제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

HMIPv6 에서 MAP 과 이동노드 사이의 Return Routability Procedure

이준섭, 정희영, 김성한, 고석주, 민재홍
한국전자통신연구원 표준연구센터
e-mail : juns@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

IETF 에서는 이동노드와 다른 엔티티들 사이에서 발생하는 시그널링을 줄이기 위하여 계층적 이동성 관리 프로토콜(HMIPv6)을 제시하고 있다. HMIPv6 는 MAP 이라는 새로운 엔티티를 도입하여 특정 지역 내에서 지역 홈 에이전트의 역할을 수행하도록 함으로써 이동노드와 다른 엔티티 간에 발생하는 시그널링을 줄이고, Mobile IPv6 의 핸드오프 성능을 개선하도록 하고 있다. HMIPv6 에서는 MAP 과 이동노드 사이의 인증을 위해 IKE 와 같은 보안 프로토콜을 사용하도록 정의하고 있다. 본 논문에서는 많은 부하가 걸리는 IKE 대신에 RR(Return Routability) 절차를 이용하여 이동노드와 MAP 사이의 인증을 제공하는 방법을 제안 한다.

1. 서론

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 시그널링을 줄이고 Mobile IPv6 의 핸드오프 성능을 개선하기 위하여 개발 되었다. MAP 은 방문망에서 MN 의 지역 HA 의 역할을 수행하며, 지역 내에서의 이동성을 관리한다.

HMIPv6 는 기존의 Mobile IPv6[2]에서 MN 의 기능을 수정하여 새로운 기능을 제공하며, HA 와 CN 에는 영향을 미치지 않는다. Mobile IPv6 와 마찬가지로 HMIPv6 는 하부의 액세스 기술과는 독립적으로 동작한다.

HMIPv6 는 MAP 과 MN 사이의 인증을 위해서 IKE(The Internet Key Exchange)[3]를 사용하도록 정의하고 있다. 그러나 IKE 는 프로토콜 자체가 복잡하고, 패킷의 크기가 크다는 단점이 있다. 이러한 문제점 때문에 Mobile IPv6 에서는 CN 과 MN 사이의 인증을 위해서 IKE 를 사용하지 않고 Return Routability Procedure 를 사용하도록 정의하고 있다.

본 논문에서는 HMIPv6 를 수정하여 MAP 과 MN 사이에서 Return Routability Procedure 를 사용하여 인증 기능을 제공하는 방법을 제시한다.

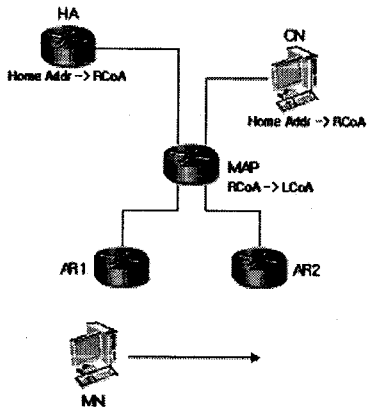
2. HMIPv6 의 개요

Mobile IPv6 와는 달리 HMIPv6 에서 MN 은 두 개의 CoA(Care-of Address)를 갖는다. MN 은 MAP 서브넷의 프리픽스 정보를 이용하여 RCoA(Regional Care-of Address)를 생성하고, Mobile IPv6 의 CoA 와 같이 디폴트 라우터의 프리픽스 정보를 이용하여 LCoA(On-link CoA)를 생성한다.

MAP 은 MAP 도메인 내에서 지역 HA 역할을 수행한다. MAP 도메인 내의 액세스 라우터들은 MAP 의 정보를 포함한 Router Advertisement 메시지를 주기적으로 발송한다. 이 메시지를 받은 MN 은 RCoA 와 LCoA 를 생성하고 MAP 에 등록한다. MAP 은 등록된

모든 MN 으로 향하는 패킷을 가로채고, 이를 캡슐화 하여 MN 으로 전달하는 역할을 수행한다.

[그림 1]과 같이 MN 은 MAP 도메인에 진입 후 RCoA 를 생성하여 HA 와 CN 에 바인딩을 갱신한다. MN 이 MAP 도메인 내에서 위치를 변경하는 경우에는 새로운 LCoA 를 생성한 후 MAP 에 등록 하는 것만으로 모든 이동성 관리가 이루어 진다. MAP 은 MN 의 RCoA 와 LCoA 의 매핑 정보를 관리한다. RCoA 는 MN 이 MAP 도메인 내에 있는 동안 변하지 않는다. 따라서 HA 와 CN 은 MN 의 실제 위치를 알지 못하고, 단지 RCoA 만을 알게 된다.



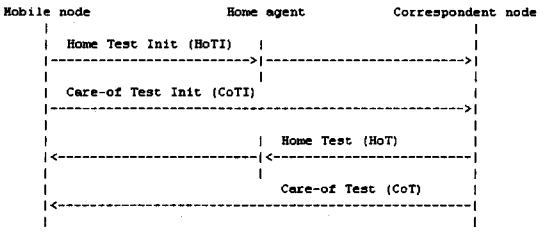
[그림 1] 계층적 Mobile IPv6 도메인

HMIPv6 를 사용함으로써 MN 이 MAP 도메인 내에서 움직이는 경우 HA 나 CN 과의 바인딩 갱신을 위한 시그널이 MAP 도메인 밖으로 나가지 않게 되며, MN 의 이동성 관리는 MAP 도메인 내에서 빠르고 간단하게 이루어 진다.

MAP 은 자신에게 등록한 MN 이 LCoA 를 바꾸는 경우, 바인딩 정보의 변경을 요구하는 MN 이 이전에 자신에게 등록한 MN 인지를 확인하기 위하여 IKE 를 사용하여 인증을 수행한다.

3. Mobile IPv6 에서의 Return Routability Procedure

Mobile IPv6 에서 MN 은 새로운 위치로 이동하는 경우 CN 에 바인딩 정보를 갱신하게 된다. 이 경우 CN 은 새로운 바인딩 정보를 보내는 MN 이 이전에 바인딩 정보를 보낸 MN 인지 인증을 수행해야 한다. 이를 위해 Mobile IPv6 에는 Return Routability Procedure 를 사용한다. Mobile IPv6 에서 Return Routability Procedure 는 [그림 2]와 같다.



[그림 2] Mobile IPv6 의 Return Routability Procedure

CN 은 바인딩에 사용되는 키의 정보를 HoT 메시지와 CoT 메시지에 분산시켜 전송하게 된다. Return Routability Procedure 의 결과로 MN 은 HoT 메시지와 CoT 메시지를 받게 된다. MN 은 HoT 메시지에 포함된 home keygen token 과 CoT 메시지에 포함된 care-of keygen token 의 정보를 이용하여 바인딩에 사용되는 키(Kbm)를 생성하게 된다. 따라서 MN 과 CN 은 같은 키를 공유하게 된다.

Return Routability Procedure 에서 HoT 메시지는 MN 의 홈 주소로 전달되고 CoT 메시지는 MN 의 CoA 로 전달된다. HoT 메시지는 MN 의 HA 에 의해 MN 으로 전달된다. 즉, 홈 주소와 CoA 로 전달된 두 데이터를 모두 받을 수 있는 MN 은 정당한 사용자로 인증 할 수 있다는 것이다.

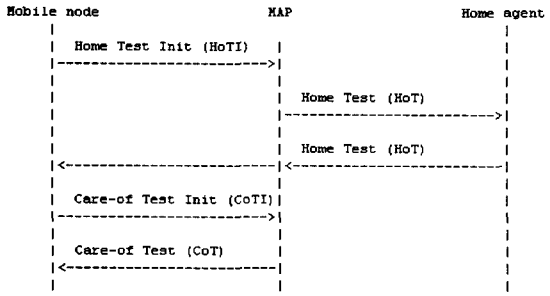
4. MAP 과 MN 사이의 Return Routability Procedure

MN 이 MAP 도메인 내에서 이동하는 경우, MN 은 MAP 에 바인딩 정보를 갱신해야 하며, 이때 MAP 과 MN 사이에 공유되는 키가 필요하게 된다. HMIPv6 에서는 MAP 과 MN 이 키를 공유하기 위해서 IKE 를 사용하도록 정의하고 있다. 본 논문에서는 Return Routability Procedure 를 이용하여 키를 공유하는 방법을 제안한다.

4.1 Return Routability Procedure

MAP 과 MN 사이의 키 교환을 위한 MAP Return Routability Procedure 는 [그림 3]과 같다. MAP 은 이런 기능을 수행하기 위해 Mobile IPv6 의 *"IPv6 Nodes with Support for Route Optimization"*와 같은 기능을 수행할 수 있어야 한다. 즉, MAP 은 Mobile IPv6 에서의 CN 과 같이 Mobility Header 를 처리할 수 있어야 한다. Mobility Header 중에서 Return Routability Procedure 의 처리를 위해 필요한 메시지로는 HoTI 메시지, HoT 메시지, CoTI 메시지, CoT 메시지가 있다. MN 은 MAP 에 바인딩 정보를 갱신할 때 HoTI 메시지에 Home Address Destination Option 을 추가하여 보낼 수 있어야

한다.



[그림 3] MAP Return Routability Procedure

MN 이 새로운 MAP 도메인에 진입한 경우, RCoA 와 LCoA 를 생성한 후, MN 은 MAP 에 바인딩 정보를 갱신하고, HA 에 RCoA 를 등록 한다. 모든 절차가 끝나면, MAP Return Routability Procedure 를 수행하여, MAP 과 공유하는 바인딩 키(Kbm)를 생성 한다. 이후, MAP 도메인 내에서 이동하여 다른 액세스 라우터의 관리 영역으로 이동한 것을 감지한 경우 MN 은 이전에 생성한 Kbm 을 이용하여 MAP 의 바인딩 정보를 갱신한다.

4.2 MAP Return Routability Procedure 의 메시지

MAP Return Routability Procedure 에 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

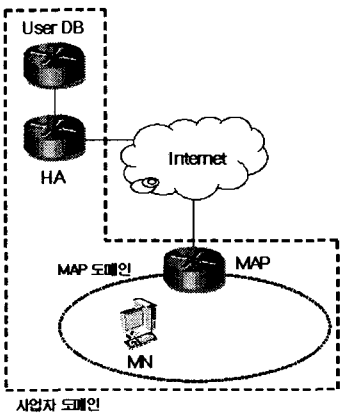
(4) Care-of Test (CoT)
- Source Address = MAP
- Destination Address = LCoA
- Parameters:
  - care-of init cookie
  - care-of keygen token
  - care-of nonce index

MN 은 HoTI 메시지에 Home Address Destination Option 을 추가하여 보내고, MAP 은 이 정보를 이용하여 HoT 메시지를 MN 의 홈 주소로 보낸다. HA 와 MN 은 상호 인증을 통해 HA 의 바인딩 정보를 갱신하였으므로, HA 가 RCoA 로 정보를 보낼 수 있다는 것은 MN 이 HA 에 RCoA 를 등록한 사실을 증명한다. 즉, HA 와 MN 사이의 인증 결과를 MAP 과 MN 의 인증에 반영하는 것이다.

MAP 은 MN 의 홈 주소와 RCoA 정보를 이용하여, home keygen token 과 care-of keygen token 을 생성한다. 즉, MAP 은 care-of keygen token 을 생성할 때, LCoA 가 아닌 RCoA 를 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, MAP 을 사용하지 않는 경우, MN 이 이동할 때 마다 HA 에 등록을 해야 하므로 홈 네트워크에 많은 부하가 가해지게 된다. 또한 HMIPv6 와 같이 MAP 을 사용하는 경우, HA 에 가해지는 부하를 줄일 수 있지만, IKE 를 이용하여 MAP 과 MN 사이에 별도의 인증을 수행하기 때문에 MAP 과 사용자 정보를 관리하는 서버 사이의 정보 교환 절차가 필요하게 된다.



[그림 4] 활용 방안

본 논문에서 제안하는 방식을 사용하는 경우 HA

가 HoT 메시지를 전달하는 과정에서 필요한 인증 및 과금 정보를 확인 할 수 있어 MAP 과 사용자 정보를 관리하는 서버 사이의 별도의 프로토콜이 필요하지 않게 된다. MAP 에 전달할 필요가 있는 사용자 정보는 HoT 메시지에 옵션으로 추가하여 보낼 수 있다.

5. 결론

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

본 논문에서는 MN 과 HA 또는 CN 간의 시그널링을 줄이고 Mobile IPv6 의 핸드오프 성능을 개선하기 위한 HMIPv6 를 소개하고, MAP 과 MN 사이의 인증을 위한 새로운 방법을 제시하였다.

Mobile IPv6 의 Return Routability Procedure 를 수정하여 MAP 과 MN 사이에서 사용할 수 있도록 함으로써, HMIPv6 의 장점을 그대로 수용하면서, IKE 의 사용을 배제할 수 있다. 또한, 사업자의 관점에서 사용자 정보 관리 등의 측면에서 보다 효율적인 해결책으로 사용될 수 있을 것이다.

참고문헌

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

[2] D. Johnson et al., "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-20.txt, January 2003.

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