주 제

Interworking Security for Public WLAN, WiBro and WCDMA : Mobile and wireless systems

ETRI 전성익, 김영세, 한진희, 정교일, 손승원

차 례

요 약

3G/PWLAN/WiBro 무선 네트워크 연동에 있어서 보안 기술이 통신 서비스의 고속화 시도 만큼이나 매우 중요한 사항으로 부각되고 있다 . 그리고 무선 네트워크는 본질적으로 유선 네트워크에 비해 취약한 점이 많기 때문에 이종의 네트워크 연동을 실현함에 있어서 무선 네트워크의 편의성을 살리면서 연동 보안 문제를 해결해야 한다. 본 기고에서는 이러한 무선 네트워크에서의 연동 보안 기술에 대한 현주소를 살펴보고 미래의 발전 방향에 대한 고려 사항 및 요구 사항을 정리하고, WCDMA, WiBro, PWLAN 등의 연동 통합 구조를 제시하고 제시된 연동 네트워크 상에서의 인증, 키 교환 및 데이터 암호화 등을 가능하게 하는 연동 보안 기술을 심도 있게 살펴 보고자 한다. 또한 본고에서는 3G/PWLAN/WiBro 무선 네트워크 연동에서 개별 네트워크는 최소 수정하면서 인증/과금/로밍 수단을 제공하는 새로운 방안을 제안하고 구현하여 보이고자 한다.

I. 서 론

무선 통신 기술의 발전으로 다양한 멀티 미디어 서비스가 가능한 초고속 무선 네트워크 시대가 현실로 다가왔고 사용자는 시간과 장소에 구애 받지 않고 언제든지 자신의 모바일 단말기를 통해 무선 인터넷 서비스를 마음껏 즐길 수 있게 되었다.

PWLAN, 2G(CDMA), 3G(WCDMA), WiBro(휴대 인터넷) 등의 다양한 무선 네트워크 서비스들은 각각의 특성과 장점을 가지고 무선 서비스 시장을 개척하고 있으며, 개별적으로 무선 인터넷 서비스 및

음성 통화 서비스를 제공하는 무선 네트워크 구축 방법을 보유하고 있다.

공중망 무선랜은 11 ~ 54Mbps 통신 속도를 제공하며 네트워크 구축 비용이 cellular 네트워크 에 비해 매우 저렴하기 때문에 hot spot 형태로 이동 인구 밀집 지형을 중심으로 급속도로 확산되고 있으며, cellular 네트워크 기반 2G, 3G 기술은 144Kbps ~ 2Mbps 통신 속도를 제공하지만, 네트워크 구축 비용이 많이 들기 때문에 광역 서비스가 가능한 장점이 있음에도 불구하고 이용자와 사업자의 기대를 충족시키지 못해 더 이상 확장되지 못하고 포화 상태에 머무르고 있다. WiBro는 2.3 GHz 대역의 주파수를 이용하며, 시속 60km 이상의 이동성과 30~50 Mbps급의 전송 속도를 제공함으로써 2G, 3G에 비해 저렴한 요금과 PWLAN이 제공해주지 못하는 이동성을 겸비한 새로운 무선 네트워크 서비스로 주목받고 있는 휴대 인터넷 서비스로 KT와 SK Telecom은 각각 내년 상반기 상용화를 목표로 준비 중에 있다. 참고로, 이동 통신 사업자는 광역 커버리지를 갖는 서비스에 대하여는 cellular 망을, 도심 지역과 같은 곳에서 초고속 인터넷 서비스를 받고자 하는 경우에는 통신 속도 및 통신 대역폭이 상대적 으로 높은 PWLAN/WiBro를 추천한다. 즉, 개별 무선 네트워크가 지니는 특징들은 향후 다양한 무선 네트워크 기술들이 연동 혹은 통합됨으로써 상호 보완적인 서비스로 발전할 수 있는 발판을 제공해주며, 이종 무선 네트워크간 연동이 활발하게 이루어질 경우, 사용자들은 상이한 무선 네트워크간 로밍 서비스는 물론 저렴한 가격으로 질 좋은 무선 인터넷 서비스를 언제, 어디서나 마음껏 사용할 수 있게 될 것이다.

이종 무선 네트워크 연동을 위해 인증/과금/ 로밍 서비스를 위한 상호 협약 체결, seamless한 음성, 데이터, 멀티미디어 서비스, QoS(Quality of Service), mobility 등 여러 가지 고려사항이 존재할 수 있지만 무엇보다 가장 중요한 것은 연동 보안 기술이라 할 수 있을 것이다.

일반적으로 무선 네트워크들은 무선 구간의 도청 및 가입자의 위장이 용이한 점으로 인해 유선 네트워크에 비해 보안 위협 요소를 많이 내재하고 있기 때문에 그러한 보안 취약 요소들을 해결하기 위한 방안으로 사용자와 망간의 양방향 상호 인증을 통한 강화된 인증 방식(strong authentication), 유/무선 구간을 포함한 보다 안전한 프로토콜을 이용한 키 관리 기법, 그리고 향상된 데이터의 기밀성 및 무결성을 제공하기 위한 비도 높은 암호화 기술 등을 이용한다.

이에 본 기고에서는 먼저 II장에서 무선 네트워크가 지니고 있는 보안 취약성 및 무선 네트워크간 연동 시 고려해야 할 다양한 보안 요구 사항과 관련 문제점 들을 소개하고 III장에서는 W-CDMA, WiBro, WLAN 연동 통합 구조를, IV장에서는 W-CDMA, WiBro, WLAN 각 네트워크에서 사용하고 있는 정보보호 요소들과 연동 구조에서 고려해야 할 다양한 연동 보안 기술들에 대해 자세히 언급할 것이다. 이후, V장에서는 연동 시스템 및 연동 보안 메커니즘의 일환으로 USIM을 활용한 단일 인증 연동 시나리오, USIM기반 WLAN, WiBro 인증 절차에 대해 구체적인 예를 제시하고 VI장에서 보안 기술과 관련된 국내외 연구 현황 및 표준화 동향에 대해서 상세히 기술한 후, 마지막으로 VIII장에서 간략한 결론과 함께 향후 과제를 언급하고자 한다.

II. 3G/PWLAN/WiBro interworking을 위한 보안 요구 사항 및 문제점들

1. 무선 네트워크 보안 위협 및 위험 분석

가. 보안 위협 및 위험 분석

보안 위협 분류방법으로 공격 포인터, 공격 방법, 보안 위협 성격[1] 등을 적용해보자. 우선 공격 포인터를 기준으로 분류하면 첫번째 공격 지점은 무선 단말 구간, 두번째 지점은 무선 구간(radio interface), 세번째 지점은 네트워크 내의 시스템 혹은 장치들이 위치한 구간이다. 이들 중 특히 세번째 지점인 폐쇄망에서는 내부자의 도움없이 공격하는 것이 불가능하다[2].

두번째로, 공격 방법에 따른 분류를 살펴보면 유선망에서 사용되는 passive attack, active attack, replay attack, man-in-the-middle attack, DoS (Denial of Service)공격, DDoS (Distributed Dos) 공격, 무선 구간 트래픽 도청, 링크 레벨 sniffing 등과 같은 공격 기법이 무선 네트워크에서도 적용되고 있으며, 유선 망에 비해 공격이 용이한점을 이용하여 다양하고 새로운 공격 기법들이 출현하고 있어 보안 위협이 더욱 증대 하고 있는 실정이다.

〈표 1〉 무선 네트워크의 보안 위협 분석

Basic Threats	Confidentiality Violation	Integrity Violation	Denial of Services	Illegitimate Uses	Repudiation
Enabling Threats	Eavesdropping User Traffic	Alternation User Traffic	Physical Intervention	Masquerading User	Charging Repudiation
	Eavesdropping Signal & Control	Alteration Signal & Control	Protocol Intervention	Masquerading Service Net	Traffic Origin Repudiation
	Masquerading User & Net Elements	Alternation ME Download	Masquerading Net Elements	Masquerading Home Environment	Traffic Delivery Repudiation
	Passive Traffic Analysis	Alteration USIM Download	Privilege Misuse	Privilege Misuse User	
	[illegible]	Alternation System Data	Service Abuse	Privilege Misuse Service Net	
	Active Traffic Analysis	Masquerading Net Elements		Stealing Terminals	
	Information Leakage User Location	Masquerading Download Origins			
			Relevant Threats	Significant Threats	Major Threats

〈표 1〉과 같이 무선 네트워크의 보안 위협요소를 위협성격에 따라 기밀성 위반, 무결성 위반, 네트워크 서비스의 교란 및 악용, 비 인가자의 서비스 접근, 부인 봉쇄로 분류해볼 수 있는데, 비 인가자가 도청, 위장 공격, 통신 트래픽 분석, 기밀 누설 등을 이용하여 기밀 데이터에 접근하는 것을 기밀성 위반이라 하며, 보호 받아야 하는 민감 데이터들을 허가 없이 조작하는 것으로 메시지의 삭제, 수정, 부정 추가, 재전송 공격 등은 무결성 위반 범주에 포함된다. 또한, 네트워크 서비스의 교란 및 악용 위반에는 DoS 공격과 서비스 가용성 저해, 물리적인 간섭, 통신로 절단, jamming등으로 공격하거나 통신 참여자로 위장하는 경우가 해당되며, 허가된 이용자로 위장하거나 데이터 불법 복제 등의 행위는 비 인가자의 서비스 접근 위반에 속한다.

〈표 2〉는 무선 네트워크에서 공통적으로 나타나는 보안 위협 요소들을 보안 위협 유형, 확률, 영향, 위험도에 따라 분류하여 보여주고 있는데, 비 인가자에 의한 데이터 접근, 서비스 이용 위장, 사용자 혹은 네트워크 요소 위장 등의 보안 위협 유형들이 높은 위험도를 지니고 있으며, 서비스 거부 및 도청은 영향은 높지만 확률이 낮기 때문에 위험도는 중간 정도로 평가되고 있음을 볼 수 있다. 따라서, 무선 네트워크 사업자들은 〈표 1〉과 〈표 2〉에 명시된 보안 위협 요소와 각 보안 위협 요소가 지니고 있는 확률, 영향, 위험도를 토대로 대응 방안을 만들고, 그에 적합한 보안 요구 사항을 수립해야 한다[1].

〈표 2〉 보안 위협의 분석

위협 유형	확 률	영 향	위 험 도
Unauthorized access to data/service	Med	High	High
Unauthorized user gains access to USIM, network, systems	Med	High	High
위장	Med	High	High
정보의 무결성 위협	Low	High	Med
서비스 거부 위협	Low	High	Med
도청	Low	Med	Med

2. 이종 무선 네트워크 연동 시 고려해야 할 보안 문제점들

이 절에서는 이종 무선 네트워크 연동 시 고려해야

할 공통적인 보안 요구사항 및 무선 네트워크 종류에 무관한 공통적인 보안 문제점을 소개 한다.

가. 사용자 신원 보호 및 프라이버시 보호

3G에서는 가입자의 전화 번호나 IP 주소 식별 번호를 가로채어 위장 하거나 무선 구간을 도청하여 사생활 정보를 부당하게 침해 받지 않도록 하기 위하여 MSISDN(telephone number 16 digits)과 구분하여 IMSI(International Mobile Subscriber Identity)를 사용하고 있고, IETF에서는 NAI(Network Access Identifier)내에 username으로 IMSI를 사용하는 것을 권고하고 있다. 하지만, 무선 구간에서 평문으로 IMSI를 전송할 경우 공격자가 쉽게 무선구간을 도청하여 사용자의 개인 정보를 가로챌 수 있기 때문에 3G에서는 사용자의 IMSI를 암호화한 TMSI를, WLAN에서는 인증 서버에서 IMSI 대신 사용할 수 있는 pseudonym을 생성하여 사용자의 단말에 전달해주는 방법을 제공한다. 3G/WLAN 연동 시 기지국에서 할당 및 변환하는 TMSI값은 WLAN AN(Access Network)상에서 공격자에게 노출 되거나 취득 될 수 없도록 보호해야 하며, 단말에 저장된 사용자의 개인 정보는 외부에서 부당하게 취득할 수 없도록 안전하게 관리되어야 한다.

나. 시그널링 및 사용자 데이터 보호

일례로, 3G/WLAN/WiBro 통합 연동 네트워크를 구축하고자 할 경우, cellular 네트워크에서 제공하는 수준의 트래픽 보호를 연동 네트워크의 모든 구간에 적용해야 한다. 만일 어느 한 곳이 다른 곳보다 트래픽 보호 수준이 낮게 적용된다면 연동 네트워크의 정보보호 수준은 가장 낮은 수준과 같아지게 된다.

다. 링크 계층 보안

3G/WLAN 연동 시 3G 핵심 네트워크는 WLAN AN을 black-box(Wa interface)로 취급한다고 하지만 AN에서 사용할 키 값들을 어떻게 안전하게 전달하고 사용할 것인가에 대한 링크 계층 보안은 IP 계층과 session 보호를 위해 매우 중요하다. 아울러 핵심 네트워크 내의 AAA 서버로부터 WLAN UE(User Equipment) 혹은 WLAN AP(Access Point)까지 안전하게 키를 배포하기 위한 키 관리 방법 및 키 관리 프로토콜의 사용도 권장된다.

라. WLAN-UE상의 보안

1) USIM(UMTS Subscriber Identity Module)을 내장할 수 있는 Dual-mode/Triple-mode 휴대 단말에 WLAN을 통합하는 경우엔 2G/3G 휴대 전화가 제공해주는 USIM interface및 security를 보장받을 수 있다. 특히, EAP(Extensible Authentication Protocol) 인증 프로토콜을 사용할 경우 EAP-AKA(Authentication and Key Agreement)/SIM을 단말이 아닌 USIM 상에서 종단하면 보다 안전하게 사용자의 개인 정보를 관리할 수 있다.
2) USIM을 리더 기능이 포함된 PCMCIA/USB/CF/ SD card를 이용하여 외장형으로 WLAN 지원 단말에 정합하는 경우엔 3G와 WLAN에서 동시에 USIM을 사용할 수 없을 뿐만 아니라 3G 단말에서 USIM을 제거한 후 WLAN 장치에 새로 추가하여 사용해야 하는 불편과 분실의 위험이 증대하는 단점이 존재한다. 이 경우, USIM을 포함하고 있는 PCMCIA/USB/CF/SD card와 WLAN 단말간에 local security가 보장되어야 한다.
3) WLAN/Bluetooth 기능을 내장한 단말과 3G/Bluetooth 및 USIM을 내장한 단말을 이용할 경우, local interface가 상당히 복잡해지기 때문에 보안 취약 구간에 각별히 신경을 써야 한다.

마. 사용자 단말에서의 보안 정책 적용

연동 네트워크에서 인증에 앞서 인증 서버와 사용자 단말간에 인증 알고리즘, 보안 프로토콜, EAP method 등을 선택하는 일련의 과정은 보안 정책에 의해서 결정된다. 연동 시 네트워크 공유 혹은 선택 등을 가입자 프로파일에 기반하여 자동으로 한다고 하면 이 또한 보안 정책 서버와 관련 지어 고려하여야 할 것이다.

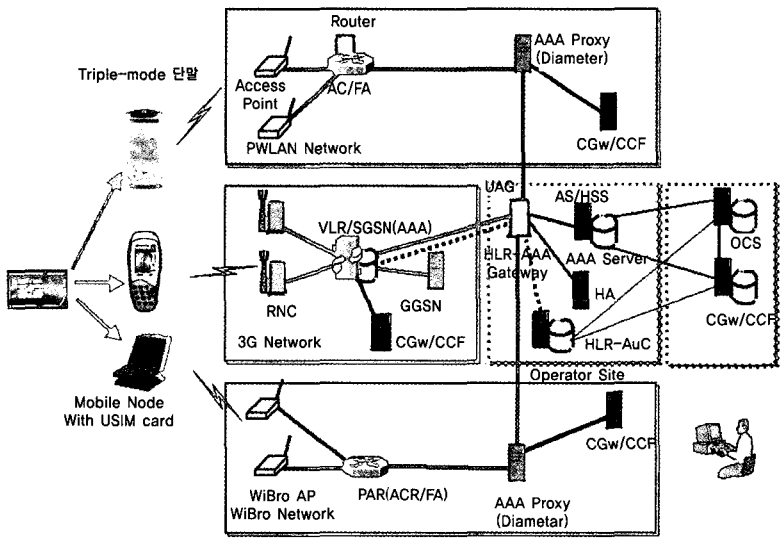
III. 무선 네트워크 통합 구조

1. 3G/PWLAN/WiBro 상호 연동 구조

3GPP는 3세대 WCDMA 네트워크와 PWLAN을 연동하는 방안으로 3G 핵심 망에 PWLAN을 AN의 일부로 수용하는 구조를 제시하고, 그에 따른 참조 모델 및 연동 시나리오 표준을 제정하고 있다[2][3][4][5][6]. 이는 향후 BcN(Broadband converg-ence Network) 연동의 표준 참조 모델이 될 것으로 예상되며 현재 각 국가별 이동 사업자들은 3GPP의 IMS(IP Multimedia Subsystem) R5~R7에 기반하여 통합 망을 계획 중에 있다.

(그림 1)은 3GPP에서 제안하는 3G/WLAN 연동 참조 모델에 바탕을 둔 3G/PWLAN/WiBro 연동 구조를 보여준다. (그림 1)에 나타낸 연동 구조는 인증/과금/로밍을 위해 UAG(USIM Access Gateway)를 채용하고 있는데, UAG는 개별 네트워크가 지니는 이질적인 부분을 통합 혹은 변환하여 IP 서비스 및 로밍 서비스를 지원하는 기능을 제공한다.

3G AAA proxy는 접근제어신호와 계정정보를 홈 3G AAA 서버에 전달하는 역할을 수행하며[4][5][7], WLAN/WiBro 사용자는 3G 인증이 완료된 후, 인터넷 서비스 혹은 3G/ WLAN/WiBro간 통신을 이용할



(그림 1) 3G/PWLAN/WiBro 연동 구조

수 있게 된다[3].

휴대 단말과 무선 접합 구간 인터페이스는 다양한 단말을 지원할 수 있도록 설계하고, 네트워크 서비스 제공자 측은 일관성을 유지하면서 보안 취약구간이 발생하지 않도록 연동 시스템을 구축해야 한다. (그림 1)에서 제안한 연동구조는 AAA 서버를 중심으로 통합된 generic 구조이며 Mobile IP 등을 통합하기 용이하도록 AAA proxy에 DIAMETER 프로토콜을 적용하고 있다.

IV. 무선 네트워크들에서의 정보보호

1. WCDMA에서의 정보보호

가. WCDMA 액세스 보안 구조

3GPP TS 33.102~205 표준 문서는 WCDMA 네트워크의 정보보호 구조 및 정보보호 수단에 대하여 정의하고 있다[7].

WCDMA 네트워크는 다음과 같이 크게 4가지 영역에 대하여 구체적인 정보보호 수단을 고려하고 있다. 우선, 사용자 영역 보안은 사용자와 USIM 간에 본인 확인 수단으로 PIN을 사용하여 USIM의 주인이 아니면 그 다음 동작은 모두 불가능하게 하는 방안을 적용하며 본인 및 서비스 제공 권한자만이 주어진 조건 하에서 USIM을 엄격히 관리한다. 그리고 본인 확인이 된 USIM과 단말기 링크 간에도 USIM 접근 권한을 취득한 단말기만이 USIM을 이용하도록 제한한다. 다음으로, USIM-ME-RNC-SN-HE 간의 네트워크 접근 보안 영역을 살펴보면 사용자 신원 기밀성을 통하여 사용자 위치 기밀성과 추적 방지를 제공하고 휴대 단말과 네트워크 간에 상호 인증을 통하여 사용자/장치/네트워크의 인증을 수행함으로써 위장 사용자 및 위장 네트워크를 방지한다. 또한, 무선 구간에 대한 데이터 보호 및 시그널링 보호와 데이터 무결성을 보장하기 위하여 암호 키 생성 및 일치성 검증을 제공하고 서비스 공급자 영역의 데이터 및 네트워크 요소 보호, 응용 영역에서의 안전성 부분에 대해 정의한다.

(그림 2)는 USIM과 HLR(Home Location Register)/AuC(Authentication Center) 측에서 수행되는 인증 및 키 일치성 메커니즘에 대한 전체 운용 과정을 내부적으로 수행되는 함수를 이용하여 설명한다[7].

각각의 함수에 대한 자세한 설명은 다음과 같다:

F0: 난수 생성 알고리즘

F1: 네트워크 인증 알고리즘

F1*: 재 동기를 위한 인증 알고리즘

F2: 사용자 인증 알고리즘

F3: 암호화 키 생성 알고리즘

F4, 무결성 키 생성 알고리즘

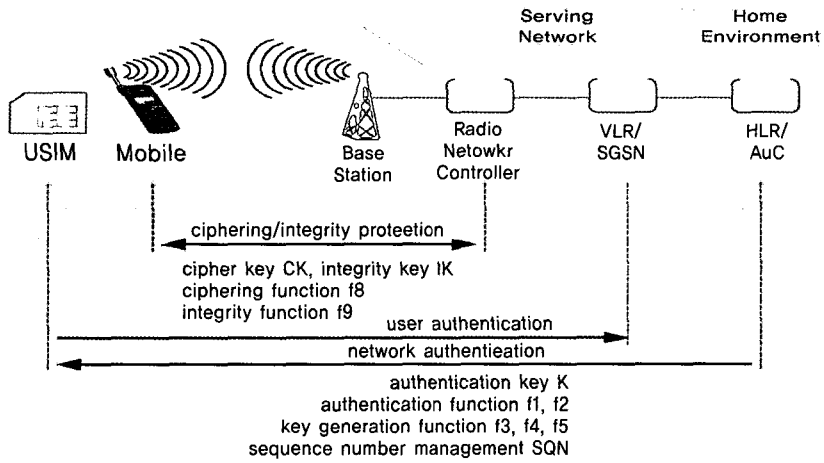
F5: 익명성 키 생성 알고리즘

F5*: 재 동기를 위한 익명성 키 생성 알고리즘

3G 인증 알고리즘은 위에 명시한 함수들의 결과값으로부터 비밀키 K를 유도 하는 것이 불가능하다는 조건을 전제로 한다. 또한, 3G 인증 알고리즘은 USIM 카드 내에서 수행되며, 인증 수행 시간은 500ms이내에 처리 될 수 있도록 설계 되어야 한다. 인증 센터(AuC)는 위의 함수들 외에 난수 생성기와 fresh sequence number를 생성하는 기능을, USIM은 인증 서버로부터 전달된 SQN 값을 검증 할 수 있는 기능을 제공하며, 키 생성 알고리즘의 핵심 커널 함수로는 AES(Advanced Encryption Standard) 알고리즘이 사용된다. 참고로, 글로벌 로밍을 위해서는 커널 함수를 일치 시킬 필요가 있다.

나. UEA(암호화)

무선 구간의 트래픽을 보호 하기 위하여 f8



(그림 2) WCDMA 정보보호 구조

(cipher) 알고리즘을 사용하며 UE와 RNC에서 암/복호를 수행한다.

다. UIA(무결성)

무선 구간의 메시지 무결성을 보장하기 위하여 f9(Integrity) 알고리즘을 사용하여 MAC-I, XMAC - I를 생성하며 UE와 RNC에서 메시지 무결성 확인을 수행한다.

2. Public WLAN 에서의 정보보호

802.11 WLAN 의 보안 수단은 802.1X, 802.11i 표준에 맞추어 구현하고 있다. 무선 단말과 AP 및 인증 서버간의 인증 절차는 802.11 SA(Security Association)를 설정하는 단계와 802.1x, EAP 기반으로 인증을 수행하고 키 생성 및 배포를 수행하는 단계로 나뉘어있으며, 무선 구간의 트래픽 보호를 위해서는 RC4암호 알고리즘이 적용된 WEP(Wired *Equivalent Privacy*)을 주로 사용하며 WPA2(Wi-Fi Protected Access 2)에서는 AES알고리즘을 사용한다. 또한, AP는 Dual Port-based 접근 제어를 통해 비 인가자의 무선 구간 접근을 제어함으로써 무선 네트워크의 보안 취약 구간을 보호한다[14][15]. 〈표 4〉는 WLAN 보호를 위해 채용되고 있는 기술들을 비교 요약하여 정리한 내용을 보여준다.

〈표 3〉 WLAN security 비교

Security Feature	Wired Equivalent Privacy (WEP)	WiFi Protected Access (WPA)	Robust Security Networks (RSN)
Encryption Algorithm	RC4	RC4	AES
Key Management	None	EAP-based	EAP-based
Cryptographic Keysize	40-bit or 104-bit	128-bit (64-bit) authentication)	128-bit
Packet Key	Created by Concatenation	Created by mixing function	Not needed
Data/Header integrity	CRC-32 / None	Michael Algorithm	CCM
Cryptographic Key life	24-bit, wrap	48-bit	48-bit
Replay protection	None	Uses IV	Uses IV

3. WiBro Network에서의 정보보호

IEEE 802.16e 표준은 privacy sublayer를 MAC 계층에 정의 하고 있으며 PKM(Privacy Key Management) 모듈을 단말과 기지국에 각각 구현하

도록 정의 하고 있다[21]. WiBro 인증은 EAP 인증 프로토콜과 RSA 알고리즘을 이용하는 X.509 인증서에 기반한 2가지 방안이 모두 사용될 수 있는데 특히 EAP-method 중 EAP-TLS(Transport level security)가 일반적으로 많이 사용되어왔으며 최근에 EAP-AKA 혹은 EAP-SIM을 적용하는 방안이 검토되고 있다. 사용 권한 획득 및 인증 키 교환에 대한 상세한 내용은 표준문서에서 언급되고 있지만 무선 단말과 인증서버간의 프로토콜은 특별히 정의하지 않는다. IEEE 802.16e 표준은 AK(Authorization Key)로부터 추출되는 키 값들을 배포하고 교환하기 위해 T-DES, AES(ECB mode), RSA 알고리즘을 사용하고(TEK 암호화), 무선 구간의 사용자 트래픽 및 시그널링 보호를 위해 DES (CBC mode), AES(CCM mode, CRT mode) 알고리즘을 사용하도록 권고 하고 있다[21][22].

4. 3G/WLAN/WiBro 상호 연동 정보보호

가. 3G/WLAN/Wibro 연동을 위한 보안 요구사항

3GPP TS 33.234 표준 문서에서는 WLAN과 3GPP 연동 환경에서 아래와 같은 보안 요소들이 제공되어야 한다고 정의하고 있다[2].

1) 가입자와 망간 상호 인증 및 SA(Security Association) 관리

3GPP/WLAN/WiBro 연동을 위한 인증 시그널링은 RFC 3748에 명시된 EAP에 기반해야 한다. Multi-vendor간의 호환성을 보장하기 위해 WLAN 무선 인터페이스 상의 액세스 시그널링은 IEEE 802.11i 표준을 따라야 한다. WLAN 액세스 네트워크와 3GPP AAA proxy 서버간의 WLAN 액세스 인증 시그널링은 Diameter 또는 RADIUS 프로토콜에 기반한다.

영구적인 가입자 식별 정보를 평문으로 전송함으로써 발생될 수 있는 문제점을 방지하기 위해 사용자 identity privacy(anonymity) 기능을 제공해야 한다. 이 기능은 네트워크와 WLAN UE에 반드시 구현되어야 하지만, 기능의 사용에 있어서는 WLAN UE에게만 필수사항으로 고려된다. 임시 ID 또는 pseudonym은 AAA서버가 생성하여 인증과정 중에 WLAN UE에게 분배한다.

WLAN 802.1x/AAA 재 인증은 WLAN UE와 AAA 서버상에서 수행되고, 3GPP AAA 서버는 특정 이벤트나 타이머를 통해 주기적으로 802.1x/AAA 재 인증 과정을 시작할 수 있다. EAP-SIM 혹은 AKA 재 인증 과정은 full 인증 과정이 수행되는 네트워크와 WLAN UE 상에 모두 구현되어야 한다.

터널의 두 종단 UE와 PDG(Packet Data Gateway)는 터널이 설정될 때 상호인증과정을 수반해야 하며, 터널설정 과정 시 SA 협정을 거쳐 터널을 통해 전송되는 데이터를 위한 기밀성 및 무결성 보호를 제공해야 한다.

2) 기밀성 보호

WLAN/WIBro AN 링크 계층을 위해 요구되며, 홈 네트워크 AAA 서버의 경우 WLAN AN에게 암호화 절차를 위한 입력 값으로 key material을 전송할 수 있어야 한다(시나리오 2). 그리고 UE와 PDG간에 설정된 터널을 통해 전송되는 IP 패킷의 기밀성을 보호할 수 있어야 한다(시나리오 3).

3) 무결성 보호

WLAN AN 링크 계층을 위해 요구되며, 홈 네트워크 AAA 서버의 경우 WLAN AN에게 무결성 보호 메커니즘의 입력 값으로 key material을 전송할 수 있어야 한다(시나리오 2). 그리고 UE와 PDG간에 설정된 터널을 통해 전송되는 IP 패킷의 무결성을 보호할 수 있어야 한다(시나리오 3).

4) WLAN UE 기능 분할

WLAN UE는 WLAN TE(Terminal Equipment)와 UICC(USIM IC Card) 또는 SIM카드를 장착한 MT(Mobile Terminal)와 같이 하나 이상의 장치로 구성될 수 있다. WLAN TE는 WLAN 접속 기능을 제공하고, MT나 UICC, SIM 카드는 EAP termination을 위해 키 도출 및 사용자 신분 관리 기능을 수행하는 인증 알고리즘을 구현할 수 있다. EAP 종단점은 항상 USIM이 장착되는 MT가 될 것이며, 인증 절차가 MT에서 종료될 때 결과적으로 파생되는 키 값들은 WLAN 접속 시 링크 계층 보호를 위해 사용될 수 있도록 WLAN TE에 안전하게 전송되어야 한다.

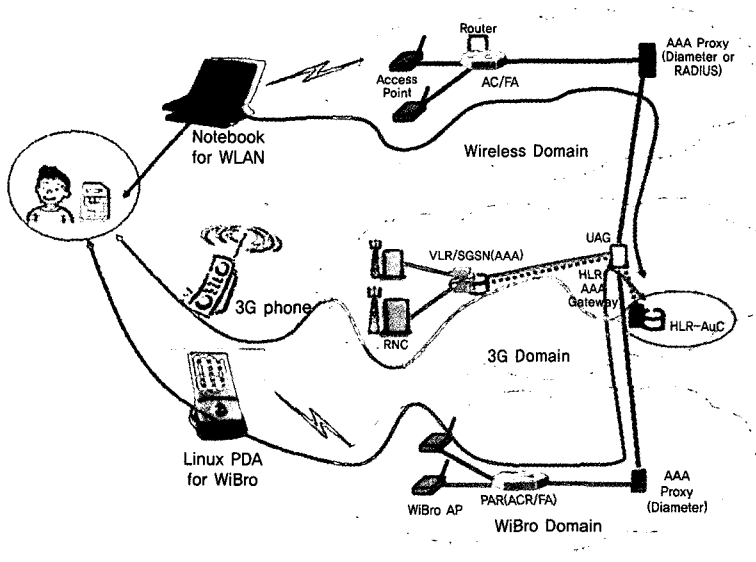
V. 연동 시스템 및 보안 메커니즘 구현

1. 연동 시스템의 설명

가. 연동 시나리오

(그림 1)의 연동 구조를 검증하기 위하여 그림3과 같이 연동 시나리오를 구성하였다. (그림 3)에서 보여주는 연동 시나리오는 인증 및 과금 통합 검증, 무선 및 유선 보호 구간의 확장, 사용자 데이터 트래픽의 터널링 기법 적용이 용이한 구조로써 WLAN과 WiBro 모두에 적용 가능하다.

(그림 3)의 연동 시나리오 구성요소는 USIM, 다양한 휴대 단말, 무선 기지국, 기타 네트워크 요소, 연동을 위한 UAG, 인증서버 등으로 볼 수 있으며, USIM을 공중망 무선랜 및 WiBro에도 적용할 수 있도록 확장하고, WCDMA의 정보보호를 위해 권고하는 AKA 방식을 3G/PWLAN/WiBro 무선 네트워크에 동일하게 적용하는 것을 주 목적으로 한다. (그림 1)에 나타낸 WLAN/WiBro AAA 인증 서버에 EAP-AKA 모듈을 추가하고 USIM 카드 상에 3G 인증용 AKA와 WLAN/WiBro용 EAP-AKA를 추가하고, 네



(그림 3) 3G/PWLAN/WiBro 네트워크 연동 시나리오

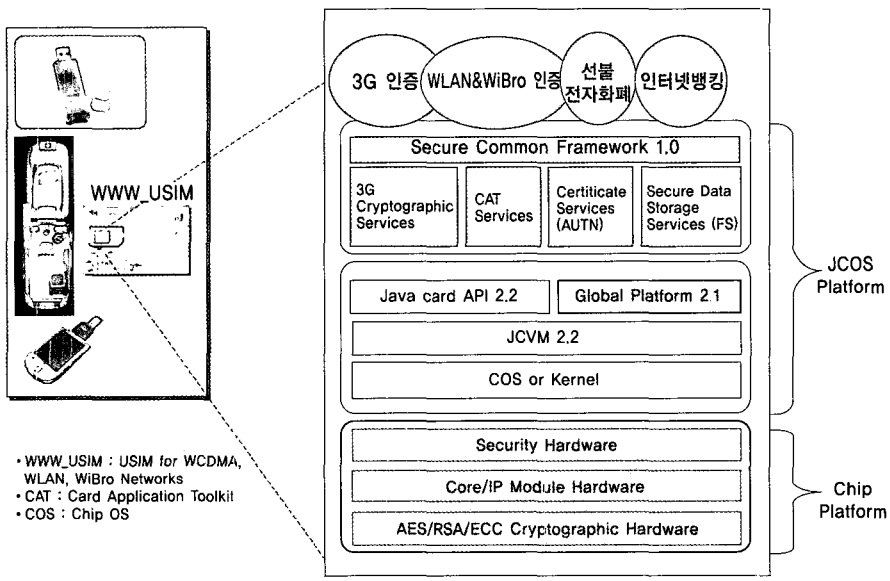
트워크 접속 지점과 AAA 서버간에는 DIAMETER 혹은 RADIUS 프로토콜을 통해EAP 패킷을 송/수신하여 인증 정보 및 사용자 프로파일과 과금 정보를 안전하게 전달한다. EAP-AKA 인증 프로토콜은 다른 EAP-method와 달리 스마트 카드의 일종인 USIM 상에 인증서 및 키 값을 안전하게 저장하고 인증 알고리즘을 카드 내에서 수행하여 상호 인증을 제공해 주는 장점을 지니고 있다.

연동 시나리오상에 표시된 UAG는 프로토콜 및 데이터 포맷의 상이한 부분을 변환해주는 역할을 수행하며 AP, AAA, HLR, AuC 등에 추가되어야 할 기능을 최소화 시켜준다. 또한, 연동 네트워크의 사업자가 동일하거나 상이한 경우에도 사업자 별로 구축하고 있는 인증 서버에 쉽게 연결되어 확장될 수 있는 융통성을 지닌다.

연동 시나리오를 자세히 살펴보면 알 수 있듯이, USIM 내부에서 인증 알고리즘 및 키 관리, 사용자 개인 정보 관리 등의 모든 일이 수행되기 때문에 휴대 단말에 탑재되는 클라이언트 프로그램은 단지 사용자 본인 확인 및 무선 네트워크 접속을 위한 일부 기능만을 제공하면 된다. 즉, AP들과 클라이언트 프로그램간의 통신 구간이 한결 간편해지며 기존 방식에 비해 안전성도 높아지게 된다. 물론 여러 가지 방식의 EAP- method들과 공존 가능하게 하고자 할 경우에는 기존 휴대 단말 클라이언트에 USIM 정합기능을 추가해야 할 것이다. (그림 3)의 연동 시나리오는 상용 AP를 그대로 사용할 수 있기 때문에 망 구축을 위한 투자비를 절약할 수 있다.

나. WLAN-UE에 USIM 정합

(그림 4)는 3G/WLAN/WiBro 연동 보안 메커니즘의 한 형태로 사용할 수 있는 USB 혹은 SD-card형 USIM 리더기를 보여주고 있는데, 이러한 형태의 USIM 리더기는 모든 종류의 WLAN UE(휴대단말,



(그림 4) USIM 카드 구조 및 USIM 정합 모델

노트북, PDA)에 USIM을 간편하게 장착할 수 있는 정합기능을 제공해 준다.

2. Authentication & Privacy

3G/WLAN/WiBro 인증 단일화는 3G망 사용자가 이용하는 AKA 알고리즘을 3G/WLAN/WiBro 연동 망에서 재사용하여 활용할 수 있게 함으로써 연동 네트워크 인증 체계를 통일하자는데 목적을 둔다. 즉, IETF에서 제정중인 EAP-AKA 인증 프로토콜을 WLAN 및 WiBro에서 동일하게 적용할 수 있도록 확장함을 의미한다[7][9][10]. EAP-AKA 인증은 3G에서 사용하는 AKA인증에 EAP개념을 도입함으로써 사용자들이 단일인증을 통해 보다 편리하게 무선 네트워크를 사용할 수 있도록 도와주며 기존 방식에 비해 호환성 및 보안성을 강화시켜준다.

가. 인증을 위한 느슨한 결합 구조의 WLAN/WiBro 제어 평면 프로토콜 스택

(그림 5)는 USIM에 기반하여 네트워크를 연동하는 경우의 제어 평면 프로토콜 스택을 보여 주고 있다.

중간에 위치한 UAG는 DIAMETER 기반 AAA 서버 혹은 Proxy 역할을 담당하며, cellular 네트워크의 HLR과 No.7 시그널링을 활용하여 연결되어야 하기 때문에 이를 위한 프로토콜 변환 기능을 구비 하고 있다.

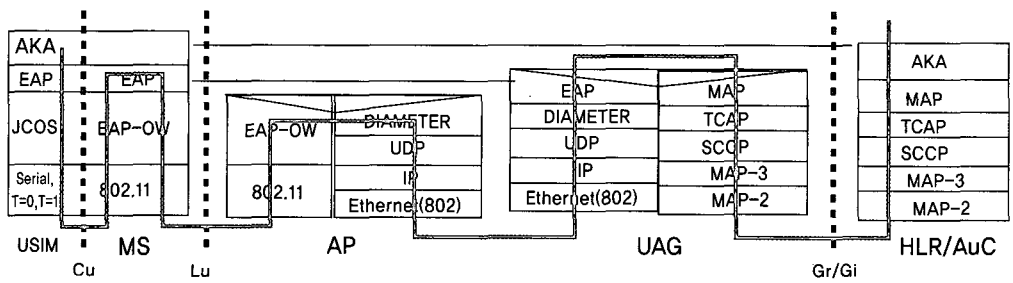
나. USIM 기반 WLAN 상의 상호 인증

1) USIM 기반 상호인증 및 EAP-AKA 인증 메커니즘 구현

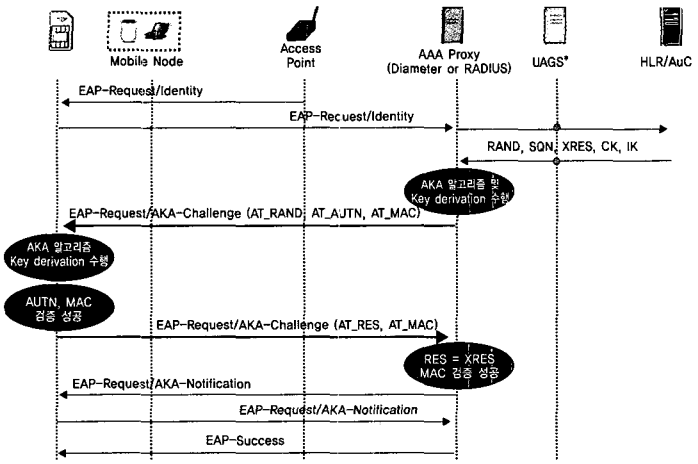
무선 네트워크와의 연동 시스템에 EAP-AKA를 사용하였을 때 단일 인증을 통해 이동통신 망 사용자가 WLAN에 접속하는 과정은 (그림 6)과 같다.

USIM카드를 이용한 EAP-AKA를 구현하기 위해 필요한 구성 요소는 AKA의 사용자인증을 위한 USIM카드, 사용자의 단말기(Client), Access Point, WLAN과 이동통신 망간의 연동은 AAA Proxy와 UAGS가 담당하고, EAP인증 및 사용자 인증을 위한 AAA 서버, 그리고 사용자 인증 데이터가 저장된 HLR 등으로 이루어 진다. 이동통신 가입자가 자신의 USIM카드와 단말기를 이용하여 WLAN을 통한 인터넷 접근을 하려 하였을 때 인증이 이루어지는 과정은 다음과 같다.

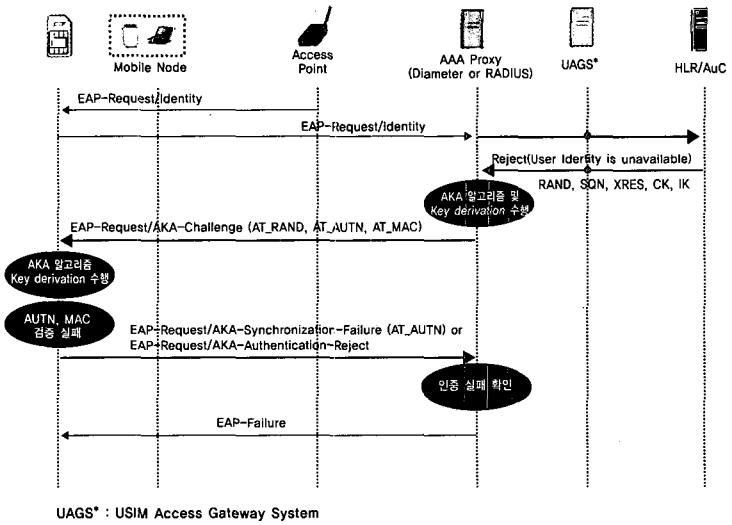
UAGS는 USIM에 저장 되어 있는 사용자의 identity(IMSI)를 EAP-Request/AKA-Identity를 통하여 요구한다. 단말기와 USIM카드는 자신의 identity를 EAP-Response/AKA-Identity에 실어 보



(그림 5) 3G-WLAN 연동 시 인증 관련 제어 평면 프로토콜 스택



(a) 인증이 성공하는 경우



(b) 인증이 실패하는 경우

(그림 6) (U)SIM Based Authentication Flow 및 USIM based authentication over WLAN

내고, 이는 AAA proxy와 UAGS를 거쳐 HLR에서 IMSI에 해당하는 인증 벡터를 추출할 수 있는 기본 벡터로 활용된다.

해당 인증 벡터는 다시 EAP-Request/AKA-Challenge를 통하여 AAA서버로부터 USIM카드에 전달되고, 카드는 메시지에 포함된 인증벡터와 자신이 저장하고 있는 비밀 데이터를 이용하여 AKA 알고리즘을 수행한다. USIM카드에서 수행된 AKA 알고리즘의 결과 값을 통해 검증 결과의 성공/실패 여부를 알 수 있으며, 일례로, 검증 결과가 성공적일 경우 USIM 카드는 결과 값(RES)을 AAA 서버에게 전달한다. 인증 관계의 마지막 단계로 AAA 서버는 수신된 RES값을 자신이 가지고 있는 값과 비교하여 사용자 인증을 수행한다[6]. 이러한 일련의 과정이 모두 성공적으로 수행될 경우에만 사용자는 비로소 WLAN을 접근할 수 있는 권한을 갖게 된다. 지금까지 설명한 USIM 기반 WLAN 인증 과정은 (그림 6)의 (a)에 자세히 나타나 있다.

EAP-Request/AKA-Identity 메시지를 통해 전달되는 사용자의 identity(IMSI) 값은 평문으로 전송할 경우에 발생될 수 있는 보안상의 문제점 때문에 사용자 identity 보호정책에 따라 인증 서버로부터 암호화된 형태(pseudonym)로 변경된 값을 전달받아 사용되어야 한다. 즉, 인증 서버는 사용자의 permanent identity와 매핑될 수 있는 pseudonym 을 안전하게 생성하고, 저장, 관리해야 할 책임을 갖고 있다.

(그림 6)의 (b)는 인증 실패의 경우를 보여주고 있는데, 인증 실패는 다음과 같은 세 가지 경우로 요약

해볼 수 있다.

1. 인증 서버에 등록되어 있지 않은 사용자 identity값을 수신한 경우
2. AKA 알고리즘 처리 시 sequence 값이 유효범위를 벗어난 경우
3. AKA 알고리즘 결과 값(mac)의 검증 실패

(그림 6)에서 보여주고 있는 full authentication과 달리 AKA 인증 메커니즘을 이용하지 않고 인증 서버와 USIM이 각각 관리하는 카운터 값을 이용하여 보다 신속하게 인증 과정을 처리해줄 수 있는 fast re-authentication 방법 역시 WLAN 인증에 사용될 수 있는데, 본 고에서는 fast re-authentication과 관련된 자세한 내용은 다루지 않을 것이다.

2) EAP-AKA 및 AKA 알고리즘과 키 생성 알고리즘

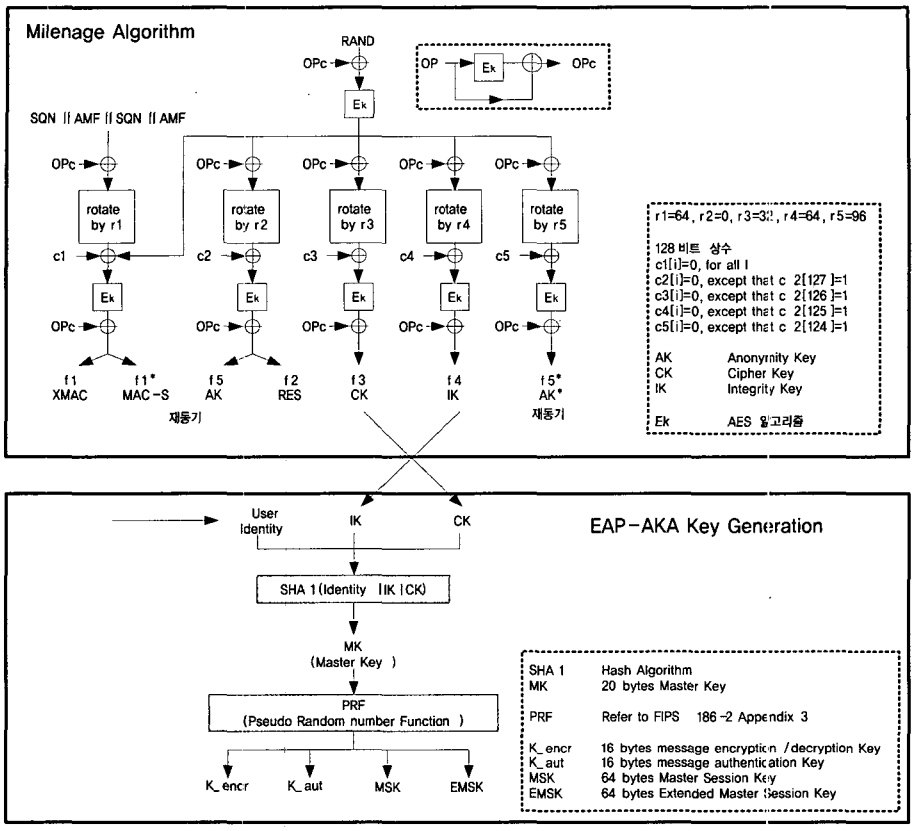
무선랜 인증에 사용되는 EAP-AKA 인증 프로토콜은 (그림 7)에서 보는 바와 같이 WCDMA에서 사용하는 AKA 인증 메커니즘의 결과값으로 얻어 지는 ciphering key(CK)와 integrity key(IK)값, 사용자의 identity 값을 SHA-1 함수의 입력 값으로 사용하여 20bytes의 master key (MK)를 생성하고, EAP-AKA 인증 프로토콜에서 정의한 PRF 함수와 MK를 이용하여 master session key (MSK), extended master session key(EMSK), encryption key(K_encr), integrity key(K_aut) 총 4가지의 키 값을 만들어낸다. MSK는 link layer 보호를 위해 사용되며, K_encr은 데이터 암호화, K_aut는 MAC 값 생성을 위해 HMAC-SHA1 함수에서 사용되는 값이다.

다. WiBro Networks에서 USIM 기반 인증의 통합

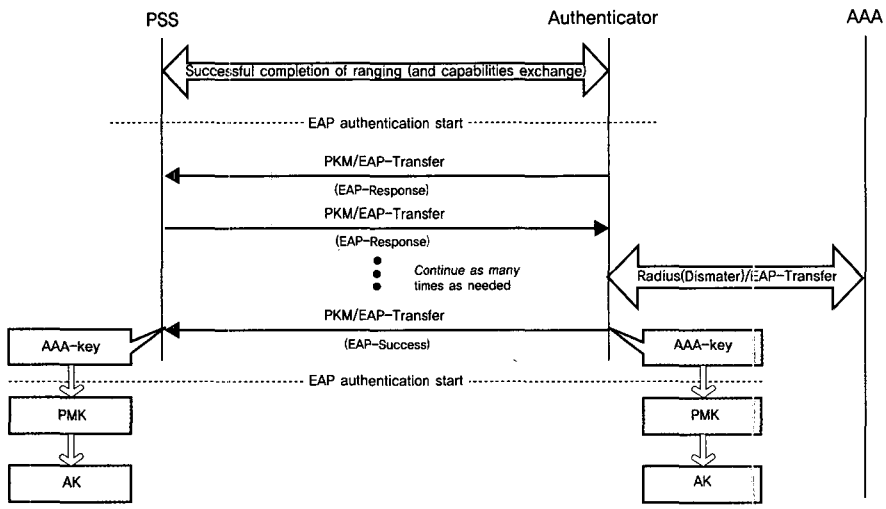
1) EAP-AKA와 WiBro Security용 PKM과 통합

휴대 인터넷의 경우 EAP 인증이 PKMv2와 통합되는 방안이 제시되었고 특정 EAP 방식에 대한 구체적인 기술이 표준화에 언급되어 있지 않다. 따라서 그림 8과 같이 다양한 EAP-method 인증 방식이 수용 가능하고, 이에 따른 인증 키 생성 과정을 별도로 정의하도록 명시한다. 아래 (그림 8)은 EAP 방식을 이용한 WiBro의 PKMv2 인증 절차를 도시한 것이다. 이는 크게 두 단계로 나누어 이루어지는데 먼저 사용자 인증을 수행하는 단계 이후 인증이 성공하면 PSS (Personal Subscriber Station)와 Authenticator 는 AAA서버에서 생성한 동일한 master key인 AAA-Key를 공유하게 되고, 이를 통해 일련의 하위 키들을 도출해내는 권한 획득 단계가 수행된다. 실제로 타 망과의 연동 등을 고려하였을 때는 EAP-AKA를 적용하는 것이 가장 바람직하다고 할 수 있으며, 이 때 인증을 위한 사용자의 수단으로 USIM이 사용된다. 다음 (그림 9)에 USIM 기반의 EAP-AKA를 적용한 WiBro 인증 절차를 도시하였다.

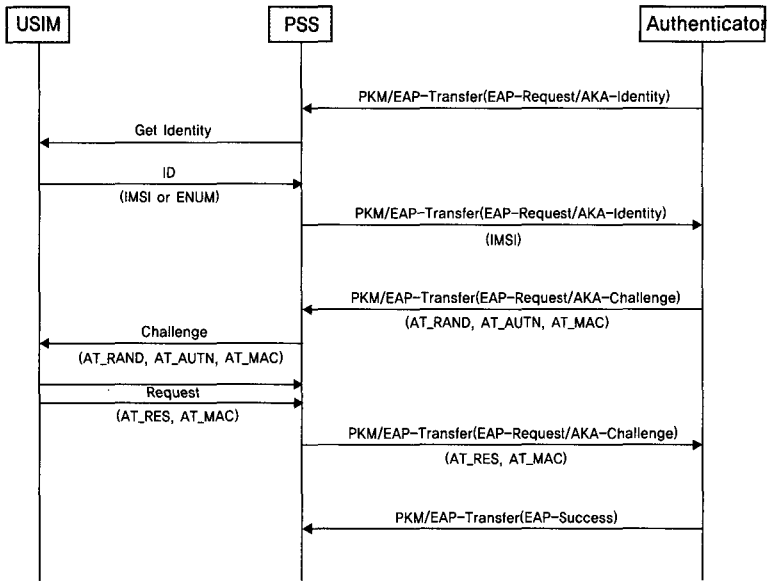
(그림 9)는 USIM 기반의 Wibro 단말과 인증 서버 간의 인증 절차를 보여 주고 있다. WLAN에서와 다른 점은 PKM/EAP 메시지로 AKA 메시지를 전달하는 것과 Key materials 생성 알고리즘 및 Key 관리 기법이 다른 점 이외에는 거의 유사한 방식이므로 자연스럽게 통합이 가능하다. 아래 (그림 9)의 USIM 기반의 WiBro EAP-AKA 인증에 있어서 인증 과정의 큰 흐름은 일반적인 EAP-AKA와 동일한 방식으로 PSS와 Authenticator 사이에서 이루어지나 중요한 데이터의 처리, 즉 user identity의 저장 및 전송이나 키 생성 등의 수행은 단말(PSS)이 아닌 USIM 내에서 이루어지게 된다. 그리고, WiBro의 경우 인증 관련 메시지는 PKM 프로토콜을 따르게 되어 있어 EAP-AKA를 위한 메시지들은WiBro의 MAC 관리 메시지 중 PKM/EAP-Transfer 메시지에 캡슐화 되어 전송된다.



(그림 7) AKA 알고리즘과 EAP-AKA의 Key 생성 알고리즘



(그림 8) EAP Authentication -PKMv2



(그림 9) USIM based authentication over WiBro

리 체계, 약한 암호화 기법 등의 다양한 보안 취약요소)을 지속적으로 보완하여 왔으며, 현재는 EAP 기반의 인증 및 키 관리, AES 암호 알고리즘을 내부 알고리즘에 적용함으로써 보다 강력한 보안 구조를 갖추려 노력하고 있다. 아울러 3G 및 WLAN과의 연동에 관련된 표준화 부분도 함께 진행할 것으로 예상된다[21][23].

VI. 연동 보안 기술 표준화 동향 및 관련 연구

1. 연동 기술 표준화 동향

이 장에서는 3GPP/WLAN/WiBro 연동 보안 기술 표준화의 기반이 될 3GPP/WLAN 연동 보안 기술 및 휴대인터넷 표준화 동향에 대해 살펴본다.

3GPP/WLAN 연동 표준화는 3GPP 중심의 3GPP/WLAN 연동관련 표준화와 IEEE 802.11 진영에서 3GPP와 연계한 표준화로 대별되며[15][21], 이동성이 보장되는 초고속 인터넷인 휴대인터넷은 802.16e를 제정하고 있는 IEEE와 휴대인터넷(WiBro)표준을 제정하고 있는 TTA에서 관련 표준화를 추진 중에 있다.

휴대 인터넷 표준은 기존에 정의되어 있던 다양한 보안상의 문제들(예를 들면 단일 인증, 취약한 키 관

2. 연동 기술 국내외 관련 연구

Nokia는 GSM/GPRS/WLAN 연동 기술을 개발하여 SIM기반 인증과 RADIUS 기반 인증 서버를 구축하여 seamless IP 서비스를 제공하였고[11], HyperLAN2 /3G 연동을 위한 연구로 인증, QoS, Mobility 및 roaming 에 대한 연구를 수행하여 MIP 및 Simple IP연동 서비스를 실현하기 위해 노력하고 있다[12]. 루슨트는 WLAN/CDMA2000 연동 기술에 대한 연구를 수행하여 MIP와 AAA를 재활용하여 loosely couple 구조의 연동 망에서의 seamless IP 로밍 서비스가 가능함을 보였고[25], 모토롤라 역시 WLAN/3G 연동과 WLAN/GPRS연동에 초점을 맞춰 cellular gateway 접근과 SIM 기반 인증을 사용하여 session mobil- ity의 중요성을 검증하고 IP 서비스 연속성에 주안점을 두고 연구하고 있다[24].

각국별로 표준화 단체에서 제정하고 있는 표준문서를 자세히 살펴보면, ETSI BRAN의 TR 101 957 표준은 IEEE 802.11a와 유사한 무선 기술인

HIPERLAN /2와 3G 망을 연동시키기 위한 요구사항 및 구조 명세에 관해 기술하고 있으며[8][14], IEEE 무선랜 관련 802.11 표준에서는 3GPP/WLAN 연동에 적용될 수 있는 표준안들로 802.11TGi에서 EAPOL(EAP Over LAN)기반 802.1X, 802.11TGf에서 AP간 프로토콜에 대한 표준화를 추진하고 있다[15][16]. 또한, WLAN Smart Card Consortium은 WLAN-SIM 사양에 시스템의 기본으로 현재 사용되고 있는 스마트 카드 기술과 핫스팟 제공자의 back end 보안, 접속 그리고 요금정산 시스템이 통신할 수 있는 방법에 대해 구체적으로 기술하고 있다[19].

VII. 결 론

본 고에서는 무선 네트워크 연동 정보보호 기술에 대하여 연동 보안 기술이라는 명제 하에 무선 네트워크가 지니는 일반적인 보안 취약성 및 보안 요구사항에 대해 살펴 보았고, 현재 대표적인 무선 네트워크라 할 수 있는 3G/WLAN/WiBro를 중심으로 한 연동 및 보안 기술가운데 USIM 기반 통합 인증 기술의 구현 방법과 연동 구조를 제시하였다.

3G/WLAN/WiBro 연동 구조의 보안 취약 요소를 해결하기 위해 사용될 수 있는 보안 기술들로 USIM 기반의 사용자 인증, AAA (DIAMETER)기반의 인증 서버와 서로 다른 프로토콜 혹은 서로 다른 사용자 및 서비스 제공자 간에 데이터의 안전성을 보장해줄 수 있는 경제적인 gateway 구축, USIM을 활용한 seamless roaming, 공통 키 관리 방안으로 EAP-AKA 수단을 갖추는 연동 기술 등을 알 수 있었다.

현재 무선 네트워크의 연동 기술은 계속 진화되는 과정에 있으며, 앞으로 새로운 무선 네트워크 서비스의 추가 등으로 인해 보다 다양한 네트워크 간의 연동을 예상할 수 있으므로, 이에 맞추어 연동 보안 기술에 대한 연구도 지속적으로 이루어져야 할 것이다.

[참 고 문 헌]

[1] 3GPP TS 21.133 "3G Security; Security Threats and Requirements; (Release 6)," Jan. 2002.

[2] 3GPP TS 33.120 "3G Security; Security Principle and Objectives; (Release 6)," Apr. 2001.

[3] 3GPP TS 33.234 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network (WLAN) interworking security; (Release 6)," Jun. 2005.

[4] 3GPP TR 23.934 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; Functional and architectural definition (Release 6)," Sep. 2002.

[5] 3GPP TR 22.934 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release 6)," Sep. 2003.

[6] 3GPP TS 23.234 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," Jun. 2005.

[7] 3GPP TS 35.205~208 "3rd Generation

Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; (Release 5)," Jan. 2005.

[8] ETSI BRAN TR 101 957 "Broadband Radio Access Networks (BRAN); HIPER LAN Type 2; Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular systems," Aug. 2001.

[9] RFC 3748 "Extensible Authentication Protocol (EAP)," Jun. 2004.

[10] draft-arkko-pppext-eap-aka-12.txt "Extensible Authentication Protocol for UMTS Authentication and Key Agreement (EAP-AKA)," Apr. 2004.

[11] Juha Ala-Laurila, J.M, and J.R, "Wireless LAN Access Network Architecture for Mobile Operators", Nokia, IEEE Communication Magazine, Nov. 2001.

[12] Stephen McCann, Helena Flygare, "Hiper-LAN/2 Public Access Interworking with 3G Cellular Systems", IEEE Communication Magazine, Nov. 2001.

[13] http://www.3gpp.org/

[14] http://www.etsi.org/

[15] IEEE, "LAN/MAN Specific Requirements- Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification- Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE Std 802.11i, Jun. 2004.

[16] IEEE, "Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," IEEE Std 802.11f, Jun. 2003.

[17] http://www.ietf.org/

[18] http://www.3gpp.org/TB/GERAN/GERAN-WG.htm

[19] http://wlansmartcard.org/

[20] IEEE, "Standard for Local and Metropolitan area networks- Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Std 802.16, Jun. 2004.

[21] IEEE, "Standard for Local and Metropolitan area networks- Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE Std 802.16e/D9, Aug. 2005.

[22] TTA, "2.3GHz 휴대인터넷 표준 - 물리계층 및 매체접근제어계층," TTAS.KO-06.0082, Jun. 2005.

[23] 김영세, 이정우, 한진희, 전성익, "무선 네트워크 연동 보안 기술 동향", 전자통신 동향 분석 제 23권 제 1호, 2005.2

[24] Apostolis K. Salkintzis, Chad Fors, and Rajesh Pazhyannur, Motorola, "WLAN-GPRS integeration for Next-Generation Mobile Data Networks", IEEE Wireless Communications, Oct. 2002.

[25] M.M. Buddhikot, G. Chandranmenon, S.J. Han, Y.W. Lee, Scott Miller, and L. Salgarelli, Bell Lab., "Design and Implementation of a WLAN/CDMA2000 interworking Architecture", IEEE Communication Magazine, Nov. 2003.

전성익

1985년 중앙대학교 전자계산학과 (학사)
1987년 중앙대학교 전자계산학과 (석사)
1987년 ~ 1998년 한국전자통신연구원 실시간 운영체제 연구팀 선임연구원
1998년 ~ 현재 한국전자통신연구원 책임연구원
1998년 ~ 2001년 한국전자통신연구원 MPLS 연구팀
2001년 ~ 현재 한국전자통신연구원 IC카드연구팀 무선보안응용연구팀 팀장
관심분야 : 운영체제, 스마트 카드, 무선 보안, 초소형 플랫폼 기술

김영세

1999년 경북대학교 전자과 (학사)
2001년 경북대학교 전자과 (석사)
2001년 ~ 현재 한국전자통신연구원 무선보안응용 연구팀 선임연구원
관심분야 : 암호 설계, 스마트 카드, 무선 보안, 초소형 플랫폼 기술

한진희

1997년 숭실대학교 정보통신공학과 (학사)
1999년 광주과기원 정보통신과 (석사)
1999년 ~ 현재 한국전자통신연구원 무선보안응용 연구팀 선임연구원
관심분야 : 암호 설계, 스마트 카드, 자바 카드, 무선 보안

정교일

1981년 한양대학교 전자과 (학사)
1983년 한양대학교 전산학과 (석사)
1997년 한양대학교 전자과 (박사)
1982년 ~ 현재 한국전자통신연구원 책임연구원 정보보호기반그룹 그룹장
관심분야 : 정보보호기반 기술 전반

손승원

1984년 경북대학교 전자과 (학사)
1994년 연세대학교 전자과 (석사)
1999년 충북대학교 컴퓨터 공학 (박사)
1991년 ~ 현재 한국전자통신연구원 책임연구원
2004년 ~ 현재 한국전자통신연구원 정보보호 연구단 단장
관심분야 : 정보보호 기술 전반