로밍 동의에 기반한 중첩 NEMO 환경을 위한 지역 인증 기법에 관한 연구☆

Loaming Agreement based Localized Authentication for Nested NEMO Environment

임 형 진* 정 태 명**
Lim Hyung-Jin Chung Tai-Myoung

요 약

이 논문은 NEMO 환경에서 AAA 서비스를 제공하기 위한 효율적인 접근을 제안한다. 이는 ISP (Internet service provider)들 간에 로밍 동의에 기반한 지역 인증 기법을 사용하고 있다. 이를 위해 우리는 NEMO 도메인을 위한 공개키 인증 구조를 제시하였고, 방문 네트워크와 이동 개체 사이의 인증 뿐만이 아니라 이동 개체간에도 로밍 동의에 기반한 인증을 수행할 수 있는 프로토콜을 제시하였다. 본 논문의 결론에서는 기존에 제안된 AAA 개념에 기반한 접근보다 통신 지연에 있어서 평균 45% 향상된 성능을 보여준다.

Abstract

Authentication for inter-NEMO roaming is an important issue for achieving the seamless mobile networking. In this proposal, the technical challenge lies in the fact that a visited network does not initially have the authentication credentials of a roaming mobile router. This paper proposes an efficient approach for providing AAA service in NEMO environments. This approach uses localized authentication based on the roaming agreement between ISPs. A public key certificate structure is proposed, tailored to the business model of wireless Internet Service Providers (ISPs). In this approach, the mutual authentication between a visited network and a roaming user can be performed locally without any contact with user's home network. In conclusion, our protocol shown that communication delay can be reduced by average 45% overhead in communication delay than the previous AAA approach.

keyword : Network Mobility, AAA(Authentication, Authorization and Accounting), Authentication Protocol

1. 서 론

이동 노드가 방문 네트워크에 연결하고 인터넷 서비스를 이용하기 위해서는 적절한 인증 과정을 거치고 권한을 해당 네트워크로부터 할당 받아야 한다. 특별히, IETF 워킹 그룹에서는 최근에 네트워크 자체가 이동하는 이동 라우터 개념(Network Mobility: NEMO)을 제안하고 이를 지원하는 메커니즘을 제안하였다[1]. 이러한 환경에서 인증, 권한, 과금 (AAA) 에 관련된 프래임워크는 특정 네트워크 안에서 이동하는 이동 사용자를 인증할 수 있다. 특히 이와 관련하여 NEMO가 가능한 특정 시나리오에서 AAA(Authentication, Authorization, Accounting)에 대한 프로토콜과 구조를 제안한 연구방법 [2]이 있고. NEMO가 가능한 환경과 시나리오에서 AAA에 대한 요구사항과 가능한 AAA 프레임워크들을 제안한 방법[3]이 존재한다. 가장 최근의 작업으로서 J. Bournelle는 실제 환경에서 개발 가능한 NEMO 시나리오의 AAA 고려사항

* 정 회 원 : 금융보안연구원 선임연구원
dream.hjlim@gmail.com
** 정 회 원 : 성균관대학교 정보통신공학부 교수
tmchung@ece.skku.ac.kr
[2007/07/16 투고 - 2007/07/26 심사 - 2007/10/04 심사완료]
☆ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-C1090-0801-0028)

및 문제점을 제시하고 있다 [4]. 그러나 이 연구는 NEMO 시나리오에 generic AAA 개념만을 적용하였기 때문에 Nested NEMO 환경에서는 이동 개체의 신원을 해당 홈 네트워크로부터 확인하기 위해서 긴 지연 시간을 야기한다. 본 논문에서 우리는 기존의 NEMO AAA 연구에서 제시되었던 몇 가지 가능한 NEMO 시나리오 중에서 중첩 NEMO 시나리오에 효율적인 AAA서비스를 제공할 수 있는 인증 방안을 제시한다. 따라서 본 연구는 이전의 연구들에서 고려하는 일반적 AAA 개념에 비하여 더 실용적이고 효율적인 솔루션임을 제시하고자 한다.

2. 관련 연구

NEMO AAA에 대한 이전의 연구들은 "버스에서의 PAN(Personal Area Network)"의 경우에 대하여 가능한 3가지 시나리오를 제시하였다. 첫 번째는 이동 라우터 기반(Mobile Router: MR)의 PAN 토폴로지에 초점을 맞춘 시나리오이다. 두 번째는 MR 기반의 버스 토폴로지에 초점을 맞춘 시나리오이다. 세 번째는 MR기반의 버스에 MR-PAN이 접속했을 때 시나리오를 제안하고 있다. 특히, 이 시나리오는 NEMO에서만 발생할 수 있는 중첩 토폴로지를 나타내고 있다 [2][3].

PAN 내부의 이동 노드 장치들은 일반적으로 단순한 기능을 한다. 예를 들면 핸드폰, MP3 플레이어 등 개인 주변 장치들 형태로 존재한다. 따라서 Saber Zrelli는 첫 번째 시나리오에 대해서 이들의 인증은 MR-PAN이 직접 인증하는 것이 적합함을 제시하였다 [3]. 마찬가지로 두 번째 시나리오도 MR로 방문한 방문 이동 노드 (Visiting Mobile Node: VMN)에 대한 인증을 MR-Bus가 직접 수행한다. 즉 토폴로지적으로 보았을 때 두 시나리오는 하나의 MR과 그 하위에 MN가 위치하는 토폴로지를 구성하고 있다. 이상의 두 개의 시나리오는 비록 일반적인 AAA 개념을 적용한다고 하더라도 이동 개체가 방문 네트워크의 엑세스 라우터(Access Router: AR)와 MR 자신의 홈 네트워크 만을 통해 신원을 확인 할 수 있다. 이는 이동 호스트 환경의 인증 절차와 동일하다.

마지막 시나리오에 대해서 Saber Zrelli과 Julien Bournelle는 AAA 서비스 제공을 위해 MR기반의 버스와 액세스 네트워크의 ISP들간에 서비스 레벨에 관련된 동의가 필요하다는 것을 지적하고 있다 [3][4]. 그러나 하위 레벨의 PAN-MR에 대해서는 두 ISP중 하나에 속할 수 있음을 언급하고 있다. 그러나 실제 환경에서 중첩을 구성하는 이동 개체들이 각기 서로 다른 ISP에 포함 될 수 있다. 마찬가지로 BUS-MR이 반드시 하나의 ISP만을 통해서 서비스를 받는 환경만이 존재하지는 않는다. 또한 이전의 연구들에서 고려하지 않은 것으로서 서로 다른 관리 도메인에 소속된 MR간도 네트워크 간에 로밍 관계가 명시적으로 설정되어야 한다는 것이다. 그 이유는 중첩을 구성하는 NEMO환경에서 상위 방문 네트워크에 접속하기 위해서는 다른 관리도메인에 속하는 중간 경로 MR 자원을 이용하기 때문이다. 특히 Julien Bournelle는 이러한 토폴로지적 특성을 가질 수 있는 MR에 대하여 이동 NAS(Network Access Server)로서 명칭하고 있다.

이러한 환경에서 일반적인 AAA 개념이 적용될 경우 최하위 이동 개체는 최악의 경우로서 모든 개체들이 서로 다른 관리 도메인에 포함될 때의 경우에는, 매 핸드오프 발생시 중첩 레벨의 수만큼 해당 AAA들에 대해서 신원 확인 요청을 해야 한다. 따라서 다중의 ISP에 의해 신원 확인을 거쳐야 하는 NEMO 환경에서는 끊김 없는 이동성 지원을 위해 최소 통신 지연을 가질 수 있는 인증 방안이 필요하다.

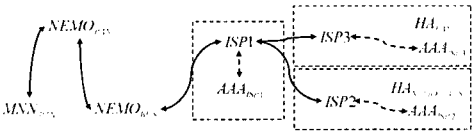
3. 로밍 동의 방식에 기반한 지역 인증 기법

M. Long은 로밍 관점에서 이동 단말에 대한 지역 인증 기법을 제안했다 [5]. 이는 다른 무선 ISP들 간에 로밍을 위해 인증 프로토콜과 결합된

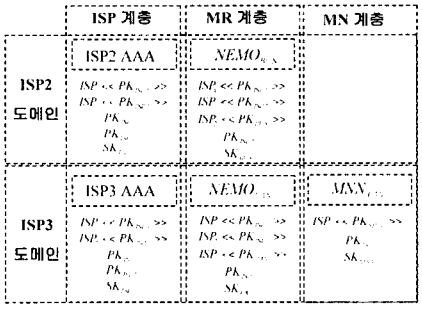
실용적인 공개키 인증 구조를 제안했다. 이 프로토콜은 상업용 CA(Certificate Authority)에 의해 발행되지 않고 해당 ISP로부터 직접 발행되는 인증서 기반의 구조를 제안했다. 우리는 본 절에서 이동 단말 중심의 M. Long의 제안 프로토콜을 다중 ISP에 의한 로밍을 요구하는 중첩 NEMO환경에 적합하도록 확장 적용한다.

3.1 NEMO 도메인을 위한 공개키 인증 구조

그림 1은 이전 절에서 논의 한 Julien Bournelle의 중첩 NEMO 시나리오인 "MR-BUS 안에 MR-PAN" 경우를 나타내고 있다[1]. 우리는 그림 1-(a)에서 보여주는 것과 같이 세 개의 ISP가 존재하는 환경을 고려한다. ISP1은 다른 두 ISP에 속하는 이동 개체들에게 액세스 네트워크 서비스를 제공한다. ISP2는 $\neq MO_{PAN}$의 홈 네트워크이다. ISP3는 $\neq MO_{BUS}$의 홈 네트워크이다. 각 ISP는 자신의 이동 개체에 대한 HA(home agent)와 AAA 서버를 보유하고 있으며, 자신의 개인키와 공개키 쌍인 SK와 PK를 생성한다.



(a) 중첩 NEMO 시나리오 : 버스에서의 PAN



(b) ISP들에 의해 형성되는 공개키 인증 구조

(그림 1) 공개키 인증 구조

1) MR-BUS(모바일 라우터를 탑재한 버스 네트워크를 의미함), MR-PAN(Personal Area Netwrok을 구성하며 모바일 라우터를 통해 외부와 통신이 가능한 네트워크를 의미함)

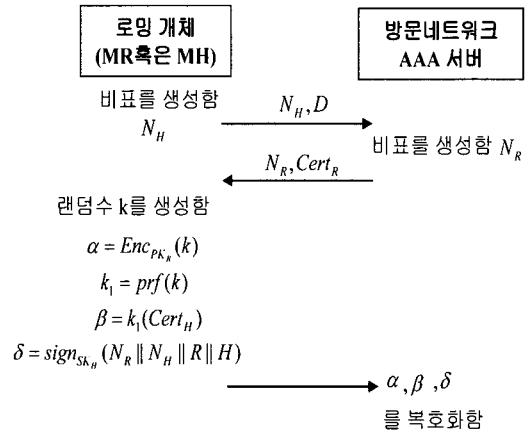
한 예로서, 그림 1에서 ISP2는 자신의 개인키 PK_{NO1}가 ISP1과 ISP3의 개인키들인 SK_{AO1}과 SK_{AO2}에 의해 서명되는 것을 허용한다. 또한 ISP2의 공개키 인증서는 $AO_1 \ll PK_{NO} \gg$와 $AO_2 \ll PK_{NO} \gg$로서 표현될 수 있다. 또한 ISP2는 다른 두 개의 ISP들을 위해 공개키 PK_{AO1}와 PK_{AO2}를 얻을 수 있다. 일반적으로 임의의 ISP가 n-1개의 ISP들과 로밍 관계를 가질 경우, 해당 ISP는 자신의 개인키 하나와, n-1개의 자신의 인증서와 n-1개의 다른 ISP들의 공개키가 저장된다. 따라서 한 개의 ISP의 AAA서버에 저장되는 키의 수는 2n-1개가 된다. 하나의 ISP는 이동 라우터나 이동 호스트와 같은 자신의 가입자들에게 공개키와 개인키의 쌍으로서 인증서를 발급하게 될 것이다. 이때 우리는 이동 라우터와 이동 호스트들에 대해서 다른 설정 방안을 선택한다. 한 예로서, ISP3에 있는 이동 호스트 가입자는 자신의 해당 공개키 인증서 $AO_1 \ll PK_{MNN} \gg$와 개인키 SK_{MNN}을 할당받는다.

부가적으로 자신의 홈 ISP의 공개키 PK_{AO2}는 MR의 ISP 혹은 방문 네트워크의 공개키를 인증하기 위해서 홈 네트워크로 부여될 것이다. 그러므로, 이 경우 호스트에 의해 저장되는 키들의 개수는 3개가 된다. 반면에, 그림 1에서 ISP3로의 이동 라우터 가입자($\neq MO_{PAN}$)는 부가적으로 로밍 동의에 관련된 ISP들의 인증서들을 함께 저장한다. 비록 부가적으로 ISP 인증서를 MR들이 저장한다고 하더라도 n 개 로밍 ISP가 존재 하더라도 MR당 n+2개 키만을 저장하게 된다.

3.2 지역 인증 프로토콜

우리는 로밍하는 이동 라우터나 호스트와 방문 네트워크 사이에 초기 인증절차를 중점적으로 기술을 한다. 그러나 우리의 제안 프로토콜은 MR이 로밍에 관련된 자신의 ISP의 공개키를 가지고

있기 때문에 중첩을 구성하는 MR들 사이나 혹은 MR과 VMN간의 인증을 가능케 할 수 있다. 그림 2에서는 NEMO네트워크를 구성하는 MR이 방문 네트워크에 접속하였을 때 인증 협상 과정을 나타내고 있다. 그림2에서 나타나는 개별 플로우는 가장 상위의 것부터 번호부여가 되며 세부적으로 설명하면 다음과 같다.



(그림 2) NEMO 네트워크를 위한 인증 프로토콜

■ 플로우 1 과 플로우2 : 이 두 플로우에서는 제안 프로토콜의 초기 부분으로서 보안 서비스에 대한 협상을 위해 동작한다. 여기서 N_R은 재전송 공격(replay attack)을 막기 위해 MR의 비표(nonce)로서 이용된다. D는 현재 로밍 상태의 MR의 도메인 네임이며, 방문 네트워크는 MR의 도메인 네임을 결정하기 위해 이를 사용할 수 있다. 부가적으로 서버는 MR의 개인키 SK_S를 사용하여 $N_R \| N_S$ 메시지를 서명한다. '||'는 결합 연산자를 뜻한다. 플로우 1에서 도메인 네임이 주어지게 되면, 방문 네트워크의 AAA서버는 해당 도메인 D에 의해 서명된 자신의 인증서를 조회한다. 만약 해당 인증서가 존재하지 않는다면 제안 프로토콜은 이 단계에서 인증 절차를 중지한다. 만약 해당 인증서가 존재한다면, 로밍 MR에게로 서버의 비표 N_S와 인증서 $Cert_S$를 전송한다.

■ 플로우 3: MR이 방문 네트워크의 인증서를 받았을 때, MR은 이 인증서를 검증하기 위해 자신의 홈 네트워크의 공개키를 이용한다. 인증서에 대한 검증이 성공적으로 끝나게 되면, MR은 자신의 개인키 SK_R을 사용하여 $N_S \| N_U \| S \| R$ 메시지를 서명하게 된다. 여기서 S와 R은 로밍 MR과 방문 네트워크의 신원을 표시한다. 여기서 전송 메시지가 비표(nonces)를 포함하는 것은 재전송 공격과 참여자의 신원을 보호하기 위해 일반적으로 사용되는 방식이다. R은 사전 마스터 키로서 랜덤 수 k를 선택하고 $Cert_S$에서 방문 네트워크의 공개키 SK_R를 사용하여 $\delta \| k$를 암호화 한다. 이때 MR은 사전 마스터 키를 사용하여 쉐도우 랜덤 함수 prf(·)를 키 유도함수로서 사용한다. 이 유도 함수는 표준 HMAC-SHA-1[6]을 사용하여 구현될 수 있다. 랜덤 수는 결과적으로 AES-128 [7]과 같은 대칭키 암호 방식을 통해 MR의 인증서 $Cert_R$을 암호화 하는데 사용될 수 있다.

■ 서버의 증명: 플로우 3으로부터 방문 네트워크는 자신의 개인키 SK_R을 사용하여 사전 마스터 키 k를 얻기 위해 수신된 메시지를 복호화하게 된다. 즉, 랜덤수를 복구하기 위해 사전 마스터 키로 공개적으로 알려진 쉐도 랜덤 함수를 사용하여 MR의 인증서를 복호화하기 위해서 사용한다. 방문 네트워크는 MR의 홈 도메인의 공개키의 인증된 복사본을 가지고 있기 때문에, 시그네쳐 $Sign_{SK_R}(N_S \| N_U \| S \| R)$의 검증과 MR의 인증서의 인증을 검증할 수 있다. 이때 모든 증명이 검증된다면, 방문 네트워크와 로밍 MR은 두 개의 비표와 사전 마스터 키에 기반하여 공유 비표(shared secret)를 유도할 수 있다. 이때 방문 네트워크 서버와 MR은 공개 키가 설립될 수 있기 때문에 성공적인 상호 인증을 수행 할 수 있다. 따라서, 로밍 MR이 부수적으로 방문 네트워크에서 핸드오프 할 때 공유키는 인증을 위해 사용될 수 있다.

4. 보안 분석 및 성능평가

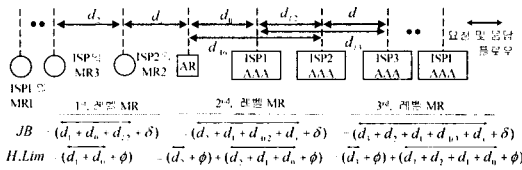
4.1 보안 분석

본 논문에서 제안된 프로토콜은 공개키 기반 구조를 요구한다. 우리는 본 논문에서$SK_{(L)}$ ($L \geq 1$, 정수)는 이동 개체에만 알려져 있다고 가정한다. 또한 이동 개체는 자신의 홈 네트워크의 공개키를 가진다. 부가적으로 방문 네트워크의 개인키는 방문 네트워크 자체가 소유하고 있으며 쉐도우 랜덤 수 생성기는 이동 개체를 제외하고 다른 어떤 참여자도 예측하지 못하는 수준으로 안전하다고 가정한다. 이러한 가정에 기반 할 때, 우리는 본 논문의 제안 프로토콜에 대해서 재전송 공격 및 위장 공격의 보안성을 분석하고자 한다.

플로우 1의 메시지 1과 플로우 2의 메시지 2는 방문 네트워크와 이동 개체의 비표를 서로 교환한다. 제안 프로토콜은 공개키 인증 구조에 기반하기 때문에 로밍하는 이동 개체는 방문 네트워크의 공개키 인증을 검증할 수 있다. 그러나 가짜 혹은 위장된 네트워크는 합법적인 네트워크로서 개인키를 가지지 않는다. 따라서 적합한 사전 마스트 키를 얻기 위한 메시지 3을 복호화 할 수 없다. 결과적으로 이동 개체와 보안 연계를 설립할 수 없다.

다른 경우로서, 악의적인 이동 개체는 ISP에 의해 인증된 합법적인 공개키를 가지지 않는다. 그러므로 악의적인 이동 개체는 두 개의 생성된 비표에 대한 서명을 수행할 수 없다. 따라서, 방문 네트워크는 메시지 3을 수락 할 수 없으며, 메시지 3에서 타당한 서명 검증을 수행 할 수 없다. 프로토콜에서 생성되는 비표들은 이동 개체의 서명이 현재 진행된 프로토콜 과정에서 생성된 것임을 보장하며, 따라서 공격자는 재전송 공격에 성공할 수 없으며 방문 네트워크와 이동 개체 사이에 위치한 임의의 공격자는 사전 마스터 키를 유도할 수 없다. 그러므로 중간 경로의 악의적인 공격자는 합법적인 이동 개체나 ISP에 대하여 보안 연계를 설립할 수 없다. 또한 메시지 3에서 공개키 암호에 포함되는 해쉬 서명은 암호문 a와 서명문 δ 이 특정 세션에서만 유효함을 보장한다. 공격자가 다른 인증 세션들로부터 암호문 a와 서명문 δ를 수집한다고 하더라도 하나의 인증 세션에서 타당한 메시지 3를 구성하기 위해 이것들을 조합하여 사전 마스터 키를 생성할 수 없다.

4.2 성능 평가



(그림 3) 로밍 MR에 대한 인증 절차 비교 평가

그림 3은 제안 프로토콜을 평가하기 위한 시스템 모델과 관련 통신 지연 및 처리 지연을 나타내고 있으며, 기존 JB의 제안과 본 논문의 프로토콜이 중첩 NEMO 환경에서 인증 절차를 나타내고 있다. ISP1에 속하는 AR하위에 ISP2에 포함되는 MR2가 연결되어 있다. 또한 그 하위에 ISP3에 포함되는 MR3가 연결되어있다. NEMO의 중첩 계층은 하나의 IP 헤더가 수용할 수 있는 중첩 정보 크기를 고려할 때 논리적으로 40계층까지 구성이 가능할 수 있다. 따라서 L계층까지 구성 가능함을 나타내고 있다. 해당 MR에 대한 ISP들이 인터넷에 연결되어 있다.

JB의 경우 1 레벨의 MR2 경우 네트워크 연결에 대한 서비스 권한을 부여 받기 위해서는 자신의 AAA로부터 인증 확인 과정을 거쳐야 한다. 따라서 우선 AR을 통해 해당 ISP1으로 인증 요청을 전송한다. 이 경우 $\overrightarrow{d_1 + d_0}$비용이 포함된다. ISP1의 경우 이 요청을 수신하고 해당 MR2의 ISP2의 AAA서버로 인증 요청을 $\overrightarrow{d_{f2}}$만큼의 전송 지연으로 전송하게 된다. ISP2의 AAA는 해당 요청을 수신 및 확인 하고(δ) 응답을 자신의 MR2

로 $\overrightarrow{d_1 + d_0 + d_{P2}}$전송하게 된다. 그림 3에서는 JB에 대하여 중첩 계층이 증가하는 경우 각 계층에서의 처리 과정을 보여주고 있다.

반면에 본 논문의 제안에서는 1레벨에서의 MR2는 $\overrightarrow{d_1 + d_0}$만큼의 전송 지연을 통해 ISP1의 AAA서버에 인증 요청을 하게 된다. 이때 해당 AAA서버는 인증 요청에 대하여 이전 절에서 제시된 프로토콜에 따라 로밍 동의된 MR인지를 확인하며(Φ) 응답을 MR2로 전송하게 된다. JB와 마찬가지로 중첩 계층이 증가함에 따른 인증 확인 절차는 동일한 결과를 갖게 된다. 다음 식(1)과 (2)는 그림 3의 인증절차에 따라 각 계층에서의 요구 지연 및 처리 지연에 대한 평가 결과를 수치적으로 표현하고 있다.

$$JB = \sum_{j=1}^{L} \overline{d_i} + \delta + \begin{cases} d_0 + d_{P2} & , L = 1 \\ d_{AtL} + d_x + d_0 & , L > 1 \end{cases} \quad (식1)$$

$$H.\mathrm{Lim} = \overline{d_L} + \Phi + \begin{cases} d_{1+} d_0 & , L = 1 \\ \sum_{i=0}^{L} \overline{d_j} + \Phi & , L > 1 \end{cases} \quad (식2)$$

우리는 두 제안의 통신 지연을 평가하기 위해서 아래와 같은 가정을 한다. 식(1)에서 나타내는 JB의 제안의 경우 중첩 레벨이 1일때(L=1), 서버의 인증 처리시간(δ), AR로부터 ISP1의 AAA서버로의 전송 지연(d_{P2}), 그리고 d_1 에 대한 무선 링크의 전송 지연만이 소요된다. 그러나 중첩 레벨이 1이상의 경우는 계층 레벨 1에서 소요 되는 지연 시간 이외에 부가적으로 방문 네트워크로부터 자신의 홈 네트워크로의 인증 요청 메시지의 전송 지연 시간(d_{AtL})을 포함하게 된다. 그러나 식(2)에서 나타내는 본 논문의 제안안 경우에는 방문 이동 개체는 자신 현재 중첩 레벨에서 접촉하는 상위 이동 라우터와의 인증 한번과 방문 네트워크 AAA 서버와 인증 한번을 요구한다. 따라서 중첩 레벨 1인 경우는 전자의 경우 지연($\overline{d_1} + \Phi + d_{1+} d_0$) 만을 포함하고, 중첩 레벨 2 이상인 경우는 전자 및 후자 모든 경우에 소요되는 지연($\overline{d_L} + \Phi + \sum_{i=0}^{L} \overline{d_j} + \Phi$)을 포함하게 된다.

$d_1 = d_2 \cdots = d_L (L > 1)\, L$: 중첩 레벨 (가정 1)

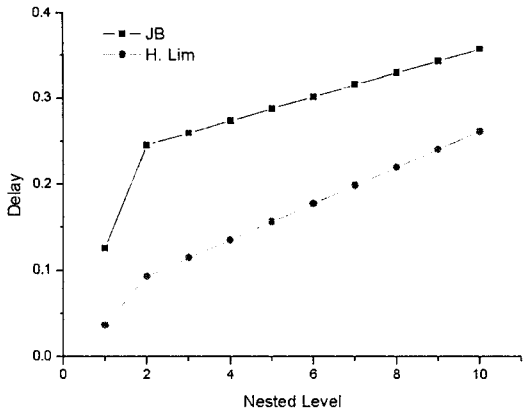
$d_0 < d_1 < d_{Ix} \simeq d_{Aty} \simeq d_x (x, y = 1 \ldots L)$(가정2)

그림 3에서 식 1과 2는 MR에 의해 요구되는 통신 지연을 보여주고 있다. 또한 표 1은 평가를 위한 지연을 야기하는 실제 값과 파라메터[5]를 나타내고 있다. 우리의 목적은 관련 ISP들 사이에 공개키에 기반한 동의를 가정하고 있다. 그러므로, 비록 중첩 레벨이 증가한다고 하더라도 그림 4와 5는 우리의 제안이 자신의 ISP AAA로 인증을 확인해야하는 통신 지연으로 인해 JB 접근보다 더 적은 영향을 가진다는 것을 보여주고 있다. 즉 우리의 제안 프로토콜이 전체 인증 절차상에 두 개의 인증 플로우를 실행 한다고 하더라도, 더 적은 통신지연을 보여주고 있다.

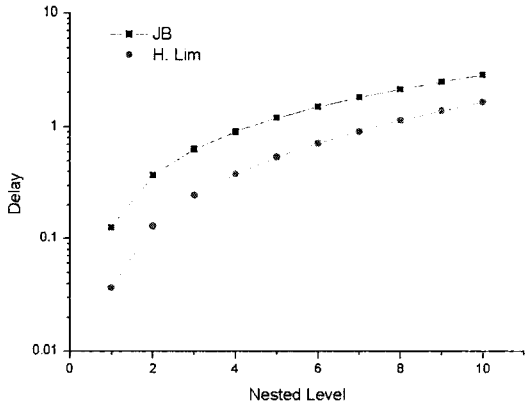
즉 , 새로운 이동 개체가 더 낮은 중첩 레벨로서 현재의 인증 중첩 네트워크에 접속한다고 하더라도, 해당 이동 개체는 상위에 이미 인증된 이동라우터와 인증 절차를 거쳐야 한다. 마찬가지로 해당 이동 개체는 현재 방문하고 있는 AAA서버와 같은 절차를 수행해야한다.

(표 1) 평가에 사용된 파라메터

파라메터	내용	값
d_L	무선 링크에서의 전송 지연	7ms
$d_{At\,Y}, d_x, d_{Ir}$	ISP 간 혹은 ISP로의 평균 전송 지연	53.4ms
Φ	암호 계산에 소요되는 지연 시간	14.52ms
d_o	AR로부터 ISP1의 AAA서버로 전송지연	0.5ms
δ	AAA서버에서 인증 처리 시간	4ms



(그림 4) 각 계층에서 MR의 인증 처리 시간



(그림 5) 각 계층에서 전체 인증 처리에 대한 총 소요시간

그림 4와 5는 는 계층에 따른 MR 인증 처리 지연 시간을 나타내고 있다. 그림 4는 각 계층에서 요구되는 인증 처리 요구량을 의미하며, 그림 5의 경우 상위 계층의 MR을 포함한 누적된 인증 처리 시간의 누적량을 보여주고 있다. 우리의 제안은 기존의 JB보다 중첩이 증가하더라도 더 좋은 효율을 보여주고 있다. 특히 중첩 레벨 증가하더라도 더 적은 지연 증가율을 보여주고 있다.

5. 결론

로밍을 요구하는 이동 단말 환경과는 달리 NEMO 환경에서는 각 이동 개체들이 속한 서비스 도메인에 따라 각 이동개체의 홈 네트워크로의 복잡한 인증 참조를 요구한다. 따라서 중첩 NEMO 환경에서는 현재 접촉을 시도하는 이동 개체 상위로 연결되는 이동 라우터들이 각기 다른 서비스 도메인에 속한다면 현재의 중첩 계층 만큼의 인증 처리 지연을 소비하게 된다. 기존의 연구들이 NEMO 환경에 일반적 AAA 개념에 기반하여 로밍의 요구사항을 간접적으로 제시하였다면, 본 논문은 중첩 NEMO 환경이라고 하더라도 짧은 인증 처리 시간을 제공할 수 있는 구체적인 로밍 구조와 절차를 제공하고 있다. 따라서 본 논문은 다중 ISP와 관련되어 있는 중첩 NEMO 환경이라 하더라도 기존 일반적 AAA 개념에 비하여 심각한 통신 지연 없이 이동 개체와 ISP들에게 효율적 인증을 수행할 수 있는 솔루션을 제공하고 있다.

본 논문에서 제안된 프로토콜은 PANA[9]와 같이 현존하는 AAA 프레임워크에 하나의 모듈로서 더해질 수 있다. 그러나 우리의 프로토콜은 동일한 인증 절차를 두 번 수행하고 있기 때문에 향후 연구로서 우리의 인증 프로토콜에 대한 보안 분석을 통해 프로토콜 최적화를 수행하는 것이 필요하다. 이를 통해서 중첩 NEMO 환경과 같은 복잡한 네트워크설정을 요구하는 실제 환경에 도입함에 있어서 아직까지 구체적으로 제시되고 있지 못하는 인증 및 접근제어 절차에 대한 방향성을 제시할 수 있을 것이다.

참 고 문 헌

[1] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility Basic Support Protocol", IETF, RFC3963, Jan. 2005.

[2] C. Ng and T. Tanaka. "Usage Scenario and Requirements for AAA in Network Mobility Support", http://www.mobilenetworks.org/nemo/drafts/ draft-ng-nemo-aaa-use-00.txt, 2002.

[3] S. Zrelli, T. Ernst, J. Bournelle, G. valadon and D. Binet., "Access Control Architecture for Nested Mobile Environments in IPv6", 4th Conference on Security and Network Architecture, Jun. 2005.

[4] J. Bournelle, G. Valadon, D. Binet, S. Zrelli and J. Combes,"AAA Considerations within Several NEMO deployment Scenarios", 1st workshop on network mobility, Japan, Jan. 2006.

[5] M. Long, C. Wu and J.D. Irwin, "Localized authentication for inter-network roaming across wireless LANs", IEE Proc.-Commun., Vol. 151, No. 5, Oct. 2004.

[6] M. Abadi, and R. Needham, "Prudent engineering practice for cryptographic protocols", IEEE trans. softw. Eng., 1996.

[7] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: keyed-hashing for message authentication", RFC2104, Feb. 1997.

[8] FIPS PUB 197, "Advanced encryption standard", Nov. 2001.

[9] D. Forsberg, Y. Ohba, B.Patil, H. Tschofenig, and A. Yegin., "Protocol for Carrying Authentication for Network Access", Internet draft, IETF, Jan. 2005,

◐ 저 자 소 개 ◑

임 형 진(Lim Hyung-Jin)

1998년 2월 한림대학교 컴퓨터공학과 졸업(학사)
2001년 8월 성균관대학교 정보통신대학원 정보통신공학과 졸업(석사)
2006년 8월 성균관대학교 대학원 컴퓨터공학과 졸업(박사)
2007년 8월 성균관대학교 BK21 Post-Doctor
2007년 10월~현재 금융보안연구원 인증관리팀 선임연구원
관심분야 : IP 이동성 관리 기술 (NetImn, Network Mobility, Ad-hoc Mobility 등), VPN 기술 (MPLS, IPSec, SSL 등), AAA(Authentication, Authorization and Accounting) 및 접근제어, 키 관리 및 인증 프로토콜, 강한 사용자 인증 기술(One Time Password 및 Multi-factor Authentication)
E-mail : dream.hjlim@gmail.com

정 태 명(Chung Tai-Myoung)

1981년 2월 연세대학교 전기공학과 졸업(학사)
1984년 6월 일리노이 주립대학 전자계산학과 졸업(학사)
1987년 12월 일리노이 주립대학 컴퓨터공학과 졸업(석사)
1995년 8월 퍼듀 대학 컴퓨터공학 (박사)
1995년 9월~현재 성균관대학교 컴퓨터공학과 교수
2005년 ~ OECD 정보보호작업반(WPISP1) 부의장
2007년 ~ 현재 한국CPO포럼 의장
2000년 ~ 현재 한국침해사고대응팀협의회(CONCERT) 위원장
관심분야 : 실시간시스템, 네트워크 관리, 네트워크 보안, 시스템 보안, 전자상거래 보안
E-mail : tmchung@ece.skku.ac.kr