미래선도기술
이슈분석보고서

이동통신-무선랜 통합망의 보안

이동통신-무선랜 통합망내에서의 통합 인증을 위한 기술적 이슈

백상헌, 동향정보분석팀

KiSTi www.kisti.re.kr 한국과학기술정보연구원 Korea Institute of Science and Technology Information

미래선도기술 이슈분석보고서는 혁신형 중소기업 정보분석 지원사업의 일환으로 작성된 보고서로서, 유망 기술에 대한 이슈분석을 통해 국내 기업들이 자사에 적합한 사업아이템 발굴 기회를 극대화 하는데 목적이 있다. 이슈 분석 대상은 글로벌 동향 브리핑(GTB) 사업에서 축적한 약 10년간의 글로벌 모니터링 정보를 키워드 빈도분석 후 수요 조사를 통해 정하였다. 또한 국내외 연구개발동향, 산업동향 및 기술/실용화/파급효과 등의 측면에서의 이슈제기 및 분석을 해당분야 전문가와 공동으로 수행함으로서 수요자 중심의 보고서가 되도록 노력하였다.

2006 미래선도기술 이슈분석보고서

• 나노셀룰로오즈 보강 복합재료	• 광촉매 박막제조기술
• 차세대 하드디스크 HAMR	• 산업용 무선 필드버스
• 멀티페로익스(Multiferroics)	• P2P 네트워크
• 탄소나노튜브	• 센서네트워크 기술
• 휴대용 연료전지	• 온라인 게임
• 칩내장형 임베디드 기술	• 임베디드 기술
• 유전자 치료	• 십진 부동소수점 연산기
• 열화학적 복합전환 공정	• 게임산업
• 자기 냉장고	• 나노소재를 이용한 전자소자
• 유기 반도체 태양전지	• 유기반도체(Organic Semiconductors)
• 중전기기용 나노절연재료	• 공기오염센서
• 무선 통신망간의 간섭	• 위성항법시스템 시험장(GATE)
• 이동통신-무선랜 통합망의 보안	• 위성합법시스템 소프트웨어 수신기
• 해외선진국 반도체장비 기술동향	• 광촉매의 성능 및 응용 기술 현황
• 동유럽의 VoIP 사업현황	• 해외 선진국의 DMB/DAB 기술동향
• 지능형 자동차에 사용되는 텔레매틱스 기술동향	• 신약개발을 위한 RNAi 제품 현황
• 주요 선진국의 냉동•공조 기술 현황	• 해외 선진국의 위성항법 시스템 기술 동향
• 영상진단기기 및 초음파영상진단기기 제품 현황	• 최근의 게임시장 동향
• 해외 주요국의 디지털 전자제품 동향	•해외 주요국의 디지털 전자제품 동향

Contents

서론

1 무선 네트워크 개요 및 보안의 중요성

1 서론

| 무선 네트워크 개요 및 보안의 중요성

가. 무선 네트워크 발전 동향

○ 무선 통신 기술의 빠른 발전으로 인해 언제 어디서든 휴대 전화를 이용하여 원하는 상대방과 통화할 수 있고, 무선랜 장치가 설치된 사무실에서는 빠른 속도의 무선 인터넷 서비스를 이용할 수 있는 등 우리 일상생활이 크게 바뀌고 있음.

○ 최근에는 세계 최초로 광대역 무선 통신 서비스인 와이브로 (Wibro) 상용 서비스가 우리나라에서 시작되었고 블루투스, 초광대역 (UWB: Ultra Wideband) 통신 등과 같은 다양한 무선 통신 기술이 발전을 거듭하고 있음.

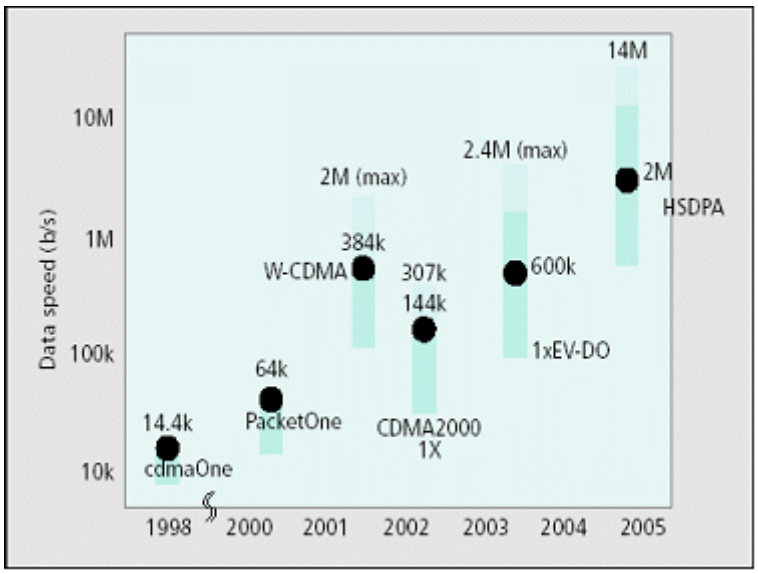
○ 뿐만 아니라, 웹 2.0, 인터넷 전화 (VoIP: Voice over IP), 인터넷 TV (IP TV) 등과 같은 다양한 응용 프로그램이 선보이고 있고 이러한 응용 프로그램들은 IMS (IP Multimedia Subsystem)의 도입과 함께 휴대용 단말기를 통해 무선 네트워크에서 사용가능하게 될 것으로 예측됨.

○ 또한 극소형의 센서들로 구성되어 우리 주변의 물리적 현상을 감지하는 무선 센서 네트워크 기술과 무선 멀티 홉 통신을 이용한 인터넷 서비스인 무선 메쉬 네트워크 기술 등도 가까운 미래에 사용 가능하게 될 것으로 기대됨.

○ 이동 통신망은 음성 위주의 서비스 제공에서 데이터 전송을 위해 대역폭을 증가시키고 있지만 [참고문헌1, 그림1 참고] 수십에서 수백 Mbps의 속도를 제공하는 무선랜에 비해서 제공할 수 있는 데이터 전송 속도가 아주 낮음.

○ 반면 무선랜은 높은 데이터 전송 속도를 제공하지만 이동성을 지원하기 힘들다는 단점이 존재.

○ 따라서, 차세대 무선 네트워크에서는 이동 통신망과 무선랜 등의 다양한 네트워크들이 서로의 단점을 보완하면서 연동된 통합망으로 발전해 나갈 것으로 예측됨 [참고문헌2].



[그림 1] 이동통신망의 발전과정

자료: M. Etoh and T. Yoshimura, "Wireless Video Applications in 3G and Beyond," IEEE Wireless Communication, August 2005.

나. 무선 네트워크에서의 보안의 중요성

○ 무선 네트워크는 유선 네트워크와는 달리 제한된 대역폭과 무선 채널 상태의 큰 영향을 받기 때문에 이러한 가변적인 채널 상황에서 대역폭을 증가시키거나 처리율을 향상시켜 보다 많은 사용자를 수용하고자 하는 연구, 개발 활동이 계속되고 있음.

○ 하지만, 이러한 무선 네트워크 기술의 상용화 과정에서 대두되는 보다 더 중요한 이슈는 보안과 관련된 문제임. 특히, 무선 네트워크는 통신을 위한 무선 채널이 타인에게 쉽게 노출되기 때문에 안전한 보안 기법을 적용시키는 것이 필수 불가결함 [참고문헌3].

○ 최근 활발히 논의되는 무선랜과 이동 통신망을 연동은 이동 통신망을 통한 광범위한 네트워크 접근과 무선랜이 이용 가능한 경우 무선랜을 통해 높은 대역폭의 네트워크 접근을 지원하고자 하는 새로운 개념임.

○ 따라서 무선랜-이동통신망 연동 네트워크에서 보안 기법을 조사 분석하는 일은 중요한 의의를 지님. 본 보고서에서는 무선랜과 이동 통신망에서의 다양한 보안 기법을 조사하고, 연동 네트워크를 위해 새롭게 연구, 개발되고 있는 보안 기법 산업의 동향을 살펴봄.

무선 네트워크에서의 보안 산업 동향

2

이동 통신망에서의 보안 산업 동향

무선랜에서의 보안 산업 동향

이동 통신망과 무선랜 연동 네트워크에서의 보안 산업 동향

2 무선 네트워크에서의 보안 산업 동향

| 이동 통신망에서의 보안 산업 동향

가. 1세대, 2세대 이동 통신망에서의 보안 산업

○ 아날로그 통신 기반의 1세대 이동 통신망에는 복제 기법을 통한 침입 기법이 존재함. 복제 기법에서는 무선 통신을 모니터링하여 전자식 순차 번호 (ESN: Electronic Serial Number)와 모바일 식별 번호 (MIN: Mobile Identification Number)를 알아낸 뒤 이를 이용해 단말기를 재프로그래밍하여 불법적으로 이동 통신망에 접근하게 됨.

○ 뿐만 아니라, 아날로그 통신의 특성으로 인해 통화중인 세션을 도청하는 침입 기법도 가능. 하지만, 1세대 이동 통신망에서는 이러한 침입에 대처할 수 있는 보안 기법이 거의 고려되지 않았음.

○ 디지털 통신 기술에 기반한 2세대 이동 통신은 미국의 IS-41과 유럽의 GSM (Global System for Mobile Communications)으로 대표됨.

○ IS-41에서는 CAVE (Cellular Authentication and Voice Encryption)라는 해쉉 알고리즘을 사용함. CAVE에서는 기지국에서 발생시킨 임의의 수를 네트워크 전체에 뿌리게 되면 단말기가 이 수를 해쉉하여 18비트의 인증 서명을 만들어냄으로써 인증 과정을 수행.

○ 하지만 18비트의 인증 서명은 길이가 짧기 때문에 그 안정성에 문제가 발생할 수 있음. 따라서 CMEA (Cellular Message Encryption Algorithm), ORYX 등의 암호화 기법이 제안됨.

○ GSM의 경우 IS-41과 유사한 인증 기법을 사용하지만 휴대가 가능한 사용자 식별 모듈 (SIM: Subscriber Identity Module)에 저장되어 있는 128비트의 마스터키를 사용하게 됨.

○ 하지만 GSM에서 사용하는 128비트의 키도 보안 모델과 암호화 알고리즘에서 취약점이 보고되었기 때문에 보다 안전한 보안 기법을 위한 노력이 3세대 이동 통신 위주로 활발히 진행되고 있음.

나. 3세대 이동 통신망에서의 보안 산업

○ 2세대 이동 통신은 디지털 통신 기법을 통해 제한된 용량을 확장하고 침입, 도청과 같은 문제를 해결하는 등 1세대 이동 통신에 비해 많은 장점을 가지고 있음.

○ 하지만 2세대 이동 통신은 음성 위주이기 통신 때문에 전자 상거래, 멀티미디어 통신, 인터넷 서비스와 같은 데이터 통신을 지원하기에는 한계점이 존재함. 따라서 이러한 한계를 극복하기 위해 UMTS (Universal Mobile Telecommunications System), CDMA2000 등과 같은 3세대 이동 통신이 발전하게 되었음.

○ 그러나 3세대 이동 통신도 인터넷 기반의 백본 네트워크를 사용함으로써 인터넷 상의 다양한 침입 위협들을 겪게 되었고 단말기의 처리 능력이 제한적이기 때문에 보다 안전한 보안 기법을 적용할 수가 없다는 문제점이 존재.

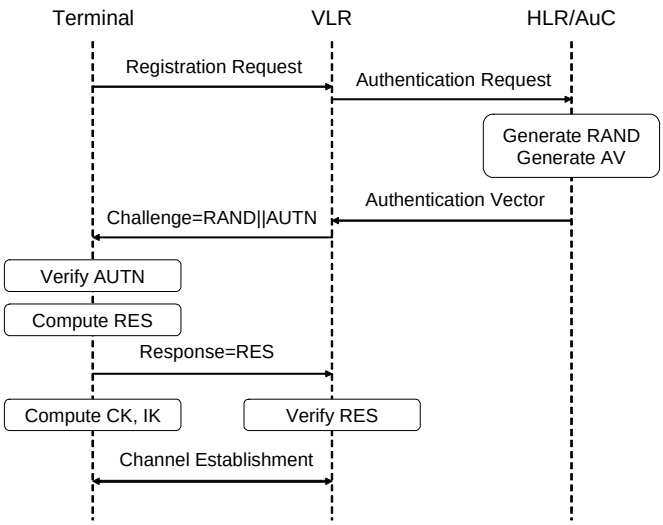
○ 유럽식 3세대 이동 통신 표준인 UMTS에서는 128비트의 키를 통해 상호인증 기법을 제공. 또한 네트워트 엑세스 보안, 네트워크 도메인 보안, 사용자 도메인 보안, 응용 도메인 보안 등의 보안 특성을 지원. UMTS에서는 또한 임시 단말기 식별자 (TMSI: Temporary Mobile Station Identifier)를 이용해서 사용자의 위치 정보를 파악할 수 있음.

○ UMTS에서 네트워크 엑세스 보안은 그림 2에서 설명하고 있는 AKA (Authentication and Key Agreement) 프로토콜을 이용하여 지원됨 [참고문헌4]. AKA 프로토콜은 GSM의 인증 기법을 확장한 것으로 사용자와 네트워크 사이의 상호 인증을 지원함.

○ AKA 프로토콜은 초기화, 신뢰정보 전달, Challenge-Response 교환의 세 단계로 구성. 초기화 과정에서 이동 단말기는 네트워크에게 IMSI (International Mobile Subscriber Identifier)나 TMSI 같은 자신의 식별자를 제공하여 네트워크 에서 인증 절차를 초기화함. 두 번째 단계에서 HLR/AuC (Home Location Register/Authentication Center)는 해당하는 사용자의 보안 신뢰 정보를 사용자 가 위치한 VLR/SGSN (Visitor Location Register/Serving GPRS Support Node)으로 전송. 사용자 인증을 위한 정보는 인증 벡터를 통해 전달되는데 빈번한 이 동이 있을 때 인증 절차로 인한 부하를 줄이기 위해서 다수의 인증 벡터를 전송할 수 있음. 마지막 단계에서 USIM (Universal Subscriber Identity Module)과 VLR/SGSN은 Challenge-Response 교환을 통해 상호 인증을 수행. 즉, VLR/SGSN은 HLR/AuC로부터 받은 인증 벡터 중 하나를 선택해서 USIM에게 인증을 위한 정보를 전달하면 USIM은 MAC (Message Authentication Code)를 생성해서 네트워크 또는 VLR/SGSN이 제대로 된 마스터 키를 가지고 있다는 것을 확인하게 됨. 이와 함께 USIM은 VLR/SGSN으로 인증 정보를 보내면 VLR/SGSN에서 USIM을 확인함으로써 상호 인증 절차가 완료.

○ 미국식 3세대 이동 통신 표준인 CDMA2000에서는 확장된 AKA 프로토콜을 사용함 [참고문헌5]. 즉, UIM (User Identity Module)을 사용해서 새로운 암호화 함수를 사용. CDMA2000의 확장된 AKA 프로토콜은 기존의 AKA 프로토콜과 호환이 되고 단방향 함수로 SHA-1를 명시하고 있고 AES (Advanced Encryption Standard)를 사용함.

○ AKA 프로토콜은 부분적인 상호 인증 기법을 제공하지만 양방향 User Subscriber Identifier Module 과정을 통한 완전한 상호 인증은 제공하지 않음. 또한 사용자가 자신의 식별자를 암호화 없이 전송하게 되는 문제점도 내포함.



[그림 2] AKA 프로토콜

자료 출처: M.Shin,J. Ma, A. Mishra, and W. Arbaugh, "Wireless Network Security and Interworking," Proceedings of IEEE, February 2006.

2 무선 네트워크에서의 보안 산업 동향

| 무선랜에서의 보안 산업 동향

가. 무선랜 개요

○ 무선랜은 사무실, 집 등과 같은 실내 공간에서 별도의 케이블 설치 없이 편리하게 네트워크를 구성할 수 있는 기술로 설치의 용이성으로 인해 행사장, 발표장 또는 학내에서 임시 네트워크 구축하는데 널리 활용되고 있음.

○ 뿐만 아니라 최근에는 대규모 통신 사업자들에 의해 공항, 호텔, 학교 등의 공공장소에 무선랜을 설치하여 상용 무선 인터넷 서비스에 널리 사용되고 있음.

○ 무선랜 기술에 대한 표준화는 전기, 전자 기술자 협회인 IEEE (Institute of Electrical and Electronics Engineers)의 주도로 진행되고 있는데 표1은 무선랜과 관련된 표준화 동향을 정리하고 있음.

나. 무선랜에서의 보안 기법

○ 무선랜 표준화를 진행 중인 IEEE에서는 무선랜 환경에서의 보안을 위해 크게 사용자 인증(Authentication)을 위한 부분과 안전한 데이터 전송을 위한 데이터 암호화 (Encryption)부분으로 나누어 작업을 진행하고 있음 [6].

표 1 무선랜 기술 표준

프로토콜	주요 사양	설명
IEEE 802.11b	2.4GHz/11Mbps/DSSS/50m	WiFi (Wireless Fidelity)라고도 불리는 전 세계적인 무선랜 표준. 보안을 위해 WEP을 사용
IEEE 802.11a	5GHz/54Mbps/OFDM/25m	IEEE 802.11b의 전송율을 향상시킴. 하지만 전파 출력 제한으로 전송거리가 짧음
IEEE 802.11g	2.4GHz/54Mbps/OFDM/50m	IEEE 802.11b에 IEEE 802.11a의 속도성능을 추가함. IEEE 802.11b와 호환되나 네트워크 공유 시 데이터 처리 효율이 현격히 하락함
IEEE 802.11i	2.4GHz/11Mbps/DSSS/50m	IEEE 802.11b 표준에 IEEE 802.1x/EAP 인증구조를 적용해 보안성을 강화. WPA/WPA2 방식의 보안구현
IEEE 802.11n	개발중	High Throughput Task 그룹에서 표준 개발 중. 320Mbps 전송가능을 목표로 2006년 이후 표준화 예상

자료 출처: 고재철, “무선랜 보안 개요”, 웹페이지: http://blog.naver.com/bunny121/140023364332.

○ 기본적인 무선랜 보안 기법은 유선랜 수준의 보안성을 확보하고자 하는 WEP (Wired Equivalent Privacy) 기법임.

○ WEP에서는 40 비트 또는 104 비트의 암/복호화 키를 24 비트 길이의 초기화 벡터 (IV : Initialization Vector)와 결합하여 생성된 64 비트 또는 128 비트의 키를 실제 데이터의 암/복호화를 위해 사용함.

○ 하지만 이러한 WEP 기법은 중앙식 인증 체계와 같은 사용자 인증 구조가 정의되어 있지 않고 WEP에서 내부적으로 사용하는 RC4 알고리즘의 취약점이 발견되었기 때문에 보안상 많은 허점을 가지고 있음.

○ WEP의 취약한 보안 구조를 보완하기 위해서 새로운 무선랜 보안 아키텍쳐인 WPA (Wi-Fi Protected Access) 구조가 발표되었는데 이러한 WPA는 개인 및 소규모 무선랜 환경에 적합한 WPA Personal (WPA-PSK)와 보다 큰 규모의 무선랜에 적용 가능한 WPA Enterprise(WPA-EAP) 구조로 나누어짐.

○ WPA Personal 구조에서는 기존 40 비트의 키를 128 비트로 늘이고 암/복호화 키를 사용자, 네트워크 세션, 또는 전송되는 프레임 별로 키를 변경할 수 있는 TKIP (Temporal Key Integrity Protocol) 방식을 채택하여 외부의 공격자가 쉽게 WEP 키를 추출할 수 없도록 하였음. 즉, 기존의 고정된 WEP 키가 아닌 동적으로 변화는 WEP 키를 사용함으로써 암/복호화 키를 외부에서 추출할 수 있는 가능성이 크게 감소.

○ WPA-Enterprise는 암/복호화 키 관리 방식의 변화뿐만 아니라 사용자 인증영역까지 보완한 방식임. WPA Enterprise 방식은 인증/암호화를 강화하기 위해서 유선랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1x 표준과 이를 통해 다양한 인증 방법을 수용할 수 있도록 IETF (Internet Engineering Task Force)의 EAP (Extensible Authentication Protocol) 인증 프로토콜을 채택.

○ 포트 기반의 네트워크 접근제어 기법인 IEEE 802.1x 표준을 구현하기 위해서는 요청자 (Supplicant), 인증자 (Authenticator), 인증서버 (Authentication Server)의 3가지 요소로 구성.

○ 요청자는 PC, PDA 등 무선랜에 접근하고자 하는 클라이언트 장치를 말하며, 인증자는 AP 또는 네트워크 스위치 등과 같이 중간에서 네트워크 트래픽을 전송하고 클라이언트 장치와 인증 서버 사이에서 인증 데이터를 전송하는 역할을 수행. 인증 서버는 클라이언트 장치 또는 사용자에 대한 인증을 수행하는 요소로 무선랜 환경에서는 RADIUS (Remote Authentication Dial-in User Service) 서버가 대부분 그 역할을 수행함 [참고문헌7].

○ IEEE 802.1x 표준은 요청자, 인증자, 인증서버 등 3가지 구성요소의 전체적인 상호동작을 규정하고 있을 뿐 실제 인증을 위한 인증 프로토콜 또는 암호 알고리즘에 대한 사항은 명시하지 않음. 단지, 요구자와 인증자 사이에서는 확장 가능한 인증 프로토콜인 EAP 프로토콜을 사용하여 다양한 알고리즘을 구현에 적용할 수 있도록 명시함.

2 무선 네트워크에서의 보안 산업 동향

| 이동 통신망과 무선랜 연동 네트워크에서의 보안 산업 동향

가. 이동 통신망과 무선랜 연동 구조

○ 무선랜-이동 통신망의 연동은 서비스 제공업자가 사용자들에게 어디서나 자유롭게 저렴하고 빠른 인터넷 서비스 및 다양한 응용들을 사용할 수 있도록 하는 융합 서비스 기술임. 즉 이동 통신망과 무선랜이 가지는 각각의 장점을 접목시켜서 하나의 새로운 서비스 모델을 만드는 것이 핵심.

○ 무선랜과 이동 통신망의 연동 구조는 결합의 밀접성에 따라 타이트한(Tight) 결합 ([그림 3])과 느슨한 (Loose) 결합 ([그림 4])으로 구분됨 [8].

○ 타이트한 결합 방법에서 무선랜의 서비스 영역은 이동 통신망의 중심망 (Core network)에 하나의 무선 엑세스 네트워크로 연결되기 때문에 이동 통신망의 한 서비스 영역이 무선랜 영역으로 대체됨.

○ 타이트한 결합 방법은 기존의 네트워크 인프라 구조와 이동 통신망의 프로토콜을 재활용할 수 있는 장점을 가짐. 즉, 세션 연결성 보장을 위해 이동 통신망의 이동성 관리 프로토콜을 그대로 사용할 수 있음.

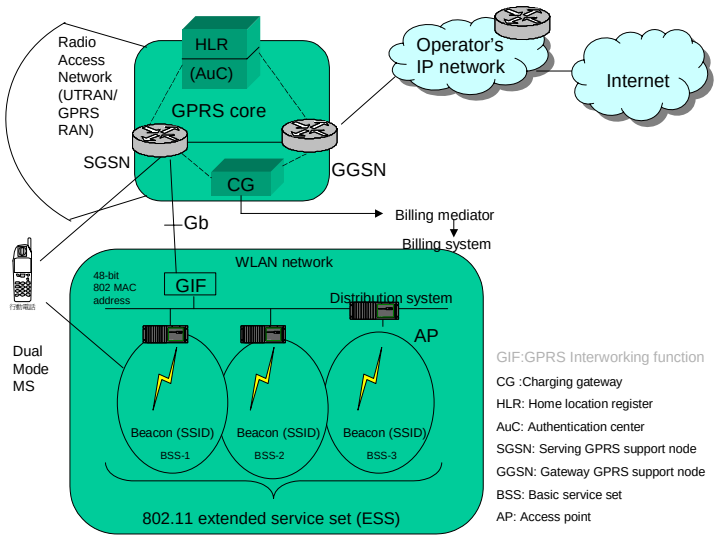
○ 하지만 이동 통신망의 프로토콜은 이동성이 빈번한 사용자를 고려하여 설계된 것이기 때문에 강의실, 호텔, 공항 등과 같이 이동성이 적은 실내 환경에서 사용되는 무선랜에 적합하지 않은 경우가 발생할 수 있음. 또한 이동 통신망의 중심 네트워크로 연결되는 인터페이스가 무선랜 네트워크로 노출될 수 있음. 이러한 인터페이스 노출로 인해 이동 통신망의 중심 네트워크에서의 과도한 트래픽이 발생하게 됨. 가장 큰 문제점은 이동 통신 사업자와 무선랜 사업자가 서로 다른 독립적인 사용자일 경우 별도의 연동 협약을 필요로 하다는 것임.

○ 반면 느슨한 결합 방법에서는 무선랜이 이동 통신망에 인터넷과 같은 외부 네트워크를 통해서 간접적으로 연결됨.

○ 느슨한 결합 방법은 기존 무선랜 표준을 거의 변경시킬 필요가 없고 무선랜과 이동 통신망이 서로 독립적으로 각각의 네트워크에 맞는 기법들을 개발, 적용할 수 있다는 장점을 가짐.

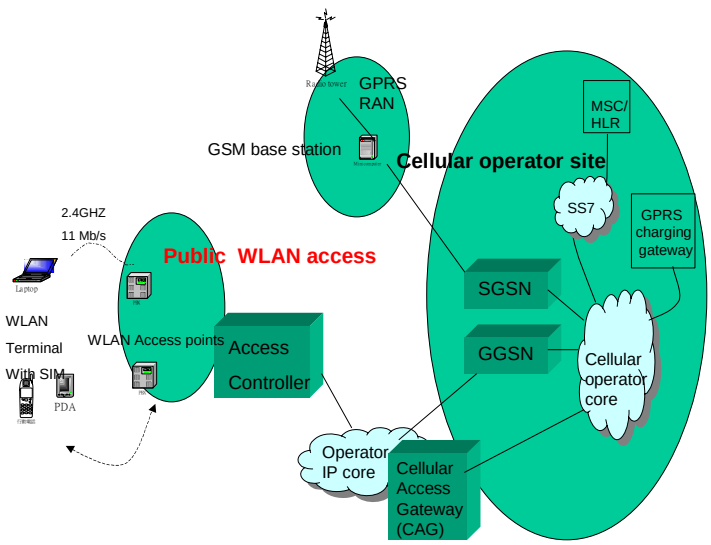
○ 하지만 이러한 느슨한 결합 방법을 지원하기 위해서는 이동성 관리와 AAA (Authentication, authorization, and accounting)을 위해서 모바일 IP (Mobile IP) [9]와 같은 별도의 기능을 이동 통신망에 추가시킬 필요가 있음. 또한 두 네트워크가 분리되어 있기 때문에 데이터 전달을 위해 더 긴 우회 경로를 따라야 하고 이는 핸드오프 지연 시간을 증가시키는 문제가 발생.

○ 그러나 이러한 핸드오프 지연 시간은 계층적인 등록 기법 등을 통해 어느 정도 줄일 수 있기 때문에 느슨한 결합 기법이 이동 통신망 사업자와 무선랜 사업자 모두로부터 더 많은 관심을 받고 있음.



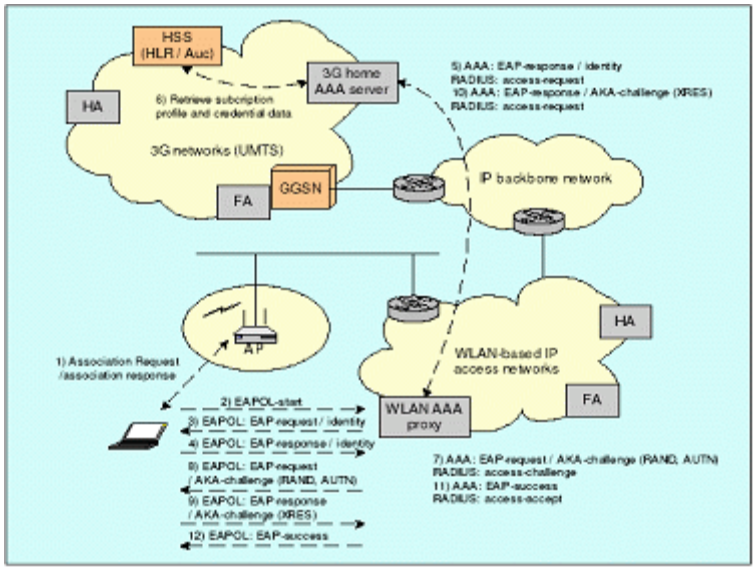
[그림 3] 타이트한 연동 구조

자료 출처: Y. Chen, “Heterogeneous Wireless Networks," 2003.



[그림 4] 느슨한 연동 구조

자료 출처: Y. Chen, “Heterogeneous Wireless Networks," 2003.



[그림 5] EAP를 통한 데이터 링크 계층에서의 통합 인증

자료 출처: W. Song, W. Zhuang, and A. Saleh, "Interworking of 3G Cellular Networks and Wireless LANs," Int. J. Wireless and Mobile Computing, 2006.

나. 이동 통신망과 무선랜 통합 인증 기법

○ 그림 5는 UMTS와 IEEE 802.11 기반의 무선랜의 연동된 네트워크를 보여줌. IEEE 802.11 무선랜은 EAP를 사용하는 IEEE 802.1x에 기반하여 엑세스 제어를 수행. 반면 UMTS 네트워크의 경우 확장성과 상호 운용성을 위해 AAA 서버가 사용되는데 AAA을 위한 프로토콜은 RADIUS나 그것의 확장판인 DIAMETER가 사용됨 [참고문헌10].

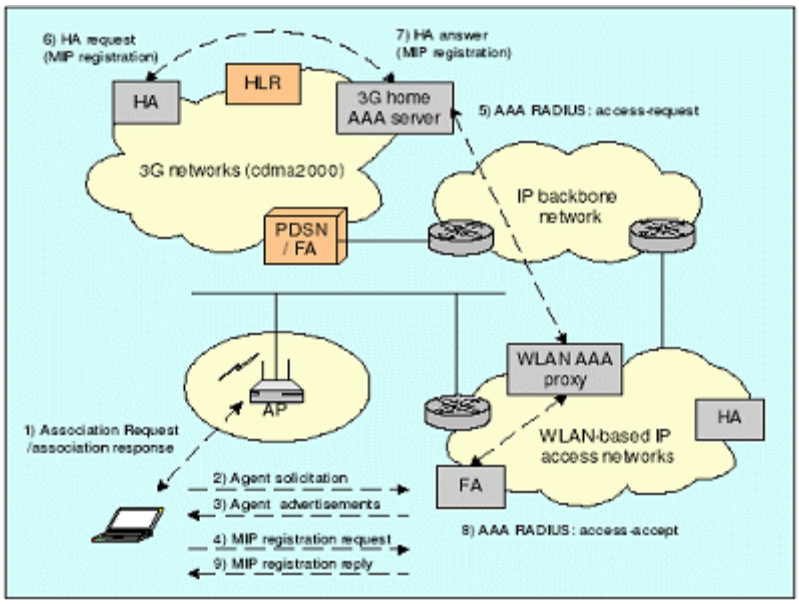
○ 무선랜 영역으로 이동한 UMTS 사용자는 자신의 인증 정보를 EAP에 포함시켜 UMTS 시스템으로 전송함. 이를 수신한 UMTS 시스템은 포함된 사용자의 인증 정보를 이용하여 UMTS의 인증 절차인 AKA 프로시져를 수행하여 사용자 인증을 수행하게 됨. 이 때 사용자의 인증 정보와 구독 정보는 HSS (Home Subscriber Server)나 HLR로부터 얻을 수 있음.

○ CDMA2000과 무선랜 연동 네트워크에서도 위와 비슷한 과정을 통해 인증을 수행할 수 있음.

○ 만약 이동 통신망-무선랜 연동망에 모바일 IP가 지원된다면 이러한 인증 과정은 그림 6과 같이 네트워크 계층, 즉 IP 계층에서 수행될 수도 있음 [참고문헌11].

○ CDMA2000 네트워크에서는 PDSN (Packet Data Serving Node)이 모바일 IP 의 외부 에이젼트 (FA: Foreign Agent)의 역할을 담당하고 홈 에이젼트 (HA: Home Agent)에서는 사용자의 위치 정보를 관리하고 사용자로 향하는 패킷을 터널링을 통해 전달시켜주게 됨.

○ 반면, UMTS에서는 3단계를 통해 모바일 IP 기능을 구현할 수 있는데 첫 번째 단계에서는 외부 에이젼트의 기능이 GGSN (Gateway GPRS Support Node) 에 추가되어 무선랜과 UMTS 사이의 이동성을 모바일 IP를 통해 지원함. 두 번째 단계에서는 GGSN 간의 핸드오프를 지원하기 위해서 모바일 IP가 적용됨. 세번째 단계에서는 GGSN과 SGSN을 결합한 IGSN (Intelligent GPRS support node)을 사용하여 모바일 IP를 지원하게 됨.



[그림 6] 모바일 IP를 통한 네트워크 계층에서의 통합 인증

자료 출처: W. Song, W. Zhuang, and A. Saleh, "Interworking of 3G Cellular Networks and Wireless LANs," Int. J. Wireless and Mobile Computing, 2006.

○ 모바일 IP가 구현된 경우 사용자가 무선랜 영역으로 이동한 경우 모바일 IP의 등록 절차를 통해 인증을 수행함. 즉, 외부 에이젼트가 보낸 에이젼트 광고 (Agent Advertisement) 메시지를 통해 새로운 IP 주소, 즉 임시 주소 (CoA: Care of Address)를 구성한 뒤에 위치 등록 요청 메시지를 외부 에이젼트로 보 냄. 외부 에이젼트는 이동 통신망의 AAA 인증 서버에 접속하여 확장된

○ Challenge-Response 과정을 통해 사용자 인증을 수행하게 됨. 인증 서버를 통한 인증이 완료되면 사용자의 위치 등록 요청 메시지는 홈 에이젼트 요청 메시지를 통해 홈 에이젼트로 전달. 홈 에이젼트로부터 등록이 올바르게 처리되었다는 메시지를 받게 되면 AAA 인증서버는 외부 에이젼트에게 확인 메시지를 보내고 그러면 외부 에이젼트는 사용자에게 위치 등록 응답 메시지를 보냄으로써 위치 등록과 인증 과정이 완료됨.

○ 데이터 링크 계층과 IP 계층뿐만 아니라 응용 계층에서도 인증 과정을 수행할 수 있음. 즉, 사용자를 HTTPS (Hypertext Transport Protocol Secured) 상에서 웹페이지를 통해 인증이 가능. 하지만 이러한 응용 계층에서의 인증 기법은 HTTP를 사용하는 특정 응용에만 적용될 수 있다는 단점이 존재.

○ 이동 통신망-무선랜 연동 네트워크에서 확장된 AAA 프레임워크를 제공하는 데이터 링크 계층의 기법은 이동 통신망에서 사용되는 인증 기법을 재활용할 수 있고 동시에 독립적인 무선랜 서비스 제공업자는 EAP-MD5 (Message Digest 5), EAP-TLS (Transport Layer Security)등과 같은 별도의 인증 기법을 사용할 수도 있음.

○ 인증 기법과 모바일 IP와 같은 이동성 지원 기법과 결합하는 방법은 시그널 링 절차를 간략화할 수 있지만 이 경우 핸드오프 지연 시간의 영향을 최소화할 필요가 있음.

○ 응용 계층에서의 인증 기법의 경우 하위 네트워크 기술과의 독립성을 제공할 수는 있지만 메시지 처리의 지연 시간이 길고 특정 응용에만 제한적으로 사용될 수 있음.

이슈 분석 및 제기

3

- 이동 통신망과 무선랜 통합 인증에서의 최근 또는 향후 이슈
- 실용화, 산업화를 위한 기술(산업)적 과제
- 경제적 파급 효과

3 이슈 분석 및 제기

| 이동 통신망과 무선랜 통합 인증에서의 최근 또는 향후 이슈

가. 통합 인증을 위한 아키텍쳐 설계

(1) 독립 인증 기법

○ 무선랜과 이동 통신망 사이의 별도의 협약을 필요로 하는 독립 인증 기법은 사용자가 이동 통신망과 무선랜, 모두에 대한 서비스 등록을 해야 하고 이동 통신망의 서비스를 받던 사용자가 무선랜으로 이동한 경우에는 무선랜 네트워크를 통해 별도의 인증 과정을 거쳐야 함. 따라서 진정한 의미에서의 통합 인증 기법으로 보기는 어려움.

(2) 중앙 인증 기법

○ 중앙 인증 기법에서는 이동 통신망 서비스 가입자가 해당 가입 정보를 이용해서 무선랜에서 가입자 인증을 받을 수 있음. 중앙 인증 기법에서는 사용자가 외부 네트워크에서 인증과 관련된 정보를 EAP 프로토콜을 이용해서 자신의 홈 네트워크로 전송. 이를 받은 홈 네트워크의 인증 서버는 정당한 사용자인지를 검증.

○ EAP 기법은 포함되는 인증 기법에 따라 GSM 방식의 인증을 지원하는 EAP-SIM과 GSM 인증에서의 상호 인증 문제를 개선한 3세대 이동 통신 시스템에서의 EAP-AKA등으로 구분됨. 하지만 EAP-SIM, EAP-AKA 등의 인증 기법에서 보안상의 문제가 발견되었기 때문에 이러한 보안 문제를 개선하기 위해 EAP 정보를 TLS (Transport Layer Security)에 포함시킨 PEAP (Protected EAP)도 제안되었음.

○ 중앙 인증 기법의 대표적인 한계점은 외부 네트워크와 홈 네트워크 사이의 인증을 위한 협약이 미리 체결되어 있어야 한다는 점. 따라서 N개의 네트워크가 있다면 필요한 인증 협약은 N2개가 되기 때문에 이를 위한 오버헤드가 많이 소비됨. 이를 줄이기 위해서 AAA-브로커 등과 같은 제 3자 요소를 통해 중앙 인증을 구현할 수 있음. 중앙 인증 기법의 또 다른 문제점은 핸드오프 과정에서 인증을 위해서 홈 인증 서버에 접속을 해야 하기 때문에 인증을 위한 지연 시간이 길어진다는 단점이 존재. 이를 줄이기 위해서 AAA-브로커를 사용자의 위치한 외부 네트워크에 두는 방법을 제안할 수 있음.

나. 핸드오프 지연시간의 최소화

○ 이동 통신망-무선랜 통합망은 기본적으로 사용자가 한 네트워크에서 다른 네트워크로 이동하는 핸드오프 과정을 가정함. 따라서 핸드오프시의 통합 인증으로 인한 지연 시간을 최소화하는 것이 필요.

(1) 새로운 네트워크에 미리 인증키를 전달

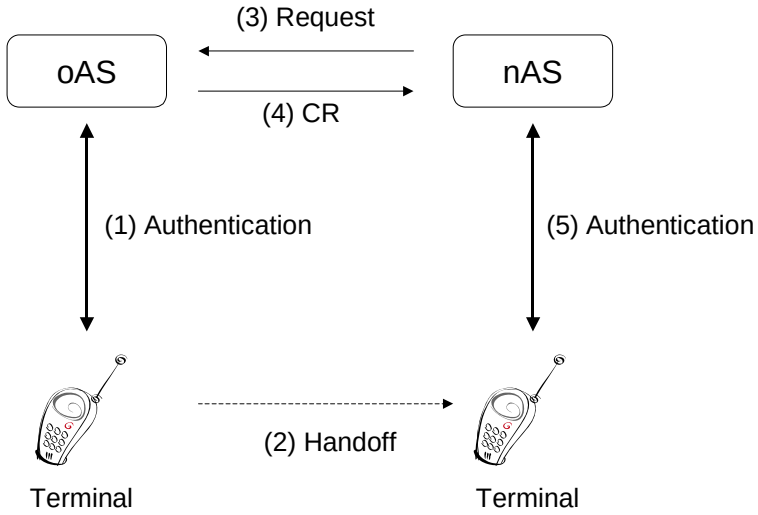
○ 인증 지연 시간을 줄이기 위해 인증키를 이동할 새로운 네트워크에 미리 전달시키는 기법을 고려할 수 있음. 즉, 한 인증 서버에서 사용자가 자신의 영역으로 이동했다는 것을 감지를 하게 되면 홈 인증 서버에게 미리 키를 분배해 줄 것을 요청. 홈 인증 서버에서는 사용자의 이동성 패턴 등을 분석하여 다음번에 이동할 곳이 어디가 될 것인지를 예측한 뒤 인증키를 선택된 인증 서버들에게 전송. 그러면 키가 미리 이동하게 될 위치로 전달이 되기 때문에 인증 절차로 인해 지연 시간을 크게 줄일 수 있음.

○ 미리 키를 전달시키는 방법을 통해 인증 지연 시간을 줄일 수 있지만 이를 위해서는 사용자의 이동성 패턴을 예측할 수 있는 알고리즘 개발이 우선되어야 함. 또한 이동성 패턴 예측이 올바르지 않은 경우에 대처할수 있는 방법도 필요.

(2) 문맥전달기법의 사용

○ 핸드오프에서의 인증 지연 시간을 줄이기 위해서 네트워크 사이에서 이전에 설정된 문맥을 다른 네트워크로 전달시켜주는 문맥 전달 (Context Transfer) 기법이 제안되었음. 문맥이란 사용자가 새로운 네트워크에서 전체 연결 절차를 수행하지 않고도 연결을 설정할 수 있도록 해주는 부분적인 정보를 의미. 이러한 문맥에는 단말기의 식별자와 이전 인증의 결과, 그리고 인증을 통해서 부여받은 권한 정보, 그리고 통신을 위한 암호화 알고리즘, 세션 키 등에 대한 인증 정보와 해당 사용자의 서비스 프로파일 등의 정보가 포함됨.

○ 문맥 전달 기법을 통해 핸드오프시의 인증 지연 시간을 줄일 수는 있지만 문맥을 주고받는 네트워크 사이의 올바른 신뢰 관계가 성립되어 있는 경우에만 적용 가능한 기법으로 사료됨.



[그림 7] 후행적 문맥 전달 기법

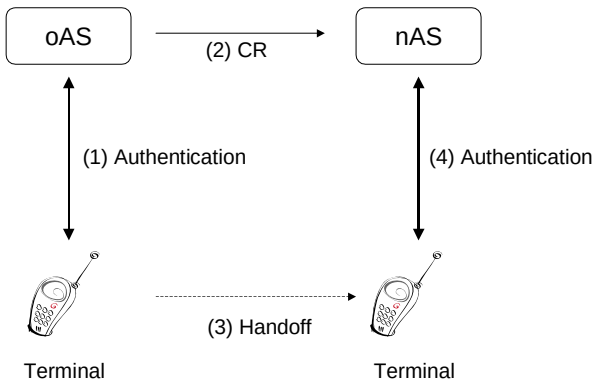
자료: M. Shin, J. Ma, A. Mishra, and W. Arbaugh, "Wireless Network Security and Interworking," Proceedings of IEEE, February 2006.

① 문맥 전달 기법은 문맥이 전달되는 시점에 따라 후행적 문맥 전달 기법 (Reactive Context Transfer)과 선행적 문맥 전달 기법 (Proactive Context Transfer)으로 구분됨.

- 후행적 문맥 전달 기법

:후행적 문맥 전달 기법에서는 사용자가 새로운 네트워크로 이동한 뒤에 문맥이 새로운 네트워크로 전달됨 (그림 7). 즉 사용자가 새로운 네트워크로 이동을 하게 되면 현재 인증 서버에서 이전 인증 서버의 주소를 파악하여 문맥 전달을 요청함. 그러면 이전 인증 서버에서 해당 사용자에 대한 문맥이 전달이 되면 그것을 통해 사용자를 인증한 뒤 접속을 허락함.

:후행적 문맥 전달 기법과 관련해서 인터넷 표준화 기구인 IETF에서 문맥 전달 프로토콜(CTP: Context Transfer Protocol)[참고문헌12]이 제안되었고 IEEE에서는 엑세스 포인트 간 프로토콜 IAPP(Inter Access Point Protocol) 프로토콜이[참고문헌13] 제안되었고 현재도 많은 연구가 진행되고 있음. 하지만 CTP, IAPP 등을 실제로 구현한 상용 제품 개발은 아직 활성화되고 있지 않음. 또한 데이터 링크 계층에서의 문맥 전달 기법과 네트워크 계층 또는 응용 계층에서의 사용자 정보 교환 기법 사이의 연동이 필수적임.



[그림 8] 선행적 문맥 전달 기법

자료: M. Shin, J. Ma, A. Mishra, and W. Arbaugh, "Wireless Network Security and Interworking," Proceedings of IEEE, February 2006.

-선행적 문맥 전달 기법

:그림 8에서 설명하는 선행적 문맥 전달 기법은 사용자가 새로운 네트워크로 이동하기 전에 문맥 전달이 수행됨. 선행적 문맥 전달 기법을 위해서 두 가지 방법이 가능한데 첫 번째는 소프트 핸드오프 (Soft Handoff) 기술을 이용해서 사용자가 핸드오프 과정에서 이전 네트워크와 새 네트워크에 모두 연결을 유지하는 것임. 또 다른 방법은 핸드오프 예측 기법을 통해 사용자가 어떤 네트워크로 이동할 것인가를 예측해서 문맥을 보내는 방법임.

:선행적 문맥 전달 기법에서는 이전 인증 서버가 사용자를 파악한 뒤에 해당 사용자가 이동할 가능성이 큰 새로운 인증 서버들을 선택함. 그런 다음에 이전 인증 서버는 선택된 새로운 인증 서버들에게 문맥 전달을 수행하게 됨.

:선행적 문맥 전달 기법이 후행적 문맥 전달 기법에 비해 더 짧은 인증 지연 시간을 제공할 수 있지만 구현하기 힘들다는 단점이 존재함. 특히, 문맥을 미리 전달하는 시점에 따라 네트워크상에서 문맥 전달을 위한 부가적인 트래픽이 많이 발생할 위험이 존재함.

3 이슈 분석 및 제기

| 실용화, 산업화를 위한 기술(산업)적 과제

가. 단말기 개발의 관점

(1) 듀얼모드 단말기의 개발

○ 이동 통신망-무선랜 통합망은 단말기가 이동 통신망과 무선랜에 대한 무선 인터페이스를 모두 가지고 있는 듀얼 모드 단말기라는 것을 가정. 현재 삼성, LG, 노키아, 모토로라 등의 단말기 제조업체에서 이동 통신망와 무선랜을 지원하는 듀얼 모드 단말기를 활발히 개발 중에 있음.

○ 듀얼 모드 단말기 개발에서 고려해야 할 사항은 다중 무선 인터페이스를 사용함으로써 발생할 수 있는 에너지 소모를 최소화하는 점과 두 개 이상의 인터페이스가 장착된 경우에도 경량화를 유지하고 사용자의 취향에 맞는 디자인의 단말기를 개발해야 한다는 점임.

(2) 단말기의 전력 소비 최소화

○ 휴대용 단말기의 가장 큰 제약 사항 중의 하나는 배터리 전원을 사용한다는 점. 따라서 휴대용 단말기에 적용되는 하드웨어와 소프트웨어는 전력 소비를 최소화할 수 있어야 함.

(3) 경량화된 암호화 알고리즘의 개발

○ 통합 인증에서 사용할 수 있는 다양한 암호화 알고리즘이 존재하지만 무엇보다도 제한된 자원을 가지는 휴대용 단말기에서도 잘 동작할 수 있고 전력 소비가 적은 경량화된 암호화 알고리즘이어야 함.

나. 서비스 제공의 관점

(1) 효과적인 연동 구조의 설계

○ 서비스 제공의 측면에서 봤을 때 느슨한 결합 방법이 이동 통신망 사업자와 무선랜 사업자를 인터넷을 통해 보다 유연하게 결합시킬 수 있음. 이동 통신망-무선랜 통합망에서는 이음새 없는 핸드오프를 지원할 수 있고 사업자 간의 인증 서버를 공유할 수 있는 연동 구조를 설계해야 함.

○ 사용자가 서로 다른 네트워크를 핸드오프를 통해 이동한 경우 각 네트워크에서 적용되는 정책에 따라 올바르게 과금할 수 있는 시스템도 필요.

(2) 서비스 품질 보장 기법의 적용

○ 이동 통신망-무선랜 통합망에서는 사용자의 핸드오프를 통해 서로 다른 특성을 가진 네트워크 사이에서 이동하게 됨. 사용자의 입장에서는 사용하는 네트워크와 무관하게 동일한 수준의 서비스 품질을 요구할 것임.

○ 특히 무선랜에서는 서비스 품질 보장 기법이 현재 적용되지 않기 때문에 이동 통신망에서 무선랜으로 핸드오프를 한 경우 동등한 수준의 서비스 품질이 보장하기 위한 기법에 대한 연구가 절실함. 이러한 서비스 품질 보장을 위해서는 인증 절차로 인한 지연 시간과 부가적인 트래픽을 최소화시킬 필요가 있음.

3 이슈 분석 및 제기

| 경제적 파급 효과

○ 음성 통화 위주의 이동 통신망의 수익 모델은 거의 포화 상태에 이른 상태이기 때문에 데이터 서비스를 통한 새로운 수익 모델을 찾고자 하는 노력이 계속되고 있음.

○ 이동 통신망-무선랜 통합망은 이동 통신 사업자의 새로운 수익 모델이 될 것으로 기대됨. 즉, 이동 통신망과 무선랜 서비스를 결합함으로써 무선랜 서비스 영역에서의 추가적인 무선 인터넷 서비스 사용으로 인해 부가적인 데이터 서비스 수익을 창출할 수 있을 것임.

○ 이동 통신망-무선랜 서비스는 전 세계적으로 경쟁력을 가지고 있는 우리나라의 이동 통신 기술에 데이터 서비스를 결합시킴으로써 단말기 수출, 서비스 제공 등으로 인한 수익 창출 효과를 낳을 수 있을 것으로 기대됨.

○ 실례로 독일의 통신 업체인 T-Mobile은 무선랜 서비스를 미국 시장에 진출시키면서 많은 수익을 창출. 아직까지 이동 통신망-무선랜 연동을 통한 서비스 형태는 널리 확산되지 않은 상태이기 때문에 이러한 서비스를 보급함으로써 많은 수익을 창출할 것으로 예측할 수 있음.

○ 이러한 이동 통신망-무선랜 연동 서비스 보급을 위한 필수적인 요소가 바로 효율적인 통합 인증 기법임.

결론

4

4 결론

○ 이동 통신망-무선랜 연동 네트워크는 낮은 데이터 전송률을 가지는 이동 통신망과 제한된 서비스 영역을 가지는 무선랜을 결합함으로써 이동 통신망 사용자에게 데이터 서비스의 수요가 많은 지역에서 빠른 속도의 무선 인터넷 서비스를 제공할 수 있음.

○ 이동 통신망-무선랜 연동은 포화 상태에 이른 음성 통화 위주의 수익 모델에서 벗어나 이동통신망 사업자가 새로운 수익을 창출할 수 있도록 해줄 것으로 기대됨.

○ 이동 통신망-무선랜 연동 네트워크의 성공적인 서비스를 위한 필수적인 요소가 사용자의 인증, 데이터 암호화 등을 통해 안전한 데이터 서비스를 제공하는 것임.

○ 본 보고서에서는 이동 통신망-무선랜 연동 네트워크에서의 통합 인증 기법을 살펴보고 통합 인증을 위한 기술적 이슈와 실용화, 산업화를 위한 과제 등을 소개하였음.

○ 따라서 본 보고서의 내용은 안전한 이동 통신망-무선랜 연동 네트워크 구축을 위한 참고 자료로 활용될 수 있을 것으로 기대됨.

참고문헌

1. M. Etoh and T. Yoshimura, "Wireless Video Applications in 3G and Beyond," IEEE Wireless Communications, August 2005.

2. D. Axiotis, T. Al-Gizawi, E. Protonotarios, F. Lazarakis, C. Paradias, and P. Philippopoulos, "Services in Interworking 3G and WLAN Environments," IEEE Wireless Communications, October 2004.

3. M. Shin, J. Ma, A. Mishra, and W. Arbaugh, "Wireless Network Security and Interworking," Proceedings of IEEE, February 2006.

4. G. Koien, "An Introduction to Access Security in UMTS," IEEE Wireless Communications, February 2004.

5. G. Rose and G. Koien, "Access Security in CDMA2000 including a COmparison with UMTS Access Security," IEEE Wireless Communications, February 2004.

6. J. Edney and W. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i," Addison Wesley Professional, 2003.

7. C. Rigney, S. Willens, A. Rubens, W. Simpson, "Remote Authentication Dial in User Service (RADIUS)," IETF RFC 2865.

8. W. Song, W. Zhuang, and A. Saleh, "Interworking of 3G Cellular Networks and Wireless LANs," Int. J. Wireless and Mobile Computing, 2006.

9. C. Perkins, "IP Mobility Support," IETF RFC 3344.

10. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "Diameter Base Protocol," IETF RFC 2865.

11. M. Buddhikot, G. Chandranmenon, S. Han, Y. Lee, S. Miller, and L. Salgarelli, "Design and Implementation of a WLAN/CDMA2000 Interworking Architecture," IEEE Communications Magazines, November 2003.

12. M. Nakhjiri, C. Perkins, and R. Koodli, "Context Transfer Protocol," Internet Draft, March 2003.

13. IEEE 802.11f, “Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation,” IEEE Standard, July 2003.

저자소개

➢백 상 헌

- 공학 박사
- 현, 서울대학교 박사 후 연구원

➢한국과학기술정보연구원 동향정보분석팀