Bounded-Flooding Algorithm Considering Differentiated QoS and QoP in the Next Generation Optical Virtual Private Network

차세대 광가상사설망에서 차등화된 **QoS** 및 **QoP**를 고려한 제한적 플러딩 라우팅 알고리즘 연구

Advisor: Prof. Sang-Un Kim

by

Jin-Ho Hwang

A thesis submitted in partial fulfillment of the requirements

for the degree of

Master of Engineering

in the Department of Telematics, The Graduate School,

Pukyong National University

August 2005

황진호의 공학석사 학위논문을 인준함

2005년 8월 31일

주 심 공학박사 하 덕 호 (인)

위 원 공학박사 박 규 칠 (인)

위 원 공학박사 김 성 운 (인)

Bounded-Flooding Algorithm Considering Differentiated QoS and QoP in the Next Generation Optical Virtual Private Network

A Dissertation

by

Jin-Ho Hwang

Approved as to style and content by :

Deockho Ha

(Chairman) Deock-Ho Ha

Kyu Chil Park

(Member) Kyu-Chil Park

(Member) Sung-Un Kim

August 31, 2005

CONTENTS

LIST OF FIGURES

LIST OF TABLES

Bounded-Flooding Algorithm Considering Differentiated QoS and QoP in the Next Generation Optical Virtual Private Network

Jin-Ho Hwang

Department of Telematics Engineering, The Graduate School
Pukyong National University

Abstract

A Routing algorithm considering differentiated QoS (Quality of Service) and QoP (Quality of Protection) has been seen as crucial network property in the next generation optical virtual private network based on DWDM networks. This thesis proposes a new routing algorithm, called bounded flooding routing (BFR) algorithm which can meet differentiated QoS requirements. Primarily, the BFR algorithm tries to reduce network overhead by accomplishing bounded-flooding to meet QoS and QoP requirements, and improve blocking probability and wavelength utilization by restricting the number of wavelength for distribution of network traffics. Also, as one effort to improve routing performance, we introduce a new concept, ripple count scheme, which does not need any link-state information and computational process. Moreover, for extensive analysis and simulation study, as a critical concern in DWDM-based networks, we deploy limited wavelength conversion capability within OVPN nodes. And the simulation results demonstrate that the BFR algorithm is superior to other predominant routing algorithms (both original flooding method and source-directed methods) in terms of blocking probability, wavelength channels required and overhead. Also, with the proposed BFR algorithm under pre-specified QoP requirements, a parallel searching scheme can guarantee dependable connections rapidly by making a primary path and a backup path in a parallel way. And by considering concepts of shared risk link group (SRLG) and trap avoidance (TA) problem, the BFR algorithm makes better for survivability ratio.

Ⅰ. Introduction

While coping with the rapid growth of IP and multimedia services, current Internet based on time division multiplexing (TDM) cannot supply sufficient transmission capacity for high bandwidth-needed services. However, the huge potential capacity of one single fiber, which is in Tb/s range, can be exploited by applying DWDM technology which transfers multiple data streams on multiple wavelengths simultaneously. So, DWDM-based optical networks have been a favorable approach for the next generation optical backbone networks [1].

In DWDM backbone networks, the problem of setting up a lightpath is generally called routing and wavelength assignment (RWA) [2-3] and the RWA plays an important role in improving the global efficiency for resource utilization. Moreover, the current multimedia applications involve real time-intensive traffics with various QoS (Quality of Service) requirements (multi-constraint). So, one of the key issues is QoS RWA that is not only selecting a path and assigning a wavelength but also enabling resource reservation and admission control by considering multi-constraint QoS requirements. That is, data flows are consistent with service requirements of the traffic and service restrictions of the network.

Though the multi-constraint QoS RWA has been regarded as a vital mechanism to support real-time multimedia communications, finding a qualified path meeting the multiple constraints is a multi-constraint optimization problem, which has been proven to be NP-complete [4] and cannot be solved by a simple algorithm. The majority of previous works [3-5] in DWDM networks has viewed QoS routing as an extension of the current Internet routing paradigm where nodes exchange QoS states through in-band or out-of-band control channel. Basically, there are two common approaches to QoS routing: source-directed and flooding-based.

In the source-directed approach (also called link-state routing) [3,6], the source node selects a path based on each connection's traffic requirements and available resources in the network. In this scheme, periodic or triggered distribution of link-state information is deployed. However, because of its high operational overhead in distributing and maintaining link-state information, source-directed routing may not scale well. And possibly, this approach can yield inaccurate route computation when inaccurate link-state information is used for QoS routing. So, even current researches for QoS routing are based on source-directed method due to its easy controllable characteristics, the source-directed approach is impractical and unattractive.

On the other hand, in flooding-based QoS routing approach, local nodes are not required to keep link-state information for the entire network [4,7-8]. The source node simply broadcasts each connection request message to its neighbors, which then relay the message to their neighbors, and so on, until the message reaches the destination. In order to limit the number of request messages, the algorithm does not flood through a link which is found unable to guarantee the connection's QoS. Although this approach incurs considerable operational overhead due to the large number of request messages, it still has its own merits as follows. First, there is no need for disseminating link-state information and calculating shortest paths, thus reducing operational overhead and implementation complexity. Second, nodes are not required to maintain the database of link-state information, thus saving space and time to store and process the information. Third, information kept for each local link is used to determine whether it can accommodate a new connection or not, the algorithm can always find a qualified route, if any, thereby outperforming link-state routing in terms of connection blocking probability ratio. This aspect will be more pronounced when the network is unstable or the size of network is large. Finally, for dependable real-time connections which need a primary path and a backup path, parallel path search scheme shortens the connection set-up time and improves survivability (restorability) ratio by considering shared risk link group (SRLG) and trap avoidance (TA) problem which are essential constraint in DWDM-based networks.

In this paper, we propose a flooding-based QoS routing algorithm called bounded flooding routing (BFR) algorithm which incurs much lower message overhead yet yields a good connection establishment success rate (blocking probability), as compared to the existing flooding-based algorithms and also source-directed methods. In order to reduce and bound the flooding overhead, we introduce the new ripple-count concept which can classify incoming messages into three types and determine whether the message is necessary or not through simple comparison without state information and operational process. And with the proposed BFR algorithm under pre-specified QoP requirements, a parallel searching scheme can guarantee dependable connections rapidly by making a primary path and a backup path in a parallel way. And by considering concepts of shared risk link group and trap avoidance problem, the BFR algorithm makes better for survivability ratio.

The rest of the paper is organized as follows: Section 2 presents OVPN reference model and preliminary RWA researches and section 3 describes ripple-count concept and BFR algorithm including analysis of QoS and QoP requirements. Moreover, as an important factor in OVPN networks, we consider limited wavelength conversion capability in OVPN nodes for extensive views in simulation. And in section 4, with the proposed BFR algorithm, we show how to guarantee dependable connections in a parallel way according to differentiated QoP. Thereafter, using extensive simulations, the proposed and other existing algorithms are comparatively evaluated in section 5. Finally, some concluding remarks are made in section 6.

Ⅱ. Preliminary RWA Researches in OVPN

1. OVPN Reference Model

The suggested OVPN structure is composed of customer sites in the electric control domain and the GMPLS (Generalized Multi-Protocol Label Switching)-based DWDM backbone network in the optical control domain. The external customer site is an IP network [9]. It aggregates IP packets, which have the same QoS and QoP level at the client edge nodes (CE) to reduce network complexity and to make operations simple. The internal OVPN backbone network is a DWDM network based on GMPLS. It consists of the provider edge nodes (PE) and the provider core nodes (P), and it forwards data traffic from the customer sites without electronic-optic-electronic (E-O-E) conversions. There is a traffic policy server (TP server) for supporting differentiated QoS and QoP among customer sites. It negotiates service level agreement (SLA) parameters describing the service level between customer site and the OVPN backbone network. And, it sets an optical path according to the negotiated parameters. In this way, it can manage the entire network to support the service that satisfies the SLA through the optical path between end users.

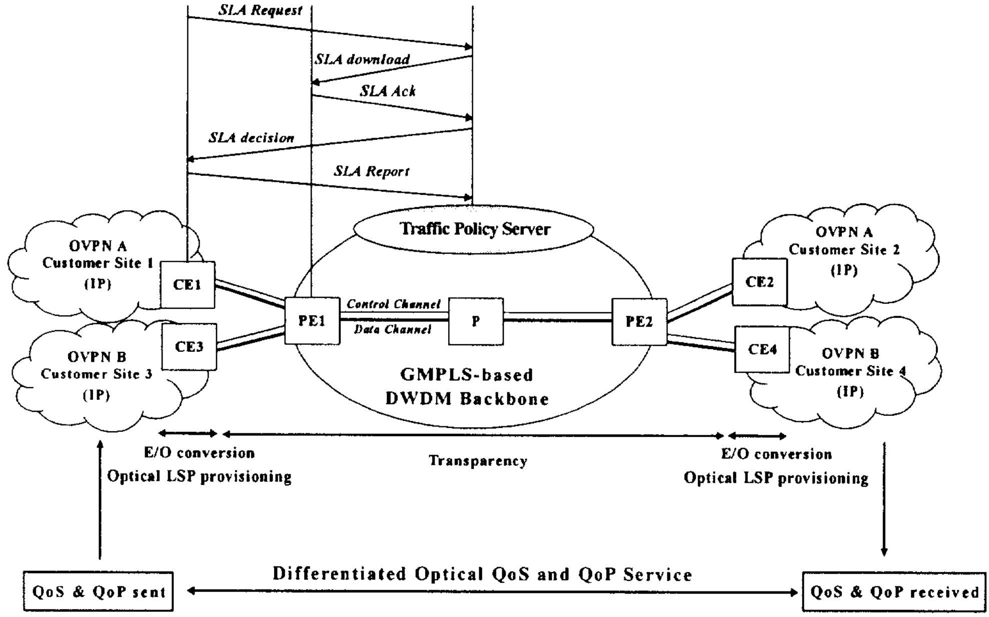


Figure 1. OVPN Reference model

The procedure of SLA negotiation between the customer site and the traffic policy server is presented in Figure 1. A CE node at the customer site sends a SLA request that specifies the source and destination IP addresses, the customer port identifier (CPI) and provider port identifier (PPI), the aggregated IP flow information, bandwidth, and QoS and QoP parameters. When the traffic policy server receives this request, it verifies the agreements of the traffic contract that was negotiated with the OVPN. If it satisfies the existing traffic contract, then the traffic policy server downloads the SLA parameters onto the policy agent in the appropriate ingress PE to request a SLA allowance decision. The PE node calculates the QoS and QoP guaranteed path, and if it satisfies the demanded bandwidth and specific parameters in all the nodes of the path, then the SLA is accepted. If the traffic policy server receives a return message that the SLA parameters have been accepted by the PE node, then it informs the ingress CE node to negotiate the SLA between the electronic and optic control domains [9].

2. GMPLS Operation in OVPN

To initiate the OVPN operation based on the GMPLS control protocol, one or more bi-directional control channels in which control-flows operate have to be activated. The control channels can be used to exchange control-plane information such as link provisioning and fault management information, path management and label distribution information, and network topology and state distribution information. The control channel can be out of band or in-band wavelength or fiber, an Ethernet link, an IP tunnel through a separate management network. Moreover, data channel that forwards data traffic between the customer sites without O-E-O conversion is managed by the control-flow [9]. The consecutive sub-flows of control-flow are illustrated in Figure 2. For the Figure 2(A), the LMP (Link Management Protocol) [10] activates control channels for all links between the CE1 and CE2, and Figure 2(B) represents the routing protocol that exchanges routing information. Figure 2(C) shows the label distribution procedure between CE1 and CE2, and O-LSPs(Optical-Label Switched Paths equal to lightpaths) establishment procedure by RSVP-TE+ (resource ReSerVation Protocol-Traffic Engineering Extension) [11]. Thereafter, data transmission is triggered, and the LMP maintains O-LSPs as described in

(D), if there are failures, signal degradation or abnormal signals detected due to fault or attack, a link that disables data transmission is localized and the traffic is recovered in accordance with pre-specified QoP level [12-13].

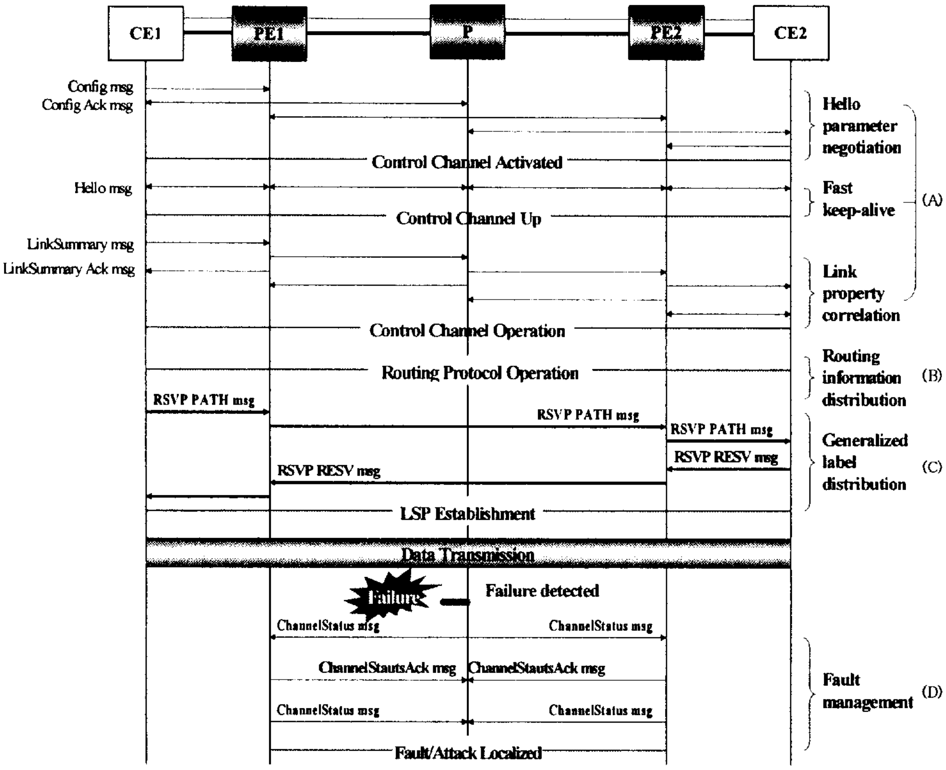


Figure 2. Operation of GMPLS Protocol in OVPN

3. Analysis of Preliminary RWA Schemes

The most of preliminary RWA researches in OVPN is derived from the RWA in DWDM-based networks. Generally, the trend of RWA researches approached to various viewpoints with respects to traffic assumptions and the possibility of wavelength conversion. Almost all existing algorithms for the RWA problem have been decoupled into two separate sub-problems, i.e., the routing sub-problem and the wavelength assignment sub-problem because finding an optimal solution by solving the RWA at the same time known as NP-complete problem [4]. Each sub-problem is independently solved as shown in Figure 3.

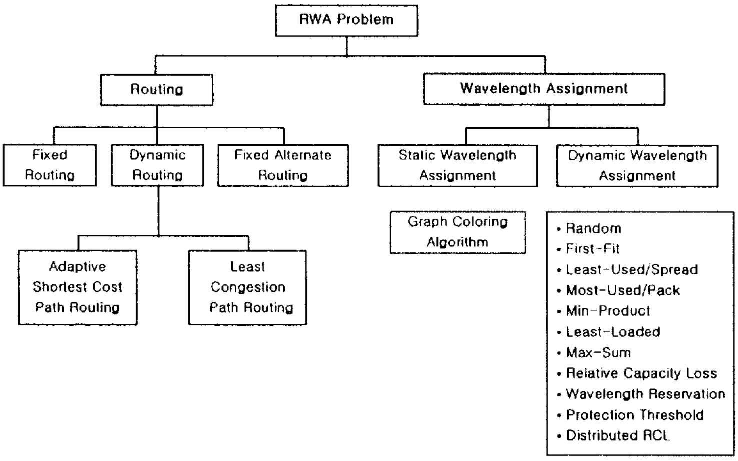


Figure 3. The previous RWA schemes

3.1 Routing Schemes

Current routing schemes are based on source-directed methods because of its easy controllable characteristics. And there are three fundamental approaches to solve routing sub-problem: fixed routing (FR), fixed-alternate routing (FAR) and dynamic routing (DR).

1) Fixed Routing (FR)

The simplest method for routing a connection always chooses the same fixed route for a given source-destination pair. Generally, the fixed shortest-path routing approach is used. The shortest-path for each source-destination pair is computed off-line in advance using standard shortest-path algorithms, e.g. Dijkstra's algorithm or Bellman-Ford algorithm. When the request comes, the light path is set up using the pre-determined route just like the fixed shortest-path from Node 0 to Node 2 as shown in Figure 4. Obviously, the disadvantage of this approach is that the routing decision is not made based on the current state of network. It might lead to the situation where some links on the network are over-utilized while other links are underutilized. This might potentially result in high blocking probability.

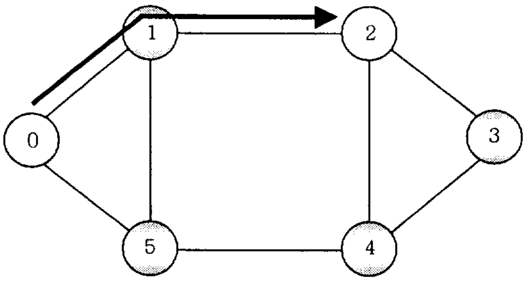


Figure 4. Fixed routing

Also, FR may be unable to handle fault situations in which one or more links in the network failure. To handle link faults, the routing scheme must either consider alternate paths to the destination, or must be able to find the route dynamically. Note that, in Figure 4, a connection request from Node 0 to Node 2 will be blocked if a common wavelength is not available on both links in the fixed route, or if either of the links in the fixed route is cut.

2) Fixed Alternate Routing (FAR)

As an improvement over FR, FAR is an approach that sequentially considers an available path among pre-determined fixed routes and selects one. Each node in the network is required to maintain a routing table that contains an ordered list of a number of fixed routes to each destination node. For example, these routes may include the shortest-path, the second shortest-path, the third shortest-path, etc. A primary route between a (S, D) pair is defined as the first route in the list routes to the destination node in the routing table at the source node. An alternate route between a (S, D) pair is any route that does not share any links with the first route in the routing table at the source node. Figure 5 illustrates multiple alternate routes from Node 0 to Node 2. When a connection request arrives, the source node will decide the best route from a list of candidate routes by some metric, e.g. the minimal hop count and then set up the lightpath over that route. This approach can reduce the blocking probability compared to FR, and provide some degree of fault tolerance upon link failures.

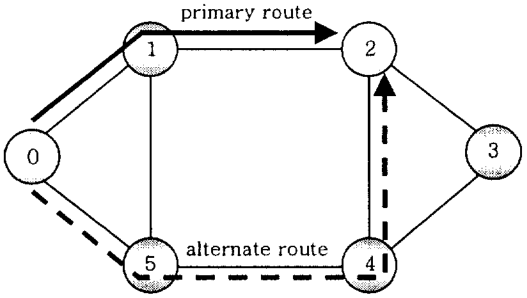


Figure 5. Fixed alternate routing

3) Dynamic Routing (DR)

In dynamic routing (DR), the route from a source to destination is determined depending on the network state that is determined by all the connections that are currently in progress. A typical form of dynamic routing (DR) is adaptive shortest-cost-path routing. When a connection request arrives, a source node computes the shortest-cost-path to a destination node based on the network state as shown in Figure 6. If no path is available, the request will be blocked.

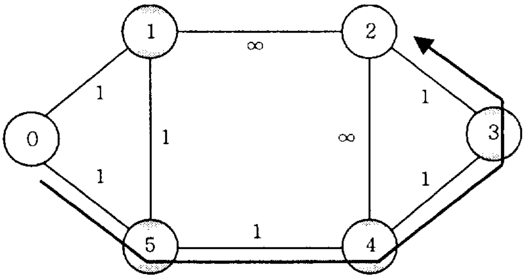


Figure 6. Dynamic routing

For example, if each unused and used link has a cost of 1 and ∞ respectively in the network in Figure 6 and the links between (1, 2) and (4, 2) are busy, then this approach can still establish a connection between Node 0 and 2, while both the FR and FAR as shown in Figure 4 and 5 would block the connection.

Another form of DR is least congested path (LCP) routing. This approach is similar to FAR that pre-selects multiple routes for each (S, D) pair. Upon the arrival of a connection request, least congested path among the pre-determined routes is chosen. The congestion on a path is measured by the number of wavelengths available on the most congested link in the path.

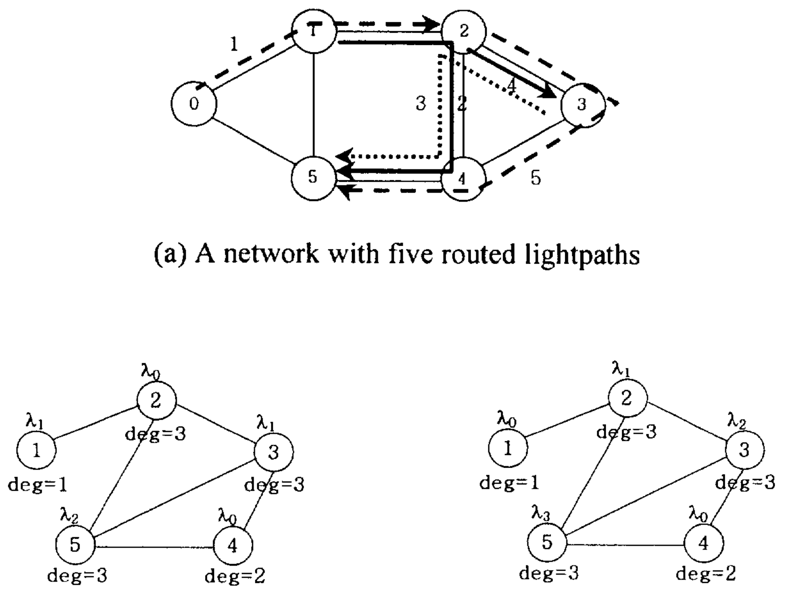
The advantage of DR is that it results in lower connection blocking probability than FR and FAR because it is too hard to find an optimal route using static routing approaches such as FR and FAR that determine the route without considering network's status [14]. Compared to static routing methods, DR approach is the most efficient because a route is dynamically chosen by considering network's status at the time of connection request, which improves network performance in terms of blocking probability [14-15]. Also, DR approach can provide the protection scheme for a connection by setting up a backup path against link or node failures in the network.

3.2 Wavelength Assignment Schemes

For the wavelength assignment sub-problem, it is the goal to efficiently assign a wavelength to each lightpath without sharing the same wavelength with other lightpaths on a given link, which has been respectively studied in terms of static and dynamic traffic.

1) Static Wavelength Assignment

Generally, graph-coloring algorithms [16] were employed to assign wavelengths for static traffic where the set of connections are known in advance. This algorithm operates to minimize the number of wavelength used as follows. First, construct an auxiliary graph G(V,E), such that each lightpath in the system is represented by a vertex(V) in graph G. There is an undirected edge(E) between two vertexs in graph G if the corresponding lightpaths pass through a common physical fiber link as shown in Figure 7. Second, coloring the vertexes of the graph G such that no two adjacent nodes have the same color. If the number of edges at a node denotes degree, then coloring vertexes from the maximum degree (Figure 7(b)) can have the minimum number of wavelengths required for the set of lightpaths in Figure 7(a).



(a) A network with five routed lightpaths

(b) Coloring vertexes sequentially from the maximum degree

(c) Coloring vertexes sequentially from the minimum degree

Figure 7. Graph coloring algorithm

2) Dynamic Wavelength Assignment

Under dynamic traffic where connection requests arrive randomly, a number of heuristics have been proposed as follows; Random Wavelength Assignment (R), First-Fit (FF), Least-Used/Spread (LU), Most-Used/Pack (MU), Min-Product (MP), Least-Loaded (LL), MAX-SUM (MΣ), Relative Capacity Loss (RCL), DRCL (Distributed RCL), Wavelength Reservation (Rsv) and Protection Threshold (Thr) [16-17].

R scheme randomly chooses one among available wavelengths for request route. FF selects the first wavelength among all the available wavelengths numbered. This scheme is preferred in practice because of no requiring global knowledge and simple computation. LU chooses the wavelength that is least used in network. This scheme causes communication overhead that collects global information to compute the least-used wavelength. MU chooses the most-used wavelength in the network contrary to LU method. This scheme is expected to have better performance than LU due to conservation the spare capacity of less-used wavelengths. But MU also has the communication overhead same as LU scheme. MP scheme computes the number of occupied fibers for each wavelength on a link and choose the wavelength with the minimal value in multiple fiber networks. LL chooses the wavelength that has most residual capacity on the most loaded link along the path selected in multiple fiber networks. M$\sum$considers all possible paths in the network and attempts to select the wavelength that minimizes the capacity loss on all lightpaths. RCL tries to minimize the relative capacity loss based on MS. Currently, RCL offers the best performance; however this scheme requires global information and complex computation. DRCL scheme based on RCL is more efficient in a distributed-controlled network. In Rsv, a wavelength on a specified link is reserved for a traffic stream. Thr assigns a wavelength only if the number of idle wavelengths on the link is at or above a given threshold.

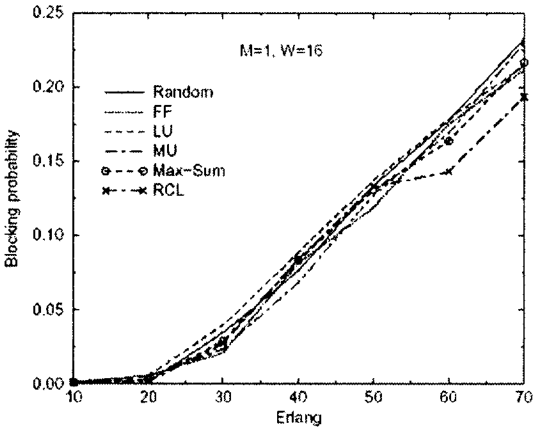
In this paper, we use FF scheme because this scheme practicvally has good performance and does not need link-state information.

3.3. Performance and Problem of Previous RWA Schemes

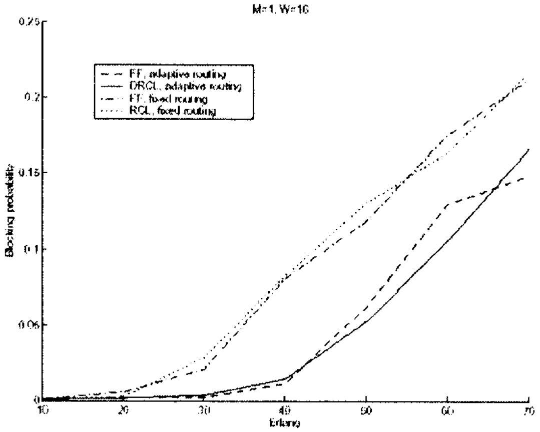
Until now, researches for the RWA problem have been divided into routing sub-problem and wavelength assignment sub-problem.

As an analysis of previous researches for RWA problem, Figure 8 shows performance of existing RWA schemes for connection blocking probability in case of DWDM network that the number of fibers per link is one (M = 1), and that the number of wavelengths per fiber is sixteen (W = 16); Figure 8(a) is comparison of various wavelength assignment algorithms when using FR scheme and Figure 8(b) is to compare performance of FR and DR for two wavelength assignment schemes such as FF and RCL.

In an overall result of previous RWA researches as shown in Figure 8, the routing scheme has much more impact on the performance of the system than the wavelength-assignment scheme [17]. That is to say, "routing scheme is more significant factor for RWA problem" conclusion is consistent with the findings in previous studies. Among approaches for the routing problem, dynamic routing (DR) yields the best performance (Figure 8(b)) [18]. On the other hand, for wavelength assignment approaches, MU is found to achieve the best performance under low load while M$\sum$ and RCL work well when the load is high (≥ 50 Erlangs), with the other approaches not that far behind; however, the differences in performance among the existing various wavelength assignment schemes are not too significant (Figure 8(a)).



(a) Comparison of the existing various wavelength assignment schemes



(b) Comparison of the existing routing schemes

Figure 8. Comparison of the previous RWA schemes

Until now, the objective in researches for the RWA problem is to set up lightpaths and assign wavelengths in a manner that minimizes the number of wavelength needed, or that maximizes the number of connection established in OVPN networks.

However, existing RWA schemes are based on source-directed methods which need a large amount of link-state information and computational process. This can lead to inefficiency for establishment of lightpaths.

To achieve successive construction of lightpaths in OVPN based on DWDM technology, we deploy flooding-based routing algorithm. And as bounding criteria, we newly introduce ripple-count concept and use QoS checking mechanism. Therefore, this paper accesses to a solution for RWA problem in OVPN and differentiated QoS and QoP model in the next generation OVPN.

Ⅲ. Bounded-Flooding Routing Algorithm

1. Ripple-Count Concept

In order to reduce network overhead, we newly introduce a ripple-count concept as a bounding criteria, which provides flexible classification by relative positions of nodes. The ripple-count of a node is relative to the particular source-nodes which receive connection request and is of multi-value which means every value is relative to a particular source-node. And related to a source-node, the 1st-wave set is formed of all nodes at which message arrives in one hop from the source, where all elements of the set are called as the 1st-wave nodes; similarly, the 2nd-wave set is formed of nodes in two hops, and so on. This approach accomplishes not to flood unnecessary messages without state information and operational process in each node.

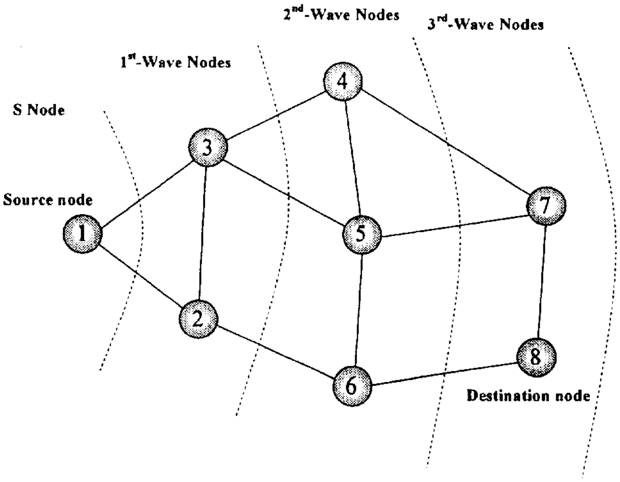


Figure 9. Ripple-count Concept

As shown in Figure 9, if a connection request arrives at node 1, a source node (S node) is node 1, and according to ripple-count concept, the other nodes can be defined as follows;

S node {1}
1st-wave set {2,3}
2nd-wave set {4,5,6}
3rd-wave set {7,8}

If a node K belongs to the jth-wave set of source S, the elements in (j-1)th-wave set are called as the lower-wave nodes, and those in (j+1)th-wave set as the higher-wave nodes. And all messages in the network can be classified into three types-the messages from the nodes with lower-wave to the nodes with higher-wave as type-I, messages between nodes with peer-wave as type-II, while messages from the nodes with higher-wave to the nodes with lower-wave as type-III.

Toward reduction of overhead, only type-I messages can really be contributed to addressing the destination node and therefore called them as 'right messages'. Reversely, type-III messages are not useful at all and therefore called them as 'futile messages', while the type-II messages might have possibility to be changed to type-I messages when some links fail or some messages are lost, so called them as 'possible messages'.

As a bounding constraint, we do not admit futile messages to flood. However, because possible messages can affect to network overhead significantly, we alternatively use possible messages (type-II) for better network performance. And the effects of type-II messages are simulated by comparing with other conditions in section 5.

2. Bounded-Flooding Routing Algorithm

Each node in the network consists of an optical cross-connect (OXC) controlled by an electronic controller (e.g. IP/GMPLS) that is a control domain. The electronic controllers communicate with each other over a control channel, either out-of-band or in band. We assume the existing of a reliable transport protocol in this control channel making sure that messages between controllers are delivered reliably in sequence.

Each node maintains the status of every wavelength on every link emerging from the node. For a wavelength λ_i on link L, the state can be one of the following:

- Free: indicates that the wavelength λ_i is available and can be used to establish a new connection.
- Reserved: indicates that λ_i is being used or reserved in some connection to transmit data.

And for the link L, the number of wavelengths that are in Free state is denoted by $F\lambda(L)$.

Upon receiving a connection request, the source node generates a request message, *Req*. A *Req* message contains the following fields.

- Connection identifier *Req.ID* which uniquely identifies the corresponding connection. For the uniqueness of each connection ID, an identifier is composed of two parts: the node ID (or address) and connection number (unique within a source). This composition of connection IDs ensures their uniqueness throughout the network.

- Source identifier *Req.src* of the requested connection.
- Destination identifier *Req.dest* of the connection.
- Ripple-count number *Req.wave* which represents the relative number of node-wave. As a bounding criterion, this identifier is used to remove the futile messages to reduce the overhead.
- List of intermediate node IDs *Req.nodeID* that the message has traversed thus far. Every time the request message is relayed to the next node, the new node ID is appended to this field. This information is needed for the destination node to confirm the establishment of the requested connection.
- Connection pertinence parameter *Req.cpp* which is increased as the *Req* passes the nodes, the metric value represents the route difficulty that the *Req* has experienced. This parameter can be used for another criterion (i.e. number of wavelengths, hop count, time to live, and etc.).
- QoS requirements parameter *Req.qos* which is used to contain the threshold to which a service needs to provide, while executing QoS admission checking procedure.

Since the information of existing connections is necessary for a new connection's admission test as well as for the completion of pending connections belonging to those connections still being processed, each node has to maintain two sets of tables for existing connections (Routing table) and pending connections (Pending table). Routing table (RT) contains established connections, one for each of its outgoing links. Each entry of a RT represents a connection which goes through the corresponding link and consists of the following fields.

- Connection identifier: this is the same as the one in the *Req* message.
- Wavelength index: the index of corresponding wavelength available. When a wavelength λ_i is occupied, λ_i.Free=0 and λ_i.Reserved=1. Reversely, when a wavelength λ_i is available, λ_i.Free=1 and λ_i.Reserved=0.

For pending table (PT), each node has to maintain fields for temporary pending connection requests, also one for each of its outgoing links. Each entry of a PT represents a connection request and contains the following fields.

- Connection identifier: same as the one in the *Req* message. When a connection request is conditionally accepted (that is, the outgoing link is able to accommodate the requested connection), it is copied from the connection ID field of the *Req* message.
- Wavelength index: the index of corresponding wavelength available for reservation. When a wavelength λ_i is occupied, λ_i .Free=0 and λ_i.Reserved=1. Reversely, when a wavelength λ_i is available, λ_i.Free=1 and λ_i.Reserved=0.
- Ripple-count number: this field is relative according to the source node and used for dividing incoming messages into right, possible, and futile messages (type – I, II and III, respectively).

- Connection pertinence parameter: this field contains *Req.cpp* of incoming *Req* message. This is used to compare the priority while the *Req* messages which have the same ripple-count number, has arrived.

Source Node Action

Upon receiving a connection request, the parameters (*Req.ID*, *Req.src*, *Req.dest*, *Req.wave*, *Req.nodeID*, *Req.cpp*, *Req.qos*) in *Req* message are set, and then the source node sends *Req* messages through each of its outgoing links only if it satisfies QoS admission checking test and the following condition:

$$F\lambda(L) > 0 \quad (1)$$

where $F\lambda(L)$ is the number of free wavelengths in link L.

Intermediate Node Action

For more efficient wavelength utilization, we apply the number of wavelengths to *Req.cpp* as a constraint. Therefore, the intermediate node sends a request message through each of its outgoing links if it satisfies QoS admission checking test and additionally the following conditions:

$$PT(Req.ID).Ripple\text{-}count \geq Req.wave \quad (2)$$

PT(*Req.ID*).Ripple-count in the equation (2) represents relative number to which this node belongs. Equation (2) functions to discard futile messages without state information and operational process, and by changing '≥' to '>', we can also discard possible messages for a tradeoff between overhead and blocking probability.

If the node and the *Req* message pass these constraints (equation (1) and (2)), then the *Req* message is updated and the pending table is set by the corresponding *Req* message. Thereafter, the node forwards the *Req* message to a neighbor node via the outgoing qualified link. Somehow, when a message returns back to the previous node, there could be loop-back situation. However, by deploying the ripple-count concept, loop-back is also prevented by comparing ripple-count values.

Destination Node Action

As for the destination node action, we append one table called path candidate table (PCT) in the destination node to store candidate paths (*Req* messages) for further selection. This table contains *Req* messages in an accepted sequence. Due to performance considerations, we have two different path selection schemes considered here:

First come first serve path selection scheme (FCFS):

In this scheme, the destination node selects the path associated with the *Req* message that arrives first. This selection criterion is based on the assumption that the first packet to arrive is the most likely the one that has taken the least delay path and, hence, is the one that encounters the minimum delay. If another succeeded *Req* message arrives for the same connection request, the destination node stores it in PCT until the upstream reservation on the first selected route is confirmed. The stored route can be used in case if the upstream reservation fails. On the other hand, if the *Req* message has arrived after the upstream reservation has already been confirmed, the destination node discards messages in the corresponding PCT. This path selection scheme minimizes the connection setup time. That is, the destination node doesn't have to wait the arrival of the second *Req* message to decide on a path to setup the connection request.

Least-congested path selection scheme (LCP):

In this scheme, the path with the minimum value of *Req.cpp/Req.wave* is selected to setup a connection. In this case the destination node has to wait until *Req* messages from all attached links are received (or the destination node opens a short time-window to absorb possible further arriving *Req* messages). If *Req* messages accepted have the same *Req.cpp/Req.wave* as a constraint, the first message which might be shorter delay than other paths is chosen. LCP scheme also distributes the traffic evenly in the network. As will be shown later, this scheme can improve the blocking probability compared to alternate path selection schemes.

In order to confirm the qualified path, we define a connection confirmation message called *Conf* message to confirm a satisfied path. The *Conf* message contains the following fields:

- Connection identifier *Conf.ID*: this is the same as the one in the *Req* message.
- List of intermediate node IDs that the *Req* message has. This information is

needed to confirm the establishment of the confirmed connection.

And we also define a reject reservation message called *Rej* message to release reserved resources of unconfirmed paths for further connection requests. The *Rej* message contains the following fields:

- Connection identifier *Rej.ID* : this is the same as the one in the *Req* message.
- Destination identifier *Rej.dest* : this is the same as the one in the *Req.src*.
- Ripple-count number *Rej.wave* which represents the relative number of node-wave. This identifier is used to remove the futile messages to reduce the overhead.

The *Rej* message is processed right after the requested connection is established or the connection is blocked.

The flowchart in Figure 10 shows the actions in LCP scheme to be taken by both in an intermediate node and in a destination node. This flowchart can easily be applied to FCFS scheme by choosing the first incoming *Req* message at the destination node.

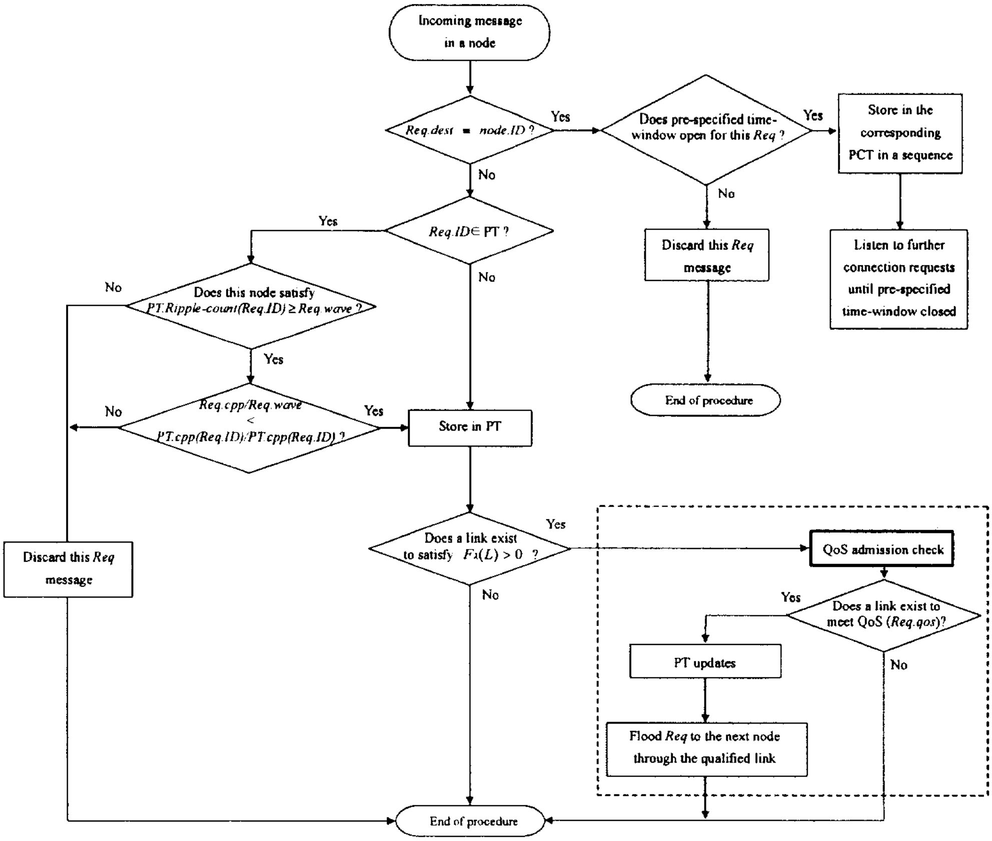

Incoming message in a node
Req.dest = node.ID ?
Yes
No
Does pre-specified time-window open for this Req ?
Yes
Store in the corresponding PCT in a sequence
No
Listen to further connection requests until pre-specified time-window closed
Discard this Req message
End of procedure
Req.ID∈ PT ?
Yes
No
Does this node satisfy PT.Ripple-count(Req.ID) ≥ Req.wave ?
No
Yes
Req.cpp/Req.wave < PT.cpp(Req.ID)/PT.cpp(Req.ID) ?
No
Yes
Store in PT
Does a link exist to satisfy Fλ(L) > 0 ?
Yes
No
Discard this Req message
QoS admission check
Does a link exist to meet QoS (Req.qos)?
Yes
No
PT updates
Flood Req to the next node through the qualified link
End of procedure

Figure 10. Flowchart of BFR operation in a node

At the destination node, when the pre-specified time-window is expired for the LCP scheme, the path is determined by the following equation.

$$\max Req.cpp/Req.wave \;=\; \max \sum_{p} F_{\lambda}(L)\,/Req.wave \qquad (3)$$

The dark dotted box represents QoS checking procedure; this prevents to flood to an unqualified path that does not satisfy *Req.qos*. The procedure of QoS admission checking mechanism is described in the next subsection.

3. Differentiated QoS and QoP

3.1. Classification of QoS and QoP

In DWDM-based OVPN networks, an optical signal passing through network components such as an optical cross-connect (OXC), fiber, wavelength converter (WC), and EDFA undergoes many transmission impairments. Then, the quality of the optical signal on each link is affected by several impairments ranging from simple attenuation to complex nonlinear effects [19-20], which are determined by calculating the bit error rate (BER) in the receiving node. BER is the most important one among several parameters proposed for monitoring signal quality [21] and is complemented by other parameters to diagnose the system problems like optical signal-to-noise ratio (OSNR) or electrical signal-to-noise ratio (el. SNR) [20]. But it is difficult to measure directly the BER from an optical signal due that an optical signal is forwarded without optical-electrical-optical conversions in OVPN networks. And the OSNR may vary significantly for a specific BER value because of nonlinear effects. We can estimate the BER in an optical network by the Q-factor as a new parameter evaluating signal quality [22]. It measures the signal-to-noise ratio (SNR) based on assuming Gaussian noise statistics in the eye-diagram. Thus, the QoS parameters related to the transmission quality of a lightpath are determined by the following Equations (4) to (6) [20].

$$BER(Q) \cong (1/\sqrt{2\pi}) \cdot (\exp(-Q^2/2)/Q) \tag{4}$$

$$el.SNR = 10 \log Q^2 \tag{5}$$

$$OSNR_{0.1nm} = \frac{(1+r)(1+\sqrt{r})^2}{(1-r)^2} \cdot \frac{Be}{Bd} \cdot Q^2 \tag{6}$$

$r = 0.15$ (*extinction ratio of the transmitted optical signal*)
$Be = 0.75 \times fo$ (*effective electrical noise bandwidth due to bit rate fo*)
$Bd = 12.6$ *GHz or* 0.1 *nm* (*optical bandwidth for OSNR measurement*)

An EDFA optical amplifier provides a relatively flat and wide gain curve so that it is commonly used for transferring optical signals. In particular, it has a gain band available in the C-band ranging from 1530 to 1565 nm and also has a low attenuation factor of 0.28 dB/km. In terms of the influence of temperature, the bands up to 1625 nm can be used for transferring optical signals, whereby the L-band has an attenuation factor of 0.35 dB/km [23]. Therefore, the C-band is selected for an O-LSP of the premium service to provide high reliability and the L-band is used for an O-LSP of the assured or best-effort service [24]. Thus, the entire currently available band of wavelengths is divided into three categories in a proper proportion (premium: 10%, assured: 30%, best-effort: 60%), thereby gaining the load balancing effect by avoiding heavy loaded links and failing optical path settings.

Since in general the optical signal has a high data rate capacity, a failure would result in considerable losses of data. Accordingly, protection and restoration mechanisms are very critical to ensure that optical paths are transparent against various problems such as a broken optical line and a damaged wavelength. The premium service that transmits real-time data like sound requires very high reliability. This service is protected by a local QoP protection mechanism on the optical channel level or a GMPLS backup procedure within a recovery time of 50 ms or less. Reliable QoP of the assured service requires using an O-LSP restoration scheme of GMPLS that generates a backup path upon any occurrence of incidents. The O-LSP restoration scheme has to find the recovery O-LSP dynamically to replace a damaged optical path between PE nodes, so it requires longer recovery time than that in premium service (tens to hundreds of ms). This scheme may have better resource utilization but lower recovery success so that there is a trade-off. Best-effort service recommends an O-LSP restoration scheme, where best-effort service with service interruption due to any failure is compensated by re-transmission of traffic within a service time ranging from 100 ms to several seconds.

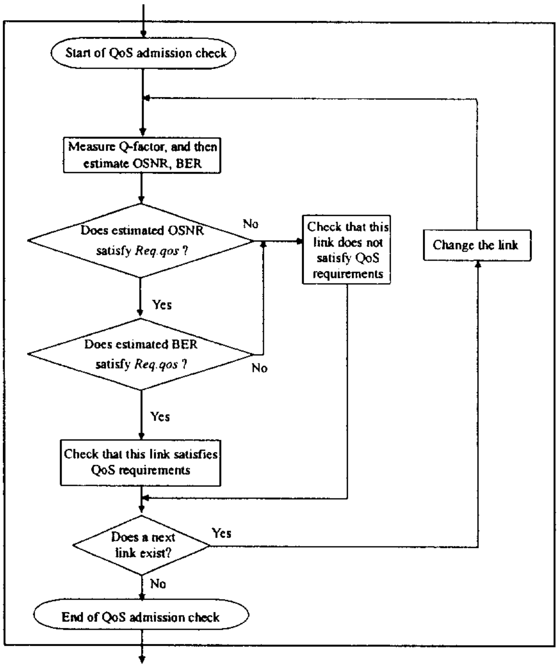
Based on the above considerations, the differentiated QoS and QoP classes in the next generation OVPN is suggested as shown in Table 1.

Table 1. Differentiated QoS and QoP Classes

Classification criteria		Class 1	Class 2	Class 3
		Premium service: Expedited Forwarding (EF) PHB	Assured service: Assured Forwarding (AF) PHB	Best Effort (BE) service: Default PHB
QoS	BER (Q)	10^{-12} (7)	10^{-9} (6) ~ 10^{-7} (5.1)	10^{-5} (4.2)
	el. SNR	16.9 dB	15.5 dB ~ 14.2 dB	12.5 dB
	OSNR (f_0=10 Gbit/s)	19.5 dB	18.2 dB ~ 16.8 dB	15.1 dB
QoP	Resource allocation	Pre-specified percentage (10%) for this service (C band: 1530 nm ~ 1565 nm)	Pre-specified percentage (30%) for this service (L band: 1565 nm ~ 1625 nm)	Best use of the remaining bandwidth (L band: 1565 nm ~ 1625 nm)
	Recovery scheme	1:1 dedicated protection	1:3 shared protection	Restoration
	Recovery time	<50 msec (Detection time: <100 msec)	50 – 100 msec (Detection time: 0.1 msec –100 msec)	1 – 100 sec (Detection time: 100 msec – 180 sec)

3.2. QoS Admission Checking Mechanism

The proposed BFR algorithm considers multiple QoS admission checks at every node as a bounding constraint. We consider the parameters, such as BER and OSNR. Figure 11 illustrates the procedure of QoS admission checks. And to compare with the threshold (*Req.qos*), we involve equations (4) ~ (6).



Start of QoS admission check
Measure Q-factor, and then estimate OSNR, BER
Does estimated OSNR satisfy *Req.qos* ?
No
Check that this link does not satisfy QoS requirements
Change the link
Yes
Does estimated BER satisfy *Req.qos* ?
No
Yes
Check that this link satisfies QoS requirements
Does a next link exist?
Yes
No
End of QoS admission check

Figure 11. Procedure of QoS admission checking mechanism

4. Limited Wavelength Conversion

In the current research, it is proved of the efficiency improvement offered by the use of wavelength converters (WCs) in DWDM networks. But it has been assumed that a full set of ideal WCs are available at every node in the network. Although full-wavelength conversion is desirable because it substantially decreases blocking probability, it is difficult to implement in practice due to technological limitations and high cost as well.

Therefore, in this subsection, we describe networks with limited wavelength conversion. This may be the result of placing WCs at a limited range of OXCs in the network, using limited numbers of WCs in each cross-connect, or using WCs whose performance limits the set of allowable conversions.

Many optical network researchers have built optically-transparent or all-optical networks, in which no optical to electrical conversions are performed. WCs used in these networks have to be all-optical WCs. However, many factors, such as optical non-linearity, chromatic dispersion, amplifier spontaneous emission, attenuate the power of signal, so that these factors degrade the SNR to maximum –20 dB [24].

Besides, separated optical space switches are used for each wavelength. So, if there are M input and M output fibers with W wavelengths on each fiber, then W separated M x M space switches are required to implement an OXC without WCs. Otherwise, a single MW x MW space switch is required to implement the cross-connect with WCs.

In this paper, we apply limited wavelength conversion to BFR algorithm and the procedures are as follows: (i) the limited range WCs are used and wavelength conversion is performed after switching, as shown in equation (7) of which output wavelengths are limited within k area based on input wavelength. (ii) the limited range WCs that are sparsely placed in selected nodes are chosen by total outgoing traffic algorithm [25]. And because the selected nodes have high nodal degree, potentially, the probability to cause the congestion situation is high.

$$\lambda_i \rightarrow \lambda_{\max(\ i-k\ ,1)} \leq \lambda_o \leq \lambda_{\min(\ i+k\ ,w)} \qquad (7)$$

Figure 12 shows the traffic at intermediate nodes and equation (8)-(11) that present drop traffic ($\rho_l(v)$), added traffic ($\rho_n(v)$) and transit traffic ($\rho_c(v)$), respectively. The nodes equipped with WCs have high traffic cost ($\tau(v)$).

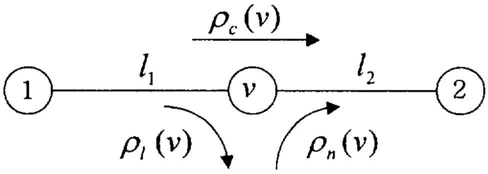


Figure 12. The traffic at intermediate nodes

$$\rho_l(v) = \sum_{\{j:l_1 \in r_j,\ j:l_2 \notin r_j\}} \lambda_j \qquad (8)$$

$$\rho_n(v) = \sum_{\{j:l_1 \notin r_j,\ j:l_2 \in r_j\}} \lambda_j \qquad (9)$$

$$\rho_c(v) = \sum_{\{j:l_1 \in r_j,\ j:l_2 \in r_j\}} \lambda_j \qquad (10)$$

$$\tau(v) = \rho_n(v) + \rho_c(v) \qquad (11)$$

Theoretically, if the blocking probability improves significantly with 20%~40% wavelength range conversion, the performance is very close to full range wavelength conversion [24]. And when WCs are placed at a few nodes (about 40%), the performance is similar with full-WCs [26]. Furthermore, to prove the results while applying the limited wavelength conversion to BFR algorithm, simulations are carried out in section 5. We adopt 30% range conversion and place 40% nodes of entire nodes.

Ⅳ. Survivability-Guaranteed Approach

Each dependable real-time connection consists of one primary and one or more backup channels. Upon detection of a failure on the primary channel, one of its backups is promoted to the new primary. Since a backup is set up before a failure of the primary, it can be activated immediately, without the time-consuming and channel re-establishment process. Generally, this scheme is called 1:1 protection or 1:N protection.

In OVPN, when establishing dependable connections, shared risk link group (SRLG) concept has to be considered to prevent a failure of both a primary path and a backup path simultaneously. So, many researches for SRLG have done, however, the results accomplished both in resource utilization and in blocking probability are not satisfactory. The proposed BFR algorithm which is carried out in a parallel way can improve both resource utilization (i.e. wavelength) and survivability ratio.

1. Network Survivability Issue in OVPN

The ramification of network survivability in OVPN is depicted in Figure 13. Fault survivability contains fault management for a sudden fault of optical components and signal degradation management. Also, attack survivability is divided into physical attack management and logical attack management depending on attack possibilities. Especially, physical attack in optical domain needs to be managed in optical layer because it causes signal degradation by maliciously using intrinsic characteristics of optical components. However, logical attack is defined as an unauthorized person's network access on purpose to modify or to eavesdrop information, and has to be dealt by quantum-cryptography, but it is beyond the scope of this paper.

Moreover, in order to manage fault and attack after data transmission, the sequential mechanism is needed as follows: detect fault and attack as soon as possible (detection), separate fault and attack from normal traffic (localization), and notify fault and attack to network elements which are responsible for network management (notification) and recover traffic to avoid fault and attack (protection/restoration). These procedures are widely researched in GMPLS that is standardizing in IETF.

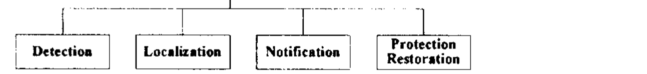


Figure 13. Network Survivability in OVPN Networks

An established lightpath between PE nodes may cross a number of intermediate P nodes interconnected by fiber segments, amplifiers and optional taps. The optical components that constitute a core node, in general, include an optical switch, a demultiplexer comprising of signal splitters and optical filters, and a multiplexer made up of signal combiners. A core node may also contain a transmitter array (Tx) and a receiver array (Rx) enabling local add/drop of the wavelengths.

In the architectural structure shown in Figure 14, we can describe three management sections taking into consideration resource types (optical components) and the coverage of fault and attack effects.

- Optical Channel Section (OCh): Channel management section for one lightpath established between PE nodes.
- Optical Multiplexing Section (OMS): Link management section for one link between adjacent nodes. This includes Optical Amplifier Section (OAS) and Fiber Intrusion Section (FIS).
- Node Section: Node management section including demux, optical switch and mux that are divided and managed by sub-management sections, i.e. Demultiplexing Section (DS), Switching Section (SS) and Multiplexing Section (MS).

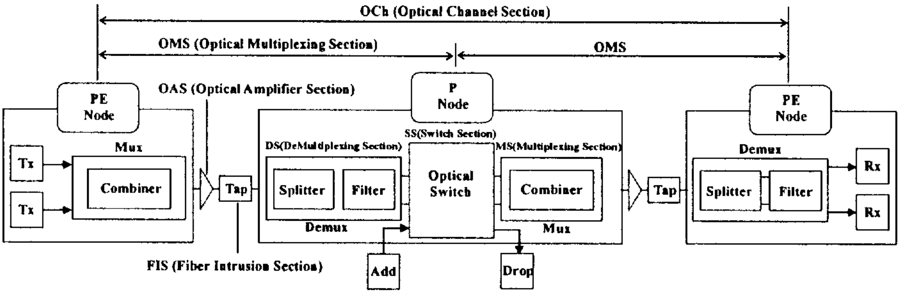


Figure 14. An architectural model for OVPN backbone networks

2. Fault and Attack Possibilities

OVPN backbone networks have many fault possibilities due to vulnerable characteristics of optical components, so short and sporadic failures of network elements may cause a large amount of data loss. In fault survivability, the physical fault (or hard fault) on optical components has to be considered firstly. It causes failure in all optical channels that are going through a link or in a specified optical channel. The coverage of fault is specified depending on the optical components. Resource types and the coverage of fault are summarized in Table 2.

On the other hand, optical components such as optical fiber or erbium-doped fiber amplifier (EDFA) can be used as an attack point to cause signal degradation or to eavesdrop information. For example, gain competition attack causes signal degradation in optical channels that are going through a link by using intrinsic features of EDFA as mentioned in [27]. With reference to the OVPN structure shown in Figure 14, we categorize attack issues at two functional levels, and attack possibilities are summarized in Table 2 [27-28].

- Direct attack: there are certain physical link elements with their own peculiar characteristics that are more likely to be exploited by an intruder as direct attack ports.
- Indirect attack: there are certain optical components (P and PE nodes) that are unlikely to be attacked directly either because a direct attack is too complicated to generate the desired effect or because the ports are not easily accessible to the potential intruders.

Table 2. Fault/Attack and SRG classification in OVPN

Cate-gory	Resource type	Fault possibility	Attack possibility		SRG	
Path (OCh)	Transmitter	Laser or laser driver electronic problem	Signal Degradation with high power laser	Direct Attack	Channel	SRLG
		Pump laser temperature due to high current				
	Receiver	Out of range power or unacceptable input optical power	Unauthorized access to information			
Link (OMS)	Fiber (FIS)	Fiber damaging or cutting	Fiber cut or optical power reduction		Fiber	
			Tapping only or jamming only			
			Tapping & Jamming			
	Amplifier (OAS)	Amplifier optical path failure (due to fiber cutting)	Gain Competition due to local attack		Conduit	
		Passive component failure with in the amplifier	Gain Competition due to remote attack			
		Pump laser or Pump laser driver electronic problem	Crosstalk due to high power signal			
	Conduit	Conduit damaging or cutting	Conduit cut or optical power reduction			
Node (OXC)	Demux (DS)	Electronic driver failure at Demux or Optical filter failure	Intentional crosstalk using high power signal	Indirect Attack	SRNG	
		Out of range power or unacceptable input optical power				
	Switch (SS)	Electronic driver failure at switch, Misrouting	Intentional crosstalk using high power signal			
		Input power is over/under threshold or out of range	Unauthorized access to information using crosstalk			
	Mux (MS)	Electronic driver failure at Mux or Optical filter failure	Intentional crosstalk propagation from preceding devices			
		Out of range power or unacceptable input optical power				

As the aspect of the above, in OVPN backbone networks, a single fault or attack has various coverage of effect (OCh, OMS, node) depending on resource types or fault and attack types. Thus recovery mechanism needs to be done by considering common risk group to avoid common fault and attack. In the following subsection, we define the SRLG concept as survivability requirements.

3. SRLG and TA Problems

As the key constraint to establish dependable paths, SRLG is being researched intensively in DWDM-based networks. SRLG is defined as a group of links or nodes that share a common risk component, whose any fault can potentially cause the failure of all the links or nodes in the group [29]. For example, all fiber links that go through a common conduit belong to the same SRLG, because the conduit is a shared risk component whose failure, such as a conduit cut, may cause all fibers in the conduit to be broken simultaneously. SRLG is introduced in the generalized multi-protocol label switching (GMPLS) and can be identified by a SRLG identifier, which is typically a 32-bit integer [30]. On the other side, SRNG is applied to the node, but SRNG has to be controlled by a network manager, because it may affect the whole network survivability.

In this paper, as shown in Table 2, to guarantee dependable connections for corresponding QoP level, in accordance with resource types and coverage of fault and attack effects, we suggest that the SRLG has three levels as follows:

- SRLG in channel level: channels that are concatenated in one established lightpath have the same risk level.
- SRLG in fiber level: a fiber that connects two nodes is composed of more than one optical channel, and these optical channels have the same risk level with failures in fiber level (such as FIS, OAS).
- SRLG in conduit level: a fiber group that connects different nodes can have a physical structure bundled by a conduit. Thus fibers in a conduit have the same risk level with failures in conduit level.

Figure 15 illustrates a simple example of the SRLG concept. The upper plane is logical topology controlled by GMPLS and the lower plane is the physical topology in which optical components (i.e., fiber, conduit, EDFA, etc.) are deployed. All links and conduits uniquely have SRLG identifiers. When there is a connection request between node N1 and node N4, N1-N2-N3-N4 {N1'-10-1-N2'-4-N3'-9-6-12-N4'} can be a primary path, and there could be two candidates for a backup path, N1-N7-N4 {N1'-10-2-N7'-5-13-N4'} and N1-N6-N5-N4 {N1'-3-N6'-8-N5'-7-13-N4'}. If we only look at the logical topology, both the two backup paths can be allowed under dedicated path protection without SRLG concept. However, if the backup path resolves N1-N7-N4, the primary path and the backup path that go through the same conduit can fail at the same time by one single fault in {10}, so the determined backup path is N1-N6-N5-N4. Consequently, in order to make a network survivable against failures, the SRLG concept should be imposed on the selection of a backup path.

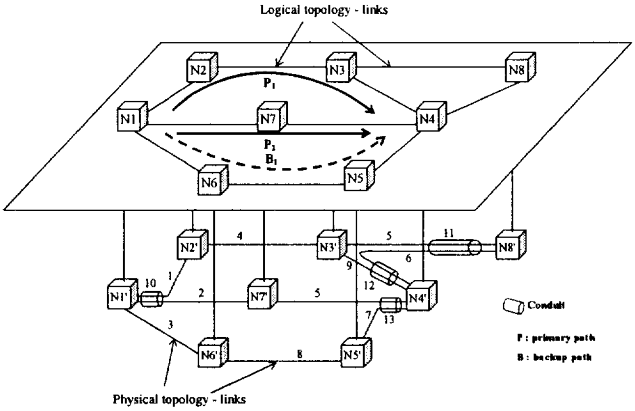


Figure 15. Concepts of SRLG and TA

Also, Figure 15 presents TA concept. TA is defined that a routing algorithm fails to find a pair of SRLG-disjoint paths for a source and a destination node pair (even though a pair of SRLG-disjoint paths do exist using a different primary path). In other words, we say that the algorithm falls into trap. From this definition, traps can be classified into real trap and avoidable trap [31]. Real trap means that a node pair like N1-N8 in Figure 15 cannot have SRLG-disjoint path pair, so this should be considered when the network is constructed. On the other hand, if a connection request N1-N4 is received, an algorithm can choose P_1 instead of P_2 because P_2 does not have a corresponding backup path while P_1 has the backup path (B_1). This is called an avoidable trap. In this paper, we check a primary path and a backup path simultaneously in a parallel way, thus improve blocking probability.

4. QoP-Guaranteed Dependable Connection Setup Method

As mentioned in section 3.3, an optical signal carrying high-speed data will experience loss or degradation of signal by various impairments. The survivability in OVPN networks is an important problem because a single failure can cause loss of vast traffic volumes. That is essentially needed to the foundation and success of the OVPN expected to transmit real-time multimedia services and many other Internet applications entail high reliability and QoP guarantees. It would be desirable resilience guarantees to all various traffic with differentiated QoP level and constraints over the Internet. However, it is not very efficient in terms of restorability. Thus, the differentiated survivability capability based on the service type is needed in the OVPN based on DWDM.

The general technique of protecting a traffic flow is to establish a backup path where the traffic is redirected when a failure occurs along its primary path. And the route computation of dependable connections (a primary path and a backup path) is generally based on the modified shortest path first (SPF) algorithm, with the constraints-based routing extension. However, this approach does not provide network performance improvement in terms of survivability (restorability) ratio.

With differentiated QoP level, for premium service and assured service, this paper introduces recovery schemes such as 1:1 dedicated protection where a SRLG-disjoint backup path and wavelength is reserved at the time of connection setup for each working path, and 1:3 shared protection where one protection path shared among several working paths. And for best effort service, we provide restoration scheme which provide a recovery procedure after link failure is occurred.

In this paper, we make dependable connections SRLG-disjoint in a parallel manner. So, we additionally define SRLG information field appended to the *Req* message.

- List of SRLG information *Req.srlg* in which the message has traversed thus far. Every time the *Req* message is relayed to the next node, the corresponding unique SRLG information is appended to this field. This information is needed for the destination node to make the establishment of SRLG-disjoint dependable connections.

At the destination node, the *Req* messages which have arrived so far or until time-window closed are compared with each other. And if there are two SRLG-disjoint paths, a primary path and a backup path are determined depending on path selection methods, i.e., FCFS or LCP.

FCFS scheme

When there are two SRLG-disjoint paths coming in sequence at the destination node, the path which has arrived firstly (the most likely minimum delay) is set to a primary path. And the other is set to a backup path.

LCP scheme

In this scheme, instead of considering incoming sequence, *Req.cpp* which represents the route difficulty (here, we assume that *Req.cpp* is the number of available wavelengths) that the *Req* has experienced is regarded. As for *Req.cpp/Req.wave*, the bigger the value is, the better the path is. So, among SRLG-disjoint paths, the bigger *Req.cpp/Req.wave* is determined by a primary path, and the other is set to a backup path. Equation (12) represents the joint path selection scheme.

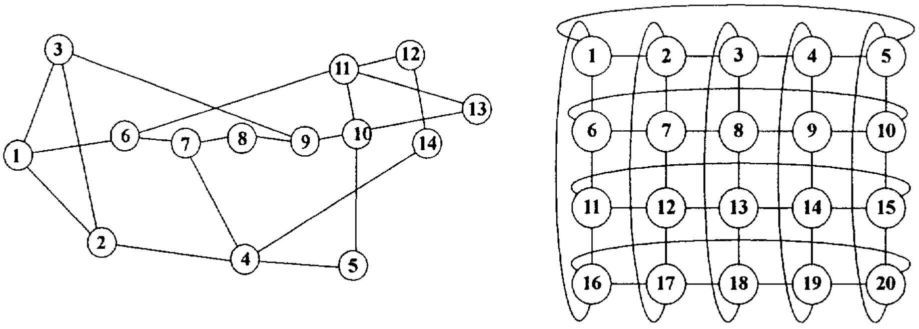
$$\max \{ \sum F_\lambda(L)\,(P)/Req.wave(P) + \sum F_\lambda(L)\,(B)/Req.wave(B) \} \qquad (12)$$

This algorithm is achieved in a parallel way, so the connection set up time is definitely shorter than serial searching methods which compute a primary path and a backup path in order.

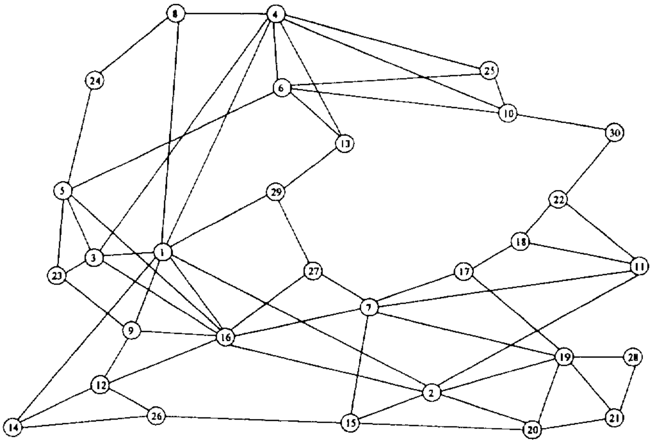
V. Performance Evaluation

1. Network Model

Simulations are carried out to prove the efficiency of the proposed BFR algorithm and dependable connection guaranteeing algorithm under BFR algorithm. Test networks used in simulations are TN(1), TN(2), TN(3), which have (14 nodes, 20 links), (20 nodes, 40 links), (30 nodes, 61 links), respectively, as illustrated in Figure 16. And we assume the connection requests arrive randomly according to the Poisson process, with negative exponentially distributed connection times with unit mean. Also, all links in the network are assumed to be bidirectional (one in each direction) and have 8 wavelengths.



(a) TN(1) (14 nodes and 20 links) (b) TN(2) (20 nodes and 40 links)



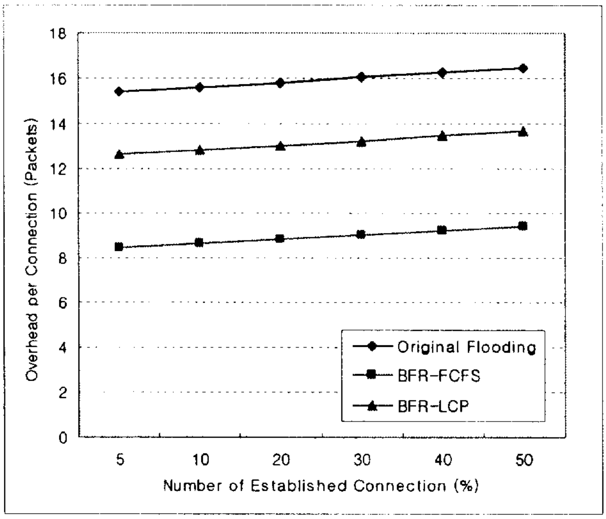
(c) TN(3) (30 nodes and 61 links)

Figure 16. Test network models

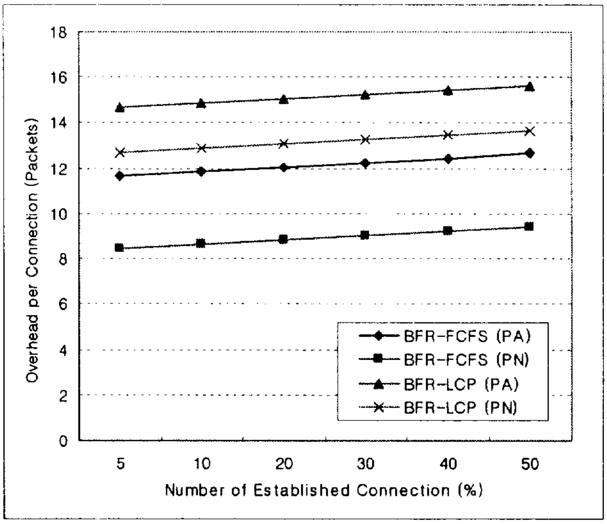
2. Analysis of Numerical Results

We carry out simulations in terms of routing overhead, blocking probability, usage of wavelength channels required and survivability ratio. For extensive simulation results, we deploy limited wavelength conversion capability (30%-range wavelength conversion and 40%-wavelength converters) in OVPN nodes as a critical concern in DWDM-based networks.

Firstly, Figure 17 shows the corresponding results for average routing overhead per successfully established connection. We compare the proposed BFR algorithm with original flooding algorithm in test network I (Figure 17(a)). By limiting the flooding area through ripple-count method and QoS checking mechanism, we accomplish the routing overhead significantly reduced. And if we admit the peer relations for further bounded area, the average routing overhead for FCFS and LCP increases as shown in Figure 17(b). In the aspect of routing overhead, BFR algorithm with FCFS methods in peer non-admitted condition performs better than other methods.



(a) Network overhead comparison with original flooding scheme

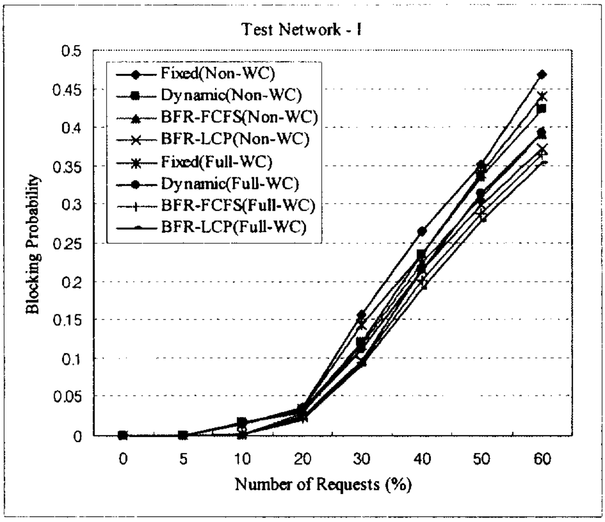


(b) Network overhead for peer-admitted (PA) and peer non-admitted (PN)

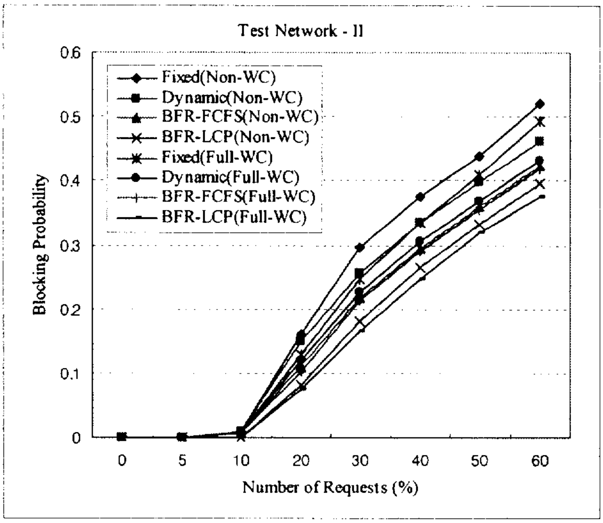
Figure 17. Network overhead (Test Network I)

From the results shown in Figure 18, it can be seen that the proposed BFR algorithm is superior to the existing routing (source directed routing - fixed routing and dynamic routing) algorithms in case of a network with full WC capability and without WC capability as well.

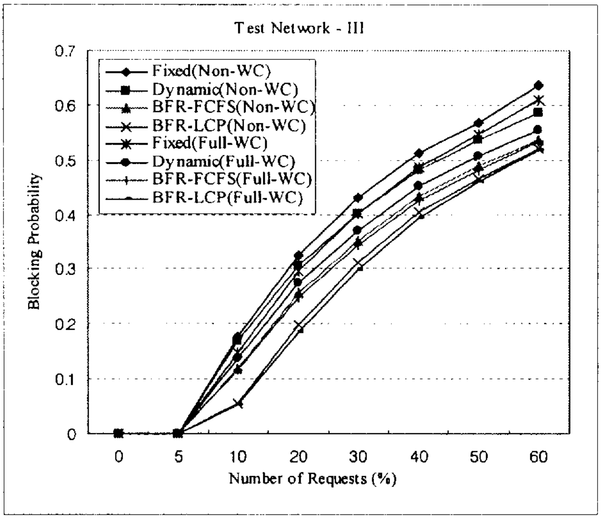
The blocking probability in three test networks shows that until 5% of connection requests, the blocking probability is almost same. But, the results make difference according to each algorithm for connections set above 5%. In the same WC condition, we observe the blocking probability of the proposed BFR algorithm with LCP method is better than dynamic routing algorithm (improved by about 5%). This means that the proposed algorithm is more effective in large scale network topology. And in all of three test networks, as the number of connection requests increases, the BFR-LCP (full-WC) is predominantly outperformed than other schemes.



(a) Blocking probability in Test network I



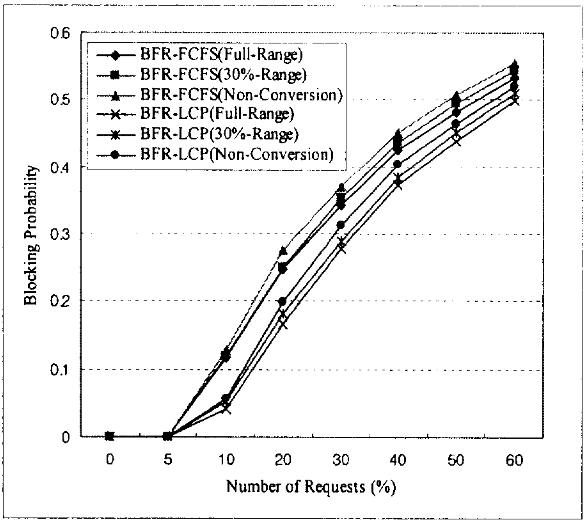
(b) Blocking probability in Test network II



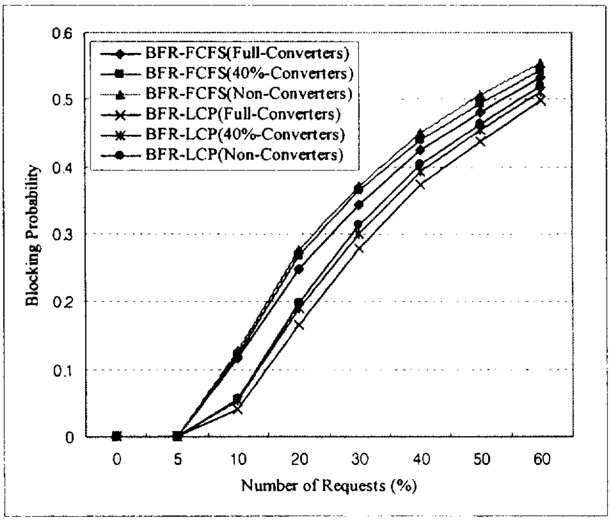
(c) Blocking probability in Test network III

Figure 18. Blocking probability for comparing with source-directed methods

Note that the wavelength conversion capability is very critical problem in DWDM-based networks because the WC is high cost and still immature technology. So, as described in section 3.4, within test network I, we deploy the limited wavelength conversion capability in OVPN nodes as a critical concern. From the Figure 19(a), we find that the blocking probability of the proposed BFR algorithm in the network equipped with 30%-range wavelength conversion capability is close to that in the network with full wavelength conversion capability. Moreover, the results presented in Figure 19(b) illustrate that even when 40% WCs of total network nodes (60% non-WC) are deployed, the blocking probability of the proposed BFR algorithm is slightly deteriorated (about 1%~2%). So, the OVPN with 30%-range or 40% converters as limited wavelength conversion capability can have almost similar performances with full WC.



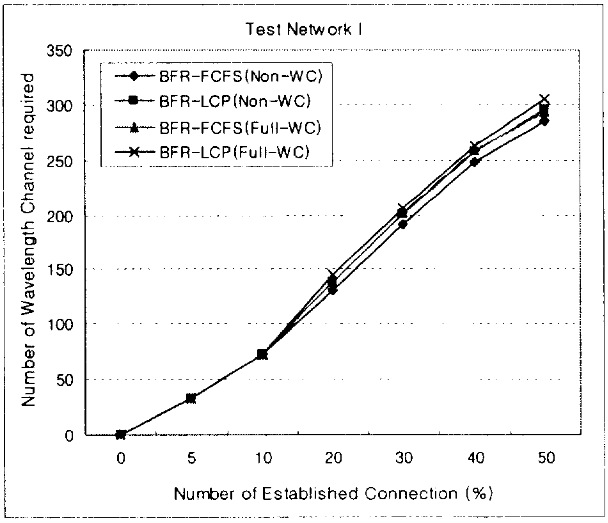
(a) Blocking probability for full, 30% and non-range wavelength conversion



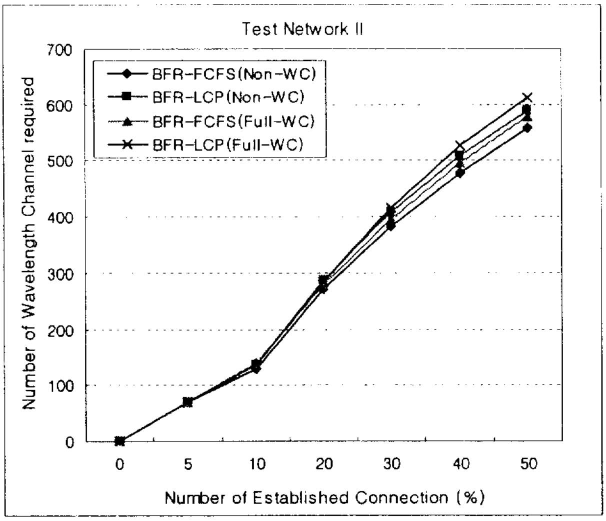
(b) Blocking probability for full, 40% and non-wavelength converters

Figure 19. Blocking probability under limited wavelength conversion

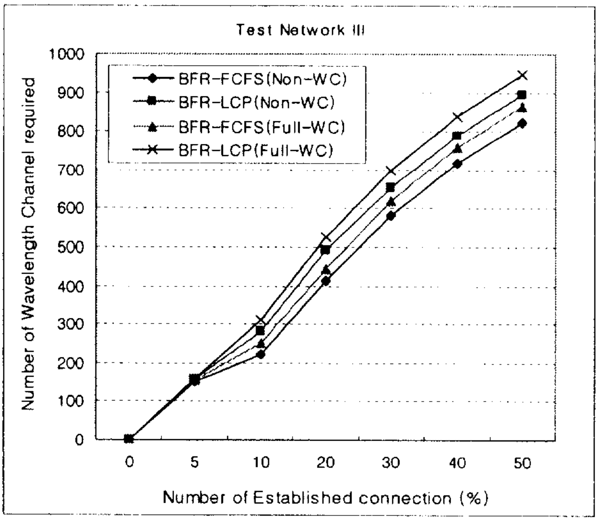
To verify resource utilization performance, we use the number of wavelength channel required as a performance metric. As shown in Figure 20, the proposed BFR algorithm with two different methods (FCFS and LCP) has different performance results. The BFR algorithm with FCFS scheme is better resource saving than LCP scheme. And the number of established connection increases, the difference among the proposed schemes is bigger. From the results in Figure 20, in the aspect of resource utilization, the proposed BFR algorithm with FCFS scheme accomplishes the best performance.



(a) Number of wavelength channel required in Test network I



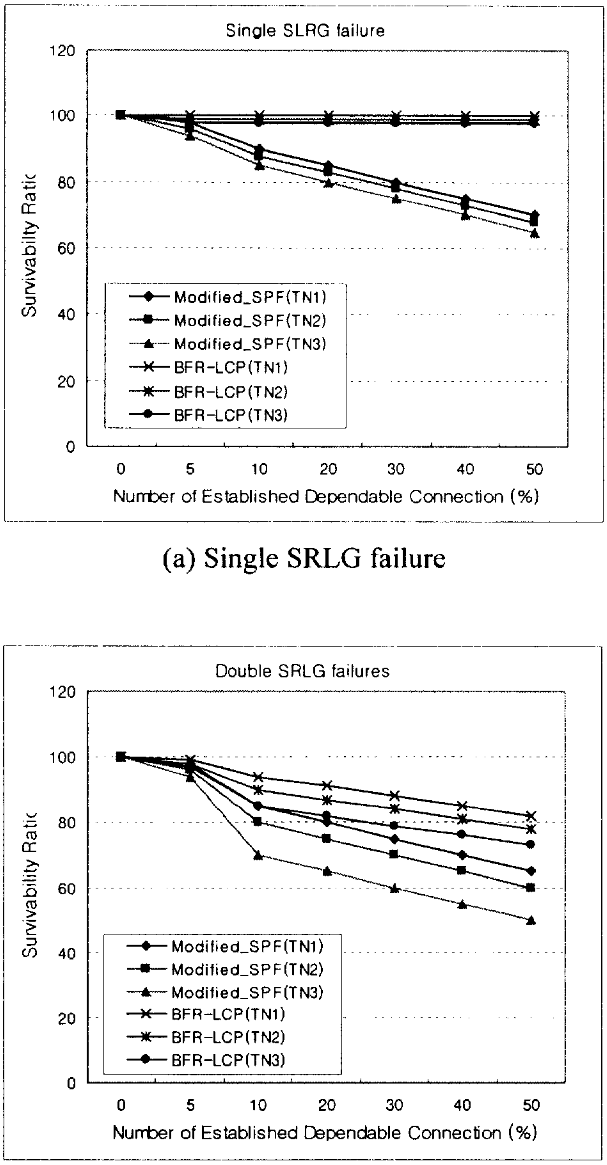
(b) Number of wavelength channel required in Test Network II



(c) Number of wavelength channel required in Test network III

Figure 20. Number of wavelength channels required

Figure 21 summarizes connection survivability (restorability) performances of modified shortest path first (SPF) algorithm and the proposed BFR algorithm in three test networks. In single SRLG failure, the BFR algorithm guarantees 100% survivability, this is due that when the proposed BFR algorithm establishes the dependable connections, SRLG constraint is considered to avoid simultaneous network failure for a primary path and a backup path. Similar observations hold for double SRLG failures, but the survivability of the proposed BFR algorithm can have simultaneous failure. So, there is a little performance degradation. However, it still guarantees over 75% survivability ratio for 50% of total established dependable connections.



(a) Single SRLG failure

(b) Double SRLG failures

Figure 21. Survivability ratio for single and double SRLG failures

As illustrated in section 3.3, differentiated QoP level affects to the network survivability (restorability). In test network I, Figure 22 presents in case of single SRLG failure (SF) and double SRLG failures (DF). For PS (1:1 protection), when a primary path and a backup path are setup under dedicated path protection, SRLG constraint is considered. So, PS achieves 100% restorability for any single failure and almost 80% for double failures. When single SRLG failure occurs, AS (1:3 shared protection) achieves about 80% restorability because AS is established by shared protection scheme considering SRLG. For double SRLG failures, AS has lower survivability ratio than PS, but it is possible to utilize the capacity more efficiently while still achieving over minimum 70%. Moreover, protection mechanisms for both services can guarantee absolute survivability under any circumstances. However, dynamic path restoration for BES can guarantee only relative survivability, according to residual wavelengths. This phenomenon occurs due to discovering a backup path after the primary path fails, not to reserve a backup path in advance.

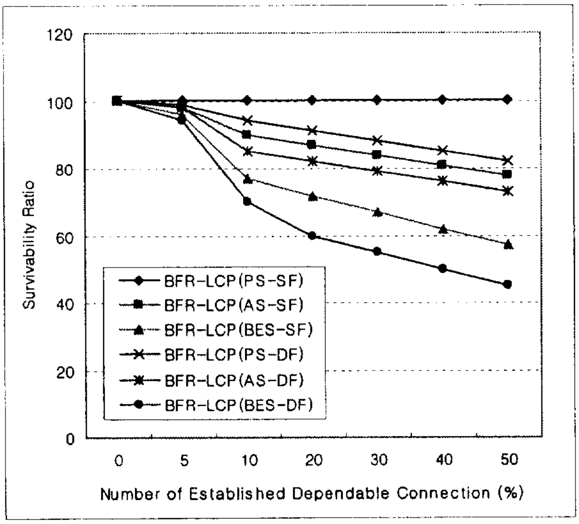


Figure 22. Survivability ratio for differentiated QoP level

VI. Conclusion

In this paper, we proposed a new routing algorithm, bounded-flooding routing (BFR) algorithm. We focused on the network performance improvements in terms of network overhead, blocking probability, resource (wavelength) utilization and survivability (restorability) ratio for dependable connections. And as a bounded criterion, we introduced a new ripple-count concept to classify the messages into three types depending on its necessity. This concept controlled the network overhead without state information and computational process. Also, in intermediate nodes, QoS admission checking mechanism was performed as bounding constraint.

Moreover, for differentiated QoS and QoP level, we analyzed the characteristics for fault and attack possibilities and survivability requirements (SRLG and TA) in OVPN networks. And we guaranteed dependable connections in a parallel way by establishing a primary path and a backup path according to differentiated QoP level for QoS differentiated services.

From the extensive simulation results, we found out that the proposed BFR algorithm is robust compared to the existing algorithms in respect with performance metrics (network overhead, blocking probability, resource (wavelength) utilization and survivability (restorability) ratio).

As a future research, we will study about the additive quality attributes that can be considered during the real path establishment and various applications of the BFR algorithm based on these quality attributes.

References

[1] T. E. Stern and K. Bala, Multiwavelength Optical networks: A layered approach, Addition Wesley Publishers, 1999.

[2] H. Zang, Jason P. Jue, B. Mukheriee, A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks, Optical Networks Mag., vol.1, pp.47-60, Jan. 2000.

[3] Jong-Gyu Hwang, Jae-Il Jung, Yong-Jin Park, Jung-Hyun Bae, Hyun-Su Song, Sung-Un Kim, A RWA Algorithm for Differentiated Services with QoS Guarantees in the Next Generation Internet based on DWDM Networks, Photonic Network Communications, vol.8, no.3, pp. 319-334, Nov. 2004.

[4] Jun Song, Hung Keng Pung, L. Jacob, A multi-constrained distributed QoS routing algorithm, ICON 2000 Proceedings, IEEE International Conference, pp.165-171, Sep. 2000.

[5] Zheng Wang, J. Crowcroft, Quailty of Service Routing for Supporting Multimedia Applications, IEEE Journal of Selected Area Communications, vol. 14, pp. 1228-1234, Sep. 1996.

[6] Shigang Chen and Klara Nahrstedt. An Overview of Quality of Service Routing for the Next Generation High-Speed Network: Problems and Solutions. IEEE Network Magazine, Special Issue on Transmission and Distribution of Digital Video, 1998.

[7] Admela Jukan, Gerald Franzl, Path Selection Methods With Multiple Constraints in Service-Guaranteed WDM Networks, IEEE/ACM Transactions

on Networking, Vol.12, No.1, pp.59-72, FEB. 2004.

[8] Kim, S., Qiao, D., Kodase, S., Shin, K.G., Design and evaluation of routing schemes for dependable real-time connections, IEEE Dependable Systems and Networks, 2001. Proeedings. The International Conference on, pp. 285-294, July 2001.

[9] Mi-Ra Yoon et al., Optical LSP Establishment and a QoS Maintenance Scheme Based on Differentiated Optical QoS Classes in OVPNs, Photonic Network Commun., vol.7, no.2, pp.161-178, March 2004.

[10] J. Lang, Link Management Protocol (LMP), draft-ietf-ccamp-lmp-10.txt, Internet Draft, October 2003.

[11] L. Berger, GMPLS Signaling Resource ReServation Protocol-Traffic Engineering (RSVP-TE) Extensions, IETF RFC 3473, Jan. 2003.

[12] Sahin, G., Subramaniam, S., Providing quality-of-protection classes through control-message scheduling in DWDM mesh networks with capacity sharing, Selected Areas in Communications, IEEE Journal on, Vol. 22, No. 9, pp. 1846-1858, Nov. 2004.

[13] Guoliang Xue, Li Chen, Thulasiraman, K., Quality-of-service and quality-of-protection issues in preplanned recovery schemes using redundant trees, Selected Areas in Communications, IEEE Journal on, Vol.21, No. 8, pp.1332-1345, Oct. 2003.

[14] L. Li and A. K. Somani, Dynamic Wavelength Routing Using Congestion and Neighborhood Information, IEEE/ACM Transactions on Networking, vol. 7, no 5, pp. 779-786, October 1999.

[15] S. Xu et al., Dynamic Routing and Assignment of Wavelength Algorithms in Multifiber Wavelength Division Multiplexing Networks, IEEE Journal on Selected Areas in Communications, vol. 18, no. 10, pp. 2130-2137, October 2000.

[16] Banerjee, D., Mukherjee, B., A practical approach for routing and wavelength assignment in large wavelength-routed optical networks, Selected Areas in Communications, IEEE Journal on, Vol. 14, No. 5, pp. 903-908, June 1996.

[17] J. S. Choi and N. Golmie et al., Classification of Routing and Wavelength Assignment Schemes in DWDM Networks, Proceedings of OPNET 2000 (Paris, France), pp. 1109-1115, January 2000.

[18] J. S. Kim and D. C. Lee, Dynamic Routing and Wavelength Assignment Algorithms for Multifiber WDM Networks with Many Wavelengths, Proceeding of ECUMN 2002 (Colmar, France), pp. 180 -186, April 2002.

[19] Paulo S. André, João L. Pinto, António L. J. Teixeira, José F. da Rocha, Optical-signal-quality monitor for bit-error-ratio assessment in transparent DWDM networks based on asynchronously sampled amplitude histogram, Journal of Optical Networking, vol.1, no.3, pp.118-127, Mar. 2002.

[20] Alcatel's White Contribution COM 15-33-E: Electrical (BER, Q-factor, el. SNR) and Optical (OSNR, OCR) System Performance Parameters for G.DSN, ITU-T SG 15 Contribution, Dec. 2000.

[21] C.P. Larsen, P.O. Andersson, Signal Quality Monitoring in Optical Networks, Optical Networks Magazine, vol.1, no.4, pp.17-23, Oct. 2000.

[22] Rec. G.976: Test methods applicable to optical fibre submarine cable systems, COM15R68 (TSB, 7 Nov. 1996), Sect. 7.6.1.1: 'Measurement of Q-Factor', pp.172-174 and Annex A.4: 'Q-factor' p.178.

[23] A. Jaekel, Z. Hu, Shared path protection based on quality of service in WDM networks, 10th International Conf. on Telecommunications, vol.1, no.23, pp.159-165, Feb.-Mar. 2003.

[24] K.R. Venugopal, M. Shivakumar, P.S. Kumar, A Heuristic for Placement of Limited Range Wavelength Converters in All-Optical Networks, INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE, vol.2, pp.908-915, Mar. 1999.

[25] Amrinder S Arora, Suresh Subramaniam, Wavelength Conversion Placement in WDM Mesh Optical Networks, Photonic Network Communications, vol.4, no.2, pp.167-177, 2002.

[26] S.Subramaniam, M. Azizoglu, A.K. Somani, On the optimal placement of wavelength converters in wavelength-routed networks, INFOCOM '98. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE, pp.902-909, 1998.

[27] Jigesh K. Patel, Sung-un Kim and David H. Su, Modeling Attack Problems and Protection Schemes in All-Optical Transport Networks, Optical Network Magazine, vol.3, no.4, pp.61-72, July/Aug. 2002.

[28] Muriel Medard, D. Marquis, R.A. Barry, S.G. Finn, Security Issues in All-Optical Networks, IEEE Networks, vol.11, no.3, pp.42-48, May/June 1997.

[29] D. Papadimitriou, F. Poppe, J. Jones, S. Venkatachalam, S. Dharanikota,

Inference of Shared Risk Link Groups, draft-many-inference-srlg-02.txt, Internet Draft, Nov. 2001.

[30] E. Mannie, Generalized Multi-Protocol Label Switching (GMPLS) Architecture, IETF RFC 3945, Oct 2004.

[31] Dahai Xu, Yizhi Xiong, Chunming Qiao, Guangzhi Li, Trap avoidance and protection schemes in networks with shared risk link groups, Journal of Lightwave Technology, vol.21, no.11, pp.2683-2693, Nov. 2003.

차세대 광가상사설망에서 차등화된 QoS 및 QoP를 고려한 제한적 플러딩 라우팅 알고리즘 연구

황진호

부경대학교 대학원 정보통신공학과

국 문 요 약

기존 인터넷망에서 사용자의 증가와 그에 따른 요구 대역폭을 수용하기 위한 방안으로 DWDM 기술이 각광 받고 있다. 이러한 DWDM 기술을 활용한 광가상사설망(OVPN - Optical Virtual Private Network)에서 차등화된 QoS (Quality of Service) 및 QoP (Quality of Protection)를 고려한 라우팅 알고리즘의 개발 연구는 중요한 기술중의 하나이다. 본 논문에서는 차등화된 QoS 와 QoP 요구사항을 만족하는 새로운 라우팅 알고리즘을 제안한다. 제안된 알고리즘은 다중 제약조건을 만족하는 QoS 를 보장하는 제한된 플러딩 (Bounded-flooding)을 수행하며, 자원의 효율적 분배를 위해 파장의 수를 제한함으로써 블록률 및 자원 사용률을 개선한다. 또한, 망의 Overhead 를 줄이기 위한 방편으로, 새로운 개념인 Ripple-count 를 소개하며, 이는 link-state 정보와 계산 프로세스 (Computational process)가 없기 때문에 network overhead 측면에서의 성능을 개선한다. 이와 더불어, DWDM 기반의 광가상사설망의 중요사항인 제한된 파장할당(Limited wavelength conversion)을 OVPN 노드에 적용하여 제안된 알고리즘의 광범위한 시뮬레이션을 통해 성능을 평가한다. 그리고, 시뮬레이션에 대한 결과는 제안된 알고리즘이 블록률, 파장 사용률, Overhead 측면에서 기존의 flooding 방식이나 source-directed 방법에 비해 성능이 우수함을 입증한다. 망생존성을 보장하기 위해 제안된 알고리즘은 Shared risk link group (SRLG)과 Trap avoidance (TA) 문제를 고려하여 미리 정해진 QoP 레벨에 따라 병렬 방식으로 주경로와 보조경로를 설정한다. 이는 기존의 Modified SPF (Shortest Path First) 알고리즘과 생존률을 비교함으로써 성능의 우수함을 평가한다.

Acknowledgments

I am deeply grateful to my adviser, Prof. Kim, Sung-Un for the completion of this dissertation. In particular, his diligent, patient guidance and his unselfish sharing of ideas made this dissertation possible. He taught me not only knowledge, but he let me think deep considerations about my life. Moreover, I am very thankful to Prof. Ha, Deock-Ho and Prof. Park, Kyu-Chil for examining this dissertation along with much good advice. Of course, I acknowledge several professors in Dept. of Telematics Engineering, PuKyong National University for considerable instructions and encouragement till now.

Meanwhile, I appreciate all members in the protocol-engineering laboratory. I would like to acknowledge many seniors: Jae-Yun, Young-Suk, Sung-Su, Jae-Ho, Heung-Sik, Eui-Sub, Seong-Kil, Seon-Kyu, Ik-Seob, Mi-Kyoung, Du-Jin, Hyun-Su, Jung-Hyun, Mi-Ra, Chang-Hyun, Kwang-Hyun, Mi-Seon who already graduated. And especially, Suk-Jin gave much advice and helped me during mater's degree course as a colleague. I also thank to Kyung-Dong, Chun-Jae, Jung-Mi, Hyun-Hun, Jong-Geun, Jin-Ho, Ji-Yun and Sang-Bo. Also, I am thankful to Myung-Jin, Jae-Kyu and Dong-Wook who have encouraged me all the time.

Finally, I would like to heartily acknowledge my parents who have devoted themselves to support me even despite of many difficulties and also my lovely sister Sun-Hye and her husband.