HMIPv6에서 MAP을 위한 Return Routability Procedure

이준섭° 정희영 김성한 고석주 민재홍
한국전자통신연구원 표준연구센터
{juns°, hyjung, sk-kim, sjkoh, jhmin}@etri.re.kr

Return Routability Procedure for MAP in HMIPv6

Junseob Lee° Heeyoung Jung Sunghan Kim Seokjoo Koh Jaehong Min
Protocol Engineering Center, Electronics and Telecommunications Research Institute

요 약

IETF에서는 이동노드와 다른 엔티티들 사이에서 발생하는 시그날링을 줄이기 위하여 계층적 이동성 관리 프로토콜(HMIPv6)을 제시하고 있다. HMIPv6는 MAP(Mobility Anchor Point)라는 새로운 엔티티를 도입하여 특정 지역 내에서 지역 홈 에이전트의 역할을 수행하도록 한다. HMIPv6를 이용함으로써 이동노드와 다른 엔티티 간에 발생하는 시그날링을 줄이고, Mobile IPv6의 핸드오프 성능을 개선할 수 있다. HMIPv6에서는 MAP과 이동노드 사이의 보안을 위해 IKE(The Internet Key Exchange)와 같은 보안 프로토콜을 사용하도록 정의하고 있다. 본 논문에서는 많은 부하가 걸리는 IKE 대신에 RR(Return Routability) 절차를 이용하여 이동노드와 MAP 사이의 보안을 제공하는 방법을 제안 한다.

1. 서 론

계층적 이동성 관리 프로토콜인 HMIPv6(Hierarchical Mobile IPv6 mobility management)[1]는 MAP(Mobility Anchor Point)를 도입하여 이동노드(MN)와 홈 에이전트(HA) 또는 상대노드(CN)간의 시그날링을 줄이고 Mobile IPv6의 핸드오프 성능을 개선하기 위하여 개발 되었다. MAP은 방문망에서 MN의 지역 HA의 역할을 수행하며, 지역 내에서의 이동성을 관리한다.

HMIPv6는 기존의 Mobile IPv6[2]에서 MN의 기능을 수정하여 새로운 기능을 제공하며, HA와 CN에는 영향을 미치지 않는다. Mobile IPv6와 마찬가지로 HMIPv6는 하부의 액세스 기술과는 독립적으로 동작하며, 같은 액세스 네트워크나 서로 다른 액세스 네트워크 간의 이동성을 제공한다.

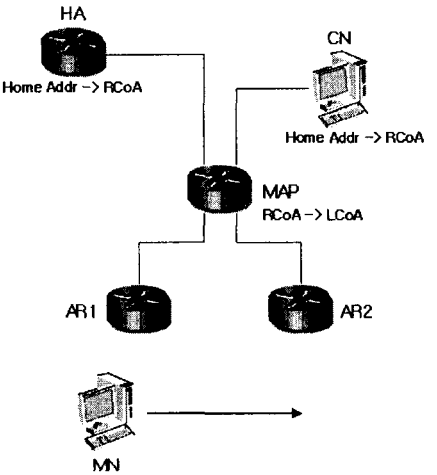
MAP과 MN 사이의 보안을 위해서 HMIPv6는 IKE(The Internet Key Exchange)[3]를 사용하도록 정의하고 있다. 그러나 IKE는 Mobile IPv6에서 볼 수 있듯이 프로토콜 자체가 복잡하고, 패킷의 크기가 크다는 단점이 있다. 이러한 문제점 때문에 Mobile IPv6에서는 CN과 MN 사이의 보안을 위해서 IKE를 사용하지 않고 Return Routability Procedure를 사용하도록 정의하고 있다.

본 논문에서는 HMIPv6를 수정하여 MAP과 MN 사이에서 Return Routability Procedure를 사용하여 보안을 제공하는 방법을 제시한다.

2. HMIPv6의 개요

HMIPv6는 Mobile IPv6와는 달리 MN이 두개의 CoA(Care-of Address)를 갖는다. RCoA(Regional Care-of Address)는 MAP 서브넷의 프리픽스 정보를 이용하여 생성된 CoA이며, LCoA(On-link CoA)는 Mobile IPv6의 CoA와 같이 디폴트 라우터의 프리픽스 정보를 이용하여 생성된 CoA이다.

MAP은 MAP 도메인 내에서 지역 HA 역할을 수행한다. MAP 도메인에 진입한 MN은 지역 MAP 정보를 포함하는 Router Advertisement 메시지를 받게 된다. MN은 MAP 서브넷을 기반으로 생성한 주소와 디폴트 라우터를 기반으로 생성한 주소를 결합시킨다. MAP은 등록된 모든 MN으로 향하는 패킷을 가로채고, 이를 캡슐화하여 MN으로 전달하는 역할을 수행한다. MN은 MAP 도메인에 진입 후 RCoA를 생성하여 HA와 CN에 바인딩을 갱신한다. MN이 MAP 도메인 내에서 위치를 변경하는 경우에는 새로운 LCoA를 생성한 후 MAP에 등록 하는 것만으로 모든 이동성 관리가 이루어진다. MAP은 MN의 RCoA와 LCoA의 매핑 정보를 관리한다. RCoA는 MN이 MAP 도메인 내에 있는 동안 변하지 않는다.



[그림 1] 계층적 Mobile IPv6 도메인

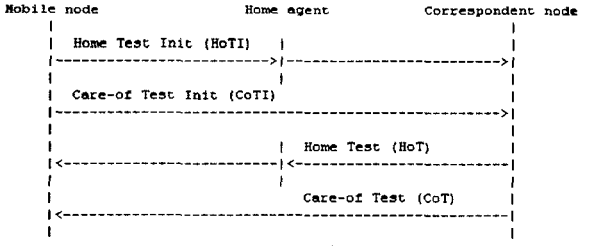
[그림 1]과 같이 MN이 새로운 MAP 도메인에 진입한 경우 HA 및 CN에 RCoA를 사용하여 바인딩 정보를 갱신하고, 도메인 내에서 이동하는 경우에는 새로운 LCoA를 생성하여 MAP에 등록된 바인딩 정보를 갱신한다. 따라서 HA와 CN은 MN의 실제 위치를 알지 못하고, 단지 RCoA 만을 알게 된다. HA와 CN의 Binding Cache는 MN의 홈 주소와 RCoA의 매핑 정보를 포함하고, MAP의 Binding Cache는 RCoA와 LCoA의 매핑 정보를 포함한다.

HMIPv6를 사용함으로써 MN이 MAP 도메인 내에서 움직이는 경우 HA나 CN과의 바인딩 갱신을 위한 시그날이 MAP 도메인 밖으로 나가지 않게 되며, MN의 이동성 관리는 MAP 도메인 내에서 빠르고 간단하게 이루어진다.

MAP은 자신에게 등록한 MN이 LCoA를 바꾸는 경우, 바인딩 정보의 변경을 요구하는 MN이 이전에 자신에게 등록한 MN인지를 확인하기 위하여 IKE를 사용하여 인증을 수행한다.

3. Mobile IPv6에서의 Return Routability Procedure

Mobile IPv6에서 MN은 새로운 위치로 이동하는 경우 CN에 바인딩 정보를 갱신하게 된다. 이 경우 CN은 새로운 바인딩 정보를 보내는 MN이 이전에 바인딩 정보를 보낸 MN인지 인증을 수행해야 한다. 이를 위해 Mobile IPv6에는 Return Routability Procedure를 사용한다. Mobile IPv6에서 Return Routability Procedure는 [그림 2]와 같다.



[그림 2] Mobile IPv6의 Return Routability Procedure

Return Routability Procedure의 결과로 MN은 HoT 메시지와 CoT 메시지를 받게 된다. CN은 바인딩에 사용되는 키의 정보를 HoT 메시지와 CoT 메시지에 분산시켜 전송하게 된다. MN은 HoT 메시지에 포함된 home keygen token과 CoT 메시지에 포함된 care-of keygen token의 정보를 이용하여 바인딩에 사용되는 키(Kbm)를 생성하게 된다. 따라서 MN과 CN은 같은 키를 공유하게 된다.

Return Routability Procedure에서 HoT 메시지는 MN의 홈 주소로 전달되고 CoT 메시지는 MN의 CoA로 전달된다. HoT 메시지는 MN의 HA에 의해 MN으로 전달된다. 즉, 홈 주소와 CoA로 전달된 두 데이터를 모두 받을 수 있는 MN은 정당한 사용자로 인증 할 수 있다는 것이다.

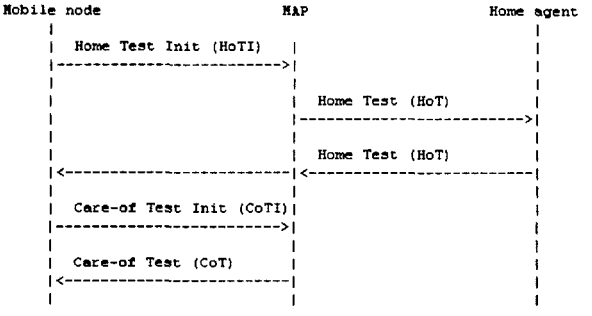
4. MAP과 MN 사이의 Return Routability Procedure

MN이 MAP 도메인 내에서 이동하는 경우, MN은 MAP에 바인딩 정보를 갱신해야 하며, 이때 MAP과 MN 사이에 공유되는 키가 필요하게 된다. HMIPv6에서는 MAP과 MN이 키를 공유하기 위해서 IKE를 사용하도록 정의하고 있다. 본 논문에서는 Return Routability Procedure를 이용하여 키를 공유하는 방법을 제안한다.

4.1 MAP Return Routability Procedure

MAP과 MN 사이의 키 교환을 위한 MAP Return Routability Procedure는 [그림 3]과 같다. MAP은 이러한 기능을 수행하기 위해 Mobile IPv6의 *"IPv6 Nodes with Support for Route Optimization"*와 같은 기능을 수행할 수 있어야 한다. 즉, MAP은 Mobile IPv6에서의 CN과 같이 Mobility Header를 처리할 수 있어야 한다. Mobility Header 중에서 Return Routability Procedure의 처리를 위해 필요한 메시지로는 HoTI 메시지, HoT 메시지, CoTI 메시지, CoT 메시지가 있다. MN은 MAP에 바인딩 정보를 갱신할 때 HoTI 메시지에 Home Address Destination Option을 추가하여 보낼 수 있어야 한다.

MN이 새로운 MAP 도메인에 진입한 경우, RCoA와 LCoA를 생성한 후, MN은 MAP에 바인딩 정보를 갱신하고, HA에 RCoA를 등록 한다. 모든 절차가 끝나면, MAP Return Routability Procedure를 수행하여, MAP과 공유하는 바인딩 키(Kbm)를 생성 한다. 이후, MAP 도메인 내에서 이동하여 다른 액세스 라우터의 관리 영역으로 이동한 것을 감지한 경우 MN은 이전에 생성한 Kbm을 이용하여 MAP의 바인딩 정보를 갱신한다.



[그림 3] MAP Return Routability Procedure

4.2 MAP Return Routability Procedure의 메시지

MAP Return Routability Procedure에 사용되는 각 메시지의 내용은 다음과 같다.

(1) Home Test Init (HoTI)
- Source Address = RCoA
- Destination Address = MAP
- Parameters:
  - home init cookie

(2) Care-of Test Init (CoTI)
- Source Address = LCoA
- Destination Address = MAP
- Parameters:
  · care-of init cookie

(3) Home Test (HoT)
- Source Address = MAP
- Destination Address = home address
- Parameters:
  · home init cookie
  · home keygen token
  · home nonce index

(4) Care-of Test (CoT)
- Source Address = MAP
- Destination Address = LCoA
- Parameters:
  · care-of init cookie
  · care-of keygen token
  · care-of nonce index

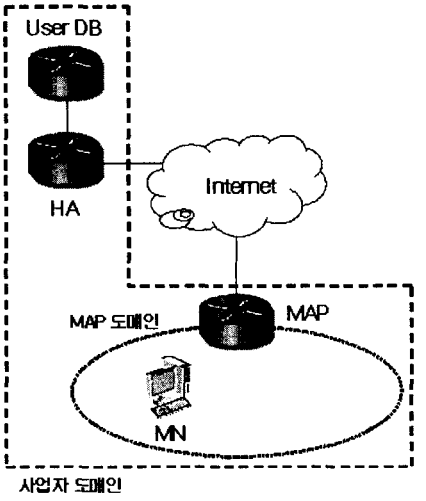
MN은 HoTI 메시지에 Home Address Destination Option을 추가하여 보내고, MAP은 이 정보를 이용하여 HoT 메시지를 MN의 홈 주소로 보낸다. HA와 MN은 상호 인증을 통해 HA의 바인딩 정보를 갱신하였으므로, HA가 RCoA로 정보를 보낼 수 있다는 것은 MN이 HA에 RCoA를 등록한 사실을 증명한다. 즉, HA와 MN 사이의 인증 결과를 MAP과 MN의 인증에 반영하는 것이다.

MAP은 MN의 홈 주소와 RCoA 정보를 이용하여, home keygen token과 care-of keygen token을 생성한다. 즉, MAP은 care-of keygen token을 생성할 때, LCoA가 아닌 RCoA를 사용한다.

4.3 활용 방안

일반적으로 망 사업자는 [그림 4]와 같이 홈 네트워크에서 사용자 관리를 위해 필요한 모든 정보를 관리하고, Hot Spot 지역에 공중 무선랜 서비스를 제공하기 위한 무선 액세스 장비를 설치 할 것이다. 또한 이동성의 제공을 위해 Mobile IPv6 기능을 제공할 것이며, MAP을 사용하지 않는 경우, MN이 이동할 때 마다 HA에 등록을 해야 하므로 홈 네트워크에 많은 부하가 가해지게 된다. 또한 HMIPv6와 같이 MAP을 사용하는 경우, HA에 가해지는 부하를 줄일 수 있지만, IKE를 이용하여 MAP과 MN 사이에 별도의 인증을 수행하기 때문에 MAP과 사용자 정보를 관리하는 서버 사이의 정보 교환 절차가 필요하게 된다.

본 논문에서 제안하는 방식을 사용하는 경우 HA가 HoT 메시지를 전달하는 과정에서 필요한 인증 및 과금 정보를 확인 할 수 있어 MAP과 사용자 정보를 관리하는 서버 사이의 별도의 프로토콜이 필요하지 않게 된다. MAP에 전달할 필요가 있는 사용자 정보는 HoT 메시지에 옵션으로 추가하여 보낼 수 있다.



[그림 4] 활용 방안

5. 결론

공중 무선랜 서비스가 점차 활성화됨에 따라 이동성 지원 및 관리 기능이 필수 요소로 부각되고 있으며, 이동성 관리를 위한 시그날링을 줄이고자 하는 시도들이 제안되고 있다.

본 논문에서는 MN과 HA 또는 CN간의 시그날링을 줄이고 Mobile IPv6의 핸드오프 성능을 개선하기 위한 HMIPv6를 소개하고, MAP과 MN 사이의 인증을 위한 새로운 방법을 제시하였다.

*Mobile IPv6의 Return Routability Procedure*를 수정하여 MAP과 MN 사이에서 사용할 수 있도록 함으로써, HMIPv6의 장점을 그대로 수용하면서, IKE의 사용을 배제할 수 있다. 또한, 사업자의 관점에서 사용자 정보 관리 등의 측면에서 보다 효율적인 해결책으로 사용될 수 있을 것이다.

참고문헌

[1] Hesham Soliman, et al., "Hierarchical mobile IPv6 mobility management (HMIPv6)," draft-ietf-mobileip-hmipv6-07.txt, October 2002.

[2] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-20.txt, January 2003.

[3] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)," *RFC 2409*, November 1998.