http://dx.doi.org/10.7236/JIIBC.2013.13.5.107
JIIBC 2013-5-14

안전한 NEMO 기반 PMIPv6 네트워크를 위한 빠른 핸드오버를 지원하는 확장 인증기법

Authentication eXtention Scheme of Fast Handover for Secure NEMO-based PMIPv6 Networks

임일균*, 정종필**

Illkyun Im, Jongpil Jeong

요 약 본 논문에서는 이동성을 지원하는 NEMO(NEwork MObility)와 네트워크 기반의 PMIPv6(Proxy Mobile IPv6)가 결합된 유·무선 통합 네트워크 환경에서 보안을 강화하고 암호계산과 인증지연 비용을 줄이는 가벼운 키 베이스의 SK-L^{2}AS(Symmetric Key-Based Light-Local Authentication Scheme)인증기법을 제안한다. 또한 PMIPv6에서 핸드오버 지연 단축을 위해 빠른 핸드오버 기법을 적용하였고, 지원되지 않는 전역 이동성을 지원하기 위해 X-FPMIPv6(eXtension of Fast Handover for PMIPv6)으로 확장 개선하였다. 더불어, 인증과 시그널링의 신호 부담을 줄이기 위해서 Piggybacks 방식을 적용하여 SK-L^{2}AS과 X-FPMIPv6을 통합한 AX-FPMIPv6 (Authentication eXtension of Fast Handover for PMIPv6)을 제안한다. 본 논문에서 제안한 AX-FPMIPv6 기법은 성능분석 결과 인증과 핸드오버 지연에서 기존 기법에 비해 성능이 우수하다는 것을 보여준다.

Abstract This paper reinforced security under the network evaluation of wire·wireless integration of NEMO (NEwork MObility) supporting mobility and network-based PMIPv6 (Proxy Mobile IPv6). It also proposes SK-L^{2}AS (Symmetric Key-Based Local-Lighted Authentication Scheme) based on simple key which reduces code calculation and authentication delay costs. Moreover, fast handover technique was also adopted to reduce handover delay time in PMIPv6 and X-FPMIPv6 (eXtension of Fast Handover for PMIPv6) was used to support global mobility. In addition, AX-FPMIPv6 (Authentication eXtension of Fast Handover for PMIPv6) is proposed which integrated SK-L^{2}AS and X-FPMIPv6 by applying Piggybacks method to reduce the overhead of authentication and signaling. The AX-FPMIPv6 technique suggested in this paper shows that this technique is better than the existing schemes in authentication and handover delay according to the performance analysis.

Key Word : AAA, NEMO, MIPv6, HMIPv6, PMIPv6, Symmetric Cryptosystem, Hash Function

Ⅰ. 서 론

최근 무선네트워크 기술의 급속한 발전에 힘입어 인터넷은 점점 더 모바일화 되어 이동 중에도 웹 브라우징, 인터넷 전화, 영상통화, 멀티미디어, 게임 등의 서비스 받을 수 있는 유비쿼터스 통신환경이 되었다. 여기에

*정회원, 성균관대학교 정보통신대학원 컴퓨터공학과
**정회원, 성균관대학교 정보통신대학
접수일자 : 2013년 9월 22일, 수정완료 : 2013년 10월 10일
게재확정일자 : 2013년 10월 11일

Received: 22 September 2013 / Revised: 10 October, 2013 / Accepted: 11 October, 2013
**Corresponding Author: jpjeong@ece.skku.ac.kr
Colleage of Information and Communication Engineering, Sungkyunkwan University, Korea

MNN(Mobile Network Node: 차량, 기차, 항공기, 배 등)에서도 이동 간에 인터넷에 접속하여 인터넷 서비스를 받고자 하는 이동형 네트워크 통신기기들도 증가하고 있는 추세이다. 그러나 이와 같은 다양하고 풍부한 인터넷 정보 서비스와 이동형 통신기기의 증가 만큼이나 정보서비스를 받는 사용자는 좀더 안전하고, 끊김없는 양질의 통신 품질을 요구하고 있다. 이에 인터넷 표준규격을 개발하는 IETF(Internet Engineering Task Force)에서는 NEMO(NEwork MObility)라는 네트워크 계층 솔루션을 제안하였다[1]. 여기에 MIPv6(Mobile IPv6)[2]을 더하여 네트워크의 연결을 유지하고, 외부 네트워크 간 이동성을 지원하도록 하였다. 그러나 NEMO는 여전히 MIPv6로부터 핸드오버 지연 이라는 단점을 물려받았고, 더욱이 이동 네트워크에서 AAA(Authorization, Authentication, Accounting)를 어떻게 처리해야 하는지에 대하여 정의가 되어있지 않다. 이는 네트워크의 상· 하위 계층 간에 안전한 정보서비스를 하기 위해서는 계층 간에 상호 신뢰할 수 있고, 안전하며 보안성이 강한 인증체계가 필수적이나, 이를 충족하지 못함을 의미하며, 이를 해결하기 위한 연구가 무엇보다 필요한 실정이다.

본 논문에서는 NEMO와 네트워크 기반의 PMIPv6(Proxy Mobile IPv6)이 결합된 유·무선 통합 네트워크에서 서버 부하가 적고, 가벼우며, 속도가 빠른 보안성이 강한 AAA모델 기반의 로컬 인증기법 SK-L^{2}AS(Symmetric Key-Based Light-Local Authentication Scheme)를 구현하였다. 이것의 특징은 첫째 대칭암호 방식(Symmetric Cryptosystem)과 해시함수(Hash Function)[30]만 사용하여 계산비용이 낮고, 로컬인증을 수행하여 인증지연을 감소시킨다. 또한 MR(Mobile Router) 과 LAAA (Local AAA) 간 세션 키를 공유하지 않아 HAAA(Home AAA)의 오버헤드를 감소시킨다. 둘째로 보안성이 강하다. 재전송 공격(Replay Attack), 서버스 푸핑 공격(Spoofing Attack), 훔친 검증자 공격(Stolen-Verifier Attack) 등을 방지하기 위해서 임의 값을 생성하여 계층 간 상호인증과 세션 키를 생성하여 보안 요건을 충분히 충족시킨다. 이 같은 로컬 인증기법을 기반으로 핸드오버의 지연과 서버의 과부하를 줄이기 위해서 FPMIPv6(Fast Hand overs for PMIPv6)의 장점인 사전 핸드오버를 PMIPv6에 적용하고, 계층 간 인증과 메시지 시그널링의 오버헤드를 줄이기 위한 방안으로 인증과 메시지 시그널링 통합하는 Piggyback 방식을 적용하였으며, MR이 지역 도메인 이동 뿐 아니라, 전역 이동 간에도 운영될 수 있도록 확장 개선한 AX-FPMIPv6 (Authentication eXtension & Fast Handover PMIPv6) 구축하였다.

본 논문에서 제안하는 AX-FPMIPv6을 성능 분석한 결과, 기존 기법들에 비해 보안성이 강하고, 빠른 인증처리와 핸드오버 지연 측면에서 성능이 우수하다는 것을 볼 수 있다. 논문의 나머지 부분은 다음과 같이 구성되어 있다. 2장은 인증보안과 PMIPv6과 NEMO가 결합된 네트워크 구조 그리고 핸드오버에 대하여 관련 연구를 서술한다. 3장은 제안한 AX-FPMIPv6의 인증기법의 동작 절차 등에 대하여 상세하게 설명한다. 4장은 정성적으로 보안성을 분석하고, 5장에서는 성능 평가 기준에 근거해서 제안한 AX-FPMIPv6 기법을 평가한다. 그리고 6장에서 연구결과를 요약한다.

표 1. 표시법
Table 1. Notation

기호	설 명
X	HAAA와 LAAA 사이에 유하는 비밀 값
GK	도메인의 그룹 키
MAC_i	이동통신 기기 i의 고유한 MAC 주소
R_i	임의의 값 i
$E_K(M)$	대칭암호 K 키를 이용한 암호화 메시지
$D_K(M)$	대칭 키 K로 해독한 한 평문
H()	일 방향 공개 해시 함수
‖	문자열 조합
$X_{service}$	HAAA 서버에서 모든 접속권한
$Y_{service}$	$Y_{service} \subseteq X_{service}$: MR의 접속권한 세트
$Z_{service}$	$Z_{service} \subseteq Y_{service}$: LAAA가 허가한 접속 권한
SK	세션 키

II. 관련 연구

1. 인증보안 측면

MIP(Mobile IP) 환경에서 이동 시 핸드오버에 관한 연구뿐만 아니라 AAA모델을 이용한 인증 관련한 많은 연구들이 진행 중이다. 이는 안전한 인증을 통해서 이동 네트워크 환경의 위협을 줄이기 위함이다. AAA모델에 관한 연구[4]는 대부분 호스트 이동성 환경[5-7]에 집중되고 있다. IETF에서는 네트워크가 이동 통신 노드로부터

외부 네트워크에서 로밍을 요청 받은 경우 문제를 해결하기 위해서 AAA모델[8,9]과 Diameter 프로토콜[10]을 제안하고 있다. AAA 모델에서는 그림 1에서 보는 바와 같이 MIPv6에는 네 가지 SA(Security Association) 관계가 있다. 여기서 SA는 네트워크 엔티티 간에 비밀정보 공유의 관계성을 보여준다. MR이 도메인에서 움직일 때 도메인의 자원에 접속하기 전에 MR은 몇 가지 인증정보를 제공하여야 한다. 그러나 그림 1에서 보는 바와 같이 MR과 LAAA 간에 직접적인 보안 연관이 부족하기 때문에 전통적인 인증 기법에서 기술적인 문제 중의 하나는 로밍을 원하는 MR과 Local AAA (LAAA) 간에 어떠한 비밀 정보도 사전에 공유할 수 없다는 것이다. 그것은 LAAA가 MR의 인증을 위한 정보가 없을 때, LAAA는 MR의 Home AAA(HAAA)에 정보를 보내고 다시 응답을 기다려야 하는 비효율적인 인증처리를 하게 된다. 더욱이, MR이 다른 도메인에서 자주 로밍을 한다면 MR의 인증처리를 위한 부하는 커지게 되고, 이는 외부 네트워크와 홈 네트워크 사이의 거리가 멀어지면 멀어질 수록 이 문제는 더욱더 심각해진다. NEMO는 이동통신 네트워크에서 AAA를 어떻게 처리해야 하는지 정의 되어 있지 않으며, 소수의 논문들 만이 NEMO 환경에서 AAA 인증을 고려하고 있다. Fathi et al.[11]는 NEMO의 보안 문제를 해결키 위해 PKI(Public Key Infrastructure) 개념 하에서 AAA모델을 사용하여 LR-AKE(Leakage-Resilient Authenticated Key Exchange)[12]체계를 제안하고 있다. PKI는 일반적으로 모든 공격을 방지하기 위해서 사용할 수 있지만, 이 방식은 암호 관련 계산이 이동통신 기기에서는 과중하다. 또한 Wang et al.[13]는 LR-AKE 체계가 클라이언트와 서버환경에서 공격에 가장 취약하다는 것을 보여주고 있다. Chuang et al.[14]는 인증 지연을 줄이기 위해서 로컬인증 개념을 제안하고 있다. 하지만, 이 제안에서는 MR이 새로운 외부 도메인으로 이동 할 때 여전히 AAA 서버에 인증을 다시 요구해야 한다. 이것은 MR이 동일 도메인 내에서만 이동 가능하도록 처리되어 새로운 도메인에 들어갔을 때 신규로 등록해야 한다.

본 논문에서는 그림 1에서 표시한 보안 연관(SAs)기반을 유지하면서도 대칭암호 방식과 해시함수 만을 사용하여 AAA모델에 기반 하에 인증 지연과 계산비용이 낮으면서, 빠르고 가벼운 로컬 인증기법을 제안한다.

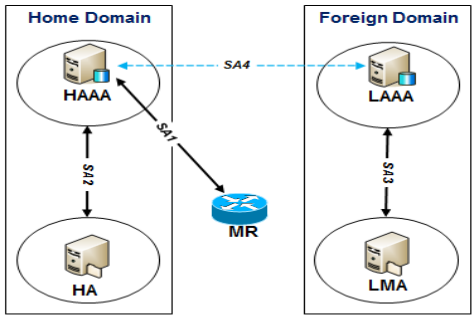

그림 1. AAA 모델과 PMIPv6 보안 연관
Fig. 1. SA of AAA Model and PMIPv6

2. 네트워크 구조 측면

이동통신 네트워크는 몇 개의 MNNs의 세션이 유지할 적어도 하나 이상의 MR을 가지고 있어야 하고, 도메인은 몇 개의 모바일 액세스 게이트웨이와 적어도 하나 이상의 LAAA를 가지고 있어야 한다. 무선통신 네트워크가 새로운 도메인에 들어갈 때, 그 새로운 네트워크에 접속하기 전에 MR은 첫 번째 인증 절차를 실행한다. MNNs이 접속하고, 끊고, 핸드오버를 실행할 때 네트워크 위상이 자주 바뀌기 때문에 안전한 그룹 통신을 효율적으로 유지하는 것은 이동통신 네트워크의 중요한 과제이다. 그림 2에서 표시한 네트워크는 이동통신 네트워크의 모든 종류의 그룹 키 관리 체계를 지원할 수 있다[15-17]. 로밍 협약을 했다면, AAA 보안 모델(그림 1에서 SA4)에 기반 하에 인증절차를 쉽게 하기 위해서 HAAA와 LAAA는 몇 가지 비밀 정보를 사전에 공유한다.

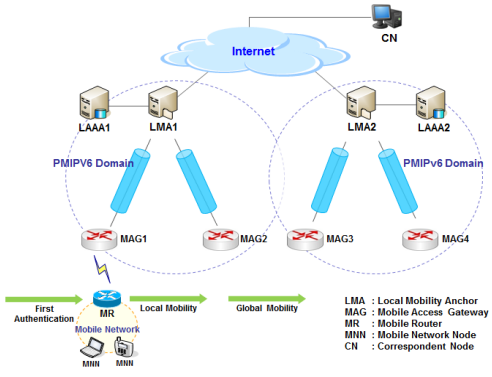

그림 2. 네트워크에 AAA 결합구조
Fig. 2. Network structure combined of AAA

더욱이, 도메인에서 LAAA와 MAGs는 GK(Group Key)(그림 1에서 SA3)와 같은 공통 비밀정보를 공유하고 있다. 이는 LAAA와 MAGs는 보안 연관이 있기 때문이다.

그림 2는 NEMO와 PMIPv6 환경 하에서 AAA모델을 결합하는 네트워크 구조이다.

3. 핸드오버 측면

NEMO는 MIPv6으로부터 확장되어 긴 핸드오버 지연 단점을 물려받아 이를 해결하기 위한 많은 접근법[18-20]이 시도 되고 있지만, 여전히 단점을 가지고 있다. 예를 들면, Malki [18]는 사전등록 방법 LLH(Low Latency Handover)를 제안하고 있지만, MNN이 Ping-Pong 상황에서는 HER(HA Error Registration) 문제라는 전송 실패를 유발할 수 있다. RFC4068[19]과 RFC4260[20]은 MIPv6의 핸드오버 성능을 개선하기 위해서 FMIPv6(Fast Handover Mobile IPv6) 체계를 제안하고 있다. FMIPv6는 핸드오버를 위해서 AR(Access Router)에 의존하지만, 매번 MN이 올바른 AR에 접속한다는 보장이 없다. 도메인 간 빠른 핸드오버를 지원하면서, 만일 MN과 AR 사이의 접속이 실패한다면 접속을 다시 시도해야 하며 이는 긴 핸드오버 지연으로 이어진다. 이것은 FMIPv6가 단순한 2 계층 트리거를 사용하기 때문이다. 또한 MIPv6에는 MN이 이동성을 위한 시그널링을 처리하기 위해 MN에 프로토콜 스택이 필요하다. 이는 제한된 MN에게 MIPv6을 지원하기 위해 기술적 난제와 과다한 리소스, 그리고 배터리 문제 등을 야기 시켜 MIPv6을 지원하는 단말기 상용화에 걸림돌이 되고 있다.

이에 IETF의 NetLMN(Network-based Localized Mobility Management) WG에서는 기존의 MIPv6의 문제점을 해결하기 위해 MN의 IP 이동성을 망에서 관리함으로써 MN의 수정 없이도 이동 중에도 서비스의 연속성을 보장하는 네트워크 기반 이동성 관리 프로토콜 PMIPv6(Proxy Mobile IPv6)를 표준화 하였다[21]. 이것은 PMIPv6에서 MN은 이동성 서비스 제공을 위해 어떠한 능력도 가지지 않아도 됨을 의미한다. 또한 PMIPv6 상당히 MIPv6의 핸드오버 지연을 감소시켰다. PMIPv6의 핸드오버 절차는 MD(Movement Detection)과 3계층의 핸드오버 절차에서 DAD(Duplication Address Detection) 프로세스를 실행하지 않는다. 하지만, PMIPV6에서는 MN으로 전달되는 모든 패킷이 LMA를 통해 전송되어 LMA에 패킷 병목현상[29]이 발생하고 있으며, 지역 이동성 만을 고려하여 설계되어 PMIPv6이 도메인 간 이동에는 연속성을 보장 할 수 없는 문제점을 가지고 있다.

이에 IETF에서는 NetLMN WG에서는 전역 이동성을 지원하기 위해서 MIPv6-PMIPv6 계층적 연동을 통한 도메인 간 이동성을 지원하는 Giaretta[22]방안, PMIPv6 도메인 간의 추가적인 시그널링 메시지를 정의하여 전역 이동성을 제공하는 Na의[23]방안 등 다양하게 제안되었지만, MIPv6-PMIPv6에서는 연동을 통해 도메인 간 핸드오버를 지원하는 방안이 MN에 MIPv6 프로토콜 스택을 반드시 가져야 한다는 문제점이 있고, Na방안은 도메인 간 추가적인 시그널링 메시지로 인한 핸드오버 지연이 그대로 발생하고 있다.

따라서 본 논문에서는 인접 도메인을 이동하기 위한 시그널링을 감소시키고, 도메인 간 연속성을 보장하기 위해 MAGs에 ND (Neighbor Discover)프로토콜을 적용하였다. 이는 인접 링크 계층 주소와 라우터 정보(즉, LMAs ‖ MAGs 와 네트워크 Prefix 정보 포함)를 가지고 있어서 시그널링 메시지를 감소시켜준다.

Ⅲ. 보안 효과적인 빠른 인증메커니즘

1. 로컬 인증기법(SK_L^{2}AS)

본 절에서는 AAA모델을 기반으로 제안한 빠르고 가벼운 SK-L^{2}AS에 대해 설명한다. 도메인 내 또는 전역 도메인 간 이동에서 SK-L^{2}AS이 동작하기 위해서는 홈 등록, 도메인에서 첫 번째 등록, 도메인에서 빠른 재-인증 등록, 그리고 외부 도메인에서 빠른 재-인증으로 4가지 절차가 있다. 네트워크에 연결하기 전에 MR은 HAAA에 등록해야 한다. MR이 처음으로 새로운 외부 네트워크에 진입할 때 SK-L^{2}AS이 첫 번째 인증 절차를 실행한다. MR이 동일한 도메인 내에서 이동할 때는 SK-L^{2}AS이 빠른 재-인증을 실행한다. 또한 도메인 내에서 핸드오버 지연 단축과 PMIPv6에서 지원되지 않는 전역 이동성을 지원할 수 있는 빠른 핸드오버 기법으로 확장 개선하여 시그널링을 줄일 수 있는 X-FPMIPv6를 구현하였다. 마지막으로 시그널링을 증가시키지 않게 하기위해 SK-L^{2}AS와 X-FPMIPv6을 통합한다.

가. 홈 등록 절차

MR이 이동 네트워크에 연결하기 전에 홈 등록 절차를 실행한다. 이러한 등록은 보안 채널이나 사람의 수작업 등록으로도 할 수 있다. 본 논문에서는 AAA모델[6-8,28]과 앞에서 설명한 Diameter 프로토콜 기반으로 MR과 HAAA 사이에 보안 채널이 있다고 가정한다. 그림 2에서 보듯이, MR과 HAAA 사이에는 보안 연관이 있다. 만약에 MR과 HAAA 사이에 보안 채널이 없다면, 시스템은 보안 채널을 설정하기 위해서 Diffie-Hellman 체계[31]를 실행할 수 있다. 그림 3은 홈 등록 절차를 보여주고 있다.

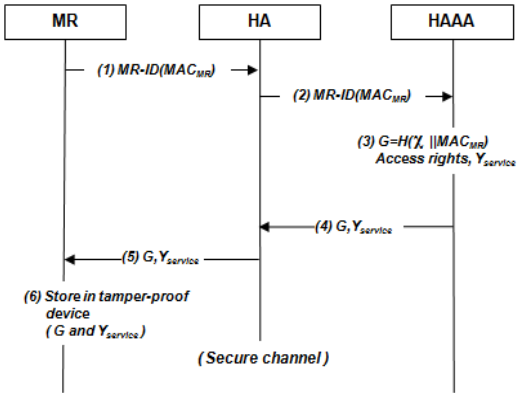

그림 3. 홈 등록절차

Fig. 3. Home registration procedure

(1,2)MR→HA→HAAA: MR은 HA를 통해서 HAAA에게 MR의 고유한 MR-ID/MAC 주소(MAC_{MR})를 보낸다.

(3)MR의 MAC 주소를 받은 후, HAAA는 비밀 값 $G=H(\chi \| MAC_{MR})$를 계산한다. H()는 충돌 회피 해시 함수로 HAAA와 LAAA사이에 안전하게 공유하는 비밀 값이다. 여기서 χ값을 구할 수 없다고 가정한다.

(4)HAAA→HA: HAAA와 HA에 매개변수 G와 Yservice를 보낸다. HAAA는 모든 접속권한 Xservice를 가지고 있고, Yservice는 MR이 접속 가능한 권한 세트를 표시한다.(즉, Yservice⊆Xservice)

(5,6)HA→MR: HA는 MR에게 매개변수 G와 Yservice를 전달하고, 이 값을 쉽게 변경할 수 없는 위치에 저장 관리한다.

나. 도메인에서 인증 절차

첫 번째 인증 절차는 아래에 그림 4 형식으로 보여주고 있다.

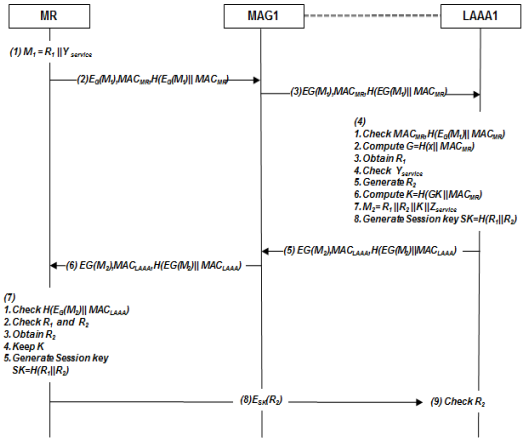

그림 4. 도메인에서 인증절차

Fig. 4. Authentication Procedure in a domain

MR이 새로운 네트워크에 들어갈 때 MR은 첫 번째 인증 절차를 실행한다. 이동통신 네트워크에서 MR은 자주 다른 도메인으로 이동하기 때문에 MR은 자주 재-인증을 받아야 한다. 일반적으로 MR의 인증정보는 HAAA로부터 확인하여야 한다. 만약에 도메인이 홈 도메인과 아주 멀리 떨어져 있다면, 인증하는데 많은 시간이 걸릴 것이다. 그러므로 효율적인 인증기법이 필요하다. 여기서 제시하는 체계는 로컬인증 기법(즉, 원격 서버를 포함하지 않고, 로컬로 인증을 지원)을 제공하며, MR과 LAAA의 상호간 인증을 용이하게 한다.

(1)MR은 임의의 값 R1과 인증정보(R1 ‖ Yservice)를 생성하고, 대칭키 G를 사용하여 암호화하고, 무결성을 위해 메시지 다이제스트($H(EG(M1) \| MAC_{MR})$)를 계산한다.

(2,3)MR→MAG1→LAAA1: MR은 MAG1에게 인증을 요청한다, 여기에 MAC_{MR}과 암호화된 M1(EG(R1 ‖ Yservice)) 메시지 다이제스트를 포함한다. MAG1은 LAAA1에 메시지를 전달한다.

(4)LAAA1의 MR 확인: LAAA1는 먼저 메시지 변조 공격을 탐지키 위해 메시지 다이제스트를 확인한다. 만일 해시 값($H(EG(M1) \| MAC_{MR})$이 메시지 다이제스트와 동일하지 않다면, LAAA1는 인증 요구를 거절한다. 이를 통해 서비스 거부 공격을 제거할 수 있다. 다음에 LAAA1는 $H(\chi \| MAC_{MR})$로 대칭 키 G를 생성하고 암호화된 메시지를 해독한다. 여기서 HAAA와 LAAA1는 보안 로밍 합의가 있고, 사전에 공유 비밀 값 χ(그림 1의 SA4)를 설정했기 때문에 χ는 HAAA 사이에 공유한 비밀 값으로 로밍이 이루어지는 도메인 간에는 MR의 접속

권한과 같은 동일한 권한을 갖는 다고 전제한다. 다음으로 LAAA1는 R1과 Yservice를 얻고, MR의 접속 권한(Yservice)을 확인한다. 만약 MR이 리소스에 접근할 수 있는 권한이 없다면, LAAA1는 요청을 거절할 것이다. 그렇지 않다면, LAAA1는 임의의 값 R2와 키 K= H(GK ‖ MAC_{MR})를 생성한다. 여기서 임의의 값과 키는 빠른 재-인증 단계에서 사용된다. GK는 그림 1의 SA3 그룹 키이다. 마지막으로 LAAA1는 인증 응답 M2를 (R1 ‖ R2 ‖ K ‖ Zservice)로 작성하고, 메시지 다이제스트 (H(EG(M2) ‖ MAC_{LAAA1})를 계산하며, MR과 LAAA1 사이의 SK를 H(R1 ‖ R2)로 생성한다. 여기서 Zservice는 LAAA1가 허가한 접속 권한을 나타낸다.(즉, Yservice⊆ Yservice)

(5)LAAA1→MAG1: LAAA1는 MAG1에게 암호화한 인증응답 EG(M2)와 MAC_{LAAA1} 메시지 다이제스트 (H(EG(M2) ‖ MAC_{LAAA1}))를 보낸다.

(6)MAG1→ MR: MAG2는 메시지를 MR에게 전달한다.

(7)MR의 LAAA1 확인: MR은 메시지 변조 공격을 탐지하기 위해서 메시지 다이제스트(H(EG(M2) ‖ MAC_{LAAA1}))를 확인하고, R1과 R2, K, Zservice를 얻기 위한 암호화된 메시지를 해독하기 위해서 G 키를 사용하며, 재전송 공격을 피하기 위해서 임의의 값 R1을 확인한다. Zservice에 근거해서, MR은 어떤 MAGs와 연관될 것인지를 결정한다. MR은 LAAA1와 함께 K 키를 저장하고 SK를 생성한다.

(8,9)MR→LAAA1: MR은 ESK(R2)를 포함하는 암호화된 메시지를 LAAA1에게 전달하고, LAAA1는 메시지를 받았을 때 그 메시지를 해독하고 임의의 값을 확인한다.

2. 빠른 프락시 모바일 IPv6 핸드오버

본 논문에서는 PMIPV6에서 전역 이동성을 지원하고 도메인 간의 핸드오버[32] 시에도 빠른 핸드오버를 적용하기 위해서 MAG에 ND 프로토콜을 적용하여 인접 링크 계층 주소와 라우터 정보(즉, LMAs ‖ MAGs 와 네트워크 Prefix 정보 포함)를 사전 핸드오버 준비 과정에서 획득하여 빠른 핸드오버를 처리 하도록 PMIPv6을 확장하고 개선한 X-FPMIPv6(eXtention & Fast Proxy Mobile IPv6)를 구축 하였다.

그림 5은 MR이 동일 도메인 내를 움직일 때 X-FPMIPv6 절차를 보여주고 있다. 특히, 도메인에서 핸드오버 지연 감소를 위해 사전 핸드오버 절차를 실행하기 위한 두 개의 2 계층(사전링크 트리거 p-LT(Pre-Link Trigger), 시작링크 트리거 s-LT(Start-Link Trigger)) 트리거를 추가했다. p-LT는 MAG로부터 받은 신호세기가 MR에 미리 설정한 임계치 보다 낮으면 작동을 시작한다. 이는 MR이 이전의 MAG로부터 멀어질 때 FPMIPv6의 핑퐁 효과로 성능 저하를 피하기 위해 “DeuceScan” [24]의 개념을 확장한 것이다. s-DT의 시작은 MR이 핸드오버 절차를 시작했다는 것을 의미한다. 그림 8에서, 1~5단계는 사전 핸드오버 절차를 실행하고, 6~10 단계는 핸드오버이다.

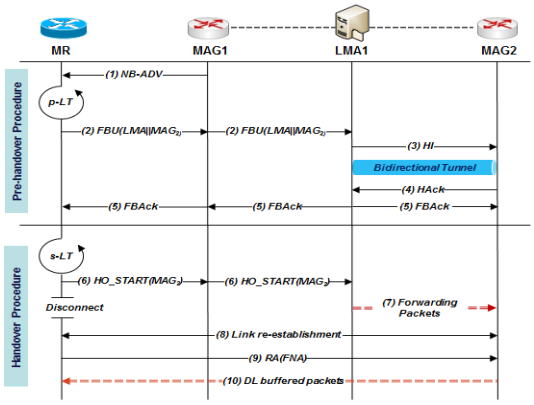

그림 5. 도메인 내에서 빠른 핸드오버 절차

Fig. 5. Fast handover procedure within domain

(1)MAG1는 주기적으로 MR에게 NB-ADV (Neighbour-Advertisement)메시지를 전송한다. 메시지는 MR이 새로운 접속 MAGs를 선택할 수 있도록 LMAs ‖ MAGs의 후보 목록(MAGs의 네트워크 Prefix 포함)이다.

(2)p-LT를 시작하면, MR은 가능한 MAGs 후보의 목록(MAG2)를 가지고 PCoA를 생성하여 FBU(Fast Binding Update)메시지를 LMA1의 MAG1를 통해 전송한다.

(3)LMA1는 후보 MAGs들에게 HI(Handover Initial) 메시지를 보냄으로써 빠른 핸드오버 절차를 시작한다. 후보 MAG2는 PCoA의 프락시 인접 케시에 저장하고, 동일 도메인 내의 MAGs인 경우 LMA1와 후보 MAG2간 터널링을 생성한다.

(4)핸드오버 응답 HAck(Handover Acknowledgment) 메시지를 LMA1에게 전송한다.

(5)LMA1는 MAG2와 MR에게 사전 핸드오버 절차 완료 통지를 위해서 FBAck(Fast Binding

Acknowledgement)메시지를 사용하고, MR은 다수의 PCoAs(on-link care- of-addresses)를 동시에 얻는다.

(6)이후에 s-LT 2계층 핸드오버가 시작되면서 MR은 실제 목표 MAG2를 선택한다. MR은 MAG2를 목표로 선정하고 핸드오버 시작 HO_START 메시지를 LMA1에게 보낸다.

(7)HO_START 메시지를 받은 후, LMA1는 선택한 MAG2에게 MR에게 보내어지는 모든 패킷 전송을 시작하고, MAG2은 패킷을 버퍼링하여 저장한다.

(8,9)MR이 핸드오버를 완료하면, MR은 MAG에게 RA(Route Advertisement)메시지를 보내 자신의 핸드오버 완료를 알린다.

(10)이후 MAG2는 MR의 새로운 PCoA에 대한 프락시 인접 케시를 삭제하고, 바인딩 케시에 PCoA를 저장한 후 버퍼링 되었던 메시지를 다운로드 한다.

3. SK-L^{2}AS와 X-FPMIPv6의 통합

AX-FPMIPv6는 MR이 지역 또는 전역 이동에 관계없이 도메인 이동에 대해서 핸드오버 지연을 줄이는 것을 목표로 하기 때문에 적절한 인증체계와 협력해야 한다. 그래서 도메인 간 이동에서 보안성이 강화하고, 가벼우며 처리 속도가 빠른 SK-L^{2}AS와 신호 부담이나 핸드오버 지연을 증가시키지 않는 X-FPMIPv6가 통합 작동하도록 Piggyback 방식을 적용하였다. 그림 6은 MR이 동일 도메인 내에서 이동 시 MR이 전역 이동성을 지원하는 환경에서 빠른 인증 절차를 보여주고 있다.

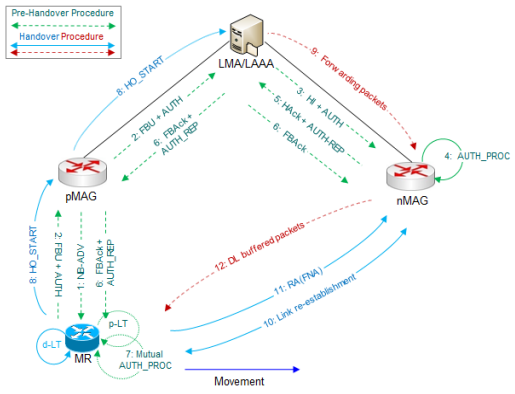

그림 6. 도메인 내 순서도

Fig. 6. Sequence diagram within the same domain

MR이 FBU메시지를 MR의 pMAG에 보낼 때, 인증 메시지 AUTH를 Piggybacks 방식을 적용 MAC_{MR}과 $M(R3 \| Yservice \| H(R3 \| MAC_{MR}))$이 포함되어 있다. 이때 MR이 유효한 것으로 인증되면, nMAG는 MR에 대한 HAck/FBAck에 대한 답으로 인증응답 메시지를 AUTH_REP를 Piggybacks 방식으로 전송한다. 이와 같이 SK-L^{2}AS와 X-FPMIPv6가 통합 작동하여 사전 핸드오버 처리를 함에 따라 시그널링 부담을 감소시켜 안전하고 끊김 없는 통신이 가능하다.

도메인 간 이동에서도 AX-FPMIPv6는 시그널링과 인증 메시지 AUTH가 통합되어 인접 MAGs가 현재 접속된 도메인 MAG가 아닌 새로운 도메인 nMAG인 경우에도 nMAG와 nLAAA에 HI와 AUTH를 각각 전송하고 그에 따른 응답으로 pLMA와 pMAG는 빠른 바인딩 FBAck과 AUTH_REP를 pLMA에게 전송할 수 있도록 하여 도메인 간 이동에서도 SK-L^{2}AS와 X-FPMIPv6가 통합되어 작동한다.

Ⅳ. 보안 분석

보안 분석을 말하기에 앞서 다음의 몇 가지 유의 사항을 추가한다. 그룹 키 GK를 LAAA와 MAGs 사이에 안전하게 사전 공유 된 것으로 정의했지만, 공격자가 충분한 시간과 고속 컴퓨터를 가진다면 장기간 사용하는 키는 무차별 대입 공격에 취약하다. 그래서 키의 길이는 충분히 길고, 무차별 대입 공격 확률을 줄이기 위해 장기간 사용하는 키는 적시에 변경한다고 가정한다. SK-L^{2}AS는 일 방향 해시 함수 H()에 대해서, χ값이 주어져있다면, H(χ)는 계산하기 쉽다(예, SHA-512[25]). 그러나 H(χ)가 주어지지 않은 경우, 이를 계산 하는 것은 매우 어렵고, 높은 계산 비용을 발생시키기 때문에 다음과 같은 보안 특성을 만족한다.

Replay Attack의 저항성: SK-L^{2}AS는 인증절차에서 MR 또는 MAGs에서 임의의 값을 매번 신규 생성하여 인증정보(Mn)에 포함하기 때문에 재전송 공격에 강하다.

Server Spoofing Attack의 저항성: MR은 AAA 인증서버를 인증하고SK-L^{2}AS는 반대로 이다. 이러한 상호 인증은 스푸핑 공격을 무력화 시킨다.

시간 동기화 문제: 재 전송 공격에 대항하기 위해 몇몇 인증체계는 타임스탬프 방식을 사용하나, 이 방식은 다른 시간대와 긴 전송 지연 등과 같은 몇 가지 단점이

있다. 그러나 본 체계는 난수 기반 인증체계이기 때문에 시간 동기화 문제가 없다.

Stolen-verified Attack의 저항성: AAA는 MR의 어떠한 검증 정보를 저장할 필요가 없어서 공격자가 AAA의 데이터베이스를 침입한다고 하더라도 인증 정보를 임으로 생성하기 때문에 사용자 인증 정보를 획득할 수 없다.

Message Alteration Attack의 저항성: 메시지 다이제스트 생성과 일 방향 해시 함수를 사용하여 정보가 변조가 될 수 없도록 하였다. 만일 공격자가 변조한 패킷을 MR이나 인증서버에 전송한다하더라도 패킷의 해시 값을 체크하기 때문에 쉽게 확인할 수 있다.

로컬인증: 로컬인증은 3가지 장점이 있다. 인증 시간을 줄인다. 네트워크 부담을 감소시킨다. 그리고 무정지 형 기법을 제공한다. 바꿔 말하면, AAA 서버가 해킹을 당하더라도 MR은 여전히 도메인에서 인증 절차를 실행할 수 있다는 것이다.

세션 키 생성: SK-L^{2}AS의 첫 번째 인증과 빠른 재-인증 절차에서, 안전한 통신을 제공하기 위해서 임의의 값을 사용하는 세션 키를 생성한다. AX-FPMIPv6에서는 그 키를 사전 핸드오버 절차에서 생성한다. 이 절차를 완료하면 MR과 MAG는 상호 안전하게 통신을 할 수 있다.

Known-plaintext Attack의 저항성: 알려진 평문 공격은 공격자가 평문과 그 평문에 해당하는 암호문을 동시에 획득하여 비밀 정보를 발견하려는 암호 해독 공격으로 공격자가 MAC_{MR}을 획득할 수 있으나, 비밀 키 G(즉, $G=H(x \| MAC_{MR})$)와 비밀 값 χ을 알지 못하기 때문에 공격자는 알려진 평문 공격을 성공적으로 실행할 수 없다. 또한, 빠른 재-인증 절차에서도 여전히 동일한 이유 때문에 평문 공격을 당하지 않는다.

V. 성능분석

1. 평가기준

성능평가 기준에 근거해서 제안한 기법은 아래 3가지 관점에서 평가한다.

계산비용(CC): 이동통신 노드 계산.

인증지연(AL): MR이 인증 요청을 보내고 그 해당 인증 응답을 받는 사이 지연 시간.

핸드오버 지연(HL): MR이 MR의 연관을 바꾸는데 필요한 시간.

2. 매개변수

그림 7은 성능평가를 위해서 사용한 네트워크 위상과 수치해석 모델이다.

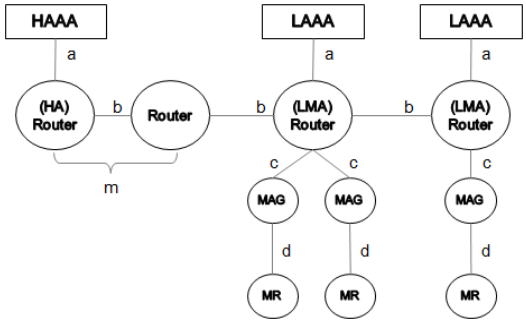

그림 7. 성능평가를 위한 네트워크 수치 모델

Fig. 7. Network phase and numerical models for performance evaluation

신호 메시지 크기는 다르나 각각의 메시지들이 동일한 전송지연과 계산비용이 소요된다 가정한다. 평가모델은 표시법은 다음과 같다.

DA-B:노드 A와 노드 B사이의 평균 전달 지연. DA-B=DB-A라고 가정한다.

DRA(FNA):빠른 인접 광고 메시지를 전송하는데 필요한 시간.

m: 홈과 도메인 사이의 홉수.

DPROC(A): 절차 A의 평균 처리 지연

핸드오버 지연은 2 계층 감지 지연(DL2), 이동 감지 지연(DMD), 중복 주소 감지 지연(DDAD), 인증 지연(DAUTH), 위치 등록 지연(DBU)의 합으로 표시할 수 있다. [2]에서 요청 받지 않은 라우터 광고(RA)를 더 자주 보낼 수 있도록 이동성을 지원하는 MAG은 작은 MinRtrAdvInterval(MinInt)와 MaxRtrAdvInterval (MaxInt) 값으로 설정해야 한다고 제시하고 있다. 또한 좀더 단순화 하기 위해 [26]에 근거에서는 MIPv6에서 DMD 값을 요청하지 않은 RA 메시지의 평균 값의 절반 (즉, (MinInt+MaxInt)/2), 그리고 HMIPv6에서 DMD 값을 요청하지 않은 RA 메시지 평균 값 4분의 1(즉, (MinInt+MaxInt)/4)이라고 가정한다.

SA: 노드 A가 보낸 신호 메시지의 숫자.(표-3)은 [27]에 근거해서 수치 해석에 사용하는 매개 변수 값들과 DAD 지연의 기본 값이 1000ms 라는 것을 보여주고 있다.

표 2. 분석에 사용한 매개변수

Table 2. Parameters used in the analysis

구 분	시간(ms)
D_{L2}	50
D_{DAD}	1000
a	10
b	10
c	10
d	100
MinInt	30
MaxInt	7
$D_{PROC(AUTH)}$	10

3. 분석결과

가. 계산비용(CC)

본 절에서는 SK-L^{2}AS와 LR-AKE 체계의 계산 비용을 비교한다. 계산 비용 분석 시, 다음과 같은 표시법을 사용한다. "-"는 계산 비용이 없다는 것을 의미한다. n은 AAA가 다루는 MRs의 수이다. Ch는 일 방향 해시 함수를 실행하는 비용이다. Csym은 대칭 암호화 해독 계산 비용이고, Casym은 비대칭 암호화와 해독 계산 비용이다. Cram는 임의의 값을 생성하는 비용을 표시한다. 표 3과 표 4는 SK-L^{2}AS과 LR-AKE의 복잡성을 보여주고 있다. LR-AKE는 로컬인증을 지원하지 않아 HAAA에서 매번 인증절차를 실행하여 HAAA에서 병목현상이 발생한다.

표 3. SK-L^{2}AS 체계의 계산 비용

Table 3. Calculation costs of SK-L^{2}AS scheme

구분	MR	HAAA	LAAA	AR
홈등록 단계	-	-	-	-
첫번째 인증 단계	C_{ram}+3 C_{asym}+6 C_h	C_{ram}+2 C_{asym}+6 C_h	-	-
재-인증 단계	C_{ram}+3 C_{asym}+6 C_h	C_{ram}+2 C_{asym}+6 C_h	-	-

표 4. LR-AKE 체계의 계산 비용

Table 4. Calculation costs of LR-AKE scheme

구분	MR	HAAA	LAAA	MAG
홈등록 단계	-	nC_h	-	-
첫번째 인증 단계	C_{ram}+3C_{sym}+3C_h	-	C_{ram}+3C_{sym}+5C_h	-
재-인증 단계	C_{ram}+3C_{sym}+3C_h	-	-	C_{ram}+3C_{sym}+4C_h

나. 인증지연(AL)

수치 해석으로 SK-L^{2}AS와 LMAM, simple NEMO (snemo), LR-AKE, Shi et al 체계의 성능을 평가 비교하고, 두 개의 이동성 시나리오에서 인증 지연을 고려한다. 아래의 표 5는 인증 지연의 수치 해석 결과이다.

표 5. 비교대상 체계의 인증 지연

Table 5. Comparison of Authentication latency

구분	처음 도메인 진입	동일 도메인 내 움직임	다른 도메인으로 이동
Proposed (SK-L^{2}AS)	*2a+2c+2d*	*(MinInt+MaxInt)/2*	*(MinInt+MaxInt)/2*
LMAM	*2a+2c+2d*	*2d*	*2(2a+2c+2d)*
snemo	*4a+2mb+2c+2d*	*4a+2mb+2c+2d*	*2(4a+2mb+2c+2d)*
LR-AKE	*10a+9mb+5c+5d*	*10a+9mb+5c+5d*	*2(10a+9mb+5c+5d)*
Shi et al.	*4a+2mb+2c+2d*	*2a+2c+2d*	*2(4a+2mb+2c+2d)*

(a) MR이 도메인에 처음 들어갔을 때, 인증 지연은 다음과 같다.

$$AL_{proposed} = 2D_{MR-MAG} + 2D_{MAG-LAM} + 2D_{LAM-LAAA} + D_{AUTH} = 2_a + 2_c + 2_d \quad (1)$$

$$AL_{LMAN} = 2D_{MR-AR} + 2D_{AR-MAP} + 2D_{MAP-LAAA} + D_{AUTH} = 2_a + 2_c + 2_d \quad (2)$$

$$AL_{snemo} = 2D_{MR-AR} + 2D_{AR-LAAA} + 2D_{HAAA-LAAA+} D_{AUTH} = 4_a + 2_{mb} + 2c + 2_d \quad (3)$$

$$AL_{LR-AKE} = 5D_{MR-AR} + 5D_{AR-HA} + 2D_{HA-HAAA+} 4D_{HAAA-LAAA} + D_{AUTH} = 10_{a+} 9_{mb} + 5c + 5_d \quad (4)$$

$$AL_{Shi} = 2D_{MR-AR} + 2D_{AR-LAAA} + 2D_{HAAA-LAAA} + D_{AUTH} = 4_{a+} 2_{mb} + 2_c + 2_d \quad (5)$$

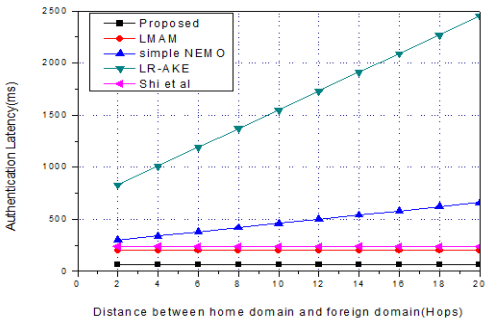

그림 8. 도메인 최초 등록 시 인증지연

Fig. 8. Authentication latency during the first domain registration

(b) MR이 동일한 도메인 내에서 움직일 때, 인증 지연은 다음과 같다.

$$AL_{proposed} = 2D_{MR-MAG} + D_{AUTH} = (MinInt + MaxInt)/2 \quad (6)$$

$$AL_{LMAN} = 2D_{MR-MAG} + D_{AUTH} = 2d \quad (7)$$

$$AL_{snemo} = 2D_{MR-AR} + 2D_{AR-LAAA} + 2D_{HAAA-LAAA} + D_{AUTH} = 4_a + 2_{mb} + 2c + 2_d \quad (8)$$

$$AL_{LR-AKE} = 5D_{MR-AR} + 5D_{AR-HA} + 2D_{HA-HAAA} + 4D_{HAAA-LAAA} + D_{AUTH} = 10_a + 9_{mb} + 5c + 5_d \quad (9)$$

$$AL_{Shi} = 2D_{MR-AR} + 2D_{AR-MAP} + 2D_{MAP-LAAA} + D_{AUTH} = 2_a + 2_c + 2_d \quad (10)$$

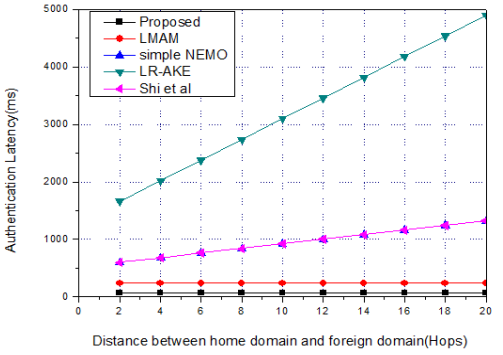

그림 9. 동일 도메인 내에서 움직일 때 인증지연

Fig. 9. Authentication latency when moving within the same domain

(c) MR이 다른 도메인으로 움직일 때, 인증 지연은 다음과 같다.

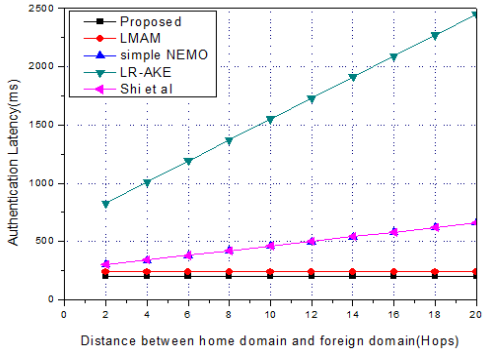

그림 10. 다른 도메인으로 이동 시 인증지연

Fig. 10. Authentication latency when moving into another domain

본 논문에서 제안한 SK-L^{2}AS는 비교하고 있는 접근법 중에서 최고의 인증 지연을 달성하고 있다는 것을 보여주고 있다. 이것은 제안한 SK-L^{2}AS이 홈 인증 대신에 로컬 인증을 사용하기 때문이다.

다. 핸드오버 지연(HL)

AX-FPMIPv6의 성능을 LE-HMIPv6와 Simple NEMO, LLH, HMIPv6와 비교한다. 본 시뮬레이션에서 열 번 실행의 평균으로부터 결과를 얻었다. HMIPv6가 지역 등록을 지원한다고 가정한다. 총 핸드오버 지연은 데이터 링크 계층 핸드오버 지연과 인증 지연, 네트워크 계층 핸드오버 지연의 합이다. 각 체계의 총 핸드오버 지연은 다음과 같다.

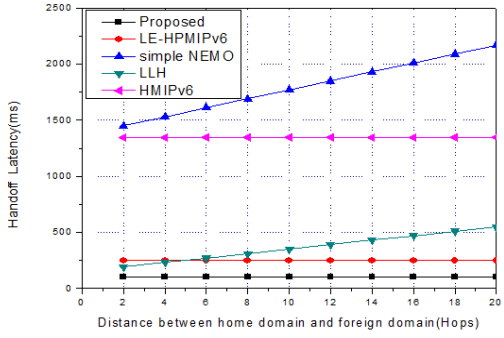

그림 11. 홈 도메인과 도메인 사이 거리 vs 도메인 내부 간 평균 핸드오버 지연 성능

Fig. 11. Distance between home domain and foreign domain vs Average handover latency within the same domain

$$HL_{AFPMIPv6} = D_{L2} + D_{RA(FNA)} = D_{L2} + 2D_{MR-MAG} = D_{L2} + (MinInt + MaxInt)/2 \quad (11)$$

$$HL_{\leq -HMIPv6} = D_{L2} + D_{FNA} = D_{L2} + 2D_{MR-NAR} = D_{L2} + 2d \quad (12)$$

$$HL_{snemo} = D_{AUTH} + D_{L2} + D_{MD} + D_{DAD} + D_{BU} = (2D_{LAAA-HAAA} + D_{PROC(AUTH)}) + D_{L2} + (MinInt + MaxInt)/2 + D_{DAD} + 2(D_{MR-NAR} + D_{NAR-HA}) = 2(a + (m+2)b) + D_{PROC(AUTH)} + D_{L2} + (MinInt + MaxInt)/2 + D_{DAD} + + 2(d + (m+1))b \quad (13)$$

$$HL_{LLH} = D_{AUTH} + D_{L2} + D_{MD} = (2D_{LAAA-HAAA} + D_{PROC(AUTH)}) + D_{L2} + (MinInt + MaxInt)/2 = 2(a + (m+1)b) + D_{PROC(AUTH)})D_{L2} + (MinInt + MaxInt)/2 \quad (14)$$

$$HL_{HMIPv6} = D_{AUTH} + D_{L2} + D_{MD} + D_{DAD} + D_{BU} = (2D_{AR-LAAA} + D_{PROC(AUTH)}) + D_{L2} + (MinInt + MaxInt)/4 + D_{DAD} + 2(D_{MR-NAR} + D_{NAR-MAP}) = 2(a+c) + D_{PROC(AUTH)} + D_{L2} + (MinInt + MaxInt)/4 + D_{DAD} + 2(c+d) \quad (15)$$

그림 12는 평균 도메인 내부 간 핸드오버 지연 성능을 보여주고 있다.

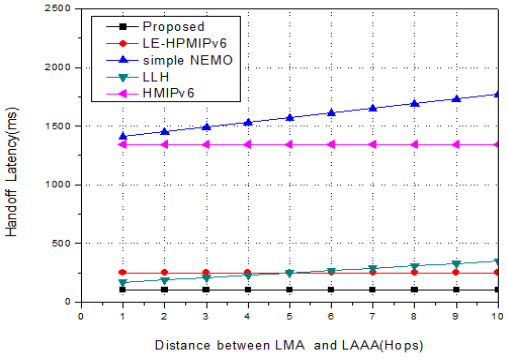

그림 12. MAG와 LAAA 사이의 거리 vs. 도메인 내부간의 평균 핸드오버 지연 성능

Fig. 12. Distance between LMA MAG and LAAA vs Average handover latency among domains

SK-L^{2}AS은 MR의 HAAA에 정보를 다시 보낼 필요 없이 로컬인증을 제공하여 지역 내 이동성 관리에 효과적으로 작동을 한다. 이에 더하여 AX-FPMIPv6는 신호 부담을 줄이는 Piggybacks 방식을 적용과 사전 핸드오버 절차를 수행하기 위해 여러 개의 데이터 링크 트리거를 사용하여 핸드오버 절차를 빨리 실행할 수 있도록 개선하였다. LE-HPMIPv6는 핸드오버를 개선한 HMIPv6 프로토콜을 적용하여 이동성 관리와 지역등록 체계를 지원하여 핸드오버 지연은 감소하고 있으나, 이동 감지와 DAD 지연이 지연을 유발하고 도메인 간 핸드오버를 지원하지 않으며, Simple NEMO 프로토콜은 MIPv6에서 긴 핸드오버 지연의 단점을 물려받고, 로컬인증을 지원하지 않아 가장 긴 핸드오버 지연을 가지고 있다. 비록 LLH는 핸드오버 지연을 줄이기 위해서 사전 등록 방법을 사용하나, 인증 절차는 여전히 HAAA에서 실행하여 이로 인해 긴 인증 지연이 발생한다. 그림 12 는 평균 도메인 간 핸드오버 지연 성능을 보여주고 있다.

본 제안 체계는 네트워크 기반의 구조와 지역 기반의 인증 그리고 인증 절차와 이동 감지 절차를 사전 핸드오버 단계에서 완료하기 때문에 AX-FPMIPv6 기법은 가장 낮은 핸드오버 지연을 가진다.

Ⅵ. 결 론

본 논문에서는 네트워크 이동성을 지원하기 위해서 SK-L^{2}AS이라고 부르는 로컬 인증기법을 제안하였다. 이는 대칭 암호화와 해시 함수를 사용하기 때문에, 암호화 관련 계산량이 감소하고, 인증 지연을 감소시키기 위해 HAAA나 LAAA 서버에서 운영되지 않고 로컬 인증 과정 만으로 처리를 할 수 있도록 하였다. 또한 인증과 시그널링 메시지를 통합하여 신호 부담을 증가시키기 않도록 하였다.

마지막으로 이동 통신 네트워크에서 지역 및 전역 핸드오버를 지원하기 위해서 PMIPv6을 개선하여 핸드오버 절차의 속도를 증대시켰다.

분석결과 계산 비용과 인증 지연, 핸드오버 지연, 신호 비용에서 기존의 모든 체계보다 제안한 기법이 성능이 뛰어나다는 것을 보여주고 있다. 보안 문제와 관련해서, SK-L^{2}AS은 로컬 인증과 재전송 공격, 훔친 검증자 공격, 세션 키 생성, 서버 스푸핑 공격을 방지하기 위한 상호

인증, 알려진 평문 공격 저항성, 메시지 변조 공격 저항성의 영역에서 매우 효과적이다.

References

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, "Network Mo bility(NEMO) Basic Support Protocol ", IETF, RFC 3963, January 2005.

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

[3] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol. 24 (11), pp.770-772, November 1981.

[4] T. Narten, E. Nordmark, W. Simpson. "Neighbor discovery for IP version 6 (IPv6)", RFC 2461, December 1998.

[5] S. Pack, Y. Choi, "Fast handoff scheme based on mobility prediction in public wireless LAN systems", IEEE Communications, Vol.151(5), pp.489 - 495, October 2004.

[6] A. Mishra, M.H. Shin, N.L. Petroni, J.T. Clancy, W.A. Arbauch, "Proactive key distribution using neighbor graphs", IEEE Wireless Communications, Vol.11(1), pp.26 - 36, February 2004.

[7] C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, "Generic AAA architecture", IETF, RFC 2903, August 2000.

[8] S. Glass, T. Hiller, S. Jacobs, C. Perkins, "Mobile IP authentication, authorization, and accounting requirements", IETF, RFC 2977, October 2000.

[9] C.E Perkins, "Mobile IP joins forces with AAA", IEEE Personal Communications, RFC 2977, pp.59-61, August 2000.

[10] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, "Diameter Mobile IPv4 application", P. McCann (Ed.), RFC 4004, August 2005.

[11] H. Fathi, S. Shin, K. Kobara, S. Chakraborty, H. Imai, R. Prasad, "LRAKE-based AAA for network mobility (NEMO) over wireless links", IEEE Journal on Selected Areas in Communications (JSAC), Vol.24(9), pp.1725 - 1737, 2006.

[12] I. Hideki, S. Seonghan, K. Kanukuni, "introduction to Leakage-Resilient Authenticated Key Exchanged Protocols and Their Applications", KIISC, December 2008.

[13] Yingjie Wang, Wei Luo, Changxiang Shen, "Analysis on Imai - Shin's LR-AKE protocol for wireless network security", Communications in Computer and Information Science, Vol.84 - 89, 2009.

[14] Ming-Chin Chubng, Jeng-Farn Lee, "A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks" Computer Networks, June 2011.

[15] Depeng Li, Srinivas Sampalli, "An efficient contributory group rekeying scheme based on hash functions for MANETs", IFIP International Conference on Network and Parallel Computing Workshops, pp.191 - 198, September 2007.

[16] W.H.D. Ng, Zhili Sun, H. Cruickshank, "Group key management with network mobility", 13th IEEE International Conference on Networks (ICON), Vol. 2, pp.716 - 721, November 2005.

[17] Y. Kim, A. Perrig, G. Tfsudik, "Group key agreement efficient in communication", IEEE transactions on computers, Vol. 53(7) PP.905-921, 2004.

[18] K. El Malki (Ed.), "Low-Latency Handoffs in Mobile IPv4", IETF, RFC 4881, June 2007.

[19] R. Koodli (Ed.), "Fast Handoffs for Mobile IPv6", IETF, RFC 5268, June 2008.

[20] P. McCann, "Mobile IPv6 fast handoffs for 802.11 Networks", IETF, RFC 4260, November 2005.

[21] S. Gundaveli, K, Leung, V. Devarapali, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6", IETF, RFC 5213, August 2008.

[22] G, Giaretta, "Interaction between PMIPv6 and MIPv6", draft-ietfnet lmm-mip-interactions-03.txt, November, 2009.

[23] Jee-Hyeon Na, Soochang Park, Jung-Mo Moon, Sangho Lee, Euisin Lee, and Sang-Ha Kim,

"Roaming Mechanism between PMIPv6 Domain",draft-park-netmm-pmipv6-roaming-o1.txt, July, 2008.

[24] Yuh-Shyan Chen, Ming-Chin Chuang, Chung-Kai Chen, "DeuceScan: deuce-based fast handoff scheme in IEEE 802.11 wireless networks",IEEE Transaction on Vehicular Technology Conference, Vol. 57(2), pp.1126 - 1141, September 2008.

[25] NIST, U.S. Department of Commerce, "Secure Hash Standard", U.S.Federal Information Processing Standard (FIPS), August 2002.

[26] Ki-Sik Kong, Wonjun Lee, Youn-Hee Han, Myung-Ki Shin,HeungRyeol You, "Mobility management for All-IP mobile networks: Mobile IPv6 vs. proxy mobile IPv6", IEEE Wireless Communications, Vol. 15(2), pp.36 - 45, 2008.

[27] S. Thomson, T. Narten, "IPv6 stateless address autoconfiguration", IETF, RFC 2462, December 1998.

[28] I. Im, YH Cho, JY Choi, J. Jeong "Security-Effective fast authentication mechanism for network mobility in proxy mobile IPv6 networks", Computational Science and Its Applications-ICCSA 2012, Vol.7336, pp.543 - 559, 2012.

[29] I. Im, J. Jeong, "Cost-effective and fast handoff scheme in Proxy Mobile IPv6 networks with multicasting support", Mobile Information Systems, IOS Press, July 2013.

[30] E.J. Lee, P.J. Lee, "Multul Authentication and Session Key Agreement Protocol Using only a Hash Function", Vol.7 No. 1, KIISC, 1997

[31] W. Diffie and M.E.Hellman, "New Directions in Cryptography", IEEE Transaction of Information Theory, IT-22, 6, pp.644-654, 1976

[32] S. Jang, J. Jeong, "Cost-Effective and Distributed Mobility Management Scheme in Sensor-Based PMIPv6 Network with SPIG Support", JIWIT, August, August 2012.

※ 이 논문은 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (NRF-2010-0024695). 교신저자: 정 종 필

저자 소개

임 일 균(정회원)

- 2013년 : 삼성SDS CSP 연구소(비즈니스아키텍처)
- 2013년 : 성균관대학교 정보통 대학원 컴퓨터공학과 석사 과정

<주관심분야 : 무선/이동 네트워크, USN, 시스템 보안, IT융합, 암호화 알고리즘 등>

정 종 필(정회원)

- 2008년 : 성균관대학교 정보통신대학 (공학박사)
- 2009년 : 성균관대학교 컨버전스연구소 연구교수
- 2010년~현재 : 성균관대학교 정보통신대학 겸 산학협력단, 산학협력중점교수

<주관심분야 : 모바일컴퓨팅, 센서 이동성, 차량 모바일 네트워크,네트워크 보안, 스마트 기기 보안, IT융합, 인터랙션사이언스 등>