논문 2005-42TC-9-10

DWDM 기반의 OVPN에서 네트워크 생존성을 위한 제어 메커니즘 연구

(A Study on the Control Mechanism for Network Survivability in OVPN over IP/GMPLS over DWDM)

조 광 현*, 정 창 현*, 홍 경 동*, 김 성 운*

(Kwang-Hyun Cho, Chang-Hyun Jeong, Kyung-Dong Hong, and Sung-Un Kim)

요 약

"인터넷을 기반으로 하는 VPN(Virtual Private Network)"은 비용과 운용측면에서 효율적이다. 하지만 광 대역폭 그리고 신뢰성 있는 서비스에 대한 요구의 증가는 IP/GMPLS over DWDM 기반의 백본 네트워크가 차세대 OVPN (Optical VPN)을 위하여 가장 적합한 백본 네트워크로 간주되게 하였다. 그러나, 높은 데이터 전송율을 가지는 OVPN망에서 광 소자의 일시적인 fault/attack에 의해서 일어나는 서비스 파괴는 순식간에 막대한 트래픽 손실을 야기 할 수 있으며, 비 인가된 physical attack으로 인하여 물리적인 구성소자를 통해 정보가 도청 될 수 있다. 또한 데이터 전송을 관리하는 제어 메시지가 변조되거나 복사되어 조작될 경우 데이터가 전송도중 실패하더라도 망의 생존성을 보장할 수가 없게 된다. 따라서, OVPN에서는 생존성문제 (i.e. fault/attack에 대한 물리적인 구조와 광 소자를 고려한 최적의 복구 매커니즘, 그리고 GMPLS 제어메시지의 보안성 있는 전송) 가 중요한 이슈로 대두되고 있다. 본 논문에서는 fault/attack을 관리하기 위해 광 소자들과 공통된 위험 요소를 포함하는 소자들을 분류하고, SRLG (Shared Risk Link Group)를 고려한 경로 설립 스킴과 GMPLS의 RSVP-TE+(Reservation Protocol-Traffic Engineering Extension)와 LMP(Link Management Protocol)의 보안성 제공 메커니즘을 제안하여, OVPN에서의 생존성을 보장한다. 끝으로 시뮬레이션 결과를 통하여 제안된 알고리즘이 망 생존성을 위하여 더욱 효율적임을 증명하였다.

Abstract

A "Virtual Private Network (VPN) over Internet" has the benefits of being cost-effective and flexible. However, given the increasing demands for high bandwidth Internet and for reliable services in a "VPN over Internet," an IP/GMPLS over DWDM backbone network is regarded as a very favorable approach for the future "Optical VPN (OVPN)" due to the benefits of transparency and high data rate. Nevertheless, OVPN still has survivability issues such that a temporary fault can lose a large amount of data in seconds, moreover unauthorized physical attack can also be made on purpose to eavesdrop the network through physical components.Also, logical attacks can manipulate or stop the operation of GMPLS control messages and menace the network survivability of OVPN. Thus, network survivability in OVPN (i.e. fault/attack tolerant recovery mechanism considering physical structure and optical components, and secured transmission of GMPLS control messages) is rising as a critical issue. In this paper, we propose a new path establishment scheme under shared risk link group (SRLG) constraint for physical network survivability. And we also suggest a new logical survivability management mechanism by extending resource reservation protocol-traffic engineering extension (RSVP-TE+) and link management protocol (LMP). Finally, according to the results of our simulation, the proposed algorithms are revealed more effective in the viewpoint of survivability.

Keywords : OVPN, GMPLS, RSVP, SRG

I. Introduction

As the Internet and optical network technology advances, the IP over DWDM has been envisioned as the most promising solution for the next generation

* 정회원, 부경대학교 정보통신공학과
(Pukyong National University)
※ 본 논문은 한국과학재단 특정기초연구과제(R01-2003-000-10526-0)의 지원으로 수행되었습니다.
접수일자: 2005년1월6일, 수정완료일: 2005년6월30일

optical Internet (NGOI). Especially, core transport networks in NGOI are currently in a transition period evolving from SONET/SDH-based time division multiplexed (TDM) networks utilizing a single wavelength to dense-wavelength division multiplexed (DWDM) networks with the multiple wavelengths strictly for fiber capacity expansion. On purpose to control for both optical and electronicnetworks, generalized multi-protocol label switching (GMPLS) has shown up and is currently under standardization at the Internet engineering task force (IETF)[1-3]. Therefore IP/GMPLS over DWDM network is emerging as a dominanttechnology for use in the next generation backbone network.

VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The primary advantages of "VPN over Internet" are cost-effectiveness and flexibility while coping with the exponential growth of Internet. However, the current disadvantages are the lack of sufficient quality of service (QoS) and provision of adequate transmission capacity for high bandwidth services. For resolving these problems, OVPN over the next generation optical Internet (NGOI)[4] has been suggested for supporting a variety of guaranteed high bandwidth-needed services in OVPN, but it still needs to provide optical QoS provisioning as described in [5], and the network survivability.

For the network survivability in OVPN, unlike in the case of the existing network, the coordinated survivability mechanism considering intrinsic OVPN features is necessary. First of all, a recoverystrategy should be determined before optical-label switched paths (O-LSPs) set up[6-9]. After data transmission starts,when failure occurs, the sequential mechanism is needed as follows: detect fault/attack as soon as possible (detection), separate fault/attack from normal traffic (localization), notify fault/attack to network elements which are responsible for network management (notification) and recover traffic to avoid fault/attack (protection or restoration)[10-12]. Recently, a key feature of GMPLS is the backup path establishment that keeps physical-diversity (which is also called by physical-disjoint). This is also a dominant issue in OVPN backbone network. In OVPN, each link set up in one O-LSPmay cross one or more optical components, where the fault/attack of optical components may result in the potential failure of the link. A component here essentially presents any part or site involved in the integrity of the links and associated with a shared risk group (SRG) defined as resource groups having shared risk in common[13-15].

On the other side, the control messages of GMPLS have to be secured such that an attacker may spoof, modify or replay control messages. Therefore GMPLS should provide authentication, integrity and replay protection because an adversary's malicious behaviors can consequently menace the network survivability by means of purposeful misuse of network resources or service denying. Especially, LMP fully depends on IP security protocol (IPsec)[16], so it concludes in delay of traffic recovery that directly affects the network survivability and low efficiency.

In this paper, we propose a new path establishment scheme under SRLG constraint in accordance with fault and physical attack coverage of optical components, and a new security mechanism for RSVP-TE+ and LMP control messages. The rest of this paper is organized as follows: section II describes OVPN structure with considering management sections and GMPLS operation. In section III, network survivability in OVPN ispresented in the aspect of both physical and logical survivability phases, and a SRG is defined according to the coverage of fault/attack. In section IV, we illustrate the proposed management mechanisms, and evaluate their performances through simulation in section V. Finally, some concluding remarks are made in section VI.

II. OVPN Structure and Operation

1. OVPN Structure and Management Sections

The suggested OVPN structure in figure 1 consists of the customer sites in the electric domain and the DWDM network in the optical domain, and GMPLS

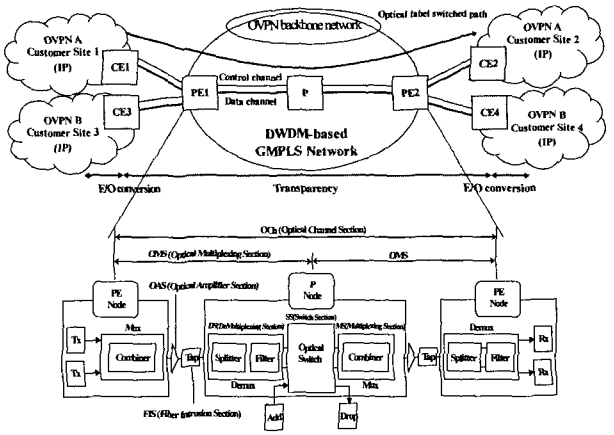


그림 1. OVPN 구조
Fig. 1. OVPN Structure.

in the control domain. The external customer sites based on IP network aggregate (or de-segregate) IPpackets at customer edge (CE) nodes and the internal OVPN backbone network composed of the provider edge (PE) nodesand the provider (P) core nodes forwarding data traffic between the customer sites without optic-electronic-optic (O-E-O) conversions[5].

An established O-LSP between the CE1 and the CE2 may cross a number of intermediate P nodes interconnected by fibersegments, amplifiers and optional taps. The optical components that constitute a P 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 P node also contains a transmitter array (Tx) and a receiver array (Rx) enabling local add/drop of the wavelengths.

In this structure, we can describe three management sections taking into consideration resource types (optical components) and the coverage of fault/attack effects. And we suggest that the OVPN has structure as follows:

- Optical Channel Section (OCh): Channel management section for one O-LSP established between CE 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).
- P (or PE) 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).

2. GMPLS Operation in OVPN

To initiate the OVPN operation based on the GMPLS control protocol, one or more bi-directional controlchannels 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[5].

The consecutive sub-flows of control-flow are illustrated in figure 2. For the figure 2(A), the LMP activates control channels for all linksbetween the CE1 and CE2, and (B) represents the routing protocol that

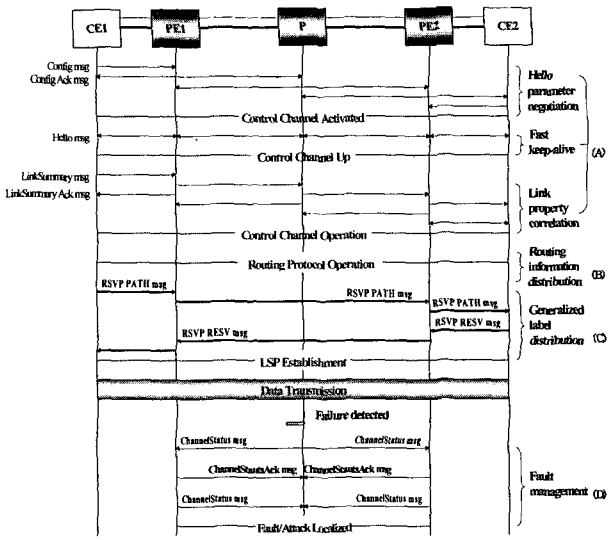


그림 2. OVPN에서 GMPLS 프로토콜 동작
Fig. 2. Operation of GMPLS protocol in OVPN.

exchanges routing information. Figure 2(C) shows the label distribution procedure between CE1 and CE2, and O-LSPs establishment procedure by RSVP-TE+. 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[17-18].

III. Network Survivability in OVPN

1. Analysis of Network Survivability

The ramification of network survivability in OVPN is depicted in figure 3. Physical survivability contains fault management (i.e. system (fault) management and signal degradation management) caused by a sudden mishap of optical components, and physicalattack management. Physical attack management needed to be managed in optical layer somehow causes signal degradationor abnormal signals by maliciously using intrinsic characteristics of optical components[10-12]. On the other hand, logical survivability in OVPN includes logical attack management, in general, logical attack in data-plane is defined as an unauthorized person's network access on purpose to modify or to eavesdrop information, and it has to be dealt by quantum cryptography. However, this is beyond the scope of this paper. We just focus on control plane security for control messages of GMPLS.

2. Physical Survivability

OVPN has many fault possibilities due to the vulnerable characteristics of optical components used in DWDM network, so short and sporadic failures of network elements may cause a large amount of data loss. In the physical

survivability, the physical fault (or hard fault) on optical components has to be considered first. It causes failure in all optical channels that are going through a link or in a specified optical channel. The coverage of faults is specified depending on the optical components, and resource types. The coverage of faults is summarized in table 1. In addition, optical components such as optical fiber or erbium-doped fiber amplifier (EDFA) can be used by the attack point to cause signal degradation or to eavesdrop information. For example, gain competition attack causes signal degradation in optical channels thatare going through a link by using intrinsic feature of EDFA as mentioned in [12]. With reference to the OVPN structure shown in figure1, we categorize attack issues at two functional levels depending on attack methods, and they are summarizedin table 1 [10-11].

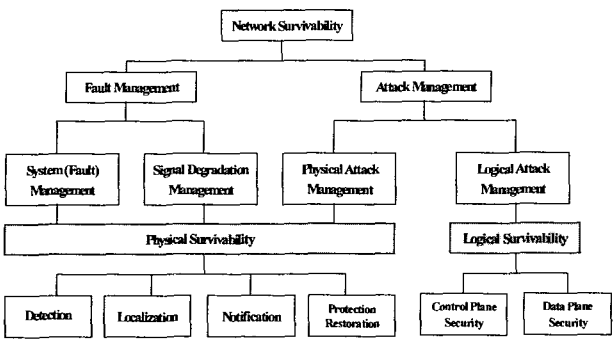


그림 3. OVPN의 생존성 분석
Fig. 3. Analysis of survivability in OVPN.

We suggest that the fault/attacks are classified in OVPN as follows:

- 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 or PE node) that are unlikely to

표 1. OVPN에서 Fault/AttacK와 SRG 분류
Table 1. Fault/Attack and SRG classification in OVPN.

Category	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
		Pump laser temperature due to high current			
	Receiver	Out of range power or unacceptable input optical power	Unauthorized access to information attack		
Link (OMS)	Fiber (FIS)	Fiber damaging or cutting	Fiber cut or optical power reduction		Fiber
			Tapping only or jamming only		S
			Tapping & Jamming		R
	Amplifier (OAS)	Amplifier optical path failure (due to fiber cutting)	Gain Competition due to local attack		Conduit L
		Passive component failure with in the amplifier	Gain Competition due to remote attack		G
		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	
		Out of range power or unacceptable input optical power			
	Switch (SS)	Electronic driver failure at switch, Misrouting	Intentional crosstalk using high power signal		S
		Input power is over/under threshold or out of range	Unauthorized access to information using crosstalk		R
	Mux (MS)	Electronic driver failure at Mux or Optical filter failure	Intentional crosstalk propagation from preceding devices		N
		Out of range power or unacceptable input optical power			G

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.

In OVPN, a single fault or attack has various coverage of effects (OCh, OMS, node) depending on resource types or fault/attack types. Thus a recovery mechanism needs to be done by making common risk group to avoid common fault/attack.

A SRG is defined as a group of links or nodes that share a common risk component, whose fault/attack can potentiallycause the failure of all link or node in the group. When the SRG is applied to the link resource, it is referred to SRLG. For example, all fiber links that go through a common conduit under the ground belonging to the same SRLG, because the conduit is a shared risk component whose failure, such as a cut, may cause all fibers in the conduit to be broken simultaneously. This SRLG is introduced in the GMPLS and can be identified by a SRLG identifier, which is typically a 32-bit integer[1]. On the other side, the SRG is applied to the node, and it is referredto SRNG[14]. SRNG has to be controlled by a network manager, because it may affectthe whole network survivability. In this paper, in accordance with resource types and coverage of fault/attack effects, we suggest that the SRLG has three levels as follows:

- SRLG in channel level: sub-channels that are aggregated in one established channel (O-LSP) have the same risk level. This SRLG information can be applied to routing constraint via multiple domains.
- 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 nodescan have physical structure bundled by a conduit. Thus fibers in a conduit have the same risk level to failure.

3. Logical Survivability

Logical survivability contains logical attack management for possibly manipulating and stopping the operation in OVPN. In a control plane of OVPN, it is needed to ensure the control messages are originating from the right place and have not been modified in transit, if not, manipulated control messages can be fatal to guarantee the network survivability. In the sub-sections, we discuss security vulnerabilities of two protocols, RSVP-TE+ and LMP [17-20].

3. 1 RSVP-TE+ Security Problem

The label distribution procedure of RSVP-TE+ to establish O-LSP in OVPN is depicted in figure 4. The PATH message allocates wavelengths or ports with RSVP-TE+ objects such as Generalized Label Request, Suggested Label, Label Set, Upstream Label, and so on. If PE2 receives a PATH message, labels are distributed through the optical path between PE1 and PE2.

The existing RSVP-TE+ provides a security mechanism through hop-by-hop authentication mechanism using an encrypted hash function. The

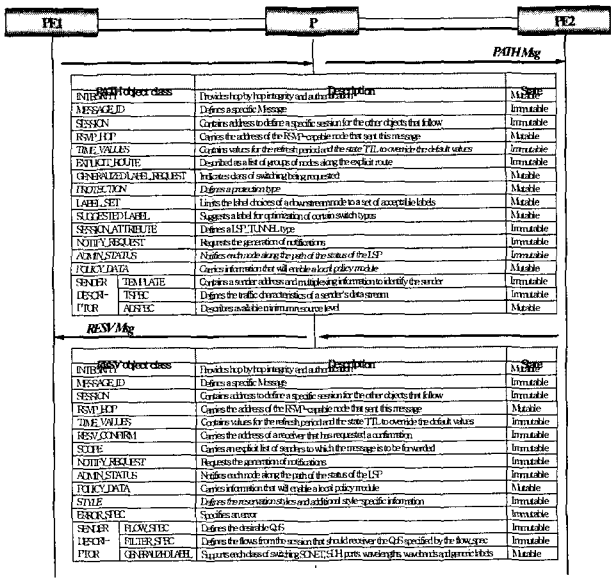


그림 4. RSVP-TE+ 객체 상태
Fig. 4. RSVP-TE+ object State.

표 2. RSVP-TE+의 논리적 attack 가능성
Table 2. Logical attack possibilities of RSVP-TE+.

Attack type		Description
Control flow attack	Denial of QoS Service	Intercept or drop all or some of the signaling messages such that the QoS reservation and O-LSP establishment can be failed or willfully delayed in a persistent way.
	Inaccurate O-LSP Establishment	Modify all or some of the signaling messages when O-LSP is established.
	Unnecessary Resources Reservation	A customer really wants to reserve low bandwidth but the attacker causes the system to reserve high bandwidth, while low bandwidth is significantly different from high bandwidth.
	Degradation of Network Utilization	The network system as a whole, has enough resources to support a set of QoS requests, S_{req}, but the attacker can, for instance, interfere with the reservation protocol such that the network can only support a small subset of S_{req}: S_{small}.
	Reserved QoS Degradation	Even if the resource reservation process is successful, the attacker can still steal the reserved resources. In other words, even the resources along the path has been reserved and maintained successfully, attackers can use the reserved resource unauthorizedly.

mechanism is supported by INTEGRITY object that may appear in RSVP-TE+ message[19]. Some of the RSVP-TE+ objects, called mutable objects as shown in figure 4, remain unchanged from PE1 to PE2 (or vice versa) and others may be updated by the intermediate nodes (P). The integrity of the mutable RSVP-TE+ objects is hard to be guaranteed at the end nodes, that is, in the intermediate nodes mutable objects can be changed by an adversary's malicious behaviors[9].

The logical attack possibilities of RSVP-TE+ are shown in table 2. An intruder can attack directly on the signaling/control protocol forthe purpose of exploiting network resources and manipulating LSP establishment procedure, which results in the victim O-LSP (Link) that is an unavailable O-LSP to other users. Furthermore, even if the resource reservation process is successful in O-LSP, an intruder can still attack the data-flow such that some or all the reserved resources are not exploited appropriately by modifying control messages. These aspects motivate an end-to-end security mechanism, so we propose the extended RSVP-TE+ management mechanism in the next section.

3. 2 LMP Security Problem

The security of LMP depends on the IPsec protocol that is a protocol suite used to secure communication between two peersbecause the LMP does not support any security mechanism by itself[17]. However, all nodesin OVPN have to be equipped with IPsec protocol, and it takes much time for encryption and decryption processes[21].

Conclusively, these may intimidate the networksurvivability into disrupting services. In order to overcome scalability and low suitability of the existing LMP security mechanism, we suggest an extended LMP in the next section.

Ⅳ. Survivability Management Mechanism

1. Physical Survivability Management Mechanism

As discussed earlier, in order to achievefault/attack tolerant recovery mechanism, a backup path has to keep physical-diversity with a primary path because the failures of optical components, as described in table 1, result in the potential failure of the link. Thus the recovery mechanism considering SRLG is essentially needed for network survivability in OVPN. On the other hand, a node failure is actually just a special case of SRNG where links are placed in groups based on whether or not they share a common node. A network manager should control it to avoid the service disruption of the whole network survivability.

Keeping in mind that SRLG is the most important criteria concerning the constrained-based path computation of O-LSPs, one can select a path taking into account diversity of physical resources and logical structure by applying the SRLG criteria to the constraint-based path computation. So, we propose a new path establishment scheme under SRLG constraint below.

The notations used in this paper are as follows:

- $G(N, L)$: The given network, where N is the set of nodes and L is the set of links.
- M: The set of source-destination connection request pairs.
- C_{ab}^{l}: The link cost between link pair (a, b) where (a, b)∈(s, d)/M.
- $srlg_{ab}^{l}$: The set of SRLG IDs in a link pair (a, b) where (a, b)∈(s, d)/M.
- $srlg_{ab}^{p/ab}$: The set of SRLG IDs used in a primary path (s, d) where (s, d)∈M.

- $R(l)$: The number of currently available wavelengths on a link l where l∈L.
- △: A threshold value of available wavelengths on a link (20 %~30 % of W)

The procedure, how to find a primary path and a backup path, is described as follows:

STEP1: Correlate the network resources and compute C_{ab}^{l} for all (a, b) included in G(N,L).

STEP2: Wait for a request between a (s, d) pair as the current demand where (s, d)∈M.
If it is a connection request, go to STEP 3.
If it is a connection release request, go to SETP 8.

STEP3: Find the k-shortest paths as the candidates for a primary path.

SETP4: SRLG identifiers are correlated between end nodes. Update $srlg_{ab}^{p/ab}$.

SETP5: Update link cost:
$C_{ab}^{l} : [(srlg_{ab}^{l} \in srlg_{sd}^{p/ab}) \cup (R(l) < \triangle)]$.

STEP6: Choose a path as a primary path that can have an alternate path among k-shortest paths, and route the request through the primary path between node s and node d.

STEP7: Reserve an alternate path as the request for a backup path between node s and node d, go to STEP 9.

SETP8: Release the primary path and the backup path pair (s, d).

STEP9: Update the network resource states, go to STEP 1.

The STEP 5 is the most important step because it updates the cost of all links depending on the condition, $C_{ab}^{l} : [(srlg_{ab}^{l} \in srlg_{sd}^{p/ab}) \cup (R(l) < \triangle)]$ which means whether or not the backup path has the same risk in common with the primary path and somewhat relieves the network congestion by limiting the number of wavelengths to reduce the number of O-LSPs that fail at the same time. The recovery mechanism provides very fast and simple and is evaluated by blocking probability (BP) and survivability ratio (SR) as the performance evaluation metrics, and these are defined as (failed connections)/(connection requests) and (service disruptions)/(successfully established connections), respectively. The service disruptions here present that when a primary path is failed, and there is no backup resource available, then the service on this primary path will be disrupted. The metrics show performance evaluation results in the viewpoint of survivability in the next section.

2. Logical Survivability Management Mechanism

2. 1 Extended RSVP-TE+ Management Mechanism

We propose an end-to-end authentication mechanism instead of using hop-by-hop mechanism of the existing RSVP-TE+. Some RSVP-TE+ objects are meant to be immutable and some to be mutable along the path. For the immutable objects, a sender digitally signs the object with its own private key. A very important observation is that some mutable objects become immutable at a certain point in the path. For the mutable objects, the receiver sends back RESV message piggybacking with, additionally, the mutable objects that just received. Piggybacked mutable objects in the RESV message are selectively and digitally

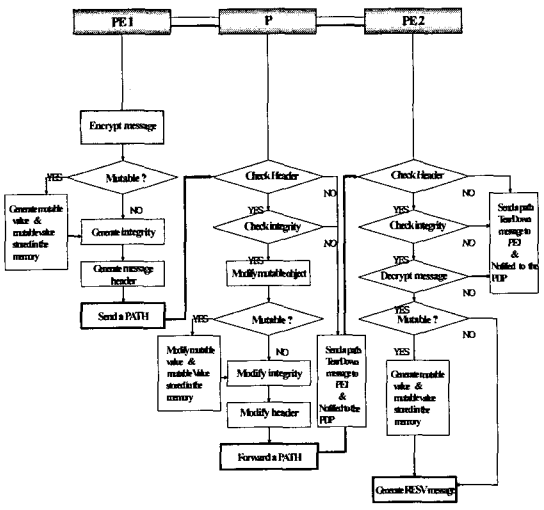


그림 5. 종단간 암호화 메커니즘(PATH 메시지)
Fig. 5. End-to-end security mechanism. (PATH Message)

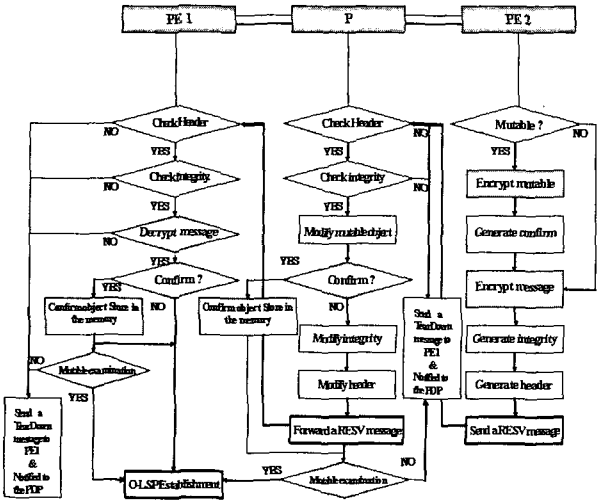


그림 6. 종단간 암호화 메커니즘(RESV 메시지)
Fig. 6. End-to-end security mechanism. (RESV Message)

signed with the receiver's private key. Although a computationally expensive operation, digital signatures can be verified at every point in path, protecting the committed messages from being tampered. Figure 5, 6 describes in detail the end-to-end security mechanism procedure of extended RSVP-TE+.

The procedure, how to provide the end-to-end security mechanism, is described as follows:

STEP1:PE1 digitally signs with its private key and encrypts the immutable object values with a public key.

STEP2: When PE1 forwards a PATH message to PE2, intermediate P node stores mutable object values in the memory.

STEP 3: Upon receiving a PATH message, PE2 verifies the integrity of immutable objects using a public key of PE1. If conflicts, PE2 sends a TearDown message to PE1 for withdrawal of a PATH message and notifies to the policy decision point (PDP) [22].

STEP 4: PE2 Generates a Confirm object that encrypts the mutable objects message with a private key. The Confirm object format is shown in Figure 7. PE2 sends RESV message piggybacking with a Confirm object. Both messages are digitally signed by PE2.

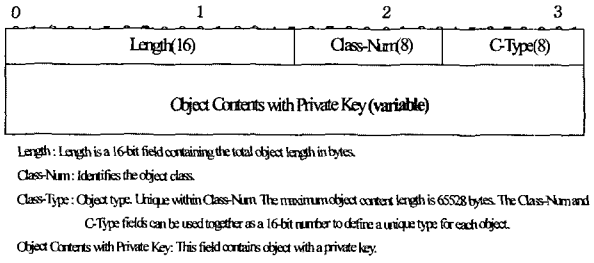


그림 7. RSVP-TE+의 Confirm 객체
Fig. 7. Confirm object of RSVP-TE+ .

STEP5: Before intermediate P node sends RESV message to PE1, intermediate P node stores a Confirm object in memory. After intermediate P node sends RESV message, Intermediate P node verifies that the piggybacked and signedConfirm object is equivalent to the mutable object values in the memory. If it is not, P node sends a TearDwon message to PE1 for withdrawal of a PATH message and notifies to the PDP.

STEP6: When PE1 receives a RESV message, it verifies that it is signedby a valid PE2. Otherwise PE2 sends a TearDwon message to PE1 for withdrawal of a PATH message and notifies to the PDP.

2. 2 Extended LMP Management Mechanism

By sending a Confirm object that is encrypted by a private key, extended LMP can optionally provide security to the objects that possibly can be attacked, and the Confirm object is depicted in figure 9. Especially, Extended LMP management mechanism achieves rapid localization needed to guarantee the network survivability and considerably low computational complexity and high efficiency due that we provide selectively security for required fields in objects. We describe security mechanism of extended LMP, as illustrated in Figure 2(D), with a failure localization of LMP between PE1 and P as the case that directly affects the network survivability. Figure 8 shows it at a glance.

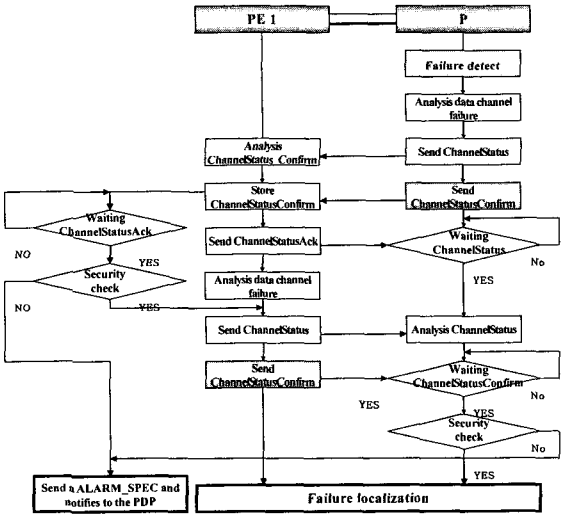
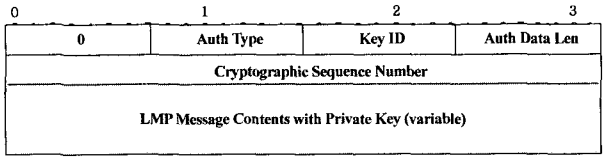


그림 8. 확장된 LMP 암호화 메커니즘
Fig. 8. Extended LMP security mechanism.



Auth Type: This defines the type of authentication used for LMP messages.
Key ID: This field is defined only for cryptographic authentication.
Auth Data Length: This field contains the length of the data portion of the authentication block.
Cryptographic Sequence Number: This field is defined unique number.
LMP Message Contents with Private Key: This field contains LMP message with a private key.

그림 9. 확장된 LMP의 Confirm 객체
Fig. 9. Confirm object of extended LMP.

P (downstream node in terms of data flow) that detects data link failures sends a ChannelStatus message to PE1(upstream node in terms of data flow) indicating that a failure has been detected and P also sends ChannelStatus_Confirm object that encrypts the ChannelStatus message with a private key. This follows right behind the original ChannelStatus message and is depicted in figure 9. Thereafter, PE1 responds to P with ChannelStatusAck message immediately, and then PE1 verifies the integrity of ChannelStatus message using a public key of P, but if conflict, PE1 sends an ALARM SPEC object [23] to P, and notifies to the PDP that can decide the security policy.

Otherwise, once the failure is correlated, PE1 should send a ChannelStatus message with ChannelStatus_Confirm message to P indicating that the channel is failed or ok.

P verifies the integrity of ChannelStatus message, and then localizes the failure. After all, the signaling protocols may be used to initiate recovery procedures.

V. Performance Evaluation

In this section, simulation is carried out to evaluate the performance for both physical and logical survivability-guaranteed mechanism. To prove the efficiency, we analyze the results of blocking probability and survivability ratio with or without SRLG constraint, and compare the processing time of extended LMP that we propose with that of LMP that uses IPsec protocol.

1. Physical Survivability Phase

A simulation is conducted to verify the performance on the test network with 30 nodes and 61 links. The network topology is shown in figure 10, and we allocate arbitrary conduit level in the physical topology, which is composed of fiber groups. The assumptions for the simulation are as follows: i) links are bi-directional, each link has two fibers to different directions and the number of wavelengths per a fiber

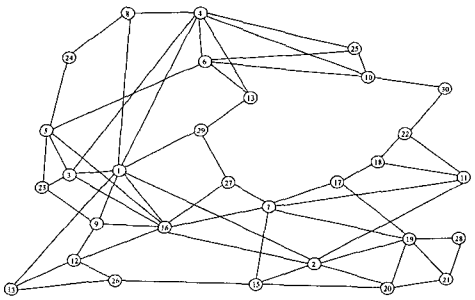


그림 10. 시뮬레이션에 사용된 시험망
Fig. 10. Test network used in simulation.

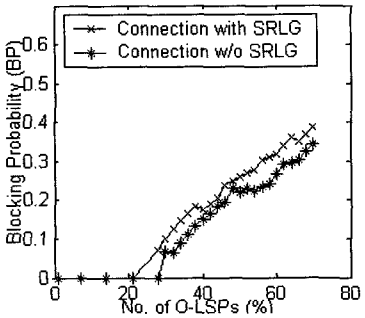


그림 11. 블럭확률
Fig. 11. Blocking probability.

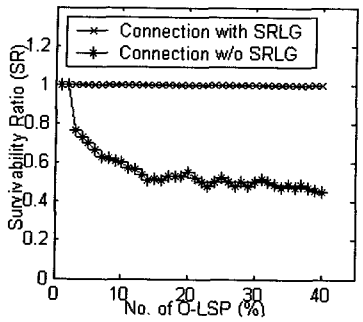


그림 12. 생존율
Fig. 12. Survivability ratio.

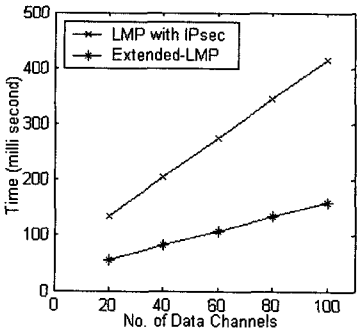


그림 14. 시간 지연
Fig. 14. Time delay.

is 8. ii) all nodes have wavelength converters. iii) the topology is static and is not reconfigured during the simulation.

The numerical results of blocking probability and survivability ratio are plotted as a function of the number of traffic O-LSPs in figure 11, 12.

In the case of the blocking probability, connection establishment with SRLG is slightly higher than connection establishment without SRLG. However, the survivability ratio guarantees that the recovery mechanism recovers the failed traffic 100% for a single conduit level failure. Thus, the results of therecovery mechanism confirm better performance in the viewpoint of survivability.

2. Logical Survivability Phase

In order to evaluate the performance of the security mechanism in LMP, we performed a simulation using socket programming. The simulation environment is

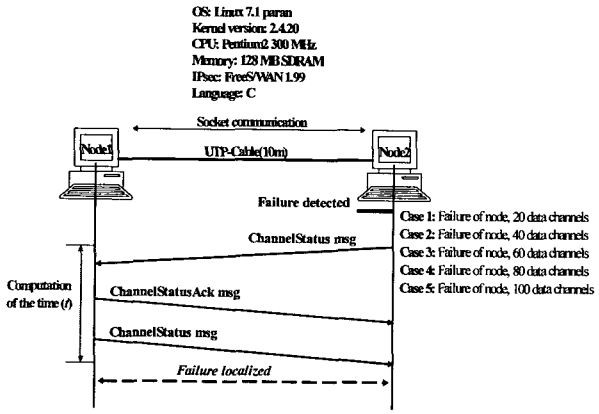


그림 13. 시뮬레이션 환경
Fig. 13. Simulation environment.

setup in figure 13 that proceeds failure localization of LMP, and socket connection between nodes which are Pentium-II with 300 MHz rate for one million 1024 byte messages, and then we compare the time (t) of extended LMP with that of the existing LMP along case 1~5. Each simulation is executed 100 cycles of localization procedure because t is too short to observe. In order to correct the time, we run 1000 cycles of the simulation. Figure 14 verifies that extended LMP that we propose is better than LMP that uses IPsec protocol. In order words, Extended LMP security mechanism guarantees rapid processing, that is, it consequently makes localization procedure fast.

VI. Conclusion

In this paper, we proposed a coordinated network survivability-guaranteed mechanism in OVPN over IP/GMPLS over DWDM. In the physical survivability aspect, the core point is to keep physical-diversity (SRLG-disjoint) between a working path and a protection path. In the logical survivability aspect, we suggested an end-to-end authentication mechanism instead of using hop-by-hop mechanism of the existing RSVP-TE+. And then we described an extended LMP mechanism to overcome scalability and low suitability of the existing LMP security mechanism. According to the results of our simulation, the proposed algorithms are revealed more effective in the viewpoint of survivability. In the near future, we have a plan to develop a more specified network survivability mechanism which includes total of

physical and logical survivability issues.

References

[1] E. Mannie et al., "Generalizaed Multi-Protocol Label Switching (GMPLS) Architecture," draft-ietf-ccamp-gmpls-archtecture-07.txt, IETF Internet Draft, Work in progress, May 2003.

[2] A. Banerjee, et al., "Generalized multiprotocol label switching: an overview of signaling enhancements and recovery techniques," IEEE Commun. Mag., vol.39, no.7, pp.144-151, January 2001.

[3] D. Papadimitriou, E. Mannie, "Analysis of Generalized MPLS based Recovery Mechanisms (including Protection and Restoration)," draft-ietf-ccamp-gmpls-recovery-analysis-02.txt, IETF Internet Draft, Work in progress, May 2003.

[4] Hamid Ould-Brahim et al., "Service Requirements for Optical Virtual Private Networks," draft-ouldbrahim-ppvpn-ovpn-requirements-01.txt, IETF Internet Draft, Work in progress, July 2003.

[5] 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.

[6] Yun Wang et al., "Dynamic Survivability in WDM Mesh Networks under Dynamic Traffic," Photonic Network Commun., vol.6, no.1, pp.5-24, July 2003.

[7] Guido Maier, Achille Pattavina, et al., "Optical Network Survivability: Protection Techniques in the WDM Layer," Photonic Network Communications, vol.4, no.3/4, pp. 251-269, July/December. 2002.

[8] Haibo Wen et al., "Dynamic RWA Algorithms under Shared-Risk-Link-Group constraints," IEEE 2002 International Conference on, vol. 1, pp.871-875, July 2002.

[9] Tsung-Li Wu et al., "Securing QoS: Threats to RSVP Messages and Their Countermeasures," Int'l Workshop on Quality of Service, pp.62-64, June 1999.

[10] Jing Zhang et al., "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges," IEEE Network, vol. 18, no.2, pp.41-48, March/April 2004.

[11] 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/August 2002.

[12] Muriel Medard et al., "Security Issues in All-Optical Networks," IEEE Networks, vol.11, no.3, pp.42-48, May/June 1997.

[13] Panagiotis Sebos et al., "Auto-discovery of Shared Risk Link Groups," Optical Fiber Communication Conference, 2001.

[14] D. Papadimitriou et al., "Inference of Shared Risk Link Groups," draft-many-inference-srlg-02.txt, IETF Internet Draft, November 2001.

[15] Sebos, P. et al., "Effectiveness of shared risk link group auto-discovery in optical networks," Optical Fiber Communication Conference and Exhibit, pp.493-495, 2002.

[16] S.kent et al., "Security Architecture for the internet Protocol," IETF RFC2401, November 1998.

[17] J.Lang et al., "Link Management Protocol (LMP)," draft-ietf-ccamp-lmp-10.txt, IETF Internet Draft, Work in progress, October 2003.

[18] F.Baker et al., "LMP Security Mechanism," draft-sankar-lmp-sec-00.txt, IETF Internet Draft, Work in progress, February 2003.

[19] F.Baker et al., "RSVP Cryptographic Authentication," IETF RFC 2747, January 2000.

[20] L. Berger, et al., "GMPLS Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP -TE) Extensions,"IETF RFC 3473, January 2003.

[21] Hyun-dong Park et al., "Design of Security Framework for Optical Internet and Performance Test,"WISC 2003 fifteenth Workshop on Information Security and Cryptography, pp. 695-707, September 2003.

[22] D.Durham et al., "The COPS(Common Open Policy Service) Protocol," IETF RFC 2748, January 2000.

저 자 소 개

Kwang Hyun Cho(정회원)

Feb. 2003: B. S. degree in Telematics Engineering from TongMyong University.

Feb. 2005: M.S. degree in Telematics Engineering from Pukyong National University.

Mar. 2005~: KT Networks Inc. Junior Engineer(R&D).

<Interest research: OVPN, QoS, DWDM, Survivability.>

Kyung-Dong Hong(정회원)

Feb. 2004: B. S. degree in Electronics from Pukyong National University.

Mar. 2004~: M. S. course in Telematics Engineering from Pukyong National University.

<Interest research: DWDM, RWA, QoS, Survivability.>

Chang-Hyun Jeong(정회원)

Feb. 2003: B. S. degree in Telematics Engineering from Pukyong National University.

Feb. 2005: M. S. degree in Telematics Engineering from Pukyong National University.

Mar. 2005~: Insopack Inc. Researcher(R&D).

<Interest research: OVPN, QoS, DWDM, Survivability.>

Sung-Un Kim(정회원)

Dec. 1982~Sep. 1985: Electronics and Telecommunications Research Institute(ETRI)

Oct. 1985~Aug. 1995: Korea telecom research Labs. (KTRL).

Aug. 1990: M. S. degree in Computer Science from Paris 7 in France.

Aug. 1993: Ph. D. degree in Computer Science from Paris 7 in France.

Sep. 1995~: Associate professor in the Department of Telematrics Engineering, Pukyong National University.

<Interest research: DWDM optical network, RWA, QoS, GMPLS, protocol engineering.>