VPN 환경에서 MIPv6를 지원하기 위한 효율적인 방안

서유화*, 성수련*, 추순호*, 신용태*
*숭실대학교 컴퓨터학과
e-mail:{zzarara, ssl, chu78, shin}@cherry.ssu.ac.kr

Efficiently Supporting Scheme of MIPv6 in VPN environment

Yuhaw Seo*, Sulyun Sung*, SoonHo Chu* Yongtae Shin*
*Dept. of Computing, Soongsil University

요 약

본 논문은 VPN 환경에서 MIPv6를 지원하기 위한 방안을 제안한다. 이동 노드가 이동한 외부 네트워크는 계층적인 MIPv6 구조를 가지며 이동노드가 외부 네트워크로 이동했을 경우 외부 네트워크의 엑세스 라우터(access router)를 관리하는 GMAP(gateway management anchor point)는 이동노드를 대신하여 VPN 게이트웨이와 IPsec 보안 협정을 맺는다. 이동 노드가 같은 GMAP 영역 안에서 이동할 경우 이미 맺어 놓은 GMAP와의 IPsec 보안 협정을 사용하기 때문에 이동 노드는 이동시마다 VPN 게이트웨이와 재 보안 협정을 맺을 필요가 없다. 이는 IPsec 재 보안 협정으로 인한 메시지 오버헤드와 지연을 감소시키며 이동노드가 외부 네트워크에 있을 경우 패킷 누출 없이 안전하게 데이터를 전송할 수 있게 한다.

1. 서 론

기업과 같이 사설망을 사용하는 기관에서는 외부 네트워크와의 정보 교환의 필요성과 재택 근무자의 수가 점차 증가하였고 네트워크의 범위가 점차 확대되어감에 따라 사설망의 규모도 함께 증가하였다. 이에 따라 발생되는 내부망의 보안성 문제와 사설망의 효율적 운영은 중요한 이슈가 되었다.

VPN(virtual private network)은 IPsec 등의 보안 기술을 이용하여 공중망을 사설망처럼 운영함으로써 적은 운영비용을 통해 넓은 범위의 네트워크를 구성할 수 있으며 기업 간의 협력이나 내부망의 보안성을 높이기 위해 사용되는 기술이다. 이러한 VPN 환경에서 MIPv6의 지원은 사설망의 규모를 확대시키고 이동성을 높임으로써 유·무선 환경의 외부 네트워크에 존재하는 사용자가 안전하게 내부 VPN 네트워크로 접근을 가능하게 한다.

그러나 기존의 VPN 환경에서 MIPv6를 지원할 경우 IPsec 보안 협정은 일반적으로 종단 대 종단의 IP주소에 의해 설정되기 때문에 이동 노드가 새로운 CoA(care of address)를 부여 받을 때마다 새로운 보안 협정을 맺어야 한다. 이동 노드의 빈번한 이동시 이는 재 보안 협정에 따른 오버헤드와 패킷 전달의 지연을 초래하게 된다.

본 논문은 이러한 문제를 해결하기 위해 기존의 계층적인 MIPv6 구조를 이용하여 VPN 환경에서 MIPv6를 효율적으로 지원하기 위한 방안을 제안한다. 계층적인 MIPv6 구조란 MIP6에 지역성(Locality) 개념을 추가한 것으로서 지역 내 이동 발생 시 지역 이동성을 총괄하는 MAP(Mobility Anchor Point)을 지역 내부와 외부의 경계에 둠으로써 경계지점에서 주소 매핑을 처리하고 이동

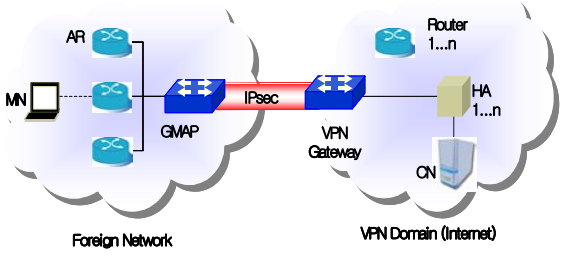
노드에 대해서는 임시 홈 에이전트 역할을, 홈 에이전트에 대해서는 이동 노드 역할을 처리하도록 한 기술이다. 이렇게 함으로써 지역 이동 발생 시 홈 등록을 위한 제어 메시지 수를 크게 줄일 수 있다. 본 논문에서 제안한 방식은 이러한 계층적 MIPv6 구조를 이용하며 GMAP(gateway mobility anchor point)이 이동노드를 대신하여 VPN 게이트웨이와 IPsec 보안 협정을 맺는다.

이동 노드가 같은 GMAP 영역 안에서 이동할 경우 이미 맺어 놓은 GMAP와의 IPsec 보안 협정을 사용하기 때문에 이동 노드는 이동 시 마다 VPN 게이트웨이와 재 보안 협정을 맺을 필요가 없다. 이는 IPsec 재 보안 협정으로 인한 메시지 오버헤드와 지연을 감소시키며 이동노드가 외부 네트워크에 있을 경우 패킷 누출 없이 안전하게 데이터를 전송할 수 있다.

본 논문의 2장에서는 MIPv6를 효율적으로 지원하기 위해 제안한 VPN의 전체 토폴로지를 제안하며 3장에서는 2장에서 제안된 토폴로지를 기반으로 동작하는 계층적인 MIPv6 구조를 소개한다. 4장에서는 제안된 프로토콜 세부적인 동작 과정을 제시한다. 마지막으로 5장에서는 결론 및 향후 연구방향을 제시한다.

2. 토폴로지

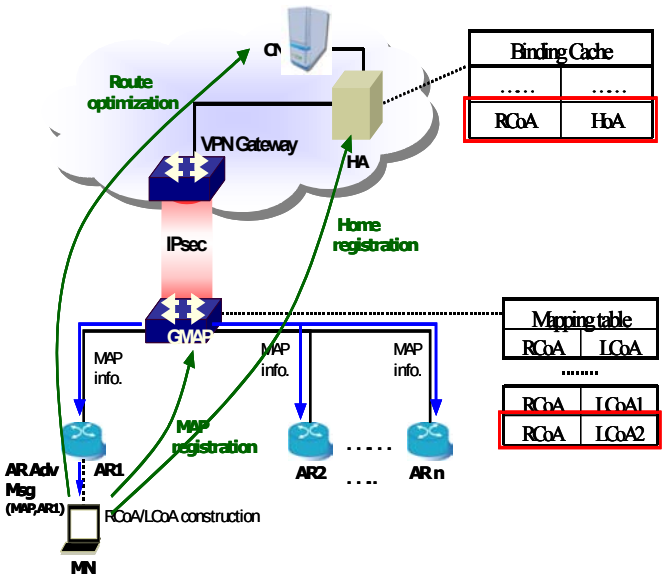
제안한 네트워크의 토폴로지는 [그림 1]과 같다. 홈 네트워크는 일반적으로 사설 주소를 사용하는 서브 네트워크이며 서브 네트워크는 HA(home agent)들과 VPN 게이트웨이 등을 포함한다. 외부 네트워크는 계층적인 MIPv6 구조를 가지며 이동 노드의 지역 내 이동 발생 시 지역 이동성을 총괄하고 이동 노드를 대신하여 VPN 게이트웨이와 IPsec 보안 협정을 맺는 GMAP(gateway mobility anchor point)를 가진다.



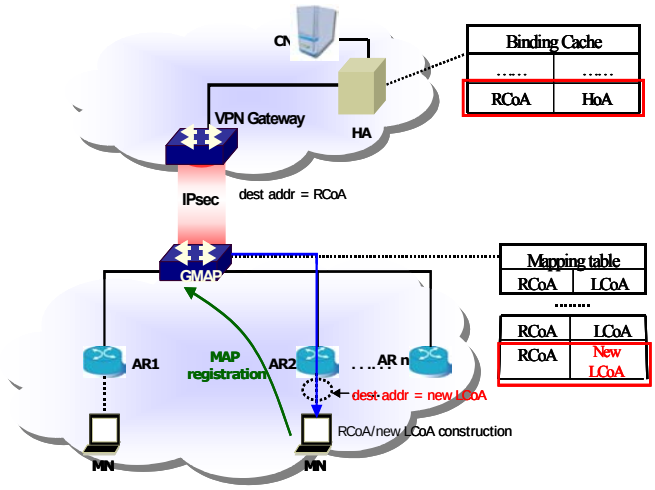
[그림 1] 네트워크 토폴로지

3. 계층적인 MIPv6 구조

계층적인 MIPv6 구조에서 이동 노드는 RCoA (Regional CoA)와 LCoA(On-link CoA) 두 개의 주소를 사용한다. RCoA는 GMAP이 관리하는 영역의 대표 주소이며 LCoA는 GMAP이 관리하는 도메인 내에서 MN이 이동 시마다 AR의 라우터 광고 메시지를 통해 부여받는 주소이다. GMAP은 RCoA와 LCoA의 매핑 테이블을 유지한다. 이동 노드는 GMAP 도메인 내에서 이동 할 경우 새로운 LCoA를 부여받고 지역적인 바인딩 업데이트만을 수행하며 홈 에이전트와 대응 노드로의 바인딩 업데이트를 수행하지 않는다. 이동 노드가 새로운 외부 네트워크 또는 다른 GMAP 도메인으로 이동 시에는 지역적인 바인딩 업데이트와 함께 홈 에이전트와 대응 노드로의 바인딩 업데이트 과정이 수행 된다. 이는 기존의 MIPv6 동작에서와 같이 이동노드가 외부 네트워크에서 지역적인 이동 시마다 바인딩 업데이트를 수행하는데 있어 드는 비용과 오버헤드 및 지연을 줄이고자 제안된 방식이다. 이 계층적인 MIPv6 구조를 이용하여 VPN은 효율적으로 운용 될 수 있다. [그림 2]는 이동노드가 외부네트워크에 처음 이동했을 경우 계층적인 MIPv6의 동작과정을 나타내며 [그림 3]은 이동노드가 외부 네트워크 내에서 지역적인 이동을 한 경우의 동작과정을 나타낸다.



[그림 2] 이동노드의 새로운 GMAP 영역으로의 이동

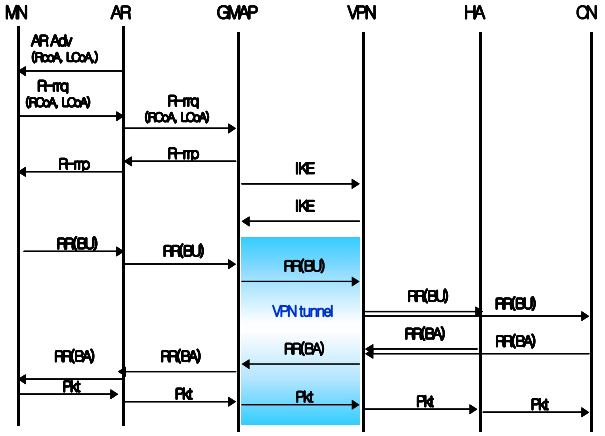


[그림 3] 이동노드의 GMAP 영역 내에서의 이동

4. 프로토콜 동작과정

4.1 GMAP으로의 등록

[그림 4]는 이동노드가 처음 새로운 GMAP 영역으로 이동했을 경우 GMAP에 등록하는 과정을 보여준다.



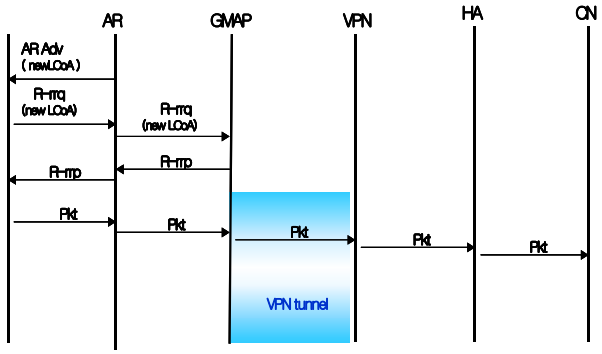
[그림 4] GMAP으로의 등록

이동노드가 새로운 GMAP 영역으로 이동시 GMAP에 이동 노드를 등록하기 위해 새로운 R-rrq(regional register request)와 R-rrp(regional register response) 메시지를 정의한다. 이동 노드가 새로운 GMAP 영역으로 이동했을 경우 이동노드는 라우터 광고 메시지를 통해 LCoA와 RCoA를 부여 받는다. 이동노드는 부여 받은 RCoA와 LCoA를 R-rrq 메시지를 통해 GMAP으로 보내고 GMAP은 자신의 영역 내로 이동한 이동노드를 자신의 매핑 테이블에 등록 후 이동노드로 R-rrq에 대한 응답 메시지 R-rrp를 보낸다. 그 후 GMAP은 VPN 게이트 웨이와 IPsec 터널을 만들기 위해 IKE 협정을 수행하고 홈 에이전트와 대응 노드로 RR과정을 수행 후 데이터 패킷을 송수신한다.

4.2 GMAP으로의 지역적 등록

이동 노드가 같은 GMAP 영역으로 이동했을 경우 이동노드는 이미 GMAP에 등록이 되어있다. 따라서 이미 GMAP은 VPN 게이트웨이와 IPsec 터널이 형성되어 있는 상태이기 때문에 IPsec 보안 재협정을 수행 할 필요가 없다. 이동노드는 라우터 광고 메시지를 통해 부여받은 새로운 LCoA를 GMAP에 등록하는 R-rrp 메시지와 그에 대한 응답 R-rrp메시지만을 송수신한 후 데이터 패킷을 보낼 수 있다.

[그림 5]은 이동노드가 같은 GMAP 영역 내에서 이동했을 경우 동작과정을 나타낸다.

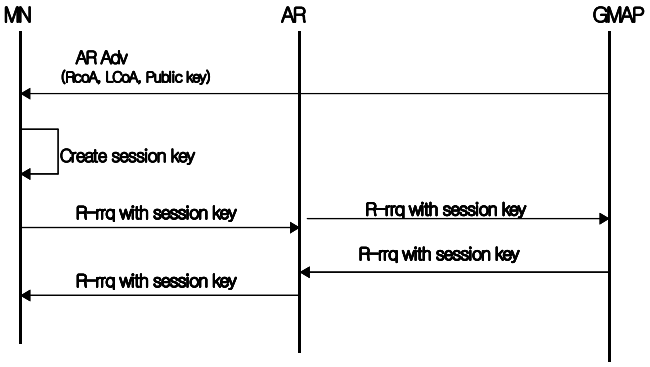


[그림 5] GMAP으로의 지역적 등록

4.3 보안적 고려사항

이동노드와 GMAP과 송수신되는 메시지의 보안을 위해 이동노드는 라우터 광고 메시지를 받을 때 GMAP과 AR이 가지고 있는 공유키를 받는다. 이동노드는 자신이 세션 키를 생성한 후 세션 키를 R-rrp 메시지에 넣어 공유키로 암호화 한 후 AR과 GMAP에게 전송한다. 그 후 이동노드와 GMAP간에 전송되는 메시지는 세션키로 암호화 되어 전송된다. 따라서 이동노드와 GMAP구간은 세션키를 통해 보안을 유지하고 GMAP과 VPN 게이트 웨이 구간은 IPsec 터널을 통해 보안을 유지한다.

[그림 6]은 이동노드와 GMAP 간의 보안 세션을 확립하는 과정을 보여준다.



[그림 6] 이동노드와 GMAP간의 보안 세션 확립

4. 결론 및 향후 연구방향

본 논문에서는 VPN 환경에서 MIPv6를 효율적으로 지원하기 위한 방안을 제안하였다. 제안한 방안은 계층적인 MIPv6 구조를 이용하여 지역적 이동성을 관할하는 GMAP이 VPN 게이트웨이와 보안 협정을 맺기 때문에 이동노드가 GMAP의 관리 영역 내에서 이동할 경우 재보안 협정을 요구하지 않는다. 따라서 이동 노드가 외부 네크워크에서 지역적 이동시 재보안 협정의 오버헤드와 지연을 감소시킬 수 있다. 그러나 계층적인 MIPv6 구조를 이용하기 때문에 계층적인 MIPv6가 가지고 있는 문제점으로 인한 보안적 위협이나 GMAP으로 인한 성능 저하 문제에 대해서 더 많은 연구가 필요하다.

참고 문헌

[1] D. Johnson, C. Perkins, J. Arkko, " Mobility Support in IPv6", RFC 3775, June 2004

[2] Perkins, c., "IP Mobility Support for IPV4,'' RFC 3344, August 2002.

[3] F. Adrangi, "Problem Statement: Mobile IPv4 Traversal of VPN Gateways“, draft-ietf-mobileipvpn-problem-statement-req-03, June 2003.

[4] Hesham Soliman, Flarion, Karim El Malki, Ericsson, "Hierarchical Mobile IPv6 mobiliey manage-ment(HMIPv6)", draft-ietf-mipshop-hmipv6-03, October, 2004

[5] Huan Liang, Kabranov, Makrakis, "Minimal cost design of virtual private networks", Electrical and Computer Engineering, 2002. IEEE CCECE 2002. Canadian Conference on, pp.1610~1615, May 2002

[6] S. Vaarala, "Mobile IPv4 Traversal Across IPsec-based VPN Gateways", draft-ietf-mobileip-vpnproblem-solution-03, September 2003.

[7] H. Xie, S.Tabbane, and D.J. Goodman, "Dynamic location area management and per-formance analysis," in Proc. 43rd IEEE Vehicular Technology conference, pp.546~539, 1993

[8] R. Caceres and V.N. Padmanabhan, "Fast and scalable handoffs for wireless internetworks," in Proc. ACM Mobicom '96, pp 55~66

[9] P.Calhoun, C.Perkins, "Mobile IP Network Access Identifier Extension for IPv4," RFC 2794, IETF, March, 2000.

[10] Pat R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application," Internet draft, Internet Engineer Task Force, November 2001.

[11] Bhagavathula, R, Rhanthry, N, Pendse, R, "Mobile IP and virtual private networks," Vehicular Technology Conference, 2002

[12] Aspas, J.P, Arroyo, F.B, "Design of a mobile VPN able to support a large number of users," Universal Multiservice Networks, 2002. ECUMN 2002

[13] Bhagavathula, R, Thanthry, N, Wanyen Lee, Pendse, R, "Mobility: a VPN perspective [mobile computing]," Circuits and Systems, 2002. MWSCAS-2002

[14] Colin Boyd, Anish Mathuria, "Key establishment protocols for secure mobile communications: A selective survey," Lecture Notes in Computer Science, 1998