the TFP constraint needs to be dealt with. A graph $G_f(V, E)$ is introduced where vertexes correspond to wavelength w. There is an edge between two vertices (w_i, w_j), only when all routes assigned w_i do not need to be partitioned with any route assigned w_j. Basically, the fiber assignment problem is similar to wavelength assignment problem. They all try to group items which can be grouped together and keep the number of the groups minimal. Therefore, the previous three methods which are used to solve the wavelength assignment problem to solve the fiber assignment problem are reused. However, in fiber assignment stage the limited number of wavelengths per fiber needs to be taken into account. The following context will

describes the extra processes to achieve this goal. For simplicity reason, all the similar details are eliminated.

- **Method Based On Maximum Matching**

  The idea of controlling the amount of the wavelengths in one fiber when applying the method based on maximum matching is very simple. Every time before trying to group two vertices which are linked by a matching, the number of the wavelengths which have already been grouped in these two vertices is checked. If the sum amount is not bigger than the maximum amount of the wavelengths which can be accommodated in one fiber, MAX_W, then these two vertices are allowed to be combined. Otherwise, the two vertices are left for the next round of calculation, trying to combine with some other vertices which have not involved so many wavelengths yet.

  However, there is a problem with this idea. The vertices are all combined in pairs, so that the amounts of contained wavelengths are more or less the same in each fiber. If two vertices fail to group together, then it is very likely that these two vertices also fail to group with others. Furthermore, when the size of each vertex grows nearly to the MAX_W, it is hard to combine them further. Then all the small spaces in each fiber will be wasted. Because of those reasons, the method based on maximum matching is not really used here to solve fiber assignment problem.

- **Method Based On Maximum Clique**

  During each iteration of finding the maximum clique, if a clique with size bigger than MAX_W is found, then choose any MAX_W of them to assign the same fiber, until there are fewer remains. Only the vertices which are assigned a fiber and its incident edges will be deleted from $G'_f(V, E)$.

- **Method Based On Coloring**

  After calculating the maximal clique among all the vertices which connect to vertex v_m, only random $MAX\_W - 1$ or fewer vertices are taken out of the found maximal clique. These $MAX\_W - 1$ or fewer vertices are stored in $G_c(V_c, E_c)$. Vertex v_m and only the

vertices in $G_c(V_c, E_c)$ are the wavelengths, which will be accommodated in the same fiber.

6.6 Heuristic Approach and TFP Constraint Aware Perturbation Mechanism

The simulated annealing (SA) approach is adopted as heuristic search algorithm to further solve the MC-RWA problems. The SA has been successfully applied in many optimization problems [51, 61, 62]. The strategies of the SA are derived from physical annealing process. The fundamental idea of the SA is that according to the calculations based on the cost function, some cost-increasing transitions are accepted to prevent the optimization process from being trapped in a local minimum which might deviates substantially from the global minimum [63]. The acceptance rate of uphill moves decreases gradually as the algorithm continues its execution, which controls by a control parameter, usually referred to as T, corresponding to temperature in the analogy with the physical annealing process. At the beginning the temperature is relatively high to accept uphill moves, so that the process avoids settling into a local minimum. When the SA process approaching to the end, the temperature becomes "frozen" and the process gets a more global optimization solution.

6.6.1 Initial Stage and Cost Function

The initial stage of route selection, wavelength assignment and fiber assignment are performed as described in Section 6.3, Section 6.4 and Section 6.5. Minimizing the number of used wavelengths ($\min \sum_{w \in W} x_w$) is chosen as the cost function for the comparison of each annealing round. The final number of the used fibers is calculated based on the optimized wavelength assignment result found by the SA.

6.6.2 Perturbation Mechanism

The basic principle of the perturbation mechanism is to find a proper route candidate and change the path of this route, aiming at decreas-

ing the cost. An innovative perturbation scheme is introduced in this section, which is called TFP constraints aware - maximum loaded link perturbation (TFP-MLL-P). In order to evaluate the efficiency of the proposed TFP-MLL-P, the TFP-MLL-P is compared with another perturbation scheme, Random Route perturbation (RR-P). The procedures of these two perturbation mechanisms are described as following:

- **Random Route Perturbation (RR-P)**

  During the process of the RR-P, route R_i is randomly selected from all the routes (i is randomly chosen from $\{0, 1, ...r-1\}$). The path (d_i^m, d_i^{m-1}) of the selected route R_i is randomly changed (m is randomly chosen from $\{0, 1, ..., k_i\}$).

- **TFP Constraints Aware - Maximum Loaded Link Perturbation (TFP-MLL-P)**

  The proposed TFP-MLL-P takes both WC and TFP constraints into account when choosing a candidate route and changing the path of the chosen route. The first step of the TFP-MLL-P is to consider the WC constraint. The maximum loaded link (MLL) on the networks is the one through which the most routes pass. It is identified following the equation $\max_{e \in E} \{RE(e)\}$. It is clear that the total number of used wavelengths is not less or at least equal to the number of wavelengths used on the MLL, $\sum_{w \in W} x_w \geq \max_{e \in E} \left\{ \sum_{w \in W} \sum_{R_i \in RE(e)} g_w^{R_i} \right\}$. It has great possibility that if the route passing through MLL could be changed to release MLL, then the number of wavelengths assigned on MLL will be reduced. Consequently the total number of used wavelengths might be decreased. Therefore, the first step of the TFP-MLL-P randomly chooses a route among the routes passing MLL, for example R_i, as a candidate route. Similar procedure is also used in other research work and proven to perform satisfactorily [49].

  In the second step, the TFP constraint is considered. It is worth noting that, as long as traffic request M_i is declared by TFP constraint, changing the path of M_i's route R_i will not help relieve

the TFP constraint on R_i and also will not decrease the number of assigned wavelengths due to trying to fulfill the TFP constraint. Although it might help loosen R_i's WC constraint bounded with some other routes which are not bounded with R_i by the TFP constraint, and consequently reduce the number of assigned wavelengths due to fulfill WC constraint. Therefore there is an assumption that if a candidate route R_i is involved in the TFP constraint, the more routes which R_i bounds with TFP constraints $(\bigcup_{j=0}^{r-1}\{R_j\}, \forall i \neq j, p_{ij} = p_{ji} = 0)$, the less impact it will have to reduce the total number of used wavelengths by changing the path of R_i. So a random number RND between $[0, 1]$ is generated. If $RND > \left(\sum_{j=0}^{r-1} R_j/r\right), \forall i \neq j, p_{ij} = p_{ji} = 0$, the path of R_i will be changed to release MLL, otherwise another route is chosen among the remaining routes passing MLL.

After reconfiguration of R_i, the number of used wavelengths and fibers could be re-calculated based on the algorithms of Section 6.4 and 6.5.

6.6.3 Cooling Schedule

Cooling schedule is referred to the way the temperature is controlled, which is based on the following parameters: the starting temperature (T_0), the final temperature (T_f), the steps of decreasing the temperature (M) and the way of decreasing the temperature. The core cooling schedule is implemented based on the strategies suggested by Lundy and Mees [64] and Connolly's Q8-7 [65], which have been widely used in many simulated annealing research work [51, 55, 62].

Based on the suggestion by Lundy and Mees, the temperature decreased following the equation 6.6. To be sure that this cooling scheme can be terminated in steps M, the β will be defined as equation 6.7.

$$T_{i+1} = \frac{T_i}{1 + \beta \times T_i}, \beta \leq T_0 \tag{6.6}$$

$$\beta = \frac{T_0 - T_f}{M \times T_0 \times T_f} \tag{6.7}$$

The starting and final temperature is defined according to equation 6.8 and 6.9, suggested by Connolly [65]. The smallest (δ_{min}) and the largest (δ_{max}) uphill steps are determined by 1000 times of random transitions.

$$T_0 = \delta_{min} + \frac{\delta_{max} - \delta_{min}}{10} \tag{6.8}$$

$$T_f = \delta_{min} \tag{6.9}$$

According to the experimental researches, Connolly stated that the more of a standard annealing search performed at, or closer to, the optimal temperature, the more successful that search became [65]. The Q8-7 algorithm is designed to try to maximize the proportion of the search performed near an (unknown) optimal temperature. The algorithm is listed as follows [65]:

1: **if** MXFAIL consecutive uphill steps are rejected **then**
2: the next uphill is accepted;
3: T is returned to TFOUND, the value at which the current best solution was found;
4: cooling is stopped by setting $\beta = 0$;
5: **end if**

The aim of this scheme is that $TFOUND$ will be a reliable indicator of the optimal temperature. $MXFAIL$ is an adjustable parameter, and is set to $M/2$, the same as [62] suggested.

A reheating schedule is further adopted, which arranges specific times of annealing trails. The appropriate initial and final temperatures for each round are calculated based on the range of objective costs it receives. It has been performed in many similar studies [55, 61, 62]. The whole simulated annealing procedure and the cooling schedule are listed in more details in the following algorithm:

1: Get SA parameters:
2: $T_0, T_f, M, Times\_of\_Trails$,
3: $Perturbation\_Mechanism$,
4: $Wavelength\_Fiber\_Assignment\_Method$;
5: Generate initial feasible solution (X);
6: $X_{orig} = X$;
7: Compute cost of initial solution ($C(X)$),

based on indicated $Wavelength\_Fiber\_Assignment\_Method$;
$MXFAIL = M/2$;
for $Times\_of\_Trails$ **do**
  $\beta = (T_0 - T_f)/(M \times T_0 \times T_f)$;
  $T = T_o$;
  $T_{best} = T_o$;
  $M_{index} = M$;
  $fail\_times = 0$;
  while $T > T_f$ && $M_{index} > 0$ **do**
    $s =$ perform route perturbation,
    based on indicated $Perturbation\_Mechanism$;
    $X' =$apply s to X;
    $\Delta C = C(X') - C(X)$;
    $p = unif\_rand(0, 1)$;
    if $(\Delta C > 0)$ && $(p > e^{-\Delta C/T})$ **then**
      $fail\_times = fail\_times + 1$;
      if $fail\_times > MXFAIL$ **then**
        $T_{min} = T$;
        $\beta = 0$;
        $T = T_{best}$;
      end if
    else
      $X = X'$;
      $fail\_times = 0$;
    end if
    if $C(X) < C_{best}$ **then**
      $C_{best} = C(X)$;
      $T_{best} = T$;
    end if
    $T = T/(1 + \beta T)$;
    $M_{index} - -$;
  end while
  $T_0 = (T_0 + T_{best})/2$;
  if $\beta = 0$ **then**
    $T_f = (T_f + T_{min})/2$;
  else
    $T_f = T_f/2$;

45: **end if**
46: $X = X_{orig}$;
47: **end for**

6.7 Numerical Results

In order to evaluate the proposed heuristic strategies, all those strategies were implemented in C++ and tested based on randomly generated traffic requests on ring networks with different sizes and traffic loads. The ring network is defined by parameter N, indicating the number of nodes along the ring. The amount of traffic requests is configured by a parameter F.

For each traffic request, the source node is randomly selected among N nodes. The size range of the destination set of each traffic request is controlled by a percentage parameter P and the pool size of the candidate destinations (DesPool). The exact size of each destination set is randomly chosen between $[1, P \times size\_of\_DesPool]$. Each destination is randomly selected from the DesPool. The DesPool is calculated depended on different traffic request scenarios. There are four types of traffic request scenarios defined to emulate different types of traffic requests:

- The first type is called random traffic, denoted by M_{random}. For each traffic request, the DesPool contains all the nodes along the ring except source node. For this type of the traffic, P can be used to control the scale of the number of the destinations, but where each destination locates is randomly decided. Therefore, the scale of the lengths of all the traffic routes cannot be predicted.

- The second traffic request scenario is called ring division traffic, denoted by $M_{division}$. The ring is divided into a specific number of parts, and this specific number is indicated by a parameter D. Regarding to each traffic request, the DesPool consists of the nodes (except source node) in the specific part where the source node locates. This traffic request scenario emulates the traffic which occurs locally on a part of the ring.

- The third traffic request scenario is named as span traffic, denoted

by M_{span}. The span, S, defines the maximum length from the source to the last destination on the far end along the ring. The source node is randomly located along the ring. A random number between $[0, S-1]$ is chosen to indicate how many nodes, on the left side of the source node along the ring in the clockwise direction, are in the DesPool. Then proper number of nodes on the right side of the source node are put into the pool, making the size of the DesPool equal to $S-1$. Based on this DesPool, the destination set of the traffic request is generated. This type of traffic request emulates the traffic with different span scales.

- The fourth traffic request scenario is introduced based on the M_{span}, which is called M_{span_partly}. The generation rule for the source and the destinations are the same as the rule of the M_{span}. Only in the M_{span_partly} scenario, a part of the traffic requests are declared need to be partitioned with some other requests. The details will be given in the next paragraph.

The number of how many pairs of traffic requests are bounded by TFP constraints is regulated by a percentage parameter C. A full connection among all the traffic requests will be $F \times (F-1)/2$. In the first three traffic request scenarios, the exact number of pairs of TFP bounded traffic routes is calculated as $C \times F \times (F-1)/2$. The TFP bounded traffic request pair is randomly generated from all the traffic requests. In the fourth scenario, M_{span_partly}, another control parameter Q is defined to regular how many percentages of traffic requests are initially declared need to be partitioned with others. Firstly, $Q \times F$ traffic requests are randomly selected. Secondly, for each selected traffic request, $C \times (F-1)$ traffic requests are randomly selected from all the other traffic requests to be bounded by the TFP constraint with this traffic request. The exact number of pairs of TFP bounded traffic requests is calculated as $Q \times F \times C \times (F-1)$. It needs to be careful that $Q \times F \times C \times (F-1)$ cannot be bigger than $F \times (F-1)/2$.

In order to introduce the setup of the simulation tests, the used symbols are summarized in the following Table 6.1.

Symbol	Meaning	Values
G	traffic request scenarios	$1 = M_{random}$ $2 = M_{division}$ $3 = M_{span}$ $4 = M_{span\_partly}$
N	number of nodes	eg. 10,20,30,...
F	number of traffic requests	eg. 10,20,...
P	control of the size of the destination set	%
Q	control of initially declared TFP bounded requests	%
C	control of pairs of TFP bounded traffic requests	%
D	number of divisions	eg. 2,4,...
S	maximal route span	eg. 5,10,...
M	wavelength and fiber assignment method	1=maximum matching 2=maxium clique 3=coloring
R	perturbation mechanism	1=RR-P 2=TFP-MLL-P
T	steps per annealing trail	eg. 500,1000,...
A	times of annealing trails	eg. 1,2,3,...

Table 6.1: Parameter table.

G	N	F	P	Q	C	D	S	M	R	T	A
				—		—			1	1000	3

∗The"—"means the parameter is not relavent to this round of the simulation.

Table 6.2: Parameter configuration for comparing different wavelength and fiber assignment mehtods.

6.7.1 The Comparison among Different Wavelength and Fiber Assignment Methods

In this section a comparison among three wavelength and fiber assignment methods is discussed: the method based on maximum matching, the method based on maximum clique and the method based on coloring. All of these three methods have been used in many other similar research work [51,60,66]. They are evaluated in here and an appropriate method is selected for further simulation studies. Some random traffic request cases of the M_{random} and the M_{span} were generated and tested on the networks with different network sizes and traffic loads. For each test case, the wavelength assignment and fiber assignment were performed by these three different methods independently. Some fixed configurations of the parameters are listed in Table 6.2.

These three different methods are tested on the ring networks with different sizes (N = 10, 20, 30), different percentages of TFP bounded requests (C= 30%, 60%) and different amount of traffic requests. Figure 6.2 and Figure 6.3 show the results of calculated minimum amount of used wavelengths and fibers under the M_{random} traffic scenario. Under this type of traffic scenario, these three methods give more or less the same performance.

Figure 6.4 and Figure 6.5 show the results of calculated minimum amount of used wavelengths and fibers under the M_{span} traffic scenario. It can be seen that in almost all the cases, the methods based on maximum clique and coloring outperform the method based on the maximum matching. The value of the span(S) of the M_{span} was set relative short in this test, which actually gave more chance for routes to be grouped together than the traffic generated under the M_{random}. The worse performance of the method based on maximum matching is resulted from the way of trying to group routes (wavelengths) into wavelength (fiber)

in pairs. The sizes of grouped route sets (grouped wavelength sets) are growing at the same time, which makes it hard to further group between sets in the late stage of grouping. The other two methods almost show the same performance in all the test cases. It is because the algorithm adopted for coloring method is derived from the algorithm for clique method and only has a little adaption. There are a lots of research work focusing on investigating the algorithms for coloring method. However they are out of the scope of this thesis. From the simulation results it is found that, with the adopted algorithms, the method based on maximum clique perform better in more cases than the method based on coloring. Therefore, the method based on maximum clique is chosen as the wavelength and fiber assignment method for the later simulations.

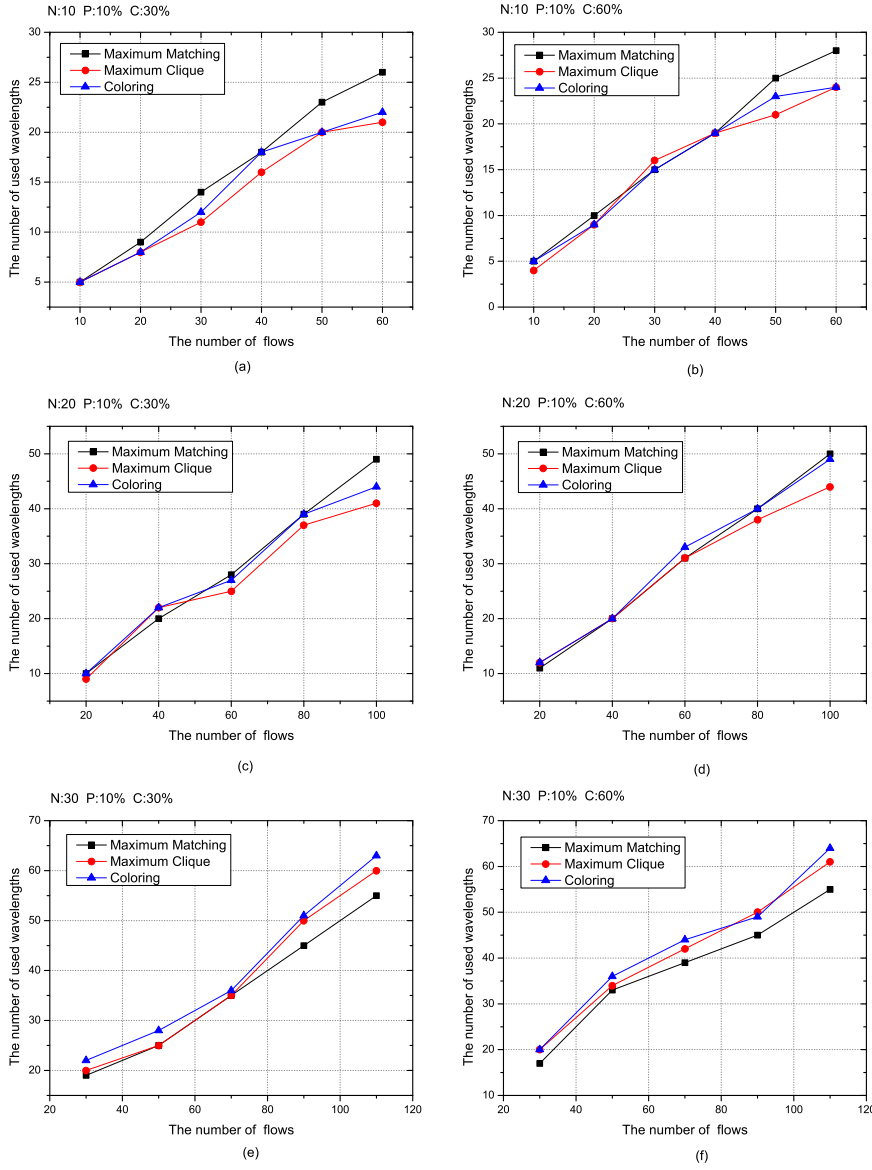


Figure 6.2: The comparison of calculated wavelengths among different wavelength and fiber assignment methods under M_{random} traffic scenario.

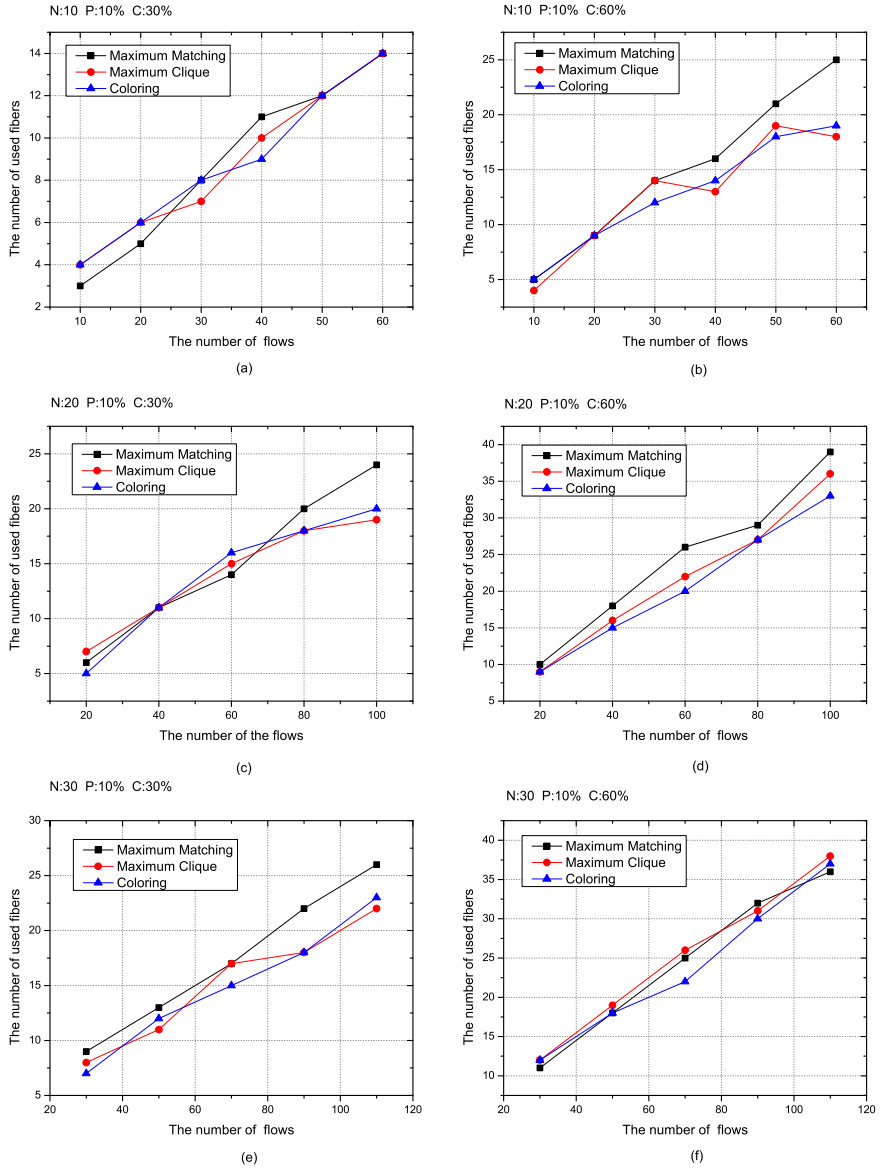


Figure 6.3: The comparison of calculated fibers among different wavelength and fiber assignment methods under M_{random} traffic scenario.

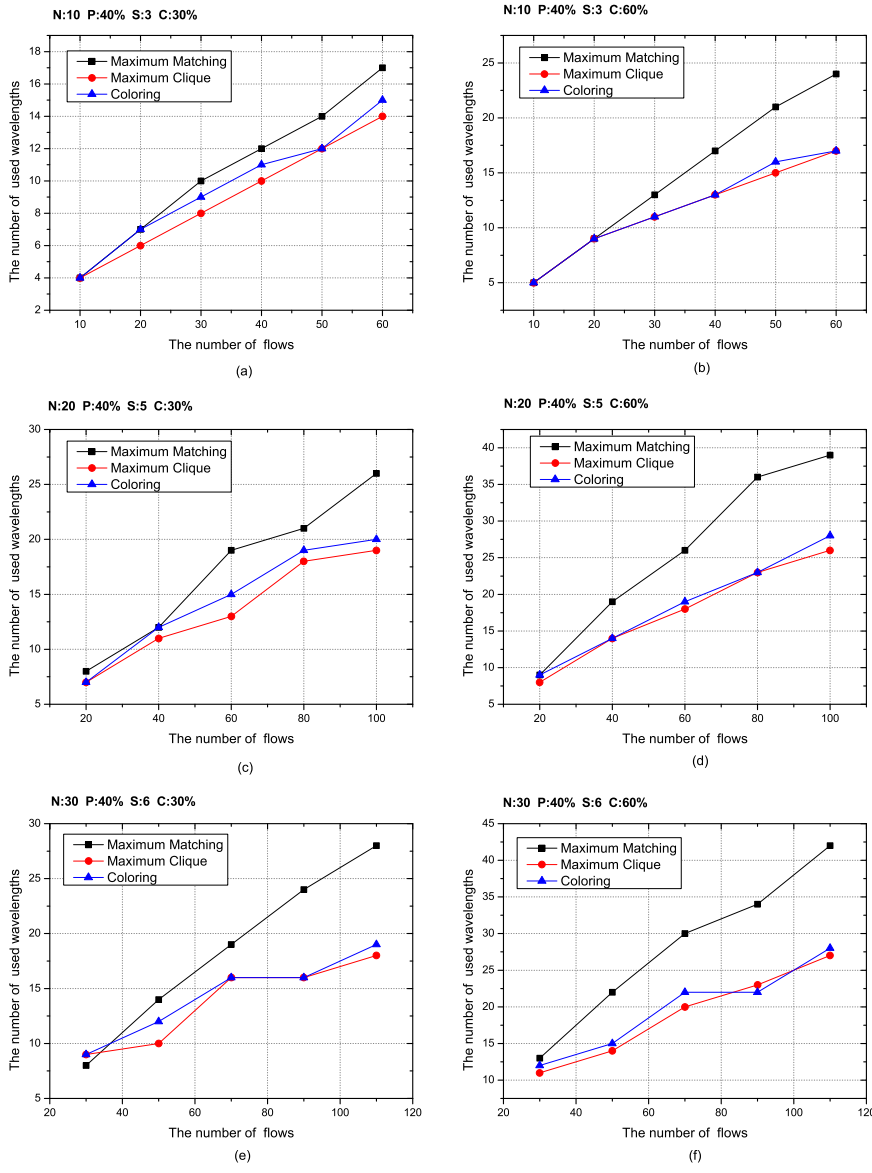


Figure 6.4: The comparison of calculated wavelengths among different wavelength and fiber assignment methods under M_{span} traffic scenario.

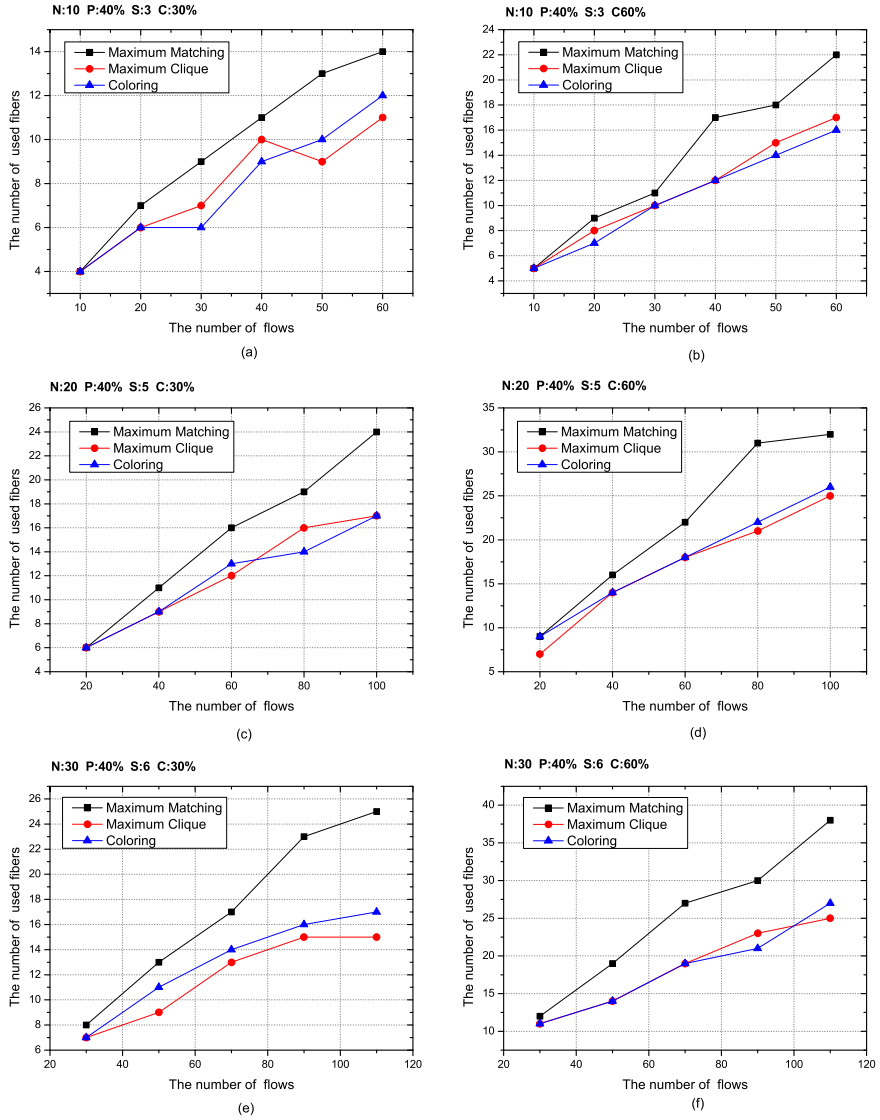


Figure 6.5: The comparison of calculated fibers among different wavelength and fiber assignment methods under M_{span} traffic scenario.

G	N	F	P	Q	C	D	S	M	R	T	A
								2		1000	3

Table 6.3: Parameter configuration for comparing different perturbation mechanisms.

6.7.2 The Comparison between Different Perturbation Mechanisms

In this section, the proposed TFP-MLL-P perturbation mechanism is compared with the RR-P perturbation mechanism. The simulations were executed on all traffic scenarios with different network sizes, different traffic loads, different sizes of the destination set and different percentages of TFP constraints. In each round of test, the two perturbation mechanisms were performed based on the same test case. Since the number of used wavelengths is used as the cost in each step of the annealing trail, only the wavelength consumption is promised to be the best result from the simulations, not the fiber consumption. Therefore these two perturbation mechanisms are compared based on the found minimum amount of used wavelengths. An Optimization Percentage is introduced to evaluate the efficiency of the perturbation mechanism, which is reflected by the ratio between the found minimum amount of used wavelengths by simulated annealing and the amount of the used wavelengths calculated by the initial state. Based on the algorithm introduced in Section 6.6.3, the Optimization Percentage is calculated as $C_{best}/C(X_{orig})$. All the results of the Optimization Percentages shown in figures are the average results of 5 random cases. The fixed parameters are shown in Table 6.3.

Figure 6.6 and Figure 6.7 give the results of the Optimization Percentages based on the test cases generated by the M_{random} scenario with different network sizes (N = 10, 20, 30), different densities of destinations (P = 10%, 40%) and different percentages of the TFP constraints (C = 30% , 60%).

Figure 6.8 and Figure 6.9 give the results of the Optimization Percentages based on the test cases generated by the $M_{division}$ scenario with different network sizes (N = 10, 20, 30), different amounts of divisions on the ring (D = {2 or 4}, {3 or 5}, {4 or 6}) and different percentages of the TFP constraints (C = 30%, 60%).

In Figure 6.10 and Figure 6.11, it is shown the results of the Optimization Percentages based on the test cases generated by the M_{span} scenario with different network sizes (N = 10, 20, 30), different maximum span values (S = {3 or 5}, {4 or 6}, {5 or 7}) and different percentages of the TFP constraints (C = 30% , 60%).

Figure 6.12 shows the results of the Optimization Percentages based on the test cases generated by the M_{span_partly} scenario. The Q was set to 30%. The S was set to 3, 4 and 5 for the ring networks with N equals to 10, 20 and 30.

Based on more than thousand of random test cases with different traffic scenarios and different network situations, it is clear from all the result graphs that the proposed TFP-MLL-P perturbation mechanism works more efficiently than the RR-P perturbation mechanism and manages to give optimized results in almost all the cases. It proves that within each step of simulated annealing, choosing the candidate route based on the WC and TFP constraints helps to improve the efficiency of the simulated annealing search.

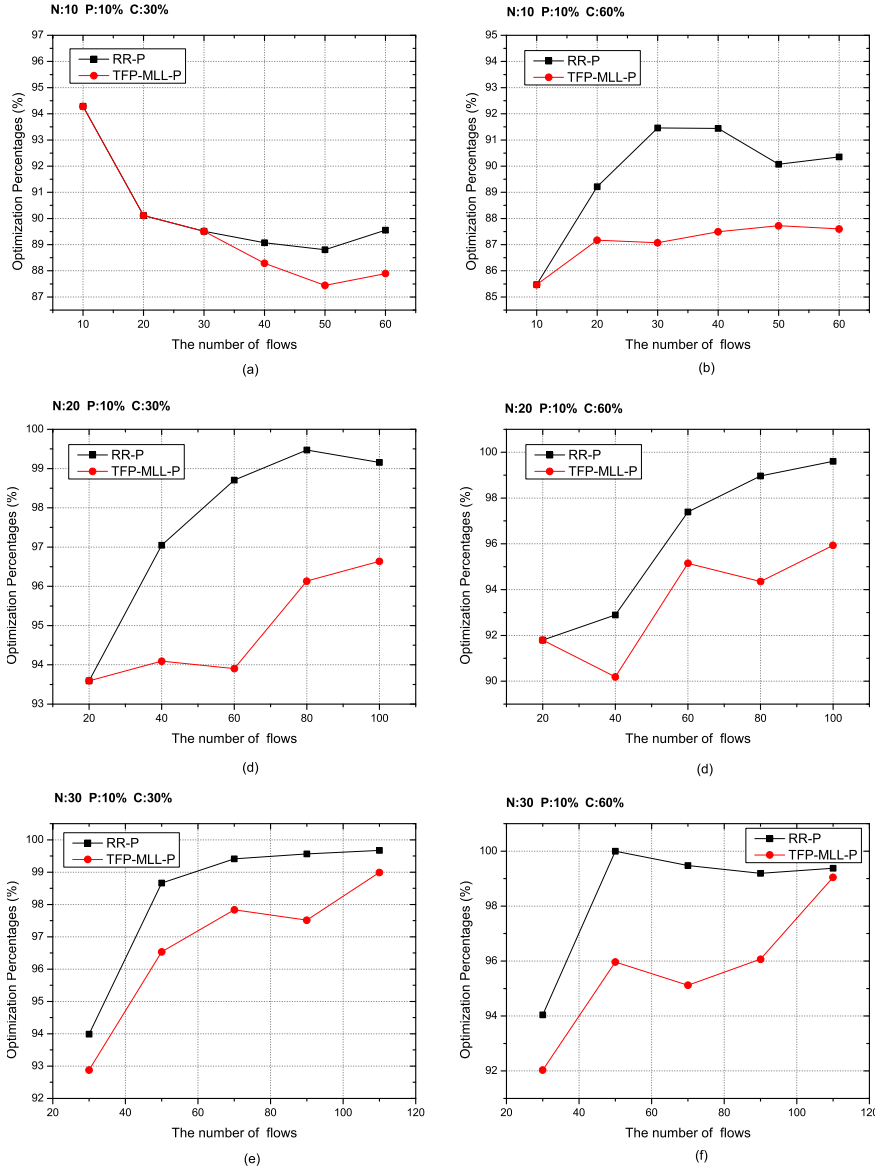


Figure 6.6: The comparison of the Optimization Percentages between different perturbation methods under M_{random} traffic scenario when P=10%.

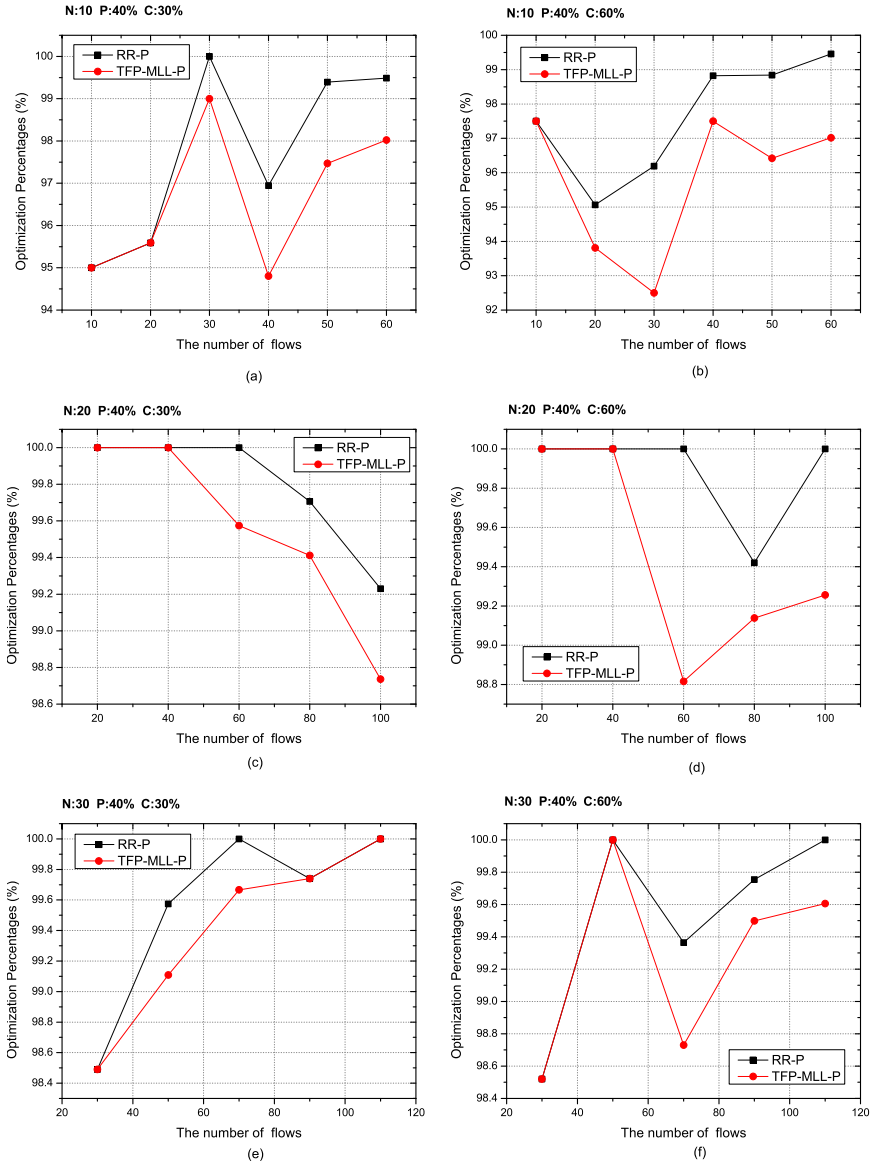


Figure 6.7: The comparison of the Optimization Percentages between different perturbation methods under M_{random} traffic scenario when P=40%.

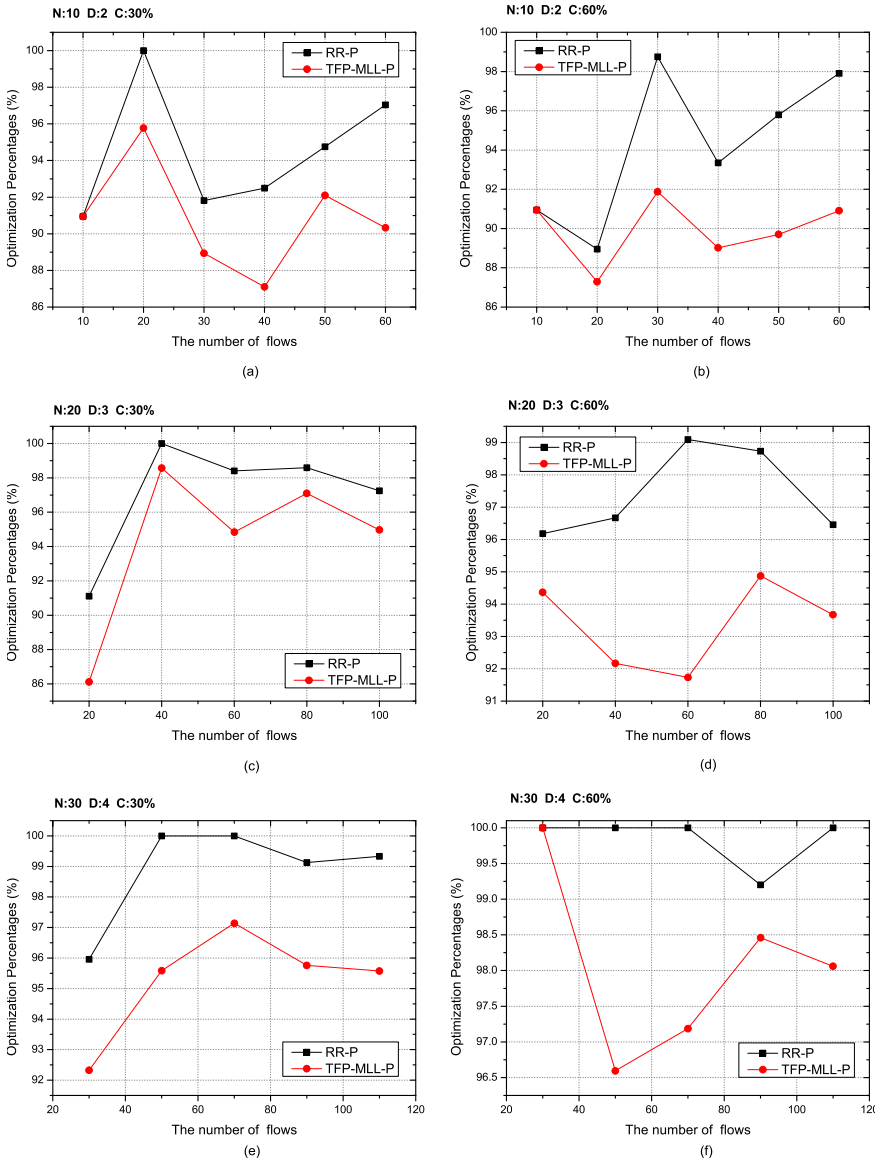


Figure 6.8: The comparison of the Optimization Percentages between perturbation methods under $M_{division}$ traffic scenario when the ring has relatively fewer divisions.

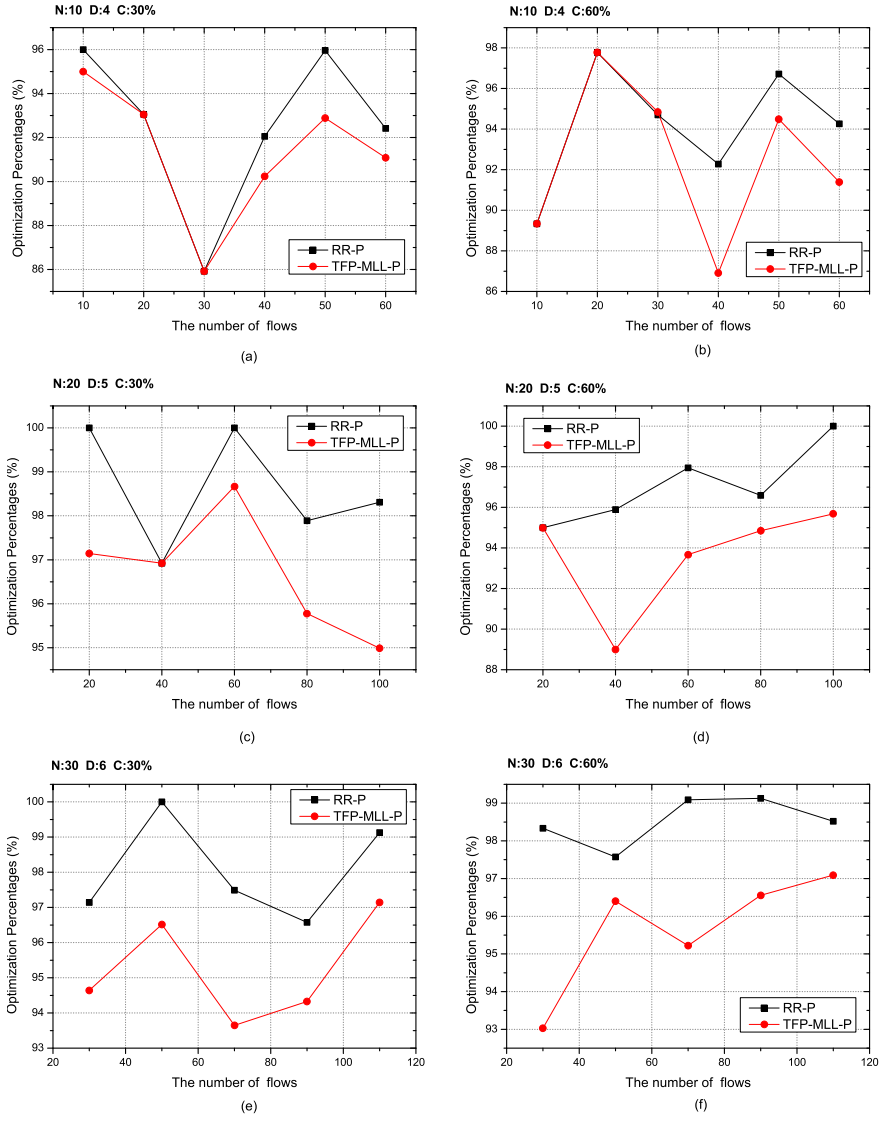


Figure 6.9: The comparison of the Optimization Percentages between perturbation methods under $M_{division}$ traffic scenario when the ring has relatively more divisions.

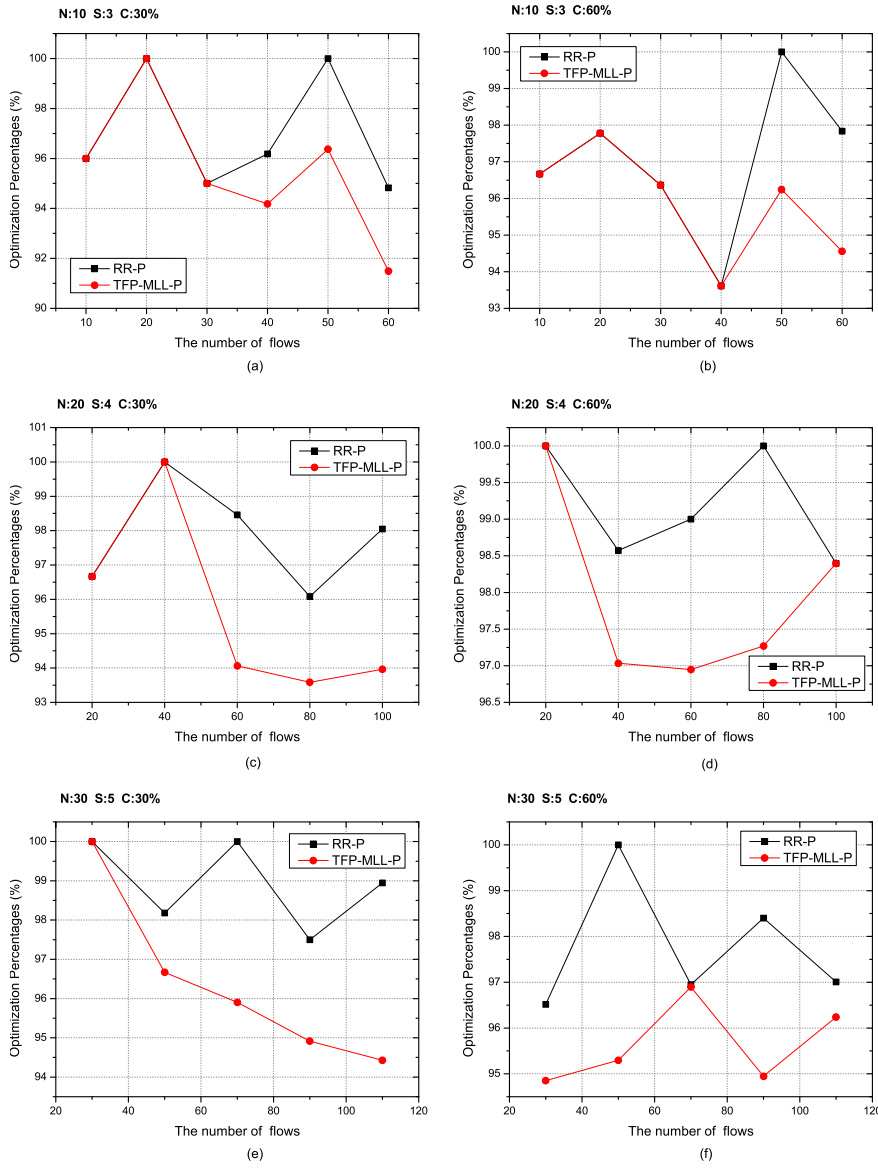


Figure 6.10: The comparison of the Optimization Percentages between different perturbation methods under M_{span} traffic scenario when the maximum span is relatively shorter.

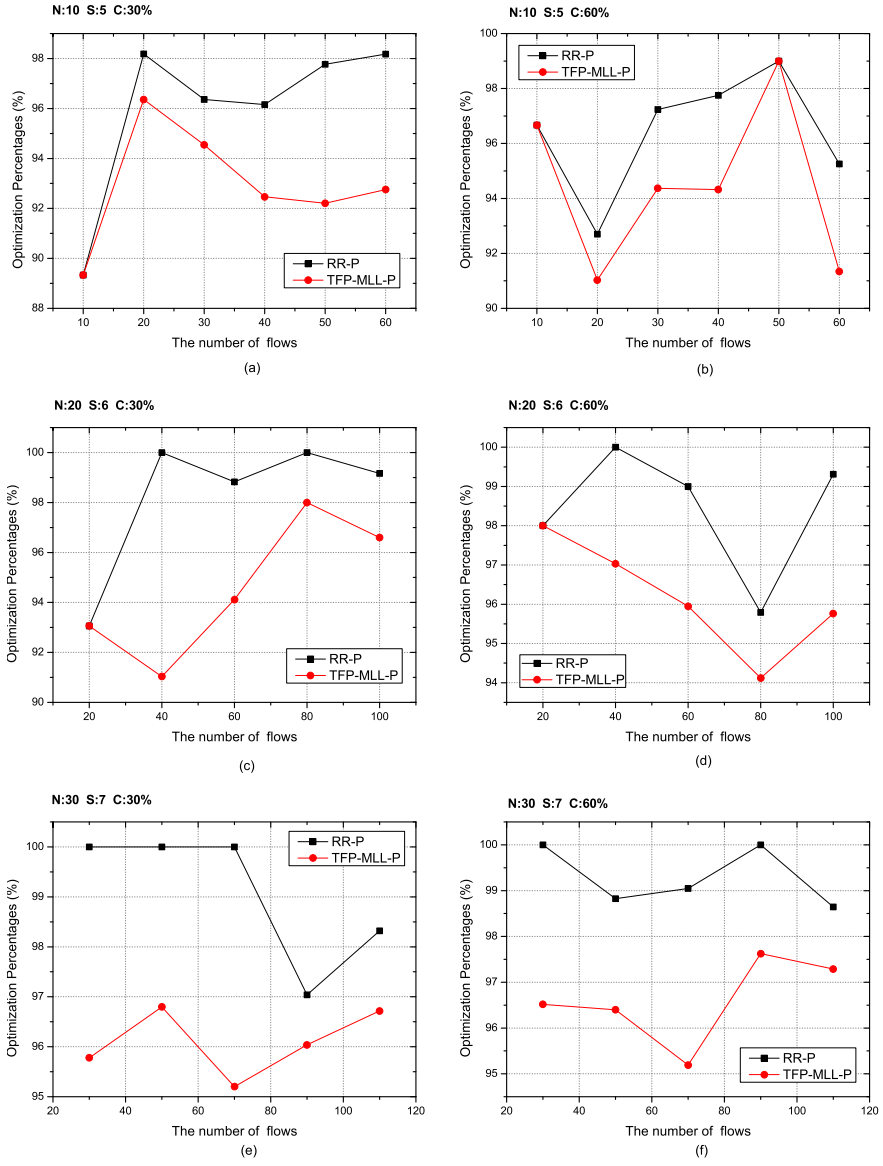


Figure 6.11: The comparison of the Optimization Percentages between different perturbation methods under M_{span} traffic scenario when the maximum span is relatively longer.

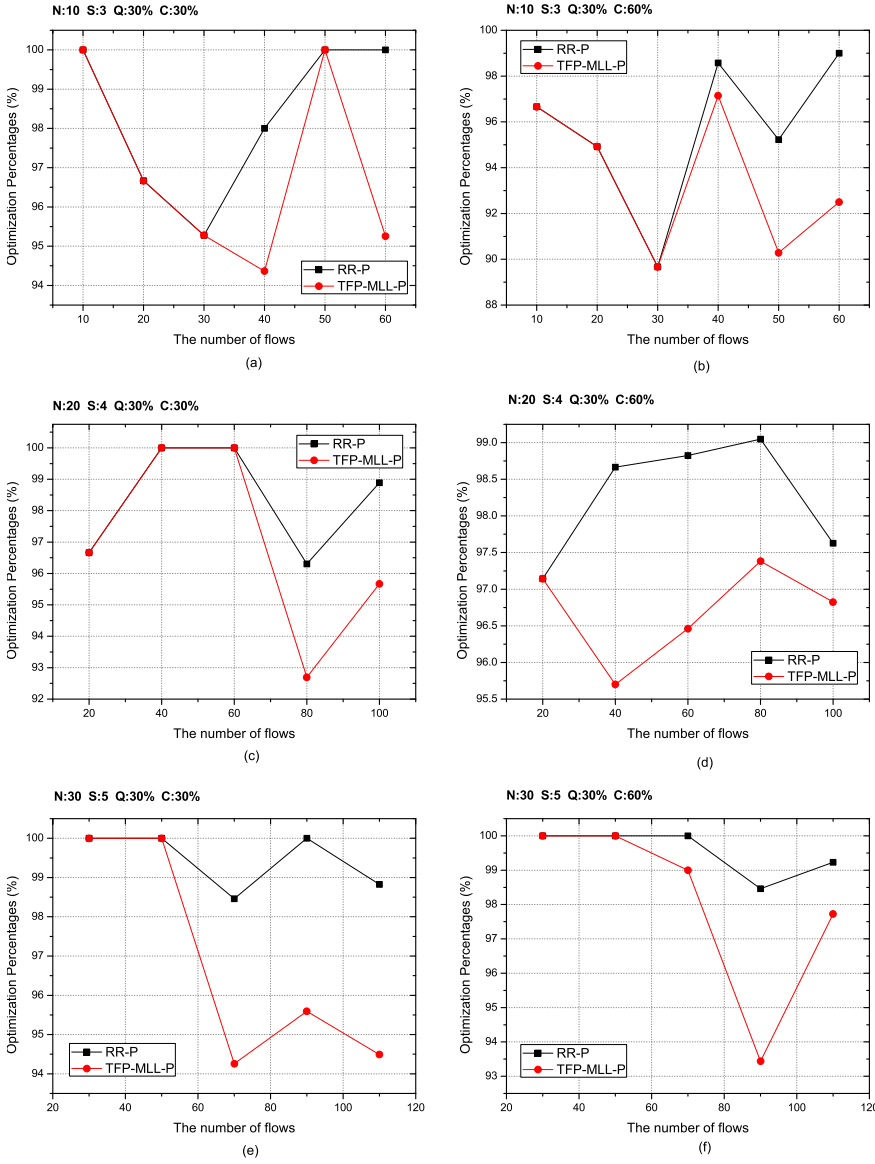


Figure 6.12: The comparison of the Optimization Percentages between different perturbation methods under M_{span_partly} traffic scenario when Q equals to 30%.

6.7.3 The Results and the Time Consumption between Different Perturbation Mechanisms

In this section four groups of simulation results are given out to show numerical scales of calculated number of used wavelengths and fibers. The found minimum amounts of wavelengths are listed under "#W" and the results of used fibers are listed under "#F". It should be noticed that there is no restriction on the maximum number of wavelengths per fiber considered yet. The column of "#T(s)" lists the time consumption for running each single test case. The test cases are the first case of 5 random cases used in Section 6.7.2. All the simulations were run on lab computers with Intel(R) Core(TM)2 Duo, 2.99GHz CPU and 3.25GB RAM.

Table 6.4 lists the simulation results using the RR-P perturbation mechanism (R=1) for the M_{random} traffic (G=1). Table 6.5 gives out the results using the TFP-MLL-P perturbation mechanism (R=3) under the same test cases.

Table 6.6 and Table 6.7 show the results of the $M_{division}$ traffic (G=2). Table 6.8 and Table 6.9 show the results of the M_{span} traffic (G=3). The results of the M_{span_partly} traffic (G=4) are listed in Table 6.10 and Table 6.11.

From the results listed under the "#F", it can be seen that the minimum number of used fibers found by the TFP-MLL-P mechanism sometimes is bigger than the number found by the RR-P mechanism. However it does not mean that the TFP-MLL-P is less efficient than the RR-P in fiber assignment. It is because that in simulated annealing process the cost function is configured as wavelength consumption, not fiber consumption. And the solution with the minimum wavelength consumption does not always result in the same solution with minimum fiber consumption. Therefore, in some of the cases, the minimum amount of used fibers found by the TFP-MLL-P mechanism is bigger than the amount found by the RR-P mechanism.

From the time consumption point of view, generally the increase of the calculation time is due to the growing complexity of solving the maximum clique problem when the network size and load increasing. Compared to the RR-P mechanism, the TFP-MLL-P mechanism spends a bit more time to solve problems. It is because the TFP-MLL-P tries to find proper route candidate to change the path. However, the time

difference is not that dramatic, and from the results of wavelength consumption it proves that the TFP-MLL-P does improve the calculation performance within confined calculation steps.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
1	10	10	10%		30%			1	5	4	71
1	10	20	10%		30%			1	8	6	82
1	10	30	10%		30%			1	13	8	96
1	10	40	10%		30%			1	15	9	114
1	10	50	10%		30%			1	18	13	139
1	10	60	10%		30%			1	22	14	174
1	10	10	10%		60%			1	5	5	75
1	10	20	10%		60%			1	10	8	91
1	10	30	10%		60%			1	12	12	108
1	10	40	10%		60%			1	15	15	135
1	10	50	10%		60%			1	21	19	167
1	10	60	10%		60%			1	25	21	207
1	20	20	10%		30%			1	11	6	83
1	20	40	10%		30%			1	19	12	119
1	20	60	10%		30%			1	27	14	178
1	20	80	10%		30%			1	34	18	276
1	20	100	10%		30%			1	45	19	406
1	20	20	10%		60%			1	11	9	93
1	20	40	10%		60%			1	23	15	142
1	20	60	10%		60%			1	30	22	221
1	20	80	10%		60%			1	36	28	338
1	20	100	10%		60%			1	46	36	502
1	30	30	10%		30%			1	16	8	99
1	30	50	10%		30%			1	28	12	147
1	30	70	10%		30%			1	36	16	227
1	30	90	10%		30%			1	50	18	340
1	30	110	10%		30%			1	61	21	508
1	30	30	10%		60%			1	20	14	117
1	30	50	10%		60%			1	32	18	180
1	30	70	10%		60%			1	45	24	287
1	30	90	10%		60%			1	52	32	427
1	30	110	10%		60%			1	66	34	641

Table 6.4: Simulation results under the M_{random} scenario using the RR-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
1	10	10	10%		30%			3	5	4	84
1	10	20	10%		30%			3	8	7	95
1	10	30	10%		30%			3	13	7	110
1	10	40	10%		30%			3	14	9	126
1	10	50	10%		30%			3	17	12	154
1	10	60	10%		30%			3	21	13	191
1	10	10	10%		60%			3	5	5	85
1	10	20	10%		60%			3	10	9	103
1	10	30	10%		60%			3	11	11	117
1	10	40	10%		60%			3	15	15	147
1	10	50	10%		60%			3	20	18	179
1	10	60	10%		60%			3	23	21	220
1	20	20	10%		30%			3	11	6	98
1	20	40	10%		30%			3	19	12	136
1	20	60	10%		30%			3	26	12	197
1	20	80	10%		30%			3	34	18	303
1	20	100	10%		30%			3	44	22	447
1	20	20	10%		60%			3	11	9	105
1	20	40	10%		60%			3	22	15	157
1	20	60	10%		60%			3	29	22	240
1	20	80	10%		60%			3	34	27	357
1	20	100	10%		60%			3	45	35	534
1	30	30	10%		30%			3	16	9	117
1	30	50	10%		30%			3	28	12	171
1	30	70	10%		30%			3	36	16	257
1	30	90	10%		30%			3	48	18	378
1	30	110	10%		30%			3	60	21	553
1	30	30	10%		60%			3	20	14	135
1	30	50	10%		60%			3	29	20	205
1	30	70	10%		60%			3	42	25	311
1	30	90	10%		60%			3	50	31	459
1	30	110	10%		60%			3	66	34	678

Table 6.5: Simulation results under the M_{random} scenario using the TFP-MLL-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
2	10	10	40%		30%	2		1	5	4	71
2	10	20	40%		30%	2		1	10	7	83
2	10	30	40%		30%	2		1	14	9	98
2	10	40	40%		30%	2		1	17	11	116
2	10	50	40%		30%	2		1	19	12	142
2	10	60	40%		30%	2		1	27	13	181
2	10	10	40%		60%	2		1	6	5	76
2	10	20	40%		60%	2		1	10	8	91
2	10	30	40%		60%	2		1	14	12	113
2	10	40	40%		60%	2		1	18	15	139
2	10	50	40%		60%	2		1	22	21	170
2	10	60	40%		60%	2		1	27	21	213
2	20	20	40%		30%	3		1	8	6	83
2	20	40	40%		30%	3		1	11	9	112
2	20	60	40%		30%	3		1	18	14	171
2	20	80	40%		30%	3		1	26	20	260
2	20	100	40%		30%	3		1	30	21	393
2	20	20	40%		60%	3		1	9	8	89
2	20	40	40%		60%	3		1	16	14	134
2	20	60	40%		60%	3		1	24	20	205
2	20	80	40%		60%	3		1	31	24	311
2	20	100	40%		60%	3		1	37	33	474
2	30	30	40%		30%	4		1	10	8	95
2	30	50	40%		30%	4		1	13	12	135
2	30	70	40%		30%	4		1	21	16	204
2	30	90	40%		30%	4		1	24	20	307
2	30	110	40%		30%	4		1	28	24	479
2	30	30	40%		60%	4		1	11	11	107
2	30	50	40%		60%	4		1	19	15	162
2	30	70	40%		60%	4		1	22	20	240
2	30	90	40%		60%	4		1	24	24	361
2	30	110	40%		60%	4		1	32	30	530

Table 6.6: Simulation results under the $M_{division}$ scenario using the RR-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
2	10	10	40%		30%	2		3	5	4	82
2	10	20	40%		30%	2		3	9	7	95
2	10	30	40%		30%	2		3	13	9	112
2	10	40	40%		30%	2		3	15	10	129
2	10	50	40%		30%	2		3	19	13	157
2	10	60	40%		30%	2		3	26	14	197
2	10	10	40%		60%	2		3	6	5	87
2	10	20	40%		60%	2		3	9	9	103
2	10	30	40%		60%	2		3	13	12	124
2	10	40	40%		60%	2		3	18	16	151
2	10	50	40%		60%	2		3	21	17	183
2	10	60	40%		60%	2		3	26	21	227
2	20	20	40%		30%	3		3	8	6	95
2	20	40	40%		30%	3		3	11	9	124
2	20	60	40%		30%	3		3	18	14	191
2	20	80	40%		30%	3		3	27	18	292
2	20	100	40%		30%	3		3	31	21	448
2	20	20	40%		60%	3		3	9	8	101
2	20	40	40%		60%	3		3	16	14	144
2	20	60	40%		60%	3		3	22	21	215
2	20	80	40%		60%	3		3	28	24	325
2	20	100	40%		60%	3		3	35	31	498
2	30	30	40%		30%	4		3	9	9	109
2	30	50	40%		30%	4		3	13	12	152
2	30	70	40%		30%	4		3	19	15	230
2	30	90	40%		30%	4		3	23	21	360
2	30	110	40%		30%	4		3	28	24	591
2	30	30	40%		60%	4		3	11	11	117
2	30	50	40%		60%	4		3	18	17	174
2	30	70	40%		60%	4		3	21	20	249
2	30	90	40%		60%	4		3	25	24	373
2	30	110	40%		60%	4		3	30	29	555

Table 6.7: Simulation results under the $M_{division}$ scenario using the TFP-MLL-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
3	10	10	40%		30%		3	1	4	3	71
3	10	20	40%		30%		3	1	5	5	78
3	10	30	40%		30%		3	1	7	7	89
3	10	40	40%		30%		3	1	10	9	107
3	10	50	40%		30%		3	1	10	9	127
3	10	60	40%		30%		3	1	12	12	157
3	10	10	40%		60%		3	1	6	6	77
3	10	20	40%		60%		3	1	8	7	86
3	10	30	40%		60%		3	1	11	11	105
3	10	40	40%		60%		3	1	14	14	128
3	10	50	40%		60%		3	1	16	16	153
3	10	60	40%		60%		3	1	17	17	185
3	20	20	40%		30%		4	1	6	5	80
3	20	40	40%		30%		4	1	8	8	106
3	20	60	40%		30%		4	1	14	12	157
3	20	80	40%		30%		4	1	14	12	239
3	20	100	40%		30%		4	1	19	16	371
3	20	20	40%		60%		4	1	8	8	89
3	20	40	40%		60%		4	1	13	13	128
3	20	60	40%		60%		4	1	17	17	189
3	20	80	40%		60%		4	1	22	22	291
3	20	100	40%		60%		4	1	24	24	451
3	30	30	40%		30%		5	1	8	7	92
3	30	50	40%		30%		5	1	10	9	126
3	30	70	40%		30%		5	1	13	11	190
3	30	90	40%		30%		5	1	15	14	294
3	30	110	40%		30%		5	1	16	16	464
3	30	30	40%		60%		5	1	12	12	108
3	30	50	40%		60%		5	1	14	14	150
3	30	70	40%		60%		5	1	19	19	231
3	30	90	40%		60%		5	1	22	21	340
3	30	110	40%		60%		5	1	26	25	504

Table 6.8: Simulation results under the M_{span} scenario using the RR-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
3	10	10	40%		30%		3	1	4	3	81
3	10	20	40%		30%		3	1	5	5	88
3	10	30	40%		30%		3	1	7	6	100
3	10	40	40%		30%		3	1	10	8	119
3	10	50	40%		30%		3	1	10	9	139
3	10	60	40%		30%		3	1	12	12	172
3	10	10	40%		60%		3	1	6	6	90
3	10	20	40%		60%		3	1	8	7	95
3	10	30	40%		60%		3	1	11	11	114
3	10	40	40%		60%		3	1	14	14	141
3	10	50	40%		60%		3	1	15	14	162
3	10	60	40%		60%		3	1	17	17	192
3	20	20	40%		30%		4	1	6	5	91
3	20	40	40%		30%		4	1	8	8	115
3	20	60	40%		30%		4	1	13	12	174
3	20	80	40%		30%		4	1	14	12	274
3	20	100	40%		30%		4	1	18	16	452
3	20	20	40%		60%		4	1	8	8	99
3	20	40	40%		60%		4	1	13	13	136
3	20	60	40%		60%		4	1	17	17	195
3	20	80	40%		60%		4	1	22	22	297
3	20	100	40%		60%		4	1	24	24	434
3	30	30	40%		30%		5	1	8	7	102
3	30	50	40%		30%		5	1	10	9	139
3	30	70	40%		30%		5	1	13	11	215
3	30	90	40%		30%		5	1	15	14	359
3	30	110	40%		30%		5	1	16	16	654
3	30	30	40%		60%		5	1	12	12	119
3	30	50	40%		60%		5	1	14	14	158
3	30	70	40%		60%		5	1	18	18	237
3	30	90	40%		60%		5	1	22	21	352
3	30	110	40%		60%		5	1	25	25	525

Table 6.9: Simulation results under the M_{span} scenario using the TFP-MLL-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
4	10	10	40%	30%	30%		3	1	4	3	67
4	10	20	40%	30%	30%		3	1	4	4	74
4	10	30	40%	30%	30%		3	1	7	7	89
4	10	40	40%	30%	30%		3	1	9	9	105
4	10	50	40%	30%	30%		3	1	12	10	128
4	10	60	40%	30%	30%		3	1	13	12	169
4	10	10	40%	30%	60%		3	1	4	3	68
4	10	20	40%	30%	60%		3	1	7	6	80
4	10	30	40%	30%	60%		3	1	10	9	97
4	10	40	40%	30%	60%		3	1	13	12	116
4	10	50	40%	30%	60%		3	1	14	13	143
4	10	60	40%	30%	60%		3	1	17	13	186
4	20	20	40%	30%	30%		4	1	5	4	75
4	20	40	40%	30%	30%		4	1	8	8	104
4	20	60	40%	30%	30%		4	1	11	11	162
4	20	80	40%	30%	30%		4	1	14	12	287
4	20	100	40%	30%	30%		4	1	16	15	578
4	20	20	40%	30%	60%		4	1	7	6	81
4	20	40	40%	30%	60%		4	1	14	10	112
4	20	60	40%	30%	60%		4	1	17	15	173
4	20	80	40%	30%	60%		4	1	20	17	285
4	20	100	40%	30%	60%		4	1	25	20	579
4	30	30	40%	30%	30%		5	1	7	4	87
4	30	50	40%	30%	30%		5	1	9	9	125
4	30	70	40%	30%	30%		5	1	12	10	211
4	30	90	40%	30%	30%		5	1	16	13	489
4	30	110	40%	30%	30%		5	1	16	14	1050
4	30	30	40%	30%	60%		5	1	9	6	89
4	30	50	40%	30%	60%		5	1	13	11	133
4	30	70	40%	30%	60%		5	1	18	14	215
4	30	90	40%	30%	60%		5	1	24	19	403
4	30	110	40%	30%	60%		5	1	26	23	1004

Table 6.10: Simulation results under the M_{span_partly} scenario using the RR-P perturbation mechanism.

G	N	F	P	Q	C	D	S	R	#W	#F	#T(s)
4	10	10	40%	30%	30%		3	1	4	3	78
4	10	20	40%	30%	30%		3	1	4	4	83
4	10	30	40%	30%	30%		3	1	7	7	102
4	10	40	40%	30%	30%		3	1	9	9	120
4	10	50	40%	30%	30%		3	1	12	10	148
4	10	60	40%	30%	30%		3	1	12	11	236
4	10	10	40%	30%	60%		3	1	4	3	80
4	10	20	40%	30%	60%		3	1	7	6	91
4	10	30	40%	30%	60%		3	1	10	9	110
4	10	40	40%	30%	60%		3	1	13	12	131
4	10	50	40%	30%	60%		3	1	14	13	165
4	10	60	40%	30%	60%		3	1	16	14	246
4	20	20	40%	30%	30%		4	1	5	4	86
4	20	40	40%	30%	30%		4	1	8	8	115
4	20	60	40%	30%	30%		4	1	11	11	210
4	20	80	40%	30%	30%		4	1	14	12	542
4	20	100	40%	30%	30%		4	1	16	15	1230
4	20	20	40%	30%	60%		4	1	7	6	94
4	20	40	40%	30%	60%		4	1	14	10	126
4	20	60	40%	30%	60%		4	1	17	15	207
4	20	80	40%	30%	60%		4	1	20	17	516
4	20	100	40%	30%	60%		4	1	25	18	1567
4	30	30	40%	30%	30%		5	1	7	4	96
4	30	50	40%	30%	30%		5	1	9	9	144
4	30	70	40%	30%	30%		5	1	11	9	416
4	30	90	40%	30%	30%		5	1	15	13	1199
4	30	110	40%	30%	30%		5	1	15	14	4067
4	30	30	40%	30%	60%		5	1	9	6	99
4	30	50	40%	30%	60%		5	1	13	11	149
4	30	70	40%	30%	60%		5	1	18	14	324
4	30	90	40%	30%	60%		5	1	22	19	904
4	30	110	40%	30%	60%		5	1	26	23	2662

Table 6.11: Simulation results under the M_{span_partly} scenario using the TFP-MLL-P perturbation mechainsm.

6.7.4 The Comparison between the Effects of the WC and TFP Constraints

In this subsection, a comparison between the effects of the increase of the WC and the TFP constraints on the wavelength and fiber consumption is discussed. The test cases were randomly generated under the M_{span} traffic scenario. Under this traffic type, for the same amount of traffic flows, transmitting the traffic with shorter span needs fewer wavelengths and fibers than the traffic with longer span. Therefore, the effects of the increase of the WC constraints can be shown by the tests running for the traffic with different span values. The increase of the TFP constraints can be controlled by increasing parameter C.

The simulations were carried out on different network sizes (N=10, 20, 30) and with relatively high traffic loads (F= 60, 80, 90). Figure 6.13 shows the found minimum amount of used wavelengths and fibers on network with 10 nodes and 60 traffic flows. The black, red and blue curves represent the traffic with span value equal to 3, 5 and 8. Figure 6.14 shows the results on the network with 20 nodes and 80 traffic flows and the values of span were set to 5, 8 and 11. The results on network with 30 nodes 90 traffic flows are illustrated in Figure 6.15, and the values of span were set to 5, 10 and 15.

Figure 6.13.(a) gives the results of the number of used wavelengths for the traffic with different S values under different percentages of the TFP constraints. The black curve (with S = 3) shows that, regarding to the traffic flows with short span when the percentage (C) of the TFP constraints is low, the increase of the C will not result in a big increase on the number of used wavelengths. Only after the C is increased to a certain stage, the amount of used wavelengths starts to grow fast due to the increase of the TFP constraints. It is because that there is more chance to assign the same wavelength to more routes for the traffic with short span, also there are many possible solutions to arrange the routes, which result in the same amount of wavelength consumption. Therefore, at the beginning of the increase of the TFP constraints, there is always another solution that can be found to keep the wavelength consumption at the same level.

Compared to the black curve, the blue curve in Figure 6.13.(a), which represents the traffic with longer span (S = 8), has larger wavelength consumption and smaller increasing slope value. That is because there

are fewer chances to assign routes with the same wavelength due to WC constraints, thus the increase of the C slowly causes the increase of used wavelengths.

Figure 6.13.(b) gives the results of the number of used fibers. The different numbers of required fibers are mainly affected by the increase of the TFP constraints. Therefore, there are not many differences between the traffic with different span values. The slight higher fiber consumption for the traffic with longer span is resulted from the larger wavelength consumption.

Figure 6.14 and Figure 6.15 show the same trend as described before on networks with 20 and 30 nodes.

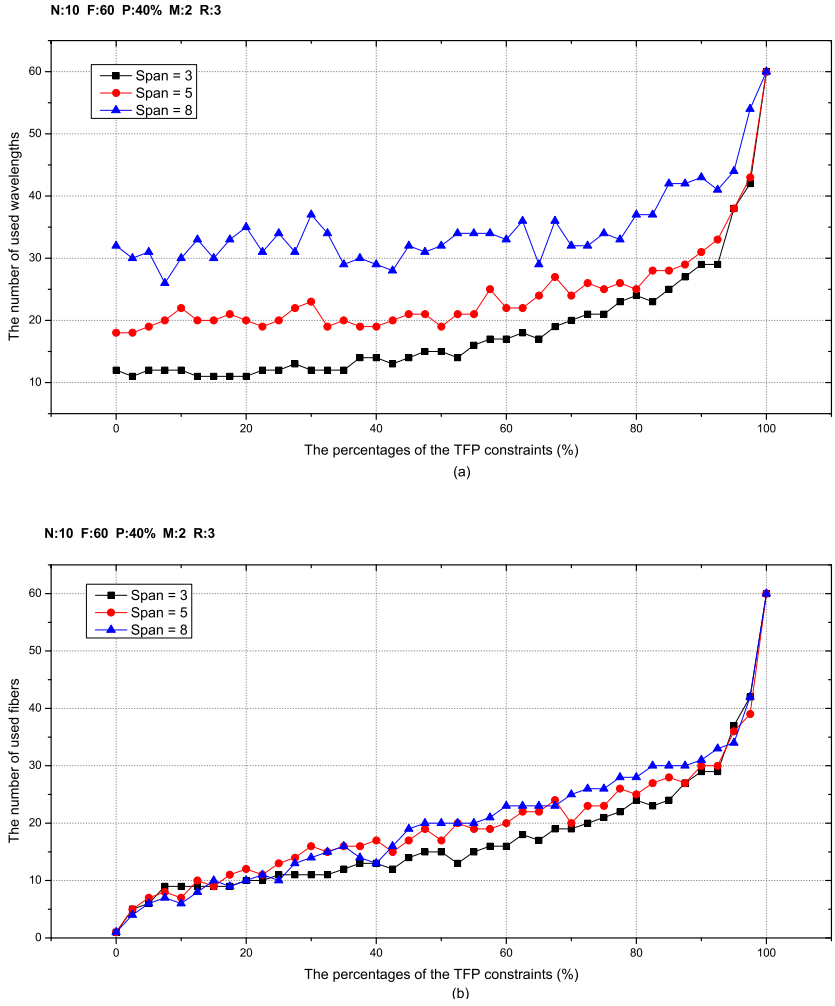


Figure 6.13: The number of used wavelengths and fibers of the M_{span} traffic scenario on the network with 10 nodes when S=3, 5 and 8.

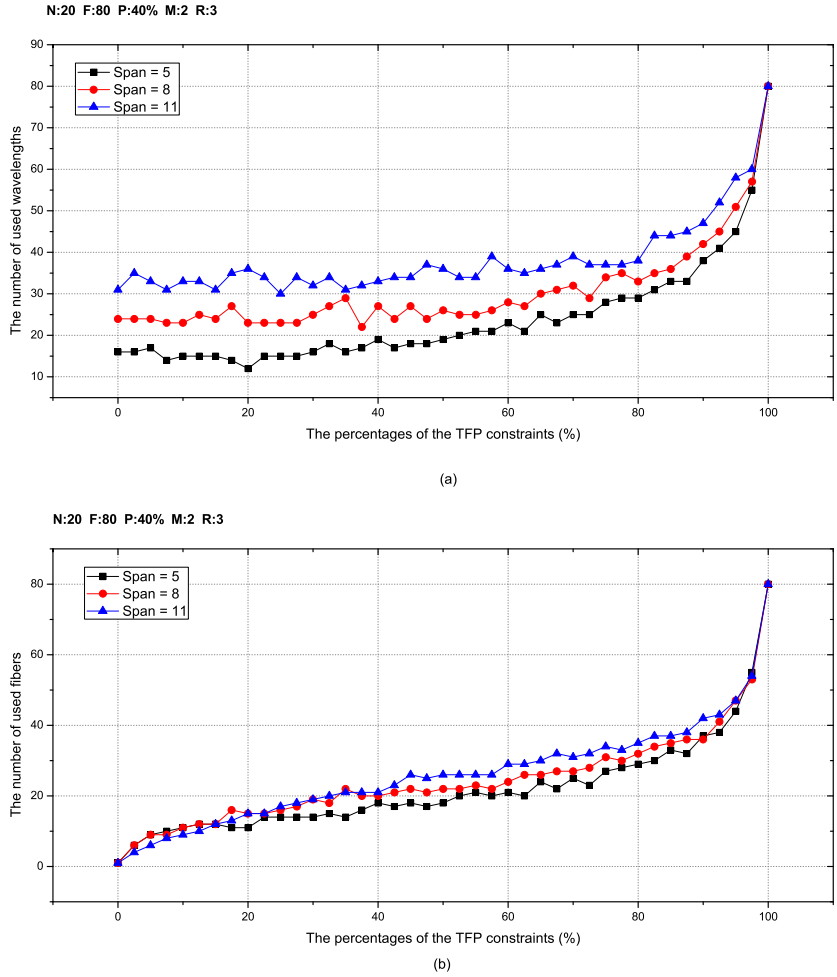


Figure 6.14: The number of used wavelengths and fibers of the M_{span} traffic scenario on the network with 20 nodes when S=5, 8 and 11.

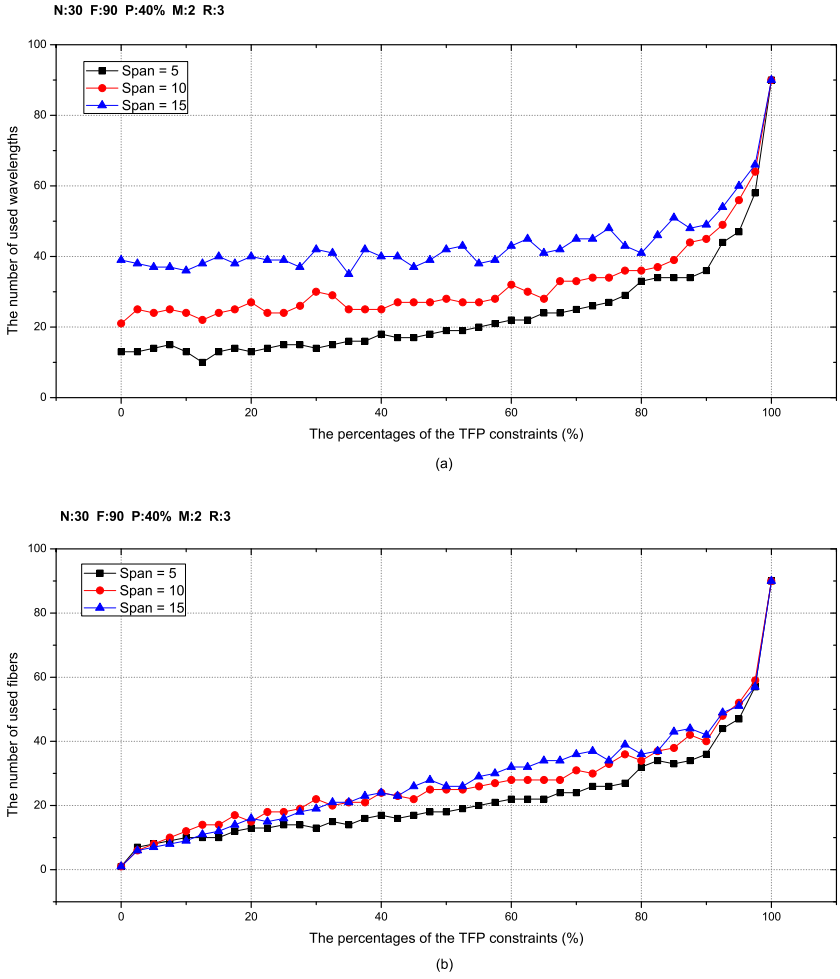


Figure 6.15: The number of used wavelengths and fibers of the M_{span} traffic scenario on the network with 30 nodes when S=5, 10 and 15.

6.7.5 The Fiber Consumption with Different Number of the Maximum Wavelengths allowed in One Fiber

In this subsection, the simulations show the changes of the number of used fibers under different number of the maximum wavelengths allowed per fiber (MAX_W). The tests were carried out on networks with 10, 20 and 30 nodes. Various amounts of traffic flows are randomly generated under the M_{span} traffic scenario. The percentage of the TFP constraints was set to a low value (4%) which makes one fiber can accommodate more wavelengths when the value of the MAX_W is large. The column of "#F($\leq$ 2)" lists the number of used fibers when the MAX_W is set to 2. The column of "#F($\leq$ 5)" lists the number of required fibers when the MAX_W is set to 5.

The results in Table 6.12 give some example numbers of used fibers under different network situations and with different value of the MAX_W. It is clear that when single fiber can accommodate fewer wavelengths, the total number of used fibers increases.

N	F	S	C	#W	#F($\leq$ 2)	#F($\leq$ 5)	#F($\leq$ 100)
10	40	5	4%	13	7	4	4
10	50	5	4%	17	9	4	4
10	60	5	4%	20	11	7	5
20	60	6	4%	13	8	7	7
20	80	6	4%	17	11	7	7
20	100	6	4%	22	13	10	9
30	70	7	4%	13	8	6	6
30	90	7	4%	19	12	9	8
30	110	7	4%	23	13	8	8

Table 6.12: Results of used fibers under different values of the MAX_W.

6.7.6 Summary

In this chapter the challenge of solving MC-RWA problems with avionic system partition constraints on the avionic transport network is addressed. Based on mathematical tools and heuristic methods, such as graph theory and simulated annealing, the optimized solutions of route configurations, wavelength and fiber assignments can be achieved by the proposed methods, which are described in this chapter.

As lots of research work did, the methods, such as matching, clique and coloring in graph theory are adopted to find a minimum cost solution of wavelength and fiber consumption for a fixed system route configuration. Through adapting the procedures of the graph methods, it is managed to fulfill the avionic system isolation constraints (TFP constraints), and at the same time still be able to find a minimum cost solution. In other words, according to isolation constraints, the possibility of assigning the TFP bounded systems with the same wavelength and fiber is manually deleted during the execution of the graph methods. In addition the number of the maximum wavelengths allowed in one fiber is taken into account when assigning wavelengths into fibers.

The simulated annealing is employed to search the minimum cost solution among a great amount of possible system route configurations. Based on the WC and the TFP constraints, a novel perturbation mechanism, named TFP Constraints Aware - Maximum Loaded Link Perturbation (TFP-MLL-P) is proposed. Compared to RR-P mechanism, a wide range of case-based simulations are carried out under four traffic scenarios and on different network sizes and with different network loads. The results prove that, with slightly increased calculation time, the proposed TFP-MLL-P mechanism works more efficiently and manages to give optimized results in almost all the test cases. In other words, it helps to improve the efficiency of the simulated annealing process by taking the WC and TFP constraints into account when choosing the candidate route within each step of simulated annealing round.

Furthermore, the effects between the WC constraints and TFP constraints on the wavelength and fiber consumption are compared. From the simulation results, it is known that the WC constraint is the main reason for the increase of the wavelength consumption when the percentage of the TFP constraints is low. However, after the percentage of the TFP constraints is increased to a certain large stage, the amount of

the used wavelengths starts to grow fast due to the increase of the TFP constraints. On the other hand the increase of the fiber consumption is mainly because of the increase of the TFP constraints.

Chapter 7

Developing a Home Environment Service Knowledge Management System

7.1 Introduction

Nowadays, family members are interested in being able to control their home devices in an easier way and with minimum installation and configuration processes. Following this tendency, home network systems gain more and more attention and the market keeps expanding. Through a home network, all the home devices can be connected and communicate with each other. Based on such a network, a home network system with intelligence features helps people to manage their home devices and simplifies maintenance work which improves the quality of daily life. However, designing such home network system faces plenty of challenges. The home network system should be heterogeneous, since there are numerous types of devices from various producers. Advanced technologies used by devices, impose complicated configurations and quite likely cause more frequent update operations of new versions of device software. For certain devices, there could even be more than one software supplier.

To address this problem, this chapter proposes a Home Environment Service Knowledge Management (HESKM) system, which manages the whole information of a home environment and helps all software configure and update procedures across multivendor environments. This work is based on the European Commission project COMANCHE, started in July 2005 and finished in July 2008, which developed a network framework for software configuration management in home environment and used ontology technology to store information [67]. The COMANCHE stands for Software COnfiguration MAnagement framework for Networked serviCes environments and arcHitectures incorporation ambiEnt intelligence features. The previous related works are described in [13, 68, 69]. The research work of this chapter gains the experiences of the COMANCHE project, using ontology to represent home environment due to its' strong ability to illustrate actual relations of world. The structure of the HESKM system's ontology has been reconstructed to improve the accuracy of demonstrating a home environment and make it easier for the system to install and extract information. The inference function of the reasoner has been researched and the theory and detailed implementation of using a reasoner to acquire the information according to user requests are described in this chapter. The proposed strategy of calculating service dependency hierarchy ensures the correct sequence of service installation steps and maintains the compatibility among a great number of various services.

The HESKM system is a context-aware system. "The context-aware system is defined as a system that uses context to provide relevant information and/or services to user, where relevancy depends on the user's task." [70] Context-aware technologies can adapt to environment and make installation processes and maintenances of devices easier for end user. The context of the HESKM system is a home environment, which includes family members, home devices and home services. The home services might be devices' software or software used by other software. The context provides the knowledge base to help the HESKM system be aware of the states of home devices, such as devices' potential capabilities and their software dependencies. The knowledge base and context of the HESKM system is implemented by ontology. By describing the properties of family members, devices, devices' software and the relationships among them, the knowledge of home environment is im-

plemented in an ontology file. The HESKM system has high level of intelligence. Based on the context, the system can keep consistency of information and automatically help family members to accomplish the software configuration and management.

The rest of this chapter is structured as follows: What an ontology is and how to use ontologies to design and represent a home environment is given in Section 7.2. Section 7.3 introduces the HESKM system ontology. How to exploit and acquire the information from the ontology by using an ontology function and a reasoner is described in Section 7.4. The implementation of the HESKM ontology is given in Section 7.5. Section 7.6 describes the aspect which focuses on solving software hierarchical dependency problem. Section 7.7 summarizes this chapter.

7.2 ONTOLOGY: Concepts and Terminology

World Wide Web Consortium (W3C) defines ontology as the terms used to describe and represent an area of knowledge. Unlike traditional databases, which present and store information by various tables, ontology technology describes the information through constructing the relationships between information pieces. In other words, ontology can be defined as "a description of the concepts in the domain and also the relationships that hold between those concepts" [71]. Such way of composing the information knowledge base strongly resembles the logic of regular world. The high realistic representation enhances the accuracy of knowledge base and eases the design, implementation and maintenance operations. More practically, in the HESKM system, the Ontology Web Language (OWL) from W3C is applied as an ontology language, Protégé is used as visual programming tool and Fact++ is used as reasoner tool.

An OWL ontology consists of Classes, Properties and Individuals. In OWL, classes are used to represent concepts. "OWL classes are interpreted as sets that contain individuals. They are described using formal descriptions that state precisely the requirements for membership of the class" [71]. On the other hand, "individuals represent objects in the domain that we are interested in, which are instances of classes" [71]. For example, there is a person named Bob. "Bob" is an individual, belonging to the class "Person". In particular, the class "Person" can contains a number of individuals, such as "Bob", "Marry", "Alice". They

all satisfy the requirements of the class "Person", which is individuals should biologically be human beings. "Properties are binary relations on individuals, - i.e. properties link two individuals together" [71]. The relationships are stored and represented by properties. For example, Owns can be defined as a property. Then the representation "Bob Owns Washing Machine", states the relationship between Bob and a washing machine, which means that Bob has a washing machine. Property Restrictions can be applied to formally describe classes. "A restriction describes a class of individuals based on the relationships that members of the class participate in" [71]. For instance, the property restriction of the description of a new class "Mother" is that has hasChild relationship to some other individuals of the class "Person". In other words, the class "Mother" contains all the individuals who have at least one child. The class can be organized in a superclass-subclass hierarchy. If only humans are considered, then the class "Mother" can be the subclass of the class "Person".

Apart from information representation, there are many plug-in tools that could be used by an ontology to provide a variety of facilities. Reasoner is one of these plug-in tools, which is used by the HESKM system. The first function of a reasoner is consistency checking. Based on descriptions of classes, consistency checking ensures that all the statements in the ontology are conflict free. Besides a description, a class also has a definition. The classes' descriptions are all the necessary conditions to describe classes. It means that individuals belonging to a particular class should satisfy the class descriptions. On the other hand, definitions of classes should be defined by necessary and sufficient conditions. If some individuals satisfy the definition of a particular class, those individuals should be classified into such class. "A class that has at least one set of necessary and sufficient conditions is known as a Defined Class" [71]. An asserted class hierarchy is the class hierarchy which is constructed when the information is manually introduced into the ontology by developer. On the other hand, an inferred class hierarchy is computed by reasoner based on defined classes which is the second function offered by a reasoner. For example, "Bob", "Mary" and "Alice" are manually classified as individuals of the class "Person". The definition of the class "Mother" is stated as having hasChild relationship with other individuals of the class "Person". The class "Mother" is a subclass of the

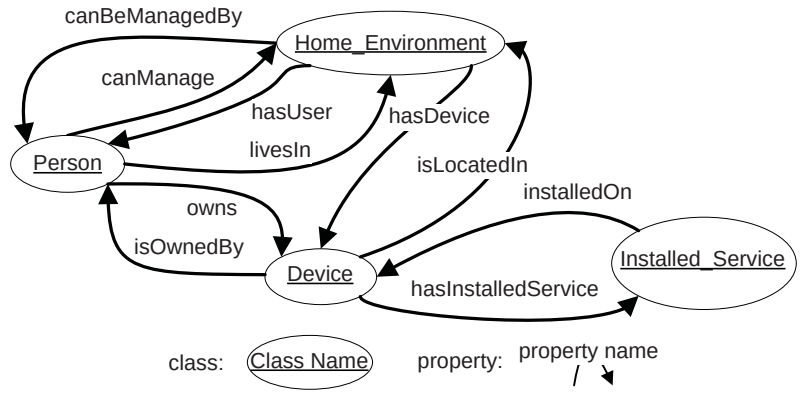


Figure 7.1: Outline of the HESKM system ontology.

class "Person". Furthermore, "Marry hasChild Alice" is stated in the ontology. In asserted class hierarchy, "Marry" is only under the class "Person". After running the reasoner, "Mary" is classified in the class "Mother" in inferred class hierarchy. Because of this function, the reasoner is also called classifier. A more detailed description about how to use this function to assist the HESKM system to exploit and acquire the information will be given in Section 7.4.

7.3 HESKM System Ontology

The HESKM system ontology describes a home environment, which includes family members, devices, devices' services and the relationships among them. Figure 7.1 illustrates the classes which gives an outline of whole HESKM system ontology.

The class "Home Environment" represents the home environment concept. For each home, an instance of this class is created. The class "Person" contains all family members. Each home connects their family members by property hasUser and family members have property livesIn linking them to their home. Furthermore, the property canManage and

canBeManageedBy define who has the right to access the home environment data. The class "Device" describes all the home devices. Each individual of the class "Device" is a real home device. Each home can record their devices by using the property hasDevice and each family member can be linked to the home devices by the property owns. The device uses property isLocatedIn to represent where it is and property isOwnedBy to show whom it belongs to. The class "Installed_Service" represents the software that has been installed in the devices. Property installedOn and hasInstalledService maintains the information about which device has installed which software. In the HESKM system ontology, the classes "Home Environment", "Person", "Device" and "Service" could be assumed as three ontology domains which are listed below. These three domains are connected to each other by the relationships illustrated in Figure 7.1.

- User and Business Domain Ontology
- Home Environment Ontology
- Service Ontology

User and Business Domain Ontology

The User and Business Domain Ontology is used for organizing and exploiting information related to business relationships, and family members' relationships with home environment, which are shown in Figure 7.2.

The class "Business_Organization" represents a business entity. In the ontology structure relationship Is-a is used to describe superclass-subclass hierarchy. The class "Business_Organization" has two subclasses, the class "Service_Provider" representing the organization offering the services and the class "Device_Provider" representing the organization selling devices. Property hasTrustedThirdParty states which service providers are trusted by a particular device provider. In order to facilitate the information acquirement function, a property Inverse_of_hasTrustedThirdParty is created as the inverse property of hasTrustedThirdParty. Properties such as isOwnedby and canBeManagedBy are also inverse properties of owns and canManage respectively.

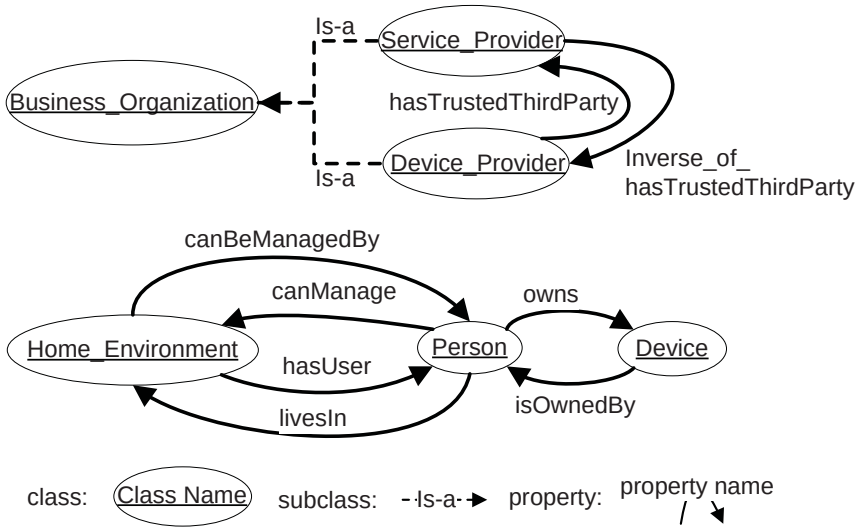


Figure 7.2: Main structure of the User and Business Domain Ontology.

Home Environment Ontology

The Home Environment Ontology is needed to describe the home environment, which includes descriptions of devices contained at home and services running on them. The main structure is illustrated in Figure 7.3. The Home Environment Ontology contains two main classes, the class "Home Environment" and the class "Device". Through an instance of the class "Home Environment" one can obtain information about a user's home, such as all devices used at home. The instance of the class "Device" represents a specific home device. For example it can be the user's washing machine. All individuals of the class "Device" are linked to the classes "Device_Model", "Device_Type", and "Device_Provider", by using hasDeviceModel isDeviceType and hasManufacturer properties respectively. The profile of a service could be interpreted as the classes and individuals the service is linked to. The profile of a service will be used to identify itself from others. The class "Device_Type" contains descriptions of devices' categories, which are used to distinguish devices, such as washing machine, oven or sensors, etc. The class "Device_Provider" contains the individuals of the device's manufacturer. The class "Device_Model" is further described by illustrating what kinds of hardware and software platform this device has. Such information helps verify whether certain software can be installed on a device or not. The class "System_Gateway" represents a software program running on a home PC, which is in charge of the gateway function between the HESKM system and the home devices, controlling the devices operating in the home environment. Because of the unique software functionalities, it is defined as a subclass of the class "Service". The Service ontology is described in the next section.

Service Ontology

The Service ontology is responsible for describing information needed for the service selection function of the HESKM system. The main structure of the Service ontology is illustrated in Figure 7.4. The class "Service" represents the home devices' software and the software which provides the functions that can be used by other software. The class "Service_Provider" represents service providers who issue the services. The class "Service_Description" represents the abilities of a service and

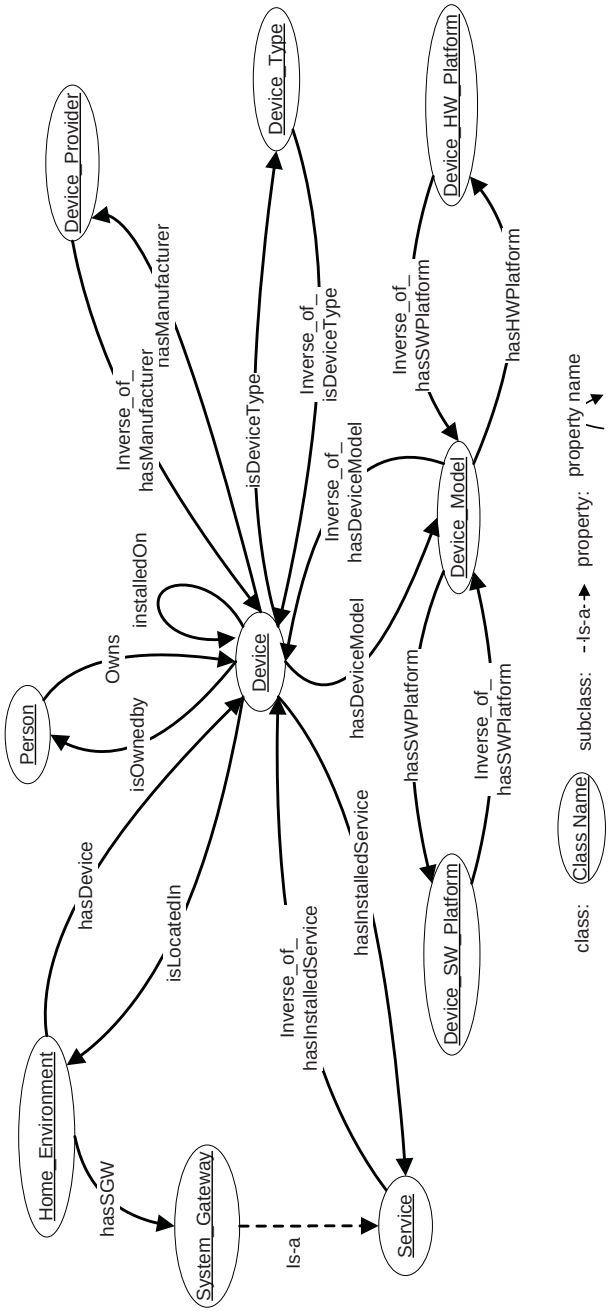


Figure 7.3: Main structure of the Home Environment Ontology.

what can be offered by a specific service. The property dependOn states the dependency between services, which tells to the system or the user that a certain sets of services should be installed before a specific service installation. There are three subclasses of the class "Service". The class "Available_Services" represents available software which can be installed on home devices to provide a new function or to update operations. The software is not only limited in home network scope, but also could be advertised by service providers through the Internet. Through the information of service Uniform Resource Locator (URL), the software can be accessed from local home network or downloaded from the Internet. The class "Available_Services" associated with the class "Device" through classes "Device_Type", "Device_Provider" and "Device_Model". Based on such information, the HESKM system can select the potential software for the devices based on users' requests or announce the available software for the devices. Furthermore, the consistent service deployment decisions made by the HESKM system are ensured. The class "Installed_Services" records the software that has already been installed on a specific home device, such as the cooking program installed on the oven. A device may have installed several services. The property hasInstalledService helps a home device record all the services that it has installed. Through the service descriptions of all the installed services and the specific functions of the device can be known.

7.4 Ontology Knowledge Inference

During the software configuration management procedure, the most intelligent and challenging task is to determine which software services need to be installed on devices, based on information stored in ontology. This section describes how the HESKM system uses the inference function of a reasoner to find out the potential services satisfying certain restrictions. The inference function and defined class have been introduced in Section7.2. Through combining "or" or "and" operators, the definitions of the defined classes can be the union or intersection of restrictions. Using the combination of conditions, the inference function of the reasoner has the ability to collect individuals which satisfy particular defined conditions under a defined class. How the HESKM system uses the inference function of reasoner will be explained in the following

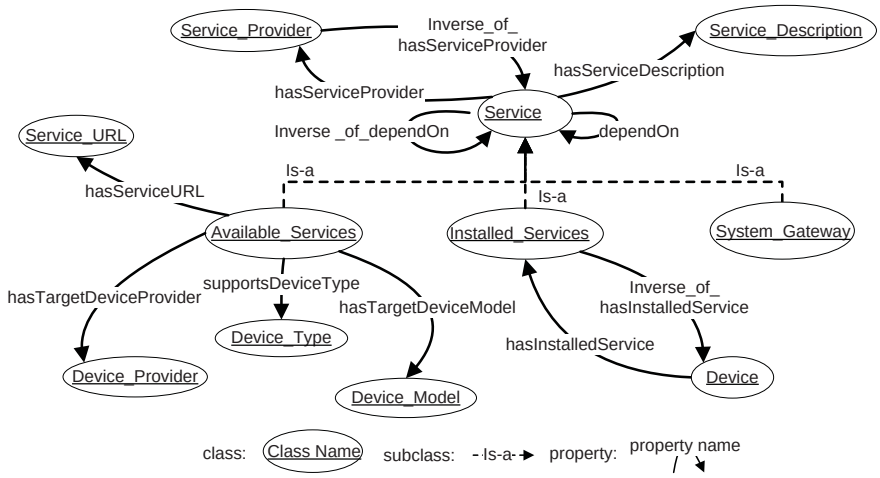


Figure 7.4: Main structure of the Service Ontology.

examples.

In a home environment, different available services can be represented as different individuals of the class "Available_Services". And the different relationships services participate in could be treated as different services' profiles. When the HESKM system requests a set of service individuals with specific requirements, a new defined class can be created using the corresponding requirements as the definition of the defined class to find the right collection of service individuals. An example is provided here. Figure 7.5 shows a small part of the HESKM ontology. Each service individual has two properties which present two different service profiles. Property hasTargetDeviceModel indicates which kind of device model the service should be installed on. Property hasServiceProvider specifies the service provider of the service.

It is assumed that a request wants to find out all available software services which can be installed on "device_model_y" and delivered by "company_x". Based on this specific request, a new defined class, named "InferredClass_BasedOn_Request", is created with the definition as shown in Figure 7.6. Figure 7.6(a) shows clearly that be-

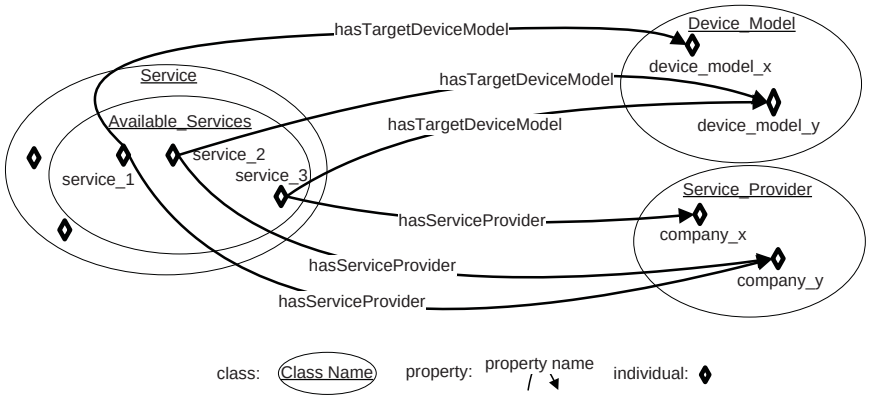


Figure 7.5: Parts of the HESKM Ontology used for illustrating the knowledge inference.

fore the reasoning the class "InferredClass_BasedOn_Request" is empty and all software services belong to the class "Available_Services". After reasoning, individual "service_3" is listed under the class "InferredClass_BasedOn_Reqest" as showed in Figure 7.6(b). This example shows that the reasoner collects all services which fulfill the definition of the class "InferredClass_BasedOn_Request" and lists them under the class "InferredClass_BasedOn_Request". In other words, reasoner finds out that individual "service_3" has the target device model of "device_model_y" and also it is delivered by "company_x". After the reasoning, the members of the class "InferredClass_BasedOn_Request", "service_3", is the required information for the request.

7.5 The Implementation of HESKM System Ontology

The ontology of the HESKM system firstly is designed via a Protégé-OWL editor, which provides a visual developing platform for modeling notologies. Secondly, the designed HESKM ontology is exported into a file which is formatted by Web Ontology Language (OWL). OWL

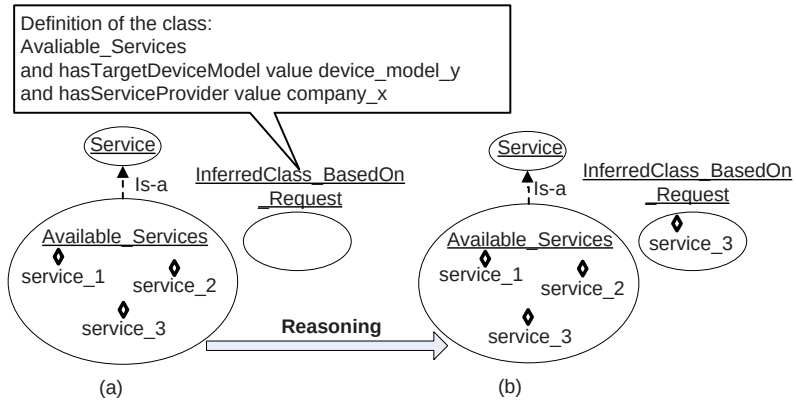


Figure 7.6: Result of using a reasoner.

is one of the standard ontology languages. It is endorsed by W3C to promote the Semantic Web vision. It is asserted that "An OWL ontology may include description of classes, properties and their instances. Given such an ontology, the OWL formal semantics specifies how to derive its logical consequences, i.e. facts not literally present in the ontology, but entailed by the semantics. These entailments may be based on a single document or multiple distributed documents that have been combined using defined OWL mechanisms" [72].

A Java application is implemented to access and manipulate the HESKM ontology. It is developed based on Protégé-OWL API, which provides classes and methods to load and save OWL files, to query and manipulate OWL data models, and to perform reasoning based on Description Logic engines [73]. Some examples of exchanging information with HESKM ontology are given in the next section.

7.6 Service Installation

When the system decides to install a service on a device, it is probably necessary to install some services first as preconditions. This relationship is called dependency and is represented by property dependOn in the Service ontology. Under most circumstances, the precondition ser-

vices are also dependent on other services, which construct a service dependency hierarchy. The system should first install a service which locates in the leaf position of the service dependency hierarchy and is not depended on any other services.

Firstly, how to use java program to query the services' dependencies is explained. The related parts of the programming are shown in Figure 7.7.

```
OWLModel owlModel = ProtegeOWL.createJenaOWLModelFromURI(HESKM_ONTOLOGY_URI);          (1)

OWLIndividual target_individual = owlModel.getOWLIndividual( "S_1" );                  (2)

OWLObjectProperty  property = owlModel.getOWLObjectProperty("dependOn");               (3)

Collection results = target_individual.getPropertyValues(property);                    (4)
```

Figure 7.7: Programming to query the service dependency of service "S_1".

The first line of the programming defines a OWLModel which provides access to the resources in the ontology. The returned object can be used to do specific operation, such as create, query or modify to the linked ontology. The HESKM ontology is indicated by the variable HESKM_ONTOLOGY_URI. The individuals in the ontology can be accessed by using the code in line 2. For example, the service dependency of the service "S_1" is wanted to be queried. Then the name of "S_1" is set as argument to be passed to the function in line 2. The property dependOn is accessed by the function in line 3. All the services which the service "S_1" depends on will be collected in a collection variable, results, based on code in line 4.

However, using the query does not solve the problem that which service should be installed first, so the installation sequence has to be calculated. The installation sequence of service dependency hierarchy is calculated by the method proposed in this section. The method is explained by using an example of service dependency hierarchy illustrated in Figure 7.8(a). This hierarchy tree describes a complete hierarchy relationship between all the involved services. Lower levels are referred to the levels closest to leafs of the tree, and higher levels are referred to

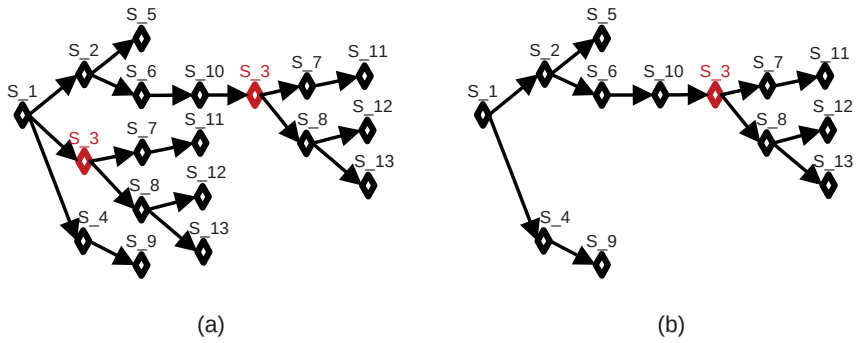


Figure 7.8: Service dependency hierarchy tree of "S_1".

levels closest to "S_1". The dependency hierarchy can be obtained by using the dependency query (Figure 7.7) for each service. The easiest way of calculating the installation sequence is to list all the services of the hierarchy tree from the leaf to the root. However, it is worth noticing that some services would be listed and therefore installed more than once, since a service could be depended by more than one service and those services would probably not have the same depth in the hierarchy tree. For example, all the services on the sub-tree with root "S_3". To solve this problem, a method to calculate the installation sequence without duplicates is designed. The method is divided into two steps. Firstly, the service dependency hierarchy is calculated and represented in a Services Relationship Matrix (SRM), aiming at finding the lowest level parent of each service. For example, "S_3" is found twice in hierarchy tree and has "S_1" and "S_10" as parent services. "S_3" has to be installed before "S_1" and "S_10" are installed, and as "S_10" has a lower level than "S_1", it is only interested in keeping "S_10" as a parent of "S_3". Secondly, based on the content of SRM, the installation sequence is calculated.

The pseudo code of the first step is illustrated in Figure 7.9. This step starts by introducing the target service, "S_1", which is also the root service and has no parent into the SRM. SRM has as many rows as

services to be installed and two columns: the first column is the service itself, and the second column is the parent of this service. For "S_1", as it is the root service, the second column is represented by Null. Then the dependency query is executed and the direct dependencis of "S_1" are returned in an array. The services in the array are introduced in the SRM, since find temp_result_array[j] in Matrix_Relation will return -1 for this first loop. The SRM matrix at this point will be as illustrated in Figure 7.10. Then the dependencies of the services in the array [S_2, S_3 and S_4] will be calculated, and so on.

Before inserting the service information into SRM, the function find temp_result_array [j] in Matrix_Relation checks whether a service is already in the SRM or not. If it is, that means the dependency query has already been done during the upper depth level of the tree, so the dependencies do not need to be queried again. However, for this case, the parent information in the SRM has to be updated as this service is founded out to be depended by another service with lower depth level. The calculation keeps running until the services do not have any more dependencies. And the tailored tree of the previous example is illustrated in Figure 7.8(b).

The second step is to calculate the installation sequence. The pseudo code of this step is shown in Figure 7.11. Since there is no redundant service in the SRM, the services are taken from this SRM and inserted to the installation sequence list from root to leaf. So the first service to be installed is found at the end of installation sequence list and the last service to be installed is in position zero. As services are copied from the SRM to the installation sequence list, they are deleted from the SRM to reduce the loops in the algorithm and make it more efficient.

7.7 Summary

This chapter describes the ontology technology and reasoner tool used by the HESKM system. In order to help the HESKM system to be aware of states of home environment and relationships between all the components of a home environment, a knowledge base is constructed by ontology. The HESKM ontology consists of three parts. The User and Business Domain Ontology represents the family members and business entities, which helps organize and exploit information related to

```
CaculateRelation(Service service_v)
{
   Service[]  Temp_Array_1 = { service_v };
   Service[]  Temp_Array_2;
   Service[][]  Matrix_Relation;
   Matrix_Relation[0][0] = service_v;
   Matrix_Relation[0][1] = null;
   m = 1;
   while(Temp_ Array_1 is not empty)
   {
      for(i = 0;  Temp_Array_1[i] != null;  i++ )
      {
         Service []  temp_result_array = QueryDependencies (Temp_Array_1[i]);
         for(j = 0;  temp_result_array[j] != null;  j++)
         {
            K = find temp_result_array[j] in Matrix_Relation;
            if(k != -1)
            {
               Matrix_Relation[k][1] = Temp_Array_1[j];
            }
           else
           {
               Matrix_Relation[m][0] = temp_result_array[j];
               Matrix_Relation[m][1] = Temp_Array_1[i];
               Add temp_result_array[j] to Temp_Array_2;
               m++;
           }
         }
       }
       Temp_Array_1 = Temp_Array_2;
       Temp_Array_2 = null;
   }
}
```

Figure 7.9: Pseudo code to construct the SRM.

business relationships, and family members' relationships with home environment. The Home Environment Ontology describes home environment, which includes descriptions of devices installed at home and services running on them. Through an instance of the class "Home Environment" one can obtain information about a user's home. The Service

$$SRM = \begin{bmatrix} S\_1 & Null \\ S\_2 & S\_1 \\ S\_3 & S\_1 \\ S\_4 & S\_1 \end{bmatrix}$$

Figure 7.10: A temporary stage of the SRM.

ontology is responsible for describing information needed for service selection function of the HESKM system. The information includes service dependencies, relationships between services and devices and relationships between services and service profile descriptions. Furthermore, a reasoner tool is applied by the HESKM system. The consistency of the ontology information is fully ensured by using the checking consistency function of a reasoner. The reasoner's inference function computes the inferred class hierarchy, which collects individuals satisfying particular defined conditions. By converting the user or system requests to the definition of a specific defined class, potential available services could be found under an inferred class hierarchy, which greatly assist the HESKM system to provide software management services across home environments. Through implementing the proposed strategy which calculates the sequence of service dependency hierarchy, correct service deployment decisions are ensured and the compatibility among diverse services is maintained.

```
Service[] Install_Sequence[0] = Matrix_Relation[0][0];
Delete the row of Matrix_Relation [0][];
Shift the rows of Matrix_Relation up;
Int count =1;
While(Matrix_Relation is not empty)
{
   For(j=0;  j< Install_Sequence.length;  j++)
   {
      i = 0;
      While(i < number of rows of the Matrix_Relation)
      {
        If (Install_Sequence [j] == Matrix_Relation [i][1])
        {
           Install_Sequence[count] = Matrix_Relation [i][0];
           count ++;
           Delete the row of Matrix_Relation [i][];
           Shift the rows of Matrix_Relation up;
        }
        else
        {
          i++;
        }
      }
   }
}
```

Figure 7.11: Pseudo code to calculate the installation sequence.

Chapter 8

Conclusions and Outlook

Networks and networked services have become increasingly critical and fundamental demands of our society. A failure or even a small service disruption can result in significant cost with serious consequences to business organizations and people's lives. This thesis addresses the challenges of providing survivability to transport networks and ensuring reliable transport services to users.

The research efforts have not only focused on the large scale networks, but also on some networks serving for particular purposes. An avionic transport network and a home network have been well studied and the research work is presented.

Providing reliable multicast services on MPLS-TP ring networks has been investigated in Chapter 3 and Chapter 4. As the results of investigation and comparison between the schemes introduced by ITU and IETF for MPLS-TP multicast ring protection, two novel MPLS-TP ring protection schemes have been proposed, the Sub-Path Maintenance Entity based Wrapping (SPME-based Wrapping) protection scheme and the Sub-Path Maintenance Entity based Ring Optimized Multicast Wrapping (SPME-based ROM-Wrapping) protection scheme. The SPME-based Wrapping protection scheme is able to keep the advantages of the traditional wrapping scheme and at the same time simplifies the operations of protection actions by employing the tunnels. The deployment of the proposed SPME-based ROM-Wrapping protection scheme does not need to disturb any traditional MPLS-TP multicast services on ring structure. Compared to the ROM-Wrapping pro-

tection scheme, the complicated LSP-based protection reconfigurations are reduced by implementing the shared protection tunnels, and at the same time the LSP identities inside the tunnels are maintained under protection situation by utilizing the RLTC method, providing network carriers the ability to deploy finer granularity traffic engineering. Furthermore, the protection label consumptions are greatly reduced in the SPME-based ROM-Wrapping protection scheme, fulfilling the requirements for adopting ring networks. However, the SPME-based ROM-Wrapping protection scheme uses more protection bandwidth than the ROM-Wrapping protection scheme, the protection hop counts are managed to remain the same.

Furthermore, the studied SPME-based Steering and the proposed SPME-based ROM-Wrapping protection schemes have been extended onto interconnected-ring topologies. The extensions contribute to the development of MPLS-TP technology according to the requirements suggested by IETF and ITU standards. The extensions also enhance the applicability of ring networks. The implementations of multicast services and protection switching procedures on interconnection parts between different rings have been well investigated and described through the thesis. Under both protection schemes, the bandwidth requirements for delivering the multicast traffic are the same. On each local ring, the SPME-based Steering protection scheme requires less protection bandwidth than the SPME-based ROM-Wrapping protection scheme. However, the SPME-based Steering protection scheme employs the 1+1 protection method, which brings much more traffic burden and consumes more power under failure free situation. On the other hand, SPME-based ROM-Wrapping adopts 1:1 protection method. Under failure free situation, the traffic burden and power consumption are greatly reduced, and the reserved protection bandwidth can be used for extra traffic transmission to increase the efficiency of resource utilization. Compared to the SPME-based Steering protection scheme, the SPME-based ROM-Wrapping protection scheme needs fewer number of OAM entities for deploying protections.

Taking the advantages of key terrestrial optical transport network technologies, in Chapter 5, a generic ring transport network for avionic systems has been proposed. It contributes to designing a state-of-art anionic optical network to fulfill the increasing demands for transmis-

sion speed and capacity, and at the same time to avoid the problems, such as overweight, complexity and lack of security faced by the expending copper cable on-board system networks. The utilization of the fiber switching, the wavelength division multiplexing, and the packet switching techniques provides different degrees of configuration and offers great flexibility to segregate and deploy diverse systems according to their security and bandwidth requirements. Based on the proposed avionic transport network, a point-to-point and a point-to-multipoint services have been implemented, which can be used as standard services to support various avionic systems. Furthermore, three redundancy schemes with different levels of reliability and cost have been introduced to ensure the reliability of the proposed generic avionic transport network.

Chapter 6 has dealt with the issue of fulfilling the isolation requirements of avionic systems with different security levels, and at the same time finding the minimum cost solution in terms of wavelength and fiber consumption on the avionic optical transport network. The maximum number of wavelengths allowed in one fiber has also been taken into account when wavelengths are assigned into fibers. The system isolation requirement is referred to as the traffic fiber partition (TFP) constraint. The graph theory methods were adopted to find the minimum amount of required wavelengths and fibers for a fixed system route configuration. By adapting the procedures of the graph methods, it has been managed to fulfill the TFP constraints when solving the minimum cost solution. The simulated annealing approach was employed to find a better solution among randomly changed system route configurations. Within each step of the simulated annealing process, one system route is changed, aiming at achieving a solution which uses fewer wavelengths. A novel perturbation mechanism, TFP constraints aware - maximum loaded link perturbation (TFP-MLL-P) mechanism, has been proposed to choose the candidate route based on current configuration information of all routes, wavelength-continuity (WC) and TFP constraints. Compared to Random Route Perturbation (RR-P) mechanism, a wide range of case-based experiments have been carried out under various traffic scenarios and on networks with different sizes and with different network loads. The results have proved that, with slightly increased calculation time, the proposed route perturbation mechanism works more efficiently and manages to give optimized results in most of the test cases.

From the simulations, it has also been found out that the increase of the wavelength consumption is mainly resulted from the increase of the WC constraints when the percentage of the TFP constraints is low, only after the TFP constraints increasing to a certain large stage, the amount of used wavelengths starts to grow fast due to the increase of the TFP constraints. On the other hand, the fiber consumption is mainly because of the increase of the TFP constraints.

Chapter 7 has proposed a Home Environment Service Knowledge Management (HESKM) system, which manages the whole information of a home environment and helps all software configure and update procedures across multivendor environments. It contributes to developing a home network with intelligent functions to help the family members in daily house work and provide software and device vendors a better solution for home environments. A knowledge base is constructed by ontology technology to store information of the home environment in terms of members, devices, services and the relationships among them. By applying the reasoner tool, the consistency among different parts of the ontology information is fully ensured. Through converting the user or system requests to the definition of a specific defined class, potential available services can be found by the reasoner's inference function, which greatly assists the HESKM system to provide software management services across home environments. Through the proposed strategy to calculate the sequence of service dependency hierarchy, correct service deployment decisions are ensured and the compatibility among diverse services is maintained.

The research work presented in this thesis provides guidance and references to the future research in transport networks, avionic system networks and home networks. Some potential research work is listed below. First, based on interconnected-ring networks, it is interesting to compare the efficiency of the local-ring based protection schemes with the protection schemes which pre-configure protection paths crossing multiple rings. Second, implementing or simulating an avionic system, such as on-board entertainment system on the proposed generic avionic transport network could be a future work in the DAPHNE project. Regarding to the work of performing network optimization, the TFP constraints could be further dealt with on the networks which allow wavelength conversion. Third, in a home environment, the functions with some levels of

intelligence would be interesting to investigate. For example, based on certain energy saving strategy and a list of house work, different tasks can be automatically triggered at the proper time and on the proper mode.

Bibliography

[1] **J. Zhang**, R. Fu, H. Yu, S. Ruepp, M. S. Berger, and L. Dittmann, "Two novel tunnel-based ring protection switching for MPLS-TP multicast services," in *IEEE 18th International Conference on Telecommunications (ICT)*, 2011.

[2] **J. Zhang**, A. Yi, M. S. Berger, C. Peucheret, and A. Clausen, "Developing a generic optical avionic network," in *IEEE 18th International Conference on Telecommunications (ICT)*, 2011.

[3] **J. Zhang**, A. Rosselló-Busquet, J. Soler, M. S. Berger, and L. Dittmann, "Home environment service knowledge management system," in *IEEE 11th International Conference on Telecommunications (ConTEL 2011)*, 2011.

[4] **J. Zhang**, M. S. Berger, and S. Ruepp, "Flow-based end-to-end OAM functions for the multicast service on the MPLS-TP ring network," in *IEEE International Conference on Communications (ICC)*, 2010.

[5] A. Rasmussen, **J. Zhang**, H. Yu, R. Fu, S. Ruepp, H. Wessing, and M. S. Berger, "High capacity carrier Ethernet transport networks," in *4th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CISST'10)*, 2010.

[6] S. Ruepp, H. Wessing, **J. Zhang**, A. Manolova, A. Rasmussen, L. Dittmann, and M. S. Berger, "Providing resilience for carrier Ethernet multicast traffic," in *4th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CISST'10)*, 2010.

[7] M. Barkauskaite, **J. Zhang**, H. Wessing, M. S. Berger, and S. Ruepp, "Modeling of reliable multicasting services," in *OPNETWORK 2010*, 2010.

[8] **J. Zhang**, M. S. Berger, and S. Ruepp, "Resilient MPLS-TP multicast service based on an interconnected-ring structure," in *OPNETWORK 2010*, 2010.

[9] S. Ruepp, H. Wessing, **J. Zhang**, A. V. Manolova, A. Rasmussen, L. Dittmann, and M. S. Berger, "Evaluating multicast resilience in carrier Ethernet," *WSEAS Transactions on Circuits and Systems*, vol. 9, pp. 101–110, 2010.

[10] A. Rasmussen, **J. Zhang**, H. Yu, R. Fu, S. Ruepp, H. Wessing, and M. S. Berger, "Towards 100 gigabit carrier Ethernet transport networks," *WSEAS Transactions on Circuits and Systems*, vol. 9, pp. 153–164, 2010.

[11] R. Fu, **J. Zhang**, and M. S. Berger, "Enhanced BRPC routing procedure for PCE based inter-domain routing," in *International conference on Communictions (ICCOM'10)*, 2010.

[12] **J. Zhang**, S. Ruepp, M. S. Berger, and H. Wessing, "Protection for MPLS-TP multicast services," in *IEEE Design of Reliable Communication Networks (DRCN 2009)*, 2009.

[13] N. Ploskas, M. S. Berger, **J. Zhang**, and L. Dittmann, "Ontology for software configuration management : A knowledge management framework for software configuration management," in *3rd International Conference on Software and Data Technologies (ICSOFT 2008)*, 2008.

[14] N. Ploskas, M. S. Berger, **J. Zhang**, and G.-J. Wintterle, "A knowledge management framework for software configuration management," in *32nd Annual IEEE International Computer Software and Applications (COMPSAC 08)*, 2008.

[15] **J. Zhang**, Y. An, M. S. Berger, V. B. Iversen, and L. Dittmann, "Solving fiber partition constraints in MC-RWA of WDM ring networks," *IEEE Communications Letters*.

[16] **J. Zhang**, Y. An, M. S. Berger, and A. T. Clausen, "Wavelength and fiber assignment problems on avionic networks," in *Avionics, Fiber-Optics and Photonics Technology Conference 2011*, 2011.

[17] **J. Zhang**, J. Wang, A. Zakrzewska, A. Rasmussen, A. Manolova, H. Yu, Y. Yan, S. Ruepp, and M. S. Berger, "Protection schemes on interconnected-ring topology for MPLS-TP multicast services," *IET*.

[18] TPACK, *PBT Carrier Grade Ethernet Transport*.

[19] B. Napier, "Developing aircraft photonic networks," *Project Description*, 2008.

[20] ITU-T Recommendation G.805, *Generic functional architecture of transport networks*, 2000.

[21] IETF RFC 3031, *Multiprotocol label switching architecture*, 2001.

[22] ITU-T Recommendation G.8110/Y1370, *Generic functional architecture of transport networks*, 2005.

[23] ITU-T Recommendation G.8110.1/Y.1370.1, *Architecture of Transport MPLS (T-MPLS) Layer Network*, 2006.

[24] ITU-T Recommendation G.8121/Y.1381, *Characteristics of Transport MPLS equipment functional blocks*, 2006.

[25] ITU-T Recommendation G.8112/Y.1371, *Interfaces for the Transport MPLS (T-MPLS) hierarchy*, 2006.

[26] IETF RFC 5654, *Requirments of an MPLS Transport Profile*, 2009.

[27] IEEE Standard 802.1D, *IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Bridges*, 2004.

[28] IEEE Standard 802.1Q, *IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks*, 2006.

[29] IEEE Standard 802.1ad, *IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks Amendment 4: Provider Bridges*, 2006.

[30] IEEE Standard 802.1ag, *IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management*, 2007.

[31] IEEE Standard 802.1ah, *IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks Amendment 6: Provider Backbone Bridges*, 2007.

[32] IEEE Standard 802.1Qay, *IEEE Standard for Local and metropolitan area networks Virtual Bridged Local Area Networks - Amendment: Provider Backbone Bridge Traffic Engineering*, 2007.

[33] IETF, *Operations, Administration and Maintenance Framework for MPLS-based Transport Networks (draft-ietf-mpls-tp-oam-frmework-11)*, 2011.

[34] IETF draft standard, *MPLS-TP Ring Protection Switching (MRPS)*, 2010.

[35] IETF draft standard, *Multiprotocol Label Switching Transport Profile Ring Protection*, 2010.

[36] IETF, *MPLS-TP Ring Protection draft-weingarten-mpls-tp-ring-protection-02*, 2009.

[37] IETF, *MPLS-TP Ring Protection draft-weingarten-mpls-tp-ring-protection-03*, 2010.

[38] IETF, *MPLS-TP Ring Protection draft-weingarten-mpls-tp-ring-protection-04*, 2010.

[39] IETF RFC 5331, *MPLS Upstream Label Assignment and Context-Specific Label Space*, 2008.

[40] IETF RFC 4427, *Recovery (Protection and Restoration) Ternimology for GMPLS*, 2006.

[41] IETF RFC 2205, *Recovery (Resource Reservation Protocol (RSVP) - Functional Specifications*, 1997.

[42] DAPHNE project, *http://www.fp7daphne.eu/Documents/DAPHNE Project overview leaflet.*

[43] Draka, *Draka private communications.*

[44] G. P. Agrawa, *Fiber-optic communication systems.* John Wiley & Sons, 1997.

[45] C. R. et al, "Dwdm 40g transmission over trans-pacific distance (10000km) using csrz-dpsk, enhanced fec, and all-raman-amplified 100-km ultrawave fiber spans," *Journal of Lightwave Technology*, vol. 22, p. 203, 2004.

[46] ISO 11898, *CAN physical layer standards.*

[47] ARINC 664, *ARINC 664, Aircraft Data Network, Part 7 - Avionics Full Duplex Switched Ethernet (AFDX) Network.*

[48] N. Charbonneau and V. M. Vokkarane, "Multicast advance reservation RWA heuristics in wavelength-routed networks," in *IEEE GLOBECOM*, pp. 1–6, 2010.

[49] X. H. Jia, X. D. Hu, L. Ruan, and J. H. Sun, "Multicast routing, load balancing, and wavelength assignment on tree of rings," *IEEE Communication Letters*, vol. 6, pp. 79–81, 2002.

[50] L. Wuttisittikulkij and M. J. O'Mahony, "Design of the optical layer in multiwavelength cross-connected networks," *IEEE J. Select. Areas Commun.*, vol. 14, pp. 881–892, 1996.

[51] D. R. Din, "Heuristic and hybrid methods for solving optimal multiple multicast problem on WDM ring network," *Telecommunication Systems*, vol. 28, pp. 245–262, 2005.

[52] T. Lee, K. Park, J. Yang, and S. Park, "Optimal multicast routing and wavelength assignment on WDM ring networks without wavelength conversion," *IEEE Communications Letters*, vol. 11, pp. 898–900, 2007.

[53] L.Wuttisittikulkij and M. O'Mahony, "Design of an efficient and practical algorithm for wavelength assignment in multi-wavelength ring transport networks," in *Global Telecommunications Conference, GLOBECOM '97*, pp. 571–575, 1997.

[54] D. R. Din, "A hybrid method for solving ARWA problem on WDM network," *Computer Communications*, vol. 30, pp. 385–395, 2007.

[55] D. Abramson and M. Randall, "A simulated annealing code for general integer linear programs," *Annals of Operations Reserch*, vol. 86, pp. 3–21, 1999.

[56] J. Baptista, S. Silva, C. Stace, N. Reimers, U. Stender, and A. Lay, "Deliverable d2.1 high level specification for daphne networks," *Project Deliverable*, 2009.

[57] L. Foulds, *Graph Theory Applications*. Springer-Verlag, 1991.

[58] C. Bron and J. Kerbosch, "Algorithm 457: Finding all cliques of an undirected graph," *Communications of the ACM*, vol. 16, pp. 575–577, 1973.

[59] D. Matula, G. Marble, and J. Isaacson, "Graph coloring algorithms," *Graph Theory and Computing,Academic Press, New York*, pp. 109–122, 1972.

[60] X.-H. Jia, D.-Z. Du, X.-D. Hu, M.-K. Lee, and J. Gu, "Optimization of wavelength assignment for QoS multicast in WDM networks," *IEEE Transactions on Communications*, vol. 49, pp. 341–350, 2001.

[61] I. Osman, "Heuristics for the generalised assignment problem: simulated annealing and tabu search approaches," *OR Spektrum*, vol. 17, pp. 211–225, 1995.

[62] M. Randall, G. McMahon, and S. Sugden, "A simulated annealing aprroach to communication network design," *Journal of Combinatorial Optimization*, vol. 6, pp. 55–65, 2002.

[63] R. V. Vidal, *Applied Simulated Annealing*. Spring-Verlag, 1993.

[64] M. Lundy and A. Mees, "Convergence of an annealing algorithm," *Mathematical Programming*, pp. 111–124, 1986.

[65] D. T. Connolly, "An improved annealing scheme for the QAP," *European Journal of Operational Research*, vol. 46, pp. 93–100, 1990.

[66] E. Yetginer, Z. Liu, and G. Rouskas, "RWA in WDM rings: An efficient formulation based on maximal independent set decomposition," in *2010 17th IEEE Workshop on Local & Metropolitan Area Networks (LANMAN)*, pp. 1–7, 2010.

[67] COMANCHE Project, *http://www.ist-comanche.eu/*.

[68] E. Meshkova, J. Riihijarvi, P. Mahonen, and C. Kavadias, "Modeling the home environment using ontology with applications in software configuration management," in *15th International Conference on Telecommunications (ICT 08)*, 2008.

[69] M. Berger, L. Dittmann, M. Caragiozidis, N. Mouratidis, and C. K. M. Loupis, "A component-based software architecture - reconfigurable software for ambient intelligent networked services environments," in *The 3rd International Conference on Software and Data Technologies (ICSOFT 2008)*, 2008.

[70] A. K. Dey, "Understanding and using context," *Personal and Ubiquitous Computing*, vol. 5, pp. 4–7, 2001.

[71] *Protégé-OWL API Programmer's Guide*, 2010.

[72] OWL Web Ontology Language Guide, *W3C,http://www.w3.org/TR/2004/REC-owl-guide-20040210/*.

[73] ProtégéOWL API Programmers Guide, *http://protegewiki.stanford.edu/wiki/*.