Hierarchical Mobile IPv6 환경에서 AAA 인증 위임 모델에 관한 연구

송 주 용° 송 주 석 김 현 곤
연세대학교 컴퓨터과학과, 한국전자통신연구원 AAA 정보보호연구팀
{jysong°, jssong}@emerald.yonsei.ac.kr hyungon@etri.re.kr

A Study on Delegated-Authentication AAA Model in Hierarchical Mobile IPv6 Environment

Jooyong Song° Joosuk Song Hyungon Kim
Dept. of Computer Science, Computer and Communication Laboratory, Yonsei University
AAA Security Information Research Team, Electronics and Telecommunications Research Institute

요 약

Hierarchical Mobile IP(HMIP)는 Micro Mobility 관리를 위한 효율적인 방안을 제공한다. 즉, HMIP 환경에서는 Mobility Anchor Point(MAP) 관리 도메인내의 이동시 MN의 지역 바인딩 갱신(Local Binding Update) 메시지를 MAP에서 처리함으로써, 홈 도메인과의 등록 메시지 교환량을 감소시킬 수 있다. 그러나 MAP 관리 도메인과 MN 사이에는 기 설정된 비밀 정보가 존재하지 않기 때문에, 사용자 이동시 필요한 인증을 수행하기 위해서는 MN과 홈 도메인과의 정보 교환이 요구된다. 본 논문에서는 HMIP 환경에서 사용자의 인증을 위해 Diameter Mobile IPv6 응용을 적용한 모델을 제시한다. 이와 함께, MAP와 연계된 방문망의 AAA 서버로의 인증 권한 위임을 통해, 홈 도메인과의 정보 교환을 감소시키는 효율적인 Micro Mobility 관리 방안을 제공한다.

1. 서 론

최근 인터넷은 괄목할만한 추세로 적용 범위를 넓혀가고 있다. 더욱이 보다 편리한 서비스의 제공을 위한 이동성의 지원은 인터넷에 있어 이제는 간과할 수 없는 요소로 자리 잡아가고 있다. 이에 따라, 유사한 성질의 서비스를 제공하는 네트워크 사업자간의 상호간의 연동이 필요하며, 상이한 사업자가 관리하는 데이터 네트워크간의 사용자 로밍은 이를 위한 필수적인 요소로 대두되고 있다.

Mobile IPv6는 사용자의 이동시 서비스의 끊김없이 네트워크 접속점을 변경할 수 있는 기능을 제공한다.[1] 사용자 노드(MN)는 도메인간의 이동시, 새로운 주소(CoA)를 획득하고, 이를 바인딩 갱신(BU) 메시지를 통하여 홈 에이전트(HA)에게 알린다. 이에 따라 HA는 이동에 따른 변경된 MN의 CoA를 계속 유지함으로써, 끊김없는 서비스를 제공할 수 있다. 그러나 사용자 노드의 접속점 변경은 패킷의 손실이나 데이터 전달의 지연 시간을 유발할 수 있다. 이를 최소화하기 위해 IETF IP Routing for Wireless/Mobile host 워킹 그룹은 Fast Handover 메커니즘[2] 및 Hierarchical Mobile IP상의 이동성 지원[3]에 대한 표준화를 진행 중이다.

이와 함께, 상이한 관리 도메인간의 이동 환경에서는 사용자가 보안성을 유지하면서 이동 인터넷을 이용할 수 있는지의 여부가 중요시된다. 이에 따라, 사용자의 인증 및 MN과 HA 간 교환되는 등록 메시지의 인증에 대한 중요성이 크게 증대되고 있다. 그러나 Mobile IP는 이러한 보안성 제공 기능이 취약하며, 타 관리 도메인간의 이동에 필요한 과금 및 인증, 권한 관리 기능을 제공하지 않는다. 이러한 취약점을 보완하기 위하여, 최근 AAA (Authentication, Authorization, Accounting) 프로토콜과 Mobile IP의 결합에 대한 연구가 활발히 진행중이다.[5] 이중 IETF Authentication, Authorization, Accounting 워킹 그룹이 표준화 진행중인 Diameter 프로토콜[4]이 기존 AAA 서버의 단점을 보완하고, PPP 및 Mobile IPv6등의 다양한 접속 기술에 적용될 수 있는 차세대 AAA 프로토콜로써 주목받고 있다.

본 논문에서는 Mobile IPv6 환경에서 Micro Mobility 관리 를 위해 요구되는 사용자의 인증 과정을 최적화한 Diameter 적용 모델을 제시한다. 제 2장에서는 Hierarchical Mobile IPv6 메커니즘을 소개하며, 제 3장에서는 Mobile IPv6를 위한 Diameter 응용을 설명한다. 제 4장에서는 사용자 인증 기능 최적화를 위한 Diameter 적용 모델을 제안하고, 제 5장에서 결론을 맺는다.

2. Hierarchical Mobile IPv6

일반적인 Mobile IP 환경에서는 사용자가 거리상 가까운 도메인으로 이동하더라도, CoA의 등록을 위해 바인딩 갱신(BU)메시지가 여러 개의 IP 네트워크를 통해서 홈 도메인까지 전달되는 경우가 빈번하다. 이에 따라, 과도한 핸드오버 지연 시간이 발생하게 되며, 경우에 따라서는 실시간 서비스나 지연 시간에 종속적인 서비스의 제공이 어려워 질 수 있다. 이를 해결하기 위해, IETF IP Routing for Wireless / Mobile host 워킹 그룹은 Micro Mobility 처리 시 HA 및 대응 노드(CN)와의 메시지 교환을 줄이기 위하여, 라우터를 계층적으로 구성하는 Hierarchical Mobile IPv6 (HMIPv6)메커니즘[3]을 제안하고 있다.

HMIPv6는 Micro Mobility를 처리하기 위한 새로운 노드인 Mobility Anchor Point(MAP)를 도입하였다. MAP의 관

리 도메인에 진입한 MN은 자신의 현재 위치(LCoA)를 MAP의 관리 도메인상의 주소(RCoA)와 바인딩시킨다. 이 경우, MAP는 지역적인 HA의 역할을 수행하게 되며, MN을 목적지 주소로 하는 패킷을 송신한 경우, 해당 패킷을 처리하여 MN에게 포워딩하게 된다. MN이 MAP의 관리 도메인 내에서 이동하는 경우, HA 및 CN은 이를 인지하지 못하며, LCoA와 RCoA와의 바인딩 변경을 위해, MN은 MAP에게 지역 바인딩 갱신(Local Binding Update) 메시지를 전달한다. CN 및 HA와의 바인딩 갱신은 MN이 MAP의 관리 도메인을 변경하는 경우에 한해서 이루어지며, 이 경우, RCoA가 바인딩 갱신의 목적으로 전달된다.

3. Diameter Mobile IPv6 응용

Diameter는 AAA 노드간의 메시지 교환 및 경로 설정을 위한 규약을 정의하고 있는 기본 프로토콜[4]을 근간으로 하여, 필요한 서비스마다 관련 응용을 정의하고 있으며, 필요에 의한 추가적인 서비스 응용이 가능한 프로토콜이다. Diameter Mobile IPv6 Application은 Mobile IPv6환경에서, 사용자에 대한 인증/권한관리, 키 분배 및 바인딩 갱신의 최적화 등을 지원하기 위한 응용이다.[5]

새로운 도메인에 진입한, MN은 홈 도메인의 AAA(AAAh)와 공유하고 있는 비밀정보(Security Association)를 이용하여, MN의 인증정보 및 바인딩 갱신 메시지, 세션키 요청 메시지등을 포함한 요청 메시지를 AAA 클라이언트(예:Access Router)에게 보낸다. 이를 전달받은 AAA 클라이언트는 관련 정보를 AAA 프로토콜로 변환하여, 방문 도메인의 AAA(AAAv)를 통해 AAAh에게 전달한다. AAA 프로토콜은 각 정보를 Attribute Value Pair(AVP) 형태로 인코딩하여 구성한다. AAAh는 MN에 대한 인증 및 관련 노드와의 세션 키 생성 과정을 수행하고, HA에게 바인딩 갱신 메시지를 포함하는 메시지를 넘겨준다. HA는 바인딩 갱신 메시지를 인증한 뒤 바인딩 캐쉬 생성을 완료하고, AAAh가 전달한 키 생성 정보를 통해 키를 생성한다. 작업이 완료되면, MN에 전달할 바인딩 응답(Binding Acknowledge)을 수반한 메시지를 AAAh에 전달한다. 해당 메시지는 AAAh - AAAv의 경로를 통해 AAA 클라이언트에게 전해지고, 최종적으로 MN이 인증 결과 및 바인딩 응답 메시지를 확인함으로써, 바인딩 갱신 과정과 MN 인증 과정을 동시에 처리하게 된다.

4. Hierarchicl Mobile IPv6 환경을 위한 Diameter 인증 위임 모델

HMIPv6 메커니즘은 HA 및 CN과의 등록 메시지의 교환량을 줄일 수 있지만, 이동한 MN과 MAP 간의 SA 부재에 따라, MAP의 도메인 내에서 단독으로 MN에 대한 인증을 수행할 수 없다. 결국 MN에 대한 인증을 위해서는, 홈 도메인으로부터 인증 관련 정보 획득이 필요하다. 이를 해결하기 위해, MN이 MAP의 관리 도메인에 진입했을 때, 최초 지역 바인딩 갱신 과정을 통해, MAP와 연결된 Anchor AAA가 AAAh로부터 인증 권한을 위임받아, MAP 관리 도메인 내의 이동에 관련된 인증을 처리할 수 있는 모델을 제안한다.

4.1 AAAh로부터 인증 권한 위임

① Registration Request (Reg Req) : MAP의 관리 도메인에 진입한 MN은 지역 바인딩 갱신을 위한 MIP 요청 메시지를 구성하여 Access Router(AR : AAA 클라이언트)에 전달한다. 해당 메시지는 지역 바인딩 갱신, MN-AAAh SA에 기반한 MN 인증정보 및 인증 위임을 위한 키 요청으로 구성된다.

② Local Registration Request (LRR) : Reg Req로부터 지역 바인딩 갱신, MN 인증정보를 추출한 AR은 다음과 같은 AVP로 구성된 AAA 메시지를 생성한다.

- User Name AVP : MN의 NAI 정보
- Local Binding Update AVP : 지역 바인딩 갱신 메시지
- EAP AVP : MN의 인증정보
- Anchor AAA Server AVP : MAP와 연계된 AAA 서버 정보. 홈망까지 AAA 체인 구성시, Anchor AAA를 경로에 추가할 수 있도록 명시한다. MAP의 주소로부터 추출할 수 있다.
- MAP Address AVP : MAP의 주소 정보. 본 AVP를 통해 Anchor AAA는 바인딩 갱신 AVP를 전달할 MAP를 인식할 수 있다.
- Security Key AVP : MN-Anchor AAA간 비밀 설정을 위한 파라미터 정보

AAAv는 Anchor AAA Server AVP를 통하여 Anchor AAA 서버를 인식하고, LLR을 포워딩한다. Anchor AAA와 AAAv가 동일한 노드인 경우에는 포워딩 과정이 생략된다.

③ MAP Authentication Request (MAR) : Anchor AAA는 현재, MN을 직접 인증할 수 없기 때문에, AAAh에 MN의 인증을 요청한다. 이 과정에서 차후 지역 내 이동시 인증을 처리하기 위해 인증 권한 위임도 요청한다. MAR은 LRR의 내용에 다음과 같은 AVP가 추가된다.

- Delegation Request Flag AVP : 인증 위임 요청

④ MAP Authentication Answer (MAA) : MAR을 수신한 AAAh는 MN에 대한 인증을 수행한다. 이와 함께, Anchor AAA-MN간 비밀정보를 생성하여 응답 메시지를 통해 전달한다. 또한, 인증의 대상이 되는 MN을 인증 위임 리스트에 저장한다. 관련 AVP는 다음과 같다.

- Delegation Info AVP : 인증 위임의 대상이 되는 MN의 NAI 정보
- MN-Anchor AAA Key AVP : MN-Anchor AAA간 SA 설정을 위한 비밀 정보. Anchor AAA는 본 AVP를 이용하여 MN와의 비밀 정보를 추출하고 SA를 구성한다.
- MIP Security AVP : MN-Anchor AAA간 SA 설정을 위한 비밀 정보. 해당 내용은 바인딩 응답 메시지 내부에 포함되어 MN으로 전달된다. MN은 바인딩 응답으로부터 전달된 해당 정보를 통해, Anchor AAA와의 비밀 정보를 추출한다.
- Action AVP : 인증 결과

⑤ MAP MIPv6 Request (MMR) : MAA를 수신한 Anchor AAA는 Delegation Info AVP를 통해 지역 이동시 인증을 수행할 수 있는 MN의 정보 인증 위임 리스트에 저장한다. MN 인증을 위한 SA 관련 정보를 추출한 뒤, MAP로 지역 바인딩 갱신 메시지를 전달한다.

⑥ MAP MIPv6 Answer (MMA) : 지역 바인딩 갱신을 완료한 MAP는 MIP Security AVP의 내용을 포함하는 지역 바인

딩 응답 메시지를 생성하여 AVP로 인코딩한다. MIP Security AVP는 MN-AAAh간 공유된 비밀로 보안성이 유지되기 때문에, MAP는 MN-Anchor AAA 공유 비밀 정보를 확인할 수 없다.

- Local Binding Acknowledge AVP : 지역 바인딩 응답

⑦ Local Registration Answer (LRA) : 인증 및 바인딩 갱신에 대한 결과를 통보하기 위해, Anchor AAA는 해당 AAA 메시지를 생성하여 AR까지 전달한다.

⑧ Registration Answer (Reg Ans) : AR은 LRA로부터 추출된 바인딩 응답 메시지 MN과 통신가능한 MIP 메시지로 변환한다. Reg Ans를 수신한 MN은 바인딩 응답 메시지와 함께 Anchor AAA와 공유하는 비밀 정보를 추출하여 SA를 구성한다. 이후, MAP 관리 도메인 내의 인증은 Anchor AAA에 의하여 이루어진다.

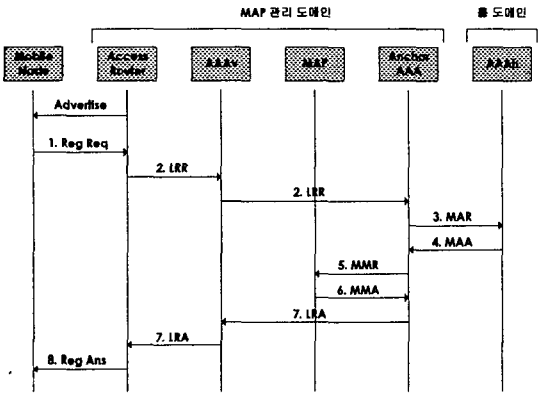

그림 1. 인증 권한 위임 과정

HA 및 CN으로 RCoA를 전달하는 바인딩 갱신 과정은 일반적인 Diameter MIPv6 응용을 따른다.[5]

4.2 Anchor AAA에 의한 MN의 인증

① Registration Request (Reg Req) : MAP 관리 도메인내의 이동시, MN은 지역 바인딩 갱신 메시지를 AR에 전달한다. 이 경우, 이미 Anchor AAA-MN간 SA가 성립되었기 때문에 MN의 인증 정보는 Anchor AAA-MN간 SA에 기반한다.

② Local Registration Request (LRR) : LRR은 인증 권한 위임의 경우와 동일한 AVP로 구성된다. 경우에 따라 Security Key AVP를 통해 MN-MAP간 비밀 키 요청이 전달될 수 있다.

③ MAP MIPv6 Request (MMR) : LRR을 수신한 Anchor AAA는 인증 위임 리스트로부터 MN를 검색한다. 인증 위임 리스트에서 MN을 확인하면, AAAh로 메시지를 포워딩하지 않고 직접 MN에 대한 인증을 수행한다. 인증이 완료되면, MMR을 구성하여 MAP에 전달한다. MN-MAP간 비밀키 요청이 존재하는 경우 비밀 정보를 생성하여 MMR에 추가한다.

④ MAP MIPv6 Answer (MMA) : 지역 바인딩 갱신을 완료한 MAP는 바인딩 응답 메시지를 생성하여 MMA를 통해 전달한다.

⑤ Local Registration Answer (LRA) : Anchor AAA는 MMA로부터 관련 정보를 추출하여 AAAv를 통해 AR에게 전달한다.

⑥ Registration Answer : MN은 해당 메시지를 통해, 바인딩 갱신이 완료되었음을 확인한다. 경우에 따라, MN-MAP간 비밀 키 요청이 처리된 경우, 키를 추출하여 저장한다.

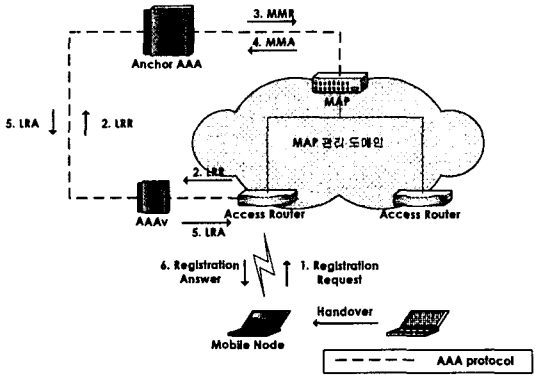

그림 2. Anchor AAA에 의한 MN 인증 과정

5. 결 론

본 논문에서는 Micro Mobility 관리 시 요구되는 MN에 대한 인증을 위해, Diameter MIPv6 응용을 도입하여 관리하는 모델을 제시하였다. 본 모델의 핵심은, 최초 지역 바인딩 갱신 메시지 전달 과정에 AAA 프로토콜을 통하여, MN에 대한 인증을 수행함과 동시에 Anchor AAA에게 MN에 대한 비밀 정보 전달과정을 통합함으로써, 인증 권한을 위임한 데 있다. 차후 지역적인 MN의 이동에 대한 인증은 홈 도메인과의 정보 교환 없이 자체적으로 처리될 수 있다. 이를 통해, HMIPv6 메커니즘이 목적하는 HA와의 메시지 교환량 감소의 장점을 유지하면서, MN에 대한 인증을 수행하는 방안을 제공할 수 있다.

참 고 문 헌

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt, IETF Mobile IP Internet Draft, Jun 2003

[2] Rajeev Koodli, "Fast Handovers for Mobile IPv6", draft-ietf-mobileip-fast-mipv6-06.txt, IETF Mobile IP Ineternet Draft, Mar 2003

[3] H. Soliman, C. Castelluccia, K. El-Malki, L. Bellier, "Hierarchical Mobile IPv6 mobility management", draft-ietf-mobileip-hmipv6-08.txt, IETF Mobile IP Ineternet Draft, Jun 2003

[4] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", draft-ietf-aaa-diameter-17.txt, IETF AAA Internet Draft, Dec 2002

[5] S. Faccin, F. Le, B. Patil, C. Perkins, "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-03.txt, IETF AAA Internet Draft, Apr 2003