情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

고속의 안전한 Proxy Mobile IPv6 인증 메커니즘*

박 창 섭,[1†] 강 현 선[2‡]
[1]단국대학교, [2]남서울대학교

The Fast and Secure Authentication Mechanism for Proxy Mobile IPv6*

Chang-Seop Park,[1†] Hyun-Sun Kang[2‡]
[1]Dankook University, [2]Namseoul University

요 약

Proxy Mobile IPv6(PMIPv6)의 이동성 지원을 위한 시그널링 메시지에 대한 적절한 보호대책 없이는 Mobile IPv6 (MIPv6)에서와 마찬가지로 리다이렉트(redirect) 공격, MITM(Man-In-The-Middle) 공격, 재생(replay) 공격, DoS(Denial of Service) 공격 등과 같은 다양한 보안공격에 노출된다. 본 논문에서는 PMIPv6와 관련한 기존의 인증기법에 대한 연구의 문제점을 지적하고, PMIPv6에 적용가능한 신속하고 안전한 인증 메커니즘을 새로이 제안한다. 또한 제안기법과 기존연구의 비교를 통해 제안기법이 안전성과 효율성 측면에서 우수함을 보인다.

ABSTRACT

Without a proper protection mechanism for the signaling messages to be used for the mobility support in the Proxy Mobile IPv6 (PMIPv6), it is also vulnerable to several security attacks such as redirect attack, MITM (Man-In-The-Middle) attack, replay attack and DoS (Denial of Service) attack as in Mobile IPv6. In this paper, we point out some problems of previous authentication mechanisms associated with PMIPv6, and also propose a new fast and secure authentication mechanism applicable to PMIPv6. In addition, it is also shown that the proposed one is more efficient and secure than the previous ones.

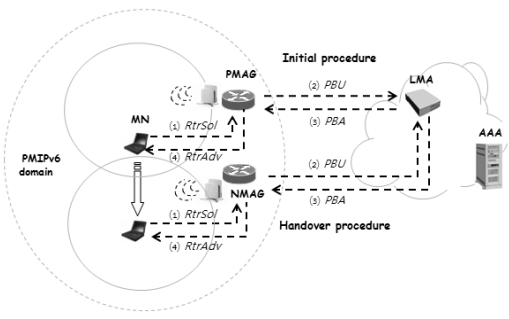
Keywords: Proxy Mobile IPv6, Handover, Security

I. 서 론

Mobile IPv6(MIPv6)[1]는 인터넷에 접속중인 모바일 노드(Mobile Node, MN)가 이동중에도 끊김없이 지속적인 서비스를 제공받을 수 있기 위한 프로토콜이다. MIPv6에서 MN은 내부에 모바일 스택을 구현해야 하고, 무선 구간에서 다수의 시그널링 메시지를 교환함으로써 이동성을 제공받는다. 하지만 이러한 과정은 성능과 자원이 한정되어 있는 모바일 노드에게 큰 부담이 되고, 이로 인해 현재 MIPv6는 실제 상용 서비스에 활용되지 못하고 있는 실정이다. 이러한 문제점을 해결하기 위해 IETF에서는 Proxy Mobile IPv6(PMIPv6)[2]를 표준화하였다. PMIPv6는 MIPv6와 같이 호스트 기반 이동성 프로토콜이 아닌 네트워크 기반 이동성 프로토콜로서, 이동성에 관련된 시그널링 메시지를 모바일 노드가 아닌 네크워크 개체들이 담당한다. PMIPv6에서 이동성을 제공하기 위한 새로운 개체로는 MAG(Mobile Access Gateway)와 LMA(Local Mobility Anchor)가 있다. MAG은 모바일 노드의 이동을 감지하고, 모바일 노드 대신 LMA와 이동성 관련 시그널링 메시지를 처리하는 역할을 담당한다. LMA는 모바일

접수일(2011년 3월 29일), 수정일(2011년 9월 5일), 게재확정일(2011년 10월 10일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2011-0002734).
† 주저자, csp0@dankook.ac.kr
‡ 교신저자, sshskang@nsu.ac.kr

노드의 이동성을 관리하며, MIPv6에서 홈 에이전트(Home Agent, HA)의 역할과 함께 PMIPv6를 지원하기 위한 추가적인 역할을 담당한다. 다음 〔그림 1〕은 PMIPv6 동작과정을 나타낸다. PMAG(Previous MAG)은 MN이 처음 PMIPv6 도메인에 진입했을 때 접속하는 MAG을, NMAG(New MAG)은 MN이 PMIPv6 도메인 내에서 이동할 경우 새롭게 접속하는 MAG을 나타낸다. MN이 처음 PMIPv6 도메인에 진입하면 초기 절차(initial procedure)를 수행한다. MN은 MAG (PMAG)으로 (1) *RtrSol*(Router Solicitation) 메시지를 전송한다. *RtrSol* 메시지는 새로운 네트워크로의 이동을 감지한 MN이 네트워크의 프리픽스 정보를 요청하기 위한 메시지를 나타낸다. MN으로부터 *RtrSol* 메시지를 수신한 MAG은 MN의 현재 위치를 등록하기 위한 (2) *PBU*(Proxy Binding Update) 메시지를 LMA로 전송한다. *PBU* 메시지를 수신한 LMA는 HNP(Home Network Prefix)를 설정하고, MN에 대한 정보를 BCE(Binding Cache Entry)에 저장하고, MAG과의 터널을 생성한다. HNP는 PMIPv6 도메인 안에서 MN이 사용하게 될 프리픽스 정보로, MN은 HNP를 기반으로 홈 주소를 설정하게 된다. LMA는 (3) *PBA*(Proxy Binding Acknowledgement) 메시지에 HNP를 포함하여 *PBU* 메시지에 대한 응답으로 MAG에게 전송한다. *PBA* 메시지를 수신한 MAG은 MN에게 (4) *RtrAdv*(Router Advertisement) 메시지를 통해 MN의 HNP를 알려주고, MN은 이를 통해 Home Address를 설정한다. 이후 MN으로 향하는 패킷들은 모두 LMA가 수신하고, 이미 생성해 놓은 터널을 통해 MAG으로 전달된다. 또한 MAG은 전달받은 패킷을 MN으로 전송한다.



〔그림 1〕 PMIPv6 동작과정

현재 PMAG에 접속중인 MN이 PMIPv6 도메인 내에서 이동하여 새로운 NMAG으로 접속할 경우 핸드오버 절차(handover procedure)를 수행한다. 초기 절차와 동일하게 먼저 MN은 NMAG으로 (1) *RtrSol* 메시지를 전송한다. MN으로부터 *RtrSol* 메시지를 수신한 NMAG은 MN의 현재 위치를 등록하기 위해 LMA에게 (2) *PBU* 메시지를 전송한다. LMA는 MN이 사용할 HNP가 포함된 (3) *PBA* 메시지로 NMAG에게 응답한다. 이 때, LMA는 MN에 대한 BCE를 생성 또는 업데이트하고, NMAG과의 터널을 생성한다. *PBA* 메시지를 수신한 NMAG은 MN에게 (4) *RtrAdv* 메시지를 통해 MN의 HNP를 알려준다. MN의 이동에 따른 핸드오버 절차는 단지 MAG과 LMA에 의해서 처리되며, MN은 초기 절차에서와 동일한 HNP를 전달받는다. 따라서, MN은 자신이 홈 링크에 연결되어 있다고 인식, 핸드오버와 관련한 어떠한 작업도 수행하지 않는다.

이와 같은 PMIPv6 환경에서 만일 이동성을 제공하기 위한 시그널링 메시지가 인증되지 않는다면 MIPv6에서와 마찬가지로〔3-5〕 공격자로부터 리다이렉트(redirect) 공격, MITM(Man-In-The-Middle) 공격, 재생(replay) 공격, DoS(Denial of Service) 공격 등 다양한 보안공격〔6〕에 노출된다. 따라서 PMIPv6 시그널링 메시지는 반드시 보호되어야 하며, 최근 이동성 지원에 대한 연구와 함께 안전한 PMIPv6를 위한 다양한 연구가 진행되고 있다〔7-12〕. 본 논문에서는 기존기법들에 대한 문제점을 지적하고, 해당 문제점을 개선한 새로운 PMIPv6 보안 메커니즘을 제안한다. 제안기법에서는 안전성과 함께 신속한 이동성 지원을 위한 시그널링 메시지 인증기법을 제안한다. 먼저 2장에서는 PMIPv6에서 발생할 수 있는 보안위협을 분석하고, 3장에서 기존연구에 대한 문제점을 지적한다. 4장에서는 제안기법의 설계원리와 동작과정을 제안한다. 5장에서는 기존기법과 제안기법을 비교, 분석하고, 6장에서 결론을 맺는다.

II. PMIPv6 보안위협

PMIPv6 개체간의 SA(Security Association)가 존재하지 않고, 시그널링 메시지가 보호되지 않으면 다양한 보안공격에 노출된다. 이번 장에서는 PMIPv6 개체 MAG과 LMA 간, MAG과 MN 간의 메시지가 보호되지 않을 경우 존재하는 보안위협을 각각 설명한다. 보안위협에는 MN의 패킷을 수신을 원치않

는 다른 주소로 리다이렉트하여 정당한 MN이 패킷을 수신할 수 없도록하는 리다이렉트 공격, 위조된 다수의 PBU 메시지를 LMA로 전송하여 LMA가 정당한 MN에 대해 정상적인 서비스를 제공하기 못하도록 하는 DoS 공격, 송수신되는 핸드오버 메시지를 공격자가 획득하여 위변조하는 MITM 공격 등이 있다.

2.1 MAG과 LMA 간의 보안위협

PMIPv6에서 MAG은 MN의 이동을 감지하고 〔그림 1〕의 (2) *PBU*, (3) *PBA* 메시지를 통해 이동된 MN의 현재 위치를 LMA에 등록하는 역할을 수행한다. 여기서 MAG과 LMA 간의 SA가 존재하지 않고, (2) *PBU*, (3) *PBA* 메시지가 보호되지 않는다면 다음과 같은 보안위협이 존재한다. 다음의 메시지 번호는 〔그림 1〕의 시그널링 메시지 번호를 나타내고, *MAGID*는 MAG의 고유한 식별자를 나타낸다.

첫째, 정당한 MAG임을 가장하는 공격자에 의해 MN에 대한 DoS 공격이 가능하다. 공격자가 MN의 트래픽을 리다이렉트하기 위해 정당한 *MAGID* 대신 위조된 *MAGID′*을 포함한 (2) *PBU* 메시지를 LMA로 전송한다고 가정하자. LMA와 MAG 간의 시그널링 메시지는 보호되지 않기 때문에, LMA는 *PBU* 메시지에 대해 확인없이 BCE의 정보를 업데이트할 것이다. 결국 MN의 트래픽은 위조된 *MAGID′*로 리다이렉트되고 MN은 트래픽을 수신하지 못하게 된다.

둘째, 정당한 MAG임을 가장하는 공격자에 의해 LMA에 대한 DoS 공격이 가능하다. 공격자가 존재하지 않는 다수의 MN에 대한 등록을 요청하기 위해 위조된 (2) *PBU* 메시지를 특정 LMA로 전송한다고 가정하자. LMA와 MAG 간의 시그널링 메시지는 보호되지 않기 때문에, LMA는 *PBU* 메시지에 대해 확인없이 존재하지 않는 MN의 정보를 BCE에 업데이트할 것이다. 결국 제한적인 LMA의 BCE는 위조된 정보로 가득 차고, LMA는 더 이상 정당한 MN에 대한 서비스가 불가능하게 된다.

셋째, 정당한 LMA를 가장한 공격자에 의해 MN에 대한 DoS 공격이 가능하다. MAG은 현재의 MN의 위치를 등록하기 위해 (2) *PBU* 메시지를 LMA로 전송한다. 이 때 공격자가 *PBU* 메시지를 도청한 후, LMA가 올바른 HNP가 포함된 (3) *PBA* 메시지로 응답하기 전에 위조된 HNP′가 포함된 *PBA* 메시지로 응답한다고 가정하자. MAG은 메시지에 대한 확인없이 (4) *RtrAdv* 메시지를 MN으로 전송하고 MN은 위조된 HNP′로 주소를 설정, 더 이상 트래픽을 수신하지 못하게 된다.

2.2 MAG과 MN 간의 보안위협

PMIPv6에서 MAG은 MN의 핸드오버 신호를 〔그림 1〕의 (1) *RtrSol* 메시지를 통해 감지하고, MN의 현재 위치를 등록하기 위한 작업을 수행한다. 또한 LMA로부터 전송받은 HNP를 MN이 (4) *RtrAdv* 메시지를 통해 수신함으로써 트래픽을 정상적으로 수신하게 된다. 여기서 MAG과 MN 간의 SA가 존재하지 않고 (1) *RtrSol*, (4) *RtrAdv* 메시지가 보호되지 않는다면 다음과 같은 보안위협이 존재한다.

첫째, MN과 다른 MAG에 접속중인 공격자에 의해 MN에 대한 DoS 공격이 가능하다. MN의 ID를 도용할 수 있는 공격자가 정당한 MN을 가장하여 MN의 핸드오버 신호인 (1) *RtrSol* 메시지를 MAG‘으로 전송한다고 가정하자. MAG과 MN 간에는 SA가 존재하지 않기 때문에 MAG'은 *RtrSol* 메시지를 받자마자 확인없이 MN에 대한 등록을 요청하기 위해 (2) *PBU* 메시지를 LMA로 전송할 것이고, *PBU* 메시지를 수신한 LMA는 BCE에 MN의 정보를 업데이트할 것이다. 결국 MN의 트래픽은 공격자에 의해 MN이 접속되지 않은 MAG‘으로 리다이렉트 되고, 결국 MN은 더 이상 트래픽을 수신받지 못하게 된다.

둘째, 정당한 MAG을 가장한 공격자에 의해 MN에 대한 DoS 공격이 가능하다. 새로운 MAG에 접속한 MN은 핸드오버를 위해 (1) *RtrSol* 메시지를 MAG으로 전송하고 MAG은 LMA로 (2) *PBU* 메시지를 전송한다. *PBU* 메시지를 수신한 LMA는 HNP를 포함한 (3) *PBA* 메시지로 응답한다. 이 때 MAG이 MN으로 HNP를 포함한 (4) *RtrAdv* 메시지를 송신하기 전에 공격자가 위조된 HNP′가 포함된 *RtrAdv* 메시지를 MN으로 응답한다고 가정하자. MN은 메시지에 대한 확인없이 위조된 HNP′로 주소를 설정하게 될 것이고, 결국 MN은 더 이상 트래픽을 수신받지 못하게 된다.

III. 기존연구

최근까지 PMIPv6 시그널링 메시지를 보호하기 위해 다양한 기법들이 제안되었다〔7-12〕. 다음의 3.1절에서는 기존연구 중 〔7〕기법의 동작과정과 문제점

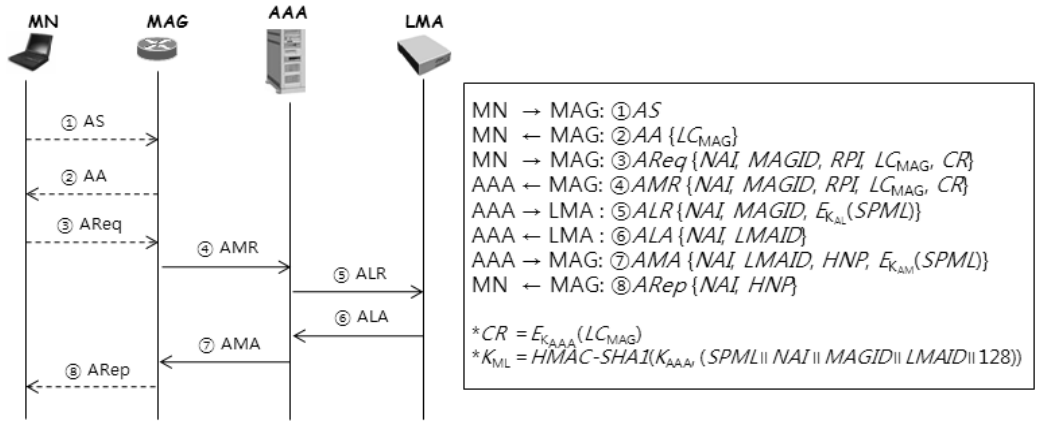
을 살펴보고, 3.2 절에서는 그 외의 기존기법들[8-12]에 대해서 살펴본다. 다음 설명에서 *HMAC_SHA1*(*K*, m)은 메시지 m에 대해서 비밀키 *K*를 이용하여 계산한 해쉬값[13]을 나타내고, '‖'은 메시지 연결 연산자를 나타낸다. E_K(m)은 메시지 m을 비밀키 *K*로 암호화한 값을, *MAC*(*K*)는 선행하는 메시지에 대해 비밀키 *K*로 계산한 MAC(Message Authentication Code) 값을 나타낸다. *NAI*, *MAGID*, *LMAID*는 각각 MN, MAG, LMA의 고유한 식별자를 나타낸다. LC_A는 A가 임의로 생성한 난수값을 나타내고, TS_A는 A의 타임스탬프(timestamp) 값을 나타낸다.

3.1 기존연구 [7]

기존기법들은 일반적으로 시그널링 메시지 보호를 위해 AAA(Authentication, Authorization, and Accounting) 서버를 기반으로 한다. [7]은 안전한 PMIPv6를 위해 AAA 서버를 기반으로 하는 방식으로, AAA 서버는 MN의 프로파일(profile)을 유지한다. 프로파일에는 MN의 HNP, 주소 설정법 등 네트워크 기반 이동성 서비스를 지원하기 위해 필요한 파라미터 등이 포함된다. AAA 서버는 MN, MAG, LMA와 각각 비밀키 K_{AAA}, K_{AM}, K_{AL}을 공유한다. 또한 동일한 PMIPv6 도메인 내의 MAG 간에는 사전에 설정된 키 K_{MAG}을 공유함을 가정한다. [7]은 처음 PMIPv6 도메인에 진입했을 때 수행하는 초기 인증절차와 동일한 PMIPv6 도메인 내에서 핸드오버할 때 수행하는 핸드오버 인증절차로 구성된다. K_{ML}은 초기 인증절차 후 MAG과 LMA 간에 동적으로 생성되는 비밀키를 나타낸다.

다음 [그림 2]는 MN이 새로운 PMIPv6 도메인에 처음 진입한 경우 수행하는 초기 인증절차를 나타낸다. 초기 인증절차를 수행함으로써 MAG은 AAA를 통해 MN을 인증하고, LMA와의 시그널링 메시지 보호에 사용될 비밀키를 분배받는다. PMIPv6 도메인으로 진입한 MN은 ① *AS*(Attendant Solicit) 메시지를 MAG으로 전송한다. *AS* 메시지를 수신한 MAG은 임의의 난수인 시도값(challenge) LC_{MAG}을 생성하여 ② *AA* (Attendant Advertise) 메시지로 응답한다. *AS*메시지와 *AA* 메시지는 각각 *RS*(Router Solicit)와 *RA*(Router Advertize) 메시지와 유사한 ICMP 메시지[14]를 나타낸다. MN은 인증 요청을 위해 ③ *AReq* (Authentication Request) 메시지를 작성하여 MAG으로 전송하고, MAG은 *AReq* 메시지를 ④ *AMR* (Aa-Mag-Request) 메시지로 구성하여 AAA로 전달한다. *AReq*와 *AMR* 메시지에서 *CR*은 MN과 AAA와의 롱텀키(long-term key) K_{AAA}로 LC_{MAG}을 암호화한 값을 나타내고, *RPI*(Replay Protection Indicator)는 재생공격을 방지하기 위한 타임스탬프 또는 임의의 난수값을 나타낸다.

AMR 메시지를 수신한 AAA는 MN과 동일한 방식으로 *CR* 값을 생성하여 전달받은 값과 동일한지를 비교한 후 MN을 인증한다. MN의 인증에 성공한 AAA는 차후 MAG과 LMA 간의 시그널링 메시지를 보호할 키인 K_{ML}을 생성한다. 키 생성에서 사용된 *SPML*은 AAA가 생성한 난수값을 나타낸다. AAA는 K_{ML} 분배를 위해 ⑤ *ALR*(Aa-Lma-Request)



[그림 2] 초기 인증절차 [7]

메시지를 작성하여 LMA로 전송하고, LMA는 ⑥ *ALA* (Aa-Lma-Answer) 메시지로 응답한다.

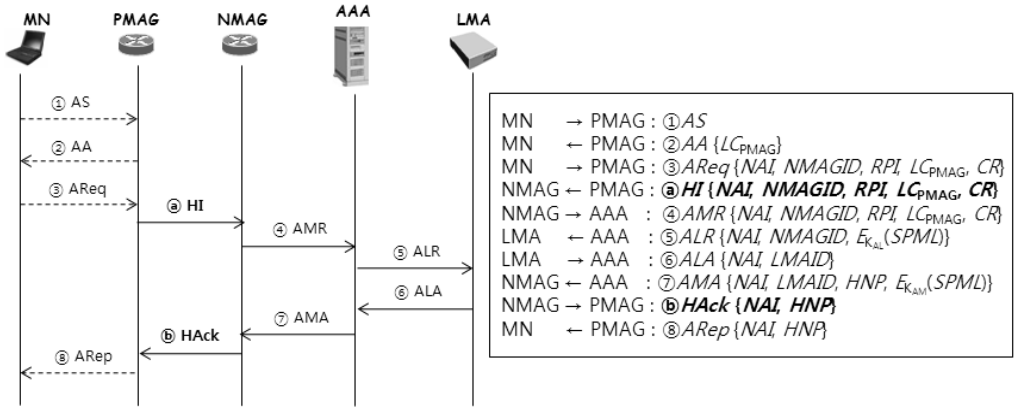
AAA는 ⑦ *AMA*(Aa-Mag-Answer) 메시지를 K_{ML} 분배를 위해 MN이 사용할 *HNP*를 포함하여 MAG으로 전송하고, MAG은 ⑧ *ARep*(Authentication Reply) 메시지를 통해 *HNP*를 MN으로 전송한다. 위의 초기 인증과정에서는 MN과 MAG 간에는 SA가 존재하지 않는다. 따라서 MN과 MAG 간의 시그널링 메시지 *AReq*와 *ARep* 메시지는 전혀 보호되지 않는다. 이와 같은 경우 공격자는 쉽게 *AReq*와 *ARep* 메시지를 위·변조하고, 2.2절에서 소개한 리다이렉트, DoS 공격 등의 보안위협에 노출된다.

다음은 MN이 PMIPv6 도메인 내에서 이동하여 새로운 NMAG으로 접속할 경우 수행하는 핸드오버 인증절차를 나타낸다. 핸드오버 인증절차를 수행함으로써 NMAG은 AAA를 통해 MN을 인증하고, LMA와의 시그널링 메시지 보호에 사용할 비밀키를 분배받는다. MIPv6에서는 MN이 새로운 라우터로 핸드오버 할 경우 등록과정에서 발생하는 지연을 최소화하기 위해 Fast MIPv6[15]를 제안하였다. PMIPv6에서도 같은 목적으로 Fast PMIPv6[16]가 제안되었다. [7]의 핸드오버 인증절차에서는 초기 인증절차에 Fast PMIPv6와 관련한 ⓐ *HI*(Handover Initiate)메시지와 ⓑ *HAck*(Handover Acknowledge)메시지가 새롭게 추가된다. 즉, MN이 NMAG으로 실제 이동을 완료하기 전에 PMAG과 NMAG 간의 *HI* 메시지와 *HAck* 메시지를 통해 NMAG은 MN의 인증과 키분배에 필요한 작업을 미리 수행하게 되며, 나머지 부분은 초기 인증절차와 동일하게 수행된다. 하지만 핸드오버 인증절차에는 안전성과 효율성 측면에서 몇 가지 문제점을 가지고 있다.

첫째, MN의 핸드오버가 발생할 때마다 AAA와 접속한다는 점이다. 이 경우 비교적 지리적으로 멀리 위치한 AAA 서버와의 접속과 메시지 송수신으로 인해 지연이 발생할 수 있으며, 이로 인해 패킷손실을 초래할 수도 있다. 둘째, 초기 인증절차와 마찬가지로 MN과 MAG 간에는 SA가 존재하지 않는다는 점이다. 따라서 MN과 MAG 간의 시그널링 메시지는 전혀 보호되지 않고, 공격자는 쉽게 해당 메시지를 위·변조, 결국 2.2절에서 소개한 리다이렉트 공격과 DoS 공격 등에 노출된다. 셋째, 불필요한 재생공격 방지 필드 *RPI*를 가진다는 점이다. *RPI*는 타임스탬프나 임의의 난수값으로 공격자로부터의 재생공격을 방지하기 위한 필드이다. 하지만 [7]에는 MAC, 암호화 등 *AReq* 메시지를 인증하기 위한 기법이 전혀 사용되지 않는다. 따라서 공격자는 *RPI* 값을 쉽게 변조할 수 있고, 결국 재생공격이 성공하게 된다.

3.2 그 외 기법들

[8]는 안전한 PMIPv6를 위해 AAA를 기반으로 하며, 등록지연으로 인한 패킷손실을 최소화시키기 위한 방법을 제안하였다. PMIPv6에서는 MN이 PMAG에서 NMAG으로 핸드오버하려고 할 때, PMAG은 LMA로 *DeReg PBU* 메시지를 송신함으로써 MN의 이동을 알린다. [8]는 이 과정에서 *DeReg*



[그림 3] 핸드오버 인증절차 [7]

*PBU*와 함께 NMAG에 대한 등록 메시지 *PBU*를 함께 전송함으로써 등록지연을 방지한다. 이후 NMAG은 MN이 접속하면 AAA를 통해 MN의 인증과정을 수행한다.

〔8〕는 *PBU* 메시지를 미리 처리함으로써 등록지연을 어느 정도는 감소시킬 수 있으나, 핸드오버마다 AAA 서버와의 접속으로 인해 여전히 지연이 발생하고, 결국 패킷손실이 발생한다는 문제점을 가지고 있다. 〔9〕는 AAA 서버를 기반으로 하는 방식으로, AAA 접속으로 인한 지연을 최소화하고자 유효기간이 설정된 티켓(ticket)〔17〕을 사용한다. 유효기간이 설정된 티켓 내에는 인증을 위한 키가 암호화되어 있는데, 티켓의 유효기간 내에는 모든 라우터들이 티켓 내의 동일한 키로 인증과정을 수행하게 된다. 이 경우 티켓 내의 인증키가 노출될 경우 backward / forward security가 보장되지 않는다는 문제점을 가지고 있다. 또한 티켓의 유효기간이 경과되면 또 다시 AAA 서버에 접속해야 한다는 근본적인 문제점은 여전히 남아 있으며, 적절한 유효기간 설정의 어려움을 가지고 있다. 〔10〕는 MN을 인증하기 위해 MNID를 일회용(one-time) 키로 사용하며, 이동성 제공을 위한 새로운 개체 L-LMA와 H-LMA를 정의해서 사용한다. MN이 새로운 MAG에 접속하면 MN의 Device ID와 타임스탬프를 기반으로 One-time key를 생성, HNP, Device ID와 함께 MNID로 구성하여 MAG으로 전송한다. 전송된 MNID는 H-LMA로 전송되어 MN을 인증하는데 사용된다. 이 기법은 MN과 H-LMA가 인증을 위한 MNID를 정확히 생성하기 위한 동기화의 어려움이 있으며, L-LMA와 H-LMA 간에 PKI를 기반으로 통신한다는 문제점이 있다. 〔11〕에서는 PMIPv6 환경에서 AAA 서버를 활용한 평문, 해쉬, 암호화에 기반한 인증방법을 제시하고 이에 따른 성능분석을 한다. 하지만 구체적인 PMIPv6 절차와 키관리기법 등은 제공되지 않는다. 〔12〕에서는 PMIPv6 기반의 global mobility를 위한 아키텍처와 프로토콜을 제안하였다. 해당 기법의 관리 도메인은 core 네트워크와 몇몇의 access 네트워크로 구성되어 있으며, access 네트워크는 PMIPv6 도메인을 나타낸다. 제안기법이 하나의 PMIPv6 도메인에서의 local mobility를 위한 기법인데 반해, 〔12〕는 여러개의 PMIPv6 도메인간의 global mobility를 위한 기법이다.

IV. 제안기법

제안기법에는 MN이 처음 PMIPv6 도메인에 진입했을 때 수행하는 초기 인증절차와 MN이 이동으로 핸드오버가 발생했을 때 수행하는 핸드오버 인증절차가 있다. 초기 인증절차를 수행함으로써 MAG은 AAA를 통해 MN을 인증하고, MN과의 시그널링 메시지 보호에 사용될 비밀키를 분배받는다. 또한 MAG은 LMA와의 시그널링 메시지 보호에 사용될 비밀키를 분배받는다. 핸드오버 인증절차를 수행함으로써 NMAG은 LMA로부터 LMA와의 시그널링 메시지 보호에 사용될 비밀키와 MN과의 시그널링 메시지 보호를 위한 비밀키를 분배받는다. 다음 절에서는 제안기법의 설계원리와 초기 인증절차, 핸드오버 인증절차를 자세히 살펴본다. 제안기법의 설명에 사용하는 모든 표기는 3장에서 사용한 것과 동일하게 사용된다.

4.1 설계원리

본 논문에서는 신속하고 안전한 PMIPv6을 위해 다음과 같은 설계원리를 가진다.

첫째, 제안기법에서 AAA는 초기 인증절차에서 단 한번만 접속한다. 〔7〕에서는 MAG과 LMA 간의 비밀키 공유를 위해 초기 인증절차와 핸드오버 인증절차마다 AAA에 접속한다. 제안기법에서는 핸드오버 인증절차에서는 LMA가 키분배 역할을 수행함으로써 AAA 접속으로 인한 지연을 방지할 수 있다. AAA와 MN, MAG, LMA 간의 사전에 공유한 long-term 키는 〔7〕과 동일하고, 같은 PMIPv6 도메인 내의 MAG 간에는 사전에 공유된 K_{MAG}과 함께 MAG 간의 암호화 공개키를 공유함을 가정으로 한다. 예를 들면, PMAG과 NMAG의 경우 PMAG은 NMAG의 암호화 공개키 PK_{NMAG}을, NMAG은 PMAG의 암호화 공개키 PK_{PMAG}을 사전에 공유한다. 둘째, 제안기법에서는 MAG과 MN 간의 SA를 설정하여 MAG과 MN 간의 시그널링 메시지를 보호한다. 〔7〕을 포함한 대부분의 기존연구에서는 MAG과 MN 간의 SA는 존재하지 않으며, MAG과 MN 간의 시그널링 메시지가 보호되지 않는다. 따라서, 2.2절에서 소개한 다양한 공격에 노출된다. 반면 제안기법에서는 MN과 MAG 간의 시그널링 메시지에 MAC 값을 첨부하여 전송함으로써 2.2절의 다양한 공격에 대응적이다. 셋째, 제안기법에서는 개체간 시그널링 메시지 보호를

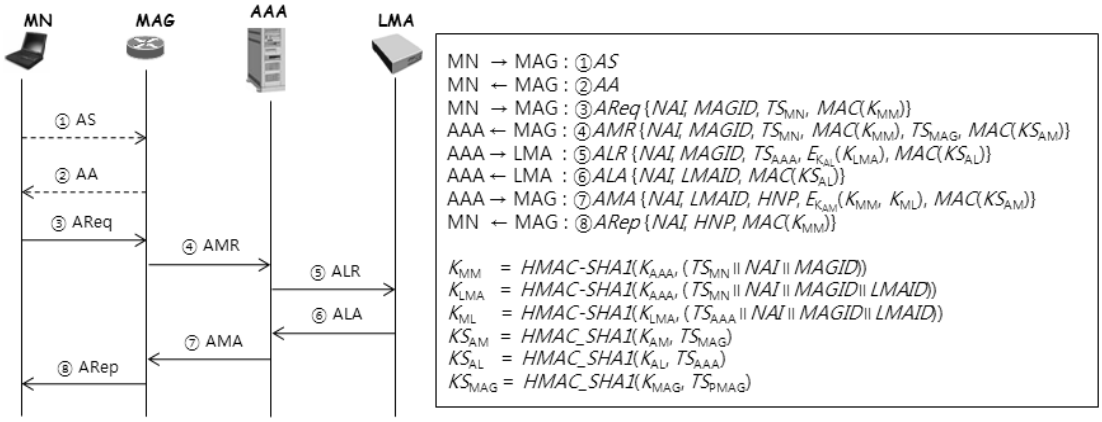
위해 long-term 키 대신 세션키를 사용한다. 즉, long-term 키를 사용하는 대신 long-term 키와 타임스탬프를 기반으로 생성한 세션키를 사용한다. 따라서 특정 세션키가 노출되더라도 전후 세션키 노출의 도미노(domino) 효과를 막을 수 있다. 반면 〔7〕에서는 개체간에 사전에 설정된 long-term 키를 지속적으로 사용한다. 넷째, 〔7〕에서는 재생공격에 대응하기 위해 난수를 사용하는 반면, 제안기법에서는 타임스탬프를 사용한다. 제안기법에서 사용하는 타임스탬프는 순번의 개념으로 사용되기 때문에 개체간 엄격한 동기화는 필요하지 않다. 타임스탬프를 수신하는 개체는 공유된 키정보와 함께 타임스탬프 값을 함께 저장, 관리해야 하고, 새로운 타임스탬프를 수신할 경우 저장된 타임스탬프와 비교하여 최신값인지를 확인하고, 최신값으로 갱신해야 한다.

4.2 초기 인증절차

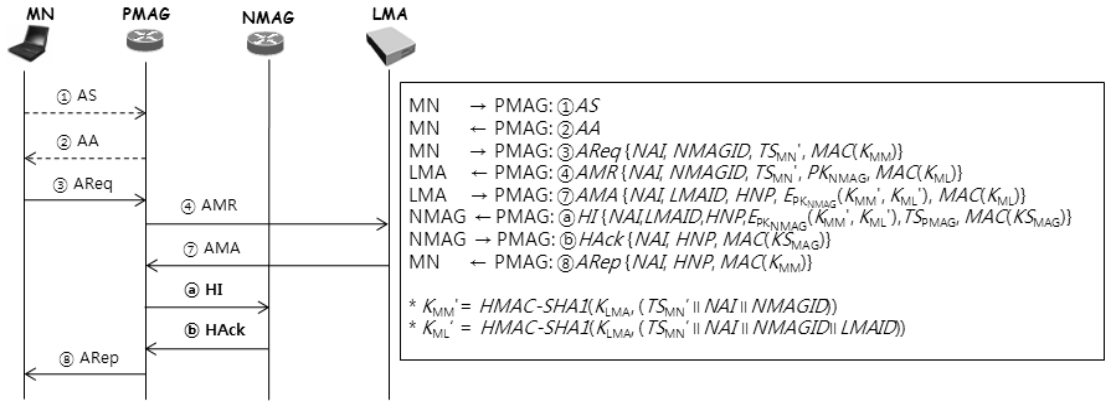
다음의 〔그림 4〕는 MN이 새로운 PMIPv6 도메인에 처음 진입한 경우 수행하는 초기 인증절차를 나타낸다. 초기 인증절차를 수행함으로써 MAG은 AAA를 통해 MN을 인증하고, MN과의 시그널링 메시지 보호에 사용될 비밀키 K_{MM}을 분배받는다. 또한 MAG은 LMA와의 시그널링 메시지 보호에 사용될 비밀키 K_{ML}를 분배받는다. K_{ML}은 MN의 현재 위치를 LMA에 등록하기 위한 *PBU/PBA* 메시지 보호를 위해 사용된다. AAA는 초기 인증절차에서 K_{LMA}를 LMA로 전달하고, 이로써 핸드오버 인증절차에서는 LMA가 AAA를 대신하여 키분배의 역할을 수행하게 된다.

MN이 처음 PMIPv6 도메인으로 진입하면 MN은 MAG으로 ① *AS* 메시지를 전송하고, MAG은 ② *AA* 메시지로 응답한다.

MN은 타임스탬프 TS_{MN}을 선택하고 K_{MM}을 생성한 후 ③ *AReq* 메시지를 작성하여 MAG으로 전송한다. 여기서 TS_{MN}은 순번과 유사하게 사용되는 타임스탬프 값을 나타낸다. *AReq* 메시지를 수신한 MAG은 TS_{MAG}을 선택하고 AAA와의 세션키 KS_{AM}을 생성한 후, ④ *AMR* 메시지를 작성하여 AAA 서버로 전달한다. *AMR* 메시지를 수신한 AAA는 MN과 동일한 방식으로 K_{MM}을 생성하여 MN을 인증한다. 이어서 MAG으로부터 수신받은 TS_{MAG}으로 세션키 KS_{AM}을 생성하여 수신한 메시지를 인증한다. 인증에 성공한 AAA 서버는 차후 MAG과 LMA 간의 시그널링 메시지를 보호할 키인 K_{ML}을 생성한다. AAA 서버는 TS_{AAA}를 선택하여 LMA와의 세션키 KS_{AL}을 생성한 후, ⑤ *ALR* 메시지를 작성, K_{LMA}를 K_{AL}로 암호화하여 LMA로 전달한다. K_{LMA}는 차후 핸드오버 인증절차에서 K_{MM}'와 K_{ML}'를 생성하기 위한 마스터 키로 사용된다. LMA는 K_{LMA}를 저장하고, AAA 서버로부터 수신받은 TS_{AAA}로 세션키 KS_{AL}을 생성하여 수신한 메시지를 인증하고, MAG과의 비밀키 K_{ML}을 생성한다. 이 후, LMA는 ⑥ *ALA* 메시지를 AAA로 전송함으로써 *ALR* 메시지에 응답한다. AAA는 MN과 MAG, LMA와 MAG이 공유할 키인 K_{MM}과 K_{ML}을 K_{AM}으로 암호화한 후, MN이 사용하게 될 *HNP*와 함께 ⑦ *AMA* 메시지를 MAG으로 전송한다. *AMA* 메시지를 수신한 MAG은 K_{AM}으로 암호화된 키를 복호화하여 K_{MM}과 K_{ML}을 공유하고, 이



〔그림 4〕 초기 인증절차 〔제안기법〕



〔그림 5〕 핸드오버 인증절차〔제안기법〕

시점에서 MAG은 MN을 간접적으로 인증하게 된다. MAG은 ⑧ *ARep* 메시지를 통해 *HNP*를 MN으로 전송한다.

4.3 핸드오버 인증절차

위의 그림은 PMIPv6 도메인 내에서 이동하여 새로운 NMAG으로 접속할 경우 수행하는 핸드오버 인증절차를 나타낸다. 핸드오버 인증절차를 수행함으로써 NMAG은 LMA로부터 LMA와의 시그널링 메시지 보호에 사용될 비밀키 K_{ML}'와 MN과의 시그널링 메시지 보호를 위한 비밀키 K_{MM}'를 분배받는다. 즉, 제안기법의 핸드오버 인증절차에서는 LMA가 AAA 역할을 수행함으로써 AAA와 전혀 접속하지 않는다. 제안기법에서는 MN이 PMAG에서 NMAG으로 핸드오버가 예상될 때, 등록지연과 피킷손실을 최소화하기 위해 Fast PMIPv6와 관련한 ⓐ *HI* 메시지와 ⓑ *HAck* 메시지를 사용한다. 즉, MN이 NMAG으로 실제 이동을 완료하기 전에 PMAG과 NMAG의 *HI* 메시지와 *HAck* 메시지를 통해 NMAG은 키분배에 필요한 작업을 미리 수행하게 된다.

먼저 MN은 MAG으로 ① *AS* 메시지를 전송하고, MAG은 ② *AA* 메시지로 응답한다. MN은 TS_{MN}'를 선택하고 K_{MM}'를 생성한 후 ③ *AReq* 메시지를 작성하여 MAG으로 전송한다. *AReq* 메시지를 수신한 PMAG은 TS_{MN}'과 NMAG의 암호화 공개키 PK_{NMAG}을 포함한 ④ *AMR* 메시지를 작성, 키 K_{ML}로 계산한 MAC 값과 함께 LMA로 전송한다.

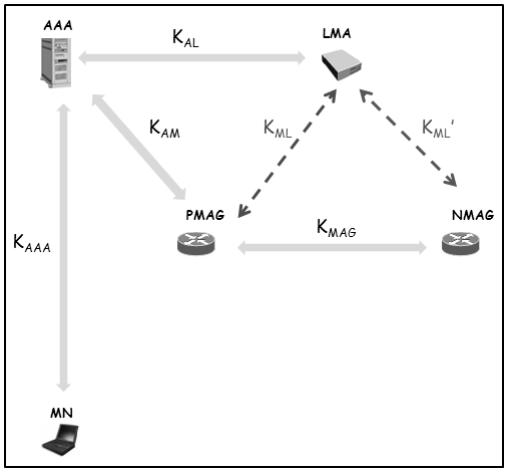
AMR 메시지를 수신한 LMA는 MN과 NMAG이 공유할 키 K_{MM}'를 생성하고, NMAG과 LMA가 공유할 키 K_{ML}'를 생성한 후 NMAG의 암호화 공개키를 이용하여 암호화한 ⑦ *AMA* 메시지를 PMAG으로 전송한다.

PMAG은 TS_{PMAG}을 선택하여 KS_{MAG}을 생성한 후, LMA로부터 수신한 암호화된 새로운 키를 포함한 ⓐ *HI* 메시지를 NMAG으로 전송한다. NMAG은 PMAG으로부터 수신한 TS_{PMAG}을 이용하여 KS_{MAG}을 생성한 후, *HI* 메시지를 인증한다. 인증에 성공하면 NMAG은 암호화된 키를 복호화하고, *HI* 메시지에 대한 응답으로 ⓑ *HAck* 메시지를 PMAG으로 전송한다.

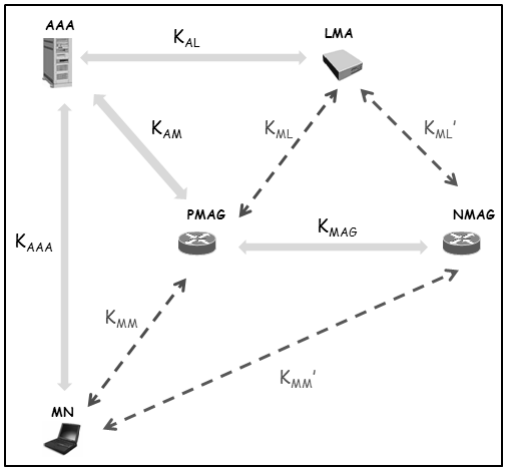
V. 비교분석

5.1 키관리 비교

다음 그림은 〔7〕과 제안기법의 키 관리 기법을 나타낸다. 굵은선으로 표시된 부분은 사전에 공유된 SA를 나타내고, 점선으로 표시된 부분은 인증절차에 의해 공유된 SA를 나타낸다. 〔7〕과 제안기법에서는 AAA와 LMA, AAA와 PMAG, PMAG과 NMAG, AAA와 MN 간에는 사전에 공유된 long-term 키 K_{AL}, K_{AM}, K_{MAG}, K_{AAA}를 사용한다. 〔7〕에서는 모든 핸드오버마다 long-term 키를 지속적으로 사용하는 반면, 제안기법에서는 long-term 키와 타임스탬프를 기반으로 생성한 세션키를 사용한다. 오른쪽의 제안기법에서는 K_{AL}, K_{AM}, K_{MAG}을 기반으로 핸드오버마다 새로운 세션키를 생성(〔표 1〕), 시그널링 메시



〔그림 6-1〕 키관리 기법〔7〕



〔그림 6-2〕 키관리 기법〔제안기법〕

지 보호에 사용한다. 이로써 특정 키가 노출되더라도 long-term 키는 안전하다. 다음 그림에서 〔7〕은 인증절차를 통해 MAG과 LMA 간의 SA만을 설정, 개체간 시그널링 메시지 보호에 사용한다.

MAG과 MN 간에는 SA가 존재하지 않으며 따라서 시그널링 메시지는 보호되지 않는다. 반면 제안기법에서는 MAG과 LMA 간의 SA 뿐만 아니라, MAG과 MN 간의 SA를 설정하여 개체간 시그널링 메시지를 보호한다. 즉, 〔7〕은 2.2절에서 소개한 MAG과 MN 간의 보안위협이 존재하고, 제안기법은 MAG과 MN 간의 보안위협으로부터 안전하다. 다음은 〔7〕과 제안기법의 키 생성법을 나타낸다.

5.2 안전성 분석

이번 절에서는 제안기법과 기존연구의 안전성을 분석, 비교한다. 제안기법에서는 MAG과 LMA, MAG과 MN 간의 비밀키를 통해 개체간 시그널링 메시지를 보호한다.

LMA와 MAG, MN과 MAG은 초기 인증절차를 통해 각각 K_{ML}과 K_{MM}을 공유하여 개체간 시그널링 메시지 보호에 사용한다. K_{ML}'와 K_{MM}'는 핸드오버 인증절차 후 LMA와 MAG, MN과 MAG 간에 동적으로 생성되는 키를 나타낸다.

제안기법에서는 리다이렉트 공격이 불가능하다. 리다이렉트 공격에 성공하기 위해서는 공격자가 *RtrSol* 메시지 또는 *PBU* 메시지를 위조해야 한다. 하지만 제안기법에서는 MN과 MAG, MAG과 LMA 간에는 각각 비밀키 K_{MM}과 K_{ML}을 공유하고, 해당 비밀키로 계산한 $MAC(K_{MM})$과 $MAC(K_{ML})$를 통해 개체간 시그널링 메시지가 보호된다. 따라서 비밀키를 모르는 공격자는 위조한 메시지에 대한 정확한 MAC 값을 계산할 수 없고, 결국 리다이렉트 공격에 실패한다.

〔표 1〕 키 생성 방법

구분	키 생성법
〔7〕	$K_{ML} = HMAC\text{-}SHA1(K_{AAA}, (SPML \| NAI \| PMAGID \| LMAID \| 128))$ $K_{ML}' = HMAC\text{-}SHA1(K_{AAA}, (SPML \| NAI \| NMAGID \| LMAID \| 128))$
제안기법	$K_{MM} = HMAC\text{-}SHA1(K_{AAA}, (TS_{MN} \| NAI \| MAGID))$ $K_{ML} = HMAC\text{-}SHA1(K_{LMA}, (TS_{AAA} \| NAI \| MAGID \| LMAID))$ $K_{LMA} = HMAC\text{-}SHA1(K_{AAA}, (TS_{MN} \| NAI \| MAGID \| LMAID))$ $K_{MM}' = HMAC\text{-}SHA1(K_{LMA}, (TS_{MN}' \| NAI \| NMAGID))$ $K_{ML}' = HMAC\text{-}SHA1(K_{LMA}, (TS_{MN}' \| NAI \| NMAGID \| LMAID))$ $KS_{AM} = HMAC\text{-}SHA1(K_{AM}, TS_{MAG})$ $KS_{AL} = HMAC\text{-}SHA1(K_{AL}, TS_{AAA})$ $KS_{MAG} = HMAC\text{-}SHA1(K_{MAG}, TS_{PMAG})$

〔표 2〕 안전성 비교

구분	Redirect공격 대응	DoS공격 대응	재생공격 대응	MITM공격 대응
〔7〕	○	X	X	X
〔8〕	X	X	X	X
〔9〕	X	X	○	○
〔10〕	○	X	○	X
〔11〕	X	X	X	X
〔proposed〕	○	○	○	○

제안기법에서는 DoS 공격이 불가능하다. LMA를 대상으로 하는 DoS 공격이 성공하기 위해서는 정당한 MAG임을 가장하는 공격자가 존재하지 않는 다수의 MN에 대한 *PBU* 메시지를 위조하거나 다수의 정당한 *PBU* 메시지를 도청, 저장하였다가 재송신해야 한다. 하지만 제안기법에서는 MAG과 LMA 간에 비밀키 K_{ML}을 공유하고, 해당 비밀키로 계산한 $MAC(K_{ML})$를 통해 개체간 시그널링 메시지가 보호되기 때문에 비밀키를 모르는 공격자는 정확한 MAC 값을 계산할 수 없고, 결국 DoS 공격에 실패한다. 반면 〔7〕, 〔10〕에서는 MAG과 MN 간의 비밀키가 존재하지 않으므로 개체간 시그널링 메시지를 보호하지 못한다. 〔9〕에서는 MAG과 MN 간에는 SA가 존재하지만 MAG과 LMA 간의 SA가 존재하지 않아서 2.1절에서 언급한 DoS 공격과 리다이렉트 공격에 취약하며, 〔8〕, 〔11〕에서는 MAG과 MN, MAG과 LMA 간의 SA가 전혀 존재하지 않기 때문에 DoS 공격과 리다이렉트 공격 등 2장에서 언급한 모든 보안 공격에 취약하다.

제안기법의 PMIPv6 시그널링 메시지에는 타임스탬프가 포함된다. 제안기법에서 타임스탬프는 앞의 설명과 같이 세션키 생성의 목적으로 사용되기도 하지만, 시그널링 메시지의 재생공격을 방지하기 위한 목적으로도 사용된다. 각 시그널링 메시지는 선행하는 메시지에 대한 MAC 값을 포함하고 있기 때문에 타임스탬프 값을 변조하는 것은 불가능하다. 따라서 타임스탬프를 포함한 시그널링 메시지로 재생공격이 불가능하게 된다. 반면 〔7〕은 재생공격을 방지하기 위한 타임스탬프를 사용하기는 하지만 메시지 인증을 위한 어떠한 인증방법도 제공하지 않기 때문에, 쉽게 타임스탬프 값의 변경이나 메시지 위조가 가능하고, 결국 재생공격과 MITM 공격이 가능하게 된다. 〔9〕, 〔10〕에서는 재생공격에 대응하기 위해 타임스탬프를 사용한다. 제안기법과에서는 타임스탬프가 순번의 개념으로 사용되므로 동기화가 불필요한 반면 〔9〕, 〔10〕에서는 반드시 동기화가 되어야 한다는 어려움이 있다. 〔8〕, 〔11〕에서는 재생공격에 대응하기 위한 어떠한 방법도 제공되지 않기 때문에 재생공격과 MITM 공격이 가능하게 된다.

본 논문에서는 AAA와 LMA, AAA와 PMAG, PMAG과 NMAG 간의 메시지를 보호하기 위해 사전에 공유한 long-term 키를 사용하는 대신 long-term 키와 타임스탬프를 기반으로 생성한 세션키를 사용한다. 즉, long-term 키를 기반으로 각 개체간 세션키가 생성되므로 특정 세션키가 노출되더라도 전후 세션키 노출의 도미노 효과를 막을 수 있다. 반면, 기존연구 〔7-11〕에서는 세션키가 사용되지 않는다.

5.3 성능분석

5.3.1 성능분석 모델

본 논문에서는 성능평가를 위해 육각 네트워크 모델과 FF(Fluid Flow) 이동모델〔11,19〕을 사용한다. 육각 네트워크 모델은 육각 셀들로 이루어져 있는데, 가장 안쪽 셀인 0번 셀을 중심 셀(center cell)이라고 하고, 중심 셀을 둘러 싼 첫 번째 ring 셀들의 라벨은 1이다. $r(r\geq 1)$을 ring의 라벨이라고 할 때 각 ring은 $6r$개의 셀들로 구성된다. 본 논문에서는 k ring으로 구성된 육각 네트워크 모델을 PMIPv6 도메인으로, 각 셀은 MN이 이동 가능한 서브넷으로 가정한다. k를 ring의 개수, R을 육각 셀 한변의 길이라고 할 때, PMIPv6 도메인의 전체 셀의 수 $N(k)$, 둘레 $L(k)$, 면적 $S(k)$는 다음과 같이 나타낸다〔11,19〕.

$$N(k) = \sum_{r=1}^{k}(6r+1) \quad (1)$$

$$L(k) = (12k + 6) \cdot R \quad (2)$$

$$S(k) = (2.6 \cdot R^2) \cdot (3k \cdot (k + 1) + 1) \quad (3)$$

〔표 3〕 초기 인증비용 / 핸드오버 인증비용

$I_{[7]} = 2H_{\text{MN-MAG}}C_{\text{wireless}} + 2H_{\text{MAG-AAA}}C_{\text{wired}} + 2H_{\text{AAA-LMA}}C_{\text{wired}} + P_{\text{MN}} + P_{\text{MAG}} + P_{\text{AAA}} + P_{\text{LMA}}$ $P_{\text{MN}} = C_{\text{enc}}$ $P_{\text{MAG}} = C_{\text{dec}} + C_{\text{key}}$ $P_{\text{AAA}} = 2C_{\text{enc}} + C_{\text{dec}} + C_{\text{key}}$ $P_{\text{LMA}} = C_{\text{dec}} + C_{\text{key}}$	$I_{\text{proposed}} = 2H_{\text{MN-MAG}}C_{\text{wireless}} + 2H_{\text{MAG-AAA}}C_{\text{wired}} + 2H_{\text{AAA-LMA}}C_{\text{wired}} + P_{\text{MN}} + P_{\text{MAG}} + P_{\text{AAA}} + P_{\text{LMA}}$ $P_{\text{MN}} = C_{\text{hash}} + C_{\text{veri}} + C_{\text{key}}$ $P_{\text{MAG}} = 2C_{\text{hash}} + 2C_{\text{veri}} + C_{\text{enc}} + C_{\text{key}}$ $P_{\text{AAA}} = 2C_{\text{hash}} + 2C_{\text{veri}} + 3C_{\text{enc}} + 3C_{\text{key}}$ $P_{\text{LMA}} = 2C_{\text{key}} + C_{\text{hash}} + C_{\text{veri}} + C_{\text{dec}}$
$C_{[7]} = 2H_{\text{MN-MAG}}C_{\text{wireless}} + 2H_{\text{PMAG-NMAG}}C_{\text{wired}} + 2H_{\text{MAG-AAA}}C_{\text{wired}} + 2H_{\text{AAA-LMA}}C_{\text{wired}} + P_{\text{MN}} + P_{\text{NMAG}} + P_{\text{AAA}} + P_{\text{LMA}}$ $P_{\text{MN}} = C_{\text{enc}}$ $P_{\text{NMAG}} = C_{\text{dec}} + C_{\text{key}}$ $P_{\text{AAA}} = 2C_{\text{enc}} + C_{\text{dec}} + C_{\text{key}}$ $P_{\text{LMA}} = C_{\text{dec}} + C_{\text{key}}$	$C_{\text{proposed}} = 2H_{\text{MN-MAG}}C_{\text{wireless}} + 2H_{\text{MAG-LMA}}C_{\text{wired}} + 2H_{\text{PMAG-NMAG}}C_{\text{wired}} + P_{\text{MN}} + P_{\text{PMAG}} + P_{\text{NMAG}} + P_{\text{LMA}}$ $P_{\text{MN}} = C_{\text{hash}} + C_{\text{veri}} + C_{\text{key}}$ $P_{\text{PMAG}} = 2C_{\text{hash}} + 2C_{\text{veri}} + C_{\text{enc}}$ $P_{\text{NMAG}} = C_{\text{hash}} + C_{\text{veri}} + C_{\text{dec}}$ $P_{\text{LMA}} = 2C_{\text{key}} + C_{\text{hash}} + C_{\text{veri}} + C_{\text{enc}}$
$AC_{[7]} = (\lambda_i \cdot C_{[7]}) + I_{[7]}$	$AC_{\text{proposed}} = (\lambda_i \cdot C_{\text{proposed}}) + I_{\text{proposed}}$

PMIPv6에서 MN이 다른 서브넷으로 이동할 경우 핸드오버가 발생하는데, MN의 핸드오버율은 MN의 이동패턴과 밀접한 관련이 있다. FF 이동모델〔11,19〕을 가정할 때, 주어진 PMIPv6 도메인에서 average cell crossing rate λ_i는 average handover rate와 동일하다〔11,19〕. v는 MN의 평균 이동속도를 나타낸다. i는 사용자 그룹을 나타내는데, 본 논문에서는 이동 속도에 따라 사용자 그룹을 보행자 그룹(pu)과 차량 그룹(vu)〔11〕으로 각각 구분하여 인증비용을 분석한다.

$$\lambda_i = \frac{v \cdot L(k)}{\pi \cdot S(k)} \quad (4)$$

5.3.2 인증비용 분석

본 논문에서 성능비교를 위한 인증비용의 계산은 일련의 핸드오버 인증절차 처리에 요구되는 유, 무선에서의 시그널링 메시지 전송비용과 처리비용의 합계로 계산한다. 인증기법 j에 대해 초기 인증절차에서 소요되는 유, 무선상에서의 시그널링 메시지 전송비용을 $I_{j,s}$, 처리비용을 $I_{j,p}$라고 하고, 초기 인증절차로 인한 인증비용을 I_j라고 하자. 인증기법 j에 대해 핸드오버 절차에서 소요되는 유, 무선상에서의 시그널링 메시지 전송비용을 $C_{j,s}$, 처리비용을 $C_{j,p}$라고 하고, 핸드오버로 인한 인증비용을 C_j라고 하자. 이 때, I_j와 C_j는 다음의 식과 같이 계산된다. 또한 인증기법 j에 대한 단위 시간당 평균 핸드오버 인증비용 AC_j는 핸드오버 인증비용에 단위 시간당 핸드오버율을 곱한값에 초기 인증비용을 더한 값으로 계산된다.

$$I_j = (I_{j,s} + I_{j,p}) \quad (5)$$

$$C_j = (C_{j,s} + C_{j,p}) \quad (6)$$

$$AC_j = (\lambda_i \cdot C_j) + I_j \quad (7)$$

C_{wired}를 유선구간의 전송비용, C_{wireless}를 무선구간의 전송비용, $H_{\text{MN-MAG}}$를 MN과 MAG 간의 홉수, $H_{\text{MAG-LMA}}$를 MAG과 LMA 간의 홉수, $H_{\text{PMAG-NMAG}}$를 PMAG과 NMAG 간의 홉수, $H_{\text{AAA-LMA}}$를 AAA와 LMA 간의 홉수, $H_{\text{MAG-AAA}}$를 MAG과 AAA 간의 홉수라고 하자. P_{MN}, P_{PMAG}, P_{NMAG}, P_{LMA}, P_{AAA}를 각각 MN, NMAG, LMA, AAA의 처리비용이라고 할 때, 기존기법과 제안기법의 초기 인증비용 I_j와 핸드오버 인증비용은 인증비용 C_j와 단위 시간당 평균 핸드오버 인증비용 AC_j는 〔표 3〕과 같이 계산된다.

5.3.3 수치결과

다음의 〔표 4〕는 인증비용과 단위시간당 평균 핸드오버 비용을 계산하기 위해 사용되는 실제 파라미터 값을 나타낸다. 유선과 무선의 전송비용과 MAC 생성/확인 비용, 암호화/복호화 비용, 키생성 비용 등은

각 작업에 소요되는 비용을 토대로 비교를 위해 설정한 상대적인 값을 나타낸다[9,11].

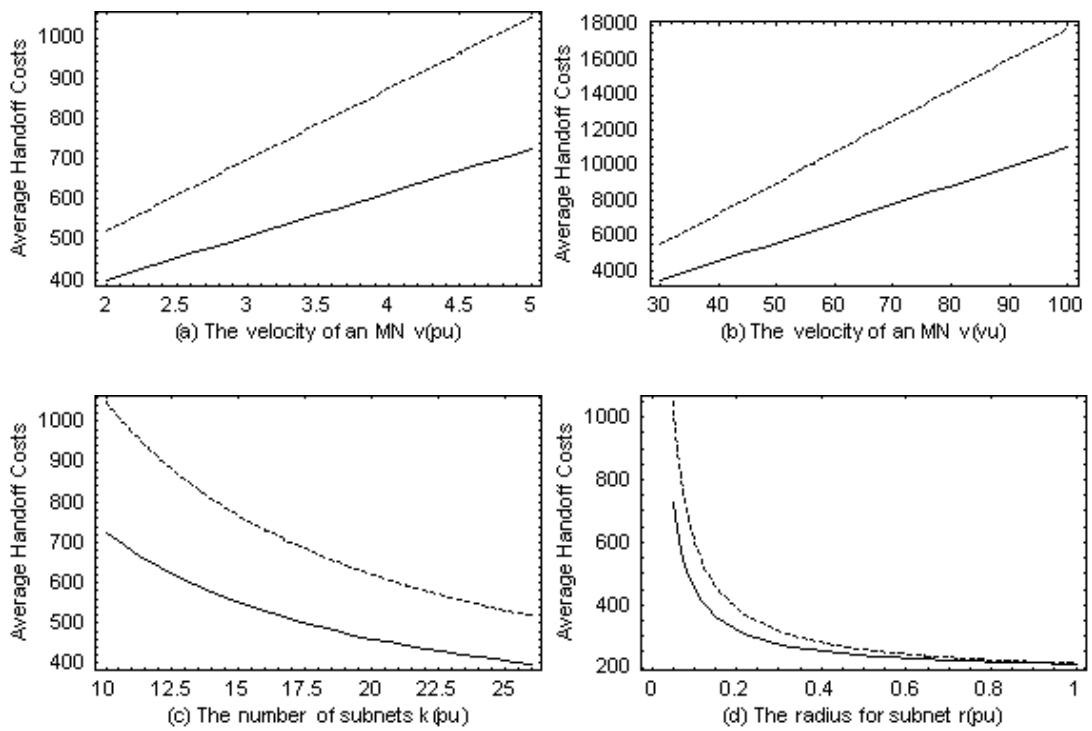
다음 그래프는 실제 파라미터의 수치값을 대입하여 계산한 단위시간당 평균 핸드오버 비용 AC_f를 그래프로 나타낸 것이다. 모든 그래프에서 실선은 제안기법의 단위시간당 평균 핸드오버 비용 AC_{proposed}를 나타내고, 점선은 [7]기법의 단위시간당 평균 핸드오버 비용 $AC_{[7]}$을 나타낸다.

〔표 4〕 인증비용 파라미터

기호	설명	값
C_{wired}	유선구간 전송비용	10
C_{wireless}	무선구간 전송비용	20
C_{hash}	MAC 생성 비용	1
C_{veri}	MAC 확인 비용	1
C_{enc}	암호화 비용	1
C_{dec}	복호화 비용	1
C_{key}	키생성 비용	1
$H_{\text{MN-MAG}}$	MN과 MAG 간의 홉수	1
$H_{\text{MAG-LMA}}$	MAG과 LMA 간의 홉수	2
$H_{\text{PMAG-NMAG}}$	PMAG과 NMAG 간의 홉수	1
$H_{\text{AAA-LMA}}$	LMA와 AAA 간의 홉수	2
$H_{\text{MAG-AAA}}$	MAG과 AAA 간의 홉수	4

그래프에서 보는 것과 같이 모든 조건하에서 제안기법이 [7]기법보다 핸드오버 비용이 적게 소요됨을 볼 수 있다. 제안기법에서는 AAA 서버와 초기 인증 절차에서 단 한번 접속하는 반면, [7]기법에서는 핸드오버가 발생할 때마다 AAA 서버와 접속하므로 더 많은 비용이 소요되는 것이다.

다음 그림에서 (a)와 (b)는 MN의 이동속도에 따른 단위시간당 평균 핸드오버 비용을 비교한 것이다. (a)는 보행자그룹(pu)에 대한 비용으로 MN이 2km/h ~ 5km/h의 속도로 이동했을 때 소요되는 비용을 나타낸 것이고, (b)는 차량그룹(vu)에 대한 비용으로 MN이 50km/h ~ 120km/h의 속도로 이동했을 때 소요되는 핸드오버 비용을 나타낸 것이다. (a)와 (b)에서는 MN이 빠른 속도로 이동할수록 단위시간당 평균 핸드오버 비용이 크게 소요되는 것을 볼 수 있다. (c)와 (d)는 서브넷의 수, 서브넷의 크기



〔그림 7〕 단위시간당 평균 핸드오버 비용

와 핸드오버 비용과의 관계를 나타내는 그래프이다. (c)에서는 서브넷 수가 많아질수록 핸드오버 비용이 감소하는 것을 볼 수 있고, (d)에서는 서브넷의 크기가 넓어질수록 비용이 급격히 감소하는 것을 볼 수 있다. 따라서 효율적인 핸드오버를 위해서는 적절한 서브넷의 수와 서브넷의 크기 설정이 중요함을 알 수 있다. 또한 (a), (b), (c), (d)의 모든 조건에 대해 제안기법이 [7]보다 단위시간당 평균 핸드오버 비용이 적게 소요됨을 볼 수 있다.

VI. 결 론

본 논문에서는 PMIPv6와 관련한 기존연구의 문제점을 지적하고, 신속하고 안전한 PMIPv6 기법을 제안하였다. 제안기법에서는 신속성을 제공하기 위해 AAA 서버와의 접속을 한번으로 최소화하였고, Fast PMIPv6를 도입하였다. 또한 안전성을 제공하기 위해 MN과 MAG, MAG과 LMA 간의 SA를 설정하여 시그널링 메시지를 보호하였다. 5장의 안전성과 성능분석을 통해 볼 수 있는 것과 같이 제안기법은 재생공격과 MIMD 공격에 안전하고, 기존기법보다 성능면에서 우수하였다. 차후 실제 모바일 응용에서 적용되기 위해서는 신속성 부분을 더욱 보완하여 결론적으로 제안기법은 안전성과 효율성 측면에서 우수한 기법이며, 차후 모바일 서비스의 특성상 신속성 부분을 더욱 보완하여 실제 모바일 서비스에 적용되어 사용되기를 기대한다.

참고문헌

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

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowd-hury, and B. Patil, "Proxy Mobile IPv6," Internet Draft, draft-ietf-netlmm-proxymip6-10.txt, IETF, Feb. 2008.

[3] T. Aura, "Mobile IP security, security protocols," The 10th Int'l Workshop, LNCS 2845, pp. 17-19, 2002.

[4] T. Aura, M. Roe, and J. Arkko, "Security of internet location management," In Proc. of the 18th Annual Computer Security Applications Conference, pp. 78-90, Dec. 2002.

[5] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark, "Mobile IP version 6 route optimization security design background," RFC 4225, Dec. 2005.

[6] C. Vogt, et. al., "Security threats to network-based localized mobility management (NETLMM)," RFC 4832, Apr. 2007.

[7] H. Zhou, H. Zhang, and Y. Qin, "An authentication method for proxy mobile IPv6 and performance analysis," Security and Communication Networks, vol. 2, pp. 445-454, Sep. 2008.

[8] S.G. Ryu, G.Y. Kim, B.G. Kim, and Y.S. Mun, "A scheme to reduce packet loss during PMIPv6 handover considering authentication," International Conference on Computational Sciences and Its Applications, ICCSA, pp. 47-51, Jun. 2008.

[9] J.H. Lee, J.H. Lee, and T.M. Chung, "Ticket-based authentication mechanism for proxy Mobile IPv6 environment," The Third International Conference on Systems and Networks Communications 2008, pp. 304-309, Oct. 2008.

[10] J.W. Song and S.Y. Ha, "One-time key authentication protocol for PMIPv6," Third 2008 International Conference on Convergence and Hybrid Information Technology, pp. 1150-1153, Nov. 2008.

[11] J.H. Lee and T.M. Chung, "A traffic analysis of authentication methods for proxy Mobile IPv6," 2008 International Conference on Information Security and Assurance, pp. 512-517, Aug. 2008.

[12] H. Zhou, H. Zhang, Y. Qin, H.C. Wang, and H.C. Chao, "A proxy Mobile Ipv6 based global mobility management architecture and protocol," Mobile Networks and Applications (MONET), vol. 15, no. 4, pp. 530-542, Aug. 2010.

[13] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC:keyed-hashing for message authenti cation," RFC 2104, Feb. 1997.

〔14〕 S.M. Baek, S.H Pack, T.M. Kwon, and Y.H. Choi, "A localized authentication, authoriza tion, and accounting (AAA) protocol for mobile hotspots," In Proceedings of IEEE/ IFIP Annual Conference on Wireless On demand Network Systems and Services (WONS) 2006, pp. 144-153, Jan. 2006.
〔15〕 R. Koodli, "Fast handovers for Mobile IPv6," RFC 4068, Jul. 2005.
〔16〕 H. Yokota, K. Ch., R. Koodli, B. Patil, and F. Xia, "Fast handovers for proxy Mobile IPv6," Internet Draft, draft-ietf-mipshop-pfmipv6- 14.txt, Sep. 2010.
〔17〕 Web page of Krb Working Group, "http://www.ietf.org/html.charters/krb-wg-charter.html," Accessed on Apr. 2008.
〔18〕 J. Laganier, S. Narayanan, and P. McCann, "Interface between a proxy MIPv6 mobility access gateway and a mobile node," Internet Draft, draft-ietf-netlmm-mn-ar-if-03, Aug. 2008.
〔19〕 W. Wang and I.F. Akyildiz, "Intersystem location update and paging schemes for multitier wireless networks," In Proceedings of International conference on Mobile computing and networking (MobiCom) 2000, pp. 99-109, Aug. 2000.

〈著者紹介〉

박 창 섭 (Chang-Seop Park) 종신회원
1983년: 연세대학교 경제학과 졸업
1983년: 한국 IBM 근무
1990년: 미국 Lehigh Univ. 전자계산학 박사
1990년~현재: 단국대학교 전자컴퓨터학부 교수
〈관심분야〉 네트워크 보안, 암호 프로토콜

강 현 선 (Hyun-Sun Kang) 정회원
2004년: 단국대학교 전자계산학 석사
2007년: 단국대학교 전자계산학 박사
2007년: 단국대학교 교양학부 강의전임강사
2009년: 단국대학교 정보기술연구소 연구원
2010년 9월~현재: 남서울대학교 교양학부 전임강사
〈관심분야〉 네트워크 보안, 암호 프로토콜