홈 게이트웨이에 기반한 가입자망에서의 인증 프레임워크

The Authentication Framework in Access Network based on Home Gateway

이원구*, 윤화묵*, 최병선**, 이성현**, 이재광**
한국과학기술정보연구원*, 한남대학교 컴퓨터공학과**
Won-Goo Lee, Hwa-Mook Yoon(wglee, hmyoon)@kisti.re.kr*,
Byung-Sun Choi, Seoung-Hyeon Lee, Jae-Kwang Lee
(bschoi, shlee, jklee)@netwk.hannam.ac.kr**

요약

현재, 홈 네트워크 보안에 있어 정보기기의 다양성과 기기간 자원의 공유 등으로 고려해야 할 요구사항은 더욱 복잡하고 다양한 특성을 지니게 된다. 따라서 홈 네트워크를 구성하는 다양한 통신매체나 프로토콜 등과 관계없이 요구되는 보안 기능을 만족할 수 있는 보안 프레임워크가 정립되어야 한다. 이에 본 논문에서는 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈 네트워크 모델에서 활용될 수 있는 보안기술을 가지고, 여러 가지의 제안된 메커니즘을 통해 모바일 호스트(사용자)가 댁내의 디바이스에 대해 안전하게 제어할 수 있는 보안 프레임워크를 구성하고, 성능을 검증하였다.

■ 중심어 : | 가입자 망 인증 | 인증 프레임워크 | 홈 게이트웨이 |

Abstract

Today, home networking security shows the complicated and various characteristics of requirements for consideration because of the variety of information appliances and share of resources among them. Therefore, security framework to satisfy with security functions is arranged ,regardless of the variety of communication medium and protocols. Thus, we construct security framework for mobile host(or user) to securely control devices in home-network through the variety of suggested mechanism, with security mechanism to be available for future home networking model, and verified the performance of our model.

■ Keyword : | Access Network Security | Authentication Framework | Home Gateway |

I. 서 론

유비쿼터스 세상은 언제 어디서나 컴퓨팅이 가능한 사회이다. 바꾸어 말하면, 언제어디서나 사이버 공격이 일어날 수 있고, 이로 인해 개인생활의 위협도 증가할 수밖에 없는 사회이다[1][2]. 이러한 유비쿼터스 컴퓨팅 환경으로 가는 시작점의 한가운데에 홈 네트워킹 환경이 자리잡고 있으며, 따라서 다양한 유·무선 네트워크와 프로토콜 등이 혼재하는 홈 네트워킹에서는 기존 인

* 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음.

접수번호 : #050311-002
접수일자 : 2005년 03월 11일
심사완료일 : 2005년 05월 09일
교신저자 : 이원구, e-mail : wglee@kisti.re.kr

터넷과 유비쿼터스 환경에서 발생할 수 있는 보안 취약성 뿐만 아니라 추가적으로 고려해야 할 보안 취약성이 존재하게 된다[2][4]. 따라서 홈 네트워크를 구성하는 다양한 통신매체나 프로토콜 등에 관계없이 요구되는 보안 기능을 만족할 수 있는 보안 프래임워크가 정립되어야 하며, 그 초석으로 인증 프레임워크의 정의가 반드시 필요하다.

이에 본 논문에서는 향후 유비쿼터스 컴퓨팅 환경에 근접한 홈 네트워크 모델에서 활용될 수 있는 인증기술을 가지고, 여러 가지의 제안된 메커니즘을 통해 모바일 사용자 혹은 인터넷 사용자가 댁내의 디바이스에 대해 안전하게 제어하기 이전에 필수적으로 지원되어야 할 인증 프레임워크를 구성하고자 하였다. 이를 위해, 2장에서는 홈 네트워킹 인증기법과 관련한 무선랜 및 모바일 보안에 대해 기술하고, 3장에서는 보안 프레임워크의 중심이 되는 홈 게이트웨이의 구조와 각각의 보안 모듈에 대해 살펴보며, 4장에서는 보안 홈게이트웨이를 기반으로 보안 프레임워크를 구성하였다. 5장에서는 이에 대한 성능을 평가하였으며, 6장에서는 결론을 맺기로 한다.

II. 홈 게이트웨이 보안구조

홈 게이트웨이/홈 서버(이후 홈 게이트웨이라 칭함)는 가정 내 홈 네트워크를 구성하는 유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경에서 통신과 제어 및 모니터링의 중심 역할과 더불어 외부 인터넷으로의 연결을 물리적으로 제공해 주는 장비이다[5]. 이를 위해 본 논문에서는 [그림 3]과 같이 기존의 기능을 포함한 보안 모듈, 미들웨어(프록시 기능 포함) 모듈을 기반으로 하는 홈 게이트웨이를 구성하였고, 그 중에서 이 시스템의 핵심인 보안모듈은 크게 상호인증 모듈, 접근제어 모듈, 명령어처리 및 암복호화 모듈, 디바이스 인증 및 서비스 지원 모듈로 나누어 볼 수 있다.

1. 상호인증 모듈

상호인증 모듈은 AAA 서버와 홈 게이트웨이 모듈간 그리고 홈 혹은 앵커 에이전트와 홈 게이트웨이 간의 상호인증을 위해 구현된 모듈이다.

우선, 이동 에이전트를 포함한 앵커 에이전트와 홈 에이전트간의 인증을 위해 AAA서버와의 상호인증을 하게 된다. 이 과정을 거쳐 이동 에이전트가 앵커 에이전트와 홈 에이전트 간에 인증을 하게 되고, 그 사이에 인증서버는 앵커 에이전트와 댁내망의 홈 게이트웨이와의 상호인증 절차를 거치게 된다. 이러한 일련의 과정을 상호인증이라 하며, [그림 1]은 이러한 상호인증 과정을 위한 홈 게이트웨이의 상호인증 모듈을 보여주고 있다.

이 모듈 중 가장 핵심적인 모듈은 AAA로부터 들어온 메시지에 대한 처리모듈인 AAA 인증처리모듈과 인증과정을 마친 후, 홈 에이전트와의 메시지 상호전송을 위한 세션키 생성 모듈이다.

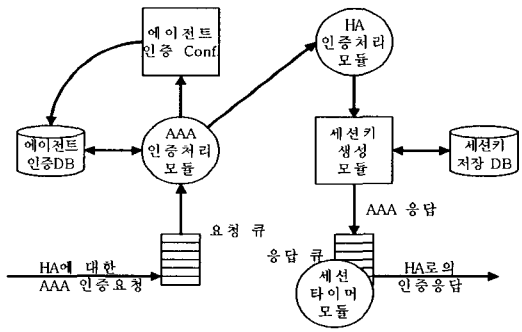

그림 1. 상호인증 모듈

2. 사용자 인증 및 접근제어 모듈

사용자인증 및 접근제어 모듈은 이전의 상호인증 모듈을 통하여 모바일 호스트로부터 홈 게이트웨이에 이르기까지 모든 개체들 간의 상호인증이 끝난 후(모바일 호스트와 홈 게이트웨이 간의 터널링이 끝난 후), 모바일 호스트와 홈 게이트웨이가 사용자의 ID와 패스워드를 가지고 원격에서 댁내망 내의 디바이스를 제어하기 위한 기초적 인증 및 접근제어 모듈이며, [그림 2]와 같다.

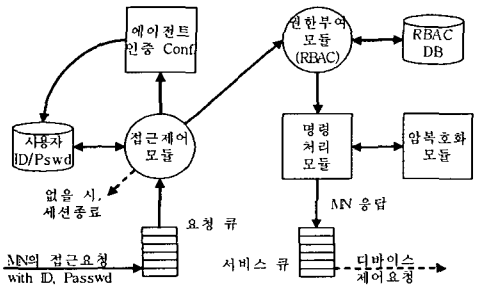

그림 2. 사용자인증 및 접근제어 모듈

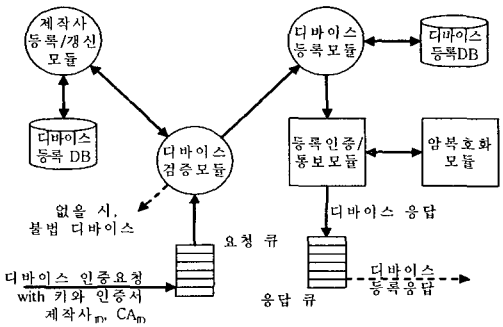

그림 3. 디바이스 인증 및 등록 모듈

우선, 모바일 호스트 사용자가 ID와 패스워드를 가지고 원격에서 홈 게이트웨이에 접속한다. 홈 게이트웨이는 사용자 ID와 패스워드 데이터베이스 안에, 전달된 사용자의 ID와 패스워드가 존재하는지 검사한다. 만일 데이터베이스에 없다면, 세션을 종료한다. 만일 존재한다면, 권한부여 모듈로 넘겨 해당 사용자에 대한 디바이스 제어에 대한 권한을 RBAC 정책에 기초하여 부여받는다. 본 논문에서는 권한부여를 위한 RBAC 정책이 실제로 어떻게 적용될지에 대해서는 연구하지 않았다.

이후, 명령처리 모듈에서는 권한을 부여받은 사용자로부터의 명령 메시지를 처리하고, 이를 원격제어를 위한 미들웨어 모듈로 보내고, 다시 넘겨받은 값에 의하여 다양한 프로토콜에 제어되는 디바이스들을 제어하게 된다.

3. 디바이스 인증 모듈

디바이스 인증에 관해서는 현재 미들웨어 수준에서 제공되고 있다. 디바이스 유효성 확인을 위한 일련 번호(serial number)나 인증서 등은 개별 제조업체 등에서 자체적으로 발행하고 있어 향후 디바이스에 대한 다양한 사후 서비스 제공이나 유비쿼터스 컴퓨팅 환경에서 디바이스 및 사용자 인증 기능과 결합한 새로운 서비스의 제공을 위해서는 디바이스 인증정보에 대한 통일된 발급체계 및 관리체계에 대한 기술적, 정책적인 연구가 필요하다.

본 논문에서는 개별 제조업체가 표준을 준수하여 인증서를 발급하고 있으며, 홈 게이트웨이는 표준에 근거하여 이를 검증할 수 있다고 가정한다. 또한, 인증서에 대한 발급은 디바이스에 키와 인증서가 발급되었다고 가정하며, 그 처리절차는 [그림 3]과 같다.

4. 에이전트 모듈

본 논문의 홈 네트워크 상에서 동작되는 에이전트는 외부 에이전트, 앵커 에이전트, 홈 에이전트로 나눌 수 있다. 하지만, 이들은 상황에 따라 서로의 역할이 바뀔 수 있으며, 기본적으로는 크게 그림 4에서와 같이 전자서명 모듈, 암복호화 모듈, 해싱 기능으로 나누어 생각할 수 있으며, 이는 기존의 MD5(혹은 ECDSA), RSA (혹은 AES/Rijandael) 및 HAS256(ECMQV) 알고리즘의 기능을 따른다. 이에 본 절에서는 에이전트에 대한 공통적인 기능만을 기술하기로 한다.

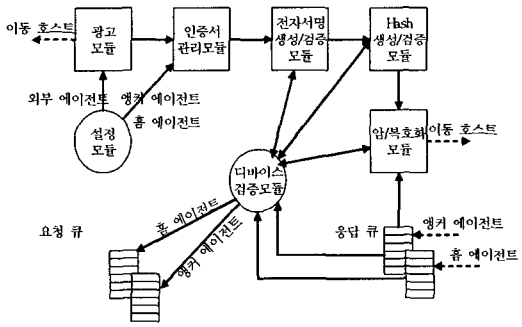

그림 4. 에이전트 인증 및 등록 모듈

에이전트에는 무선랜 카드와 유선랜 카드를 각각 1개씩 필요로 한다. 무선랜 카드는 클라이언트와의 통신을 담당하며, 유선랜 카드는 AAA 서버를 비롯한 유선랜과의 통신을 담당한다. 세부적인 모듈로는 인증서 관리 모듈, 전자서명 생성/검증모듈, 해싱 및 암/복호화 모듈, 디바이스 검증모듈 등으로 구성된다.

III. 인증 프레임워크

1. 기존의 인증 프레임워크

1.1 공개키 기반 인증 프레임워크

비밀키 기반 인증 메커니즘은 상대와 통신을 하기 전에 안전한 방법으로 상대방과 비밀키를 나누어 가져야 한다. 따라서 비밀키는 키 분배 방법에 있어서 유연성이 떨어지고 특히 많은 사용자를 수용하기에는 적당하지 못하다는 한계점이 있다. 또한 상업적인 면에서 필요한 부인방지 서비스가 없다는 면을 극복하기 위하여 공개키를 기반으로 한 인증 메커니즘이 제시되었다.

비밀키 기반 메커니즘이 MAC 값을 사용하는 반면 공개키 기반 메커니즘은 공개키를 이용한 전자서명을 사용한다. 공개키 기반 인증 메커니즘에서는 인증과 관련된 내용을 담은 확장인증서(certificate extension)를 모든 제어메시지 뒤에 추가하도록 정의하여 인증과 관련된 정보를 주고받는다.

여기서는 이동 호스트, 외부 에이전트, 홈 에이전트 간에 서로에 대한 인증을 한다. 메시지를 새로 만들거나 받은 메시지를 전달하는 경우, 메시지 뒤에 전자서명을 추가함으로써 메시지가 변하지 않았다는 것을 확인시키고, 또한 자신이 메시지를 만들었음을 증명할 수 있다.

그러나 이 메커니즘은 세 참여자 서로에 대한 인증 메시지를 받고, 전달할 때마다 수행한다. 등록과정에 참여하는 세 참여자가 모두 서로에 대한 신뢰 가능한 인증을 할 수 있기 때문에 보안측면에서 이상적이나 반복되는 인증은 성능저하를 가져올 수 있다는 단점을 가지

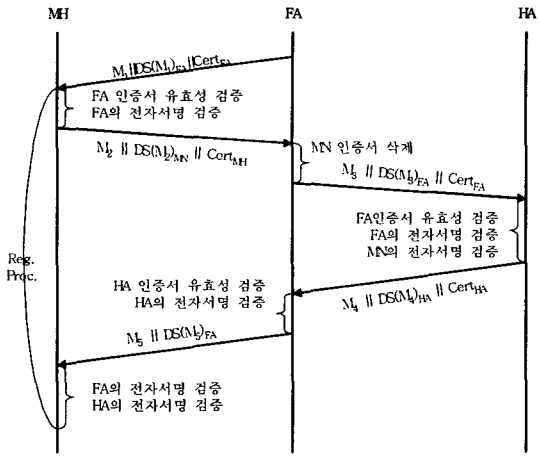

그림 5. 공개키 인증절차

고 있다. 또한, 이 메커니즘에서 사용하는 RSA 알고리즘이 암·복호화의 비용이 높아 인증서를 증명하기 위한 인증서 검증 작업과 함께 이동 호스트에게 성능저하를 가져올 수 있다. 공개키 기반 인증과정 및 문제점은 [그림 7]에서 보여지고 있다.

1.2 최소 공개키 기반 인증 프레임워크

최소 공개키 기반 인증 메커니즘은 공개키 기반 인증이 가진 단점을 줄인 방법으로 공개키 암호화를 최소로 사용한다. [그림 6]에서와 같이 이동 호스트는 모든 암호화 동작을 비밀키 기반으로 수행하며, CRL (Certificate Revocation List) 접근과 인증서 증명과 같은 무거운 작업에 대해서 벗어난다. [그림 6]에서와 같이 이동 호스트는 홈 에이전트를 비밀키로 인증하며, 외부 에이전트에 대해서는 홈 에이전트로부터 등록응답을 받음으로써 외부 에이전트의 인증서가 유효하다는 것을 간접적으로 보장 받게 된다. 인증서를 캐쉬에 저장하여 후에 사용할 때 효율을 높일 수 있다. 그러나 만약 이동 호스트가 공개키 기반 암호화를 수행할 수 있을 정도로 자원이 풍부하다면 홈 에이전트가 제공하는 서비스와 무관하게 선택적으로 공개키 기반 인증을 할 수도 있다. 외부 에이전트는 이동 호스트에 대해 홈 에이

전트가 이동 호스트에게 돌려준 등록응답에서 간접적으로 인증 받으며, 홈 에이전트와는 직접적으로 공개키 기반 인증을 수행한다. 이동 호스트는 홈 에이전트와 언제나 비밀키 기반 보안연관을 유지하기 때문에 이동 호스트와 홈 에이전트 사이에 부인방지서비스가 제공되지 않는다.

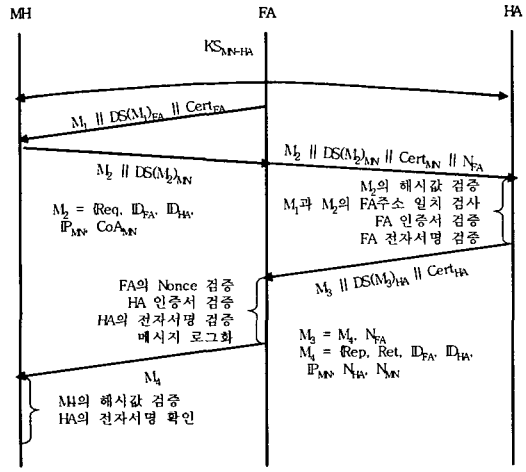

그림 6. 최소공개키 기반 인증절차

이 메커니즘은 공개키를 사용하여 확장성을 높이면서도 이동 호스트가 해야 하는 인증관련 관리와 이동 호스트에게 부여된 공개키 계산을 최소로 줄였다. 그러나 이동 호스트와 홈 에이전트 사이에는 비밀키를 이용하여 MAC을 생성하였기 때문에 부인방지 서비스가 결여되어 있다. 외부 에이전트와 홈 에이전트 사이에서는 공개키를 이용한 전자서명을 교환하기 때문에 네트워크에서 제공한 것에 대하여 부인할 수 없다. 다만, 홈 에이전트는 외부 에이전트에게 공개키로 전자서명을 보냄으로써 이동 호스트에게 제공한 서비스에 대하여 부인할 수 없다. 그러나 전자상거래와 같이 보안이 중요한 환경에서 이동 호스트의 위치 등록에 대한 부인방지 서비스가 결여되어 있다.

2. 통합 인증 프레임워크

2.1 세션키 기반 인증 프레임워크

앞서 기존의 인증 프레임워크에 대하여 각각의 인증 절차를 살펴보고, 이에 대한 문제점을 기술하였다. 본 논문에서는 이를 기초로 하여 각 프레임워크의 단점을 극복하면서 세션키에 기반한 새로운 통합 인증 프레임워크를 구성하였다.

우선, 지금까지의 인증 메커니즘이 이동 호스트가 현재 속해 있는 네트워크에 다른 네트워크로 이동할 때마다 홈 에이전트에 저장되어 있는 CoA를 변경해야 하므로 홈 에이전트에 이동 호스트를 빈번하게 등록해야 하고, 이동 호스트가 홈 네트워크에서 멀리 떨어질수록 홈 에이전트로 등록할 때 발생하는 핸드오프 지연시간이 증가함으로써 패킷 손실이 증가하고 처리율이 감소한다는 문제점을 가지고 있다.

이에 본 논문에서는 지역등록방식에 기초한 세션키 기반 인증 프레임워크를 구성하였으며, 핸드오프 시에 발생되는 지연을 줄이기 위해 최소지연 핸드오프(LLH, Low Laterncy Handoffs) 기법을 이용하였다.

기존의 지역등록을 이용한 세션키 교환기법은 다음과 같다. 우선, 이전에 할당된 세션키를 재사용한다. 그리고 공개키 동작 대신에 신뢰할 수 있는 제 3자를 두어 키를 공유하는 프로토콜을 적용한다. 이 기법에서는 앵커 에이전트가 외부 에이전트 간에 신뢰할만한 제 3자 역할을 수행한다.

[그림 9]에서와 같이 이전에 할당된 K_{SMN-FA}와 KS_{FA-HA}를 재사용한다. 이 세션 키들을 암호화하고 복호화하기 위해서 이전의 외부 에이전트(FAprev)와 현재의 외부 에이전트(FAnow) 사이에 세션키인 $KS_{FAprev-FAnow}$를 사용한다. 이 키는 신뢰할 수 있는 앵커 에이전트에 의해 동적으로 분배되고 공유된다.

이와 같은 방법으로 제안된 기법은 세션의 기밀성과 무결성을 제공하며, 지역 내에서 최소지연 핸드오프를 안전하게 수행한다. 이전에 제안된 공개키 암호화 동작에 비해서 지연과 계산비용이 훨씬 적다.

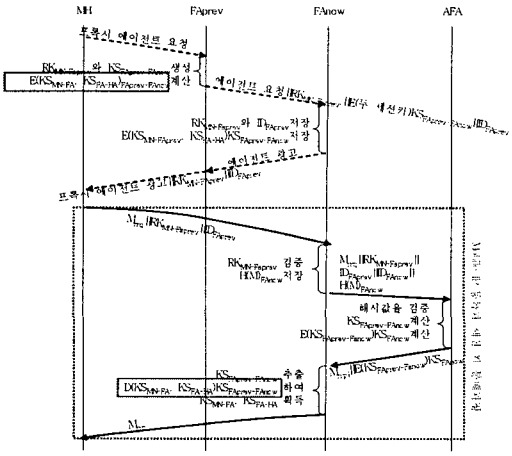

그림 7. 세션키 기반 인증절차

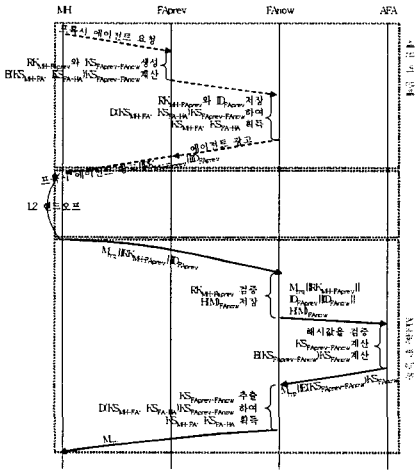

그림 8. 세션키 기반 인증절차

하지만, 이 기법을 위해서는 별도의 FAprev와 FAnow가 세션키의 암호화 및 복호화를 수행해야 한다는 단점이 존재한다. 이러한 단점을 극복하며, 지연을 최소화하기 위해 다음과 같이 최소지연 핸드오프방식에 기반하고, 암복호화를 배제한 세션키 기반 인증 프레임워크를 제안하였다.

2.2 제안된 인증프레임워크

홈 게이트웨이 및 AAA 인증서버를 포함한 홈 네트워킹 환경에 앞서 제안한 인증기법 및 모듈을 적용하여 통합된 인증 프레임워크를 구성하였다.

이를 위해 AAA서버와 홈 게이트웨이 간의 인증을 위해서는 이전의 인증절차-즉 모바일 호스트와 HA 간의 인증절차와 AAA서버와 홈 게이트웨이 간의 인증절차-를 중첩하여 메커니즘을 구성하여야 하였으며, 통합 프레임워크에 대한 인증절차는 [그림 9]에서 보는 바와 같다.

우선 모바일 호스트는 중간의 개체들(외부 에이전트(FA, Foreign Agent), 앵커 에이전트(AFA, Anchor Foreign Agent), 홈 에이전트(HA, Home Agent))에게 홈 게이트웨이를 인증하기 위한 홈 게이트웨이 식별자(ID_{HG})와 모바일 호스트와 홈 게이트웨이 간의 안전한 통신을 위한 세션키(KS_{MH-HG})를 보내게 된다. 이때, 홈 게이트웨이를 인증하기 위한 AAA_H에게 세션키를 안전하게 보내기 위해 이전에 주고받은 모바일 호스트와 홈 에이전트의 AAA_H 서버간의 세션키($KS_{MH-AAAH}$)로 그 세션키(KS_{MH-HG})를 암호화해서 보내게 되며, 홈 게이트웨이는 이를 복호화하여 세션키(KS_{MH-HG})를 풀게 된다. 물론, 이 세션키(KS_{MH-HG})는 모바일 호스트에서 생성하여 디바이스를 제어하고 서비스하기 위한 세션을 안전하게 유지하는데 사용된다. 이 세션키를 포함한 메시지를 받은 홈 에이전트의 AAA 서버는 홈 게이트웨이의 공개키(KU_{HG})를 가지고 이를 암호화하여 홈 게이트웨이에게 보내게 되며, 홈 게이트웨이는 이를 복호화한 후, 홈 에이전트에게 응답 메시지를 보내는 동시에 디바이스에게 서비스를 하기 위한 부팅작업을 요청한다. 물론, 이전에 홈 게이트웨이와 디바이스는 상호간에 인증작업을 수행하였다고 가정한다.

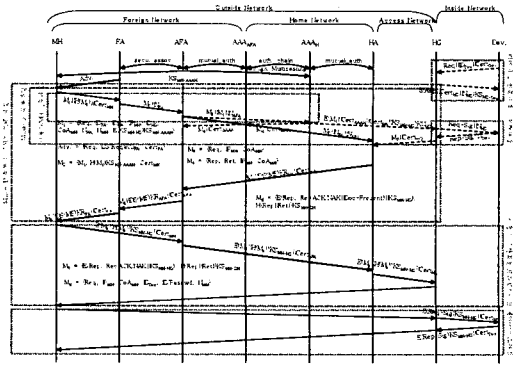

그림 9. 통합 프레임워크

모바일 IP 등록과 세션키 분배과정 및 디바이스 인증/부팅과정이 끝난 후, 실질적으로 모바일 호스트는 홈 게이트웨이에 댁내망 프리젠테이션 서비스를 요청하게 되고, 이를 받은 홈 게이트웨이는 사용자에 대한 인증 및 권한을 할당하게 된다. 이어서 모바일 호스트는 홈 게이트웨이로부터의 프리젠테이션 문서를 통해 직접적으로 디바이스를 제어하고 댁내망을 관리하게 된다.

IV. 성능평가 및 비교분석

시뮬레이션 환경은 [그림 10]에서와 같이 구성하였다. 이동 호스트는 홈 네트워크에서 시작하여 홈 에이전트로부터 고정 IP를 부여받고 외부 네트워크로 이동하여 앵커 에이전트에게서 등록시킨다. 이 때, 앵커 에이전트는 홈 에이전트와의 상호인증 뿐만 아니라 홈 게이트웨이와의 인증을 수행하게 된다.

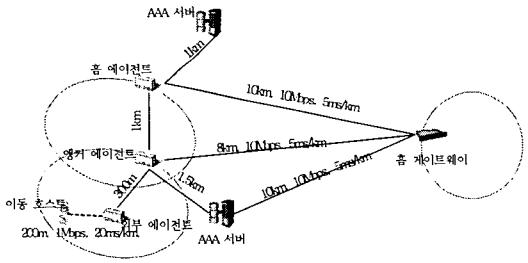

그림 10. 시뮬레이션 환경

우선, 기존의 방식과 제안된 프레임워크에 적용된 방식을 비교하여 보았다.

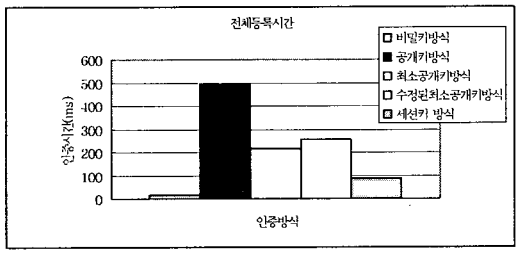

그림 11. 등록시간 비교

기존의 방식에 있어, 비밀키방식은 공개키 방식에 기반한 다른 방식에 비해 등록시간(16ms)이 현저하게 적음을 볼 수 있다. 공개키 방식은 492ms, 최소공개키방식은 217ms, 전자서명을 포함한 최소공개키방식은 254ms의 시간이 소요되었으며, 각각 비밀키 방식에 비해 30.8배, 13.6배, 15.9배가 더 소요되었으며, 공개키 방식을 기준으로 전자서명을 포함한 최소공개키방식은 약 2배의 시간이 더 소요되었다.

본 논문에서 제안한 세션키 기반 방식의 등록시간(86ms)은 비밀키 방식에 비해 5.3배가 더 걸리지만, 일반적인 공개키방식에 비해 3-5배 정도가 덜 소요된다.

이를 토대로, 본 논문에서 제안한 통합 인증프레임워크에서의 등록시간 및 암복화을 비교하면 아래의 [그림 12]와 같이 측정된다.

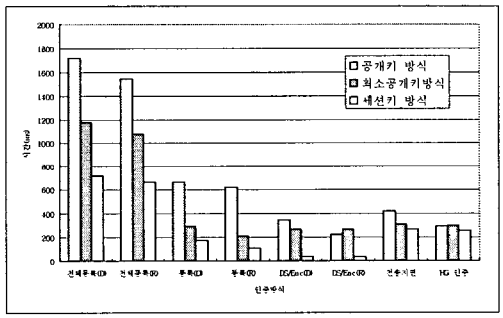

그림 12. 인증방식 및 등록기법별 비교

세션키기반 방식에서의 등록시간은 공개키기반 방식이나 최소공개키기반 방식의 등록시간에 비해 1.6~2.4배 정도가 덜 소요된다. 즉, 암복호화 및 전자서명 연산의 횟수가 상대적으로 적고, 수행속도가 오래 걸리는 암복화 및 전자서명 연산 대신에 연산속도가 상대적으로 빠른 해싱 연산을 이용하고 있기 때문이다.

또한, 전체등록시간에서 암복호화 연산이 차지하는 비중은 공개키방식이나 최소공개키 방식에서 20~25% 정도 차지하는 반면, 세션키 방식에서는 5% 정도를 차지함으로써 상대적으로 전체 수행시간이 적게 소요되는 것을 알 수 있다. 추가적으로 지역등록방식과 로컬 핸드오프 방식을 이용할 경우, 전체등록시간이 방식에 무관하게 10%정도 줄어드는 것으로 실험에서 나타났다.

V. 결론 및 향후연구

현재의 홈 네트워크 보안에 관한 개발 및 연구는 댁외망과 댁내망 사이의 보안을 기존의 PKI 구조를 기초로 하고, 댁내망 내부에서의 인증 및 보안에 대해서 중점적으로 연구가 이루어지고 있다는 것이다. 이러한 구조의 문제점은 댁내망이 완벽한 보안구조를 가지고 있다고 하더라도 댁내망으로 접근하기 이전의 보안구조에 문제가 발생하게 되면, 홈 네트워크에 대한 보안이 완벽하게 이루어질 수 없다는 것이다. 이에 본 논문에서는 인터넷 사용자뿐만 아니라 모바일 사용자가 댁내의 디바이스에 대해 안전하게 제어하기 위해 댁외망에서의 안전한 인증 프레임워크를 구축하고자 하였으며, 이를 통해 앞서 언급된 문제점을 해결하고자 하였다. 이와 같이 제안된 유무선 구간의 통합 인증 프레임워크는 기존의 인증 프레임워크에 비해 암복호화 횟수를 배로 줄이고, 등록시간을 핸드오프 시에 처리함으로서 처리시간을 배로 증가시켰으며, 또한 세션키를 이용함으로서 낮은 컴퓨팅 능력을 갖고 있는 모바일 기기에서의 사용을 용이하게 하였다.

참 고 문 헌

[1] H. Schulzrinne, X. Wu, and S. Sidiroglou, "Ubiquitous Computing in Home Networks," IEEE Communications Magazine, Vol.41 No.11, 2003.

[2] M. Kim and Y. Mun, "Localized Key Management for AAA in Mobile IPv6," IETF internet Draft, draft-mun-aaa-localkm-mobileipv6-01.txt, 2003.

[3] S. Pack and Y. Choi, "Performance Analysis of Fast Handover in Mobile IPv6 Networks," in Proceeding IFIP PWC 2003, 2003.

[4] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," draft-ietf-aaa-diameter-17.txt, IETF Work in progress, 2002.

[5] T. B. Zahariadis, "Home Networking Technologies and Standards," Artech House, Inc., Boston, 2003.

[6] C. M. Ellison, "Interoperable Home Infrastructure Home Network Security," Intel Technology Journal, Vol.6, 2002.

[7] M. Kreutzer, "Identity Management," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, Sep. 2002.

[8] N. Shankar and W. Arbaugh, "On Trust for Ubiquitous Computing," Workshop on Security in Ubiquitous Computing, UBICOMP 2002, 2002.

저 자 소 개

이 원 구(Won-Goo Lee) 준회원

- 2002년 2월 : 한남대학교 컴퓨터공학과 (공학석사)
- 2002년 3월~2005년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 2월~현재 : 한국과학기술정보연구원 재직중

<관심분야> : 정보보호, 유비쿼터스 보안 등

윤 화 묵(Hwa-Mook Yoon) 정회원

- 1992년 2월 : 서울산업대학교 전자계산학과(이학사)
- 1997년 2월 : 공주대학교 전자계산학과(이학석사)
- 현재 : 한국과학기술정보연구원 정보시스템부 정보유통기술개발실 재직 중

최 병 선(Byung-Sun Choi) 준회원

- 2002년 2월 : 한남대학교 컴퓨터공학과 (공학사)
- 2004년 2월 : 한남대학교 컴퓨터공학과 (공학석사)
- 2004년 3월~현재 : 한남대학교 컴퓨터공학과 박사과정 재학

<관심분야> : 홈 네트워크 보안, 시스템 보안 등

이 성 현(Seoung-Hyeon Lee) 준회원

- 2003년 2월 : 한남대학교 컴퓨터공학과(공학사)
- 2003년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2003년 3월~현재 : 한남대학교 컴퓨터공학과 박사과정 재학

<관심분야> : 그리드, PKI 보안 등

이 재 광(Jae-Kwang Lee) 정회원

- 1993년 2월 : 광운대학교 전자계산학과(이학박사)
- 1986년 3월~1993년 8월 : 군산전문대학 전자계산학과 부교수
- 1993년 8월~현재 : 한남대학교 컴퓨터공학과 교수

<관심분야> : 정보보호, 네트워크 보안 등