2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

가상 사설망의 현황과 보완책

권윤주*, 정태명*
*성균관대학교 전기전자 및 컴퓨터공학부

e-mail:yjkwon@rtlab.skku.ac.kr, tmchung@ece.skku.ac.kr

The Current Status of VPN and the complement method

Yoon J. Kwon, Tai M. Chung
*Real-Time Systems and Network Laboratory
School of Electrical and Computer Engineering, Sungkyunkwan University

요약

기존의 사설망에서 쉽게 제공될 수 있었던 QoS가 가상 사설망에서는 새로운 패러다임을 요구하게 되었다. 가상 사설망이 고려되고 구현되는 형태가 다양한 만큼 보안이 아닌 QoS도 여러 가지 형태의 VPN에서 고려되고 있다. 본 논문에서는 보안성과 QoS보장 모두를 제공할 수 있는 방법들에 대해서 살펴보고 요즘에 크게 대두되고 있는 MPLS VPN 기법에 대해서 기술하고 개선되어야 할 점들에 대해서 논의한다.

1. 서론

근래 들어 컴퓨터, 네트워크가 각 사회제반 조직의 업무수행 및 개인의 주요한 통신수단으로 자리잡으면서, 컴퓨터 네트워크를 이용하는 모든 이들이 안전한 데이터 통신 수단을 필요로 하게 되었다. 일반적으로 사용되고 있는 공중망을 통해서 왕래되는 정보는 충분한 안전을 보장할 수 없기 때문에, 이를 해결하기 위한 수단으로 전용선을 이용한 사설망이 사용되었다. 그러나 이와 같이 전용선을 이용한 사설망은 조직이나 개인에게 비용적인 면에서 매우 큰 부담으로 작용하게 하였다.

공중망을 사용하여 사설망과 같은 기능과 환경을 제공하는 방식인 가상 사설망(Virtual Private Network, 이하 VPN)은 사설망에서의 비용적인 부담을 없애고자하는 노력에서 제안되었다. 이러한 VPN을 구현하는 방식은 2계층에서는 가상 회선 기술을 기반으로 하여 연구되어왔고, 3계층에서는 터널링과 암호화 기법이라는 방식으로 발전되어왔다.

2계층 방식은 가입자에 한해서 가상 연결(Virtual Connections) 서비스를 제공하는 프레임 릴레이나 ATM 같은 WAN(Wide Area Network)기술을 하나의 VPN으로서 도입하였다. 이를 통해 조직의 입장에서는 비용 절감과 더불어 QoS를 보장받을 수 있으나 가상 연결 관리와 라우팅의 설정 관리에 있어서 확장성의 결여를 가져온다는 문제점이 제기되었다[1].

IP를 기반으로 하는 VPN은 IP의 비연결성을 통한 융통성과 더불어 암호화를 이용한 종단간의 통신 보안을 가능하게 한다. 그러나 이 방식의 경우, IP의 구현 철학인 best-effort 정책으로 인해 사용자들에게 QoS를 보장해야 하는 응용에는 적합하지 않다는 문제점이 있다.

조직을 구성하는 부 영역들의 수가 증가하고 지역적으로 산개될수록, 전용선을 이용하여 이들간의 안

전한 통신을 보장하기란 더욱 어려운 일이므로 VPN은 최선의 선택이 된다. 그러나, 공중망을 통해 사설망과 같은 안전함(safety)과 QoS, 그리고 확장성을 동시에 만족시키기는 기술적으로 힘든 상황이었다. 이러한 상황에서 그간의 VPN에 대한 연구는 보안성에 치우치는 경향을 갖고 있었다. 또한, 근래들어 응용 서비스 기술의 다양화로 인해 VPN이 다양한 형태의 데이터를 수용할 수 있는 능력이 요구된다. 이러한 현실에서, 현대의 VPN에서의 QoS 보장이 새로이 관심을 갖는 영역이 되고 있다.

따라서, 본 논문은 QoS를 보장하기 위해 IP 기반 VPN에서 연구된 RSVP의 적용방식에 대해서 살펴보고, 이의 문제점들을 알아본다. 그리고 또 다른 방식으로 QoS와 보안성을 보장하고 있는 MPLS VPN 기법을 소개한다. MPLS VPN의 경우 현재 새로운 VPN 솔루션으로서 많은 연구가 활발히 이루어지고 있다. 따라서 이 기법에 대해서 중점적으로 알아보고, 이 기법에서 보완되어야 할 점에 대해서 논의한다.

본 논문의 구성은 2장에서는 RSVP를 이용한 VPN 기법에 대해서 기술하고 3장에서는 MPLS VPN에 대해서 중점적으로 서술할 것이다. 그리고 4장에서는 앞서 설명한 방식들의 장단점에 대해 논의하며 결론을 짓고, 향후 전망에 대해서 기술한다.

2. RSVP를 이용한 VPN

앞서 언급한 바와 같이 IP를 기반으로 VPN(IP VPN)을 제공하게 될 경우, 인터넷을 경유하여 자원을 공유하기 때문에 QoS의 보장이 상당한 난점으로 지적된다[3].

IETF에서는 IP 네트워크을 경유하여 네트워크 자원을 예약하기 위한 방법으로서 RSVP를 채택하였다. IP VPN의 경우 RSVP를 통한 대역폭 보장에 관한 연구가 진행되어 왔다. RSVP를 IPSec에 적용시킬 때의 고려할 점은 네트워크 자원 예약을 위해 각 패킷의 TCP 또는 UDP의 포트 번호를 필요로 한다는 점이다[2]. 그런데 IPSec의 경우 패킷 형태가 일반적인 패킷 형태와 다르기 때문에 각 패킷마다 TCP 또는 UDP 포트의 값을 얻어내기가 용이하지 않다. 또한 IPSec 패킷이라고 하여도 모드에 따라, 그리고 IPSec 헤더에 따라 일정위치에 트랜스포트 계층의 헤더가 있다고 단정할 수 없기 때문에 RSVP의 적용이 더욱 어렵게 된다.

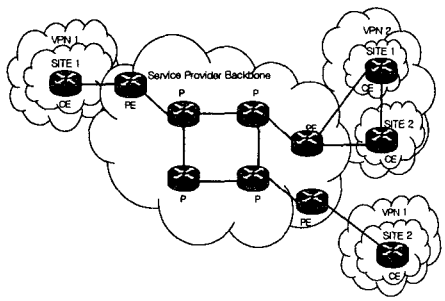
RSVP를 이용한 IP VPN의 경우 두 가지 방식으로 제안되었다. 하나는 RSVP를 확장시켜서 TCP/UDP의 포트 대신 IPSec의 SPI(Security Parameter Index)를 사용하는 방식[2]이고 나머지 하나는 각 패킷마다 UDP로 다시 캡슐화 하는 방식이다[3].

전자는 사용하는 값을 SPI로 대치시킴으로써, IPSec 패킷에 어떠한 수정도 요구되지 않으나, IPSec 패킷을 처리하기 위해 RSVP의 변용을 요구한다. 후자의 경우, 중간의 라우터를 통해 IPSec 패킷을 UDP로 캡슐화하여 전달하므로 전송되는 패킷 단위로 처리를 해야한다는 오버헤드는 발생하나 RSVP와 IPSec 모두 어떠한 수정도 요구되지 않는다.

3. MPLS에서의 VPN

현재 데이터 링크 계층의 레이블 스위칭 전송 기술을 네트워크 계층의 라우팅과 통합하는 기반 기술인 MPLS(Multi-Protocol Label Switching)를 이용하여 일정수준의 대역폭과 보안성을 보장하면서 융통성을 지닌 MPLS VPN에 대한 연구가 진행중이다.

MPLS의 경우 하부에 프레임 릴레이 또는 ATM이 사용되기 때문에 앞서 언급한 바와 같이 가상회선과 유사한 형태의 기술인 LSP(Label Switched Path) 또는 가상 경로(Virtual Path)[4]를 통하여 통신 연결 정보를 관리할 수 있어 QoS의 보장을 가능하게 한다. 또한, 이것은 IP VPN에서의 터널링과 같은 기능을 제공함으로써 보안성도 만족시킨다.



[그림 1] 서비스 제공자 백본에서의 VPN

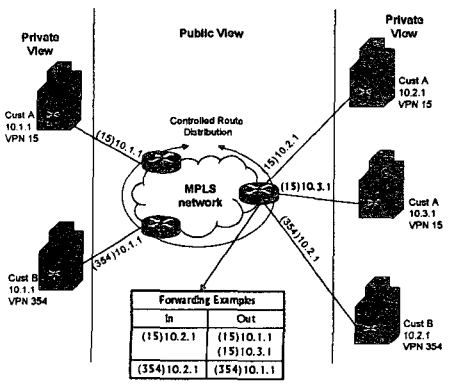
[그림 1]에서와 같이 MPLS VPN은 서비스 제공자(SP : Service Provider)의 백본(backbone)을 기반으로 제공된다. 여기서 CE(Customer Edge)는 사용자와 연결되어 있는 장치를 의미하고 PE(Provider Edge)는 백본망을 구성하고 있는 노드들 중에서 CE와 연결되어 있는 종단의 백본 노드를 의미한다.

이 예에서는 안전한 정보 교환을 필요로 하는 VPN 1그룹, VPN 2그룹이 있다. SITE 1과 SITE 2로 분산되어 있는 각각의 VPN 그룹은 각각 독립적인 가상 경로가 설정되어야 한다. MPLS에서의 VPN은 백본에 구성된 가상 경로를 통하여 일정한 단위의 VPN 그룹간 정보 보안 서비스를 제공한다.

(1) 가상 경로(Virtual Path)

일반적으로 백본은 CE가 연결되어 있는 PE 라우터와 라우터들간의 패킷 전송을 위한 P(Provider) 라우터로 구성되어 있다. 백본을 구성하는 모든 라우터들이 VPN을 위한 라우팅 정보를 유지한다는 것은 여러 가지 확장성에 대한 문제를 발생시킨다. 따라서 특정 VPN 그룹에 대한 라우팅 정보는 해당 VPN 그룹에 연결되어 있는 PE 라우터에만 존재한다. 결과적으로 P 라우터들은 각 VPN에 대한 라우팅 정보를 유지할 필요가 없다.

각각의 PE들은 그러한 VPN 정보인 VPN 경로를 전송 테이블에 저장하게 되는 데, 이 때 PE들은 CE의 정보를 VPN-IP 주소 형태로 전환하여 저장하여야 한다. 이는 두 개의 VPN 그룹이 같은 IPv4 주소 prefix를 사용할 때, PE가 이것을 유일하게 식별할 수 있게 하기 위해서이다.



[그림 2] MPLS를 이용한 VPN 형성

[그림 2]와 같이, VPN-IP 주소는 8바이트의 RD(Route Distinguisher)와 4 바이트의 IP 주소로 구성되어 있다[5]. 이러한 방식은 같은 주소를 가진 시스템에서 다수의 VPN 형성을 보장하고, 그 주소에 있는 각각의 VPN이 완전히 다른 경로를 설정할 수 있도록 지원한다.

(2) VPN-IP 경로 분산

하나의 AS(Autonomous System)에 존재하는 PE들이 연결되어 있는 VPN 사이트들은 IBGP 연결을 통해 VPN-IPv4 경로를 분산할 수 있다. 만약 두 VPN 사이트가 다른 AS에 존재한다면, PE 라우터는 ASBR(Autonomous System Border Router)에 VPN-IPv4 경로를 재분산하기 위해서 IBGP를 사용할 필요가 있다. ASBR은 또 다른 AS에 존재하는 ASBR로의 경로를 재분산하기 위해서 EBGP를 사용할 필요가 있다. 이것은 다른 서비스 제공자들에 속한 다른 VPN 사이트들과의 연결성을 제공한다. 이 때 EBGP를 이용한 VPN-IPv4의 경로는 신뢰할 수 있는 두 SP(Service Provider)의 백본 사이에서만 분산되어야 한다[6].

이러한 방식으로 분산되는 MPLS 레이블은 어떤 한 경로를 설정한 라우터와 그 경로의 BGP next hop간의 레이블 스위치 경로(label switched route)가 존재하는 경우에서만 사용 가능하다는 것을 인지하여야 한다. 따라서 VPN의 아키텍쳐도 라우터와 그것의 BGP next hop이 존재하는 레이블 스위치 경로 하에서 구성될 수 있으며, P 라우터와 같이 어떤 VPN과도 연결되지 않은 라우터는 결코 어떤 VPN-IPv4도 설정될 수 없다.

(3) 패킷 전달 방식

백본에서의 패킷 전송은 두 단계의 레이블 스택을 가진 MPLS 방식을 사용하여 구현된다. PE가 CE로부터 패킷을 받으면 그것은 패킷의 목적지 주소를 참조하여 특정 전송 테이블의 한 엔트리를 선택한다. 그 패킷의 목적지가 같은 PE에 연결되어 있으면, 그 패킷은 직접적으로 해당 CE에 보내진다. 만약 그 패킷의 목적지가 같은 PE 내에 있는 것이 아니라면, 백본을 경유하게 되는 데 그 동안에는 패킷의 IP 헤더는 사용되지 않고 레이블을 이용하여 MPLS 방식으로 패킷을 해당 CE까지 운반한다. 그

패킷은 최하단 스택에 "BGP next hop"이라는 해당 VPN에 관련된 레이블을 넣고, 그 상위에는 그 백본에서의 라우팅 레이블을 담아서 그 패킷의 목적지를 관리하는 PE에 도착할 때까지 상위 스택에 있는 라우팅 레이블을 교환하면서 전송된다. 최종 PE라우터는 CE로 패킷을 보내기 전에 최하단의 레이블을 제거하는 작업을 한다. 따라서 CE는 일반적인 IP 패킷을 전달받는다.

두 단계의 레이블링은 P(Provider) 라우터들에서 모든 VPN 경로를 유지하게 하며, 백본에서는 PE에 대한 경로만 알뿐, CE에 대한 경로는 알 수 없도록 한다.

4. 결론 및 향후 전망

IP를 기반으로 발전되어 온 VPN의 경우, 기존에 IP 네트워크의 QoS보장을 위해 제시되어 온 RSVP를 기반으로 하는 기술의 적용을 고려해왔다. 그리고 프레임 릴레이 또는 ATM의 기술을 이용하여 VPN을 제공하고자 하는 측에서는 MPLS라는 네트워크 계층을 이용한 스위칭 방식의 도입으로 QoS의 보장 및 보안성을 제공할 수 있는 VPN에 대한 연구가 각 네트워크 장치 벤더들과 IETF에 의해서 진행중이다.

RSVP를 이용한 VPN의 경우 기존의 프로토콜에 많은 변화를 가져와야 한다는 점에서 그 기술을 적용하기 어려운 반면, MPLS VPN 방식의 경우에는 광대역 통신망에서의 스위칭 기술을 기반으로 하여 초고속 전송을 가능하게 한다는 점에서 이점을 가지고 있다.

그러나 아직 MPLS VPN 구조의 보안은 프레임 릴레이나 ATM 백본에서 제공되는 VPN과 동일한 수준에 머물러 있다는 점이 보완되어야 할 사항으로 논의되고 있다. MPLS VPN은 보안 서비스를 받고자 하는 사람의 요구 혹은, 보호될 데이터의 중요성에 따른 다양한 보안 인자들을 수용할 수 없다는 한계가 존재한다. 그리고, 통신을 수행하는 두 개체 사이에 보안 경로가 백본 내에서만 형성되고 백본 외의 경로에서는 보안이 보장되지 않는다. 또한, 백본 내의 보안 경로 상에서 실제로는 아무런 처리가 되지 않은 패킷이 전송되므로 그 경로 영역도 완전히 신뢰할 수 없는 영역일 수 있다. 따라서, 앞으로도 MPLS에서의 VPN은 좀 더 강도 있는 보안 기술이 필요하다고 말할 수 있다.

MPLS VPN상에서의 보안을 위해서는 패킷 보안과 MPLS의 에지 라우터인 LER에서의 인증 메카니즘을 고려할 수 있다. 현재 백본에서 패킷보안을 위해 IPSec을 사용하는 방법[7]과 LER에서의 인증을 위해 LDP(Label Distribute Protocol)을 통한 인증 메카니즘[8]이 제시되고 있다. 한편으로, MPLS는 각 네트워크 장비 벤더들과 IETF에 의해 세부 기술이 활발히 연구 및 구현되고 있고, 빠른 속도로 각 요소 기술들이 표준화되고 있는 추세이며, MPLS VPN에서는 앞으로 앞서 언급한 문제점들을 해결하기 위한 연구가 필요할 것으로 보인다.

5. 참고 문헌

[1] 1999 Frame Relay Forum, http://www.frforum.com/4000/vpn.html

[2] L.Berger and T.O'Malley, "RSVP Extensions for IPSEC Data Flows", RFC2207, 1997

[3] Ito, Y., Maeshima, O., Ishikura and M., Asami, T., "Bandwidth-guaranteed IP Tunneling Router with RSVP", Performance, Computing and Communications, 1998. IPCCC '98., IEEE International , 1998

[4] Grenville Armitage, "MPLS : The Magic Behind the Myths", IEEE Communication Magazine, pp.124-pp.131, January 2000

[5] Cisco, "Delivering New World Virtual Private Networks with MPLS", white paper, Cisco Systems, 1999

[6] E.Rosen and Y.Rekhter, "BGP/MPLS VPN", RFC2547, March 1999

[7] Jeremy De Clercq, Yves T'Joens, et al., "BGP/IPsec VPN", Internet draft-declercq-bgp-ipsec-vpn-00.txt, July 2000

[8] Peter De Schrijver and Yves T'Joens, "End to end authentication for LDP", Internet draft-schrijvp-mpls-ldp-end-to-end-auth-01.txt, July 2000