2006년도 대한전자공학회 하계종합학술대회 제29권 제1호

F-HMIPv6 지원을 위한 보안 아키텍처

손상우*, 김문기**, 이병호***
한양대학교 정보통신학과

A Study on Security Architecture for F-MIPv6

Sangwoo Son*, Munki Kim**, Byungho Rhee***
Dept. of Information and Communications, Hanyang University
E-mail : *cyberscv@naver.com, **clevermg@nate.com, **mailto:bhrhee@hanyang.ac.kr

Abstract

F-HMIPv6 is protocol that supports fast handovers for Hierarchical Mobile IPv6. Unlike HMIPv6 (Hierarchical Mobile IPv6), it sends FBU(Fast Binding Update) by predicted Router's Information for a potential handover. But, The current version of this protocol doesn't ensure impeccably between mobile node and router. To make up for the weak points of the security, we propose the architecture for F-HMIPv6 protocol to structurally reinforce the security and improve weak security of among mobile node, MAP(Mobility Anchor Point), and routers for binding update when mobile node conducts handovers.

I. 서론

무선 인터넷의 주된 핵심은 가장 개인화 된 단말기인 이동전화 또는 PDA 등 휴대장비에서 고정된 단말기(PC)환경과 같은 인터넷 서비스를 사용할 수 있다. 이러한 무선 인터넷 환경에서의 이동성을 지원하기 위한 핵심기술이 Mobile IP 이며, Mobile IP 기술은 차세대 인터넷 기술로 각광을 받고 있다.

Mobile IP 는 IP 주소를 가진 단말의 이동시 그 연결을 항상 보장하는 기술이다. 이것은 이원화된 주소체계를 통하여 이동성을 지원하고, 임시 주소를 이용하여 단말이 이동한 라우팅 지역이 변하는 것에 따라 지속적인 인터넷 서비스를 가능하게 하는 것이다. 이와 같은 서비스 제공을 위해 이동성을 극대화 할 수 있는 Mobile IPv6[1] 기술이 주목을 받고 있으며, 그 중 Fast Handover for Hierarchical MIPv6 (F-HMIPv6)의 방법이 관심을 받고 있다.

본 논문에서는 F-HMIPv6 에서의 핸드오버시에 이동노드와 맵, 라우터간의 바인딩 업데이트시 보안 취약점을 개선하기 위한 방법을 제안한다.

II. 본론

Mobile IPv6 에서의 Fast 핸드오버를 지원하기 위한 방안인 F-HMIPv6 는 지역망을 관리하는 MAP(Mobility Anchor Point)을 이용한다. MAP 은 이동노드와 AR(Access Router)간의 시그널링을 줄임으로써 딜레이를 감소시킨다. 그림 1 의 구조를 가진다. 그리고, FMIPv6 (Fast Handovers for Mobile IPv6)[2]에서의 핸드오버가 일어날 대상인 nAR(new Access Router)의 정보를 기반으로 예측이동하는 방안을 조합하여, 기존의 HMIPv6[3]보다 향상된 결과를 가져온다. 그 프로토콜 절차는 그림 2 과 같다.

이 기본 절차에는 보안상 취약점이 있다. 그것은 바인딩 업데이트시에 전송된 주소만으로는 전송한 노드가 합법적인 노드인지 판단할 수 없다는 것이다. 그래서 반드시 임시적인 SA 를 MN 과 AR, MAP 사이에 맺어 신뢰적인 체인을 형성해야한다. 하지만, 빈번한 SA 설

. 본 연구는 대학 IT 연구센터 육성 지원 사업의 연구결과로써 HY-SDR 연구센터의 연구비 지원으로 수행되었음

정은 핸드오버시에 딜레이를 증가시킬 수 있다.

위에서 언급한 문제점을 개선하기위해서 본 논문에서는 다음과 같은 아키텍처를 제안한다. 이 시나리오에서는 보안요소를 적용할 범위를 MAP 이 관리하는 영역으로 한정한다. 그리고 각 노드들은 CA 의 위임을 받은 MAP 으로부터 인증서를 받는다. MAP 은 관리 영역안에서 적용할 공개키, 알고리즘, 보안 파라미터들을 관리하게 된다. 그림 1 에서 처럼 각각 지역 셀을 관리하는 AR 에게 영역안에서 사용될 보안 요소정보를 알려주게 되고, 보안요소가 변경되었을 시에 재분배하게 된다. 그 후 AR 들은 받은 보안 요소를 적용하고 노드와 통신시에 사용하게 된다. 이동 노드와 AR 사이에 SA 설립 후 이동 노드가 새로운망으로 이동시에 PAR 은 NAR 로 핸드오버 전에 SA 정보를 전달하게 된다. NAR 은 전달 받은 SA 정보에 대한 ID 를 발급한다. 핸드오버가 일어난 후에 MN 은 ID 를 전달하고 일치한다면 SA 재사용이 허락되고, 그렇지 않으면 NAR 은 SPI 값을 다시 할당하여 SA 설정을 한다. 이것은 새로운 SA 설립하지 않고 재사용 함으로써 보안파라미터 교환 딜레이를 줄일 수 있다는 장점이 있다. 또한, SA 설립시에 간편하게 설정할 수 있다.

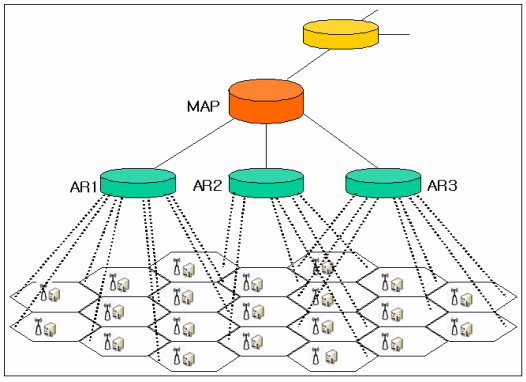

그림 1. F-HMIPv6 기본 구성도

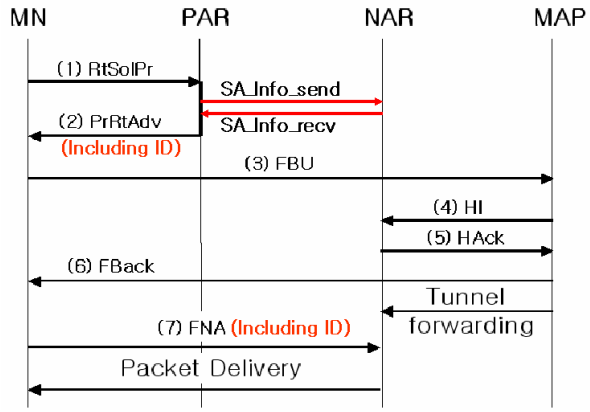

그림 2. 제안된 F-HMIPv6 핸드오버시 절차

Ⅲ. 결론

Mobile IPv6 의 빠른 핸드오버를 지원하기 위한 프로토콜인 F-HMIPv6 는 핸드오버 발생시에 이동할 새로운 망의 정보를 이동하기 전에 갖고, Fast Binding Update 를 시도하기 때문에 반드시 노드와 라우터간의 인증절차는 필요하다.

이 논문에서는 공개키 알고리즘에 기반하여 특정 MAP 커버리지 영역안에서 이동 노드가 이동시에 기존망과의 SA 를 다른 AR 영역에서도 사용함으로써 노드를 인증하고 빠른 핸드오버를 지원할 수 있는 방안에 대하여 제안하였다. 이동 노드와 PAR 간의 SA 를 맺고 핸드오버가 일어난 후에 이 SA 정보를 NAR 에 전달하여 새로운 설정없이 다시 재사용하여 SA 설정 비용을 줄이는 방안을 제시하였다.

향후, 이 영역 안에서의 AR 와 MAP 사이의 인증 방안과 다른 도메인 이동시에 키 교환에 대하여 연구가 필요하고, Mobile 이라는 특성을 고려한 보안 키 최소화가 요구된다.

참고문헌

[1] ISO/IEC 14496-1:2002, “Information techno-logy coding of audio-visual objects ”

[2] Aaron E. Walsh and Mikael BougesSevenier, MPEG-4 Jump Start. Prentice Hall PTR, 2002.

[3] A. Smolic and R.Yamshita, “Application and Requirements for 3DAV”, ISO/IEC JTC1/ SC29/WG11 N4982, July 2002.

[4] Yunjong choi, Sukhee cho, “Limitation on 3D realvideo coding using MAC”, ISO/ IEC JTC1/ SC29/WG11 M8627, July 2002.