[4-39]

차세대 OVPN에서 보안이 보장되는 네트워크 서비스를 위한 제어 프로토콜 확장

조광현*, 정창현**, 윤미라+, 김성운++
부경대학교 정보통신공학과
{hyun*, jch123**, eggshape+}@mail1.pknu.ac.kr, kimsu@pknu.ac.kr++

Control Protocol Extension for Secured Network Service In Next Generation Optical VPN

Kwang-Hyun Cho*, Chang-Hyun Jeong**, Mi-Ra Yoon+, Sung-Un Kim++
Dept. of Telematics Engineering, Pukyong National University

요 약

IP 망을 활용한 VPN(Virtual Private Network)에서 QoS 보장과 광대역폭 제공에 대한 해결책으로 차세대 광 인터넷을 통한 OVPN(Optical VPN) 기술이 제시되고 있다. 차세대 광 인터넷의 구현이 IP/GMPLS(Generalized Multi-Protocol Label Switching) over DWDM(Dense Wavelength Division Multiplexing) 프로토콜 프레임워크로 표준화되고 있는 현실에 비추어, IP/GMPLS over DWDM 백본망을 통한 OVPN 은 차세대 가상 사설망으로써 보안을 요구하는 대용량의 서비스 제공을 위한 최적의 방안이다. 본 논문에서는 OVPN 에서 전송경로를 설정하고 각 노드의 자원을 데이터 전송에 이용할 수 있도록 예약하는 제어 프로토콜인 RSVP-TE+(ReSerVation Protocol Traffic Engineering)와 LMP(Link Management Protocol)의 보안상의 문제점을 분석하고 그에 따른 해결책으로 확장된 RSVP-TE+와 LMP 를 제시하고 보안 메커니즘을 제안한다.

I. 서론

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/R, IP망 등의 다양한 망을 이용하여 구축할 수 있지만, IP망을 이용한 인터넷의 급속한 발달로 IP망을 활용한 VPN 기술들의 개발이 활성화되고 있다. 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 DWDM광 네트워크 기술을 활용한다. 그리고 IP 전달을 위한 제어 프로토콜은 GMPLS 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.

OVPN은 데이터의 원활한 소통을 위해 데이터가 전송될 경로를 먼저 설정하고 데이터를 전송하는 방식을 취한다. 즉, 데이터 전송 이전에 제어 메시지가 노드를 순회하여 경로를 먼저 형성하는 것이다. 그리고 데이터 전송 중에 여러 가지 에러들에 대해 대비하기 위하여 제어 메시지에 의하여 지속적으로 관리된다. 데이터가 전송도중에 장애가 발생 한다면 이러한 사실을 즉시 감지하고 복구되어야 하기 때문이다. 만약, 경로를 형성하기 위한 제어 메시지가 변조되거나 복사된다면 필요하지 않은 경로가 설정되어 자원을 낭비할 수 있고, 필요한 양보다 적은 자원이 할당되어 데이터 전송을 방해할 수도 있다. 또한, 제어 메시지의 처리가 완료될 때까지 데이터 전송은 시작될 수 없으므로 제어 메시지를 재전송함으로써 일종의 서비스 거부 공격을 시도할 수도 있다. 그리고 데이터 전송을 관리하는 제어 메시지가 변조되거나 복사된다면 데이터가 전송도중 실패하더라도 복구가 되지 않아 네트워크 생존성에 대한 공격이 될 수도 있다. 이러한 이유로 인해 제어 메시지의 송신자 인증, 무결성 검증 등의 보안이 필요하다. 즉, 차세대 광인터넷을 기반으로 하는 OVPN에서 가장 중요한 정보 보안 기능은 OVPN의 제어메시지에 대해 정보의 송신자를 인증하는 것과 메시지의 무결성을 검증하는 보안성을 절실히 요구한다.

따라서 본 논문에서는 차세대 OVPN에서 제어 프로토콜인 GMPLS의 종단간의 경로수립을 위한 RSVP-TE+와 링크관리를 위한 LMP에 대한 보안성 메커니즘을 제시한다. 이를 위해 2장에서는 OVPN의 전체 동작을 살펴보고, 제어 메시지의 보안상의 문제점을 분석한다. 그리고 이에 대한 해결책으로 확장된 RSVP-TE+와 LMP를 제안한다. 3장에서는 본 연구에 대한 결론과 향후 연구 추진 방향에 대해 서술한다.

II. OVPN 구조 및 동작

(그림 1)은 OVPN 의 구조 및 동작과정을 나타낸다. OVPN 구조는 전기적 제어 도메인인 고객 사이트 (customer site)와 제어 도메인인 DWDM 기반의 백본망으로 구성되고, 이들 사이의 효율적인 제어를 위해 IP/GMPLS over DWDM

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