주 제

와이브로 접속 및 응용 서비스 통합제어 구조

KT 정한욱, 방정희, 이덕기

차 례

I. 서 론

IP 네트워크를 기반으로 하여 어떤 접속망을 통해서도 동일한 통신 서비스 및 멀티미디어 컨텐츠를 고객 단말에게 전달해 줄 수 있는 All-IP 기반 유무선 통합망에 대한 필요성과 관심이 증대하고 있다. 전통적으로 유선과 무선망은 서로 분리된 영역에 존재하여, 각기 다른 기술과 서비스가 적용되며 시장 또한 분리되어 있으나, 유무선 통합 기술은 각 사업자들이 고객에게 유, 무선에 제한되지 않는 모든 종류의 서비스를 제공할 수 있도록 물리적인 장벽들을 제거하고 있다. 유무선 통합을 통하여, 유선 통신 사업자는 점점 좁아지는 유선 사업 영역에만 국한되지 않고 사업 영역을 확장할 수 있으며 무선 통신 사업자는 점점 까다로워지는 무선 이용자의 요구에 부응하여 좀더 넓은 대역폭의 견고한 네트워크 자원을 제공할 수 있다.

국내에서 세계 최초로 상용화가 추진되고 있는 와이브로는 기존의 유선 사업자에게 이러한 유무선 통합망을 통해 종합 통신 사업자로의 진화를 가능하게 하는 첫걸음을 제공하며, 무선 사업자에게는 기존의 고비용의 셀룰러 망을 대신하여 대용량의 대역폭을 이동통신 고객에게 안정적으로 제공할 수 있는 기회를 제공한다.

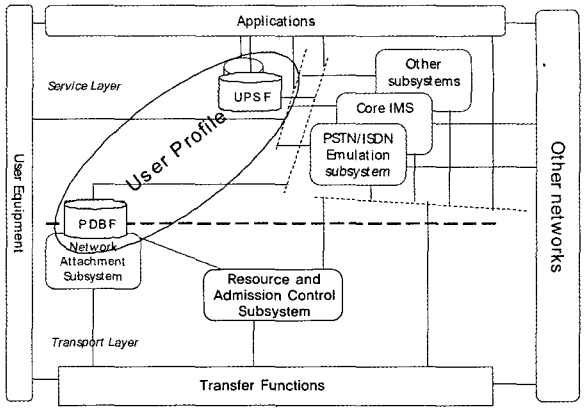
본 고에서는 All-IP 기반 유무선 통합망의 표준화 동향과 함께 와이브로의 기술적, 전략적 위치를 살펴보고, 스마트카드 기반의 와이브로 접속인증에 대해 상세히 설명한다. 또한 와이브로 플랫폼에서의 다양한 서비스 인증 및 과금 기능과 접속/서비스의 연계를 통한 SSO에 대해 기술한다. 마지막으로 KT의 유무선 통합 인증/과금 플랫폼인 U-BRAIN (Ubiquitous Broadband Roaming Accessible InterNet)을 통한 와이브로의 접속 및 응용 서비스의 유기적인 연계와 통합 제어 전략, 그리고 향후 진화 방향에 대해 설명하고자 한다.

II. All-IP 유무선 통합 네트워크 표준화 동향

현재 3GPP, ETSI, ITU 등 여러 표준화 단체에서 정의되고 있는 All-IP 기반 유무선 통합 차세대 네트워크의 개념은, 전체 네트워크 구조를 크게 전달 계층과 서비스 계층으로 분리하여, 서비스 계층에서 정의되고 있는 서비스들을 접속망의 종류에 제한받지 않고 동일하게 가입자에게 제공할 수 있게 하는 구조이다. 전달 계층에 포함되는 IP 접속망 (IP-CAN; IP-Connectivity Access Network)의 종류는 유선의 xDSL, Cable 등과 무선의 WLAN, GPRS, CDMA2000 등이 있으며, 개념적으로 와이브로 또한 새로운 무선 IP-CAN으로 정의될 수 있다.

3GPP에서 추구하는 목표는 단기적으로는 현재 회선 및 패킷 방식이 혼재하는 이동통신 시스템을 진화하여 단일화된 패킷 방식의 IP 네트워크를 통해 음성 및 멀티미디어 서비스를 제공하는 것이며, 궁극적으로는 All-IP 망을 기반으로 한, 어떤 접속망을 통해서도 동일한 멀티미디어 서비스의 제공이 가능하며 각 네트워크 간에 중단 없는 이동성을 제공하는 유무선통합 통신 인프라를 구축하는 것이다. 그러기 위해서 기본적으로 접속망과 IM Core Network를 분리하여 IMS 아키텍쳐 설계를 하였지만, 설계의 또 다른 핵심 사상인, 서비스 별로 차별화된 정책 (SBLP; Service Based Local Policy)이 적용되는 QoS 기반의 서비스가 아직까지는 자신들의 태생 기반인 GPRS 망에서의 접속 시에만 가능한 정도로 규격 작업이 진행되고 있다[1~2].

이에 따라 유럽의 이동통신 사업자에 국한되지 않는, 전세계의 다양한 IP 접속망 사업자를 위한 All-IP 차세대 네트워크(NGN)의 개념 및 규격이 강력하게 요구되었고, ETSI, ITU 등에서 현재 그 작업을 진행 중이다. 하지만 ETSI, ITU 등에서도 3GPP에서 작업한 IMS의 설계 사상 및 규격을 버리지 않고 그대로 적용하면서, 3G 이동통신 사업자만을 위한 것이 아닌 범 IP 접속망 사업자의 유무선 통합 서비스를 위한 NGN의 추가적인 개념과 규격을 새롭게 도입하여 표준화 작업을 진행하고 있고, 그 결과물을 다시 3GPP 쪽으로 반영하고 있는 추세이다.



(그림 1) TISPAN NGN 구조

이를 위해 ETSI TISPAN에서는 전체 네트워크 구조를 (그림 1)과 같이 크게 서비스 계층 (Service Layer)과 전달(접속) 계층 (Transport Layer)으로 나누고, Core IMS를 서비스 계층에서 가능한 여러 서브시스템 중의 하나로 정의하였고, NGN에서 기존 POTS 서비스를 제공하기 위한 PSTN/ISDN Emulation Subsystem에 대한 규격 작업을 독자적으로 수행하고 있다[3].

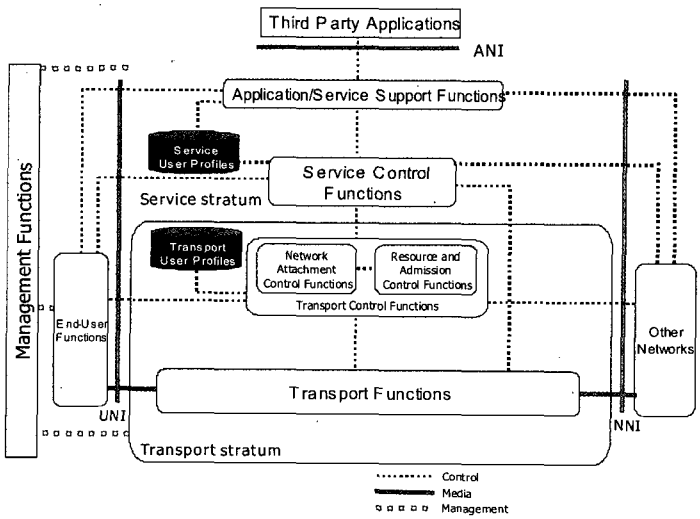
GPRS 망 이외에 다양한 IP 접속망을 위해서는, 전달 계층에서 NASS (Network Attach-ment SubSystem)와 RACS (Resource and Admission Control Subsystem)를 새롭게 정의하였고 이를 통하여 xDSL, WLAN 등을 통한 SBLP를 가능하게 하는 구조를 개념적으로 정립하였다. NASS는 전달 계층에서 가입자 프로파일에 기반한 접속 인증, 권한검

증, 동적인 IP 할당, 접속망 구성, IP 계층에서의 위치 관리 등을 수행하며, RACS는 서비스 제어 기능 및 전달 기능과 연동하여 자원 예약, 승인 제어 등의 QoS 관리, NAPT/FW 제어, NAT traversal 등의 기능을 담당한다.

가입자 프로파일 관련으로는, 서비스 계층의 서브시스템들이 기능하는 데 필요한 가입자 정보를 UPSF (User Profile Server Function), 접속 계층의 서브시스템들이 기능하는 데 필요한 가입자 정보를 PDBF (Profile DataBase Function)로 논리적으로 구분하였다. 실제적으로는 그 안에서도 각 부분 별로 상세히 나뉘어 질 수 있으며, 실제 구현은 사업자의 선택에 따라 적절히 분리 및 통합이 가능한데, 가입자에게 좀더 다양한 컨버전스 형 서비스를 제공하고 다양한 사업 모델과 기회를 창출하기 위해서는 전체적인 통합 모델로 가는 것이 바람직한 것으로 보인다.

ITU의 NGN은 SG13에서 출발한 NGN Focus Group (FGNGN)이 작년까지 여러 표준화 단체와의 협력을 통해 기본적인 NGN 개념의 틀을 정립한 상태로써 (그림 2), 유무선 통합 All-IP 망을 위한 TISPAN의 NGN 모델과 상당히 유사하다.

TISPAN과 마찬가지로 전체적인 네트워크 구조를 서비스 계층 (Service Stratum)과 전달 계층 (Transport Stratum)으로 나누었으며, 전달 계층에서의 핵심 기능인 NACF (Network Attachment Control Function)와 RACF (Resource and Admission Control Function)도 TISPAN의 NASS, RACS와 거의 유사하다. 또한 Service User Profile은 UPSF과, Transport User Profile은 PDBF와 유사한 개념이다 [4].



(그림 2) ITU-T NGN 구조

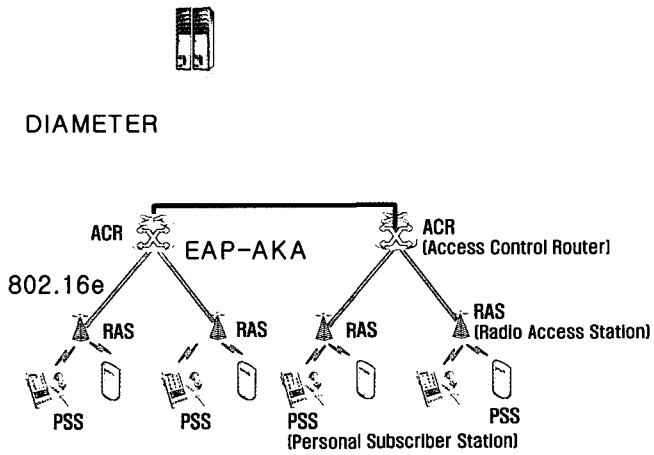
III. 와이브로에서의 접속, 응용 통합 서비스

1. 접속 인증

KT 와이브로의 인터넷 접속 서비스는 KT 무선랜 서비스의 NESPOT CM (Connection Manager)과 유사하게, 와이브로 단말에 설치된 네트워크 접속용 프로그램 WCM (Wibro Connection Manager)를 통하여 이루어 진다. 인증 방식은 3G 이동통신망에서 안정성과 보안성이 검증된 서버-단말간 상호인증 방식인 AKA (Authentication and Key Agreement)를 이용하며 [5], 실제로는 범용 인증 프로토콜인 EAP (Extensible Authentication Protocol)와 결합된 EAP-AKA 방식을 통해 인증 및 무선링크 암호화를 위한 키 생성이 이루어 진다[6].

또한 WCDMA 서비스에 필수

적으로 적용되는 스마트카드 장치인 UICC (Universal Integrated Circuit Card)에 EAP-AKA 인증을 위한 WSIM (Wibro Subscriber Identity Module) 응용모듈을 구현하여, 인증에 이용되는 키 정보를 안전하게 저장할 수 있는 보안성과 함께 여러 개의 단말을 하나의 카드로 이동해 가면서 사용할 수 있는 등의 사용자 편의성을 한층 강화하였다. 추후 UICC 카드에 추가적인 응용모듈 탑재를 통해 신용카드, 뱅킹 등 다양한 기능도 제공할 예정이며, 여기에 WCDMA용 인증 모듈인 USIM (Universal Subscriber Identity Module) 기능을 추가하면 하나의 UICC 카드로써 와이브로-WCDMA 듀얼 모드 단말의 접속인증을 모두 처리할 수 있다.



(그림 3) 와이브로 접속 인증 구성도

이러한 단말과 인증서버간의 EAP-AKA 인증을 위해서, 단말 (PSS; Personal Subscriber Station)과 기지국 (BS; Base Station) 간에는 802.16e 규격인 PKMv2 (Privacy Key Management version 2) 프로토콜에 캡슐화된 형태로 EAP 패킷이 전송되며 [7], 기지국~인증서버 (AAA; Authentication, Authorization, Accounting)간에는 차세대 인증/과금 프로토콜인 DIAMETER를 이용하여 EAP 패킷이 전송된다 [8]. 와이브로에서는 802.16e에서 정의하고 있는 기지국 (BS)의 기능이 물리적으로 무선접속장치 (RAS; Radio Access Station)와 접속제어국 (ACR; Access Control Router)으로 나뉘어 구현되어 있고, 두 장치 간의 역할 분담은 장비 제조사 별로 약간씩 다르게 구현되어 있다(그림 3). 단말-기지국-인증서버 간의 인증/보안 관련 메시지 흐름은 (그림 4)에 나타내었다.

가. PSS는 BS와의 무선구간 협상이 정상적으로 완료된 후, PKMv2 EAP Start 메시지를 전송하여 인증 절차를 시작한다.

나. BS는 EAP-Request/Identity를 PKMv2 EAP-Transfer 메시지에 실어서 PSS로 전송한다.

다. PSS는 EAP-Response/Identity 메시지를 AAA로 전송한다.

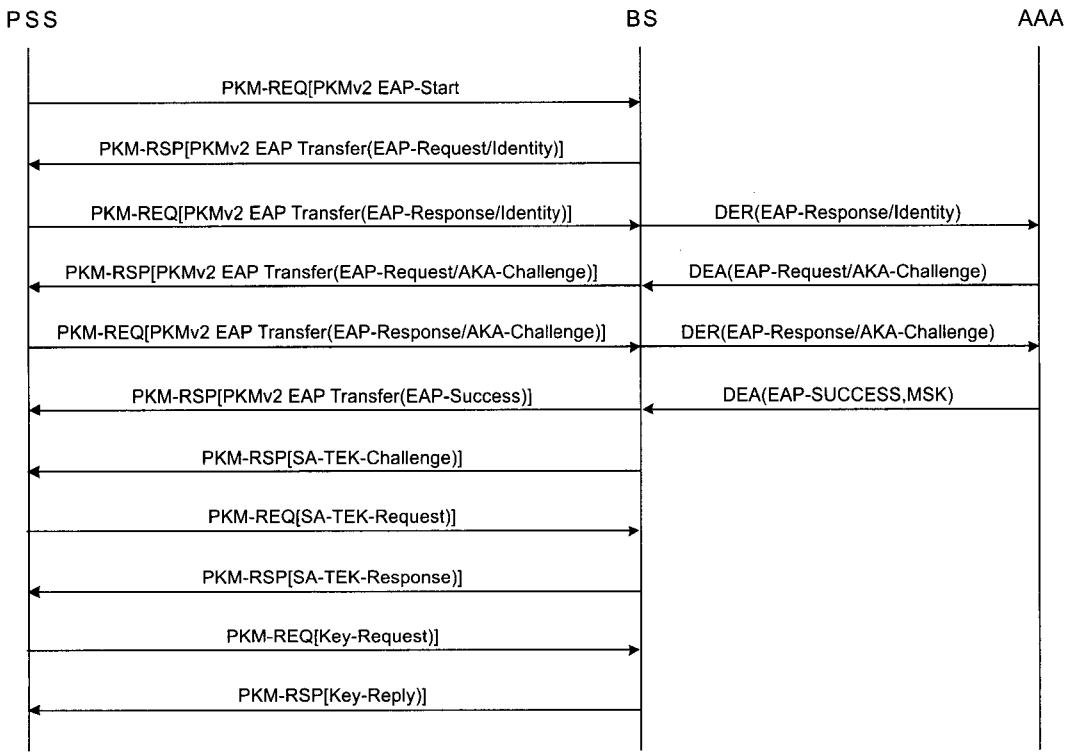
A. PSS는 EAP-AKA identity (NAI 형식)로 AT_IDENTITY attribute를 생성한다.

B. PSS는 AT_IDENTITY를 이용하여 EAP-Response/Identity를 생성하고, PKMv2 EAP-Transfer 메시지에 실어서 BS로 전송한다.

C. BS는 EAP-Response/Identity를 DER (Diameter EAP Request) 메시지에 실어서 AAA로 전송한다.

라. AAA는 EAP-Request/AKA-Challenge 메시지를 PSS로 전송한다.

A. AAA는 PSS로부터 전송된 identity와 그에



(그림 4) 인증/보안 메시지 흐름도

맞는 기 저장된 비밀키 K, OPc를 이용하여 AKA 알고리즘을 실행하고, RAND, AUTN, XRES, MSK 등을 생성한다.

B. AAA는 RAND와 AUTN을 이용하여 EAP-Request/AKA-Challenge를 생성하고, DEA (Diameter EAP Answer) 메시지에 실어서 BS로 전송한다.

C. BS는 EAP-Request/AKA-Challenge를 PKMv2 EAP-Transfer 메시지에 실어서 PSS로 전송한다.

마. PSS는 EAP-Response/AKA-Challenge 메시지를 AAA로 전송한다.

A. PSS는 저장된 identity, K, OPc를 이용하여 AKA 알고리즘을 실행하고, AAA로부터 전송된 AUTN과 MAC을 검사한다.

B. PSS는 AKA 알고리즘을 통해 RES와 MSK (Master Session Key)를 생성하고, RES를 이용하여 EAP-Response/AKA-Challenge 메시지를 생성한다.

C. PSS는 EAP-Response/AKA-Challenge를 PKMv2 EAP-Transfer 메시지에 실어서 BS로 전송한다.

D. BS는 EAP-Response/AKA-Challenge를 DER 메시지에 실어서 AAA로 전송한다.

바. AAA는 EAP-Success 메시지를 PSS로 전송한다.

A. AAA는 PSS로부터 전송된 MAC을 검사하고, 전송된 RES가 라-A에서 생성했던

XRES와 같은지 검사한다.

B. AAA는 EAP-Success를 생성하고, 라-A에서 생성했던 MSK와 함께 DEA 메시지에 실어서 BS로 전송한다.

C. BS는 전송된 MSK를 이용하여 PMK (Pairwise Master Key), AK (Authorization Key), KEK (Key Encryption Key), CMAC_KEY_U, CMAC_KEY_D를 생성하여 저장하고, EAP-Success를 PKMv2 EAP-Transfer 메시지에 실어서 PSS로 전송한다.

D. PSS는 BS로부터 EAP-Success 메시지를 포함한 PKMv2 EAP-Transfer 메시지를 수신한 후, 마-B 에서 생성된 MSK를 이용하여 PMK, AK, KEK, CMAC_KEY_U, CMAC_KEY_D를 생성하여 저장한다.

사. BS는 PSS로 SA-TEK-Challenge 메시지를 전송한다.

A. BS는 8바이트 길이의 난수(BS_Random)를 생성한다.

B. BS는 AK와, AK의 sequence number, PSS의 MAC주소, BS의 BSID를 입력 값으로 하는, Dot16Kdf를 수행하여 얻은 값을 AKID로 한다.

C. BS는 PMK lifetime 값을 메시지에 포함시키고 본 메시지에 대한 CMAC tuple을 붙여 전송한다.

아. PSS는 BS로 SA-TEK-Request 메시지를 전송한다.

A. PSS는 8바이트 길이의 난수(MS_Random)를 생성한다.

B. PSS는 BS로부터 받은 BS_Random을 메시지에 포함시킨다.

C. PSS는 BS로부터 받은 AK sequence number를 검증하고 메시지에 포함시킨다.

D. PSS는 BS로부터 받은 AKID를 검증하고 메시지에 포함시킨다.

E. PSS는 지원 가능한 cryptographic suite를 Securities capabilities TLV로 메시지에 포함시킨다.

F. PSS는 SBC 절차를 통해 결정된 Security Negotiation Parameter를 메시지에 포함시킨다.

G. PSS는 본 메시지에 대한 CMAC tuple을 붙여 전송한다.

자. BS는 PSS로 SA-TEK-Response 메시지를 전송한다.

A. PSS로부터 받은 MS_Random, BS_Random, AK sequence number, AKID을 검증하고 메시지에 포함시킨다.

B. BS는 Primary SAID, SA type, SA service type cryptographic suite 값이 들어간 SA descriptor를 메시지에 포함시킨다.

C. PSS로부터 받은 Security Negotiation Parameter를 검증하고 메시지에 포함시킨다.

D. BS는 본 메시지에 대한 CMAC tuple을 붙여 PSS로 전송한다.

차. PSS는 BS로 Key-Request 메시지를 전송한다.

A. PSS는 Key Sequence Number, SAID, 랜덤하게 생성한 Nonce 값을 메시지에 포함시키고, CMAC tuple을 붙여 BS로 전송한다.

카. BS는 PSS로 Key-Reply 메시지를 전송한다.

A. BS는 Key Sequence Number, SAID, PSS로부터 받은 Nonce 값을 메시지에 포함시킨다.

B. BS는 랜덤하게 생성한 TEK (Traffic Encryption Key)를 KEK로 암호화시켜

TEK-Parameters에 담아 메시지에 포함시키고, CMAC tuple을 붙여 PSS로 전송한다.

C. PSS는 전달받은 TEK-Parameters로부터 KEK를 이용하여 TEK를 복호화하여 저장한 후, 이후 BS와의 통신시 트래픽 데이터를 암호화하는 키로써 이용한다.

위와 같은 과정을 통해 접속 인증이 성공하여 무선구간 데이터 암호화를 위한 키가 도출되면, 단말에 IP Address가 할당되고 무선구간 데이터 전송을 위한 채널이 단말과 기지국 사이에 생성된다. 이 채널은 일반적으로 QoS 정보가 설정되지 않은 Best Effort (BE) 채널이며, 데이터 다운로드를 위한 서비스 플로우 (SF; Service Flow)와 업로드를 위한 서비스 플로우, 모두 2개의 SF로 이루어지며 SF 생성에 따른 과금 세션이 시작됨으로써 휴대인터넷을 이용할 수 있는 준비가 완료된다.

와이브로의 접속인증에는 이와 같이 EAP-AKA 방식을 이용하지만, U-BRAIN은 이외에도 PAP, CHAP 및 EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PSK 등 다양한 EAP method를 지원하므로, 와이브로 뿐 아니라 다른 접속상품에도 다양한 인증 서비스를 제공할 수 있다. 또한 시간/패킷 기반의 종량제 서비스를 위한 과금 수집 기능과 함께 선불 구매 금액이 소진된 경우, 혹은 분실신고 및 유해트래픽 신고가 들어온 경우 실시간으로 해당 단말의 접속을 종료할 수 있는 Diameter 기반의 세션 제어 기능이 구현되어 있다.

2. 서비스 인증

2.1. Best Effort 서비스

앞서 설명한 바와 같이 접속 인증을 통해 기본적인 BE 서비스 플로우 2개(Uplink/Downlink)가 생성되며, 이를 통해 사용자는 웹서핑과 같은 기본적인 인터넷 이용과 함께 사업자 혹은 3rd Party 서비스 제공자로부터 VoD, VoIP, 사진 및 만화 컨텐츠 이용 등 특화된 서비스를 제공받을 수 있다.

이런 특화된 서비스는 일반적으로 특정 응용서비스 서버 (AS; Application Server)를 통하여 이루어지며, 사용자가 접속인증을 통해 인터넷에 연결된 후 단말의 응용 소프트웨어를 통해 원하는 AS로 접속함으로써 시작된다. 이때 AS는 단말의 접속 및 서비스 요청 시 해당 서비스를 제공하기 전에 서비스 인증을 수행하여 사용자가 누구인지, 요청하는 서비스에 대한 사용 권한이 있는지, 제공한 서비스에 대한 과금은 어떤 방식으로 되는 것인지에 대한 확인을 마친 후 서비스를 제공하게 된다.

이때 일반적으로는 가입자 프로파일을 가지고 있는 사업자의 중앙 플랫폼에서 서비스 인증, 과금수집 및 빌링 기능을 수행하고, AS는 그 인증 결과를 전달받아 사용자에게 서비스를 제공하고 그에 따른 원시 과금정보를 중앙 플랫폼에 전달하는 기능을 수행한다.

U-BRAIN은 이를 위해 다양한 서비스 인증 방식 및 과금 처리 기능을 구현하여, 새로운 서비스가 출시될 때 플랫폼의 구조 변경 없이 즉각적인 상용화를 지원할 수 있도록 설계되었다. SIP 서비스 등을 위한 HTTP Digest (MD5, Digest-AKA) [9~10] 등 표준화된 서비스 인증 및 다양한 비표준 인증방식을 지원하며, 실시간 접속세션 정보를 이용하여 서비스 인증을 수행하는 SSO (Single Sign On) 기능을 제공한다.

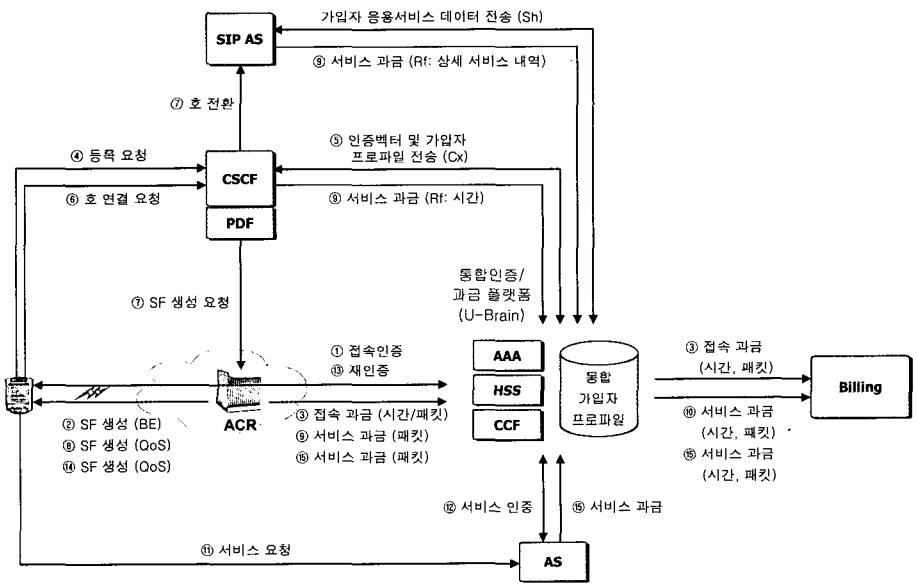
2.2. QoS 서비스

와이브로의 네트워크 접속제어장치인 ACR은 무선구간 채널 생성시 Policy를 적용할 수 있는 PEP (Policy Enforcement Point) 역할을 수행하며, 이

에 따라 와이브로 가입자에게 서비스 별로 차별화된 (SBLP; Service Based Local Policy) end-to-end QoS 보장형 서비스를 제공할 수 있다. 단말의 QoS 보장형 서비스 요청시, 이에 대한 인증 및 권한 검증이 수행된 후, PDF (Policy Decision Function)는 COPS (Common Open Policy Service) 프로토콜을 이용하여 ACR로 하여금 해당 서비스 세션을 위한 QoS 보장형 서비스 플로우 집합을 생성시키고, 이후 해당 서비스의 미디어 트래픽은 생성된 서비스 플로우들을 통하여 전송된다. 이때 서비스를 위한 세션 생성 및 제어 시그널링 트래픽은 처음 접속 인증 시 생성된 BE 서비스 플로우를 통해 전달되므로, QoS 서비스 세션 생성을 위해서는 기본 BE 접속 세션이 미리 존재해야 하며, 접속 세션을 종료하게 되면 모든 서비스 세션도 함께 종료된다.

이러한 서비스는 IMS 기반 또는 비 IMS 기반으로 제공될 수 있으며, U-BRAIN은 두 가지 방식을 모두 지원한다. IMS 기반 서비스를 위하여 U-BRAIN에는 통합 가입자 프로파일을 기반으로 한 HSS (Home Subscriber Server) 기능과 그에 수반되는 Cx, Sh 인터페이스 및 IMS 기반 과금 정보 수집을 위한 CCF (Charging Collection Function) 기능이 구현되었다[11~13]. 다음 그림에서 이를 나타내었는데, 간략화를 위하여 상세한 메시지 흐름은 생략하였다.

먼저 접속 인증을 통해 생성된 BE 서비스 플로우를 통하여 인터넷에 접속된 후 (①②③) 단말은 P-CSCF를 통해 IMS 망에 등록을 요청하고 (④), U-BRAIN은 이때 Cx 인터페이스를 통하여 S-CSCF로 가입자 인증을 위한 Digest-AKA 인증벡터와, 등록 이후에 S-CSCF가 가입자에 대한 호처리를 할 수 있도록 해당 가입자 프로파일을 전송해 준다 (⑤). 등록이 성공적으로 완료되면, 단말은 IMS 망을 통한 호착신 또는 호발신을 할 수 있는 상태가 되는데, 그림에서는 호발신을 하여 세션을 생성하는 것을 보여준다.



(그림 5) 와이브로 접속/서비스 인증 및 과금 구성도

단말이 접속인증 시 생성된 BE 서비스 플로우를 통해 CSCF로 호연결 메시지를 전송하면 (⑥), CSCF는 U-BRAIN으로부터 전송받은 가입자 프로파일을 이용하여 호연결 요청에 대한 권한 검증을 수행하고, 호 처리를 수행하는 한편 (⑦), 호연결 요청 메시지에 포함된 SDP (Session Description Protocol) 정보를 이용하여 PDF (Policy Decision Function)를 통해 ACR로 하여금 QoS 보장형 서비스 플로우들을 생성하게 한다 (⑧). 예를 들어 단말이 화상전화 호연결 요청을 한 경우, Audio UP/Audio Down/Video Up/Video Down 이렇게 4개의 서비스 플로우가 생성되어, 각 미디어 트래픽은 해당 서비스 플로우를 통해 전송이 된다. 하나의 IMS 세션에 포함된 서비스 플로우 각각의 과금 메시지에는 3GPP 규격을 준용한 ICID (IMS Charging ID)가 포함되어 있어, ACR, CSCF, SIP AS로부터 전송되는 과금 메시지 안에 들어있는 ICID를 이용하여 Correlation을 통해 하나의 과금 세션으로 처리가 가능하다 (⑨⑩).

비 IMS 기반 서비스 제공시 단말이 직접 AS로 QoS 서비스 이용요청을 하는 경우에는 (⑪), AS가 U-BRAIN에 서비스 인증을 요청하면 U-BRAIN이 서비스 인증을 수행한 후 (⑫), Diameter-EAP 재인증 과정을 통해 ACR이 서비스 플로우를 생성하는 데 필요한 Policy 정보를 전달해 줌으로써 (⑬), IMS 기반 서비스와 마찬가지로 QoS 보장형 서비스 플로우를 생성할 수 있다 (⑭). 또는, IMS 기반 서비스에서 CSCF가 PDF를 통해 ACR로 하여금 서비스 플로우를 생성하게 하는 것과 같은 방식으로, U-BRAIN이 PDF와 연동하여 해당 서비스 플로우 조합을 생성하는 것도 가능하다. 사용할 수 있는 서비스 인증 방식으로는 사용자가 인증 화면에 자기 ID/Password를 입력하는 방식, 단말에 인증인자를 저장하여 인증시 이를 읽어서 이용하는 방식, 또는 접속 세션 정보와 연계된 SSO 방식 등이 이용될 수 있고, 인증 프로토콜로는 HTTP Digest를 이용하여 Nonce-Response 구조를 통한 패스워드 보안이 이루어 진다. 그리고 AS는 인증 결과에 따라 단말에게 해당 서비스를 제공하고, 그에 따른 과금 정보를 U-BRAIN에 전송한다.

3. 접속 계층과 서비스 계층

앞서 설명한 바와 같이 응용서비스는 일단 네트워크 접속이 완료된 후에야 가능하며, 접속 세션이 종료되면 그 위에서 진행되던 모든 서비스 세션도 끊어지게 된다. 이동전화의 시스템 진화모델로 진행되어 온 3GPP IMS 표준과의 큰 차이점은, GPRS 망에서도 접속 인증은 존재하지만 이후 생성되는 최초의 접속 세션은 데이터 트래픽을 위한 채널이 아니라 이후의 IMS 서비스 세션을 생성하기 위한 SIP signaling bearer일 뿐이고, 단말의 전원을 끄기 전까지는 해제되지 않으며 또한 과금도 되지 않는 채널이라는 점이다.

반면에 와이브로에서는 접속 인증 후에 생성되는 접속 세션을 통하여 IMS 서비스 세션의 생성 및 제어를 위한 SIP 메시지를 전달할 뿐만 아니라, 접속 세션을 통하여 기본적인 시간/패킷 종량제 기반의 인터넷 접속 서비스 및 다양한 BE 응용 서비스들을 제공하며, 이를 통해 다양한 선불/후불제 접속 상품을 가입자에게 제공한다. 또한 GPRS 망에서는 Signaling path를 위한 접속 세션이 단말을 켜면 자동적으로 생성되며 단말의 전원을 내리기 전까지 항상 존재하는 데 비해, 와이브로에서는 접속 세션이 (설정에 의해 자동으로 접속시도를 하는 것도 가능하지만) 기본적으로 WCM을 이용한 사용자의 액션에 의해 시작되며, 일정량 이용 후 사용자의 접속종료 요청에 의해 종료가 되거나, 또는 선불 금액 소진 등의 경우 AAA에 의해 강제 종료가 된다.

특히 AAA에 의한 접속 세션 종료의 경우 서비스 계층 입장에서는 아무런 통보 없이 갑자기 데이터 및 시그널링 트래픽 전송을 위한 무선 구간 자원이 모두 사라지는 비정상적인 형태이므로, 이를 서비스 계층에서 자체적으로 파악하고 해결하기 위한 시간과 자원의 낭비가 발생하며, 완전한 정보 보정이 이루어지기 전까지는 물리적으로 접속이 종료됐음에도 불구하고 서비스 계층에는 계속 등록 상태로 되어 있는 등 일시적인 불일치가 발생하게 된다.

비정상 종료 시 예상할 수 있는 상황은, 서비스 계층에서는 단말이 계속 등록상태로 되어 있기 때문에 호 연결 요청이 들어온 경우 쓸데없는 라우팅 시도에 의한 시간 및 자원의 낭비가 발생하며 프레즌스 서버에도 일정시간 동안 부정확한 정보가 유지되게 된다.

참고로 3GPP IMS에서는 미디어 트래픽을 전달하는 IP-CAN bearer가 유실된 경우에 망 접속장치(GGSN, 와이브로에서는 ACR)는 COPS를 이용하여 PDF로, PDF는 Gq 인터페이스를 통해 P-CSCF로 그 사실을 알려주며, 이때 특정 IMS 세션에 포함된 모든 IP-CAN bearer가 유실된 경우에는 P-CSCF가 채널이 유실된 단말을 대신하여 상대편 SIP User Agent로 SIP BYE 메시지를 전송함으로써 세션을 종료하는 과정은 마련되어 있다. 그러나 서비스 계층에서 어떠한 신호 메시지도 없이 무선구간 IP-CAN bearer (특히 signaling bearer)가 유실된 경우, 이것이 일시적으로 커버리지를 벗어난 것인지, 아니면 완전히 접속이 종료된 것인지 판단하기 힘들기 때문에, 즉각적인 IMS 서비스 계층에서의 등록 해지를 지양하고 타임아웃 루틴에 의해 해결하고 있는 실정이다.

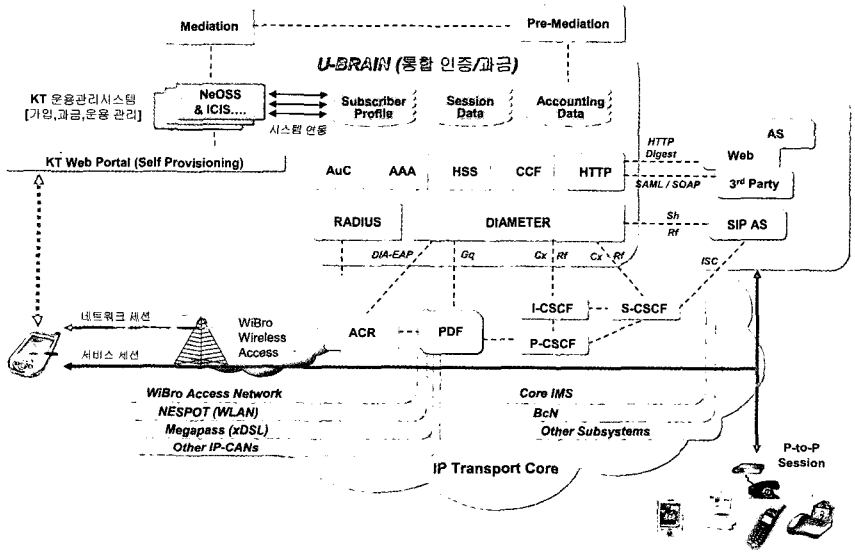
하지만 U-BRAIN에서 접속 계층의 제어를 담당하는 AAA 기능은 단말의 물리적인 연결 상태를 (특히 자신에 의해 상태가 변경된 경우) 정확히 판단할 수 있기 때문에 서비스 계층을 담당하는 HSS 블록으로 이에 대한 실시간적인 정보를 (단말의 물리적인 위치정보를 포함하여) 정확히 전달할 수 있으며, 또한 두 기능간의 연동을 통해 서비스 계층의 제어와 접속 계층의 제어를 유기적으로 연계하여 끊김 없고 낭비 없는 최적의 솔루션을 제공할 수 있다.

4. 접속 및 응용 서비스 통합 제어를 인증/과금 플랫폼 구조

U-BRAIN은 접속, 서비스 통합 가입자 프로파일을 기반으로 다양한 접속 인증 방식과 서비스 인증 방식을 제공한다(그림 6). 기본 인증 프로토콜로서 RADIUS와 DIAMETER를 지원하며, PAP, CHAP 및 EAP-AKA, EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PSK 등 다양한 EAP method를 통한 접속 인증과, DIAMETER-SIP 응용모듈을 통한 IMS 기반 인증 및 HTTP-Digest 방식을 이용한 서비스 인증을 수행한다. 또한 SAML(Secure Assertion Markup Language)/SOAP(Simple Object Access Protocol) 또는 HTTP-Digest 프레임워크를 이용하여, 접속 인증 결과와 다양한 서비스 인증을 연계하여 수행하는 SSO 기능을 제공한다.

한편 U-BRAIN은 UICC 기반의 다양한 접속 및 서비스 인증을 지원하는데, 이를 위하여 U-BRAIN 내의 AuC (Authentication Center) 블록은 USIM, WSIM, ISIM (IP multimedia Services Identity Module) 등 UICC 내 다양한 접속/서비스 인증 응용모듈을 지원할 수 있도록, 인증벡터 (AV; Authentication Vector)를 필요로 하는 AAA와 HSS 블록에 요청된 개수만큼의 인증벡터를 생성하여 전달하는 단일화된 생성 알고리즘과 인터페이스를 제공한다.

네트워크 접속인증 관련하여, 현존하는 대부분의 표준 접속 인증 방식을 지원함으로써 통합된 가입자



(그림 6) 접속 및 서비스 인증, 과금을 위한 통합 플랫폼 구조

프로파일을 기반으로 Megapass, NESPOT, WiBro 등 어떠한 접속망으로부터의 인증 요청도 수행이 가능하며, 이를 기반으로 추후 이기종 네트워크 간의 Seamless 이동성 제공시 접속 계층에서의 제어 기능을 담당할 수 있다.

또한 SIP, 웹 서비스 등을 위한 HTTP Digest (MD5, Digest-AKA)와 SAML/SOAP 등 표준화된 서비스 인증 및 다양한 KT 내 비표준 인증방식을 지원함으로써 KT 내 서비스는 물론, 3rd party 사업자와의 제휴를 통하여 KT 접속 서비스 가입자에게 네트워크 접속만으로 별도의 로그인 없이 제휴 웹사이트와 서비스를 이용할 수 있는 SSO 기능을 제공한다.

IV. 결 론

와이브로는 현재의 초고속 인터넷 서비스가 유선에서 무선으로 옮겨가고, 언제 어디서나 네트워크에 접속할 수 있는 유비쿼터스 환경을 창출하기 위한 핵심 기술로서 주목받고 있다. 한편 KT의 유무선 통합 인증/과금 플랫폼인 U-BRAIN은 멀티 서비스 환경과 IP 서비스의 확장에 따른 IP 네트워크 관리 도메인의 지능화 요구에 대비한 IP 기반 코어 플랫폼이다. 또한 U-BRAIN은 통합 프로파일을 기반으로 접속 서비스의 고 기능화 및 다양화를 지원하고, IP 기반 서비스 프로비저닝과 제공을 위한 백엔드 시스템 통합을 주 목적으로 하며, 다양한 접속 상품간 연계 및 결합도 강화를 통한 경쟁력 제고를 염두에 두고 있다. 이를 위한 가장 강력한 수단은 KT의 모든 가입자 프로파일에 의거한 네트워크와 서비스에 대한 제어권을 확보하는 것이며, 단순한 접속 연결에서 벗어나 네트워크 접속과 서비스 연계를 통한 서비스 이용 통제에 기반한 다양한 BM 구현의 기반구조를 제공하는 것이다. 이러한 기반은 컨버전스 환경에 적합한 개방형 연동 체계 구축을 추구하며, IP 이동성을 기반으

로 한 All-IP 환경에 적합한 인증-위치-접속 제어 기능을 제공한다.

이러한 사상으로 설계된 U-BRAIN은 일차적으로 KT 와이브로 상용서비스에 적용되어, 카드 한 장에 접속 가입자의 정보 이외에 다양한 뱅킹, 결제 기능을 수행하는 정보를 탑재하여 고객의 편의를 증대할 수 있는 인증 수단인 UICC 기반의 다양한 접속 및 서비스 인증을 지원하고, 다양한 응용서비스 연동이 가능한 SSO 기능을 제공한다.

추후에는 기존의 메가패스, 네스팟 및 다른 IP 기반 신규 서비스로 확대 적용함으로써, 접속망에 관계없이 고객에게 단일화된, 끊김 없는 IP 기반의 접속/응용 서비스를 제공할 수 있는, 명실상부한 All-IP 기반 유무선 통합 네트워크에서의 Brain 역할을 하게 될 예정이다.

[참 고 문 헌]

[1] 3GPP TS 23.228 V6.12.0, "IP Multimedia Subsystem (IMS); Stage 2", (2005-12)

[2] 3GPP TS 23.207 V6.6.0, "End-to-end Quality of Service (QoS) concept and architecture", (2005-09)

[3] DES/TISPAN-02007-eNGN "Overall TISPAN NGN R1 Architecture"

[4] ITU-T FGNGN-FRA Version 7.1 (FGNGN-OD-00244R2)

[5] 3GPP TS 33.102 V6.3.0, "3G Security; Security architecture", (2004-12)

[6] RFC 4187, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", (2006-01)

[7] IEEE Std 802.16e-2005, "Air Interface for Fixed and Mobile Broadband Wireless Access Systems", (2005-12)

[8] RFC 3588, "Diameter Base Protocol", (2003)

[9] RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication", (1999)

[10] RFC 3310, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", (2002)

[11] 3GPP TS 29.229 V6.7.0, "Cx and Dx interfaces based on the Diameter protocol; Protocol details", (2005-12)

[12] 3GPP TS 29.329 V6.6.0, "Sh interface based on the Diameter protocol; Protocol details", (2005-09)

[13] 3GPP TS 32.240 V6.3.0, "Charging management; Charging architecture and principles", (2005-09)

정한욱

1982년 경북대학교 전기전자공학과 학사
1984년 경북대학교 전기전자공학과 석사
1996년 뉴욕주립대 전기전산공학과 박사
1985년 ~ 현재 KT 컨버전스본부
관심분야 : 무선통신기술, 유무선통합서비스

방정희

1991년 경희대학교 컴퓨터 공학과 학사
1993년 경희대학교 컴퓨터 공학과 석사
1999년 경희대학교 컴퓨터 공학과 박사
1993년 ~ 현재 KT 컨버전스본부
관심분야 : 유무선통합서비스, 유무선 통합 인증/
과금 기술, 휴대인터넷 인증/보안 기술

이덕기

1998년 서울대학교 전기.컴퓨터공학부 학사
2000년 서울대학교 전기.컴퓨터공학부 석사
2005년 서울대학교 전기.컴퓨터공학부 박사
2005년 ~ 현재 KT 컨버전스본부
관심분야 : 유무선통합서비스, 인증/보안기술