제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

HMIPv6를 위한 Diameter 기반의 AAA 서비스에 관한 연구

황선웅*, 송주석*
*연세대학교 컴퓨터과학과
e-mail:{swhwang, jssong}@emerald.yonsei.ac.kr

A Study on Diameter-based AAA Services for Hierarchical Mobile IPv6

SunWoong Hwang*, JooSeok Song*
*Dept. of Computer Science, Yonsei University

요 약

Mobile IPv6에 Diameter 기술을 적용하여 모바일 유저의 인증, 권한 검증, 과금 뿐만 아니라 미래 서비스를 수용할 수 있는 확장성을 보장할 수 있는 AAA 서비스 기술이 IETF의 WG에서 연구되고 있다. 본 논문에서는 Diameter 기반의 AAA 서비스를 Mobile IPv6의 문제점 중 위치 등록에 따른 시그널링 수와 긴 핸드오프 지연을 개선한 Hierarchical Mobile IPv6 기술에 적용하여 강화된 보안 및 빠른 핸드오프를 통해 끊김 없는 서비스 제공 방안을 제시하고자 한다.

1. 서론

이동 정보화 사회가 빠르게 현실화 되면서 유·무선 고속 데이터 전송이 가능한 개방형 네트워크 기반 구조가 구축되고 있으며, 새롭고 흥미 있는 서비스가 모바일 유저에게도 제공될 것이다. 현재 음성, 데이터, 영상들을 전송하는 기본 프로토콜은 인터넷 프로토콜(IP)이며, 향후 서비스의 다양화에 따른 방대한 IP 주소의 요구가 있을 것이고 IPv4 주소체계는 한계에 도달할 것으로 예상된다. 이 문제를 해결하기 위해 IPv6의 도입이 준비중이며, IPv6는 지구상의 모든 개체에 주소를 부여할 수 있을 만큼 충분한 IP 주소가 공급된 것이다.

Mobile IPv6[1]는 모바일 유저가 홈 네트워크나 방문 네트워크를 통해 어느 곳에서든지 서비스 제공 네트워크에 접근해서 서비스를 받을 수 있도록 설계된 프로토콜이다. MIPv6는 차세대 셀룰러 전화 네트워크의 기반이 될 기술로서 모바일 유저의 등록 정보 인증 및 데이터 전송에 대한 보안 기능이 보장되어야 하며, 모바일 유저의 이동에 따른 끊김없는 서비스 제공을 위해 빠른 핸드오프 기능이 제공되어야 한다.

IETF의 WG에서는 네트워크 사용자의 인증(Authentication), 권한검증(Authorization), 과금(Accounting)에 관련된 AAA 개념을 정의하였고, MIPv6 환경에서 AAA 기능을 제공하기 위해 Diameter 프로토콜을 연구 중에 있다. 또한 MIPv6의 도메인 상에서 핸드오프 기능 개선을 위해 Hierarchical Mobile IPv6(HMIPv6)[3] 기술을 연구하고 있다.

본 논문에서는 모바일 유저가 인증을 받고 바른 사용 권한을 할당받아 이동시에도 끊김이 없는 신뢰성 있는 서비스를 제공 받을 수 있도록 HMIPv6 기술에 Diameter 프로토콜을 적용한 AAA 서비스 방안을 제시하고자 한다. 2장에서는 관련 연구를 살펴보고, 3장은 HMIPv6와 AAA Architecture를 통합하는 방안을 제안하고, 4장에서는 성능 분석, 5장에서는 결론과 향후 연구분야에 대해 기술하고자 한다.

2. 관련 연구

가. Mobile IPv6

Mobile IPv6는 IPv6의 기능을 그대로 이용하면서 이동성을 제공하고자 하기 때문에 Mobile IPv4보다 효과적으로 이동성을 지원할 수 있으며 탁월한 확장성도 지니고 있다. Neighbor Discovery와 Address Autoconfiguration 기능을 이용하여 이동 단말이 이동하였을 때 자동으로 자신의 위치 정보를 구성할 수 있도록 하였으며, 자신이 이동한 위치 정보를 필요한 노드들에게 알릴 수 있도록 Destination 옵션을 추가함으로써, IPv4에서는 필요했던 일부 시그널 메시지들과 에이전트를 제거하였다. 또한 Route

Optimization을 위한 프로토콜이 기본 기능으로 제공되고 있다.

Mobile IPv6는 홈 에이전트(HA), 홈 네트워크, Correspond Node(CN), CoA(Care Of Address)등의 Mobile IPv4의 기본개념을 그대로 수용하고 있다. Mobile Node(MN)은 이동하면서 방문 링크로부터 CoA를 획득하고 HA에게 이동 서비스를 요청하는 객체이다. 홈 네트워크를 떠나면 MN은 먼저 Neighbor Discovery 매커니즘을 통해 이동을 감지하고, 로컬 라우터에서는 ICMPv6 Router Advertisement 메시지를 주기적으로 보낸다. MN은 Stateless나 Stateful Address Autoconfiguration을 통해 새로운 CoA를 획득한다. 그리고 MN은 Binding Update(BU) 매커니즘을 통해 HA에 새로운 CoA를 등록한다. MN은 BU 메시지를 Binding ACK(BA) 메시지가 되돌아 올 때까지 HA에 보내고, 이 후 MN의 홈 어드레스와 CoA가 Binding 되고 HA의 캐쉬에 등록된다. HA라는 홈 네트워크 상의 라우터는 등록된 CoA의 Binding Cache를 유지한다. 등록 후 HA는 MN에게 오는 패킷을 터널링하여 MN에 보낸다. MN은 소스 어드레스처럼 CoA를 사용하여 패킷을 CN에게 직접 전달 할 수 있고, CN이 패킷의 근원지를 식별할 수 있도록 MN은 Destination Options[1]안에 홈 어드레스를 실어 보낸다.

나. Hierarchical Mobile IPv6

핸드오프 속도 측면에서 Mobile IPv6의 성능을 향상시키고 CN과 HA에 보내는 BU 메시지의 수를 줄이기 위해 IETF에서 HMIPv6를 연구중에 있다. 그림 1에는 HMIPv6의 기본 구조를 보여 주고 있다. MAP(Mobility Anchor Point)이라는 새로운 Mobile IPv6 노드 개념을 도입하고, AR(Access Router)로부터 시작하며 계층상의 어떤 레벨에도 위치할 수 있도록 하여 추가적인 이동성관리 기능을 제공한다. MN이 MAP 도메인 내의 다른 AR로 이동되었을 때, MAP 도메인의 RCoA(Regional CoA)를, AR로부터 LCoA(on-link CoA)를 얻는다. 그리고 나서 MN은 BU 메시지를 MAP 에게 보내고 이 메시지를 통해 RCoA와 LCoA가 Binding 된다. MAP은 이 Binding 정보를 Binding Cache에 저장한다. MN은 MAP 도메인이 변경되었을 때 만, BU 메시지를 자신의 HA와 CN에 보내서 홈 어드레스와 RCoA를 Binding 한다.

MAP은 HA처럼 동작하고, HA나 CN들로부터 오는 MN의 RCoA로 지정된 패킷들을 받는다. 패킷들은 MAP으로부터 IPv6 Encapsulation 기법을 통해 MN의 LCoA로 터널링 된다. MN은 받은 패킷을 Decapsulation하여 처리한다.

HMIPv6는 Mobile IPv6에 비해 핸드오프 속도를 많이 개선할 수 있고, MN이 도메인 내에서 이동시는 BU를 HA와 CN에 보낼 필요가 없기 때문에, 실제적으로 도메인 내의 이동이 많은 모바일 유저의 특성을 고려하며 메시지의 수를 많이 줄일 수 있다.

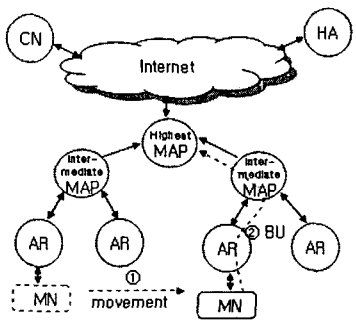

그림1 Hierarchical Mobile IPv6 구조

다. Diameter 기반의 AAA 구조[2]

AAA는 다중 네트워크상에서 인증(Authentication), 권한검증(Authorization), 과금(Accounting)등의 기능들을 조정하는 프레임 워크이다. Diameter는 이러한 AAA 서버에서 사용되는 프로토콜로, 기존의 Point-to-Point(PPP)와 Roaming, Mobile IP와 같은 새로운 정책과 AAA 서비스를 위한 확장 기반을 제공하기 위한 가벼운 Peer 기반의 AAA 프로토콜이다.

Diameter Base Protocol은 독립적으로 사용되지 않고 특정한 응용들을 위해 확장된 형태로 사용된다. 현재까지의 Diameter 확장은 NASREQ, Mobile IP, CMS, Strong Security 등이다. 기본 Diameter 프로토콜은 자체 능력 협상, Peer간 메시지 송수신 방법과 종료 방법 등을 규정하고, 다른 Diameter 사이에 교환되는 모든 메시지에 대한 규칙을 규정한다. 이 프로토콜을 IPsec과 같은 하위 레벨의 보안 프로토콜이 없는 경우 응용 레벨의 보안 Attribute Value Pairs(AVP)를 선택적으로 사용할 수 있도록 하였다.

Mobile IPv6에 Diameter 구조를 적용하기 위해 Mobile 개체와 3가지 AAA 개체를 포함한 구조를 정의하고 있다.

- Home AAA(AAAH) 서버는 MN의 홈 네트워크에 위치하여, MN을 인증하고 특정 HA에 MN을 등록할 때 권한을 부여 한다. 또한 AAAH는 Diameter 개체들에 키를 분배한다.
- Foreign AAA(AAAF/AAAL) 서버는 MN의 방문(로컬) 네트워크에 위치하고 자체적으로 MN의 인증을 처리할 수 없을 때 AAAH에 인증 요청을 포워드 한다.
- Attendant는 MN과 AAAL과의 서비스 인터페이스를 제공하는 노드로서 Mobile IPv4에서는 FA가

그 역할을 담당한다.

Mobile IPv6는 FA가 없기 때문에 AAA 구조를 쉽게 매핑 할 수 없다. MN을 전송 전에 서버에 연결시킬 수 있는 가능한 방법은 Address Auto-configuration 절차를 Attendant 기능과 결합시키는 것이다. Stateful Autoconfiguration은 Attendant를 DHCPv6 서버 상에 위치시키고, Stateless Auto-configuration은 ICMPv6 프로토콜을 채용하여 로컬 라우터에 ICMPv6 모듈을 탑재한다.

3. HMIPv6와 Diameter 기반의 AAA 구조의 통합

가. 통합 Protocol의 요구사항

HMIPv6와 Diameter 기반의 AAA 구조를 통합한 프로토콜의 요구사항과 설계목표는 다음과 같다.

- 고가의 무선네트워크에서 MIPv6 시그널링의 수를 줄임
- 핸드오프 속도 향상
- 최소 변화를 통한 사용자 확장성 제공
- Replay Protection 보장
- Authentication 서비스
- Security Association(SA) 협상
- Security Parameter들의 기밀성 보장

본 논문에서는 [3], [4]의 장점을 유지하면서 보다 확장성을 가진 신뢰성 있는 이동성 관리가 지원되는 AAA 서비스 모델을 개발하고자 한다.

나. 통합 Protocol 구조 설계

본 논문에서는 현재 IETF의 mobileip WG에서 제안한 HMIPv6[3]과 aaa WG에서 제안한 Diameter Mobile IPv6 Application[4]를 통합하여 보다 향상된 프로토콜 구조를 설계하고자 한다.

그림1은 HMIPv6 구조로서 MAP을 계층 구조로 설계하여 확장성을 보장하고 Intra-domain 핸드오프 시 MAP 도메인 내에서 BU를 처리 할 수 구성되었다.

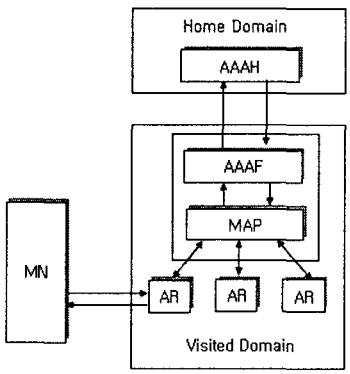

그림2 Message Sequences in HMIPv6 with AAA Architecture

그림2는 AAA 기반 구조를 그림1의 Hierarchical 네트워크 구조를 포함한 HMIPv6 구조에 적용하여 확장시킨 것이다. 특히 MAP과 AAAF를 통합함으로서 인증에 필요한 메시지 수를 줄일 수 있다. MN은 AR을 통해 MAP에 접속하게 되고 MAP은 사용자가 요구하는 서비스에 대해 인증 및 권한 검증의 역할을 도메인 내에서 수행한다.

AAA 기반 구조 내에서 MN은 네트워크 접근 권한을 얻기 위해 Dynamic Home Agent Address Discovery[1]를 수행하고 선택된 HA에게 Diameter 메시지인 AVP들에 기반을 둔 특정 보안 응용(e.g. IKE)을 사용하여 AAA 메시지 교환을 보호하기 위한 SA를 협상한다. 이 절차는 Visited Domain과 Home Domain간에 많은 Round trip 메시지를 필요로 하지만 AAA 기반구조를 사용함으로서 효율적이고 빠른 대안을 제시한다.

다. Inter-domain 핸드오프

그림3의 메시지 전달에서 보듯이 Mobile IPv6의 Payload와 키 값들을 Diameter 메시지 내에 Piggy-back하여 전달하는 것이다. 즉 MN이 HA와 SA를 공유하면 MN은 자신의 RCoA를 포함한 BU를 생성하여 MAP과 AAA 서버를 거쳐 HA에 보내서 자신을 등록한다. 그렇지 않은 경우, AAAH가 MN에 대한 HA를 할당하고 BU를 생성하여, 향후 MN을 인증하는데 사용할 키 값들을 HA에 보낸다. 정상적인 BU가 이루어지면 HA는 Hop-by-hop을 거쳐 MN에 포워딩 되는 Diameter 메시지에 BA 메시지를 Encapsulation 하여 보낸다.

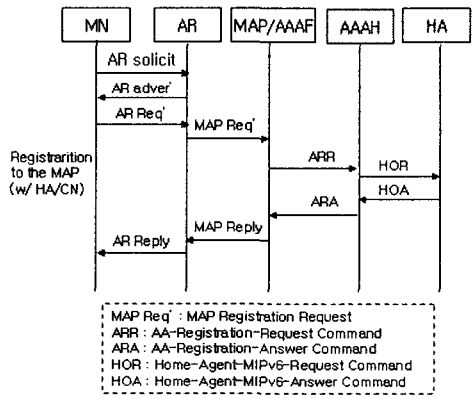

그림3 Diameter Message Sequences in Inter-domain Handoff

라. Intra-domain 핸드오프

MN이 이동을 탐지한 후 MAP에서 유지하는 Binding Cache를 참조하여 동일한 MAP 내에서 이동하였음을 알았을 때 MN은 MAP에 새로운 LCoA

를 등록한다. 이 때 HA와 CN을 위한 RCoA는 변경되지 않는다. 이 때 Old AR에 저장되어 있던 인증정보가 New AR로 전송되어 New AR에 이동되어 온 MN이 등록될 시 사용된다.

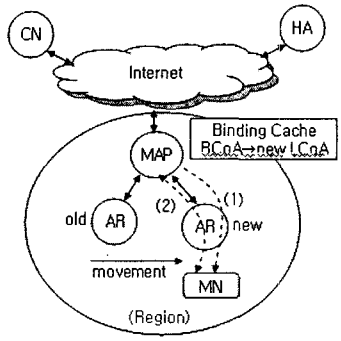

그림4 Intra-domain Handoff operation

로컬 핸드오프의 경우 위치등록 시그널링 메시지가 동일 MAP상에서만 전송되기 때문에 시그널링에 대한 지연을 줄일수 있고 시그널링에 대한 오버로드도 감소시킬 수 있다.

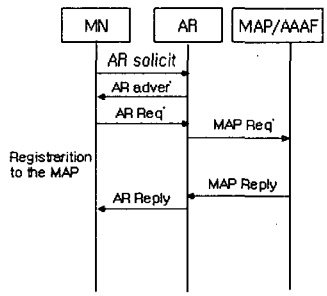

그림5 Message Sequences in Intra-domain Handoff

4. 성능 분석

AR이 LC(Local Challenge) 필드를 Router Advertisement 메시지에 실어 보냄으로서 MN의 Request 가 새로운 것인지를 검증하고 Replay 공격을 탐지 할 수 있다.

인증 서비스는 MN은 Network Access Identifier (NAI)에 의해서 식별되고 Request 메시지내의 Credential 에 포함된 전자서명을 보고 AAAH에 의해 홈 어드레스가 인증된다. MN과 HA간에 하부계층의 보안 프로토콜인 IPsec을 통한 SA 협상이 지원되지 않는 상태에서 IKE 프로토콜의 사용이 가능하다. 또한 SA가 협상된 상태에서 Diameter 메시지들의 전달시 기밀성과 무결성도 보장된다고 하겠다.

동일 MAP으로 구성된 Region 내에서 MN이 이동시 BU를 HA나 CN에 보낼 필요가 없기 때문에 시그널링 수를 감소시켜 무선 자원을 낭비하지 않고, 핸드오프 처리에 대한 속도도 향상시킬 수 있다. 또한 Diameter 프로토콜의 응용 시 Broker 모델을 도입하면 확장성 측면도 매우 강화가 되며, MAP을 이용한 계층구조의 네트워크 연결도 확장성을 보강해 주는 방법론이다.

5. 결론 및 향후 연구

본 논문에서는 모바일 유저의 핸드오프 속도를 빠르게 하고, 무선네트워크 상에서 교환되는 위치등록 시그널링 메시지 수를 줄이며, 유저의 인증과 권한 검증, 과금의 문제를 해결하고, 미래 서비스를 수용할 수 있는 확장성을 보장할 수 있도록 HMIPv6 구조와 Diameter 기반의 AAA 구조를 통합한 모델을 제시하였다. IPv6 주소체계가 도입이 되고, Mobile IPv6가 차세대 셀룰러 네트워크 기반 기술로 발전함에 따라 신뢰성 있고 빠른 이동성 관리 기술을 제공할 것으로 기대한다.

향후 연구에서는 Mobile IPv6망에서 핸드오프 속도 개선 및 보안 성능 강화 뿐 만 아니라 QoS 보장을 위한 기법에 대해서도 연구가 필요하고 제안된 각 기법에 대한 시뮬레이션을 통하여 실제적으로 어떠한 성능 효과를 나타내는지에 대한 연구가 필요하다.

참고문헌

[1] Perkins, C et al., "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-18 (work in progress), July 2002.

[2] Calhoun, P., "Diameter Base Protocol", draft-ietf-aaa-diameter-12, July 2002.

[3] Castelluccia, C., Soliman, H et al., "Hierarchical MIPv6 mobility management (HMIPv6)", draft-ietf-mobileip-hmipv6-06,July 2002.

[4] Faccin, S., "Diameter Mobile IPv6 Application", draft-le-aaa-diameter-mobileipv6-01, November 2001.

[5] Laurent-Maknavicius, M.; Dupont, F. "Inter-domain Security for Mobile IPv6", Universal Multiservice Networks, 2002.

[6] X. Fu et al., "SeQoMo Architecture: Interactions of Security, QoS and Mobility Components", TKN Technical Report TKN-02-008, April 2002