http://dx.doi.org/10.3745/KIPSTC.2012.19C.2.099

프록시 모바일 IPv6 네트워크에서 LMA도메인 간 핸드오버 기법의 보안성 분석 및 구현

채 현 석[†] · 정 종 필[††]

요 약

PMIPv6는 기존 프로토콜과는 다르게 MN이 이동성의 주체가 아니라, 네트워크 구성 요소들이 MN의 이동성을 보장해준다. MN이 해야 했던 일들을 네트워크를 구성하는 요소들이 대신 수행해줌으로써 MN은 소형화 및 경량화가 가능하다. 그중에서PMIPv6(Proxy Mobile IPv6)[1] 프로토콜에서 인증, 권한 검증, 과금을 지원하는 AAA 프로토콜을사용하여 이동성과 MN장치의 보안성을 제공하는 방법이 제안되었다. 이 방법은 MN장치의 보안성을 제공하고 패킷손실을 줄일 수 있는 좋은 이점에도 불구하고, 보호되지 않는 시그널링 메시지에 대한 보안 위협이 있으며, 도메인간의 전역 이동성은 지원하지 않는다.

본 논문에서는 You-Lee-Sakurai-Hori의 ESS-FH 기법과 Kang-Park[3] 기법을 분석하여 PMIPv6 환경에 적용하여 AAA 프로토콜을 통해 각 객체간의 상호인증과 비밀키 설정 및 관리를 통해 안전한 핸드오버를 수행할 수 있음을 설명하고, 서비스 거부 공격 및 리다이렉트 공격으로부터 안전함을 설명하고, 논리적인 BAN로직 도구를 이용하여 및 이동성 모델링을 통해 검증하였다. 또한 PMIPv6 환경하에서 도메인간의 고속 핸드오버 기법을 제안하다.

키워드 : FPMIPv6, CGA, AAA, 반 로직, 보안 분석, ESS-FH

Security Analysis and Implementation of Fast Inter-LMA domain Handover Scheme in Proxy Mobile IPv6 Networks

Chai Hyun Suk[†] · Jeong Jong Pil[††]

ABSTRACT

In PMIPv6-based network, mobile nodes can be made smaller and lighter because the network nodes perform the mobility management-related functions on behalf of the mobile nodes. The one of the protocols, Fast Handovers for Proxy Mobile IPv6(FPMIPv6)[1] has studied by the Internet Engineering Task Force(IETF). Since FPMIPv6 adopts the entities and the concepts of Fast Handovers for Mobile IPv6(FMIPv6) in Proxy Mobile IPv6(PMIPv6), it reduces the packet loss. Conventional scheme has proposed that it cooperated with an Authentication, Authorization and Accounting(AAA) infrastructure for authentication of a mobile node in PMIPv6, Despite the best efficiency, without begin secured of signaling messages, PMIPv6 is vulnerable to various security threats such as the DoS or redirect attAcks and it can not support global mobility between PMIPv. In this paper, we analyze Kang-Park & ESS-FH scheme, and then propose an Enhanced Security scheme for FPMIPv6(ESS-FP). Based on the CGA method and the pubilc key Cryptography, ESS-FP provides the strong key exchange and the key independence in addition to improving the weaknesses for FPMIPv6. The proposed scheme is formally verified based on Ban-logic, and its handover latency is analyzed and compared with that of Kang-Park scheme[3] & ESS-FH and this paper propose inter-domain fast handover sheme for PMIPv6 using proxy-based FMIPv6(FPMIPv6).

Keywords : FPMIPv6, CGA, AAA, BAN-logic, Security Analysis, ESS-FH

1. 서 론

현재 이동 통신은 모든 네트워크에 IP를 적용하는 All-IP 형태로 발전하고 있다. 유·무선 통합망을 기반으로 다양한 종류의 MN(Mobile Node)과 장비를 통해서 모든 장치와 콘텐츠에 접근이 가능하며 각종 멀티미디어를 복합적으로 응용할 수 있는 서비스와 홈 네트워크 및 광대역 통합망(BcN)

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(2011-0027030).
† 준 회 원 : 성균관대학교 정보통신공학부 공학석사
†† 정 회 원 : 성균관대학교 정보통신공학부 공학박사(교신저자)
논문접수 : 2011년 12월 26일
수 정 일 : 1차 2012년 2월 2일
심사완료 : 2012년 2월 8일

서비스 구축를 위해 IPv6의 이동성 관련 연구가 진행되고 있다. 이동성 연구의 중요한 목표는 이동 중에도 연속적인 통신을 유지하는 것이다. 이에 따라 MIP(Mobile IP)를 시작으로 연구와 표준화 작업을 진행하였으며, IETF(Internet Engineering Task Force)에서는 MIPv6(Mobile IPv6) [1]를 시작으로 FMIPv6(Fast Mobile IPv6) [2], HMIPv6 (Hierarchical Mobile IPv6) [3]를 비롯하여 MN이 스스로 HA(Home Agent)에 위치 등록을 하고 새로운 도메인의 CoA(Care-of-Address)를 생성하는 클라이언트 기반의 이동성 지원연구가 이루어져 왔다.

그러나 MIPv6나 HMIPv6를 이용한 이동성 지원 기법은 네트워크뿐만 아니라 클라이언트에도 이동성 지원을 위한 시스템이 추가되어야 하는 단점을 가지고 있다. IETF의 NetLMM(Network based Localized Mobility Management) 워킹그룹에서 이를 해결하기 위해 네트워크 기반의 이동성 지원 기법인 PMIPv6(Proxy Mobile IPv6)[4]가 제안되었다. PMIPv6는 MAG(Mobile Access Gateway)가 MN의 이동성 관리를 대신해주기 때문에, MN이 새로운 네트워크로 이동하였을 때 MN의 부담을 줄이고 핸드오버 지연시간을 줄일 수 있다. 그러나 PMIPv6는 기본적으로 MIPv6 의 동작을 따르기 때문에 MN의 핸드오버 동안 패킷손실이 일어나는 문제점이 있다.

PMIPv6의 문제점을 해결하기 위해서, IETF의 MIPSHOP 워킹그룹에서는 PMIPv6의 네트워크 기반의 이동성관리 프로토콜 기반에서 FMIPv6의 고속 핸드오버 기법을 접목한 FPMIPv6(Fast Handovers for Proxy MIPv6) [5]를 제안하여 표준화하였다. FPMIPv6는 기존의 PMIPv6에 FMIPv6를 적용하여 네트워크계층 아래의 하위 계층과 네트워크 계층의 연동을 통해 고속 핸드오버를 가능하게 해주는 방법이다. 이는 네트워크 기반의 이동성관리와 고속 핸드오버 기법을 사용함으로써 패킷손실을 줄일 수 있지만, RS(Router Solicitation)/RA(Router Advertisement) 및 PBU(Proxy Binding Update)/PBA(Proxy Binding Acknowledgement)의 보안취약성에 대한 조치가 필요하다. 기존 F-HMIPv6(Fast Handover for Hierarchical Mobile IPv6)에서는 RS/RA 및 PBU/PBA 메시지의 보안 취약성에 대해 MN의 인증 및 시그널 메시지를 안전하게 보호하기 위해 Kang-Park 프로토콜[6]과 CGA(Cryptographically Generated Address)에 기반한 ESS-FH를 제안하였다[7].

본 논문에서는 FPMIPv6기반의 핸드오버 과정에서 바인딩 갱신 과정에서 시그널링 메시지가 안전하게 보호되지 않는다면, MIPv6에서의 보안 위협과 마찬가지로 리다이렉트(Redirect) 공격과 DoS(Denial of Service) 공격 등 다양한 보안 위협에 노출시키는 결과를 초래하게 되므로 안전한 바인딩 갱신을 위하여 안전한 공개키 기반의 CGA 기법을 PMIPv6에 도입한다. CGA[8]는 제공되는 보안 강도가 높고 절차가 간단하지만 각 MN에서 처리해야 하는 암호학적 연산의 양이 많아지므로 일반적으로 성능이 낮은 MN에서는 적용하기 어렵기 때문에 네트워크기반의 이동성을 지원하는 FPMIPv6에 적용하기 위해 BAN로직를 통한 암호 프로토콜의 안전성에 대한 분석과 마코브 체인(Markov Chain)을 적용한 이동성 모델링을 통해 기존기법에 비해 향상된 이동성을 얻을 수 있음을 검증하여 이동 성능의 향상과 보안 문제를 해결하도록 한다.

본 논문의 구성을 다음과 같다. 제1장은 본 연구를 수행하게 된 배경과 목적을 살펴보고 본 연구 내용을 제시한다. 제2장은 관련연구로 제안 방안의 내용 이해를 돕기 위한 개념 및 동작 원리에 대해 살펴본다. 제3장은 본 논문이 제안하는 방안에 관하여 설명한다. 제4장은 제안하는 방법의 성능평가에 대하여 살펴보고자 한다. 제5장은 결론을 도출한다.

2. 관련 연구

2.1 PMIPv6(Proxy Mobile IPv6) 개요

PMIPv6는 네트워크 기반 이동성 지원 프로토콜로서 도메인을 관리하는 LMA(Local Mobility Anchor)와 MN의 이동을 감지하고 MN의 위치 정보를 등록하는 MAG로 구성된다. MN이 MAG에게 최초로 접속하게 되면, MAG는 MN로부터 MN-ID를 획득하여, MN의 인증을 위한 AAA (Authorization, Authentication and Accounting) 서버와 인증과정을 수행하고 LMA 주소와 이동성 지원에 필요한 정보를 획득한다. 이후 MAG는 LMA에게 PBU 메시지를 전송한다. PBU 메시지를 수신한 LMA는 MN만의 고유한 MN-HNP를 생성하고 BCE(Binding Cache Entry)에 MN의 정보를 추가한다. LMA는 MN-HNP를 PBA와 함께 MAG에게 전송하고 양방향 터널을 형성한다. MN은 MN-HNP를 이용하여 IP 주소를 생성하게 된다. 이후의 MN의 모든 패킷은 MAG와 LMA의 양방향 터널을 통해서 송수신 된다.

2.1.1 PMIPv6 주요 용어

- Local Mobility Anchor(LMA) : LMA는 PMIPv6 도메인에서 MN에 대한 일종의 HA(Home Agent) 역할을 한다. LMA는 도메인 내부에서 보통 게이트웨이 위치에 배치되고 HNP(Home Network Prefix)를 할당하고, 이를 MN에 보내주는 역할을 담당한다. LMA는 자신이 관리하는 도메인 내부의 모든 MN들의 주소와 위치정보를 유지하여 연결을 보장한다. 즉, LMA는 MN의 위치 정보를 관리한다. 도메인 외부에서 내부의 MN에 보내지는 패킷은 무조건 LMA가 받게 설계되어 있으며, 이 패킷을 MAG와의 터널링을 통하여 MN에게 보내지게 된다. 반대로 도메인 내부에서 외부로 보내지는 패킷들은 MAG에서 터널링하여 LMA로 전달되며 LMA가 외부로 전송하게 된다.
- Mobile Access Gateway(MAG) : MAG는 MN이 직접적으로 접속하는 AR이며, MN을 대신해서 이동성 지원 시그널링을 관리 수행을 한다. 또한, MAG는 MN의 네트워크에 대한 연결 기능과 라우팅 기능을 담당한다. MN이 해당 AR에 접속하면, 대신해서 MN의 정보를 이용하여 LMA와의 연결설정을 하고 LMA에서 온 패킷을 대신 받아 MN에게 전달한다. 그러므로 MAG는 인증된 노드여야 한다.

• LMA Address(LMAA) : LMA와 MAG간의 양방향 터널 형성에 사용되는 LMA의 전역 주소이며 MAG가 PBU(Proxy Binding Update) 메시지를 보낼 때 사용된다.

• Proxy Care-of Address(Proxy-CoA) : Proxy-CoA는 LMA와 MAG간의 터널에서 전송 시 사용되는 전역 주소이다. LMA는 서비스하려는 MN의 CoA를 보고 바인딩 캐시에 등록한다. MAG와 LMA 사이의 전송 계층이 IPv4네트워크이고 해당 CoA가 IPv4로 등록되었다면 IPv4 CoA를 사용한다.

• Mobile Node Home Network Prefix(MN-HNP) : MN-HNP는 MN과 MAG사이의 링크에 할당된 프리픽스이다. 하나 이상의 프리픽스는 MN과 MAG 사이의 링크 지정할 수 있으며, 이 경우 할당된 프리픽스를 이동성 세션처럼 관리한다. MN은 자신의 HNP로 부터 인터페이스와 하나 또는 여러 개의 주소를 구성한다. 만약 MN이 다수의 인터페이스들을 통해서 PMIPv6도메인에 연결 되었다면, 각 접속된 인터페이스들은 동시에 유일한 HNP를 할당 할 것이고, MN의 주어진 인터페이스에 할당된 모든 프리픽스를 하나의 이동성 세션에서 관리할 것이다.

• Mobile Mode Home Address(MN-HoA) : MN-HoA는 MN이 자신의 HNP로 생성한 주소이다. MN은 자신이 Proxy MIPv6도메인에 연결되는 동안까지 MN-HoA를 사용할 것이다. 만약 MN이 자신의 HNP로부터 생성된 하나 이상의 주소를 사용한다면, 그 주소들 중 하나는 MN의 홈 주소로 사용될 것이다. MIPv6와는 달리, PMIPv6에서 HA는 MN-HoA를 MN의 홈 주소로 생각한다.

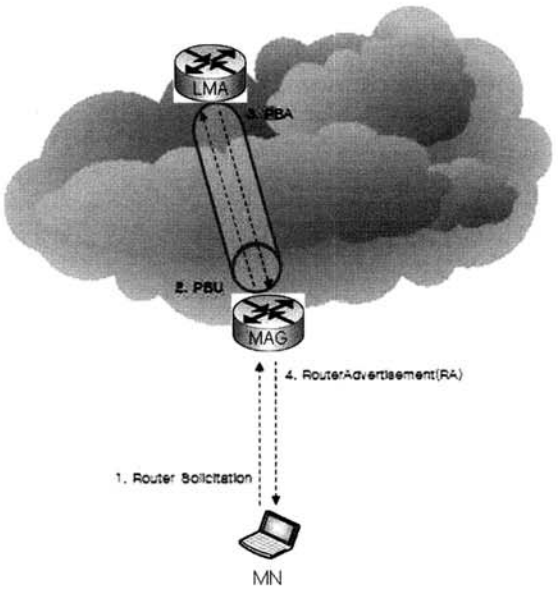
• Mobile Node Identifier(MN-Identifier) : PMIPv6의 도메인에서 MN의 식별자이며, 보통 NAI(Network Access Identifier) 또는 MAC address처럼 식별자 역할을 한다.

• Proxy Binding Update(PBU) : PBU는 MAG가 MN의 LMA에게 전송하는 요청 메시지로서, MN의 통신을 연결을 위해 MN의 HNP와 Proxy-CoA를 바인딩하여 전송된다.

• Proxy Binding Acknowledgement(PBA) : PBU 메시지에 대한 응답으로서, LMA가 MAG에게 전송하는 메시지이다.

2.1.2 PMIPv6 기본 동작

MN이 L2에 연결되어 MAG의 영역에 도달하면 MN은 새로운 네트워크의 MAG를 인식한다. MN은 자신의 MN-ID와 프로파일을 담은 RS 메시지를 MAG에게 전송하여 AAA인증을 수행한다. MAG는 프로파일에 포함된 LMA의 주소로 PBU 메시지를 담아서 보냄으로써 MN의 현재위치를 갱신한다. PBU 메시지를 받은 LMA는 자신의 BCE에 MN-ID에 해당되는 정보가 있는지 검사하게 되고, 없다면 해당 정보를 추가하며, 있을 경우에는 기존의 정보를 갱신한다. 이 과정이 끝난 후 LMA는 MAG에 PBA 메시지를 보내게 된다. 그리고 LMA는 MAG의 주소를 이용하여 LMA와 MAG간의 양방향 터널을 형성하고 통신을 준비한다. LMA로부터 응답을 받은 MAG는 자신에게 접속된 MN에게 LMA가 할당해준 HNP와 IP 주소를 할당하는 RA 메시지를 보낸다. Neighbor Discovery 프로토콜에서는 RA 메시지를 멀티캐스트 하도록 되어 있지만, PMIPv6에서는 MN마다 고유한 프리픽스가 할당되어야 하기 때문에 RA 메시지가 유니캐스트로 전달되어야 한다[9]. RA 메시지를 받은 MN은 정책 프로파일(Policy Profile)에서 정의된 주소 설정 방법에 따라 RA 메시지에 포함된 MN-HNP를 이용하여 자신의 HoA를 생성한다. 연결설정이 완료되면, MAG는 해당 MN에게서 오는 모든 데이터를 LMA와 연결된 터널을 이용하여 LMA에게 전송한다. LMA는 외부에서 오는 모든 데이터를 해당 MN을 관리하는 MAG에게 전송하고, MAG는 받은 데이터를 MN에게 전송해 준다. 이후 MN은 PMIPv6 도메인 내에서 이동성을 제공받는다. (그림 1)에서는 PMIPv6의 기본 수행 동작을 보여주고 있다.



(그림 1) ProxyMIPv6의 기본 동작

2.2 FPMIPv6(Fast Handovers for Proxy Mobile IPv6) 개요

PMIPv6는 이동성관리를 제외한 MIPv6의 수행과정을 동일하게 수행하므로, MN이 PMIPv6 도메인으로 진입할 때마다 MAG가 MN의 진입을 감지하여 LMA에게 자신의 위치정보를 알리는 핸드오버 과정을 거쳐야 한다. 핸드오버 과정을 거치는 동안, MN과의 통신이 끊어지기 때문에 패킷 손실이 발생한다. 이러한 패킷 손실을 막기 위해서 IETF에서는 FPMIPv6를 제안하여 표준화하였다. FPMIPv6는 PMIPv6 환경에서 FMIPv6의 고속 핸드오버 기법을 적용하였으며, MN이 이동하기 전에 이동을 감지하여 이전의 MAG(pMAG)가 새로운 MAG(nMAG)에게 MN의 정보를 전송하하기 위해 HI(Handover Initiate)와 HAck(Handover Acknowledge) 메시지를 사용하여 이동을 알린다.

이 과정에서 pMAG와 nMAG 사이에 터널이 형성되고, MN과 통신이 끊기는 동안에 LMA로부터 오는 데이터를 nMAG가 버퍼링한다. MN이 nMAG에게 접속하여 통신이 연결되면 nMAG가 버퍼링 했던 데이터를 MN에게 전송함으로써 패킷 손실에 대한 피해를 줄이게 된다. 앞에서 언급

했듯이 MN에 직접적으로 IP 이동성 프로토콜 동작을 추가할 수 없으므로, FMIPv6에서 사용되던 RS, RA, FBU (Fast Binding Update), FBAck (Fast Binding Acknowledgement), UNA (Unsolicited Neighbor Advertisement) 메시지 등은 사용되지 않는다.

2.2.1 FPMIPv6 주요 용어

- Access Network(AN)

AN은 AP(Access Point)와 같이 링크 계층의 연결 장치들 또는 AR(Access Router)와 연결성을 제공하는 네트워크 장비

- Previous Access Network(p-AN)

핸드오버 이전에 MN이 접속했던 이전의 AN

- New Access Network(n-AN)

핸드오버 이후에 MN이 접속한 새로운 AN

- Previous Mobile Access Gateway(pMAG)

핸드오버가 일어나기 전에 MN의 시그널링 관련 이동성을 관리 해주는 MAG

- New Mobile Access Gateway(nMAG)

핸드오버가 일어난 후 MN의 시그널링 관련 이동성을 관리해주는 MAG

- Report 메시지

MN이 자신과 연결된 AN에게 주기적으로 전송하는 메시지

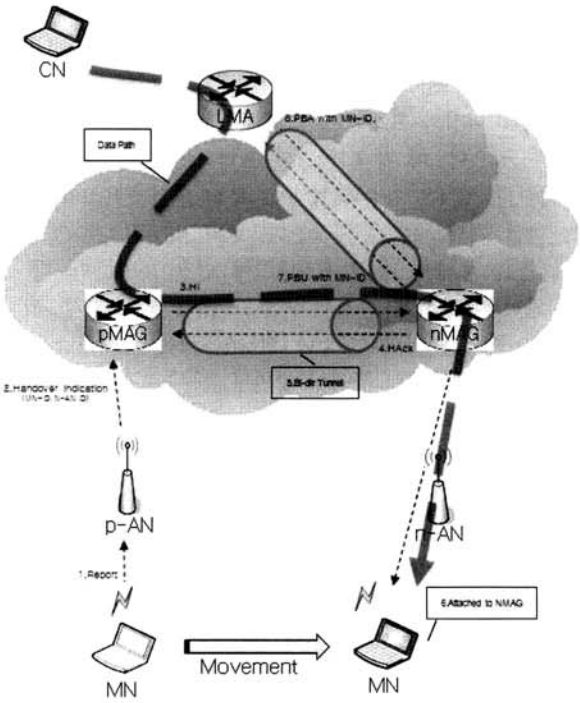
- Handover indication(HI) 메시지

MN의 핸드오버를 나타내는 시그널링 메시지, HI은 p-AN이 MN의 이동을 감지하여 pMAG에게 전송

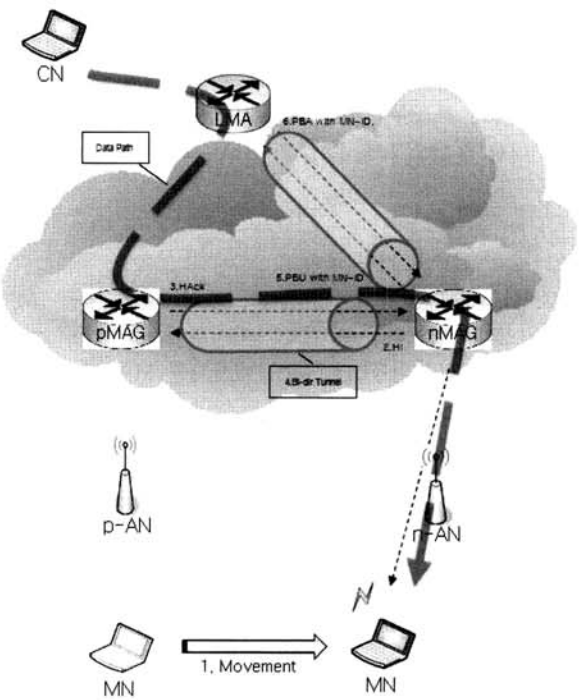
2.2.2 FPMIPv6의 기본 동작

FPMIPv6는 FMIPv6와 같이 두 가지 모드로 나뉘어 수행되며, Predictive 모드와 Reactive 모드가 있다. (그림 2)는 Predictive 모드의 메시지 흐름을 나타내고 있다. Predictive 모드는 MN이 nMAG로 이동하기 전에 pMAG와 nMAG 사이에 양방향 터널이 형성되는 모드이다. 따라서 MN이 이동하기 전에 p-AN에게 이동이 예측되는 n-AN의 정보와 MN의 정보(MN-ID)를 포함한 Report메시지를 전송한다. Report메시지를 받은 p-AN은 pMAG에게 MN-ID와 n-AN ID를 포함한 HI 메시지를 전송하여 MN의 이동을 알린다. pMAG는 MN의 정보와 LMAA를 담은 HI메시지를 nMAG에게 전송한다. HI메시지를 받은 nMAG는 응답으로 HAck 메시지를 pMAG에게 전송한다. pMAG가 HAck메시지를 받은 후, pMAG와 nMAG 사이의 양방향 터널이 형성된다. 양방향 터널이 형성된 시점부터 pMAG는 LMA가 MN에게 전송한 패킷들을 nMAG에게 전송하며, nMAG는 pMAG에게 전송받은 패킷들을 버퍼링하여 저장한다. MN의 L2 핸드오버가 끝난 후 nMAG에게 연결이 되면 nMAG는 저장했던 패킷들을 MN에게 전송하고, LMA에게 MN의 바인딩을 위해 PBA 메시지를 전송한다. LMA는 PBU 메시지를 받은 후 BCE에 MN에 대한 상태 정보를 등록하고 PBA 메시지를 nMAG에게 전송한다. MN은 nMAG가 LMA에게 PBA 메시지를 응답 받음으로서 바인딩 과정을 완료한다. 이후 MN로 전송되는 패킷들은 nMAG를 통해서 전송하게 된다.

Reactive 모드는 MN이 nMAG로 이동한 후에 pMAG와 nMAG 사이에 양방향 터널이 형성되는 모드이다. 따라서 MN이 nMAG로 빠르게 이동하여 Predictive 모드가 실패하고 nMAG에게 연결되었을 때 수행하며, nMAG는 HI메시지



(그림 2) FPMIPv6 Predictive 모드의 메시지 흐름



(그림 3) FPMIPv6 Reactive 모드의 메시지 흐름

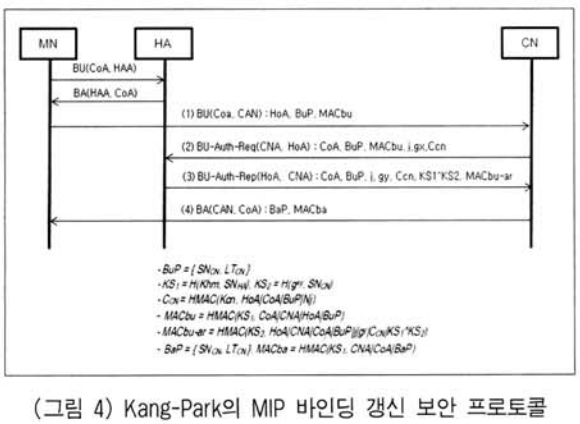
를 pMAG에게 전송하고, HI 메시지를 받은 pMAG는 응답으로 HAck 메시지를 nMAG에게 전송한다. Predictive 모드와 동일하게 pMAG와 nMAG 사이에 양방향 터널이 형성되고, nMAG는 MN의 패킷들을 버퍼링하여 저장한다. 또한, nMAG는 LMA에게 MN의 바인딩을 위해 PBU 메시지를 보낸다. LMA는 PBA 메시지를 nMAG에게 전송하여 바인딩 과정을 완료한다. 그림 3는 Reactive 모드의 메시지 흐름을 나타낸다.

2.3 Kang-Park 기법

MIPv6는 IPv6 네트워크 환경의 구성 MN이 움직임과 위치에 상관없이 지속적인 통신을 할 수 있도록 이동성을 제공하는 프로토콜이다. 이를 위해 MIPv6는 각각의 MN에게 두 개의 주소 HoA와 CoA를 부여하고 MN의 HA로 하여금 MN을 위한 데이터 패킷을 중계 하도록 한다. 그러나 이러한 삼각 라우팅 방식은 MN과 CN 사이의 모든 통신이 항상 HA를 통하여 이루어지기 때문에 비효율적이다.

따라서 MIPv6는 MN과 CN이 직접 통신을 할 수 있도록 경로 최적화(RO: Route Optimization) 모드를 지원한다. 이처럼 RO 모드에 의해 삼각 라우팅 문제가 해결되고 효율적인 통신이 가능해 졌으나 그에 상응하는 새로운 보안 위협이 대두되었다. 즉, RO 모드의 적용을 위해 MN가 위치 변경할 때 마다 외부 네트워크에서 할당된 새로운 CoA를 HA와 CN에게 알리는 바인딩 갱신(Binding Update)을 수행해야 하는데 바인딩 갱신 과정이 안전하게 보호되지 않는다면 RO 모드는 구성 요소 모두를 다양한 보안 위협에 노출시키는 결과를 초래한다. 안전한 바인딩갱신을 위하여 MIPv6는 주소 테스트 기반의 경량화 된 암호화 연산을 제공하는 RR(Return Routability) 프로토콜을 표준안으로 채택하였다.

그러나 RR 프로토콜이 효율성과 보안성에 있어서 한계를 드러냄에 따라 이를 개선하기 위하여 다양한 공개키 기반의 프로토콜들이 제안 되었으며, 그 결과 OMIPv6(Optimized MIPv6) 프로토콜이 RR 프로토콜의 최적화 옵션의 하나로서 표준화 되었다[10]. 이러한 공개 키 기반 프로토콜 중에서 2005년도에 강현선과 박창섭이 제안한 프로토콜은 HA 중심의 독창적인 보안 프록시 구조를 바탕으로 MN의 연산 부담을 최소화함과 동시에 보안성 강화하였다[6].



(그림 4) Kang-Park의 MIP 바인딩 갱신 보안 프로토콜

- Msg(SA, DA) : 프로토콜 메시지를 나타내며 Msg는 메시지의 이름이고 SA는 메시지의 송신자 주소, DA는 수신자 주소를 나타냄
- H(msg) : msg의 해쉬값을 계산하는 일방향 해쉬 함수를 의미함
- HMAC(k, msg) : 대칭키 k를 통해 msg의 HMAC 값을 계산하는 HMAC 함수를 의미함
- | : 메시지 결합 연산자, ^ : 배타적 논리합 연산자
- MN : MN, HA: HA, CN: CN
- CNA : CN의 주소, HAA: HA의 주소
- SNx : X에게로 보내는 메시지의 일련번호, LTx: X의 바인딩 정보의 생명주기
- (H-1)과 (H-2)는 홈 등록 과정을 나타냄
- Khm : HA와 MN 사이의 공유 대칭키
- gx, x : 각각 CN의 Diffie-Hellman 공개키와 개인키를 의미함
- gy, y : 각각 MN의 Diffie-Hellman 공개키와 개인키를 의미함
- Kcn : CN의 비밀키, KHA : HA의 비밀키
- Nj: CN의 j 번째 nonce값을 의미함

2.4 ESS-FHMIPv6 기법

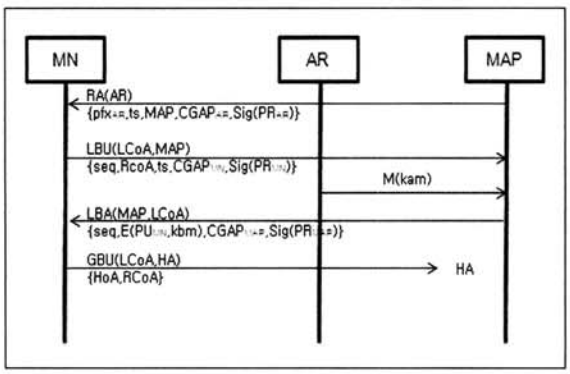
FH-HMIPv6는 MAP 등록 단계와 고속 핸드오버 단계로 구성된다. MAP 등록단계는 MN이 새로운 MAP (Mobility Anchor Point) 도메인으로 이동할 때, MN과 MAP 사이에서 발생한다. 접속 라우터는 프리픽스 정보를 광고한다. 프리픽스 정보를 수신한 MN은 MAP 도메인상의 RCoA (Regional CoA)와 접속라우터의 서브넷상의 LCoA(on-Link CoA)를 생성한다. MN과 MAP은 LBU 메시지와 LBA 메시지를 주고받고, MAP은 두 개의 CoA 주소를 BCE에 저장한다. 이 때, MN의 HoA로 예정된 패킷들을 현재 위치인 RCoA로 전달을 요청하기 위하여, MN은 HA에게 메시지를 전송한다. MN로 전달해야 할 패킷을 수신한 HA는 RCoA로 패킷을 전송하므로 MAP이 수신한다. 전달해야 할 패킷을 수신한 MAP는 MN의 현재 위치인 LCoA로 패킷을 전달한다.

반면에, MN이 다른 MAP 도메인에서 이동한 것이 아니라, 한 개의 로컬 MAP 도메인 내에서 접속라우터 AR에서 다른 접속 라우터 nAR로 이동한다면, 고속 핸드오버단계는 시작된다. 이때에는 RCoA가 변경 되지 않았으므로, 새로운 LCoA를 등록하기 위하여 MN과 MAP 사이에서 LBU메시지와 LBA메시지만 전송한다. MAP 등록단계에서는 RA 메시지, LBU 메시지, LBA 메시지인 3개의 시그널링 메시지들로 구성된다. CGA 기법을 이용하여 3개의 시그널링을 보호하는 방법을 제안하였다[7]. X의 인터페이스 식별자(Interface Identifier)인 IIDx는 H64(pfxAR, CGAx)로부터 만들어지고, X의 IPv6주소 CGA는 pfxAR||IIDX 이다. 여기서, X가 속해있는 접속 라우터 AR의 프리픽스인 pfxAR와 CGAPx = {modifierX, Collision_countX, PUx}는 CGA를 생성하기 위한 파라미터들 이다. 수식을 간단하게 하기 위하여 modifierX와 collision_countX는 본 논문의 설명에 다시

나오지 않으므로, 더 이상 사용하지 않고 CGAPx는 PUx를 대신하여 표현한다. 즉 IIDx = H64(pfxAR, CGAPx)를 IIDx = H64(pfxAR, PUx)로 나타낸다. X의 의해서 전송된 메시지들은 공개키 PUx와 개인키 PRx 로서명 된 메시지를 같이 보냄으로서 보호된다. 서명확인은 공개키 PUx를 사용하여 이뤄진다. 접속 라우터 AR과 MAP의 프리픽스는 각각 pfxAR, pfxMAP으로 나타낼 때, MN의 LCoA와 RCoA, AR과 MAP은 다음과 같이 계산된다.

LCoA = pfxAR||H64(pfxAR,PUMN)
RCoA = pfxMAP||H64(pfxMAP,PUMN)
AR = pfxAR||H64(pfxAR,PUAR)
MAP = pfxMAP||H64(pfxMAP,PUMAP)

MAP 등록 단계는 아래그림과 같고, 전송되는 시그널링 메시지는 CGA에 기반한 전자서명으로 보호된다. MN이 RA 메시지를 수신하면 MN은 먼저 AR이 pfxAR과 PUAR으로부터 생성된 유효한 CGA가 맞는지 CGA 검증을 하고, 공개키 PUAR을 이용하여 Sig(PRAR)의 서명 검증을 한다. 두 개의 검증이 성공하면, MN은 타임스탬프(ts)로 동기화 시키고, RA 메시지에 있는 서브넷 프리픽스 정보를 기반으로 하여 LCoA와 RCoA를 생성한다. LBU 메시지와 LBA메시지도 CGA 검증과 서명 검증을 사용하고, 순차번호(seq)도 함께 전송한다. LBU 메시지의 검증이 성공하면, MAP의 바인딩 캐시에 RCoA와 LCoA를 등록한다. LBU 메시지가 MAP으로 전송될 때, AR도 MAP에게 M(Kam)을 보낸다. M(Kam) = {LBU, HMAC(Kam)} 이다. Kam은 AR과 MAP 사이에서 미리 생성된 비밀키이다. MAP는 수신한 LBU 메시지와 미리 공유한 Kam을 가지고 M(Kam)을 계산하고, 확인하여 수신한 MN이 실제로 AR의 서브넷에 있는 것인



(그림 5) You-Lee-Sakurai-Hori 기법

* PUX, PRX : MN X의 공개키, 개인키 쌍
* H64() : 해쉬함수 SHA-1 결과의 왼쪽으로부터 64비트
* HMAC(K) : 키 K를 이용한 메시지 인증 코드
* Sig(PRX) : 개인키 PRX에 기반한 전자서명
  Sigx = S(PRx, x)
* E(K,m) : 메시지 m을 키 K로 암호화
* Msg(S,D){list} : 소스 IPv6 주소 S로부터 목적지 IPv6 주소 D로 전송되는 시그널링 메시지, list는 Msg를 보호하는 역할을 함

지를 확인 할 수 있다. MN 또한 CGA 검증과, 서명 검증을 통하여 LBA메시지 검증이 성공하면, 현재의 위치인 RCoA를 알리기 위하여 HA에게 GBU(Global Binding Update)메시지를 전송한다. 암호화키 'Kbm'은 MN로 전송되고 고속 핸드오버 단계에서 사용된다.

3. 제안기법

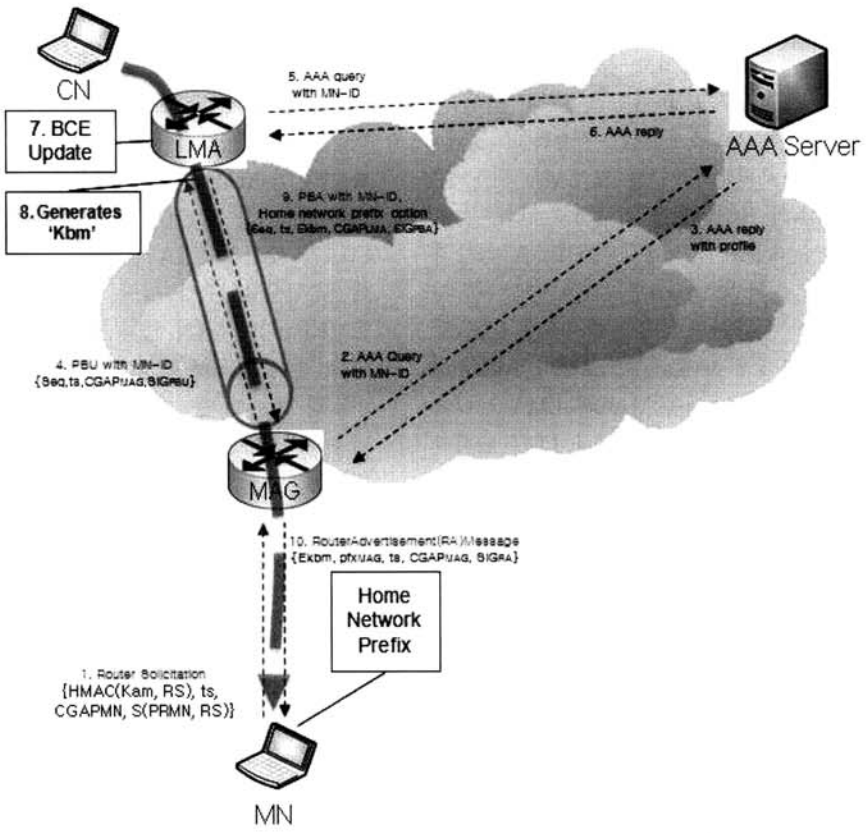
이번 장에서는 관련 연구에서 분석한 내용을 기반으로 CGA 기반에 FPMIPv6의 보안 향상 방안을 제안한다.

3.1 제안 방법의 개요

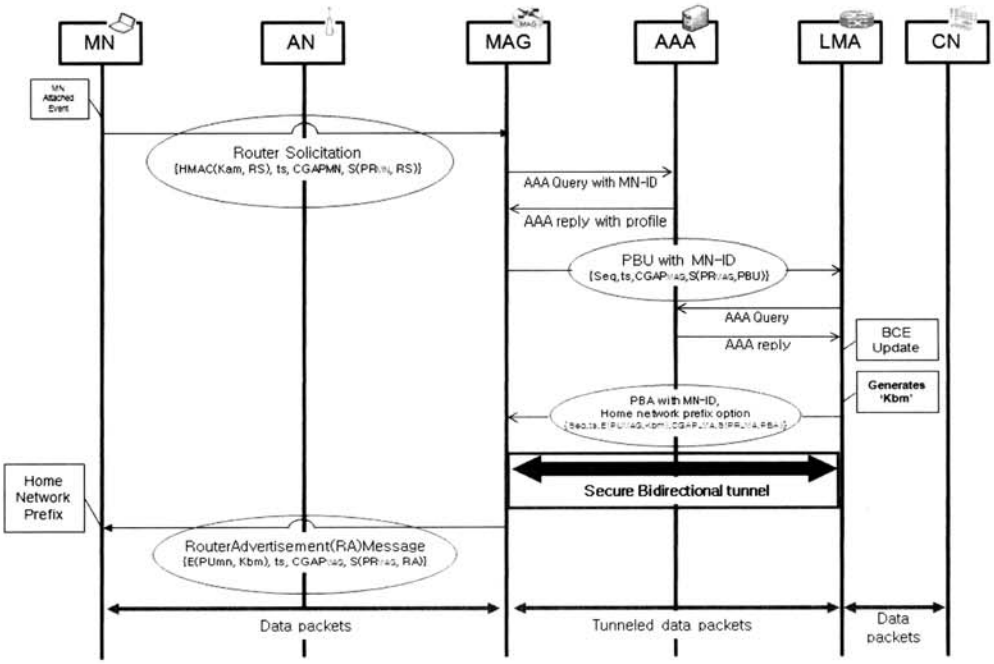
PMIPv6/FPMIPv6기반의 핸드오버 과정에서 바인딩 갱신 과정에서 시그널링 메시지들에는 인증 메커니즘이 포함 되어야 한다. 그렇지 않을 경우, 리다이렉트(redirect) 공격과 DoS 공격 및 중간자 공격(MITM, man- in-the-middle)이 발생할 수 있다[6][7]. FPMIPv6 기반에서 AAA인증 프로토콜이 사용되고 있지만, MN과 MAG 간의 시그널링 메시지가 보호되지 않는 단점이 있으므로 MN과 MAG, MAG과 LMA 간의 SA(Security Association)를 생성하기 위한 메시지 구성을 재정립 하여 높은 보안성을 제공한다. 또한 PMIPv6 기반에서 도메인간의 고속 핸드오버 기법도 제안한다.

3.2 제안 방법의 수행 과정

제안한 방법은 네트워크 기반의 이동성 지원 기술인 PMIPv6/FPMIPv6와 AAA의 인증 프로토콜과 CGA 기법을 연동하여 수행한다. 전송되는 시그널링 메시지는 CGA에 기반한 전자서명으로 보호된다. MN이 RA 메시지를 수신하면, MN은 먼저 MAG의 pfxMAG와 PUMAG 로부터 생성된 유효한 CGA가 맞는지 CGA 검증을 하고, 공개키 MAG을 이용하여 Sig(PRMAG)의 서명 검증을 한다. 두 개의 검증이 성공하면, MN은 타임스탬프(ts)로 동기화 시키고, RA메시지에 있는 HNP를 이용하여 IP를 설정한다. PBU 메시지와 PBA 메시지에서도 CGA 검증과 서명 검증을 사용하고, 순차번호(seq)도 함께 전송한다. PBU메시지의 검증이 성공하면, LMA의 BCE에 MN-ID 등록한다. PBU메시지가 LMA으로 전송될 때, MAG도 LMA에게 M(Kam)을 보낸다. M(Kam) = {PBU, HMAC(Kam)}이다. Kam은 MAG과 LMA 사이에서 미리 생성된 비밀키이다. LMA는 수신한 PBU 메시지와 미리 공유한 Kam을 가지고 M(Kam)을 계산하고, 확인하여 수신한 MN이 실제로 MAG의 서브넷에 있는 것인지를 확인 할 수 있다. MAG 또한 CGA 검증과, 서명 검증을 통하여 PBA 메시지 검증이 성공하면 터널 형성 후 데이터를 전송한다. 암호화키 'Kbm'은, MAG로 전송되고 고속 핸드오버 단계에서 사용된다. 제안된 PMIPv6/FPMIPv6와 AAA프로토콜 및 CGA 연동은 초기접속과 핸드오버 인증과정으로 나누어 수행한다. 초기접속 인증과정에서는 RS/RA 메시지, PBU 메시지, PBA 메시지에 대한 시그널링를 보호한다.



(그림 6) 제안기법의 초기접속 절차



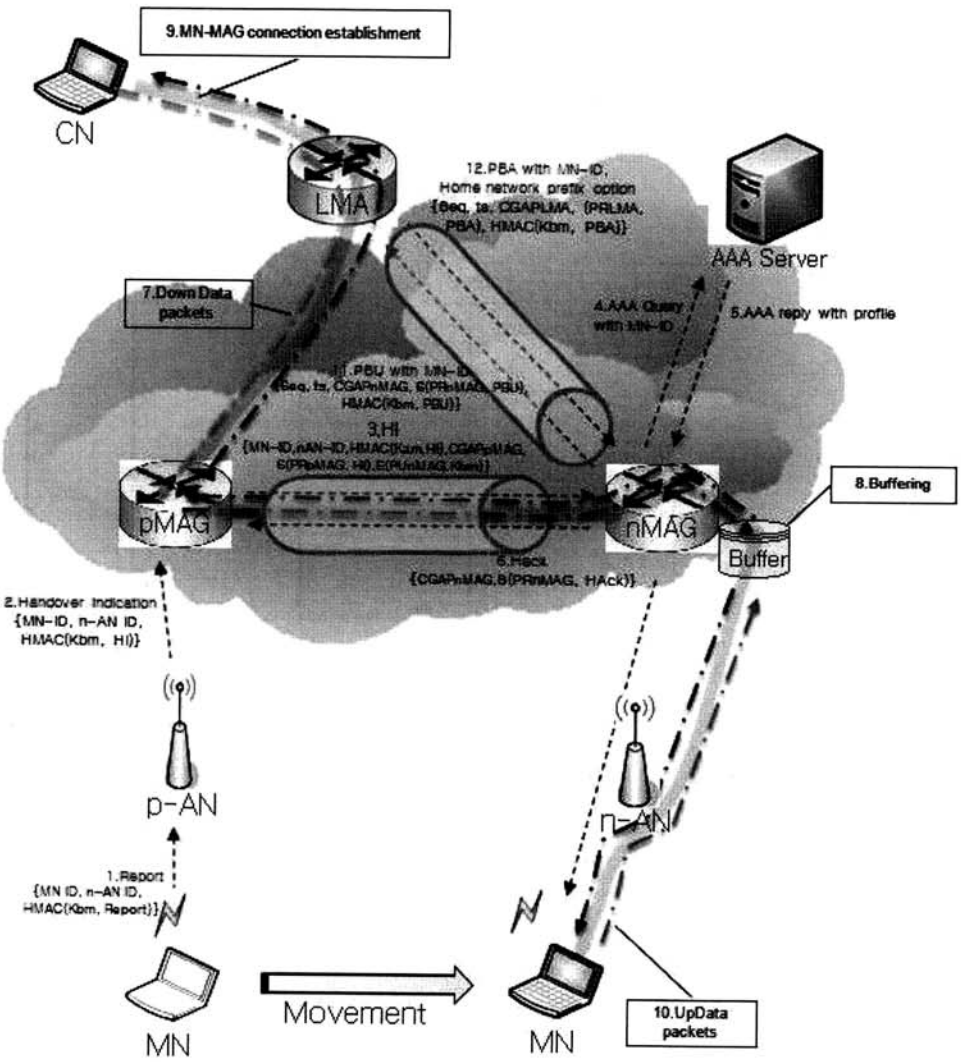
(그림 7) 제안한 방법의 초기접속 절차 메시지 흐름

초기접속 인증과정은 (그림 6)에서처럼, MN Attached Event를 통해 RS{HMAC(Kam, RS), ts, IIDMN, CGAPMN, S(PRMN, RS)} 메시지를 MAG에 전송하면서 시작된다. 이 때, MN과 MAG간에 신뢰관계 수립할 때 설정한 비밀키 kam를 통해 HMAC(Kam, PBU)를 보냄으로써, RS가 자신의 네트워크로 부터 전송되었음을 증명하며, 타임스탬프(ts)

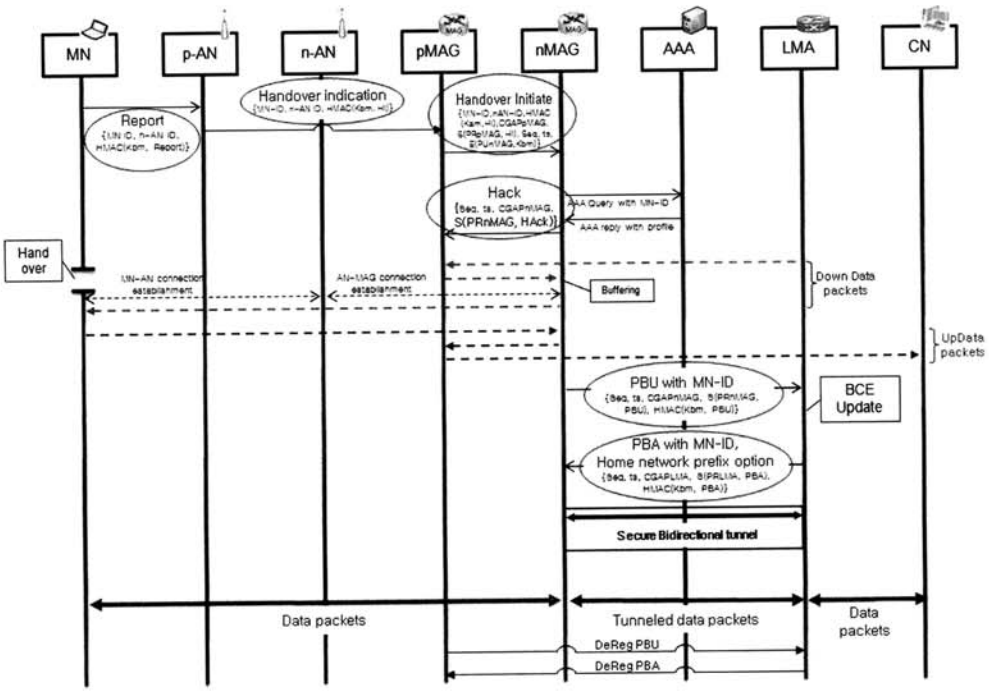
를 통해 현재 시간기준으로 적절한 범위 내에 있는지 확인하여 서비스 거부 공격를 차단할 수 있다. 또한, CGA 기법을 적용하여 MN의 공개키를 인증하고 성공시 전자서명을 검증함으로써 인증과정을 마무리 한다. 검증 후 MAG는 AAA Query메시지를 AAA인증서버로 전송하고 AAA Reply 메시지를 수신함으로써 MN 인증 및 LMA 주소, 주소설정 정책과 같은 MN의 프로파일을 획득하게 된다.

그 후 MAG는 MN 대신 PBU 메시지를 CGA 검증과 서명 검증을 사용하여 순차번호(seq)도 LMA에게 전송하고, PBU 메시지 검증이 성공하면, PBU 메시지가 LMA로 전송될 때, MAG도 LMA에게 M(Kam)을 보낸다. M(Kam) = {PBU, HMAC(Kam)}이다. Kam은 MAG과 LMA 사이에서 미리 생성된 비밀키이다. LMA는 수신한 PBU 메시지와 미리 공유한 Kam을 가지고 M(Kam)을 계산하고, 확인하여 수신한 MN이 실제로 MAG의 서브넷에 있는 것인지를 확인할 수 있다. LMA는 AAA Query/Reply 메시지 교환을 통해 MAG와 인증과정을 거치고, 인증과정이 완료되면 해당 MN에 대하여 새로운 HNP를 할당하고 관련 BCE 정보를 등록하고 고속 핸드오버 단계에서 사용될 'Kbm'를 생성한다. MAG 또한 CGA 검증과, 서명 검증을 통하여 PBA메시지 검증이 성공하면 MAG와 LMA간의 양방향 터널 형성으로 바인딩 절차는 완료하게 된다. 'Kbm'은 MAG의 공개키로 암호화하여 PBA에 포함되어 보내진다. PBA를 수신한 MAG는 MN에게 RA 메시지를 송신하며, MN은 먼저 MAG의 pfxMAG와 PUMAG 로부터 생성된 유효한 CGA가 맞는지 CGA 검증을 하고, 공개키 MAG을 이용하여 Sig(PRMAG)의 서명 검증을 한다. RA 메시지 안에서도 'Kbm'은 MN의 공개키로 암호화하여 보내진다. 두 개의 검증이 성공하면, MN은 재생공격에 대응하기 위해 타임스탬프(ts)로 동기화 시키고, RA 메시지에 있는 HNP를 이용하여 IP를 설정하고 이를 통해 CN와 통신할 수 있게 된다.

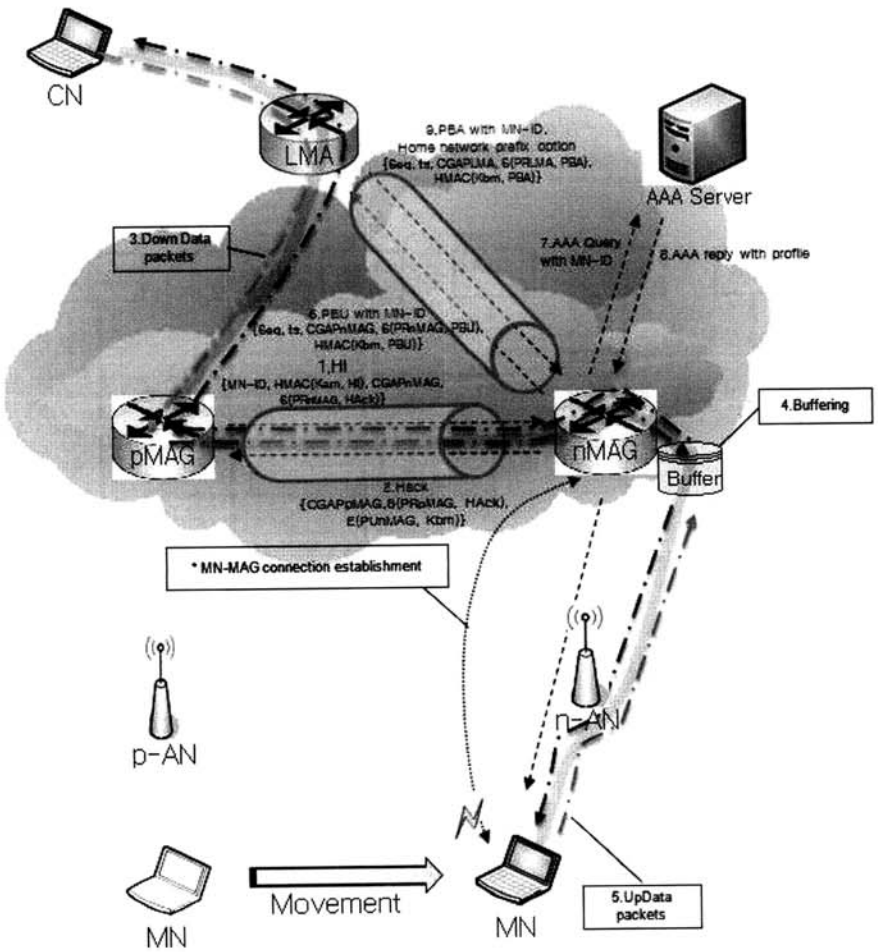
도메인 내 핸드오버 중 MN이 nMAG로 이동하기 전에 pMAG와 nMAG 사이에 양방향 터널이 형성되는 Predictive 모드에 대한 인증과정은 (그림 8)와 같이 수행되며, MN와 LMA간의 6개의 시그널링 메시지를 보호한다.



(그림 8) 제안기법의 도메인 내 핸드오버에서 Predictive 모드 구조



(그림 9) 제안기법의 도메인 내 핸드오버에서 Predictive 모드 메시지 흐름



(그림 10) 제안기법의 도메인 내 핸드오버에서 Reactive 모드 구조

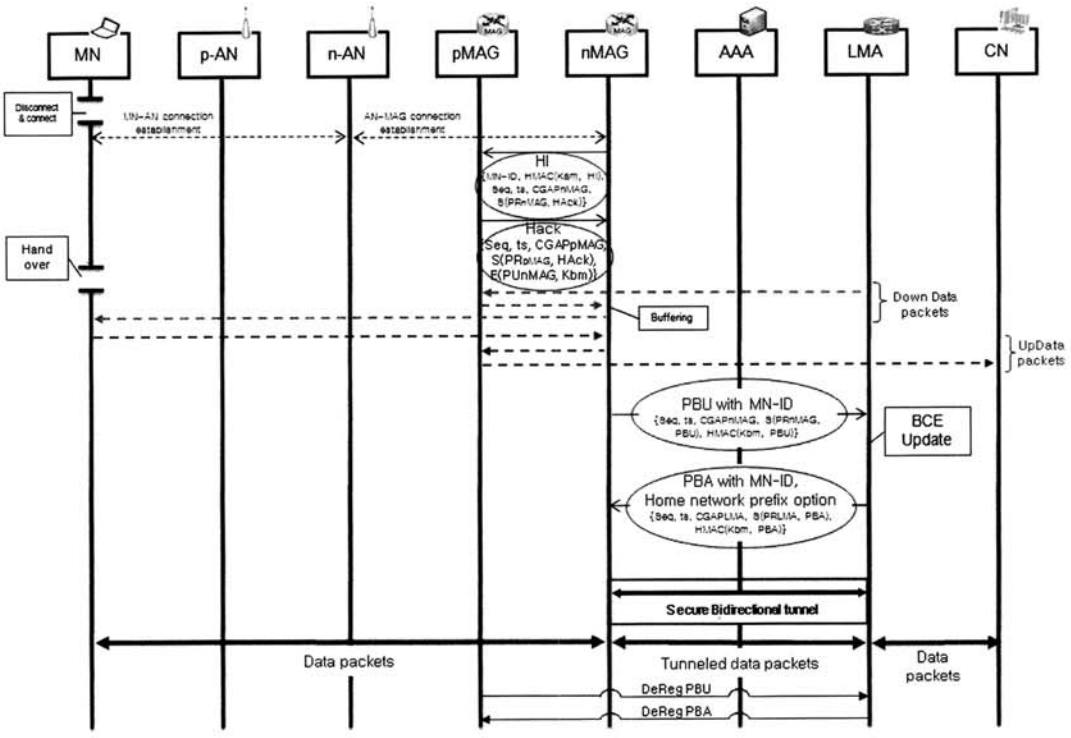
MN이 이동하기 전 p-AN에게 이동이 예측되는 n-AN의 정보와 MN의 정보(MN-ID)를 포함한 Report{MN ID, n-AN ID, HMAC(Kbm, Report)} 메시지를 전송한다. Report 메시지를 받은 p-AN은 pMAG에게 MN-ID와 n-AN ID를 포함한 HI{MN-ID, n-AN ID, HMAC(Kbm, HI)} 메시지를 전송하며, pMAG는 MN의 정보와 LMAA를 담은 HI{MN-ID, n-AN ID, HMAC(Kam, HI), EKbm} 메시지를 nMAG에게 전송한다. nMAG는 MN를 인증하기 위해 AAA에 MN의 인증요청을 보내고 응답 수신 후 인증 성공시, HI 메시지를 받은 nMAG는 응답으로 SigHAck = S(PRnMAG, HAck) 메시지를 pMAG에게 전송하게 된다. pMAG가 HAck 메시지를 받은 후, pMAG와 nMAG 사이의 양방향 터널이 형성 후 형성 된 시점부터 pMAG는 LMA가 MN에게 전송한 패킷들을 nMAG에게 전송하게 된다. nMAG는 pMAG에게 전송받은 패킷들을 버퍼링하여 저장하며, MN의 L2 핸드오버가 끝난 후 nMAG에게 연결이 되면 nMAG는 저장했던 패킷들을 MN에게 전송하게 된다. nMAG는 LMA에게 MN의 바인딩을 위해 초기인증과정에서 생성하여 pMAG에게 전송받은 'Kbm' Key를 이용하여 PBU{Seq, HMAC(Kbm, PBU)} 메시지를 전송하고 LMA는 PBU 메시지를 받은 후 BCE에 MN에 대한 상태 정보를 등록하고 PBA{Seq, HMAC(Kbm, PBA)} 메시지를 nMAG에게 전송한다. nMAG는 LMA에게 PBA 메시지를 응답 받고 바인딩 과정 완료 후 MN으로 전송되는 패킷들은 nMAG를 통해서 전송 되게 된다. (그림 9)에서는 제안한 방법의 도메인 내 핸드오버 Predictive 모드 메시지 흐름을 보여주고 있다.

도메인 내 핸드오버 중 MN가 nMAG로 이동한 후에 pMAG와 nMAG 사이에 양방향 터널이 형성되는Reactive 모드에 대한 인증과정은 (그림 10)와 같이 수행된다.

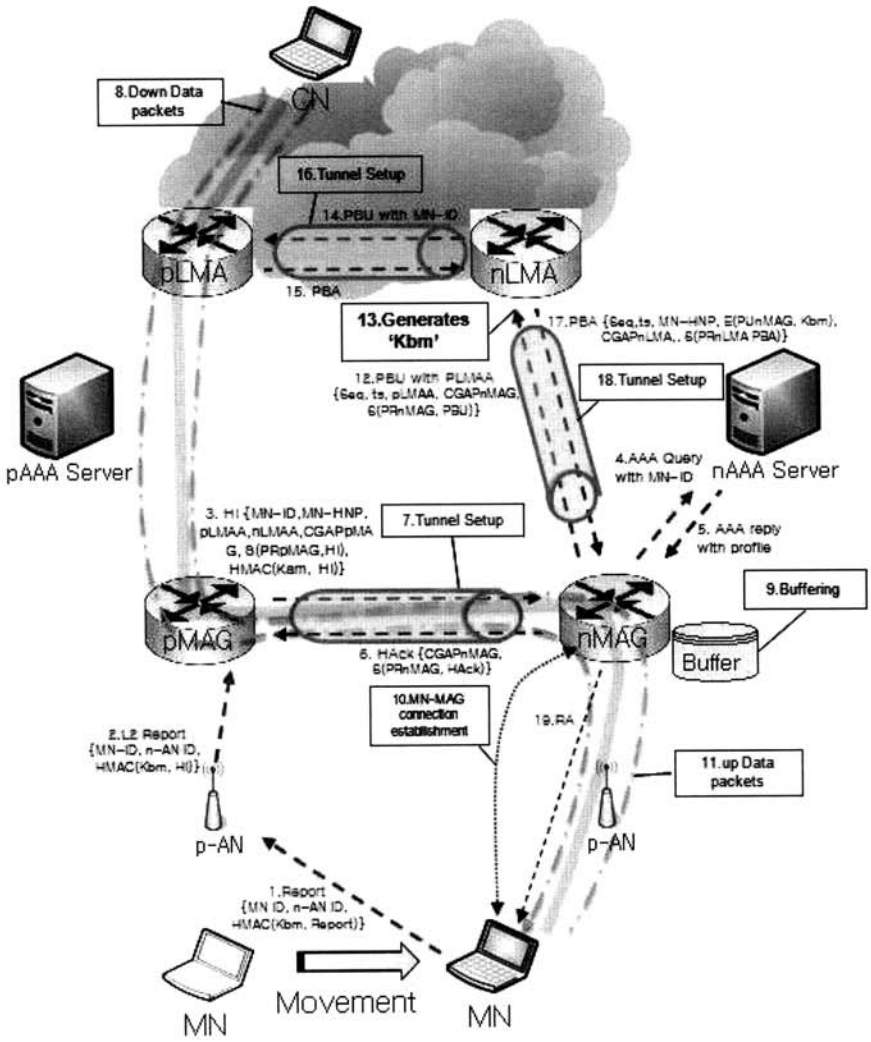
MN가 nMAG로 빠르게 이동하여 Predictive 모드가 실패하고 nMAG에게 연결되었을때 수행하며, nMAG는 HI{MN-ID, HMAC(Kam, HI)}메시지를 pMAG에게 전송한다. HI메시지를 받은 pMAG는 응답으로 HAck{Sig -HAck, E(PUnMAG, Kbm)} 메시지를 nMAG에게 보내고, pMAG와 nMAG 사이에 양방향 터널을 형성한다. nMAG는 MN의 패킷들을 버퍼링하여 저장하고 nMAG는 LMA에게 MN의 바인딩을 위해 PBU{Seq, ts, S(PR- nMAG, PBU), HMAC(Kbm, PBU)} 메시지를 전송한다. nMAG가 LMA에게 PBA{Seq, ts, S(PRLMA, PBA), HMAC(Kbm, PBA)} 메시지를 응답 받고 바인딩 과정 완료 후 바인딩 완료 후 MN으로 전송되는 패킷들은 nMAG를 통해서 전송 된다. (그림 11)에서는 제안한 방법의 도메인 내 핸드오버 Reactive 모드 메시지 흐름을 보여주고 있다.

PMIPv6에서는 도메인 간 핸드오버를 지원하지 않으므로, 본 논문에서 도메인 간 핸드오버를 (그림 12)와 같이 제안한다.

도메인 간 핸드오버 절차는 L2 Report{MN ID, n-AN ID, HMAC(Kbm, Report)}를 통해 이동하려는 MN- ID와 AP-ID 수신 한 후 pMAG는 자신이 가지고 있는 정보를 검색하여 AP-ID와 바인딩된 엔트리에 MN이 새로운 도메인에서 서비스 받을 nLMA 주소가 존재 한다면, pMAG는 nMAG에게 MN-ID, MN-HNP, pLMAA 그리고 nLMAA를



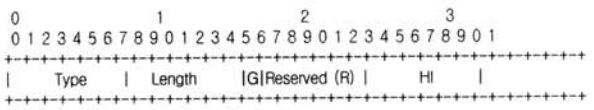
(그림 11) 제안기법의 도메인 내 핸드오버에서 Reactive 모드 메시지 흐름



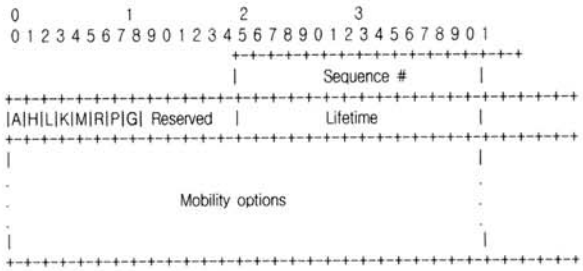
(그림 12) 제안기법의 도메인 간의 핸드오버 구조

담은 HI{MN-ID, MN-HNP, pLMAA, nLMAA, S(PRpMAG, HI), HMAC(Kam, HI)} 메시지를 보낸다. 이때 HI메시지의 예약되어 있는 비트중 하나를 아래 (그림 13)같이 G flag(도메인의 외부를 나타내는 플래그)로 사용하여 도메인 간 핸드오버임을 값을 1로 설정함으로써 알린다. G flag가 1로 설정 된 HI 메시지를 받은 nMAG는 HAck{MN-ID, S(PRnMAG, HAck)} 메시지로 응답하여 pMAG와 양방향 터널을 형성한 후 MN로 향하는 패킷들을 pMAG를 거쳐 nMAG에서 버퍼링된다.

MN이 이동을 마치고 nMAG와 연결이 되면 nMAG는 버퍼링되었던 패킷들을 MN에게 전송하고 HI 메시지에서 얻은 nLMA의 주소로 pLMAA를 담은 PBU{Seq, ts, pLMAA, CGAPnMAG, S(PRnMAG, PBU)} 메시지를 보낸다. 이때에



(그림 13) 수정된 Handoff Indicator Option 메시지

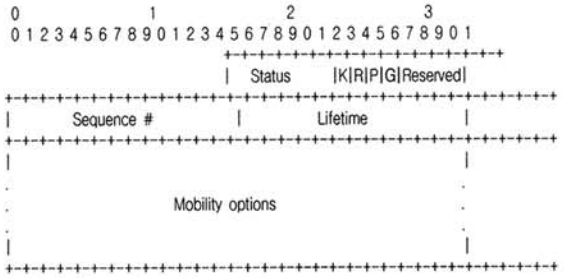


(그림 14) 수정된 Proxy 바인딩 Update 메시지

도 PBU메시지의 예약되어 있는 비트 중 하나를 (그림 14) 같이 G flag로 사용하여 도메인 간 핸드오버 중 이라는 것을 알린다.

PBU 메시지를 수신한 nLMA는 pLMA로 다시 PBU 메시지를 보낸다. pLMA는 PBU메시지에 담긴 MN-ID를 이용하여 자신의 BCE를 검색하여 현재 HLMA와 터널이 형성되어있는지 확인 한 후 없을 경우, MN에 대하여 새로운 HNP를 할당하고 관련 BCE 정보를 등록하고 고속 핸드오

버 단계에서 사용될 'Kbm'를 생성한 후 pLMA는 nLMA로 PBA{Seq,ts, MN-HNP, E(PUnMAG, Kbm), CGAPpLMA, S(PRpLMA, PBA)} 메시지를 보냄으로써, pLMA와 nLMA 사이에 양방향 터널이 형성된다. PBA 메시지의 G flag 역시 (그림 15)과 같이 1로 설정해서 보내야 한다.



(그림 15) 수정된 Proxy 바인딩 Acknowledgement 메시지

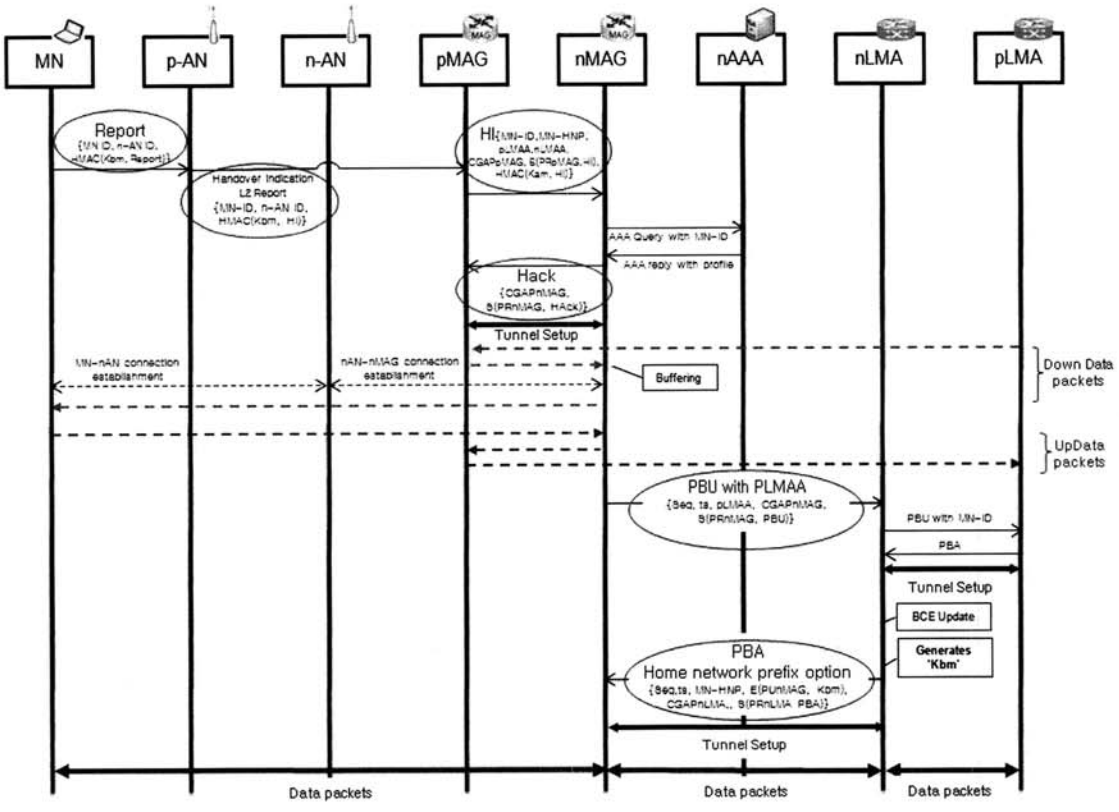
하지만 pLMA가 HLMA와 터널이 형성되어있을 경우, pLMA는 PBA 메시지의 상태 플래그 값을 이용하여 자신의 HLMA에게 보낸다. 이를 수신한 nLMA는 pLMA와 PBU와 PBA 메시지를 교환함으로써 터널을 형성한 후 CN에게 nLMA 정보를 전달한다. 그 다음 nMAG에게 PBA 메시지를 보내어 nMAG와 터널 형성 후 nLMA와 nMAG를 통해 전송된다. (그림 16)에서는 제안한 방법의 도메인 간 핸드오버 메시지 흐름을 보여주고 있다.

4. 성능평가

본 장에서는 암호프로토콜의 특성상 부주의한 설계로 인하여 의도하지 않은 오류가 포함되지 쉬우며, 그로인해 원래 목적에 치명적인 결함이 발생될 수 있다. 안전성 분석방법은 확률적 안전성 분석과 논리적 안전성 분석으로 크게 나누어 볼 수 있다. 본 논문에서는 보안 분석을 위해 논리적 안전성에 대해 전용 논리도구인 BAN로직을 통해 암호프로토콜의 안전성을 검증하고 보안성에 대한 성능을 분석한다.

4.1 BAN 로직

1989년 Burrow, Adadi, 그리고 Needham이 제안한 BAN 로직은 암호 프로토콜분석을 위한 논리도구로 알려져 있다 [11]. BAN논리는 믿음에 관한 논리로써 적은 수의 추론규칙을 통해 많은 인증 프로토콜의 목적 성취 유무를 추론해 낼 수 있다. 따라서 분산 환경에서 인증프로토콜을 분석하는 도구로써 논리를 제공한다. BAN로직은 크게 네 부분의 명세 사항으로 나누어진다. 일반적인 프로토콜 명세(usual notation), BAN표기법을 이용한 이상화된 프로토콜(idealized protocol), 이러한 이상화된 프로토콜을 나타내기 위한 가정(assumption), 그리고 프로토콜이 나타내려고 하는 궁극적인 목적으로 구성된다. BAN 로직을 사용하여 프로토콜 검증하기 위해서는 우선 원래의 프로토콜 명세로부터



(그림 16) 제안기법의 도메인 간의 핸드오버 메시지 흐름

〈표 1〉 BAN의 기본적인 표기법

표기법	의미	설명
A $\mid\equiv$ M	A believes M	A는 M를 신뢰한다.
A $\lhd$ M	A sees M	누군가가 M를 A에게 전송하였다. (A는 M를 수신함)
A $\mid\sim$ M	A once said M	A는 M를 전송한 적이 있다. (A는 M를 송신함)
A $\mid\Rightarrow$ M	A controls M	A는 M에 대한 권한이 있다.
#M	M is fresh	M는 현재 세션에 유효한 최근의 것이다.
$A \xleftrightarrow{Kbm} B$	shared key K	A와 B는 공유된 비밀정보 K로 통신할 수 있다.
$\overset{PU_B}{\mapsto} B$	B has K as a public key	PUB는 B의 공개키이다.
$A \overset{Kbm}{\rightleftharpoons} B$	Kbm is a secret known only to A and B	Kbm이 A와 B의 공유된 비밀키이다.
{M}K	encrypted under K	M는 비밀정보 K로 암호화되어 있다.
〈X〉 Z	combined with Z	〈X〉 Z를 전송한 근원은 인증정보 Z를 알고 있다.

BAN 표기법을 이용하여 이상화된 프로토콜을 명세해야 한다. 그 다음에 처음 상태에 관한 가정들을 기술한 다음 프로토콜의 문장에 논리적인 의미를 덧붙인다. 그리고 BAN 규칙들을 이용하여 검증한다. BAN의 기본적인 표기법은 <표 1>과 같다.

앞에서는 설명한 표기법을 이용하여 아래와 같은 추론규칙들로 구성된다.

R1 : Message Meaning 규칙

$$R1: \frac{A \mid\equiv (A \overset{K}{\longleftrightarrow} B), A \lhd \{M\}_K}{A \mid\equiv (B \mid\equiv M)}$$

이 규칙은 만약 하나의 개체인 A가 다른 개체 B와 대칭키인 K를 공유한다고 믿고, 개체 A가 K으로 암호화된 메시지 M를 받는다면, 개체 A는 개체 B가 메시지 M를 보낸 적이 있다는 것을 믿는다는 것을 의미한다. 이 규칙은 대칭키 암호화에 대해 기술한다.

R2 : Nonce Verification 규칙

$$R2: \frac{A \mid\equiv (\#(M)), A \mid\equiv (B \mid\equiv M)}{A \mid\equiv (B \mid\equiv M)}$$

이 규칙은 만약 개체 A가 어떤 정보 M이 신선하다고 믿고, 거기에다 Q가 이 정보를 전송했다고 믿는다면, A는 'Q가 스스로 그 정보를 믿는다'는 것을 믿는다는 것을 의미한다. 이 규칙은 메시지가 신선한지에 대해 검증한다. 메시지가 신선하다는 것을 이전에 한 번도 사용된 적이 없다는 것을 의미한다.

R3 : Jurisdiction 규칙

$$R3: \frac{A \mid\equiv (B \mid\Rightarrow M), A \mid\equiv (B \mid\equiv \{M\}K)}{A \mid\equiv B \mid\equiv M}$$

이 규칙은 만약 개체 A가 다른 개체 B가 어떤 정보 M를 관리 한다고 믿고, B가 그 정보를 믿는다는 것을 믿는다면, A와 B가 그 정보를 믿는다는 것을 말한다.

R4 : Hash 함수

$$R4: \frac{A \mid\equiv B \mid\sim \{H(M)\}, A \lhd \{M\}K}{A \mid\equiv B \mid\sim M}$$

A는 'B가 M의 해쉬 함수 값을 보낸 것'을 믿고, 메시지 M를 받았다면 A는 'B가 메시지 M를 보냈다는 것'을 믿을 수 있다.

CGA 환경를 고려한 확장된 BAN 로직을 위한 추론 규칙을 제안한다.

$$E1: \frac{A \mid\equiv \overset{PU_B}{\mapsto} B, A \rhd \{H(M)\}PR_B}{A \mid\equiv B \mid\sim M)}$$

이 규칙은 A는 'PUB가 B의 공개키'이고 B의 개인키로 암호화된 해쉬 값 M를 보냈다면, A는 'B가 M를 보냈다는 것'을 믿을 수 있다.

$$E2: \frac{A \mid\equiv \overset{PU_A}{\mapsto} A, A \mid\equiv B \mid\equiv \{M\}PU_A}{A \mid\equiv B \mid\equiv M}$$

이 규칙은 A는 'PUA가 A의 공개키'이고 'B가 A의 공개키로 암호화된 M를 믿는다는 것'을 믿는다면, A는 'B가 M를 믿는다는 것'을 믿을 수 있다.

$$E3: \frac{A \mid\equiv A \xleftrightarrow{K} B, A \mid\equiv B \mid\equiv \{M\}K}{A \mid\equiv B \mid\equiv M}$$

이 규칙은 A가 'K가 B와 A의 대칭키라는 것을 믿고, A는 'B가 {M}K를 믿는다는 것'을 믿는다면, A는 'B가 M를 믿는다는 것'을 믿을 수 있다.

위 규칙을 기반으로 인증 프로토콜을 분석한다. MN이 처음으로 접근할 때 발생하는 초기인증과 다른 MAG 및 LMA로 이동할 때 발생하는 핸드오버 인증와 같이 두 가지로 인증절차를 설명한다. 초기인증/핸드오버인증 분석을 위한 가정사항은 아래와 같다.

- 각 MN과 MAG는 IEEE 802.21 신호를 지원한다.
- MN과 인증 서버간에는 대칭키가 공유된다.
- MAG/LMA와 AAA 사이에는 대칭키가 공유된다.
- MAG/LMA는 이웃하는 MAG와 LMA간에 대칭키를 공유한다.
- 각 MAG의 시간은 동기화 되어있다.
- MN/MAG/LMA는 각 AAA에 의해 생성된 키를 신뢰한다.

4.1.1 초기인증 절차

BAN 로직 표기법에 기반하여 CGA 이용한 키 공유에 필요한 초기인증 메커니즘의 목적 및 가정 사항을 의미하며 (그림 17)과 같다. (그림 17)에서의 목표사항은 (1-1), (1-2), (1-3), (1-4) 이며, 가정사항은 A11, A12...A1e 로 나타낸다.

초기 인증에 대한 목적을 검증하기 위해 BAN 로직 추론 규칙들을 적용하여 검증해보면 아래와 같다.

(1-1)으로부터,

$(1) MAG \mid\equiv MN \mid\sim RS[By\_A11, A12, A13, A14, R1]$

$(2) MAG \mid\equiv MN \mid\equiv RS[By\_R2\_if\_MAG \mid\equiv \#(ts)]$

(1-2)으로부터,

$(3) LMA \mid\equiv MAG \mid\equiv PBU[By\_E1, A15, R2, A16, A17]$

$(4) LMA \mid\equiv MAG \mid\equiv \#(seq)[By\_(4)]$

(1-3)으로부터,

$(5) MAG \mid\equiv LMA \mid\equiv PBA[By\_A18, E1, A19, A1a, A1b, R2]$

$(6) MAG \mid\equiv LMA \mid\equiv LMA \overset{Kbm}{\rightleftharpoons} MAG[By\_(6), A1c, E2]$

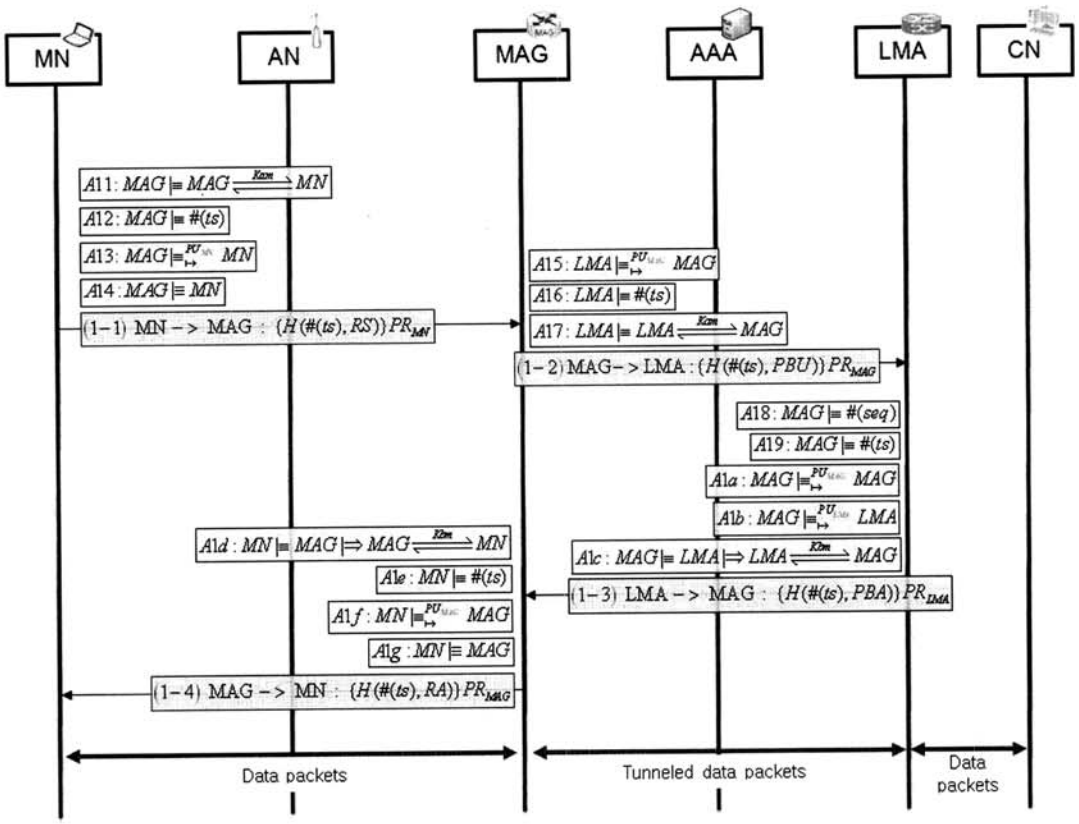
$(7) MAG \mid\equiv LMA \overset{Kbm}{\rightleftharpoons} MAG[By\_(7), A1c, R3]$

(1-4)으로부터,

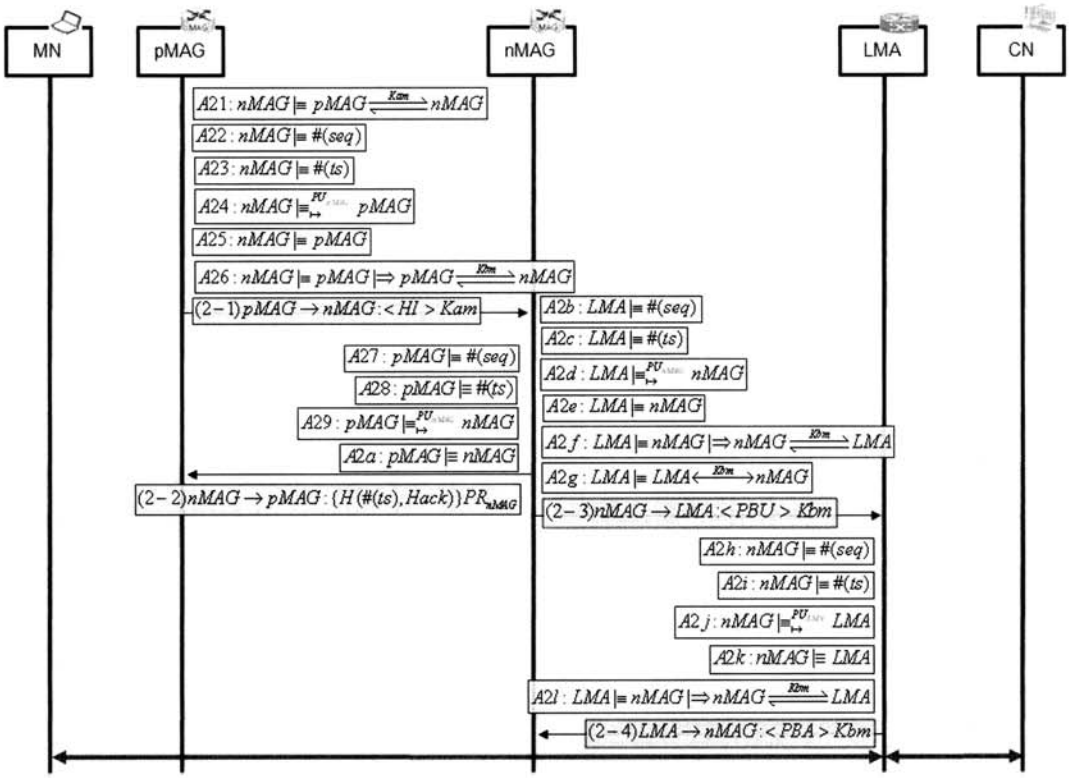
$(8) MN \mid\equiv MAG \mid\sim RtAdv[By\_A1d, A1e, A1f, A1g, R1]$

$(9) MN \mid\equiv MAG \mid\equiv RtAdv[By\_R2\_if\_MN \mid\equiv \#(ts)]$

객체 간에 신뢰관계 수립할 때 설정한 비밀키 'kam'를 통해 HMAC(Kam, RS)를 보냄으로써, RS 메시지가 자신의 네트워크로 부터 전송되었음을 신뢰할 수 있으며, 타임스탬프(ts)를 통해 현재 시간기준으로 적절한 범위 내에 있는지 확인하여 서비스 거부 공격를 차단할 수 있고, CGA 기법을 적용하여 MN의 공개키에 대한 소유권 증명과 메시지 보호 및 베타적 사용를 신뢰하며 인증 성공시 전자서명을 검증함으로써 객체 간에 신뢰할 수 있다.



(그림 17) 초기 인증 메커니즘의 목적 및 가정



(그림 18) 도메인 내 핸드오버에서 인증 메커니즘의 목적 및 가정

4.1.2 도메인 내 핸드오버의 인증 절차

BAN 로직 표기법에 기반하여 CGA 이용한 키 공유에 필요한 도메인 내 핸드오버인증 메커니즘의 목적 및 가정사항을 의미하며 (그림 18)과 같다. (그림 18)에서의 목표사항은 (2-1), (2-2), (2-3), (2-4) 이며, 가정사항은 A21, A22....A2c 로 나타낸다.

도메인 내 핸드오버에서 인증에 대한 목적을 검증하기 위해 BAN 로직 추론 규칙들을 적용하여 검증해보면 아래와 같다.

(2-1)으로부터,

(1) $nMAG \mid\equiv pMAG[by\_R1, A21, A22, A23, A24, A25, A26, R2]$

(2-2)으로부터,

(2) $pMAG \mid\equiv nMAG[by\_A27, R1, A28, R2, A29, A2a]$

(2-3), (2-4)으로부터,

(3) $LMA \mid\equiv MAG \mid\equiv PBU[by\_A2b, A2c, A2d, R1, A2e, R2, A2f, A2g]$

(4) $MAG \mid\equiv LMA \mid\equiv PBA[by\_A2h, A2i, A2j, R1, A2k, R2, A2l]$

객체 간에 초기인증과정 중 교환한 세션키 'kbm'를 통해 HMAC(Kbm, HI/PBU/PBA)를 보냄으로써, HI/PBU/PBA 메시지가 자신의 네트워크로 부터 전송되었음을 신뢰할 수 있으며, 타임스탬프(ts)를 통해 현재 시간기준으로 적절한 범위 내에 있는지 확인하여 서비스 거부 공격를 차단할 수 있고, CGA 기법을 적용하여 MN의 공개키에 대한 소유권 증명과 메시지 보호 및 베타적 사용를 신뢰하며 인증 성공 시 전자서명을 검증함으로써 객체 간에 신뢰할 수 있다.

4.1.3 도메인 간 핸드오버의 인증 절차

BAN 로직 표기법에 기반하여 도메인 간 핸드오버인증 메커니즘의 목적 및 가정사항을 의미하며 (그림 19)와 같다. (그림 19)에서의 목표사항은 (3-1), (3-2), (3-3), (3-4), (3-5), (3-6) 이며, 가정사항은 A31, A32....A3l 로 나타낸다.

도메인 간 핸드오버에서 인증에 대한 목표와 정의된 가정들과 BAN 로직 추론 규칙에 기반하여 분석 및 아래와 같이 도출한다.

(3-1), (3-3)으로 부터,

(1) $nLMA \mid\equiv nMAG \mid\equiv PBU[by\_A36, R1, A37, R2, A38, A39]$

(2) $nLMA \mid\equiv \#(seq)[by\_(1), A36, R3]$

(3) $nMAG \mid\equiv pMAG \mid\equiv HI[by\_A31, A32, A33, E1, (2), R2]$

(3-2)으로부터,

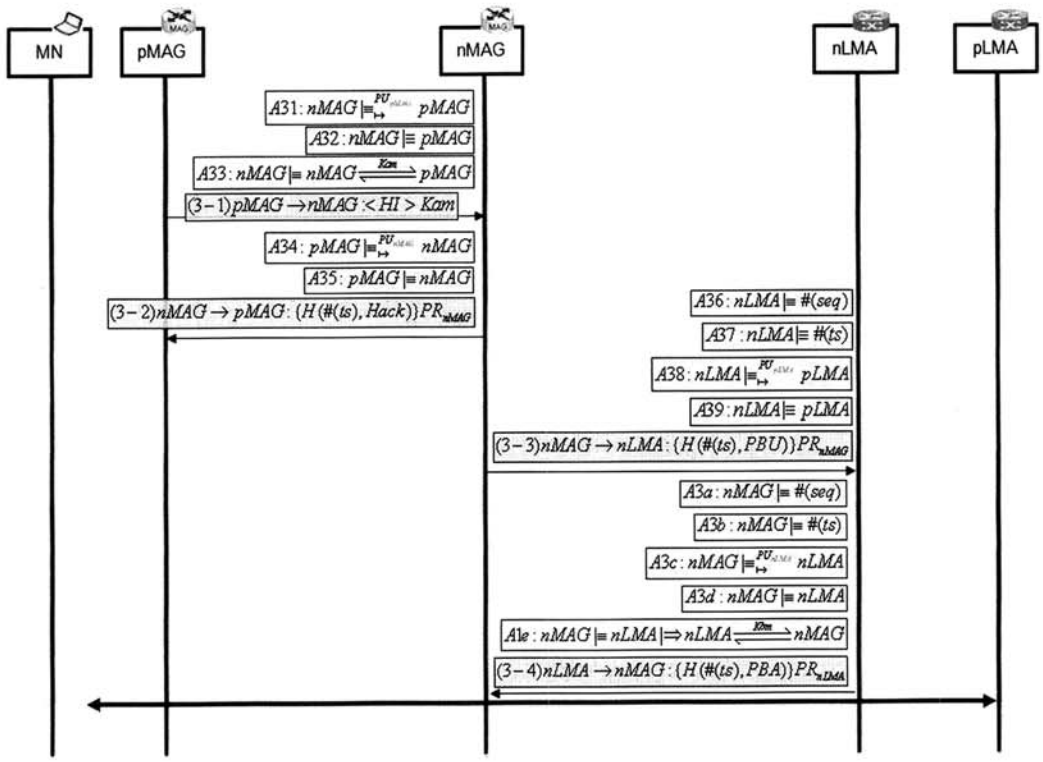
(4) $pMAG \mid\equiv nMAG \mid\equiv Hack[by\_R1, A34, R2]$

(5) $pMAG \mid\equiv nMAG[by\_(4), A35, R1, R2]$

(3-4)으로 부터,

(7) $nMAG \mid\equiv nLMA \mid\equiv PBA[by\_A3a, A3b, A3c, R1, A3d, A3e, R2]$

객체 간에 초기인증과정 중 교환한 세션키 'kbm'를 통해 HMAC(Kbm, HI)를 보냄으로써, HI 메시지가 자신의 네트워크로 부터 전송되었음을 신뢰할 수 있으며, 타임스탬프(ts)를 통해 현재 시간기준으로 적절한 범위 내에 있는지 확



(그림 19) 도메인 간 핸드오버에서 인증 메커니즘의 목적 및 가정

인하여 서비스 거부 공격를 차단할 수 있고, CGA 기법을 적용하여 MN의 공개키에 대한 소유권 증명과 메시지 보호 및 베타적 사용를 신뢰하며 인증 성공시 전자서명을 검증함으로써 객체 간에 신뢰할 수 있다.

4.2 보안성 분석

이동성 지원 기술에서는 다양한 보안 취약점이 존재할 수 있으며, 네트워크 객체 및 각 객체 간 전송되는 메시지는 아래와 같은 보안 요구 사항을 충족해야할 필요성이 있으므로, 본 논문에서는 보안성이 검증된 AAA (Authentication, Authorization, Accounting) 기반 구조를 이용한 인증방식과 CGA 기반의 보안 프로토콜에 대한 보안성을 분석하면 아래와 같다.

- 기밀성(Confidentiality) : 각 객체간에 신뢰관계 수립시 설정한 비밀키(Kam)와 세션키(Kbm)로써 기밀성을 제공한다.
- 무결성(Integrity) : 제안 방식에서는 해쉬 값(HMAC)과 전자서명을 이용하여 검증함으로써 무결성 제공
- 인증(Authentication) : 제안 프로토콜에서는 각 객체에 대한 인증은 AAA 인증서버를 통해 상호인증을 수행
- 접근제어(Access Control) : 정당하게 AAA 서버를 통해 인증을 받은 사용자만 서비스를 제공
- 서비스 거부 공격 / 리다이렉트 공격 : PMIPv6에서 각 객체간의 시그널링 메시지가 보호되지 않으면 MN과 MAG에 대한 DoS 공격이 가능하다. MN와 MAG의 ID를 도용할 수 있는 공격자가 정당한 노드로 가장하여 nMAG로 핸드오버한 것처럼 RS메시지를 위조하여 nMAG로 전송한다고 가정한다면, PMIPv6에서는 MN과 MAG간의 시그널링 메시지가 보호되지 않기 때문에 nMAG는 위조된 RS메시지를 받자마자 확인없이 MN에 대한 핸드오버를 위한 PBU 메시지를 LMA로 전송할 것이고, LMA는 이후 수신되는 MN의 패킷을 nMAG로 리다이렉트할 것이다. 결국 MN은 더 이상 패킷을 수신하지 못하게 된다. 하지만 제안기법에서는 MN과 MAG 간의 시그널링 메시지는 초기 인증과정에서 공유된 비밀키로 보호된다. 공격자는 MN과 MAG 간의 비밀키를 모르기 때문에 MAC 값을 계산할 수 없고, 결국 공격자는 RtrSol 메시지 위조가 불가능하여 공격에 실패하게 된다.

4.3 성능 분석

이번 장에서는 제안된 방법과 기존의 Kang-Park 기법과 ESS-FH의 기법에 대한 핸드오버 지연시간을 비교하여 분석한다. Random-Walk 이동성 모델의 2차원 마코브 체인 모델을 사용하여 MN의 이동성을 모델링 하였다[12]. 이 모델에서는 MN의 다음 위치는 이전 위치에 임의의 값을 더한 것이 된다. 여기서 임의의 값은 임의의 분포에서 독립적으로 선택된 값이다. 또한 MN이 네트워크에 머무를 확률을 P라고 할 때 다른 네트워크로 이동할 확률은 1-P이며, 확률의 메트릭스는 아래와 같다.

$$Pi,j = \begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

다음의 식에서 MN이 LMA상에 그대로 머무를 확률 π_0과 MN이 다른 곳을 움직일 π_1를 나타내면 아래와 같다.

$$\pi_0 = p\pi_0 + (1-p)\pi_1,$$
$$\pi_1 = (1-p)\pi_0 + p\pi_1,$$
$$\pi_0 + \pi_1 = 1.$$

4.3.1 수학적 분석

핸드오버 지연시간은 MN이 AN에게 Report 메시지를 전송하고 다시 MAG로부터 ARep메시지를 받는 시점까지의 등록과정과 인증과정을 나타내었다. 핸드오버 분석을 위해 초기접속 인증과정에서의 핸드오버 지연시간과 핸드오버 인증과정에서의 핸드오버 지연시간을 구한다.

먼저 초기접속 인증과정에서 기존연구의 핸드오버 지연시간을 $L_{Initial-HO}^{(KP)}$, $L_{Initial-HO}^{(ESS-FH)}$로 표기하며 수식 (1), (2)로 나타내고, 제안기법의 초기접속 지연시간은 $L_{Initial-HO}^{(SA-FP)}$로 표기하며 수식(3)으로 나타낸다.

$$L_{Initial-HO}^{(KP)} = \frac{(MinInt + MaxInt)}{4} + \mathrm{Retrans}Timer \times DADTransmits + 3t_{MN-AR} + 2(t_{AR-MAP} + t_{MAP-HA}) \quad (1)$$

$$L_{Initial-HO}^{(ESS-FH)} = \frac{(MinInt + MaxInt)}{4} + \mathrm{Retrans}Timer \times DADTransmits + 3t_{MN-AR} + 2(t_{AR-MAP} + t_{MAP-HA}) \quad (2)$$

$$L_{Initial-HO}^{(SA-FP)} = \frac{(MinInt + MaxInt)}{4} + 2t_{MAG-LMA} + t_{MN-AAA} \quad (3)$$

식 (3)은 일반적인 PMIPv6의 최초 접속 및 핸드오버 지연시간으로 MN가 인지되는 지연시간 $\frac{(MinInt + MaxInt)}{4}$, MN을 로컬 네트워크에 등록하기 위한 시간 $(2t_{MAG-LMA})$으로 나뉜다. 다음으로 도메인 내 핸드오버 지연시간은 (4), (5), (6)으로 나타낸다.

$$L_{Intra-HO}^{(KP)} = 2t_{MN-AR} \quad (4)$$

$$L_{Intra-HO}^{(ESS-FH)} = L_{Intra-HO}^{(KP)} \quad (5)$$

$$L_{Intra-HO-\mathrm{Pre}}^{(SA-FP)} = \frac{L_{Intra-HO}^{(KP)} = L_{Intra-HO}^{(ESS-FH)}}{2} = t_{MN-MAG} \quad (6)$$

식 (6)은 FPMIPv6의 Predictive 모드의 도메인내의 핸드오버의 지연시간이다. (그림 3-2)을 보면 일반적인 PMIPv6의 경우 MN이 nMAG가 인지되는 지연시간이 존재 한다.

$$L_{Intra-HO-Re}^{(SA-FP)} = t_{MN-MAG} + 2t_{MAG-LMA} \quad (7)$$

식 (7)은 FPMIPv6의 Reactive 모드의 도메인내의 핸드오버의 지연시간이다. MN이 nMAG가 인지되는 구간에서의 지연시간과 nMAG와 LMA간 바인딩 업데이트를 위한 지연시간이 존재한다.

$$L_{Inter-HO}^{(KP)} = L_{Initial-HO}^{(KP)} \quad (8)$$

$$L_{Inter-HO}^{(ESS-FH)} = L_{Intra-HO}^{(ESS-FH)} \quad (9)$$

$$L_{Inter-HO}^{(SA-FP)} = \min(L_{Intra-HO-\mathrm{Pre}}^{(SA-FP)}, L_{Intra-HO-Re}^{(SA-FP)}) \quad (10)$$

식 (10)은 PMIPv6/FPMIPv6에서는 도메인 간 핸드오버를 지원하지 않지만, 본 논문에서 제안한 도메인 간 핸드오버를 통해 MN의 인지되는 시간은 도메인 내 핸드오버와 동일한 지연시간이 존재한다.

4.3.2 성능 평가 결과

수학적으로 분석한 수식을 기반으로 그래프를 이용하여 성능을 평가한다. 시뮬레이션에 설정된 매개변수 값은 관련 논문의 가정을 참고 한다[13], [14], [15].

(그림 20)은 제안된 기법인 SA-FP와 기존 기법들의 핸드오버 지연시간들을 비교한 그래프이다 [6] [7]. 수학적 분석을 통해 산출된 SA-FP기법의 성능은 기존 기법에 비해 초기접속 과정에서는 11배, 도메인 간 핸드오버접속 과정에서는 약 2배의 성능이 향상되었음을 확인할 수 있다.

도메인간 이동 횟수증가에 따른 핸드오버 지연시간을 수학적으로 분석한 식 (8), (9), (10)를 이용하여 (그림 21)로 나타낸다. 일반적인 PMIPv6에서는 도메인간 핸드오버를 지원하지 않기 때문에 대신 제안된 도메인간 핸드오버와 기존 기법의 핸드오버의 지연시간을 비교하였다. KP-FHMIPv6는 도메인간 핸드오버의 증가에 따라 급속하게 지연시간이 증가한다. 왜냐하면 제안된 SA-FPMIPv6 도메인간 핸드오버와 달리 FHMIPv6는 이전 HA로 바인딩 업데이트를 하는 시간이 존재하기 때문이다. 또한 제안한 기법인 SA-FPMIPv6는 상대적으로 무선구간 지연에 따른 영향을 덜 받게 되므로 도메인간 핸드오버에 적용하면 핸드오버 지연시간이 기존 기법에 비해 매우 작기 때문에 먼 거리를 이동할 때도 고속 핸드오버가 가능하다.

또한 이동성 모델를 통해 성능를 비교한다. 기존 기법과 제안된 기법 하에서 MN의 평균 도메인 상주 시간 동안 이동에 따른 Handover 지연시간에 대한 수식은 (11), (12), (13)과 같다. T는 MN이 셀에 머무는 평균 시간을 의미한다.

〈표 2〉 분석에 사용된 매개변수 값

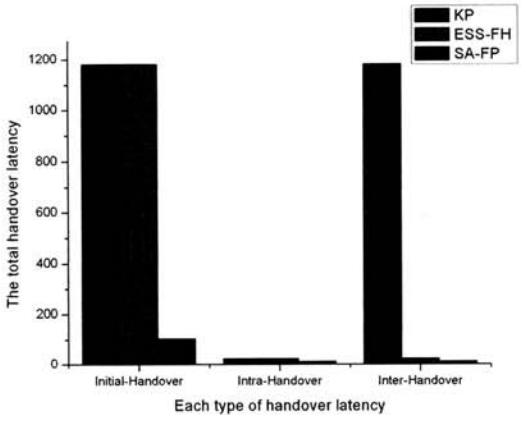
매개변수	의 미	지연시간 (ms)
$t_{MN-pMAG(pAR)}$	MN와 pMAG(pAR) 간의 전송지연	12
$t_{MN-nMAG(nAR)}$	MN와 nMAG(nAR) 간의 전송지연	12
$t_{pMAG(pAR)-nMAG(nAR)}$	pMAG(pAR)와 nMAG(nAR) 간의 전송지연	20
$t_{pMAG(pAR)-nLMA(nMAP)}$	pMAG(pAR)와 nLMA(pMAP or HA) 간의 전송지연	20
$t_{nMAG(nAR)-nLMA(nMAP)}$	nMAG(nAR)와 nLMA(nMAP) 간의 전송지연	20
$t_{nLMA(nMAP)-HA}$	nLMA(nMAP)와 HA간의 전송지연	40
$t_{pLMA(pMAP)-nLMA(nMAP)}$	pLMA(pMAP)와 nLMA(nMAP)간의 전송지연	40
t_{MN-AAA}	MN와 AAA 인증을 위한 지연시간	40
$t_{MAG(AR)-AAA}$	MAG(AR)와 AAA 인증을 위한 지연시간	40
$t_{LMA(MAP)-AAA}$	LMA(MAP)와 AAA 인증을 위한 지연시간	40
MinInt	MN의 이동을 인식하는 지연시간 계산하기위한 최소값	30
MaxInt	MN의 이동을 인식하는 지연시간 계산하기위한 최대값	70
Re*TranceT*	Neighbor Solicitation(NS) 재송신 시간	1000
DADTrance	IP주소 중복 확인 시간	1

$$L_{HO}^{(KP)} = \frac{L_{Intra-HO}^{(KP)}(1-\pi_1) + L_{Inter-HO}^{(KP)}\pi_1}{T} \quad (11)$$

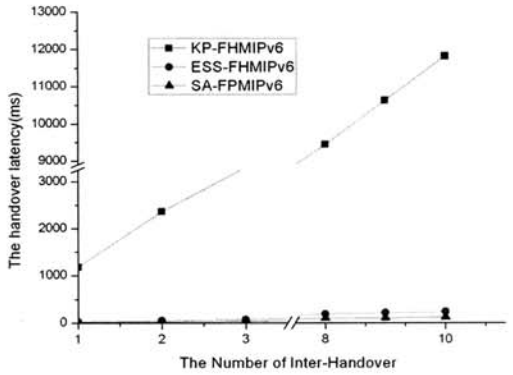
$$L_{HO}^{(ESS-FH)} = \frac{L_{Intra-HO}^{(ESS-FH)}(1-\pi_1) + L_{Inter-HO}^{(ESS-FH)}\pi_1}{T} \quad (12)$$

$$L_{HO}^{(SA-FP)} = \frac{L_{Intra-HO}^{(SA-FP)}(1-\pi_1) + L_{Inter-HO}^{(SA-FP)}\pi_1}{T} \quad (13)$$

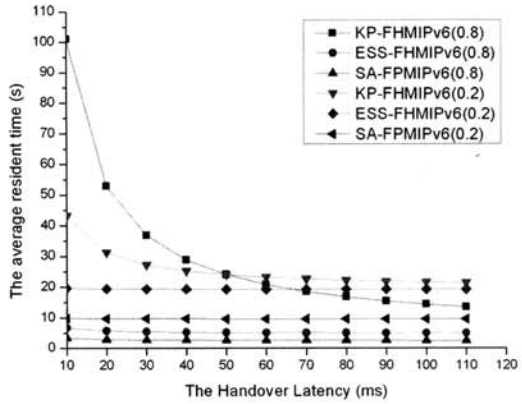
(그림 22)은 Random-Walk 이동성 모델에서 MN이 네트워크에 머무르는 시간에 따라 전체 핸드오프 시간의 변화를 타낸다. 모든 시스템에서 전반적으로 전체 핸드오프 시간은 네트워크에 머무르는 시간이 길면 길수록 낮아지는 것을 알 수 있다. 네트워크에 머무르는 시간은 곧 MN이 이동하는 횟수가 적다는 것으로 생각하면 결과를 쉽게 이해할 수 있다. 즉, π1(이동하려는 값) 큰 것은 MN이 자주 이동한다는 것을 의미하고, MN이 자주 이동하는 경우는 Handover 지연시간이 길어진다는 것을 알 수 있다. 따라서 전체적으로 MN의 이동이 잦아지게 되면 시스템의 성능은 전반적으로 낮아지게 된다. (그림 4-6)와 같이 제안된 기법에서는 MN의 이동이 잦아져도 성능에 미치는 영향이 적은 반면, KP-FHMIPv6의 기법은 크게 성능이 저하되었다. 결과적으로 제안한 SA-FPMIPv6기법은 네트워크 기반의 이동성을 관리해주므로써 기존의 FHMIPv6에 비해 이동성 성능이 향상되므로 핸드오버 지연시간을 줄일 수 있다.



(그림 20) 핸드오버 지연시간 비교



(그림 21) 도메인간 이동 횟수증가에 따른 핸드오버 지연시간 비교



(그림 22) MN의 네트워크에 머무르는 시간(T)에 따른 전체 핸드오버 시간

5. 결 론

현재 MIPv6에서 이동 성능을 향상시키기 위한 많은 방법이 연구되고 있다. 그 중 MN 기반의 이동성 지원 기술인 MIPv6, FMIPv6, HMIPv6에서 발생할수 있는 무수히 많은 시그널링의 낭비되는 단점을 보완하고자 네트워크 기반의 이동성 지원 기술인 PMIPv6은 2008년 RFC 표준 완성 이후 다양한 연구가 진행되어온 프로토콜이다. PMIPv6은 MN의 신호를 획기적으로 줄임으로써 이슈가 되고 있는 무선 신호 간 간섭 문제를 줄이고, 유선 구간을 확대함으로써 안정적인 전송 속도를 확보할 수 있지만, 도메인 내에서의 핸드오버에 있어서는 이동성 지원방법에 대한 연구가 상당부분 진척된 데 비해 도메인 외에서의 이동성 지원을 위한 도메인 간의 핸드오버가 지원되지 않는 치명적인 단점이 있고, 보안적인 측면에서는 시그널링 메시지를 보호하기 위해 다양한 기법들이 제안되었지만, 대부분의 기존기법들은 PMIPv6 시그널링 메시지를 보호하기 위해 AAA 서버를 기반으로 한다.

본 논문에서는 프록시 모바일 네트워크 환경에서 핸드오버 기법의 보안 분석을 통해 PMIPv6/FPMIP6기반의 시그널링 메시지를 보호하기 위한 AAA 프로토콜과 공개키 기반의 CGA기법을 도입하여 이동성과 안전성이 향상된 결과를 얻을 수 있었으며, 기존 PMIPv6에서 지원하지 못했던 도메인 간의 핸드오버를 추가적으로 제안하였다. 본 논문에서는 논리도구인 BAN로직를 통해 인증 프로토콜을 검증하였고, 마코브 체인 모델을 통해 이동성을 모델링하여 네트워크 기반의 이동성 지원 기술인 PMIPv6을 기반으로 안정적인 전송 속도를 확보한 후, 시그널링에 대한 메시지 보안 메커니즘을 통해 보다 높은 보안성 얻을 수 있었다.

참 고 문 헌

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," RFC 3775, June, 2004.

[2] R. Koodli, "Mobile IPv6 Fast handovers," RFC 5568, July, 2009.

[3] El. Malki, L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)," RFC 4140, August, 2005.

[4] S. Gundavelli, K. Leung, V. Devarapalli and K. Chowdhury, "Proxy mobile IPv6," RFC 5213, August, 2008.

[5] H. Yokota, K. Chowdhury and R. Koodli, "Fast handovers for Proxy Mobile IPv6," RFC 5949, September, 2010.

[6] Kang, H.S., Park, C.S. "MIPv6 Binding Update Protocol Secure Against Both Redirect and DoS Attacks," CISC 2005, Lecture Notes in Computer Science, LNCS Vol.3822, Springer-Verlag pp.407-418, 2005.

[7] I. You, J. Lee, K, Sakurai, and Y.Hori, "ESS-FH:Enhanced Security for Fast Handover in Hierarchical Mobile IPv6," IEICE Tr. on Information and Systmes, Vol.E93-D, No.5, pp.1096-1105, May, 2010.

[8] T. Aura, "Cryptographically Generated Address," RFC 3972, March, 2005.

[9] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6(IPv6)," RFC 4681, September, 2007.

[10] J. Arkko, C. Vogt and W. Haddad, "Enhanced Route Optimization for Mobile IPv6," IETF RFC 4866, May, 2007.

[11] M Burrows, M Abadi and R Needham, "A logic of authentication," ACM Trans. Comput. Syst., Vol.8, No.1, pp.18-36, February, 1990.

[12] I. F. Akyildiz and W. Wang, "A dynamic location management scheme for next-generation multitier PCS systems," IEEE Trans. Wireless Commun., Vol.1, No.1, pp.178-189, January, 2002.

[13] Ki-Sik Kong, Youn-Hee Han, Myung-Ki Shin, HeungRyeol Yoo, and Wonjun Lee, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6," IEEE Wireless Communications, Vol.15, pp.36-45, April, 2008.

[14] Y. Han, J. Choi, and S. Hwang, "Reactive Handover Optimization in IPv6 Based Mobile Networks," IEEE JSAC, Vol.24, No.9, pp.1758-72, September, 2006.

[15] K. S. Kong, W. Lee, Y. H. Han, M. K. Shin, "Handover Latency Analysis of a Network-based Localized Mobility Management Protocol," IEEE ICC'08, pp.5838-5843, 2008.

채 현 석

e-mail : hyunsukv@skku.edu
2012년 성균관대학교 정보통신공학부
(공학석사)
관심분야 : 차세대 통합망, 모바일컴퓨팅, 스마트기기 보안, 네트워크 보안, IT융합 등

정 종 필

e-mail : jpjeong@skku.edu
1997년 성균관대학교(공학사)
2003년 성균관대학교 정보통신공학부
(공학석사)
2008년 성균관대학교 정보통신공학부
(공학박사)
관심분야 : 모바일컴퓨팅, 센서 이동성, 차량 모바일 네트워크, 스마트기기 보안, 네트워크 보안, IT융합, 인터랙션 사이언스 등