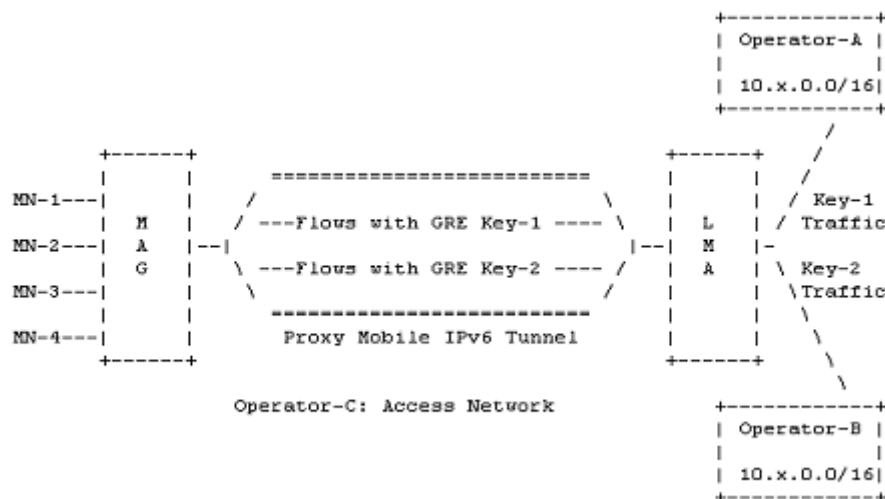


[IPv6] 네트워크-기반 이동성 관리 기법 관련 표준화 동향

PMIPv6(Proxy Mobile IPv6) 프로토콜은 MIPv6(Mobile IPv6) 기능이 구현되어 있지 않은 노드가 이동을 하더라도 기존에 설정되어 있는 연결이 계속 유지될 수 있도록 액세스 망에서 노드의 이동성을 관리하기 위한 네트워크-기반 이동성 관리 기법이며, 현재 IETF의 netlmm(Network-based Localized Mobility Management) 워킹 그룹에서 표준화가 진행 중이다. PMIPv6 프로토콜에 대한 설명은 TTA의 'IT Standard Weekly' 2007-19호 (http://www.tta.or.kr/data/weekly_view.jsp?news_id=1766)에 간략히 설명되어 있다. 지금까지 IETF의 netlmm 워킹 그룹에서는 PMIPv6 프로토콜과 PMIPv6 환경에서의 IPv4 제공 방안에 대한 표준화가 진행되어 왔다. 최근 3월 미국 필라델피아에서 개최된 IETF 71차 회의에서는 향후 일 년 동안 표준화를 진행하기 위한 항목에 대한 논의가 있었다. 이번 회의에서는 워킹 그룹 charter에 포함하기 위한 표준화 대상 항목으로 (1) LMA(Local Mobility Anchor) 발견 기법, (2) AAA 확장, (3) PMIPv6를 위한 GRE(General Routing Encapsulation) 확장, (4) LMA에 의한 MAG와 MN(Mobile Node)간 연결 해지를 위한 바인딩 파기, (5) MAG와 LMA가 각각 상대방이 동작하고 있는지를 검사하기 위한 기능, (6) PMIPv6와 MIPv6 연동, (7) PMIPv6와 MIPv4 연동, (8) NEMO(Network Mobility)와 PMIPv6 연동 및 (9) PMIPv6에서의 경로 최적화 기법 등이 논의되었다. 이 중에서 (1) GRE key 옵션, (2) PMIPv6/MIPv6 연동, (3) AAA 지원, (4) LMA 발견 기법 등에 대한 항목이 향후 일 년 동안 netlmm WG에서 수행할 표준화 항목으로 선택되었다. 이번 보고서에서는 이 항목 중에서 (1) GRE key 옵션과 (2) PMIPv6/MIPv6 연동 기법에 대해서 살펴보고자 한다.

PMIPv6를 위한 GRE key 옵션



<그림 1> 사설 IPv4 주소가 중복되는 경우의 예

그림 1은 이 기법에서 고려되는 네트워크 환경을 보여준다. 서로 다른 네트워크 관리자에

의하여 관리되는 여러 개의 외부 망이 PMIPv6 기반 액세스 망에 접속되고 있는 환경을 고려해보자. 관리자 A는 자신이 관리하는 망(즉, 네트워크 A)에 접속하는 이동 노드인 MN1과 MN2 각각에게 자신이 관리하는 사설 IP 주소 풀에 속하는 서로 다른 IP 주소를 할당한다. 관리자 B는 자신이 관리하는 망(즉, 네트워크 B)에 접속하는 이동 노드인 MN3과 MN4 각각에게 자신이 관리하는 사설 IP 주소 풀에 속하는 서로 다른 주소를 할당한다. MN1과 MN2는 동일한 관리자에 의해서 IP 주소가 관리되기 때문에 서로 다른 IP 주소가 할당되며, MN3과 MN4에게도 마찬가지로 다른 주소가 할당된다. 그렇지만 MN3 또는 MN4에게 할당된 것과 동일한 IP 주소가 MN1 또는 MN2에게 할당될 수 있다. 이는 사설 IP 주소는 전역 주소가 아니며 따라서 주소의 유일성이 보장되지 않기 때문이다. 만일 이러한 서로 다른 네트워크 관리자에 의해서 관리되는 망에 접속했던 노드가 PMIPv6 기반 액세스 망으로 이동하는 경우에는 동일한 (사설) IP 주소가 설정된 여러 개의 MN이 PMIPv6 망에 존재할 수 있으며, PMIPv6 망을 구성하고 있는 구성 요소인 LMA 또는 MAG는 자신이 수신한 패킷을 어떤 노드에게로 전송할 것인지 또는 어떤 망으로 전송해야 하는지를 알 수 없는 문제가 발생한다. GRE Key 옵션 기법은 서로 다른 네트워크 관리자에 의해서 관리되는 망마다 서로 다른 GRE key를 할당하고, 이 key를 IP 패킷의 헤더에 포함함으로써 이 패킷이 어느 곳으로 전송되어야 하는지를 구분하도록 함으로써 위에서 언급한 문제를 해결하기 위한 방법이다. 예를 들어, 그림 1에서 네트워크 A를 위해서 GRE key 1이 설정되고, 또한 네트워크 B를 위해서 GRE key 2가 설정된다고 가정해보자. MN1 또는 MN2로부터 전송되는 패킷을 수신한 MAG는 GRE key 1을 포함하는 GRE 헤더를 붙인 후에 MAG와 LMA 간에 설정된 터널을 통하여 트래픽을 전송한다. 또한 MAG와 설정된 터널을 통하여 전송된 패킷을 수신한 LMA는 GRE 헤더에 있는 키를 이용하여 이 패킷이 네트워크 A로 전송되어야 한다고 판단하고, GRE 헤더를 제거한 후에 이 패킷을 네트워크 A로 전송한다. 또한 네트워크 A로부터 전송된 패킷을 수신한 LMA는 이 패킷에 GRE key 1이 포함된 GRE 헤더를 덧붙인 후에 터널을 통하여 MAG에게로 전송하며, MAG는 수신한 패킷의 GRE 헤더에 있는 key를 이용하여 해당 노드에게로 전송한다. MAG로부터 LMA로 전송되는 패킷에 덧붙여지는 GRE 헤더에 포함되는 것과 동일한 key가 LMA로부터 MAG로 전송되는 패킷에 덧붙여지는 GRE 헤더에도 사용되는 것을 GRE 대칭 key 방법이라고 하며, 다른 key가 사용되는 것을 GRE 비대칭 key 방법이라고 한다. PMIPv6를 위한 GRE key 옵션은 이러한 서로 다른 네트워크 관리자에 의해서 관리되는 망에 접속되어 있던 노드가 하나의 netlmm 도메인에 들어오는 경우에 발생할 수 있는 주소 중복 문제를 해결하기 위한 GRE 캡슐화 모드 협상 및 GRE key 교환 방법을 위한 방법을 표준화하기 위한 것이다.

PMIPv6-MIPv6 연동 시나리오 및 이슈

PMIPv6 프로토콜은 액세스 네트워크 내에서 노드가 이동을 하는 경우에 노드 대신에 네트워크에서 노드의 이동성을 관리하여 주는 네트워크-기반 이동성 관리 기법이며, MIPv6는 IETF에서 개발된 전역 이동성 관리 프로토콜이다. 로컬 이동성 관리를 위하여 PMIPv6가 사

용되고 전역 이동성 관리를 위하여 MIPv6가 사용되는 계층적 구조 환경에서 노드가 이동하는 경우에는 다양한 종류의 시나리오가 고려될 수 있다. 즉, MIPv6는 서로 다른 액세스 네트워크 간에 이동성을 관리하기 위하여 사용되고, 액세스 네트워크 내에서의 이동성은 PMIPv6에 의해서 관리되는 시나리오가 고려될 수 있다. 또한 네트워크-기반 이동성을 제공하고자 하는 노드와 MIPv6 프로토콜을 이용하여 이동성을 관리하고자 하는 노드가 동일한 네트워크 내에 존재하는 경우도 있을 수 있다. 반면 네트워크-기반 이동성을 제공하는 액세스 네트워크와 그렇지 않은 액세스 네트워크가 혼재되어 있는 환경에서 노드가 이동하는 시나리오가 고려될 수 있다. 이 시나리오에서는 다음과 같은 문제점이 발생할 수 있다.

- (1) 바인딩 캐쉬 엔트리 내의 MN에 대한 정보를 등록하거나 검색하기 위한 key 정보로 MIPv6의 경우에는 MN의 홈 주소가 사용되는 반면에 PMIPv6에서는 MN-ID 또는 MN-HNP(Home network prefix)가 사용된다. 따라서 서로 다른 key 정보가 사용되기 때문에, MN이 자신의 홈 네트워크에서 다른 네트워크로 이동을 하는 경우에는 MN에 대한 새로운 바인딩 캐쉬 엔트리가 불필요하게 만들어질 수 있다. 또한 MN이 다른 네트워크에서 자신의 홈 네트워크로 돌아오는 경우에는, MN는 자신의 바인딩 캐쉬 엔트리 삭제를 위하여 등록을 취소해야 한다. 그렇지만 MIPv6에서 이러한 등록 취소는 필수사항이 아니라 권고 사항이다. 만일 MN이 등록 취소를 하지 않으면, 잘못된 바인딩 캐쉬 엔트리에 의해서 패킷 전달에 오류가 발생할 수 있다.
- (2) MN으로부터 전송되는 MIPv6 등록 취소 바인딩 업데이트 메시지로 인하여 PMIPv6 바인딩 캐쉬 엔트리까지 삭제될 수 있다.
- (3) MIPv6와 PMIPv6는 바인딩 업데이트 메시지의 순서를 처리하기 위하여 서로 다른 방법을 이용한다. 즉, MIPv6는 순서 번호 방법을 사용하는 반면에 PMIPv6는 타임스탬프 방법을 이용한다. MN이 PMIPv6 기반 액세스 네트워크로 이동하자마자 다시 non-PMIPv6 기반 액세스 네트워크로 이동을 한 후에 새로운 CoA 주소를 설정하여 이 주소를 포함하는 바인딩 업데이트 메시지를 자신의 홈 에이전트에게로 전송하는 경우를 고려해보자. 만일 MN으로부터 전송된 바인딩 업데이트 메시지보다 MN이 속해있던 PMIPv6 기반 액세스 네트워크에 있는 MAG로부터 전송되는 Proxy 바인딩 업데이트 정보가 HA/LMA에 늦게 도착하게 되면, HA/LMA에는 MN의 위치에 대한 최신 정보가 아닌 이전 정보가 저장되게 되어 MN으로 전송되는 트래픽은 MN으로 전달되지 못하고 MAG로 전송되어 패킷 손실이 발생하는 문제가 발생하게 된다.
- (4) PMIPv6 도메인에 여러 개의 LMA가 존재하고 또한 MN이 MIPv6 외부 네트워크에서 PMIPv6 네트워크로 이동을 하는 경우에, PMIPv6에 있는 MAG가 MN에 대한 HA 기능이 있는 LMA가 아닌 다른 LMA로 Proxy 바인딩 업데이트 메시지를 전송하는 경우에는 외부 네트워크에 있는 호스트로부터 전송되는 트래픽은 MN에게 전달되지 못하는 문제가 발생할 수 있다.

PMIPv6-MIPv6 연동 시나리오 및 이슈에서는 앞에서 언급한 이슈를 해결하기 위한 해결 방법을 표준화하는 것을 목표로 하고 있다.

결언

3GPP와 WiMAX 포럼과 같은 단체에서 액세스간 이동성 지원 프로토콜로서 PMIPv6 프로토콜을 적용하기로 결정하였기 때문에, PMIPv6 프로토콜의 사용이 보편화될 것으로 생각한다. 비록 이번 charter에는 포함되지 않았지만 우리나라에서 PMIPv6 기반 경로 최적화 기법에 대한 표준화를 주도하고 있으므로 향후에 이 기법이 표준화 항목에 포함되기를 기대한다.

이재훈 (동국대학교 정보통신공학과 교수, jaehwoon@dongguk.edu)