情報保護學會論文誌
第17卷 第3號, 2007. 6

HMIPv6 환경에서의 안전한 Fast Handover를 위한 인증 메커니즘

김 민 경,[1†] 강 현 선[1†], 박 창 섭[1†]
[1]단국대학교

Authentication Mechanism for Secure Fast Handover in HMIPv6

Min-Kyoung Kim,[1†] Hyun-sun Kang[1†], Chang-Seop Park[1†]
[1]Dankook University

요 약

본 논문에서는 HMIPv6 환경에 Fast Handover를 통합시킴으로써 안전성과 효율성을 지원하는 프로토콜을 설계, 제안한다. AAA를 기반으로 한 HMIPv6환경의 제안 프로토콜에서 MN이 최초의 MAP 도메인으로 진입할 때에 인증을 위해 초기 LBU(initial Local Binding Update) 프로토콜을 수행한다. 이 과정에서 MN은 MAP으로부터 인증을 위한 비밀키가 포함되어 있는 티켓을 제공받아 Fast Handover 과정에 사용하는 안전한 Fast Handover 기법을 제안한다. 또한 본 논문은 다양한 공격 시나리오를 통해 안전성을 분석하고, 기존 방법들과 비교·분석한다.

ABSTRACT

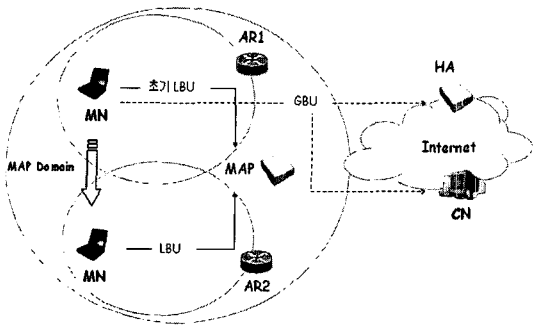
In this paper, We design and propose a protocol for supporting secure and efficient mobility in integrating fast handover and HMIPv6. In the proposed protocol which is AAA-based HMIPv6, if the MN enters the MAP domain for the first time, then it performs an Initial Local Binding Update for authentication. We propose a secure Fast Handover method using the ticket provided by MAP, which includes the secret key for authentication. Also, we analyze and compare security properties of our proposed scheme with those of other scheme using various attack scenario.

Keywords : *HMIPv6, Fast Handover, Ticket, initial Local Binding Update*

Ⅰ. 서 론

Mobile IPv6(MIPv6)[1]에서는 모바일 노드(Mobile Node, MN)에게 끊임없는 전송계층 연결을 제공하기 위한 두 가지 유형의 IP 주소가 정의된다. 그 중 하나는 MN의 홈 도메인 또는 홈 네트워크에서 정의된 고정된 HoA(Home Address)이고, 다른 하나는 MN이 외부 네트워크(foreign network)로 이동함에 따라 동적으로 할당받게 되는 CoA(Care-of-Address)이다. MN은 이동 시 자신의 홈 에이전트(Home Agent, HA)와 대응노드(Correspondent Node, CN)에게 자신의 현재 위치를 알리기 위한 바인딩 업데이트(Binding Update, BU) 프로토콜을 수행한다. 이를 통해 이동 중에도 지속적인 패킷 포워딩(packet forwarding) 서비스를 받게 된다. MIPv6에서는 MN이 새로운 접속 라우터(Access Router, AR)

접수일: 2007년 1월 17일; 채택일: 2007년 5월 17일
* 이 연구는 2006학년도 단국대학교 총동창회지원 연구비로 연구되었습니다.
† 박창섭, csp0@dankook.ac.kr
‡ 김민경, mashimaro@dankook.ac.kr



〔그림 1〕 HMIPv6 프로토콜

로 이동할 때마다 BU 프로토콜이 수행된다. 따라서 소규모 기지국에서의 잦은 이동으로 인해 발생하는 BU 프로토콜 지연은 패킷손실을 초래할 수 있으며, 이로 인해 서비스의 QoS(Quality of Service)가 떨어질 수도 있다. 이와 같은 BU 지연으로 인한 패킷손실을 최소화하기 위해서 Hierarchical Mobile IPv6(HMIPv6)[2]와 Fast Handover[3]가 제안되었다.

〔그림 1〕에서와 같이 HMIPv6에는 MIPv6의 구성에 MAP(Mobile Anchor Point) 개체가 새롭게 추가된다. 모바일 노드가 이동한 외부 네트워크에는 하나 또는 그 이상의 MAP이 존재하며, MAP은 이동 네트워크에서의 지역 홈 에이전트의 역할을 수행한다. 새로운 MAP 도메인으로 진입한 경우, MN은 AR1이 광고하는 프리픽스(prefix) 정보를 기반으로 MAP 도메인 상의 RCoA (Regional CoA)와 링크 상의 LCoA(Link CoA)를 설정한다. MN은 처음으로 MAP에게 자신의 LCoA와 RCoA를 등록하기 위해 **초기 LBU** 메시지를 전송하고, 순차적으로 HA와 CN에게 새로운 RCoA를 포함한 **GBU**(Global BU)[4,5,6] 메시지를 보낸다. 반면, 만약 MN이 〔그림 1〕 에서와 같이 동일 MAP 도메인 내에서 AR2의 서브넷으로 이동시에는 RCoA는 변경되지 않고 단지 LCoA만 변경되기 때문에 새로운 LCoA를 등록하기 위해 MAP으로 LBU 메시지만을 보내게 된다. 결국, LBU가 원격지간의 메시지 교환을 수반하는 GBU를 대신하기 때문에 바인딩 정보 갱신에 따른 지연을 줄일 수 있게 된다. 하지만, LBU 역시 이동탐지(movement detection), 새로운 CoA 설정 등으로 인한 지연을 초래할 수 있다. Fast Handover 기법〔3〕은 LBU 과정에서 발생하는 지연을 최소화시키기 위해 적용될 수 있다. Fast Handover에 대한 내용은 2장과 3장에서 Fast Handover에 적용이 가능한 인증 메커니즘을 설명할 때 자세히 소개된다.

안전한 HMIPv6를 위해서는 LBU 메시지에 대한 인증이 필요하다. LBU 메시지가 인증이 되지 않으면 플러딩 공격(flooding attack), 리다이렉트 공격(redirect attack) 등의 DoS 공격이 발생할 수 있다. 만약 공격자가 MN으로 향하는 패킷을 가로채기 위해 MN의 RCoA와 자신의 LCoA를 포함한 위조된 LBU 메시지를 송신한다면, 해당 패킷은 공격자에게로 리다이렉트 될 것이다. 또한, 수신을 원치 않는 또 다른 호스트로 대량의 멀티미디어 패킷을 리다이렉트하여 해당 호스트에 대해 플러딩 공격을 발생시킬 수도 있다. 현재 표준으로 제안된 Fast Handover 기법에도 인증기능이 포함되어 있지 않기 때문에 유사한 공격에 노출이 되어진다. 본 논문에서는 프로토콜의 효율성과 안전성을 고려한 Fast Handover와 통합한 HMIPv6 프로토콜을 제안한다. 2장에서는 본 연구와 관련된 기존 연구와 문제점을 분석하고, 3장에서는 Fast Handover와 HMIPv6의 통합 환경에서의 안전하고 효율적인 프로토콜을 제안하고, 프로토콜의 안전성과 성능을 분석한다. 마지막으로 4장은 결론을 제시하면서 논문을 마친다.

Ⅱ. 기존연구

최근 IETF MIPSHOP(Mobile IP : Performance, Signaling, and Handoff Optimization) 워킹그룹에서는 본 논문의 주제와 연관된 2개의 Draft가 발표되었다. 〔7, 8〕에서는 LBU 메시지에 대한 인증을 위해 CGA (Cryptographically-Generated Address)에 기반을 둔 인증 메커니즘을 제안하였고, 〔9〕에서는 AAA(Authentication, Authorization, and Auditing) 서버를 기반으로 하는 안전한 Fast Handover 방식을 제시하였다. 이번 장에서는 제안된 기존 방식들의 특성과 문제점을 살펴본다.

2.1 CGA 기반의 인증된 HMIPv6

〔7, 8, 10〕에서는 LBU 메시지 인증을 위해 CGA 기반의 인증된 대칭키 교환 프로토콜을 제안하였다. H( ) 를 일방향 해쉬함수, *subnet_prefix*를 AR의 subnet prefix, PK_{MN} - SK_{MN}을 각각 MN의 공개키/개인키라고 할 때, MN의 LCoA와 RCoA의 IID(Interface IDentifier)는 $H(subnet_prefix, PK_{MN})$의 64비트를 선택하여 선정

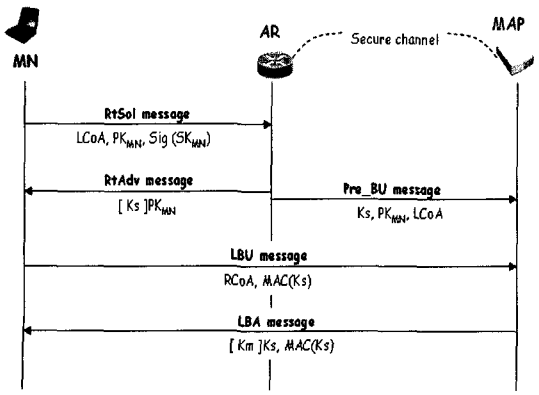
된다. 이런 방식으로 생성된 MN의 IPv6 주소를 CGA라고 한다. 좀 더 상세한 CGA 생성과정은 [11, 12]에서 참조할 수 있다.

MN이 MAP 도메인으로 진입하면, MN은 자신의 공개키를 이용하여 생성한 CGA 주소 *LCoA*와 자신의 공개키 PK_{MN}에 대한 서명값 $Sig(SK_{MN})$을 첨부한 RtSol 메시지를 AR에게 전송한다. RtSol 메시지의 서명을 확인한 후, AR은 MN에게는 RtAdv 메시지를 MAP에게는 Pre_BU(Pre-Binding Update)메시지를 전송한다. 이때 AR은 바인딩 업데이트 메시지에 대한 인증목적의 대칭형 세션키 *Ks*를 생성하여, MN의 공개키로 암호화한 $[Ks]PK_{MN}$을 RtAdv 메시지에 포함시킨다. Pre_BU 메시지에는 *Ks*, PK_{MN}, *LCoA*가 포함된다. Pre_BU메시지는 AR과 MAP 사이에 보안이 설정된 채널(secure channel)을 통해 보호되어 진다.

Pre_BU 메시지를 수신한 MAP은 BCE(Binding Cache Entry)를 생성하여, AR이 보낸 파라미터 값들을 저장한다. MAP이 LBU 메시지를 수신하면, MAP은 자신의 BCE 테이블에 RCoA를 등록한다. 물론, 이때 LBU메시지에 포함된 *MAC(Ks)*을 기반으로 메시지에 대한 인증 확인 작업이 수행된다. 여기서, *MAC(Ks)*는 LBU 메시지 내의 모든 필드값을 대칭키 *Ks*로 계산한 MAC 값을 의미한다.

MAP은 LBA(Local Binding Acknowledgement) 메시지를 통해서 바인딩 업데이트가 성공적으로 수행되었음을 MN에게 알리고, 앞으로 MN과 MAP 간의 LBU 프로토콜에 사용될 세션키 *Km*을 *Ks*로 대칭형 암호화하여 전달한다.

해당 프로토콜은 CGA의 부적절한 사용으로 DoS 공격에 노출된다[13]. 공격자가 서명처럼 보이는 의미 없는 데이터를 포함한 다수의 위조된 RtSol 메시지를 AR로 전송한다고 가정하자. 결국 AR은 위조된 서명을 확인하기 위한 다수의 무의미한 계산을 수행해야 한다. 또한 현재성을 보장할 수 있는 파라미터가 포함되어 있지 않기 때문에 재생공격에 노출될 수 있다.

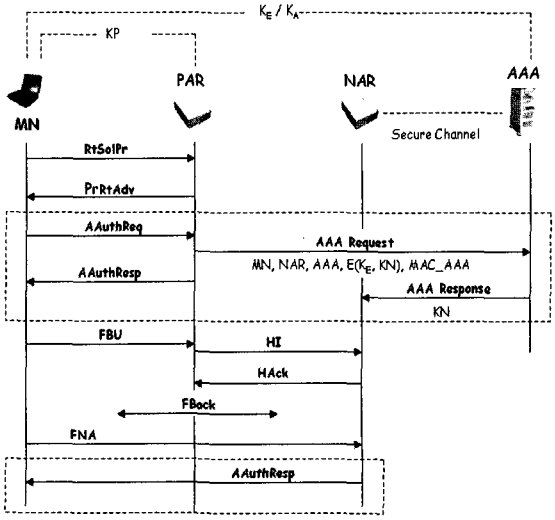


[그림 2] CGA에 기반을 둔 초기 LBU 프로토콜

2.2 AAA 기반의 인증된 Fast Handover 프로토콜

[그림 3]의 점선박스를 제외한 나머지 부분이 [3]에서 제안하는 Fast Handover 기법이다. Handover가 필요할 경우에 MN은 자신의 현재 접속 라우터 PAR(Previous AR)과 RtSolPr / PrRtAdv 메시지를 주고받은 후에, 자신의 새로운 접속 라우터 NAR(New AR)의 IP 주소와 해당 링크에서의 subnet prefix를 획득한다. MN은 NAR 링크에서 사용할 새로운 LCoA를 구성하고 FBU (Fast Binding Update) 메시지를 통해서 PAR에게 자신이 NAR 링크로 이동할 예정임을 통보한다. 후속적인 HI, HAck, FBack 메시지의 교환을 통해서 PAR로 보내어지는 MN에 대한 패킷들이 NAR로 전달되어 버퍼링 된다. MN이 PAR에서 NAR로 이동을 완료한 이후에는 FNA(Fast Neighbor Advertisement) 메시지를 NAR에게 보냄으로써 버퍼링된 패킷들을 전해 줄 것을 요청하게 된다.

[9]에서는 기본적인 Fast Handover 프로토콜의 보호를 위하여 AAA 서버를 기반으로 한 인증 기법을 제



[그림 3] AAA 기반의 인증된 Fast Handover 프로토콜

안하였다. 기본적인 가정은 MN과 PAR은 이미 세션키 KP가 공유되어 있고, MN과 AAA 간에도 K_E / K_A가 사전에 공유되어 있다. 또한 NAR과 AAA 간에 교환되는 메시지들은 이미 보안이 설정된 채널(secure channel)을 통해서 안전하게 보호되어진다. 점선 박스안에 있는 AAuthReq / AAuthResp / AAA Request / AAA Response 메시지의 목적은 MN과 NAR 간에 새로운 세션키 KN을 공유시키기 위한 목적이다. 이 새로운 세션키는 FBU / FNA 메시지에 대한 인증목적으로 사용된다.

하지만 제안된 기법은 다음과 같은 보안상의 오류를 내포하고 있다. AAA Request 메시지를 통해서 전달되는 사항은 *MN, NAR, AAA,* $[KN]K_E$, *MAC_AAA*이다. KN은 MN이 생성하여 AAA와 공유하고 있는 K_E로 암호화하여 AAuthReq 메시지를 통해서 PAR에게 전달된 값이고, $MAC\_AAA = H(MN \| NAR \| AAA, [KN]K_E)$ XOR $H(K_A)$. 이때, *MAC_AAA*로부터 $H(K_A)$가 도출될 수 있고, 특히, 이 값은 고정된 값이기 때문에, 원래의 메시지 인증목적을 수행할 수가 없게 된다. 결국 위조된 또는 재생된 AAA Request 메시지의 조작이 가능하게 된다. 효율적인 측면에서도 매번의 Handover마다 원격지의 AAA 서버를 경유해야 하기 때문에 긴 지연이 발생된다. 특히, 제안방식에서는 MN과 PAR 간에 공유된 *KP*를 기반으로 MN과 NAR 간에 *KN*을 공유하는 방식을 제안하는 데, 초기의 *KP*가 어떻게 설정되어지는 데에 대한 언급은 하지 않고 있다. [14]에서도 [9]와 유사한 방식의 초기 LBU에 대한 프로토콜이 제안되어 있으나, [14]의 프로토콜은 Fast Handover시, 즉 MN과 PAR이 키를 공유한 상황에서도 PAR에서 NAR로 이동시에는 NAR을 경유한 AAA와의 개별 접촉이 요구된다. 따라서 잦은 Handover가 발생하는 상황에서는 매우 비효율적인 방법이다.

Ⅲ. 제안 메커니즘

3.1 기본적인 가정과 설계원리

NSP(Network Service Provider)는 MN에 대한 인증과 함께 기본적인 네트워크 접근 서비스를 제공한다. 한편, MSP(Mobile Service Provider)는 NSP에 의한 인증이 성공적으로 이루어진 이후에 MN에게 MIPv6 서비스를 제공한다. 제안 프로토콜에서는 [10]에서 소개된 통합 시나리오를 사용한다. 즉, 네트워크 접근 서비스와 MIPv6 서비스가 하나의 운영자에 의해 제공됨을 의미한다. MN은 홈 네트워크의 서비스 제공자에 가입되어 있으며, 만약 홈 서비스 제공자와 또 다른 외부 네트워크의 서비스 제공자가 로밍협약을 체결하였다면 MN이 외부 네트워크로 로밍 하였을 경우 네트워크 서비스와 이동 서비스를 제공받을 수 있게 된다. 로밍 과정에서 MN은 PKI 기반 인증서 방식과 AAA 방식으로 인증 받을 수 있다. 제안 프로토콜에서는 안전한 바인딩 업데이트를 위해 AAA를 기반으로 한다. AAA 서버에는 홈 서비스 제공자가 운영하는 AAAH와 외부 네트워크의 서비스 제공자가 운영하는 AAAF가 있다. MN은 홈 서비스 제공자에게 가입함으로써 AAAH와의 SA (Security Association)가 설정된다. 즉, AAAH에는 MN의 MIPv6 관련 파라미터인 HA(Home Agent Address), HoA 등과 함께 대칭키 KMN이 저장된다. 또한 AAAH와 AAAF 간에는 로밍협약 체결 시 SA가 설정되어 서로 송수신되는 메시지를 보호할 수 있게 된다. MN이 외부 네트워크에 처음 진입하면 MAP에 의해 제어되는 AP(Access Point) 또는 AR에 배치된 NAS(Network Access Server)로부터 인증을 받는다. 하지만 MN과 NAS 간에는 SA가 존재하지 않기 때문에 MN은 AAAF를 경유한 AAAH 간의 AAA 프로토콜을 기반으로 인증을 받아야 한다. 이 경우, AAAF는 인증자(Authenticator)의 역할을 수행하는 NAS와 인증서버 AAAH사이에서 프록시(proxy)의 기능을 수행한다. 제안프로토콜에서는 802.1x와 같은 링크 레벨에서의 인증은 언급하지 않으며, IP 레벨에서의 인증만을 고려한다.

HMIPv6를 지원하는 외부 네트워크에는 1개의 MAP과 다수의 AR로 구성된 MAP 도메인이 여러 개 존재할 수 있다. 제안 프로토콜에서는 MAP 도메인 내의 MAP과 AR 간에는 그룹키 GK_F를 분배, 관리하는 그룹키 관리기법이 존재함을 가정한다. 본 논문에서의 그룹키의 개념은 사용자의 가입과 탈퇴가 빈번한 동적인 환경에 적용되는 것이 아니라, 거의 멤버쉽 변동이 없는 정적인 환경이다. 특정 AR이 추가 또는 삭제되는 방식은 마치, 관리자가 라우터에 인증서를 설치하는 것과 같이 프로토콜 외적인 방식으로 처리가 가능하다. 따라서, GDOI와 같은 트리기반의 그룹키 관리기법 등은 필요하지 않다. 하지만 그룹키가 노출되는 경우, 프로토콜에 이상이 발생할 수 있음을 밝힌다. 새로운 MAP 도메인

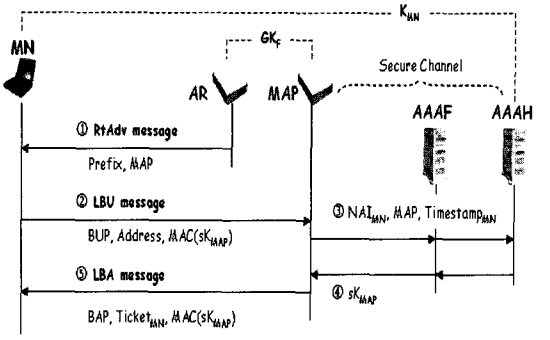
으로 진입할 때, MN은 MAP과의 성공적인 MAP 등록을 통해 MAP 도메인 내에서의 인증을 위한 인증티켓 $Ticket_{MN}$ = 〔sK_{MAP}, *RCoA*, *Exp*〕GK_F을 제공 받는다. sK_{MAP}은 안전한 Fast Handover와 LBU를 위해 사용되는 세션키이다. *RCoA*는 MAP 도메인 내에서의 MN의 CoA이고, *Exp*는 티켓의 만기(expiration)를 나타낸다. 즉, 인증티켓은 sK_{MAP}, *RCoA*, *Exp*를 대칭형 그룹키 GK_F로 암호화한 값이다.

3.2 제안 프로토콜

이번 절에서는 MN이 새로운 MAP 도메인에 처음 진입했을 때 실행되는 안전한 초기 LBU 프로토콜을 위해 개선된 HMIPv6를 소개한다. 제안 프로토콜에서 GBU 프로토콜은 언급하지 않는다. 다음에서 ','은 연결(concatenation)을 나타내고, *H*( )은 일방향 해쉬함수, *MAC*(*K*)는 선행하는 모든 필드값을 대칭키 *K*로 계산한 MAC 값, 〔*m*〕*K*는 메시지 *m*을 대칭키 *K*로 암호화한 값을 나타낸다. BUP와 BAP는 바인딩 업데이트와 바인딩 응답에 관련된 파라미터를 나타낸다. 또한 제안 프로토콜에서 개체이름은 IPv6 주소를 나타낸다.

3.2.1 MAP 등록

새로운 MAP 도메인으로 이동한 경우, MN은 현재 자신의 LCoA를 알리기 위한 목적의 초기 LBU(MAP 등록)프로토콜을 수행해야 한다. 제안 프로토콜에서는 HMIPv6에서 언급된 순번(sequence number) 대신에 MN에 의해 생성된 TimestampMN을 사용한다. 본 논문에서 Timestamp는 MN-Network간의 정확한 동기화를 필요로 하지 않으며, MN이 생성한 Timestamp은 이미 MAP/AAA에 저장되어 있는 그 이전 MN의 Timestamp와 비교를 하는 목적이다. 즉, 현재 LBU에 포함된 $Timestamp_{MN}$은 MAP/AAA에 저장된 MN의 $Timestamp_{MN}$보다 최신의 것인지를 점검한다. 순번대신 Timestamp를 이용하게 된 동기는 순번의 "Rollover"문제와 MN/MAP/AAA등에서 순번에 대한 기록이 오작동으로 인하여 삭제될 경우에 이를 복구하기 위한 추가의 조처가 필요하다는 판단에서이다. 하지만 본 논문의 Timestamp는 MAP/AAA에 이미 저장되어 있는 Timestamp가 최근에 도착한 Timestamp보다 앞선 시간의 것이라는 보장만을 원하기 때문에 앞서 기계의 오작동



〔그림 4〕 초기 LBU 프로토콜

시 순번을 사용할 때 발생하는 추가 조처는 필요하지 않다.

$$BUP = (H/M, Timestamp_{MN}, Lifetime)$$
$$BAP = (Status, Timestamp_{MN}, Lifetime)$$
$$Address = (NAI_{MN}, RCoA, LCoA)$$
$$Ticket_{MN} = \{sK_{MAP}, RCoA, Exp\}GK_F$$
$$sK_{MAP} = H(K_{MN}, NAI_{MN}, MAP, Timestamp_{MN})$$

〔그림 4〕는 안전한 초기 LBU를 위해 MN, MAP, AAA 서버들 간의 교환되는 일련의 메시지를 나타낸다. 새로운 MAP 도메인으로 이동할 경우, MN은 AR로부터 전송된 RtAdv(Router Advertisement) 메시지 (①번 메시지)에 포함된 프리픽스정보를 기반으로 *LCoA*와 *RCoA*를 설정하고, 바인딩 업데이트를 위한 파라미터, *BUP* = (*H/M*, $Timestamp_{MN}$, *Lifetime*)를 준비한다. ***M***은 해당 LBU 메시지가 MAP 등록을 위한 메시지임을 나타내기 위한 플래그(flag)이고, $Timestamp_{MN}$는 MN이 생성한 타임스탬프를 나타낸다. *Lifetime*은 해당 바인딩의 만기 전까지 남은 시간을 나타낸다. *BUP*와는 별도로 메시지에 *Address* = (NAI_{MN}, *RCoA*, *LCoA*)가 포함된다. NAI_{MN}은 MN의 NAI(Network Access Identifier)를 나타낸다. MN은 MAP과 공유해야 할 세션키 sK_{MAP}을 계산하고, BUP와 Address를 $MAC(sK_{MAP})$으로 보호한 후, 초기 LBU 메시지 (②번 메시지)를 MAP에게 전송한다.

MN과 MAP 간에는 사전에 설정된 SA가 없기 때문에, MAP은 $MAC(sK_{MAP})$을 확인하지 못한다. 따라서 MAP은 AAAF를 통해 AAAH에게 MAC을 확인할 세션키 sK_{MAP}를 생성하여 전송할 것을 요청한다. ③번 메시지에 포함된 정보를 기반으로, AAAH는 sK_{MAP}을 생

성하여 ④번 메시지를 통해서 MAP에게 전달한다. MAP은 RCoA에 대한 DAD(Duplicate Address Detection) 검사를 수행하고, $MAC(sK_{MAP})$을 확인한다. 만약 모든 테스트에 성공하면, MAP은 MN에 대한 BCE를 생성하고 인증티켓 $Ticket_{MN}=[sK_{MAP}, RCoA, Exp]GK_F$을 구성한다. MAP은 MN으로 LBA 메시지 (⑤번 메시지)를 전송한다. 메시지를 수신한 MN은 $MAC(sK_{MAP})$을 확인한 후, MAP과의 다음 LBU를 위해 sK_{MAP}과 $Ticket_{MN}$을 유지한다.

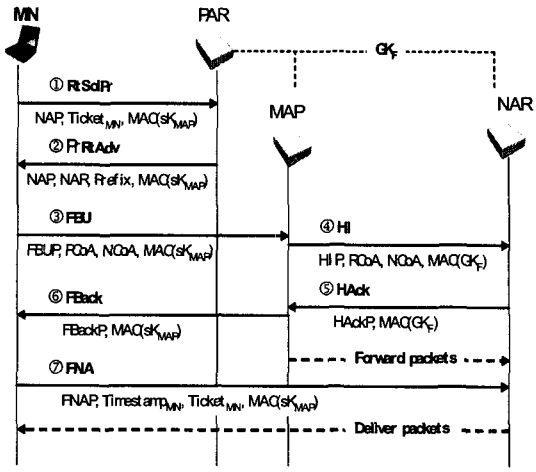
3.2.2 Fast Handover in HMIPv6

여기서는 앞에서 소개한 키 관리기법을 기반으로, HMIPv6에서도 논의된 바 있는 HMIPv6에서의 Fast Handover에 적용 가능한 인증기법을 소개한다. 모바일 노드가 두 개의 AR 사이를 이동할 때, IP 계층에서의 핸드오버 지연을 최소화하기 위해 Fast Handover 기법[15,16]이 필요하게 된다. 제안 프로토콜 설명을 위해 다음과 같은 용어를 정의한다. *NAR*은 MN의 핸드오버 이후의 라우터 NAR의 IP 주소, *PAR*은 핸드오버 이전의 라우터 PAR의 IP 주소를 나타낸다. *NAP*는 NAP(New Access Point)의 MAC 계층 주소 또는 BSSID(Base Station Subsystem ID)이다.

MN이 이동하기 시작하고, 여전히 현재의 서브넷 PAR에 연결되어 있는 상태에서, 링크 계층의 특정 메커니즘을 사용하여 새로운 AP를 발견한다고 가정하자. MN은 해당 AP가 PAR에 연결되어 있는지 또는 NAR에 연결되어 있는지 알 수가 없기 때문에 MN은 PAR로 다음과 같은 RtSolPr(Router Solicitation for Proxy Advertisement) 메시지 (①번 메시지)를 전송하여 라우터 탐색과정을 수행해야 한다.

NAP, $Ticket_{MN}$, $MAC(sK_{MAP})$

Fast Handover의 안전성 문제에 주안점을 두기위해, PAR은 NAR에 연결될 NAP의 정보를 가지고 있다고 가정한다. PAR, NAR, MAP은 GK_F를 공유하기 때문에 $Ticket_{MN}$내의 sK_{MAP}을 구할 수 있다. *Exp*를 검사하고, $MAC(sK_{MAP})$을 확인한 후, PAR은 MN으로 PrRtAdv (Proxy Router Advertisement) 메시지 (②번 메시지)를 전송한다.



[그림 5] Fast Handover in HMIPv6

FBUP = (*H*/***M***, $Timestamp_{MN}$, *Lifetime*)
FBackP = (*Status*, $Timestamp_{MN}$, *Lifetime*)
HIP = (*Code*, $Timestamp_{MAP}$)
HAckP = (*Code*, $Timestamp_{MAP}$)
FNAP = (*Code*)

②번 메시지의 의미는 NAP가 네트워크 프리픽스가 *Prefix*인 NAR에 연결되어 있음을 나타낸다. MN은 $MAC(sK_{MAP})$을 확인하고, *Prefix*를 기반으로 새로운 링크에서의 CoA인 NCoA를 계산한다. 이제 Handover의 발생이 예상된다면 MN은 PAR의 링크로부터 MAP으로 다음과 같은 FBU 메시지 (③번 메시지)를 보낸다.

FBUP, *PCoA*, *NCoA*, $MAC(sK_{MAP})$

FBUP = (*H*/***M***, $Timestamp_{MN}$, *Lifetime*)는 FBU와 관련한 파라미터로, MAP 등록일 경우에만 플래그 ***M***이 설정되며, *PCoA*는 MN의 이전 링크에서의 CoA를 나타낸다. sK_{MAP}과 이전에 MN의 BCE에 저장해 놓았던 타임스탬프를 이용하여, MAP은 $MAC(sK_{MAP})$을 확인하고, *FBUP*내의 $Timestamp_{MN}$을 검사한다. 만약 모든 검사에 성공한다면, MAP은 타임스탬프를 갱신하고 *PCoA*를 *NCoA*로 대체한다. 이후 MAP은 NAR로 HI(Handover Initiate) 메시지 (④번 메시지)를 전송한다.

HIP, *RCoA*, *NCoA*, $MAC(GK_F)$

*HIP*는 HI 메시지와 관련한 파라미터이다. HI 메시지는 NAR에게 *RCoA*로 향하는 패킷을 링크상의 *NCoA*로 포워딩해 줄 것을 요청하기 위한 목적으로 사용된다. $MAC(GK_F)$이 유효하면, NAR은 *NCoA*가 링크상에서 중복되는가에 대해 검사한다. 만약 모든 검사에 성공하면, *NCoA*로의 패킷 포워딩이 시작된다. NAR은 HI 메시지의 처리 결과를 MAP으로 알리기 위해 HAck(Handover Acknowledgement) 메시지 (⑤번 메시지)를 전송한다. HAck 메시지의 MAC을 확인한 후, MAP은 MN의 BCE에 *RCoA*와 *NCoA* 간의 바인딩을 생성하고, MN에게 FBU 메시지의 처리결과를 알리기 위해 FBack(Fast Binding Acknowledgement) 메시지 (⑥번 메시지)를 전송한다. 이 과정에서 만약 *RCoA*로 향하는 패킷이 MAP으로 도착되었다면, 해당 패킷은 NAR로 전달되고 버퍼링될 것이다. 새로운 링크로 이동하자마자, MN은 FNA 메시지 (⑦번 메시지)를 NAR로 전송하고, 해당 메시지로 인해 도착하여, 버퍼링된 패킷이 MN으로 전달되기 시작한다. FNA 메시지는 $MAC(sK_{MAP})$으로 보호되며, $Ticket_{MN}$에서 sK_{MAP}을 구한 후에 NAR에 의해 확인된다.

3.3 안전성 분석

3.3.1 위조된 RtAdv 메시지에 대한 대응

인증되지 않은 HMIPv6 과정에서 MN이 새로운 MAP 도메인으로 진입할 경우, MN은 AR로부터 전혀 보호되지 않은 RtAdv 메시지를 통해 MAP의 prefix와 IP주소를 제공받는다. 만약 MN이 MAP의 IP 대신 공격자의 IP로 위조된 RtAdv 메시지를 수신했다고 가정하자. MN은 초기 LBU 메시지를 작성하여 공격자에게로 전송하고, 공격자는 LBA 메시지를 작성하여 MN으로 전송하게 된다. 이 경우 MN으로 향하는 모든 패킷이 이동하기 전의 CoA로 전달되며, MN은 해당 패킷들을 수신하지 못하게 된다. 하지만 제안 프로토콜에서는 LBA 메시지는 MN과 MAP 간의 공유키로 계산한 MAC 값을 통해 인증 받는다. 따라서 위조된 RtAdv 메시지를 송신한 공격자는 MN과 MAP 간의 공유키 sK_{MAP}을 모르기 때문에 정당한 LBA 메시지를 작성할 수 없게 된다. 또한 만약 MN이 임의의 키를 사용하여 작성된 LBA 메시지를 수신한다면, 해당 메시지를 단지 폐기하게 된다.

3.3.2 위조된 LBU 메시지에 대한 대응

MN이 위치를 이동하여 링크주소가 변경되었을 경우 MAP으로 새로운 주소를 포함한 LBU 메시지를 전송한다. 인증과정이 전혀 수행되지 않는 일반적인 LBU 프로토콜에서는 위조된 LBU 메시지를 통해 리다이렉트 공격, 플러딩 공격 등의 DoS 공격이 발생할 수 있다. 만약 공격자가 MN의 RCoA와 함께 자신의 LCoA 또는 임의의 공격대상 호스트의 LCoA를 포함하여 위조된 LBU 메시지를 MAP으로 전송한다고 가정하자. MN으로 향하는 모든 패킷은 공격자에게 리다이렉트되거나 수신을 원치 않는 또 다른 호스트로 리다이렉트 될 것이다. 이때 공격자가 대량의 멀티미디어 스트림의 수신을 위조된 LBU 메시지를 통해 공격대상 호스트로 리다이렉트한다면 해당 호스트에 대한 플러딩 공격도 쉽게 성공할 수 있게 된다. 하지만, 제안 프로토콜에서는 LBU 메시지는 MN과 MAP 간의 공유키 sK_{MAP}으로 계산한 MAC 값을 통해 인증 받는다. 따라서 MN과 MAP 간의 공유키를 모르는 공격자는 정당한 LBU 메시지를 작성할 수 없게 된다. 또한 만약 공격자가 임의의 키를 사용하여 작성한 위조된 메시지를 송신한다면, 인증과정에서 실패하게 되므로 제안 프로토콜에서 위조된 LBU 메시지로 인한 공격은 불가능하게 된다. 위조된 LBU 메시지를 통한 DoS 공격의 경우, 공격자는 다수의 위조된 LBU 메시지를 전송하여 프로토콜 수행동안 많은 계산량을 유도하게 된다. 하지만 제안 프로토콜에서는 인증을 위해 단지 한 번의 공유키를 통한 해쉬 계산만을 수행하므로 제안 프로토콜에서 DoS 공격은 불가능하게 된다.

3.3.3 재생된 LBU 메시지에 대한 대응

기본적인 HMIPv6에 대한 재생공격은 정당한 MN이 전송한 LBU 메시지를 저장해 두었다가 일정시간이 지난 후 해당 메시지를 재생하여 MN의 이전 LCoA를 등록함으로써 MN이 서비스 받지 못하도록 하는 공격이다. 기존연구에서도 현재성(freshness)을 검사할 수 있는 속성을 포함하고 있지 않기 때문에 재생공격이 발생할 수 있다. 하지만 제안 프로토콜에서는 LBU 메시지에 현재성을 검사하기 위한 $Timestamp_{MN}$를 포함하고 있기 때문에 재생공격에 안전하다. 만약 공격자가 정당한 MN의 LBU 메시지를 저장하였다가 일정시간이 흐

른 후 재생한다고 가정하자. 해당 메시지를 수신 받은 MAP은 BUP 내의 $Timestamp_{MN}$를 통해 현재성 검사를 수행하기 때문에 위와 같은 재생공격은 성공할 수 없게 된다.

3.3.4 위조된 FBU 메시지에 대한 대응

Fast Handover 과정에서 MN의 FBU 요청을 받은 PAR은 NAR로 HI 메시지를 보내고 NAR로부터 HAck 메시지를 수신함으로써 MN의 패킷을 NAR로 전달하게 된다. 만약 MN과 PAR 간의 메시지가 인증되지 않는다고 가정하자. 공격자는 다수의 위조된 FBU 메시지를 PAR로 전송할 수 있으며, PAR은 해당 메시지를 NAR로 전달한다. NAR은 단지 DAD(Duplicate Address Detection) 테스트 후 HAck 메시지를 PAR로 전송할 것이다. 이 후 위조된 FBU 메시지에 포함된 주소로 전송되는 모든 트래픽이 NAR로 전달되며, 결국 NAR에 대한 플러딩 공격을 성공하게 된다. 하지만 제안 프로토콜에서 FBU 메시지는 초기 LBU 과정에서 MN과 MAP 간의 공유된 세션키 sK_{MAP}을 기반으로 계산한 MAC으로 인증 받는다. 따라서 MN과 MAP 간의 공유키를 모르는 공격자는 정당한 FBU 메시지를 작성할 수 없으며, 임의의 키로 작성된 메시지는 MAP에서의 인증과정에서 실패하게 된다. 따라서 제안 프로토콜에서 위조된 FBU 메시지로 인한 공격은 불가능하게 된다.

3.3.5 재생된 FBU 메시지에 대한 대응책

인증된 Fast Handover 기법이라도 정당한 MN이 송신한 FBU 메시지를 저장해 두었다가 일정시간이 지난 후 해당 메시지를 재생하는 재생공격에는 여전히 노출된다. 제안 프로토콜에서는 FBU 메시지에 현재성을 검사하기 위한 $Timestamp_{MN}$를 포함하고 있다. 따라서, 만약 공격자가 정당한 MN의 FBU 메시지를 저장하였다가 일정시간이 흐른 후 재생한다고 해도 해당 메시지를 수신 받은 MAP은 FBUP 내의 $Timestamp_{MN}$를 통해 현재성 검사를 수행하기 때문에 위와 같은 재생공격은 성공할 수 없게 된다.

3.4 성능평가

MIPv6 BU 프로토콜에 소요되는 계산량, 메시지 오버헤드는 지연에 민감한 응용환경에서는 심각한 영향을 초래할 수 있다. 따라서 BU 프로토콜에서 MIPv6 개체들 사이에 교환되는 메시지 수를 최소화하고, 계산적 오버헤드를 최소화하는 것이 바람직하다. 다음의 〔표 1〕에서는 기존 프로토콜과 제안 프로토콜을 초기 LBU와 Fast Handover 측면으로 나누어 메시지 수, 각 개체에서의 계산량, 그리고 안전성을 비교하였다. 안전성 비교에서는 앞에서 언급한 안전성 분석에서의 공격 시나리오를 대상으로 하였다. 초기 LBU 메시지 수 측면에서는 CGA 기반의 기존 프로토콜과 본 논문에서 제안하고 있는 프로토콜이 차이를 보이지 않았다. 하지만 CGA 기반 프로토콜은 서명을 이용하기 때문에 계산량이 많아지는 문제를 안고 있을 뿐만 아니라, 앞에서 언

〔표 1〕 제안된 프로토콜들의 안전성 및 효율성 비교
CGA〔7〕: CGA 기반 인증된 HMIPv6
AAA〔9〕: AAA 기반의 인증된 Fast Handover 프로토콜
DS : 전자서명 생성/확인, E/D : 암호화/복호화, Hash : 해쉬계산/확인

	초기 LBU		Fast Handover	
	CGA〔7〕	Ours	AAA〔9〕	Ours
메시지 수	5	5	13	7
MN의 계산	DS (1) E/D (2) Hash (2)	DS (0) E/D (0) Hash (2)	DS (0) E/D (3) Hash (6)	DS (0) E/D (0) Hash (5)
AR의 계산	DS (1) E/D (1) Hash (0)	DS (0) E/D (0) Hash (0)	DS (0) E/D (2) Hash (4)	DS (0) E/D (0) Hash (3)
MAP의 계산	DS (0) E/D (1) Hash (2)	DS (0) E/D (0) Hash (2)	DS (0) E/D (0) Hash (0)	DS (0) E/D (0) Hash (5)
위조된 RtAdv /PrRtAdv 메시지 공격	insecure	secure	insecure	secure
위조된 LBU /FBU 메시지 공격	insecure	secure	insecure	secure
재생공격	insecure	secure	insecure	secure

급했던 공격 시나리오에도 모두 불안전하므로, 보안상 치명적이다. 반면, 제안 프로토콜은 계산량이 많이 필요한 서명 대신에 MAC을 사용함으로써 계산량을 현저히 떨어뜨려 오버헤드를 최소화하는 장점을 가지고 있다. 물론, 제안 프로토콜 또한 MN과 AAAH간에 K_{MN}을 공유하고 있지만, AAA 서버에서 MN을 인증하는 파라미터가 존재하지 않음으로 인해, 무의미한 LBU 메시지를 대량 전송함으로써 AAA 네트워크의 트래픽 양을 증가시킬 수 있는 문제점을 가지고 있다. 하지만, 이는 일반적인 네트워크 상황에서 불가피하게 일어날 수밖에 없는 메시지 전송 및 키 확인 방법이다. 또한 제안 프로토콜의 방법을 사용함으로써 기존 네트워크의 DoS 공격을 심화시키지 않음으로, 이에 대한 언급은 하지 않는다. [9]는 제안 프로토콜과 같은 AAA를 기반으로 하고 있으나, 메시지 수 측면에서도 제안 프로토콜보다 현저히 많은 메시지 수를 가질 뿐 아니라, MAP의 계산량은 차치하고라도 제안 프로토콜이 MAC 계산만을 수행함으로써 MN과 AR에서의 계산량이 작은데 반해, [9]는 암·복호화 및 해쉬계산이 빈번이 발생함으로 비효율적이다. 또한 여러 가지 공격 시나리오에도 불안전하다. 기존 프로토콜은 위의 공격으로부터 완전한 안전성을 보장하지 않는 반면, 제안 프로토콜은 플러딩 공격과 재생공격, DoS 공격으로부터 안전성을 제공한다. 즉, 제안 프로토콜은 다양한 공격으로부터 안전성을 제공한다.

Ⅳ. 결 론

본 논문에서는 HMIPv6 환경에 Fast Handover가 통합된 환경에서 소규모 기지국에서의 효율적이고 안전한 이동성 지원을 위한 인증 메커니즘을 제안하였다. 해당 프로토콜에서는 MN이 최초의 MAP 도메인으로 진입할 때에 AAA를 도입한 HMIPv6 환경에서 초기 LBU 프로토콜을 통해 인증과정을 수행하며, 이 과정에서 인증을 위한 비밀키가 포함되어 있는 티켓을 제공받아 Fast Handover 과정에서 사용함으로써 안전한 Fast Handover 기법을 제안하였다. 또한 본 논문은 다양한 공격 시나리오를 통해 안전성을 분석하였다. 앞에서 보여준 것과 같이 본 논문의 제안 프로토콜은 다양한 공격에 안전할 뿐만 아니라, MAC을 통한 가벼운 계산량을 가짐으로써 오버헤드 측면에서도 효율적이다.

참고문헌

[1] A. Jari, J. David B., P. Charles E., Mobility Support in IPv6, RFC 3775, 2004.

[2] B. Ludovic, C. Claude, M. Karim, S. Hesham, Hierarchical Mobile IPv6(HMIPv6), RFC 4140, 2005.

[3] K. Rajeev, Fast Handovers for Mobile IPv6, RFC 4068, 2005.

[4] O. Greg, R. Michael, Child-proof Authentication for MIPv6(CAM), ACM Computer Communications Review, 31(2), July 2001.

[5] C. Claude, M. Gabriel, Statistically Unique and Cryptographically Verifiable Identifiers and Addresses, In Proc, ISOC Symposium on Network and Distributed System Security (NDSS 2002), San Diego, Feb. 2002.

[6] B. Feng, D. Robert H., Z. Jianying, Defending against Redirect Attacks in Mobile IP, IN Proc. The 9th ACM conference on Computer and Communications security, Washington D.C., Nov. 18-22, 2002.

[7] H. Wassim, K. Suresh, Combining Cryptographically Generated Address and Crypto-Based Identifiers to Secure HMIPv6, Internet Draft, draft-haddad-mipshop- hmipv6-security-06, 2006.

[8] K. James, K. Rajeev, Bootstrapping a Symmetric IPv6 Handover Key from SEND, Internet Draft, draft-kempf-mobopts-handover-key-01. txt. 2005.

[9] C. Jaejuck, J. Souhwan, Access Authentication Protocol in FMIPv6, Internet Draft, draft-jung-mipshop-access-auth-00.txt,. 2006.

[10] C. Kuntal, Y. Alper, MIP6-bootstrapping via DHCPv6 for the Integrated Scenario, Internet Draft, draft-ietf-mip6-bootstrapping-integrated-dhc-00.txt, 2005.

[11] A. Tuomas, Cryptographically Generated Addresses, RFC 3972, 2005.

[12] C. Claude, M. Gabriel, Crypto-Based Identifiers(CBID), Concepts and Applications, ACM, Transaction on Information and System Securi-

ty, Vol.7, No.1, pp. 97-127, 2004.

[13] K. HyunSun., P. ChangSeop, MIPv6 Binding Update Protocol Secure Against Both Redirect and DoS Attacks. CISC, Lecture Notes in Computer Science, Vol.3822 of LNCS, Springer-Verlag, pp. 407-418, 2005.

[14] N. Vidya, T. Hannes, V. Narayanan, Establishing Handover Keys using Shared Keys, Internet Draft, draft-vidya-mipshop-handover-keys-aaa-04.txt, Mar. 2007

[15] J. HeeYoung, K. EunAh, L. HyeongHo, Y. JongWha, A Scheme for Supporting Fast Handover in Hierarchical Mobile IPv6 Networks, ETRI Journal, vol.27, No.6, pp.798-801, Dec. 2005.

[16] J. HeeYoung, K. SeokJoo, L. JaeYong, S. Hesham, Fast Handover for Hierarchical MIPv6(F-HMIPv6), Internet Draft, draft-jung-mobopts-fhmipv6-00.txt, April 2005.

〈著者紹介〉

김 민 경 (Min-Kyoung Kim)
2003년 2월: 단국대학교 전자계산학과 졸업
2005년 9월~현재: 단국대학교 전자계산학과 석사과정
<관심분야> 보안프로토콜, 네트워크보안, IPv6

강 현 선 (Hyun-Sun Kang)
2002년 2월: 단국대학교 전자계산학과 졸업
2004년 2월: 단국대학교 전자계산학 석사
2007년 2월: 단국대학교 전자계산학 박사
2007년 3월~현재: 단국대학교 인재개발원 강의전임 강사
<관심분야> 암호이론, 보안 프로토콜, IPv6

박 창 섭 (Chang-Seop Park)
1983년: 연세대학교 경제학과 졸업
1983년: 한국 IBM 근무
1990년: 미국 Lehigh Univ. 전자계산학 박사
1990년~현재: 단국대학교 컴퓨터학부 컴퓨터과학전공 교수
<관심분야> 부호이론, 암호학