융합 미디어 서비스 제공을 위한 통합 프로파일 및 인증 제어 기술 연구

종신회원 이 현 우*, 정회원 김 귀 훈*, 류 원*

A Converged Profile and Authentication Control Scheme for Supporting Converged Media Service

Hyun-woo Lee* *Lifelong Member*, Kwihoon Kim*, Won Ryu* *Regular Members*

요 약

본 논문에서는 유무선 통합 환경에서 융합 미디어 서비스를 제공하기 위한 통합 프로파일 및 인증 제어 기술로써, 시스템 구현을 통한 결과를 제시한다. 가입자의 접속, 서비스, 이동성, 방송형 프로파일을 관리하고 개방형 API(Application Program Interface)를 통해서 제3사업자에게 가입자 프로파일 정보를 PUSH/PULL 방식으로 제공하는 방안을 제안한다. 이때 개방형 API는 웹 서비스, REST(Representational State Transfer) 기반으로 구현하여 제3사업자가 쉽게 서비스를 제공할 수 있는 방식을 제안한다. 또한, 한번 접속 인증에 성공하면 액세스 망이 변하거나 혹은 IMS(IP Multimedia Subsystem) 기반의 서비스 망에 접속하게 될 때 동일한 인증 정보를 유지할 수 있는 SSO(Single Sign-On) 기능을 제안한다. 제안된 방식은 CUPS(Converged User Profile Server) 시험 네트워크 구현 연구를 통하여 기능 검증 및 성능 분석을 수행하였다.

Key Words : Converged Profile, Personalization, Converged Media, Mobility Profile, IPTV Profile

ABSTRACT

In this paper, we propose the converged profile and authentication scheme for supporting converged media services of broadcasting & communications convergence in fixed mobile convergence networks. The proposed scheme supports the management of access, service, mobility and IPTV profiles on subscriber and a function of open API(Application Program Interface) for providing the subscriber profile for the third party service provider with the PUSH/PULL method. The open API is based on a web service and a REST(Representational State Transfer) and provides various services for the third party service provider with ease. In addition, the proposed scheme supports a function of SSO(Single Sign-on). After user succeeded in establishing an access connection, user can sustain the same authentication state with this function although connected access network is changed or IMS(IP Multimedia Subsystem) service network is attached. We evaluate and analyze the performance of the proposed scheme through the implementation of CUPS(Converged User Profile Server) system test-bed.

※ 본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업의 일환으로 수행하였습니다 [2009-S-018-01, IPTV 융합서비스 및 콘텐츠 공유를 위한 개방형 IPTV 플랫폼 기술 개발].
* 한국전자통신연구원 방송통신융합연구부문 IPTV연구부 융합서비스네트워킹연구팀 (kwihooi@etri.re.kr)
논문번호 : KICS2009-12-659, 접수일자 : 2009년 12월 31일, 최종논문접수일자 : 2010년 3월 15일

I. 서 론

NGN (Next Generation Network) 망에서 다양한 단말과 네트워크 기술을 수용하기 위해 NGN은 대부분의 네트워크 프로토콜을 포함하여 접속을 관리하며 이러한 네트워크 접속을 기반으로 다양한 멀티미디어 서비스를 지원하기 위해 준비하고 있다. 이를 위해 NGN은 서비스 품질, 이동성, 보안 등과 같은 다양한 사항들을 고려하여야만 한다. NGN 망은 그 특성상 3G, WiBro, WLAN (Wireless LAN) 등 다양한 무선망 기술이 융합되어 고속으로 IP 기반의 복합 서비스를 제공하고 있기 때문에 기존의 접속 보안 기술들을 모두 포함하여야 하며 이를 위해 인증의 단일화를 위한 표준화가 인증 프로토콜의 다양한 계층에서 수행되고 있다. 또한 IMS를 위한 보안 기술이 연구되어 3GPP에 제안되고 이 기술이 NGN의 멀티미디어 기술로 활용될 것이다. 그러나 인증은 사용자를 확인하고 안전한 통신을 위한 키 교환으로 구성되기 때문에 통신 및 계산 과부하와 지연 시간을 유발하게 된다. 더욱이 NGN에서 접속을 위한 인증을 수행하고 멀티미디어 서비스를 위한 인증을 다시 수행하는 것은 중복적인 처리이며 과부하를 더욱 가중시키는 단점을 가지게 된다. 따라서, 이러한 과부하를 줄여 보다 안전하고 끊김 없는 멀티미디어 서비스를 제공해주는 것이 필요하다.

최근에 각 표준기관에서 이러한 중복적인 인증 과정을 줄이기 위해 번들 인증이라는 개념을 도입하여 사용자의 네트워크 접속 인증 후에 추가적인 서비스 인증은 생략하는 과정에 관하여 연구하고 있다. NGN 망에서 번들 인증 기술 표준을 연구하는 표준 기관은 ETSI, ITU-T, 3GPP 등이 대표적이다. 이러한 표준화 기구들에서는 NGN상에서의 안전한 통신을 지원하기 위한 방법들에 대한 요구사항을 정리하고 구체적으로 위협을 분석하기 위한 다양한 위협 시나리오에 대해서 정의하고 있다. 또한, 액세스 인증 기술에 대해 3GPP에서 USIM(Universal Subscriber Identity Module) 기반 AKA(Authentication and Key Agreement) 인증과 멀티미디어 서비스를 관한 IMS-AKA 인증을 제공하는 상세한 절차들을 제시하며 표준화를 진행하고 있다. 또한 이를 간소화하는 번들 인증의 기본 절차에 관하여 표준화를 시작하였다. ID 관리 기술은 인터넷 서비스들이 다양해짐에 따라 개인마다 사용하는 ID의 숫자가 증가하고 있으며 이로 인해 다양한 공격들이 가능하다. 이에 따라 ITU-T IdM-GSI 에서는 ID 관리 기술의 구조를 정의하고 있으며, 상세한 시나리오를 분석하여 다양한 공격의 가능성을 줄이고자 노력하고 있다.

현재의 초고속 통신망 서비스가 고정망 시장의 축소와 이동망 시장의 성장 및 정체, 대역폭 및 품질의 한계에 이르면서 사용자는 유비쿼터스 환경을 기반으로 한층 진보된 새로운 서비스와 개인화, 이동성 지원 서비스를 추구하게 되었고, 통신사업자는 보다 많은 고객의 확보와 비용절감, 새로운 수익창출을 위한 새로운 서비스의 제공과 같은 미래의 고품질 서비스 욕구를 해결해야 하는 상황에 직면하게 되었다. 이러한 상황에서 NGN에서의 서비스 및 제어 기술은 통신사업자 측면에서 통신과 방송이 융합되어 생성된 다양한 멀티미디어 콘텐츠를 안정된 네트워크를 통해 가입자에게 제공함으로써 고부가가치의 수익을 창출할 수 있고, 가입자 측면에서는 품질보장형 서비스를 장소나 단말에 관계없이 끊김 없이 제공 받기 위한 필수 요소 기술이라 할 수 있다. 서비스의 제공 형태도 영상전화, IPTV, WiBro 등을 중심으로 서비스별 개별 가입, 다양한 접속 기술 및 단말 의존적 서비스로부터 IP를 기반으로 한 단말 독립적인 서비스 이동성 제공과 한 번의 가입으로 모든 서비스를 제공 받는 형태로 변화되고 있으며, 이에 따른 내포된(implicit) 인증이 보편화되고 있는 추세이다[1],[2]. 이러한 변화에 부응하기 위해서는 단말 기능의 통합은 물론이고 All-IP를 기반으로 한 전달 인프라의 통합이 이루어져야 한다. 또한 다양한 단말 중심의 서비스를 제공하기 위한 제어 및 관리 인프라의 단일화된 제어 체계가 필수적인 요인이라 할 수 있다. 최근에는 ITU-T를 중심으로 하여 NGN 제어 계층의 기술에 대한 표준화가 급속히 추진되고 있으며, 이 표준화에 세계 주요 통신사업자와 제조업체들이 모두 참여하여 자사에서 추진하고 있는 기술과 제품을 표준안에 반영시키기 위한 노력들이 진행 중이다.

기존의 통합 네트워크 기술은 사업자 내에서 개별 프로파일을 구축하고 개별 인증을 제공했지만 All-IP 기반의 통방 융합 서비스 환경에서 효과적인 서비스 제어와 가입자 관리를 위해 통합 프로파일 관리 체계 및 통합 인증이 가능해야 한다. 이를 실현하기 위한 통합 프로파일 관리 및 통합 인증 기술 분야의 주요 목표 기술은 사업자간 연동 프로파일 관리 및 인증 제어 기술, 유무선 가입자/서비스 프로파일 관리 및 유무선 가입자 통합 인증 제어

기술, 통신·방송 융합 프로파일 관리 및 통합 인증 제어 기술 등을 들 수 있다.

본 논문에서는 이와 같이 NGN 내에서 수행되는 서비스와 장비들을 가장 효율적으로 활용하기 위해서 유무선 통합 환경에서 다양한 융합 미디어 서비스를 제공하기 위한 통합 프로파일 관리 및 인증 제어 기술을 제안하고, 시스템 구현을 통한 성능 분석 결과를 제시한다.

본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 NGN 통합 프로파일 및 인증 제어 기술 관련 기술 현황에 대하여 기술한다. 3장에서는 본 논문에서 제안된 접속, 서비스, 이동형, 방송형 프로파일 관리 기능, 개방형 프로파일 관리 기능, 통합 액세스 인증 기능, 고속 핸드오버 인증 기능, 액세스 및 서비스망간 번들 인증 기능에 대하여 기술한다. 4장에서는 제안된 CUPS 방식의 프로토타입 시스템 구현, 성능분석 및 토의에 대하여 기술하고, 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 관련 기술

2.1 ITU-T 프로파일 관리 기술

ITU-T NGN에서 정의하고 있는 프로파일의 구성은 전달망 접속상태를 포함하여 서비스 사용에 따른 가변적인 상태정보의 서비스 사용자 프로파일(user profile)과 단말장치 프로파일(device profile)로 구분되는데 각각의 프로파일 구성은 다음의 데이터 정보로 이루어진다[7].

2.1.1 서비스 사용자 프로파일 구성요소

- 사용자 ID(User identity, attribute information of individual user)
- 사용자 위치정보(User location information)
- 사용자 상태정보(User presence information)
- 다양한 서비스와 응용별 가입정보(User's subscription information of services and applications)
- 사용자 취향정보(User preference information)
- 사용자 개인정보(User personal information)
- 사용자 또는 단말별 특이정보(User-specific or device-specific service profiles)
- 과금 정보(Billing information)

2.1.2 단말장치 프로파일 구성요소

- 단말장치 ID/주소/이름
- 일반적인 단말정보(S/N, 단말모델, 형태 등)
- 단말에서 지원 가능한 미디어 종류
- 단말에서 사용이 가능한 서비스 종류
- 탑재된 프로토콜, NIC 접속속도, 대역폭, CPU 성능 등의 고정 속성 정보
- 단말 형태, 지역적 위치, 현재 수행중인 응용서비스 등의 가변 속성 정보
- 통신 품질, 코덱, 접속 망/포트 등의 구성 정보
- OS 종류와 응용서비스 관리자, 접속 클라이언트 등의 탑재 소프트웨어 버전 정보
- 망 접속 상태, 단말 소프트웨어 상태, 단말 자원 및 각종 on/off 상태 정보

2.2 3GPP 프로파일 관리 기술

3GPP에서는 서로 다른 기능 노드나 제어 노드에서 사용자와 관련된 프로파일 정보를 효율적으로 관리하기 위한 프로파일 데이터에 대한 표현방법으로 GUP(Generic User Profile)를 정의하고 있다. 이러한 GUP는 세분화된 사용자 관련 데이터를 사용하여 다양한 서비스가 제공될 수 있도록 프로파일 정보를 관리, 제공하며 다음과 같은 기능적인 특징을 가지고 있다[7].

- 접속 인터페이스의 제공: GUP는 프로파일 정보를 서로 다른 목적을 가진 애플리케이션 간의 원활한 정보 교환이 이루어지도록 편리한 접속 방법을 제공한다.
- 서버를 통한 접속 관리: 3GPP에서 사용되는 모든 애플리케이션은 GUP 서버를 통해 모든 프로파일 정보를 획득할 수 있으며, 이를 통해 원활한 서비스를 제공한다.
- 프로파일 접근에 대한 인증 및 허가: GUP는 모든 애플리케이션에 대한 데이터접속을 승인하며, 모든 애플리케이션에 이용되는 프로파일 정보를 사용할 수 있도록 접속하는 애플리케이션에 대한 사용여부를 허가한다. 이러한 인증과 허가를 통해 가입자의 사생활 보호와 관리가 이루어진다.
- 저장 데이터의 동기화: GUP의 데이터 저장소는 GUP 구성요소에 대한 최종 파일을 보관하고 있어 애플리케이션이나 GUP 서버에서 데이터를 요청할 때 데이터 전송에 관한 동기화 작업을 수행한다.
- 타 망으로부터의 프로파일 접속: GUP는 서버를 통한 접속관리 기능을 이용하여 서로 다른

망에 위치한 애플리케이션이 GUP 서버로 접근할 경우 이를 도와주는 역할이 가능하다.

- 프로파일 구성 요소 위치 정보 관리: GUP는 기능적으로 GUP 구성요소에 대한 데이터 위치 정보를 보관하고 있다.

통합 프로파일 관리 및 인증 제어 기술은 기존 3GPP의 HSS(Home Subscriber Server) 서브시스템의 기능을 기반으로 하며, 기존 3GPP의 HSS 서브시스템은 3G R99에서 정의하는 HLR(Home Location Register) 기능(CS/PS 서비스 지원)과 멀티미디어 서비스 지원 기능으로 구성된다. 통합 가입자 프로파일 서버는 유무선 통합 환경에서 단말 및 가입자 정보를 실시간으로 처리하는 서브시스템으로 저장된 가입자 정보와 이동성 관리 기능, 호/세션 처리기능, 인증기능 및 IP 멀티미디어 서비스 제어 지원 기능을 이용하여 단말 이동성과 가입자 및 서비스 이동성 기능을 제공한다. 또한 통합 가입자 프로파일 서버는 IP 멀티미디어 서비스 지원을 위한 주소 번역 기능, 보안관련 데이터를 생성/저장/관리하는 기능 및 가입자의 서비스 프로파일, 서비스 이동성, S-CSCF (Serving Call Session Control Function) 관련 정보들을 저장 및 관리한다. 세션기반의 서비스 제어 기술인 IMS는 가입자와 서비스 프로파일을 관리하고 접속 및 서비스 레벨의 인증 서버 기능을 제공하고, 가입자가 어떤 액세스 네트워크에 접속해도 상관없이 동일한 IMS 기반의 멀티미디어 서비스를 제공한다. 그림 1은 IMS에서 HSS와 CSCF의 구성도를 나타내고 있다. 3GPP IMS의 서브시스템은 논리적으로 CSCF와 AS(Application Server), HSS의 세 개의 서브시스템으로 구성되며, CSCF는 기능에 따라 I-CSCF(Interrogating Call Session Control Function), P-CSCF(Proxy Call Session Control Function) 그리고 S-CSCF로 구분된다. 통합 프로파일 서버는 단일 시스템으로 동작하지 않고, 다른 네트워크 장비들과 연동하여 동작한다. 그림 1처럼 유무선 액세스 네트워크 위에 다양한 액세스 가입자 프로파일을 관리한다. 또한, IMS 기반의 호 제어 서버에게 가입자 및 서비스 프로파일과 인증 벡터를 제공하며, QoS(Quality of Service)를 관리하는 RACF(Resource and Admission Control Functions)에게 QoS 프로파일을 제공한다.

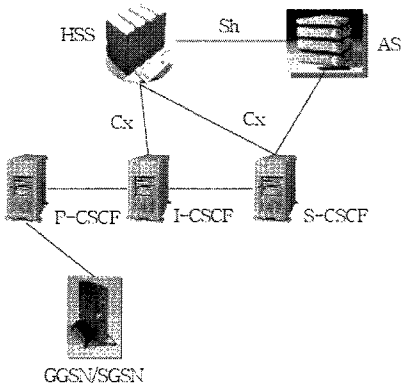


그림 1. IMS에서 HSS와 CSCF 구성도

2.3 IEEE 802.11 WLAN 인증 및 보안

SSID(Service Set IDentifier) 방식이나 사전에 키를 공유하여야 하는 WEP(Wired Equivalent Privacy) 방식은 비교적 신뢰성이 높지 않은 방식이다. 이를 보완하기 위해 802.1x 액세스 인증 [17] 기법은 유동적인 사용자 인증 기능을 제공한다. IEEE 802.1x 방법은 액세스 제어를 위해 두 개의 포트를 사용하고 이러한 포트 제어 방식을 통해 망을 보호한다. 인증된 후에 사용하는 제어 포트와 인증 되기 전에 사용하는 비 제어 포트로 용도를 위한 포트 구분을 통해 네트워크로의 접근을 제한하고 있다. 사용자 인증을 수행하기 위해 AP를 통해 정의된 비 제어 포트를 사용하여 인증 서버에 인증을 요청하면, 해당하는 사용자의 인증이 이루어지고 제어포트를 개방하여 네트워크의 접근을 수락한다. 그러나 인증이 수행되지 않는다면 제어포트를 개방하지 않는다. 그림 2는 EAP(Extensible Authentication Protocol) [18] 기반의 IEEE 802.1x 인증 과정을 설명하고 있고 절차는 다음과 같다.

1) 사용자가 EAP-start 메시지를 AP(Access Point)에게 보내어 네트워크 연결을 요청한다.
2) AP는 EAP-start 메시지를 받으면 가입자 인증에 필요한 가입자 Identity 정보를 단말에게 요청한다.
3) 요청을 받은 사용자는 자신의 Identity를 AP에게 전달한다.
4) AP는 전달 받은 Identity를 AAA EAP 메시지에 담아 인증 서버에게 전달한다.
5) 최종적으로 AP는 인증 서버로부터 인증 성공/실패 메시지를 받으면 인증 과정이 종료된다. 이 때 생성된 마스터 세션키는 Access Accept에 포함되어 AP로 전달된다.

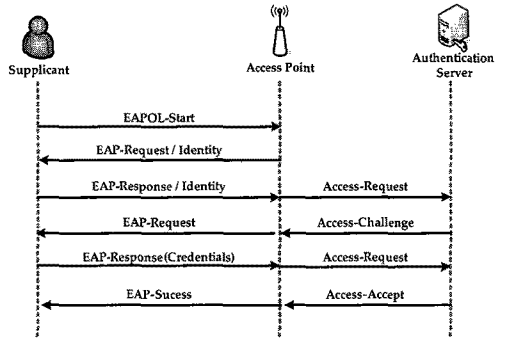


그림 2. EAP 기반의 IEEE 802.1x

6) AP는 무선랜 접속이 허용되었음을 사용자 단말에게 알린다.

IEEE 802.1x는 그림 2와 같이 보다 신뢰성 있는 보안을 제공하기 위해 EAP를 채택하여 인증을 수행하다. 앞선 방식들과 다른 점은 앞선 방식들에서는 사용자 인증을 AP가 했지만, EAP 기반의 IEEE 802.1x EAP에서는 AP가 단순히 사용자와 인증서버간의 중개 역할만 하며, 실제적인 사용자 인증은 인증 서버가 수행한다. 이러한 모든 작업으로 인해 발생하는 메시지는 EAP 규격을 따라야 한다. 따라서 IEEE 802.1x에서는 사용자와 AP 간의 통신은 EAPoL(EAP over LAN) 또는 EAPoW(EAP over Wireless)으로 규정하였고 무선랜에서는 EAPoW를 사용한다. 그러나 IEEE 802.1x는 구체적인 인증 방법을 정의하고 있지 않으며, 인증에 필요한 기법만을 제공하기 때문에 스마트 카드를 이용한 인증, 커버로스(Kerberos), TLS(Transport Layer Security), OTP(One Time Password)등과 같은 다양한 보안 방법 중에 선택적으로 적용 가능하다.

2.4 IEEE 802.16 WiBro 인증 및 보안

PKMv2(Privacy Key Management version 2)는 RSA(Rivest, Shamir, Adleman) 기반의 인증과 EAP 기반의 인증방식을 제공한다. 앞서 기술된 RSA 기반의 인증 기법은 앞서 설명된 것처럼 인증 서버 없이 동작하도록 설계 되었고, EAP 기반의 PKMv2 기법은 신뢰된 인증 서버를 통해 인증 및 키 분배가 수행된다. EAP는 포트 제어 기반의 인증 프로토콜 IEEE 802.1x에서 사용자 인증 데이터 전송을 위한 표준 프로토콜로 다양한 인증 방법의 적용할 수 있다. EAP 기반의 PKMv2는 단말과 기지국 사이의 MAC(Media Access Control) 계층에서 EAP 시작을 알리는 PKMv2 EAP Start와 진행을 알리는 PKMv2 EAP Transfer 메시지를 정의한다.

그림 3은 PKMv2 EAP 기반 인증 및 키 교환 절차를 보여준다. 단말은 EAP 기반의 인증 절차의 시작을 기지국에 알리고 앞으로의 EAP 메시지를

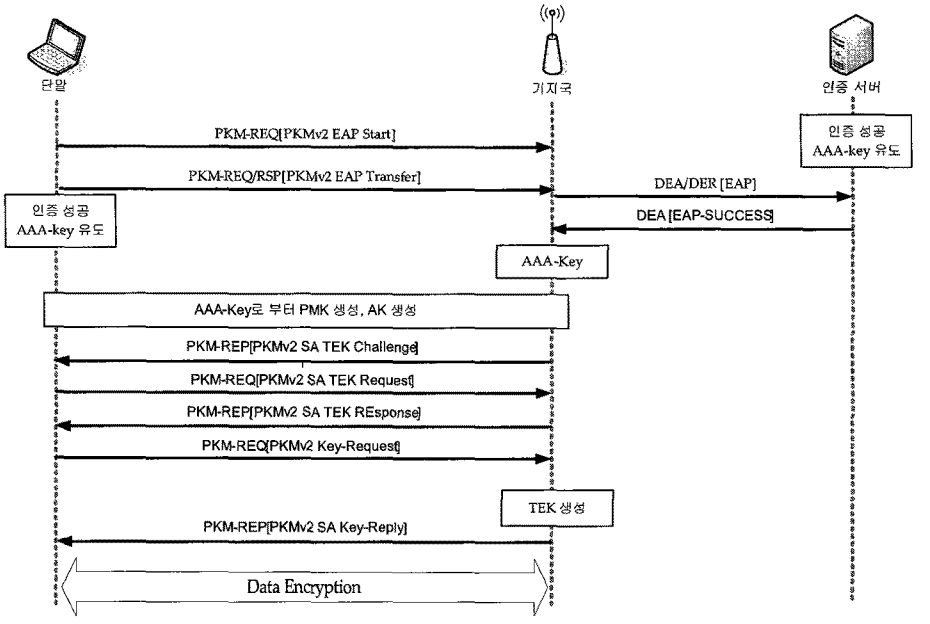


그림 3. EAP 기반의 PKMv2 인증 및 키 교환

인증서버에 전달할 것을 요청한다. 요청 이후에 기지국은 인증 과정에서 송수신되는 트래픽을 인증서버로 전달하는 중계자 역할을 한다. 단말과 기지국 간 EAP 기반의 인증방식에 따른 데이터는 PKMv2 EAP Transfer 메시지 안에 포함되고 기지국/제어국과 인증 서버 사이에서는 Diameter 메시지에 포함시켜 전달한다. 성공적으로 인증이 수행되면 단말과 인증서버는 AAA-key를 생성하고, 인증서버는 제어국에 AAA-key를 전달한다. 각각의 단말과 제어국은 공유된 AAA-Key로부터 PMK(Pairwise Authorization Key) 및 AK(Authorization Key)를 유도하고 제어국은 AK를 기지국에 전달한다. 상호간에 가지고 있는 AK의 정당성을 확인하기 위한 3-way handshake 과정을 수행하고 확인이 되면 기지국은 데이터 암호화 키를 생성하여 단말에 전달한다. 이러한 인증이 완료된 이후 발생하는 모든 트래픽은 TEK(Traffic Encryption Key)로 암호화하여 무선 구간에서 안전하게 전달된다.

단말의 초기 인증을 성공적으로 수행한 후에 단말은 서비스의 연속적인 지원을 위해 서비스를 받고 있는 BS(Base Station)에서 다른 BS로의 핸드오버를 지원해야 한다. 그러나 IEEE 802.16e [5]에서는 핸드오버 인증 시에 AK와 TEK에 대한 PBS (Public Broadcasting Service)가 제공되지 않는 문제가 발생 할 수 있다. 그림 4는 IEEE 802.16e에서의 핸드오버 절차이다.

그림 4의 절차를 보면, old BS와 new BS간 security context 전달 방법의 문제가 존재한다. Old BS는 SS(Subscriber Station)와 공유하고 있는 인증키를 해시하여 new BS에게 전달하게 되면 SS가 new BS로 핸드오버 한 후 새로운 세션을 맺지만, old BS는 new BS와 SS가 통신하는 내용을 알 수 있게 되는 문제가 발생한다. 기존 무선랜 서비스의 경우, 상용화 이후 많은 보안 문제점들이 발생되었기 때문에 WiBro 서비스는 이런 전철을 밟지 않기 위해, 매체 접근 제어 계층에 보안을 위한 보안 부계층이 포함되어 있으며, 여러 가지 보안 메커니즘이 적용되어 있다. 앞서살펴본바와같이초기인증및키관리표준인 PKMv1은 여러 가지 문제점이 있기 때문에 이런 문제점을 개선한 PKMv2는 다양한 인증방식을 적용할 수 있도록 하기 위해 EAP 기반 인증방식을 지원하고 있다. WiBro는 현재 서비스 상용화 초기 단계로, 적용된 보안 메커니즘에 대한 검증이 지속적으로 요구되며, IPv6 도입, CDMA/WLAN과 같은 이기종망 연동 등 향후 등장할 기술에 대한 보안 문제도 함께 고려되어야 한다.

2.5 3GPP 인증 및 보안

3GPP의 정보보호와 관련된 3세대 네트워크는 그림 5와 같이 사용자 영역, 서비스 네트워크 영역, 홈 환경 영역으로 나누어진다. 사용자 영역은 3G 서비스에의 접근을 위한 사용자 신분 확인 및 인증에 필요한 데이터 및 함수를 저장한 USIM (User Service Identity Module)과 ME (Mobile Equipment)

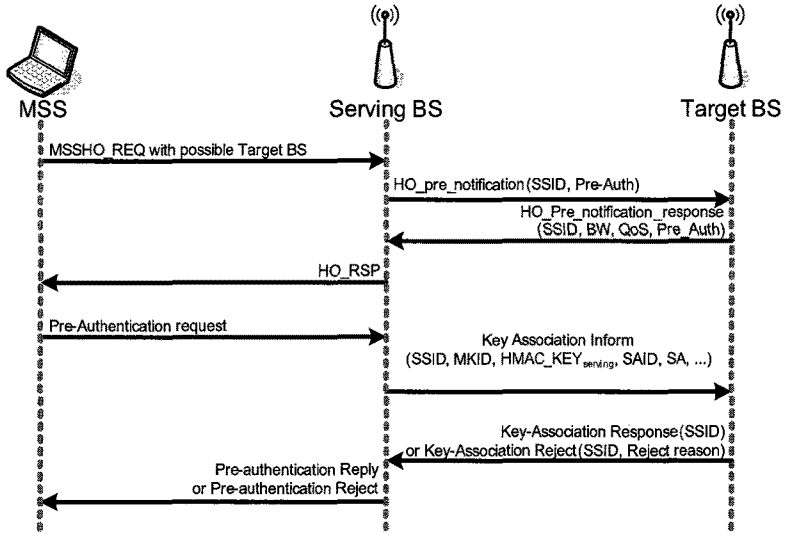


그림 4. IEEE 802.16e의 핸드오버 인증 절차

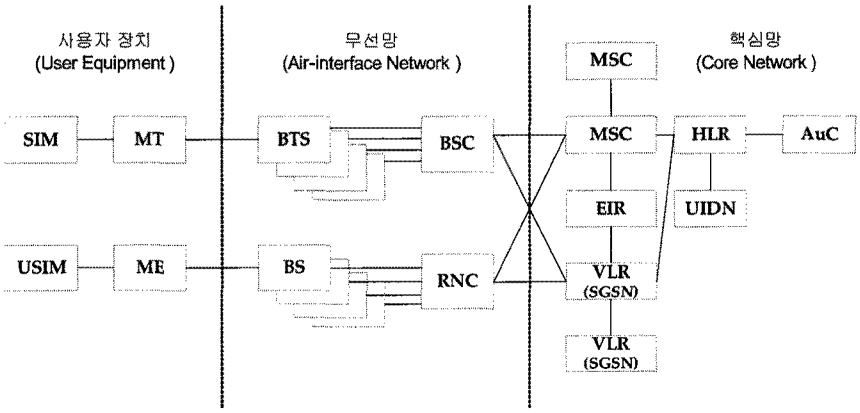


그림 5. 3GPP 보안 구조

로 구성된다. 서비스 제공 영역은 무선 접근을 제어하는 RNC (Radio Network Controller), 서킷 전환 서비스와 패킷 전환서비스를 위한 위치 등록소인 VLR (Visitor Location Register)과 SGSN (Serving GPRS Support Node)로 구성되며, 홈 환경영역은 3세대 서비스 가입자에 대한 서비스 제공에 전반적인 책임이 있는 HLR (Home Location Register), 인증센터 AuC (Authentication Center), UIDN (User Identity Description Node)으로 이루어진다.

3GPP Digest AKA 인증은 보다 빠르고 안전한 인증을 위해 IETF RFC 3310에서 제안하는 SIP (Session Initiation Protocol) Digest 인증과 AKA를 적용한 인증기법이다. 그림 6은 3GPP의 시그널링 프로토콜인 SIP 인증 기법에 AKA를 적용하여 인증과 함께 키 교환 기능을 제공한다. 3GPP Digest AKA에서는 인증 절차를 위해 SIP의 등록 과정을 적용하여 인증 여부를 확인하고 IK(Integrity Key) 및 CK(Cipher Key)를 생성하여 서비스를 이용할 수 있도록 한다. 다음의 그림 6은 Digest AKA의 인증 절차이다.

1) SIP 기반의 등록과정을 통해 서버는 AKA 알고리즘을 실행시키고 인증에 필요한 값인 RAND과 AUTH값을 생성한다.
2) SIP 메시지인 401 메시지를 통해 RAND와 AUTH를 사용자에게 전달하면 사용자는 AKA 알고리즘을 ISIM(IP Multimedia Services Identity Module) 기반에서 실행하고, AUTH를 확인한다.
3) 인증 값 비교를 위한 RES와 세션 키를 생성하고 SIP의 과정처럼 다시 등록을 신청한다.

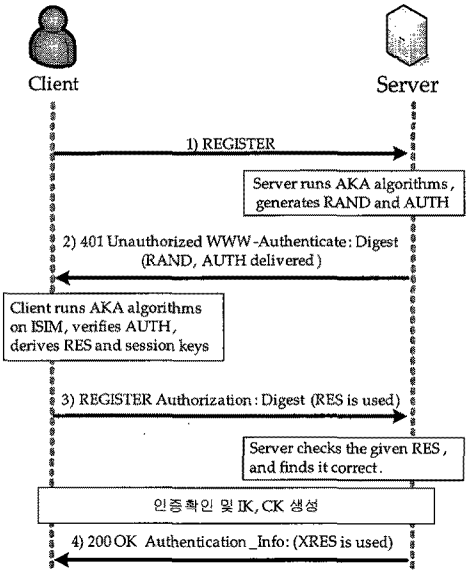


그림 6. 3GPP Digest AKA 인증 절차

이때 생성한 RES정보를 사용하게 된다.
4) 서버는 얻게 된 RES를 정보를 얻게 되면, 이 값이 정확한 값인지 확인하고 인증정보인 XRES를 사용하여 200 OK 메시지로 인증이 되었음을 알리고 양 단간에는 인증확인과 IK와 CK를 서로 생성할 수 있게 된다.

Ⅲ. 제안된 통합 프로파일 및 인증 제어 기술

본 장에서는 유무선 통합 환경에서 개인화된 융합 미디어 서비스를 제공하기 위하여 2장에서 기술한 관련 기술을 발전 시킨 CUPS 시스템 기반의 통

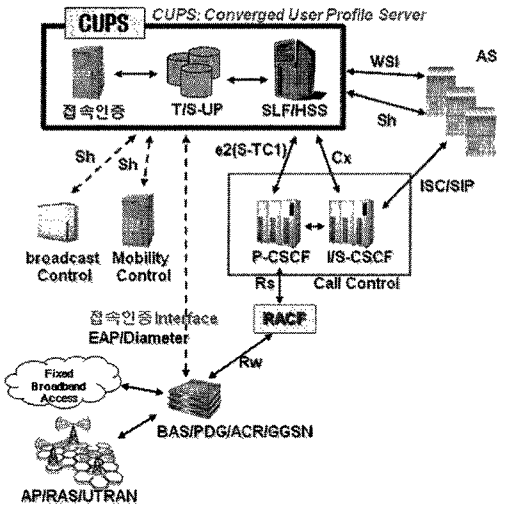


그림 7. 네트워크 구성도

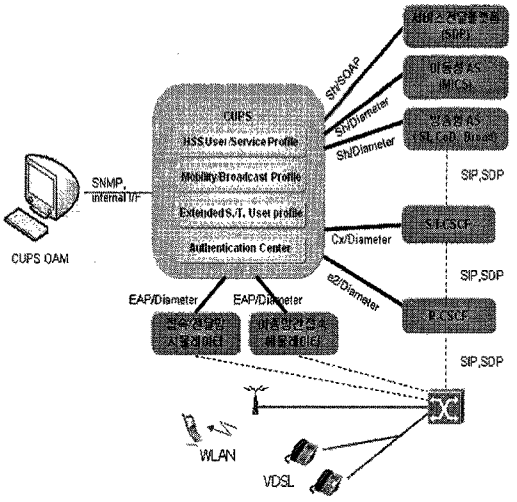


그림 8. CUPS 시스템 외부 인터페이스

합 프로파일 및 인증 제어 시스템을 제시한다. 본 시스템은 세션기반의 서비스 제어 기술인 IMS의 가입자 와 서비스 프로파일을 관리하고 접속 및 서비스 레벨의 인증 서버 기능을 제공하는 것이 목적이다. 또한, 가입자가 어떤 액세스 망에 접속해도 상관없이 동일한 IMS 기반의 멀티미디어 서비스를 제공할 수 있어야 한다.

CUPS는 단일 시스템으로 동작하지 않고, 다른 네트워크 장비들과 연동하여 동작한다. 그림 7 처럼 유무선 액세스 망 위에 다양한 액세스 가입자 프로파일을 관리한다. IMS기반의 호 제어 서버에게 가입자 및 서비스 프로파일과 인증 벡터를 제공하고 응용서버에게 공통으로 필요한 서비스 프로파일을 필요로 한다. 또한, 네트워크 레벨에서 QoS를 관리하는 RACF에게 QoS 프로파일을 제공한다.

CUPS는 이동성 제어 서버와 멀티캐스트 제어 서버에게 각각에 필요한 프로파일 및 인증 정보를 제공한다. 방송형 서비스와 이동성 제공 서비스를 위하여 응용서비스 제공 인터페이스(Sh)를 통해서 통합 프로파일 정보를 제공한다. 또한, 액세스 및 서비스 네트워크 간 번들 인증 기능과 공통 프로파일 웹서비스 개방화 기능을 제공한다.

3.1 시스템 인터페이스

CUPS 시스템은 서킷 기반의 음성 호 서비스, 패킷 데이터 서비스, 그리고 IP 멀티 미디어 서비스 제어를 지원하기 위해, 이들 서비스를 제어하는 서브 시스템들과 표준화된 외부 인터페이스들을 통해 접속한다.

호 세션 제어 시스템인 S/I-CSCF 와는 Diameter 기반의 Cx 인터페이스를 통해서, 세션제어에 필요한 가입자 데이터와 인증 벡터를 처리한다. 응용 서비스 시스템인 AS 와는 Diameter 기반의 Sh 인터페이스를 통해서, 응용서비스에 필요한 가입자 데이터를 얻는다. 또한, 방송형 서비스 제어 및 이동성 제어 프로파일 관리를 위해서 Sh 인터페이스의 확장을 통해서 제공한다. 접속/전달망 시뮬레이터와 이종망간 접속 에뮬레이터로부터 받은 인증 요청은 EAP 메시지를 통해서 처리한다.

한편, CUPS OAM(Operation And Management)과 SNMP(Simple Network Management Protocol)와 internal 인터페이스를 통해, 형상 관리, 시스템 유지 보수, 데이터 관리, 측정 및 통계관리, 성능 관리 기능을 제공한다.

3.2 시스템 구조

CUPS 시스템은 그림 9와 같은 시스템 구조를 가진다. 크게 CUPS와 CUPS DBMS, CUPS OAM 장비로 구성되어 있다.

Diameter 메시지를 기본적으로 처리하는 Diameter base 처리 모듈이 있고, Diameter base 스택을 기본으로 Cx, Sh, e2 와 EAP Diameter 응용 프로그램으로 구성된다. 서비스 인증을 위한 인증 벡터 생성 및 액세스의 인증 처리를 위한 인증처리 모듈이 있다. CUPS 내부에 OAM 에이전트와 DB 서버가 존재하고, 여러 대의 CUPS OAM 에이전트가 OAM

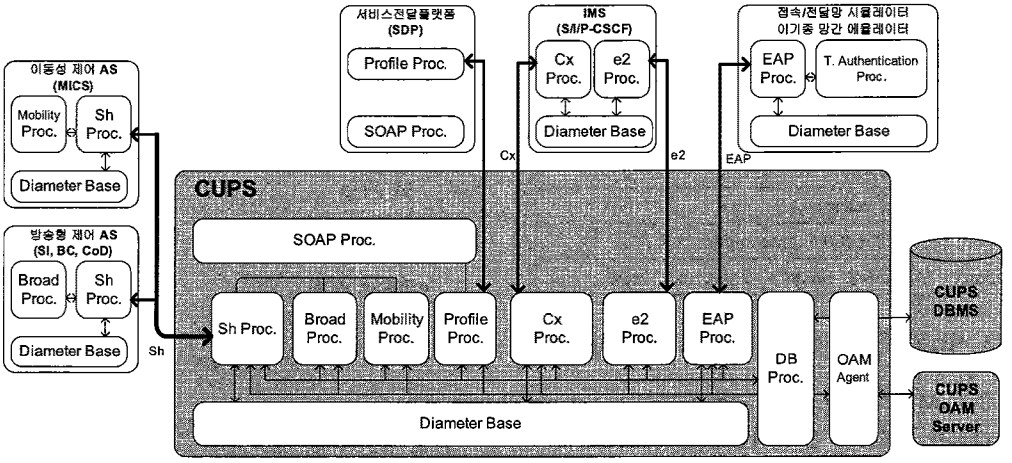


그림 9. CUPS 시스템 구조

표 1. CUPS 시스템 외부 인터페이스

종류	설명
Cx/ Diameter	S/I-CSCF와 인터페이스로 가입자정보, 서버할당, 인증벡터, 등록, 해지, 위치정보 메시지 처리
Sh/ Diameter	IMS AS와 인터페이스로 서비스 등록, 정보, 공지 메시지 처리 기본 Sh 메시지를 기반으로 이동성 제공 서비스 프로파일, 방송형 서비스 프로파일, 개인정보 통합관리 프로파일 정보 처리
Sh/SOAP	서비스 전달 플랫폼(SDP)과 인터페이스로 CUPS 공통프로파일정보를 개방화 처리
EAP/ Diameter	접속/전달망 시뮬레이터와 이종망간 에뮬레이터와 인터페이스로 EAP 기반의 접속 인증 처리
e2/ Diameter	번들 인증을 위해, 액세스의 line 혹은 context 정보 조회 기능을 처리
OAM/ SNMP, internal I/F	CUPS OAM과 인터페이스로 운영 관리 메시지 처리

client 로 동작하고, CUPS OAM 서버로 관리가 되어 운영자가 용이하게 운영관리를 한다. DBMS는 CUPS가 고성능을 요구하기 때문에 MMDB를 사용한다.

CUPS 시스템을 구성하는 주요 표준 규격은 표 2와 같다.

3.2.1 하드웨어 구성

- CUPS 시스템은 SUN blade 나 Fire 계열의 하드웨어 또는 CPCI(Compact Periperipheral Component Interconnect) 확장 장비
- CUPS DBMS는 CUPS 시스템과 동일

표 2. CUPS 시스템 표준 규격

규격 종류	버전	참조 규격	비고
Diameter Base		IETF RFC 3588	Diameter 기본 규격
EAP interface		IETF RFC 3748/4072	CUPS와 접속/ 전달망시뮬레이터와 이기종망간에 뮬레이터간의 인증 I/F 규격
Cx interface	Rel 7.0	3GPP 29.228/29.229	CUPS와 S/I-CSCF 간의 규격
Sh interface	Rel 7.0	3GPP 29.328/29.329	CUPS와 AS 간의 규격
MILENAGE(AKA) 인 증	Rel 7.0	3GPP 33.102/35.205/ 35.206/35.207/ 35.208	Digest-AKAv1-MD5인증을 수행할 수 있도록 AKA 인증 벡터를 제공
방송형 프로파일		ETSI TS 102 822-3-1/822-3-2/ 822-3-3 3GPP TS 26.234 R7 DVB-H/IPDC	방송형 프로파일 관리 정보
이동성 프로파일	D05.01	IEEE802.21	이동성 프로파일 관리 정보
e2 interface	Rel 1.0	ITU-T Q.3221	CUPS와 P-CSCF 간의 규격
Sh SOAP interface	Rel 7.0	3GPP 29.328/29.329	CUPS와 SDP 간의 규격

- CUPS OAM은 x86 기반의 PC 사용

3.2.2 소프트웨어 구성

- CUPS 시스템의 소프트웨어 구성은 표 3과 같다.

표 3. CUPS 시스템 소프트웨어 구성

종류	사양
OS	Solaris 2.10
컴파일러	SunStudio11
DBMS	Altibase 3.5
	isql release 3.5
	SES C/C++ Precompiler 3.5
Library	openssl, libxml2, expat, mel, scew

3.3 시스템 주요 기능 및 경쟁 기술과의 차별점

3.3.1 IMS 호 제어 서버와 연동 처리 기능
- 가입자 프로파일 관리 기능
- 가입자 Registration 관리 기능
- 세션 처리 관련 기능
- IMS 호 제어 서버(S/I-CSCF) 연동 메시지 처리 기능

3.3.2 응용 서버와 연동 처리 기능
- 가입자 별 서비스 프로파일 관리 기능
- 서비스 정보 구독 및 통지 기능
- 응용서버(AS) 연동 메시지 처리 기능

3.3.3 인증 처리 기능
- "Digest-AKAv1-MD5" 인증 처리 기능
- S-CSCF에 AKA 인증 벡터 제공
- 접속 Authentication Center 기능

3.3.4 이동성 제어 서버와 연동 처리 기능
- 가입자 별 등록 서비스 프로파일 관리 기능
- MIH(Media Independent Handover) IS(Information Server) 기반 이기종 네트워크 정보 관리 기능
- 특정 응용 공통 정보 제공 기능

3.3.5 방송형 제어 서버와 연동 처리 기능
- 가입자 별 서비스 프로파일 관리 기능
- 가입자 별 네트워크 프로파일 관리 기능
- 가입자 별 디바이스 프로파일 관리 기능
- 가입자 별 컨텐츠 프로파일 관리 기능
- 특정 응용 공통 정보 제공 기능

3.3.6 액세스 및 서비스 네트워크 간 번들 인증 처리 기능
- 접속 인증 시 인증 정보 전달 기능
- e2 메시지 처리 기능
- 서비스 인증 시 번들 인증 처리 기능

3.3.7 공통서비스 프로파일 개방화 처리 기능
- SOAP(Simple Object Access Protocol) 메시지 처리 기능
- 특정 사용자의 접속 위치 조회 기능
- 특정 지역, 시간, 성별, 나이의 사용자 목록 조회 기능

3.3.8 운용 관리 기능
- OAM 서버 기능
- OAM 클라이언트 기능
- NMS(Network Management System) 연동 기능

CUPS 시스템의 일반 HSS와 AAA 비교하여 주요 특징 및 차별점은 표 4와 같다.

표 4. CUPS 시스템의 경쟁 기술과의 차별점

항목	CUPS	HSS/AAA
인증 속도 및 범위	• 이종 액세스망 통합 인증 • 이종 액세스망간 고속 핸드 오버 인증 • 액세스망과 IMS 서비스망간 통합 인증	• 각 액세스 망별 접속 인증 • IMS 기반의 서비스 인증
프로파일 구성 방식	• 액세스망 통합 접속 사용자 프로파일 • MIH IS 기반 이동성 프로파일 • 사용자 선호도 기반 방송형 프로파일	• 액세스 망별 접속 사용자 프로파일 • IMS 기반의 서비스 사용자 프로파일
프로파일 제공 방식	• Diameter Sh 기반의 프로파일 제공 • SOAP/REST 기반의 프로파일 개방화 • 연방형(Federation) 프로파일 관리	• Diameter Sh 기반의 프로파일 제공
ID 관리 방식	• 프로파일과 연계된 IdP(Id Provider) 관리 • Open ID 발급, 인증 및 타켓 관리	• 해당 사항 없음

Ⅳ. 기능 시험 및 분석

본 장에서는 CUPS 시험 네트워크 구성 및 프로토타입 시스템 구현에 관련된 내용을 기술하고 분석한다.

4.1 시험네트워크 구성

그림 10은 CUPS 시스템에 대한 시험망 환경이다. 시험 환경을 설명하면, 장비 구성에는 크게 3가

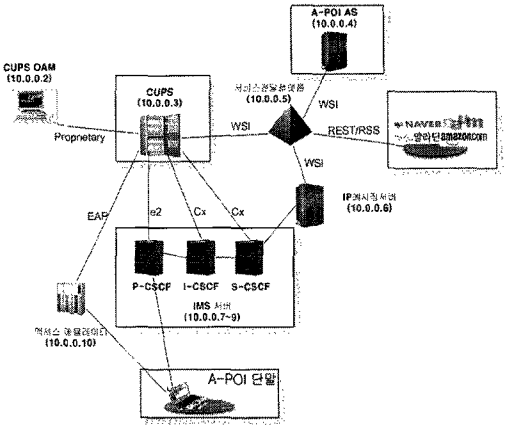


그림 10. CUPS 시험 네트워크 구성도

지 분류가 있다. 첫째는 CUPS 자체와 CUPS를 관리하는 OAM 장비가 있다. 둘째는 CUPS와 직접 연동하는 장비들이다. 호 세션 제어를 위한 IMS (P-CSCF, I-CSCF, S-CSCF), 방송서비스를 제공하는 방송형 AS, 이동성 정보를 관리하는 MICS, WCDMA, WiFi, WiBro 액세스망을 에뮬레이션해 주는 이기종 액세스망 에뮬레이터, 서비스전달플랫폼과 같은 4가지 장비가 있다. 마지막으로 CUPS와 연동 장비들을 이용하여 테스트 하기 위한 AS, IP 메시징서버, 웹포털 Open API, 단말과 같은 테스트 장비들이 있다.

4.2 시험 네트워크에서의 성능분석 및 검증

CUPS 서버의 성능 측정 자료를 기술한다. CUPS는 가입자 프로파일 및 인증을 처리하는 장치로써 성능 기준으로써 TPS(Transaction Per Seconds) 단위로 성능을 측정한다. 본 개발에서는 Diameter의 Device-Watchdog 메시지의 초당 처리량을 이용하여 성능을 측정하였고, CUPS 시스템을 SunFire v440과 IBM System p5 2가지 시스템을 통하여 성능을 검증하여 장비에 따라 성능이 어떻게 변화하는지 확인해보도록 한다. 측정 변수로써 동시에 띄울 수 있는 쓰레드 수를 조정하였고, 순수하게 메시지 처리할 경우, 통계 처리 여부, 로그 기록 여부, 로그 기록시 CPU Idle을 30% 이상일 경우를 달리해서 측정해 보았다.

4.2.1 SunFire v440 - Solaris 10 - 4CPU

표 5. SunFire v440에서 초당 메시지 처리량

쓰레드 수	1	2	3	4	5	6	7	8
메시지 처리	41597	74085	99585	116994	117568	120881	122560	125617
통계 수집	34324	61581	83252	97197	96615	98945	101428	102232
통계, 로그 기록	22819	37675	46184	49738	48172	47704	47281	46893
통계, 로그 기록※	15378	22153	20978	20458	20495	20470	20509	20197

※ 로그 메시지를 매번 파일에 기록한 경우 : CPU Idle 30% 이상

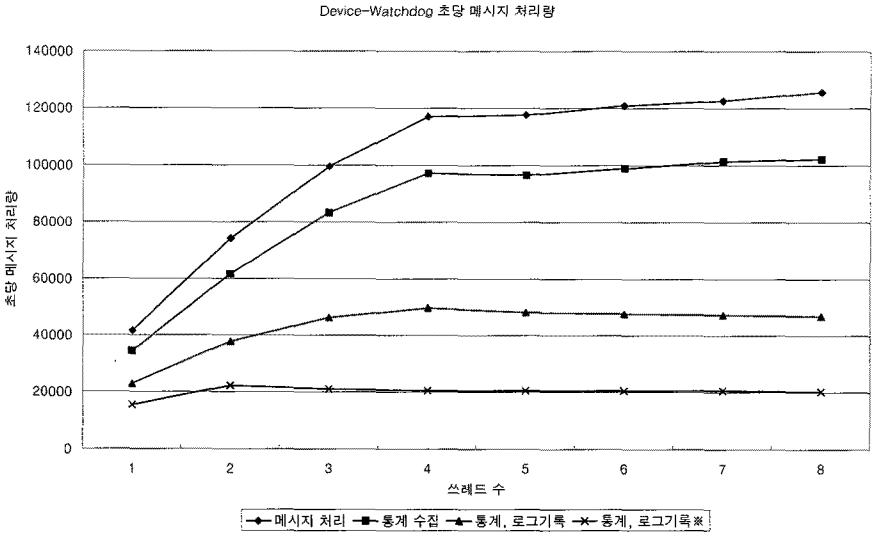


그림 11. SunFire v440에서 초당 메시지 처리량

4.2.2 IBM System p5(9113-550) - AIX 5.3 - 4CPU

측정 결과를 먼저 각 지표별로 살펴보도록 한다. 순수한 메시지 처리할 경우에 쓰레드를 많이 띄울수록 처리 용량이 늘어남을 알 수 있다. 전체 시스템 처리 용량이 제한되어 있으므로 SunFire, IBM 둘 다 쓰레드가 4개까지 선형적으로 증가하다가 그 이후부터는 거의 서서히 증가됨을 볼 수 있다. 통계 수집을 하였을 경우에는 순수 메시지 처리와 비슷한 추이를 볼 수 있었고, 다만 처리 성능이 20% 정도 감소함을 확인 할 수 있었다. 통계 수집과 로그 기록까지 할 경우는 SunFire 경우에는 비슷한 추이를 확인할 수 있었고 60% 정도 성능이 감소함을 확인 할 수 있었다. IBM의 경우에는 쓰레드가 2개까지 선형으로 증가하고 오히려 시스템 과부하가 일어나 쓰레드가 증가할수록 성능이 감소되었다. 이를 방지하기 위해서, CPU Idle 시간을 30% 이상으로 유지되도록 하였고, 그럴 경우에는 쓰레드가 3개까지 선형으로 증가하였고, 그 이후에는 약간 감소하기는 하지만 비슷한 추이를 나타내었다.

결론적으로 SunFire와 IBM 두 시스템을 비교해 보면, 순수 메시지 처리할 경우 IBM 이 15% 정도 성능이 좋게 나옴을 볼 수 있다. 그러나, 통계 수집과 로그를 추가했을 경우에는 반대로 IBM이 성능이 떨어지는 것을 볼 수 있다. 이것은 통계 수집과 로그 기록시 File IO 처리를 많이 하게 되는데, IBM 시스템이 File IO 처리가 SunFire 보다 약함을 알 수 있다. 즉, SunFire는 IBM에 비해 프로세스 처리 속도가 부족하지만, File IO 처리가 좋고 시스템이 안정적 임을 확인할 수 있었다.

표 6. IBM System p5 에서 초당 메시지 처리량

쓰레드 수	1	2	3	4	5	6	7	8
메시지 처리	41990	76986	108624	139504	144616	147645	149331	148996
통계 수집	33747	61520	82047	93623	92383	93892	90371	90313
통계, 로그 기록	24028	36644	30606	27389	23314	21088	19222	16400
통계, 로그 기록※	17741	19758	20530	19234	18232	17105	15861	15267

※ 로그 메시지를 매번 파일에 기록한 경우 : CPU Idle 30% 이상

V. 결론 및 향후 연구

통합 프로파일 구축의 의미는 사업자 관점에서 통합 DB 구축을 위한 DB 스키마 및 프로세스의 표준화를 통해 운용 비용(OPEX) 및 설치 비용(CAPEX) 절감 효과를 가져온다. 제 3 사업자는 사업자와의 서비스를 공유함으로써 개방형 API 및 프로파일 공유를 통해 신규 서비스를 창출하고, 사용

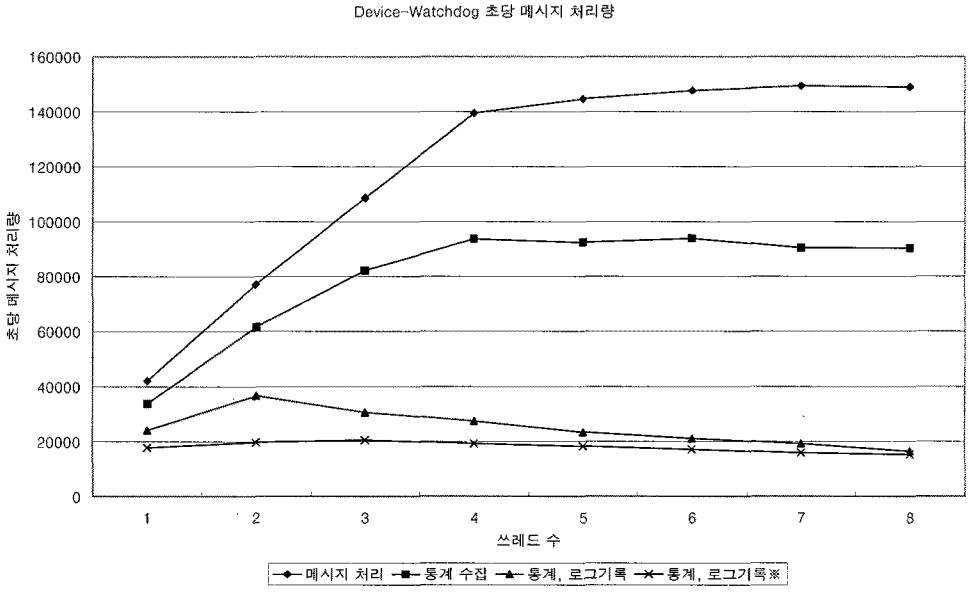


그림 12. IBM System p5 에서 초당 메시지 처리량

자와의 가입 관계를 단순화 할 수 있는 효과를 얻을 수 있다. 또한, 사용자는 한 번의 가입에 의한 단일 ID로 다양한 서비스를 누릴 수 있는 일관된 사용자 경험의 유지 및 개인화 서비스 제공 환경이 구축될 수 있다. 기술적 측면에서는 가입자 데이터를 통합 관리할 수 있는 CUPS를 제공함으로써 사업자에 상관없이 신규 서비스를 개발 및 제공할 수 있는 기반기술을 확보할 수 있으며 사업자 통합 인증/과금 제어기술 확보 및 새로운 응용 서비스를 유연하게 개발할 수 있는 API 확보가 가능하다. 또한 국내외 표준화 활동을 통하여 국제 규격의 NGN 표준화, 국내 표준 규격 확보 및 국제 표준화를 주도할 수 있는 기반을 마련할 수 있다.

통합 프로파일 관리 및 통합 인증 제어 분야의 향후 응용 분야와 활용 방법은 모든 통신사업자의 통합 프로파일 관리 시스템과 통합 인증 시스템 구축에 적용이 가능하고 통신·방송 융합 서비스 제어 시스템과 연계한 통합 제어 기술 및 NGN 사업자간 서비스 연동 시스템에 활용이 가능하다. 본 연구를 통해서 단말, 사용자, 서비스 프로파일 통합 가상화를 통한 사용자 중심 서비스를 제공할 수 있고, 접속 및 서비스 인증 절차 간소화를 통한 핸드오버 고속화 및 네트워크 ID 기반의 SSO 기능을 제공할 수 있었다. 이를 통해 융합 미디어 서비스를 위한 가입자/서비스 통합 프로파일 관리 및 제어를 할 수 있고, IPTV 및 이동성 제어 서비스를 위한 번들 인증 기능을 제공하고, 서비스 전달 플랫폼 기반의 개방형 프로파일을 활용한 신규 융합 서비스 및 프로파일 인에이블러 기능을 제공하게 될 것이다. 또한, 본 연구를 통해 제안한 번들 인증 기능은 기존 번들 인증 기법에서 사용자의 IP 주소 또는 위치 정보만을 통해 번들 인증을 제공하던 방법에 비해 초기 액세스 인증 과정에서 생성된 EMSK(Extended Master Session Key)로부터 유도한 BAK(Bundled Authentication Key)를 통해 번들 인증을 제공한다. 때문에 제안하는 기법은 기존 기법들에 비해 암호학적으로 안전하며, 표준화되고 있는 네트워크 구조를 거의 수정하지 않고 활용할 수 있기 때문에 효율성 또한 기존 기술에 비해 높다. 마지막으로, 향후 본 연구를 통해 제안하고 있는 암호학적 키를 이용한 번들 인증 기술에 대해 실제 망에서 적용해 보기 위한 구현 작업을 통해 실제적인 성능 평가를 필요하다.

참 고 문 헌

[1] 김영세 외 4명, "무선 네트워크 연동 보안 기술 동향", 전자통신동향분석, 제20권 제1호, pp.100-111, 2005. 2.

[2] 방정희, "BcN 기반에서 통합 프로파일 구축 전략", BcN 핵심기술 워크숍, 2006. 8.

[3] 정한욱 외 2명, "와이브로 접속 및 응용 서비스 통합 제어구조", 한국통신학회지, Vol.23, No.4, pp.47-58, 2006. 4.

[4] Naotaka Morita, "Functional Requirements and Architecture of the NGN," ITU-T Y.2012, July, 2006.

[5] Kwihoon Kim, Hyunwoo Lee, and Won Ryu, "Proposed Addition of Transport Stratum User Profile in Draft Q.NGN-trx.profile," ITU-T COM11-D143, July, 2006.

[6] 이상연 외 5명, "All-IP Core Network 기술," Telecommunication Review, 제 11권 6호, pp.826-837, 2001. 11.

[7] 유명식, 오돈성, "차세대 이동 통신 서비스 지원을 위한 프로파일 관리 기술 동향", 한국통신학회지, Vol.22, No.9, pp.77-88, 2005. 9.

[8] 박용문 외 3명, "통합 프로파일 관리 및 인증 제어 기술 동향", 전자통신동향분석, 제21권 제6호, pp.86-94, 2006. 12.

[9] "IP Multimedia Subsystem (IMS); Stage 2," 3GPP TS 23.228, June, 2008.

[10] "Service requirements for 3GPP Generic User Profile (GUP); Stage 1," 3GPP TS 22.240, Dec., 2008.

[11] "3GPP Generic User Profile (GUP); Stage 2; Data Description Method," 3GPP TS 23.941, June, 2007.

[12] "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents," 3GPP TS 29.228, Dec., 2008.

[13] "Cx and Dx interface based on the Diameter Protocol; Protocol details," 3GPP TS 29.229, Dec., 2008.

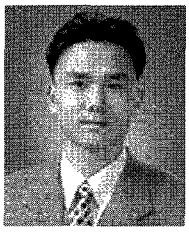
[14] "IP Multimedia (IM) Subsystem Sh Interfaces; Signalling flows and message contents," 3GPP TS 29.328, Dec., 2008.

〔15〕 "3G Security; Security architecture," 3GPP TS 33.102, Dec., 2008.
〔16〕 J. Rosenberg et al, "SIP: Session Initiation Protocol," IETF RFC 3261, June, 2002.
〔17〕 "IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control," IEEE 802.1x, Dec., 2004.
〔18〕 B. Aboba et al, "Extensible Authentication protocol (EAP)," IETF RFC 3748, June, 2004.

이 현 우 (Hyun-woo Lee) 종신회원

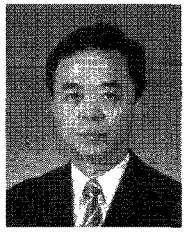
1993년 한국항공대학교 항공전자공학과(학사)
1995년 한국항공대학교 정보통신공학과(석사)
2005년 한국항공대학교 정보통신공학과(박사)
1995년~현재 한국전자통신연구원 방송통신융합연구부문 IPTV연구부 융합서비스네트워킹연구팀 팀장
<관심분야> 서비스 제어기술, 통신망 연동, 트래픽 혼잡제어

김 귀 훈 (Kwihoon Kim) 정회원



1998년 KAIST 전기및전자공학과(학사)
2000년 KAIST 전기및전자공학과(석사)
2000년~2005년 LG데이콤 종합연구소 BcN서비스연구팀 주임연구원
2005년~현재 한국전자통신연구원 방송통신융합연구부문 IPTV연구부 융합서비스네트워킹연구팀 선임연구원
<관심분야> 서비스 플랫폼 기술, 서비스 오버레이 기술, 이동성, IPTV, IMS, M2M 기술

류 원 (Ryu Won) 정회원



1983년 부산대학교 계산통계학과(학사)
1988년 서울대학교 계산통계학과(석사)
2002년 성균관대학교 정보공학과(박사)
1989년~현재 한국전자통신연구원 방송통신융합연구부문 IPTV연구부 부장
<관심분야> IPTV, 이동성, 이종망간 핸드오버, 유무선 연동, BcN