차세대 OVPN에서 망의 생존성을 위한 LMP 확장

조광현[0], 배효진*, 정창현, 서미선, 김성운
부경대학교 정보통신공학과
안동대학교 컴퓨터교육과*
{hyun[0] , jch123, jljpms@mail1.pknu.ac.kr, aslay@kebi.com* , kimsu@pknu.ac.kr

LMP Extension for Network Survivability In Next Generation Optical VPN

Kwang-Hyun Cho[0], Bae Hyoe Jin*, Chang-Hyun Jeong, Mi-Seon Seo, Sung-Un Kim
Dept. of Telematics Engineering, Pu-Kyong National University
Dept. of Computer Education, An-Dong National University*

요 약

본 논문에서는 차세대 OVPN(Optical Virtual Private Network)에서 제어 프로토콜인 LMP(Link Management Protocol)를 IPsec(IP Security Protocol)을 사용하여 보안성을 제공하는 메커니즘의 문제점을 제시한다. 그리고 이에 대한 해결책으로, IPsec를 사용하지 않고 보안성을 제공하면서 빠른 속도로 처리되는 확장된 LMP 메커니즘을 제안한다.

1. 서 론

VPN(Virtual Private Network)이란 인터넷 또는 통신사업자의 공중통신망을 이용하여 보안성 있는 논리적인 망을 구성하여, 마치 가입자가 고유의 사설 통신망을 운용하고 있는 것과 같은 효과를 주는 네트워크 기술이다. 이러한 VPN은 ATM, F/R망 등의 다양한 망을 활용하여 개발될 수 있지만, 인터넷의 급속한 발달은 IP망을 활용한 VPN 기술의 개발을 활성화 시키게 되었다. 그러나 IP망을 활용한 VPN은 보안이 필요한 대용량의 서비스 요구에 따른 QoS 보장 문제와 현재의 IP망은 TDM(Time Division Multiplexing) 전송체계를 사용하기 때문에 전송용량이 부족한 문제점을 안고 있다. 이러한 IP 기반의 VPN에서 광대역폭 요구에 대한 해결책으로 차세대 광 인터넷을 통한 OVPN 기술이 제시되고 있다.

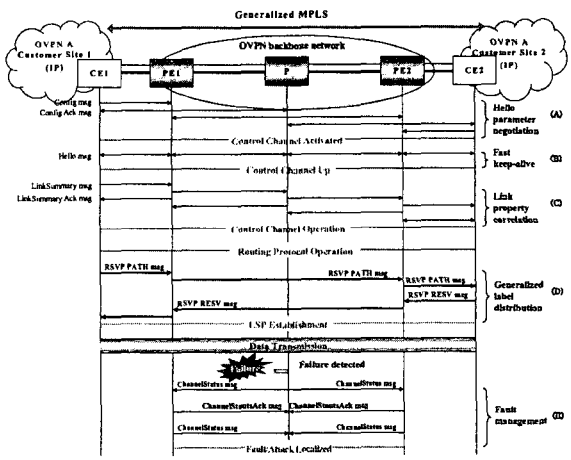
OVPN 구현에 있어 차세대 광 인터넷 백본망 기술은 DWDM(Dense Wavelength Division Multiplexing) 광 네트워크 기술을 활용한다. 그리고 IP 전달을 위한 제어 프로토콜은 GMPLS(Generalized Multi-Protocol Label Switching) 기술을 사용하는 IP/GMPLS over DWDM 프로토콜 프레임워크로 표준화되고 있는 현실에 비추어, IP/GMPLS over DWDM 백본망을 통한 OVPN(OVPN over IP/GPMLS over DWDM)은 차세대 VPN으로써 보안이 필요한 대용량의 서비스 제공을 위한 최적의 방안이 될 것이다.

그러나 높은 데이터 전송율을 가지는 OVPN에서 발생할 수 있는 광 소자의 fault/attack에 의한 서비스 파괴는 짧은 시간에 전송 용량에 비례한 막대한 데이터의 손실을 야기 시킨다. 그리고 서비스 파괴를 즉시 감지하고 복구해야 하는 제어 메시지가 변조되거나 복사되어 조작될 경우, 서비스 파괴는 지속되어 OVPN의 망 생존성(Network survivability)에 심각한 영향을 미치게 된다. 결과적으로 차세대 OVPN으로써 다양한 보안 서비스의 원활한 전개를 위해서는 망 생존성 보장을 위한 빠른 속도로 처리되는 보안성 있는 제어메시지가 필수적이다[2].

※ 본 연구는 한국과학재단 목적기초연구 (R01-2003-000-10526-0) 지원으로 수행되었음.

본 논문에서는 차세대 OVPN에서 제어 프로토콜인 LMP에 대한 확장된 보안 메커니즘을 제안한다. 이를 위해 2장에서는 OVPN의 제어 프로토콜의 전체 동작을 살펴본다. 3장에서는 LMP의 보안상의 문제점을 분석하고, 이에 대한 해결책으로 확장된 LMP의 보안 메커니즘을 제안한다. 끝으로 4장에서는 본 연구에 대한 결론과 향후 연구 추진 방향에 대해 서술한다.

2. OVPN 구조 및 동작



[그림 1] OVPN 구조 및 동작

[그림 1]은 OVPN의 구조 및 동작과정을 나타낸다. OVPN구조는 전기적 제어 도메인인 고객 사이트(customer site)와 제어 도메인인 DWDM 기반의 광 백본망으로 구성되고, 효율적인 제어를 위해 IP/GMPLS over DWDM 프로토콜을 사용한다. 외

부 고객 사이트는 IP, Sonet, Gigabit Ethernet등의 다양한 망으로 구성될 수 있다. 내부 OVPN 백본망은 GMPLS 기반의 DWDM 망으로, PE(Provider Edge)와 P(Provider) 노드로 구성된다. 최소한 각 노드는 망 제어를 위한 제어 채널과 데이터 전송을 위한 데이터 채널의 두개 이상의 링크로 구성된다.

OVPN의 동작은 Control flow와 Data flow로 나눌 수 있다. Control flow는 제어 채널에서 수행되며 가입자 사이트간의 광 경로를 수립하고 Data flow를 지속적으로 관리한다. Dataflow는 데이터 채널에서 수행되며 Control flow에서 수립된 광 경로를 통하여 광전 변화 없이 데이터 트래픽을 광으로 전송한다. Control flow 단계는 다시 네 가지 하위단계로 나눌 수 있다. 첫째, LMP에 의하여 각 노드간의 제어채널이 동작된다. 둘째, 제어채널을 통하여 경로설정을 위한 라우팅 정보가 분배된다. 셋째, RSVP-TE+시그널링 프로토콜에 의하여 종단간의 경로인 LSP(Label Switched Path)가 수립된다. 넷째, Dataflow단계에서 지속적으로 링크가 관리된다[1].

(그림 1)에서 (A),(B),(C),(E)는 LMP에 의하여 수행되며 (D)는 RSVP-TE+에 의하여 수행되는 Control flow과정이다.

(A)는 노드간에 제어 채널을 활성화 하기 위하여 Hello 메시지를 교환하는 시간 간격과 Hello 메시지의 최초의 Sequence number를 협상하는 정보가 있는 Config 메시지를 상호 교환하여 협상한다.

(B)는 노드간에 제어 채널을 활성화된 상태로 유지하도록 Config 메시지에서 협상된 시간 간격과 Sequence number를 준수하여 지속적으로 노드간의 Hello 메시지를 교환한다.

(C)는 노드간에 활성화된 제어 채널을 동작시키기 위하여 Link의 특성 및 정보가 있는 LinkSummary 메시지를 상호 교환한다. (A),(B),(C)의 절차가 수행되고 나면 각 노드간의 제어 채널이 동작하게 되고 라우팅 프로토콜에 의하여 각 노드에 라우팅 정보가 분배된다.

(D)는 OVPN의 LSP수립을 위한 GMPLS의 RSVP-TE+를 이용한 Generalized Label을 분배하는 과정이다.

(E)는 OVPN의 망 생존성을 위한 매우 중요한 동작으로써 빠른 처리가 요구되는 과정이며, Optical data를 전송하는 과정에서 모든 노드의 장애를 관리하는 LMP가 수행되는 Control flow 과정이다. 노드에 장애가 발생한다면 장애 위치를 통보하여 고장 난 요소를 기존의 트래픽과 분리시키는 지역화 과정으로, ChannelStatus 메시지를 사용하여 이웃 하는 업스트림(Upstream) 노드로 장애의 발생을 알린다. ChannelStatus 메시지는 장애가 발생한 데이터 링크의 식별자(Interface_Id), 데이터 링크의 상태(Signal Okay, Signal Degrade, Signal Fail) 및 데이터 채널의 방향을 나타낸다. ChannelStatus 메시지를 수신한 업스트림 노드는 먼저 ChannelStatusAck 메시지로 ChannelStatus 메시지의 수신에 대한 응답을 하고, 해당 LSP에 또 다른 장애 발생의 유무를 확인한다. 그 결과를 다시 ChannelStatus 메시지로 다운스트림(Downstream) 노드에게 알림으로써 두 노드사이의 장애를 지역화 한다. 장애를 인지한 후 이를 알리는 ChannelStatus 메시지가 수신되지 않으면 ChannelStatusRequest 메시지를 보내어 ChannelStatus 메시지를 요청하여 장애를 지역화 한다.

3. LMP 차등화 보안 메커니즘 제안

LMP는 자체적으로 어떠한 보안성도 제공하지 않는다. 이러한 이유로 LMP의 보안성 제공은 IPsec(IP Security Protocol) 프로토콜에 의존한다. 그러나 IPsec 프로토콜을 사용하기 위해서는 광 망의 수많은 모든 노드가 IPsec을 지원해야 하며, 망생존성을 위해 빠른 메시지의 처리가 요구되는 링크의 장애관리를 수행하는 과정에서 IPsec 프로세싱을 하는 시간이 상당히 오래 걸릴 수 있는 문제점이 있게 된다. 이는 속도를 중요시하는 광 인터넷을 기반으로 하는 OVPN에 IPsec를 적용하는 것이 아직은 시기상조라는 것을 의미한다[2]. 따라서 본 논문에서는 IPsec를 사용하지 않고 LMP 메시지에 대한 보안성을 제공하면서[1], 빠른 속도로 처리될수 있수 있도록 차등적으로 보안성을 제공하는 확장된 LMP를 제안한다.

LMP는 제어 정보를 전달하는 메시지로써 메시지의 무결성, replay attack 방지, 사용자의 인증의 보안이 요구되나, 기밀성은 요구되지 않는다[4]. [표 1]는 LMP 메시지를 구성하는 오브젝트에 대한 보안 요구사항을 나타낸다. 메시지의 무결성은 전체

Protocol	Object	Confidentiality	Authentication	Integrity	Replay attack
L M P	LOCAL_CCID		●	●	●
	MESSAGE_ID		●	●	●
	LOCAL_LINK_ID			●	
	LOCAL_NODE_ID			●	
	MESSAGE_ID_ACK			●	
	REMOTE_CCID			●	
	REMOTE LINK ID			●	
	LOCAL_INTERFACE_ID			●	
	REMOTE_INTERFACE_ID			●	
	TE LINK			●	
	DATA_LINK			●	
	HELLO			●	
	BEGIN_VERIFY			●	
	BEGIN_VERIFY_ACK			●	
	VERIFY ID			●	
	ERROR_CODE			●	
	CHANNEL_STATUS			●	
	CHANNEL_STATUS_REQUEST			●	

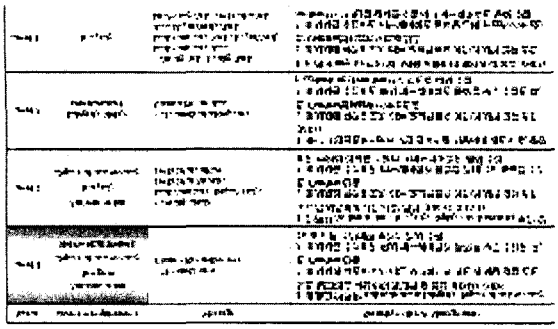
[표 1] LMP Object별 보안 요구사항

오브젝트에 대하여 보장해야 하나, replay attack 방지와 사용자의 인증은 LMP 메시지의 유일한 값을 가지는 LOCAL 또는 MESSAGE 오브젝트가 모든 메시지에 포함되어 있는 점을 이용하여, 이 오브젝트에만 개인키로 서명을 함으로써 전체 메시지에 대한 보안성을 제공할 수 있다. 또한 LMP 메시지 중 ACK, NACK, RESPONSE 메시지는 이전 메시지에 대한 개인키 인증을 한 후에 전송할 수 있기 때문에 개인키로 다시 서명을 할 필요가 없다. 따라서 LMP 메시지는 [표 2]와 같은 보안성이 요구되며, 추가적으로 망생존성을 위하여 장애 관리를 위한 LMP 메시지는 지연 없이 빠른 속도로 처리되어야 한다.

Protocol	Message	Confidentiality	Authentication	Integrity	Replay attack	Delay sensitiveness
L M P	Config		●	●	●	
	Config Ack			●		
	Config Nack			●		
	Hello		●	●	●	
	Link Summary		●	●	●	
	Link Summary Ack			●		
	Link Summary Nack			●		
	BeginVerify		●	●	●	
	BeginVerify Ack			●		
	BeginVerify Nack			●		
	EndVerify		●	●	●	
	EndVerify Ack			●		
	TestStatusSuccess		●	●	●	
	TestStatusFailure		●	●	●	
	TestStatusAck			●		
	ChannelStatus		●	●	●	●
	ChannelStatusRequest		●	●	●	●
	ChannelStatusResponse			●		●
	ChannelStatusAck			●		●

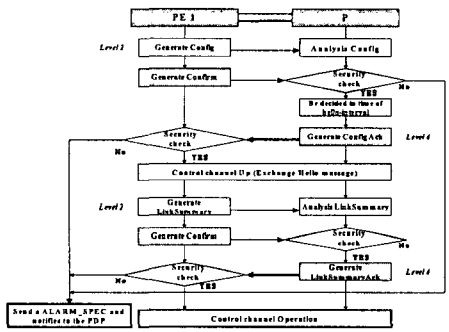
[표 2] LMP Message별 보안 요구사항

[표 3]에서는 LMP 메시지를 [표 2]의 보안 요구 사항에 따라 4 가지 등급으로 차등적으로 보안성을 제공하는 방법을 제안하였다. 기존의 IPsec를 이용한 LMP에서 대한 보안성 제공 메커니즘은 모든 메시지가 동일한 보안성이 제공되어 메시지를 처리하기 위한 불필요한 추가 시간이 많았지만 제안된 차등적인 보안성 제공 메커니즘은 메시지의 보안 요구사항에 따라서 알맞은 보안성을 제공하여 추가 시간을 감소시켜 LMP 메시지가 빠른 속도로 처리 될 수 있게 하였다. [표 3]의 보안 정책에



[표 3] LMP Message별 차등화된 보안정책

따른 확장된 LMP 메커니즘은 [그림 2, 3]과 같다. [그림 2]는 제어 채널을 관리하는 확장된 LMP 메커니즘을 순서도로 나타낸 그림이다. 다음과 같은 절차로 수행된다.



[그림 2] Extended LMP의 Control channel management

가. PE1 노드는 Hello 메시지의 시간 간격 협상을 위하여 level 2 의 보안성 제공으로 Config 메시지를 인접한 P 노드에게 전송한다.

나. P 노드는 Config 메시지를 수신하면 협상 가능 여부를 판단한 후, 이에 대한 응답으로 level 4 의 보안성 제공으로 ConfigAck 메시지를 PE1 노드에게 전송한다. 그리고 이전에 PE1 노드가 보냈던 Config 의 Confirm 메시지를 수신하게 되면 수신했던 Config 메시지와 일치하는지 확인함으로써 사용자 및 메시지 인증의 보안성 검사를 수행한다.

다. PE1 노드는 ConfigAck 메시지를 수신하는 즉시, piggybacking 된 ConfigAck 의 Confirm 메시지와 일치하는지 확인한다. 일치 한다면 PE1 노드와 P 노드는 링크의 관계유지를 위한 Hello 메시지를 일정한 시간 간격으로 상호 교환한다.

라. 링크의 속성을 협상하기 위한 LinkSummary 메시지는 level 2 의 보안성 제공을 하는 가.의 Config 메시지와 동일하게 처리된다. 이에 대한 응답인 LinkSummaryAck 메시지는 level 4 의 보안성을 제공하는 나. 의 ConfigAck 메시지와 동일하게 처리된다.

[그림 3]는 망 장애에 대한 지역화를 수행하는 확장된 LMP 의 보안 메커니즘을 순서도로 나타낸 그림이다. 메시지를 수신하면 즉시 처리한 후, Confirm 메시지로 보안성 검사를 수행하기 때문에 지연 없는 빠른 처리 속도의 보안 메커니즘을 제공하여 다음과 같은 절차로 수행된다.

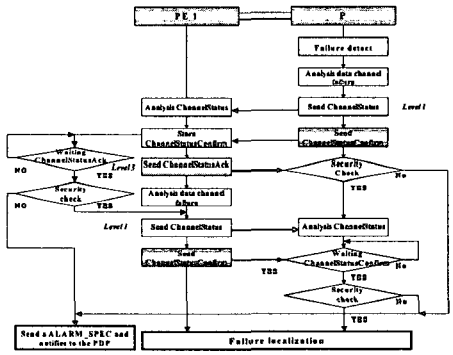
가. P 노드는 장애가 발생한 것을 인접 노드에게 알리기 위하여 level 1의 보안성 제공으로 ChannelStatus 메시지를 PE1 노드로 보낸다.

나. PE1 노드는 ChannelStatus 메시지를 수신하면 P 노드에서 장애가 발생한 것을 알게 되고 이에 대한 응답으로 level 3 의 보안성 제공으로 ChannelStatusAck 메시지를 보낸다. 그리고 이전에 P 노드가 보냈던 ChannelStatus 의 Confirm 메시지를 수신하게 되면 수신했던 ChannelStatus 메시지와 일치하는지 확인함으로써 사용자 및 메시지 인증의 보안성 검사를 수행한다.

다. P 노드는 ChannelStatusAck 메시지를 수신하는 즉시, piggybacking 된 ChannelStatusAck 의 Confirm 메시지와 일치하는지 확인한다.

라. PE1 노드는 해당 WDM 채널에 또 다른 장애의 발생의 유무를 확인한 후, 그 결과를 P 노드에게 level 1 의 보안성 제공으로 ChannelStatus 메시지로 보내고, 장애 노드 사이의 지역화할 준비를 한다.

마. 마지막으로 P 노드가 ChannelStatus 의 Confirm 메시지를 수신하면 ChannelStatus 메시지의 보안성을 검사하고 이상이 없다면 지역화 한다. 이상이 있다면 초기화 메시지인 LMP 알람 메시지를 사용하여 지역화 하기 위한 이전의 모든 메시지를 무효화 시킨다.



[그림 3] Extended LMP의 Fault management

4. 결론 및 향후 과제

본 논문에서는 LMP 의 보안상의 문제점을 분석하고 이에 대한 해결책으로 보안 요구사항에 따른 차등화된 LMP 보안 메커니즘을 제안하였다. 앞으로 확장된 LMP 메커니즘을 OVPN 에 적용하기 위하여 여러 프로토콜들(Routing Protocol, RSVP-TE+ / CR-LDP+)의 구체적인 기능 확장에 대한 연구가 필요하다.

참 고 문 헌

[1] Kwang-Hyun Cho et al., " Coordinated Network Survivability Mechanism in OVPN over IP/GMPLS over DWDM," The 5th International Workshop on Information Security Applications (WISA), August 2004.

[2] Hyun-dong Park et al., " Design of Security Framework for Optical Internet and Performance Test," The 15th Workshop on Information Security and Cryptography (WISC), September. 2003.

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

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