情報保護學會論文誌
第17卷 第4號, 2007. 8

퍼베이시브 로밍 서비스를 위한 보안 관리 프레임워크

김 관 연[1†], 황 지 온[1†], 김 용[1†], 엄 윤 식[1†], 박 세 현[2‡]
[1]중앙대학교, [2]홈네트워크연구센터

A Study of Pervasive Roaming Services with Security Management Framework

Gwanyeon Kim[1†], Zion Hwang[1†], Yong Kim[1†], Yoonsik Uhm[1†], Sehyun Park[2‡]
[1]Chung-Ang University, [2]Home Network Research Center

요 약

유비쿼터스 및 자동화된 컴퓨팅 환경은 개방적이고 동적이어야 하며, 끊김 없는(seamless) 소프트웨어와 시스템 구조의 연동을 통한 일반적인 무선 접근으로 사용자에게 다가가는 퍼베이시브 서비스를 제공해야한다. 하지만 다양한 네트워크에서 모든 이동 기기들 간에 미리 정의된 보안 인증을 포함한 로밍 서비스를 제동하기는 매우 복잡하고 어렵다. 더욱이 퍼베이시브 서비스 환경에서 끊김 없는 통신 서비스를 제공하기 위해, 다양한 무선 사업자간에 로밍 협정을 세팅하거나 스마트카드 기반의 효율적인 사용자 프로파일 모델링 연구나 다양한 종류의 사용자 인터페이스를 이용하여 자동화된 사용자 인증 시스템을 위한 보안 방안에 관한 연구는 많지 않다. 사용자에게 다가가는 네트워크 도메인 간의 퍼베이시브 보안 서비스를 포함한 상호 로밍이 가능한 로밍 코디네이터 기반의 보안 관리 프레임워크를 제안한다. USIM(Universal Subscriber Identity Module Card)을 이용한 상용 이동 통신은 하나의 서비스 도메인에서만 가능하지만 본 논문에서 제안한 로밍 코디네이터(Roaming Coordinator)는 PWLAN(Public Wireless Local Area Network)이나 3G 이동통신 그리고 WMAN(Wireless Metropolitan Area Network) 등의 다른 네트워크 도메인에서의 보안 서비스를 보다 안전하고 쉽게 제공할 수 있다.

ABSTRACT

The ubiquitous and autonomic computing environments is open and dynamic providing the universal wireless access through seamless integration of software and system architectures. The ubiquitous computing have to offer the user-centric pervasive services according to the wireless access. Therefore the roaming services with the predefined security associations among all of the mobile devices in various networks is especially complex and difficult. Furthermore, there has been little study of security coordination for realistic autonomic system capable of authenticating users with different kinds of user interfaces, efficient context modeling with user profiles on Smart Cards, and providing pervasive access service by setting roaming agreements with a variety of wireless network operators. This paper proposes a Roaming Coordinator-based security management framework that supports the capability of interoperator roaming with the pervasive security services among the push service based network domains. Compared to traditional mobile systems in which a Universal Subscriber Identity Module(USIM) is dedicated to one service domain only, our proposed system with Roaming Coordinator is more open, secure, and easy to update for security services throughout the different network domains such as public wireless local area networks (PWLANs), 3G cellular networks and wireless metropolitan area networks (WMANs).

Keywords : *4G, AAA, Pervasive Computing, Roaming, Security, Smart card, Ubiquitous Networks*

접수일: 2007년 7월 4일; 채택일: 2007년 7월 23일
* 본 논문은 2004년도 중앙대학교 일반연구비 지원에 의한 것으로 이에 감사 드립니다.
† 주저자, gykim@hnrc.cau.ac.kr
‡ 교신저자, shpark@cau.ac.kr

Ⅰ. 서 론

최근에는 컴퓨터나 통신 기기들이 생활에서 사용하는 기기에 내장됨으로써 일상의 한 부분으로 시스템이 적용되고 있다. 컴퓨팅이나 통신 서비스를 언제 어디서나 받길 원하는 수요를 충족시키기 위해서는 보안적인 연동이나 단대단 QoS와 같은 서비스 측면에서의 관리가 필요하다. 이와 같은 서비스를 일반적으로 유비쿼터스 통신 서비스라고 하고 언제 어디서나 서비스에 연결될 수 있음을 의미한다. 다양한 기기와 여러 서비스 도메인을 아우르는 유비쿼터스 통신 서비스의 경우 사용자의 이동과 여러 무선 네트워크 기술이 적용되기 때문에 끊김 없는 보안, 이동성 및 QoS 관리가 가장 중요한 기술이 되고 있다.

이와 같은 유비쿼터스 통신 서비스에서는 다양한 네트워크 도메인이 연결되고 연계되어지므로, 각 네트워크 도메인을 쉽게 이동할 수 있어야 한다. 이와 같은 다양한 네트워크 도메인 간 로밍서비스가 필수적이며, 로밍 서비스는 사용자가 원하는 상황에 적합한 서비스가 편재될 수 있는 퍼베이시브 로밍 서비스를 의미한다. 그러나 이러한 일반적인 로밍 서비스는 "이동통신에서 서비스 지역이 다른 사업자간의 무선 네트워크를 접속함으로써 고객이 가입 네트워크의 범위를 넘어선 이동을 하여도 통신이 가능하게 되여, 그에 따른 요금의 결재도 가능하도록 하는 서비스"라고 정의되는 단순한 서비스이며, 단순한 사용자 인증과 접근제어, 요금 과금 등에서 사업자간 협약이 중요한 이슈가 되고 있다. 서비스에서의 연계성을 고려하기 보다는 접속 서비스에 중점을 두고 있기 때문이다. 기존 모바일 네트워크에서의 이동성은 사업자의 사업지역에 의하여 제약을 받게 된다. 즉, 특정한 사업자에 가입한 이용자는 해당 사업자의 서비스 제공영역을 벗어나게 되면, 이동통신 서비스의 이용에 제한을 받게 된다. 이러한 경우에는 이동통신 서비스가 완전한 이동성을 제공하지 못하게 되어 가입자의 불편으로 귀결된다. 따라서 이러한 네트워크 접속을 가능하게 하는 부분만이 고려되고 있다.

최근 WCDMA(Wideband Code Division Multiple Access) 망을 이용한 국제 로밍 및 영상통화 로밍 서비스는 단일 WCDMA 무선 네트워크 구조에 기반한 것으로 여전히 이기종 네트워크간 로밍을 위한 QoS 및 로밍 서비스의 제공에 어려움이 있다. 따라서 유비쿼터스 통신 서비스를 이용하는 사용자라면 네트워크 간의 연결을 위해 특별히 정보를 제공해야 하지 않는 것은 물론 사용자가 의식하지 않고 필요한 서비스를 제공받을 수 있기를 원하며, 다양하게 편재된 네트워크 환경에서의 퍼베시브 로밍 서비스 인프라를 구축하기 위한 이기종 시스템간의 통합 및 로밍 서비스 지원은 중요한 이슈로 떠오르고 있다.

그러나 현재 로밍기술은 서비스 도메인 간 끊김 없는 로밍 서비스가 이루어지고 있지 않으며, 버티컬 핸드오프(Vertical Handoff)가 이루어지고 있지 않는 등 로밍 서비스에서의 QoS 제공에는 다양한 기술적 한계점을 가지고 있다. 무선 망간 끊김 없는 로밍 서비스가 이루어지기 위해서는 연동망간 로밍기술의 연구를 기반으로 안전한 인증 서비스를 위한 USIM기반의 단말용 보안 플랫폼 및 서버의 개발, 로밍을 지원하는 연동망 AAA(Authentication, Authorization, Accounting) 기술 개발, 로밍 에이전트 설계, 로밍 동의(Roaming Agreement) 및 SLA(Service Level Agreement) 표준화 기술 연구가 필요하다.

그중에서도 특히 AAA 지원을 위한 로밍 시 지연을 최소화 할 수 있는 보안 서비스가 가장 선결되어야 할 기술이다. 보안 서비스에서 사용자 인증은 사용자 프로파일 기반의 특성, 소유권, 정보 등의 요소들 중 최소한 하나 이상의 것에 의존한다. 스마트카드는 위에서의 요소를 사용하는 것[1]에 의존적이지 않는 사용자 인증 시스템을 구성하는데 도움이 된다. 따라서 스마트카드는 사용자 편의성과 내구성 있는 보안을 제공하기 때문에 중요한 의미를 지닌다. 이처럼 사용자의 편의가 중요한 요인이라면 네트워크 인증 체계에 스마트카드를 이용함[2]으로써 유선 네트워크에서 사용되고 있는 PC에서처럼 단일 사용자 인증 체계에 기반을 두어 서비스 접근을 관리할 수 있을 것이다.

이처럼 스마트카드는 비밀 ID를 저장할 수 있고 데이터 전송에서 암호학적으로 보호할 수 있는 프로토콜을 구성할 수 있기 때문에 일반적으로 사용자 보안 인증에서 유용한 역할로 사용되어 왔으며, 이미 모바일 어플리케이션과 서비스에서 사용되고 있다. 10억이 넘는 이동통신 네트워크 사용자들이 사용하는 SIM(Subscriber Identity Module)이라 일컬어지는 인증 토큰에 기반한 스마트카드가 서비스 중에 있다. 이미 유럽등지에서는 이기종 네트워크 도메인에서 다양한 모바일 사업자들 간에 사용자가 단일 SIM을 이용해 사용하거나, 사용자에 따라 사용하기 편리하도록 여러 사업자간 사

용자 계정을 열어 상황에 맞게 사용할 수 있다.

모바일 사업자의 적절한 선택과 연결이 가능한 끊김 없는 보안 로밍 네트워크는 4G 네트워크에서 뿐만 아니라 유비쿼터스 네트워크 환경에서 필요한 유무선의 다양한 네트워크 서비스 도메인 간 퍼베이시브 로밍 서비스를 위한 중요한 기능이다. 그러나 제시된 스마트카드나 SIM 기술은 여러 가지 이유에 의해 직접적으로 끊김 없는 보안 로밍 서비스에 활용될 수는 없다. 왜냐하면 표준 SIM기반의 사용자들은 로밍을 위한 초기 상황에서 약간의 장애물이 존재하기 때문이다. 그것은 SIM 카드와 리더기, 드라이버와 다양한 운영체제 요소 사이에서의 복잡한 상호작용처럼 사용자 클라이언트 측면에서 너무 많은 설정과 셋업 기능이 존재한다는 것이다. 게다가 다른 종류의 사용자 인터페이스와 스마트카드에서 사용자 정보를 사용하는 컨텍스트 모델을 통해 사용자를 인증할 수 있는 이동통신-공중무선랜 연동 네트워크 구조 설계를 실제화하기 위한 보안 방안을 구현하는데도 아직은 좀 더 많은 연구가 필요하다. 따라서 무선 네트워크 사업자의 다양성을 가지고 로밍 허가를 설정함으로써 퍼베이시브 접근(Pervasive Access) 서비스를 제공하는 방안에 대한 연구가 필요하다.

본 논문에서는 모바일 네트워크를 위한 상호작용하는 로밍 서비스와 스마트카드 어플리케이션과 같은 사용자 인증 매체를 기반으로 사용자 보안 인증을 위한 끊김 없는 보안 관리 프레임워크를 제안한다. 차세대 모바일 네트워크를 위한 로밍 서비스에서의 클라이언트 및 인증 서버간의 신뢰 설정과 사용자 인증(Authentication)의 특별한 요구를 이용하는 보안 구조의 새로운 형태를 제안한다. 그로 인해 다양한 네트워크 도메인 간의 동적 보안 등록(Association)을 가능하게 하고, 스마트카드 기반의 사용자 프로파일을 사용하는 로밍 코디네이터를 구현한다. 본 논문에서의 보안 프레임워크 구조는 이동 노드에서 서비스 설정을 위한 오버헤드와 프로토콜을 최소화하여 끊김 없는 로밍 서비스를 제공하며, 서비스 도메인 간의 보안 연계성의 관리에 관련된 문제를 해결한다. 또한 서비스와 성능 향상을 얻기 위해 지능적인 시스템 구조를 가지기 위해 보안 컨텍스트 모델을 구성한 스키마를 제안한다.

본 논문은 다음과 같은 구성을 갖는다. 본문 2장에서는 미래 무선 네트워크에서 보안과 로밍 서비스에 대한 관련 기술 및 연구를 소개한다. 3장에서는 로밍 서비스의 상호작용을 위한 보안 및 이동성 컨텍스트 모델을 구현한다. 4장에서는 로밍 코디네이터를 포함하는 보안 로밍 관리 프레임워크에 대해 설명한다. 5장에서는 테스트베드의 설계 및 어플리케이션 예제를 통해 성능 분석을 한다. 마지막으로 6장에서는 본 논문의 결론을 기술한다.

Ⅱ. 관련 연구

4G 모바일 네트워크는 다양한 기술과 구조가 상호 관계성을 지니는 복잡한 시스템이 될 것으로 기대되고 있다. 여러 가지 모바일 네트워크 서비스 영역과 통신 속도 및 관리체계를 가지고 상호 연결된 무선 네트워크로 인해 자연스럽고 끊김 없는 로밍을 위한 보안 기술과 사용자 인증 및 권한 설정과 같은 보안 기술의 상호작용, QoS의 보장, 정보 보호등 기본적인 특성이 요구된다.

기존 연구에서는 무선 네트워크간 자연스러운 로밍을 위해 IPv6에서 빠른 핸드오버 관리와 MIP-LR (Mobile IP Location Registers)의 강도를 결합시키는 통합 관리를 만들기 위한 다양한 연구가 진행되었다. VoWLAN (Voice over WLAN)에서의 보안 및 끊김없는 연동에 관한 연구[3]와 같이 무선랜 AP간 연동에 관한 연구도 진행되었다. 특히 3G와 무선랜 서비스를 통합하기 위한 해결책으로써 게이트웨이[4], 상호작용하는 기술과 구조[5], 로밍과 인증 서비스 프레임워크[6]에 관한 연구들이 진행되었다. 또한 상용화를 위해 가능한 방법에 관한[7] 연구는 주로 3GPP(3rd Generation Partnership Project)에서 연구되고 구성되었다. 그러나 현재까지 진행된 연구는 차세대 무선 네트워크에서 복잡하고 다양한 여러 환경 및 서비스 요구에 적응적이고 지능적으로 대처하기 위해 필수불가결한 특성인 로밍 관리 기술과 연계된 지식기반의 보안을 다루고 있지 않았다. 최근 연구[8]는 이동 통신과 IP 기반 웹 통신이 복합된 인증 환경과 사업자간 로밍을 구성하는 정책적인 고려를 포함하여 무선랜에서 로밍을 위한 정보 네트워크를 구성하는 방법이다. 하지만 이동통신-공동무선랜 네트워크에서 동적인 상호작용 로밍을 위한 끊김 없는 보안 코디네이터(Security Coordinator)의 문제는 QoS 보장을 만족시키는 것뿐만 아니라 보안 핸드오버 신호의 감소 측면에서 적절하게 고려되고 있지 않다.

본 논문은 4G 시스템에서 끊김 없는 상호작용을 위해 보안을 강화하고 사용자 프로파일을 지닌 컨텍스트

전송과 로밍 코디네이터를 포함한 능동적인 보안 스키마를 중심으로 구현한다.

Ⅲ. 퍼베이시브 로밍 서비스를 위한 보안 컨텍스트 모델

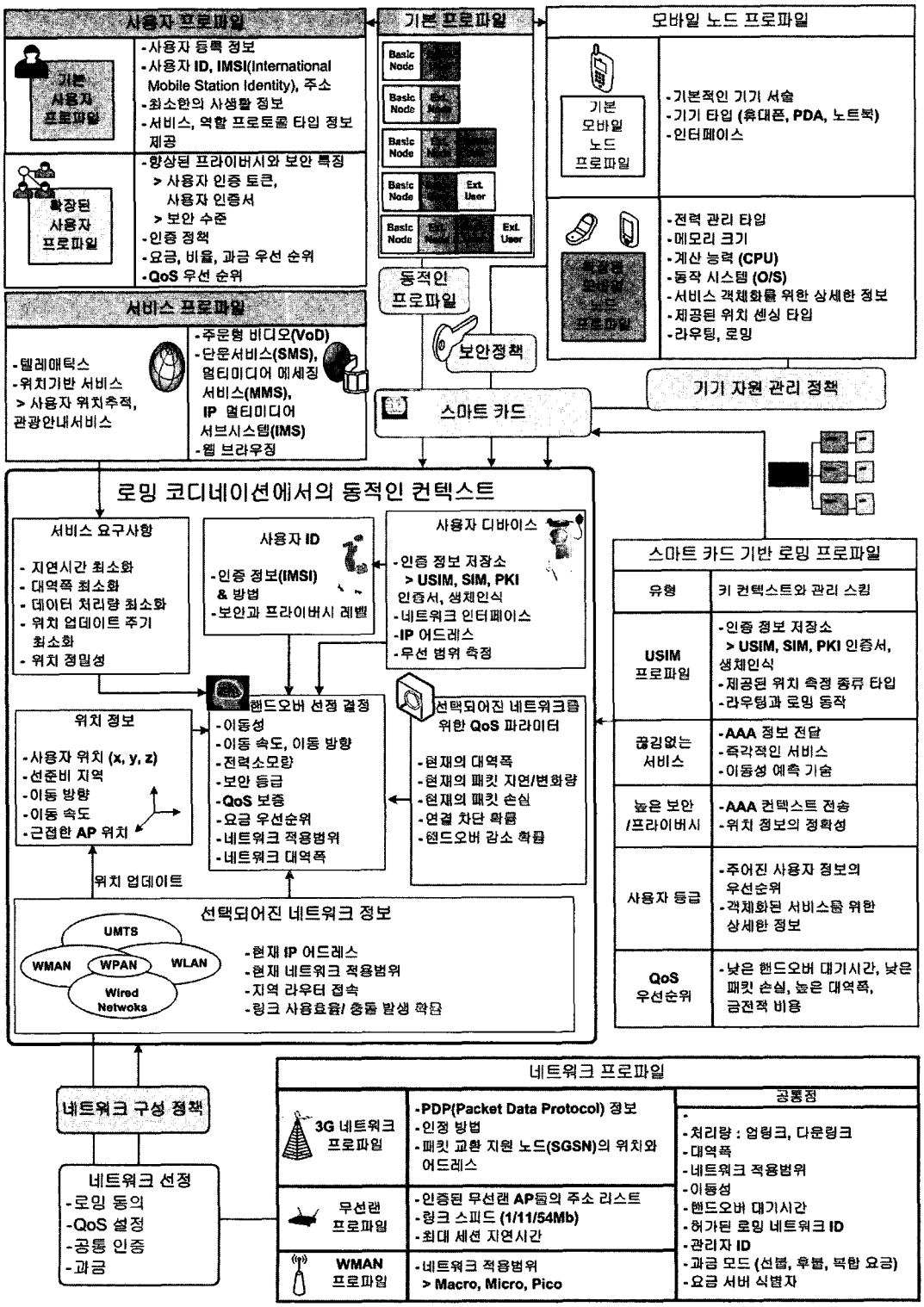
4G 네트워크와 같은 퍼베이시브 서비스 도메인에서 끊김 없는 로밍 서비스를 위해서는 사용자 정보가 간단한 형태로는 충분하지 않으며 체계적인 접근이 어렵기 때문에 충분한 컨텍스트 모델이 요구된다[9]. 그러나 일반적인 컨텍스트 정보는 관련 세부적인 정보가 굉장히 많으며 위치에 의존적이기 때문에 관리하기가 어렵다. 이런 이유로 이기종(Heterogeneous)의 무선 네트워크에서의 보안 로밍 관리를 위한 적응적이고 자동적인 기술을 적용할 수 있는 보안 컨텍스트 모델이 필요하다.

본 논문에서는 스마트카드 기반의 끊김 없는 보안 로밍 서비스를 제공하기 위해서 이동 노드의 이동에 관련되고 로밍에 필수적인 사용자의 인증 정보를 포함하는 보안과 이동 컨텍스트에 중점을 두어 컨텍스트 모델링을 수행하였다. 따라서 네트워크 장치에서 제공하는 정확한 컨텍스트를 수용하기 위해 〔그림 1〕과 같이 컨텍스트 모델을 제안한다.

본 논문에서는 로밍 사용자를 위한 최적의 서비스 환경을 제공하도록 컨텍스트 모델링에서 분류된 프로파일

〔표 1〕 퍼베이시브 서비스를 위한 요구사항

구 분	요구사항	스마트 카드에 있는 로밍 코디네이터와 사용자 프로파일의 자율적 서비스 관리
서비스	- 사용자가 사용하는 이동 기기의 설정 변경 없이 끊김 없는 서비스의 이동성 제공 - 대부분의 서비스의 이용은 연동 로밍 환경에서 동적 컨텍스트(Context)의 제한 조건으로 인해 선정의 필요	- 서비스를 선정의 하지 않고 이동 노드의 위치 변경에 따라 적응적이고 유동적인 서비스 제공 - 위치 정보를 사용하여 로밍 코디네이터를 통해 지능적으로 끊김 없는 서비스 제공
자원관리 및 QoS 지원	- 자원관리는 현재 네트워크 환경에 제한되어 있음 - 사용자 프로파일, 네트워크 특성에 의한 최적의 상태에서 고정적인 QoS 지원을 원함 - 버티컬 핸드오버 서비스에서 제한된 QoS 보장	- 선준비에 의한 이종 네트워크를 통해서 효과적인 자원 보존과 QoS 제공 - 로밍 코디네이터를 통해 통합적이고, 상호연동적인 위치 컨텍스트에 의해서 위치적으로 확인되지 않은 어플리케이션에서도 상황인식 QoS 보장이 강화된 서비스를 능동적으로 변경 가능하도록 보장 받음
보안 및 프라이버시	- 이종 무선 네트워크의 복잡한 보안문제 - 보안 설정 동적 재구성 기술 및 적응적이고 가벼운 보안 메카니즘 개발이 필요	- UMTS 인증, 키 허가(AKA)와 무선랜에서 확장 가능한 인증 프로토콜 EAP-AKA 또는 EAP-SIM을 기반으로 안전한 상호인증과 키 관리가 이루어짐. - 정확하고 빠른 AAA 상황 전환에 의한 핸드오버 전에 기존 AP/BS와 새로운 AP/BS 사이에 미리 신뢰 관계가 구축됨
상호작용	- 서로 다른 통신 패턴 및 네트워크 범위에 관한 지식 부족 - 동질 네트워크 사이의 상호작용 관리의 제한된 범위	- 다음 핸드오버를 위해 최적의 무선 네트워크를 추측하는 선준비에 의해 끊김 없이 상호작용 함 - 네트워크 범위, 위치와 이동 노드들의 사용자 프로파일 사이의 이질성을 고려하여 이종 네트워크의 로밍 코디네이터에 의한 광범위한 상호작용 관리
확장성	- 사용자가 로밍할 때마다 3G 네트워크의 홈 AAA 서버로부터 인증 받아야 함 - 인증 효율성을 고려해야함 - 수많은 이동 노드들은 로밍 지연 증가를 초래	- AAA 서버의 로드 균형을 지원하는 로밍 코디네이터로 인해 네트워크 확장 가능 - 로밍 코디네이터가 선 경고를 통해서 정확하고 빠른 AAA 상황 전환을 지원하여 지역 네트워크에서의 보안 능력을 높여주는 안전한 로밍 중계자 역할을 함
핸드오버 관리	- 핸드오버를 위한 새로운 AP/BS는 신호 세기에 의해 결정됨(반응적인 핸드오버)	- 먼저 위치 상황에 의한 최적의 새로운 AP로 핸드오버 - 로밍 코디네이터와 상황 전환을 통해 상황인지 핸드오버



〔그림 1〕 끊김 없는 로밍 서비스를 위한 보안 컨텍스트 모델

[10]과 동적 컨텍스트를 강화한다. 분류된 프로파일의 중요한 장점은 사용자의 특성화된 요구에 맞출 수 있는 QoS와 이동성 기반의 로밍 서비스를 위한 정보를 체계적으로 분류된 것이다. 예를 들어 사용자가 이기종 무선 네트워크 도메인 간을 이동하면 스마트카드에서 적절하게 프로파일 사용을 수정한다. 로밍 서비스를 제공하는 서비스 사업자의 입장에서는 수정된 컨텍스트 및 프로파일을 이용하여 사용자의 요구뿐만 아니라 서비스 사업자의 통신 자원을 적절하게 관리 할 수 있다. 따라서 사용자 프로파일에 기반한 로밍 메커니즘은 로밍 시 필요한 사용자 인증에서 서비스 보안과 사용자 인증정보 보호로 인한 자원의 부족을 최소화하며 서비스 제공에 필요한 보안 QoS를 최대화할 수 있다.

컨텍스트 특성에 따른 제안된 모델의 설계는 프로파일 타입(사용자, 모바일 노드, 서비스, 로밍과 네트워크 프로파일)에 따라 개인화, 특성화될 수 있어 기존 로밍 정보 관리 방법에 비해 사용자의 서비스 QoS에 적응적일 수 있다. 이와 같은 프로파일 종류는 정책 서버(Policy Server)와 컨텍스트 전송 프로토콜에 따라 사용하기 위한 개별적 특성화가 기재되며, 부가적인 항목들과 같이 저장된다. 그리고 자주 내용이 변경되는 동적 컨텍스트로는 현재의 사용자 위치, 사용자 기기, QoS와 서비스 요소 같은 사용자 및 네트워크에 관련된 필요 정보가 포함된다. 또한 동적 컨텍스트에는 로밍과 핸드오버 변수를 포함해야 한다.

이와 같은 사용자 프로파일, 클래스 프로파일, 이동 노드 프로파일, 서비스 프로파일, 네트워크 프로파일등으로 구성된 프로파일들과 함께 스마트카드로 관리되는 로밍 프로파일을 포함하여 동적 컨텍스트에 따라 적절한 로밍 정책을 구현할 수 있다. 동적 컨텍스트에서 분류된 것처럼 사용자의 네트워크 선택 및 설정은 사용자의 위치 정보 및 QoS 파라미터, 사용자 기기, 사용자 정보, 서비스의 형태에 따라 로밍을 위한 핸드오버를 결정할 수 있도록 구성되어진다.

다음 장에서는 모델 구성 결과에 기반을 두어 실제 이동 노드의 네트워크 간 이동에 따라 로밍을 하는 경우 필요한 보안을 적절하게 관리 할 수 있는 보안 관리 프레임워크를 제안한다.

Ⅳ. 퍼베이시브 로밍을 위한 보안 관리 프레임워크

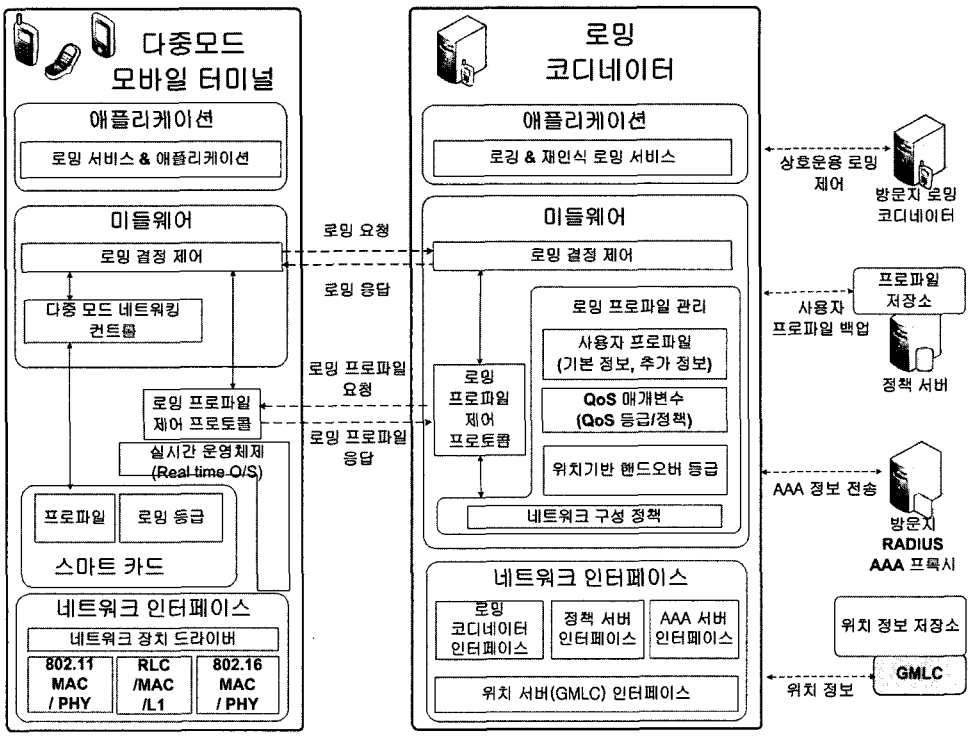
4.1. 시스템 구조

이동 노드들 사이에서 정보를 전송하는 네트워크 경로를 동적으로 찾는 능력은 이기종 네트워크의 기본이다. 링크 계층에서 차이가 있는 여러 네트워크 도메인으로 구성된 경우 당연히 단말의 물리 계층에서의 연결성은 필수적이지만 링크 계층이나 네트워크 계층 및 상위 응용 계층을 포함한 서비스의 로밍 및 연계가 자동적으로 되는 것은 아니다. 그 중에서도 이동 통신-공중무선랜 환경에서의 관점에서만 본다면, 네트워크 특성이 차이가 나는 네트워크 도메인 간의 상호운용 로밍(Interoperator Roaming)을 지원하기 위해서는 서로 다른 물리 계층을 수용할 수 있는 듀얼 모드(Dual Mode) 터미널이나 적절한 네트워크 계층으로의 장치, 게이트웨이를 포함한 네트워크에 사용하기 적합한 스위치 등이 요구되고 있다. 또한 상이한 네트워크에서 접근이 가능한 사용자인지 결정하는 사용자 인증을 비롯한 통합 또는 연계 보안 서비스가 필요하다.

본 논문에서 제안하는 로밍 코디네이터와 스마트카드에서 분류된 프로파일을 가지고 있는 보안 로밍 프레임워크는 로밍 시 끊김 없는 보안 서비스를 위한 모든 프로토콜 순서를 사용자의 선택이나 모바일 노드의 추가적인 과정을 포함하지 않으면서도 로밍을 위한 컨텍스트 전송 후보(Context Transfer Candidate)를 성립할 수 있도록 하는 보안 관리 프레임워크이다. 그림 2 에서는 보안 관리 프레임워크에서 제안하는 기본 구조로서 로밍 서비스를 지원하는 로밍 코디네이터와 이동 통신-공중 무선랜 사이의 연동이 가능한 다중 모드 이동 노드(Multi-mode MN)를 보여주고 있다. 앞에서 제시한 [표 1]에서는 4G시스템에서의 필요성 분석을 통해, 본 논문에서 제안하고자 하는 프레임워크의 장점에 대하여 설명하고 있다.

다음은 본 논문에서 구현한 보안 관리 프레임워크의 특징을 3GPP에서 제안한 기술제안서(Technical Specification 22.934)에 포함된 상호작용 측면과 실제적인 시스템에 기반하여 설명한다.

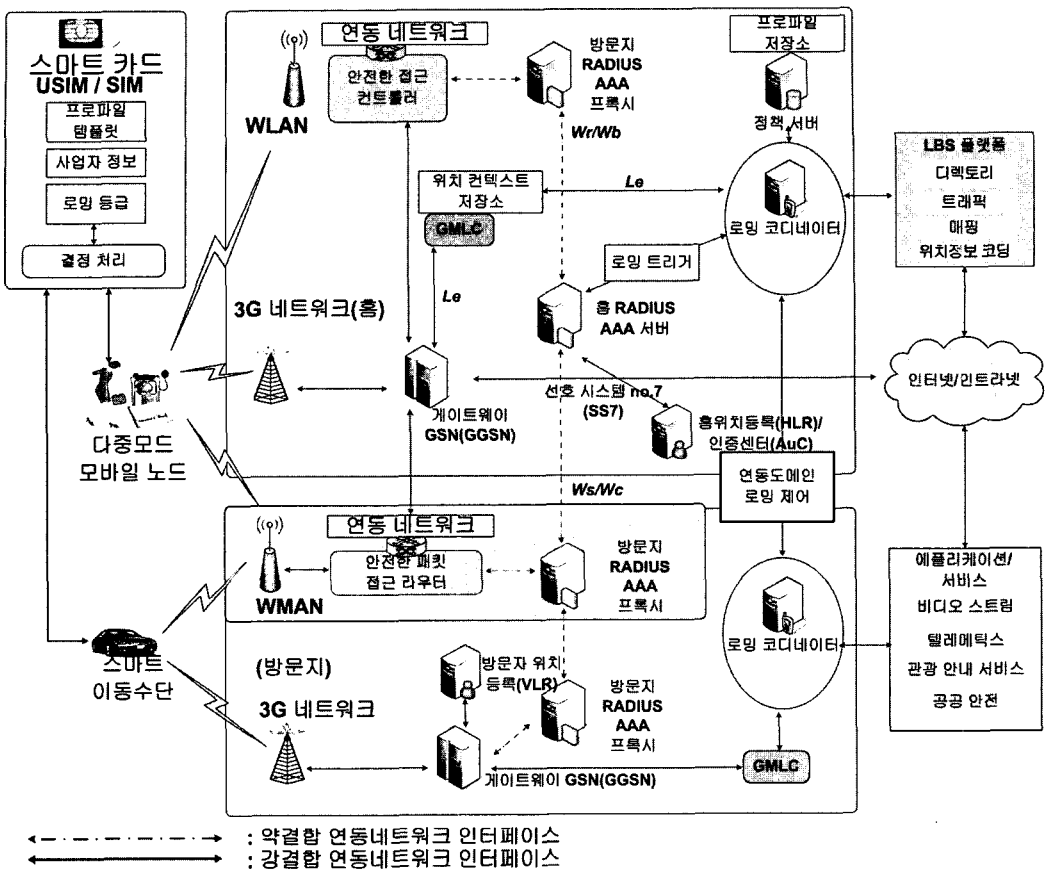
보안과 인터네트워킹 측면 : 이동 노드가 3개의 네트워크 인터페이스 (3G, 무선랜(WLAN), WMAN)를 가진 트리플 모드(Triple-mode) 터미널이라고 가정한



〔그림 2〕 끊김 없는 로밍 서비스를 위한 제안된 기본 구조

다. 모든 네트워크들이 보안을 유지하기 위해서는 연계된 네트워크 도메인들은 보안이 보장되는 인증과 키 관리를 고려해야 한다. 기존 시스템의 인증과 키 관리는 무선랜 환경을 위한 EAP(Extensible Authentication Protocol)와 UMTS(Universal Mobile Telecommunications System)를 위한 인증과 키 관리 (AKA - Authentication and Key Agreement) 기술이 있다. 실제적인 보안 관리 프레임워크를 제안하기 위해서는 이와 같은 기존 시스템에서의 기술에 기반한 설계가 필요하다. 따라서 3G/WLAN 연동을 위한 실행 가능한 연구를 위해 연계 네트워크는 3GPP에 의해 연결되어야 한다. 일반적인 약결합(Loosely Coupling) 방식은 사용자가 무선랜과 3G에서 PS(Packet-Switched) 서비스에 접속 허가 및 서비스 세션동안 3G와 무선랜 네트워크를 바꾸기 위한 접속을 허가하는 방식이다. 강결합(Tightly Coupling) 방식은 무선랜이 3G 네트워크의 GGSN (Gateway GPRS support node)와 연결되어 3G 네트워크 접속 인터페이스와 무선랜 인터페이스의 밀접한 네트워크 연결을 제공한다. 이러한 솔루션의 이점은 UMTS 네트워크에서의 보안, 이동성, QoS를 위한 메커니즘으로 즉시 재사용될 수 있다는 것이다. 또한 IEEE 802.16 표준에 있는 WMAN과의 연동도 고려해야 한다. 따라서 본 논문에서는 다양한 네트워크 인터페이스를 위해[11]에 명시되어 있는 정의와 기능 분류를 채택한다.

상호운용 로밍 측면 : 연동 네트워크 구조의 확장 가능한 관리를 위하여 로밍 코디네이터의 구현과 로밍 코디네이터간의 협력에 의해 로밍 관리 중심이 분산되어야 한다. 따라서 서비스 도메인 내부(Micro-mobility)에서 필요한 AAA 서비스는 로밍 코디네이터와 AAA 서버가 같이 연동하여 구성한다. 그리고 이동 노드가 다른 서비스 도메인으로 이동(Macro-mobility)할 경우에서는 로밍 코디네이터 그리고 AAA 프록시(Proxy)들과 AAA 서버들이 협력하여 재인증 과정을 담당한다. 이 경우 발생하는 신호 오버헤드를 최소화하기 위해 AAA를 위한 컨텍스트 전송 프로토콜을 이용하여 홈 PLMN(Public Land Mobile Network)의 AAA 서버와 AAA 프록시 간에 빠른 안전한 로밍을 가능하게 한다.



HLR : Home Location Register
AuC : Authentication Center
(U)SIM : (Universal) Subscriber Identity Module
GGSN: Gateway GSN (GPRS Support Node)
CGW : Charging Gateway
HSS : Home Subscriber Server
PLMN : Public Land Mobile Network

VLR : Visitor Location Register
SS7 : signaling system no. 7
LBS : Location Based Service
GMLC : Gateway Mobile Location Center
CGF : Charging Collection Function
IMS : IP Multimedia System

Le : 외부 사용자와 모바일 위치 센터(외부 인터페이스)간의 인터페이스
Wr/Wb : 안전한 방법으로 무선랜과 **3G**망 또는 홈 **PLMN** 간 **AAA** 신호를 전송하는 인터페이스
Ws/Wc : 3G AAA 프록시와 **3G AAA** 서버 간에 실행되는 인터페이스이지만, **Wr/Wb**와 같은 기능을 제공
D'/Gr': 3G AAA 서버와 **HLR** 간 서명 정보를 교환하기 위해 사용하는 선택적인 인터페이스

〔그림 3〕 이동 네트워크에서의 제안된 스마트 카드 기반 보안 로밍 관리 프레임워크

로밍 코디네이터 디자인 측면 : 재구성 가능한 구성 요소를 가진 로밍 코디네이터의 추상적 계층을 기존 연구 모델[12]과 같이 비슷한 미들웨어 플랫폼으로 고려하고 있다. 일반적으로 미들웨어 플랫폼은 분산처리를 위한 가상 실행 환경이다. 따라서 미들웨어에서는 선인증을 통한 빠른 안전한 로밍을 이동 노드들에게 제공하며 이동노드와 AAA 주체간의 상호작용을 하는 로밍 코디네이터를 포함한다. 로밍 요청(Roaming Request)을 받은 후에 로밍 코디네이터는 이동 노드의 로밍 프로파일을 평가한 후 AAA 컨텍스트 전송을 수행한다. 네트워크 인터페이스 모듈은 다른 로밍 코디네이터, 정책 서버들이 가지고 있는 프로파일과 AAA 관리의 상호 작용을 수행하기 위한 여러 인터페이스를 포함 한다. 본 논문에서 주장하는 주요 제안은 상호 동작하는 네트워크에서 다른 적절한 네트워크를 인정하기 위해 낮은 계층에서의 로밍 컨텍스트(Roaming Context) 인터페이스와 로밍 코디네이터에서의 로밍 결정 제어(Roaming Decision Control)이다.

네이밍(Naming)과 주소할당(Addressing) 측면 : 사용자 ID는 3GPP 에 따라 NAI(Network Access Identification) 포맷에 기반한다. 특별히, IMSI (International Mobile Subscriber Identity)는 로밍 코디네이터에서의 사용자 ID로써 사용한다.

이동 노드 설계 측면 : 로밍 제어 기능은 단대단 서비스처럼 이동 노드에서도 포함되어져야 한다. 대체적으로 자원의 제한으로 인해, 로밍 제어 모듈은 단지 하나의 운영체제 플랫폼으로 간주된다. 따라서 이동 노드의 미들웨어 계층은 제한된 가상 실행 환경을 가지고, 전형적으로 엄격히 제한되어 진다. 로밍 코디네이터와 비교해서 스마트카드는 새로운 구성요소이다.

스마트카드 기반의 인증 측면 : 로밍 코디네이터 접속을 위한 이동 노드는 UICC(Universal IC Card) 리더기(스마트카드 리더기는 마이크로 소프트 윈도우즈 플랫폼이 탑재되어 있는 표준 장치로써 구현함)를 실행시킨다. UICC 리더기는 인증 정보를 얻기 위해 UMTS용 SIM 카드와 상호 작용을 한다. 사용자 확인과 사용자용의 분류된 프로파일을 포함하는 스마트카드는 이상적으로 전자 지갑처럼 사용자 인증 서비스에 사용될 수 있다.

4.2. 로밍 코디네이터를 통한 부가 서비스

운영자의 관점으로부터 이동통신-공중무선랜 네트워크에서의 로밍 코디네이터는 예를 들어 위치기반서비스(LBS: Location Based Service)와 같은 부가 서비스로부터 부가적인 항목을 제공할 수 있는 위치에 있다. 사용자는 이동 네트워크 서비스의 일부분으로써 위치기반 서비스가 익숙하다. 이동통신-공중무선랜 네트워크에서 위치 정보는 두 가지 모든 타입으로부터 가능할 것이다. 3G 이동통신 네트워크에서 위치 서비스(Location Service)는 GMLC(Gateway Mobile Location Center)나 MLC(Mobile Location Center) [13]에서 논리적으로 만들어 진다. 그러나 로밍 코디네이터는 GMLC 인터페이스로부터 공간 히스토리를 가져올 수 있다.[14] 따라서 이동 노드들이 무선랜을 사용했을 때 이동노드의 위치는 이동노드에 의해 받아지는 무선랜 AP(Access Point)의 MAC 주소에 기반을 둔 핫스팟이나 AP에서의 위치를 참조 실행함으로써 결정될 수 있다.

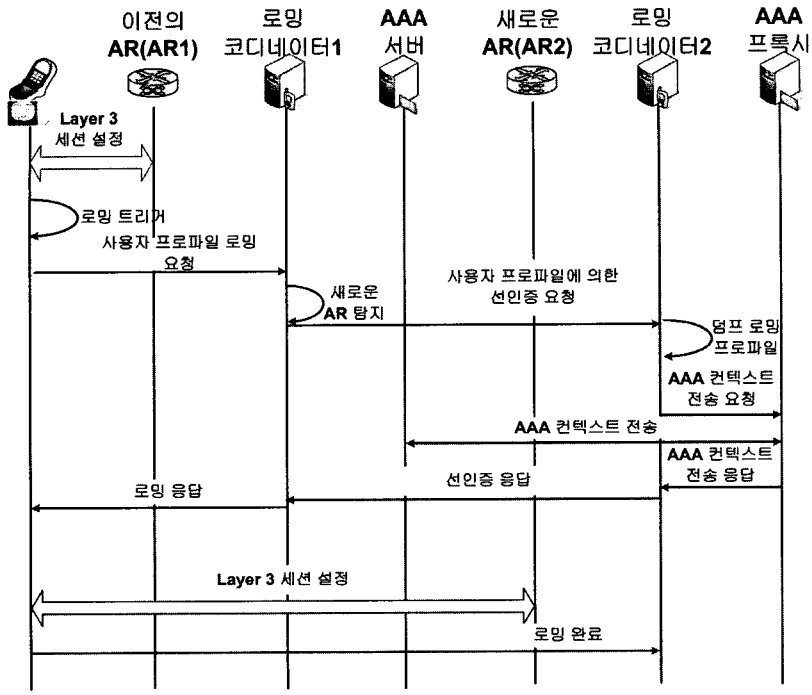
이동통신-공중무선랜 연동 네트워크에서 비즈니스 모델의 일치를 위해 미리 이동통신 사업자는 제공되는 무선랜 사업자와 로밍의 일치를 설정하고 무선랜과의 네트워크를 허용해야 한다. 따라서 제안된 로밍 코디네이터의 소유권은 사업자간 로밍을 허용하는 것으로써 중요할 것이다.

또한 로밍 코디네이터는 보안이 적용되지 않은 어플리케이션이나 서비스에서의 숨겨야할 사용자 위치 정보에 대해 책임이 있기 때문에 기기마다 개별적인 인증을 해야만 한다. 그래서 일반적으로 홈 3G 사업자가 로밍 코디네이터를 소유하고 동작시키는 것으로 가정한다. 따라서 다른 부가 서비스 공급자는 로밍 코디네이터를 소유한 사업자로부터 자신의 서비스에 가입한 사용자에게 위치기반 서비스를 제공할 수 있다. 이미 현재에도 존재하는 이와 같은 서비스 독점은 새로운 플레이어가 시장으로 들어가기 어렵게 되어있다. 따라서 로밍 코디네이터의 소유권은 상호연동 시스템으로 갈수 있는 주요한 필수 기능 중에 하나이다. 또한 로밍 코디네이터의 소유권을 시장의 성장에 따라 허가된 로밍 권한을 설립하는 것이 바람직 할 것이다. 만일 로밍 코디네이터가 공동으로 접근이 용이하다면 새로운 부가 서비스 공급자들의 시장으로의 진입이 훨씬 쉬워질 수 있기 때문이다.

4.3. 안전한 로밍 프로토콜(Secure Roaming Protocol) 기반의 USIM

본 논문에서 제안하는 보안 프레임워크의 장점인 범용적인 로밍 연계와 같은 중요한 이점과 요구사항을 강조하기 위해 기존 SIM 기반의 이동통신-공중무선랜 로밍 연구뿐만이 아니라 광대역 로밍 프로토콜 기반의 USIM의 동작 예를 보인다. 유비쿼터스 컴퓨팅 환경에서 끊김 없는 이동성과 보안 요구사항을 충족하기 위해서는 보안 버티컬 핸드오버(Vertical Handover) 프로토콜의 생성이 중요하다. 이와 같은 로밍을 위한 보안 핸드오버(Handover) 프로토콜은 서로 다른 형태의 네트워크[15] 사이를 이동하는 사용자를 위한 것이다. 게다가 끊김 없는 로밍 서비스에서 주요 문제의 하나는 어떻게 핸드오버 중에 보안 컨텍스트를 즉시 보안에 문제없이 교환하는가이다.

일반적인 SIM 기반의 셀룰러 사용자는 초기에 약간의 장애가 있다. 주로 SIM 카드/리더, 드라이버와 다양



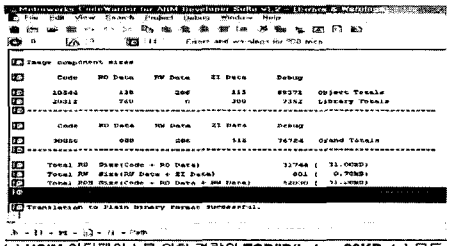
〔그림 4〕 보안 로밍 상호동작을 위한 로밍 프로토콜

한 요소들 사이의 복잡한 상호작용처럼 사용자가 로밍을 위해서는 클라이언트 측면에서 너무도 많은 장치의 설정이 필요하다. 이러한 요구를 맞추기 위해서 우리는 로밍 정보를 자동적으로 등록, 관리하고 끊김 없는 세션 전송을 지원하는 지능적 로밍 프로토콜을 제안한다. 〔그림 4〕에서의 예에서 상호 도메인 간의 보안 로밍을 적용하는 메시지 전송 프로토콜을 보여준다. 제안된 프로토콜은 로밍 코디네이터의 추가적인 로밍 제어 신호의 전송에서 사용자를 위해 로밍을 위한 세션의 연결을 위한 잠재 시간을 감소시키는 것을 돕는다. 그림 4에서 보이는 예제는 상호 동작하는 로밍에서 로밍 코디네이터 사이의 상호작용을 나타낸다. 우선 이동노드는 새로운 AP를 감지하고 목적하는 AR(Access Router)를 선택한다. 다음으로 AR1에서 AR2로의 요청은 현재의 로밍 코디네이터에서 나온다. 이러한 로밍 코디네이터는 AR2가 다른 도메인에 위치되어 있는 것을 감지해야만 한다. 로밍 요청은 이후에 새로운 도메인으로부터 보안 선 등록(Pre-association)을 요청하기 위해 로밍 코디네이터1로부터 로밍 코디네이터2로 보내진다. 요청 메시지의 검증 후에, 로밍 코디네이터2는 이동노드의 로밍 프로파일을 평가하고 AAA 서버와 AAA 프록시 사이에 AAA 컨텍스트 전송을 일으키도록 한다. 이와 같은 구조의 결과에 따라 로밍 코디네이터2는 인증 결과에 관해 이동노드에게 알리고, 로밍 코디네이터1에게 등록(Association) 결과에 대한 응답 메시지를 전송한다. 만일 선 인증이 성공하게 되면 로밍 코디네이터2는 이동노드로부터 로밍 인증 메시지를 기다린다. 그러나 무한정 기다릴 수 없기 때문에 이동노드로부터 로밍 인증 메시지를 특정 시간 내에 받지 못하면 로밍 코디네이터2는 이동 노드가 미리 결정한 AR2로 이동하지 않았음으로 판단하게 되고 설정된 선인증은 자동적으로 취소된다. 이와 같이 제안된 로밍 프로토콜은 로밍시에 필요한 보안 컨텍스트를 로밍 코디네이터끼리의 연동을 통해 기존 AAA 구조인 인증서버와 프록시를 통해서 빠른 로밍 응답을 가능케 하여 서로 다른 사업자간의 로밍도 가능하게 할 수 있는 장점을 가진다.

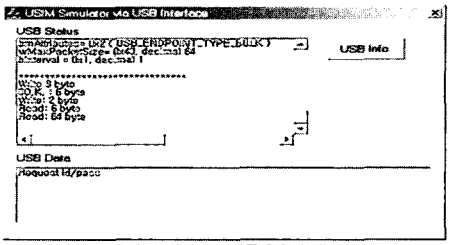
V. 테스트 베드 구현과 어플리케이션의 예

5.1. 시스템 구축

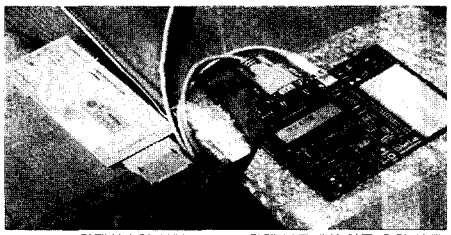
본 논문에서 제안된 보안 프레임워크는 기존 로밍 구조와는 USIM 기반의 사용자 프로파일을 도입함으로써 클라이언트의 부담을 감소하면서 보다 안전하게 보안



(a) USIM 인터페이스를 위한 경량의 TCP/IP(below 30KByte) 모듈



(c) 모바일 터미널에서 인증 처리 상태



(b) USB 인터페이스가 연결된 USIM 타켓 보드에서 인증 요청 상태

〔그림 5〕 테스트베드에서 인증 예제에 기반한 USIM

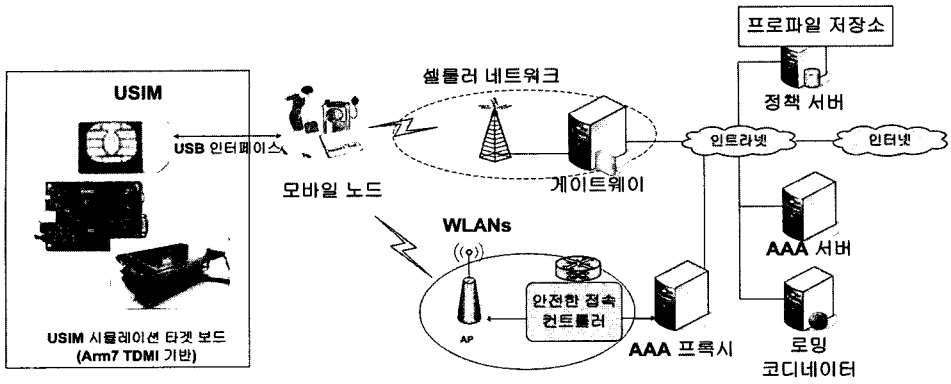
컨텍스트를 관리할 수 있도록 도와준다. 그러나 USIM이 포함되어야 하기 때문에 USIM을 사용하지 않는 기존 공중무선랜 또는 WMAN에서 검증하기 어려운 부분이 있다. 따라서 이번 장에서는 실제와 비슷한 환경을 구현하여 제안된 프레임워크가 실제 서비스의 가능성을 검증하고자 한다.

다음 〔그림 6〕은 제안된 보안 로밍 프로토콜 및 프레임워크의 가능성을 보여주고, 이동통신-공동무선랜 구조에서의 실행 가능성을 검증하기 위해 개발된 테스트베드를 나타낸다. 제안된 프로토콜 및 프레임워크를 일부 테스트베드로 구현하고, 성능을 측정하기 위해 일부는 시뮬레이션 형태로 구현하였다. 실제로 그림 5에서 보듯이 로밍 코디네이터를 통한 보안 로밍 관리의 테스트베드와 시뮬레이션 환경에서의 보안 컨텍스트 전송을 개발하였다.

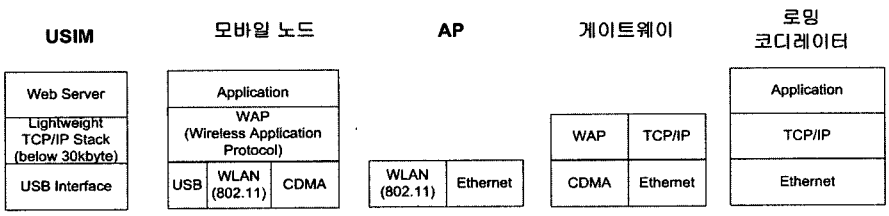
로밍 코디네이터(펜티엄 III 933MHz), 정책 서버와 AP들은 512MB RAM의 Solaris 8서버에서 동작한다. AAA 서버와 AAA 프록시는 펜티엄 III 800MHz의 리눅스 OS 기반 서버와 쉽게 확장이 가능한 RADIUS (Remote Authentication Dial-In User Service) 기능을 구현할 수 있는 FreeRADIUS[16] 라이브러리를 수정하여 적용하였다. 여기서 AP는 Lucent Orinoco 802.11b 무선랜 네트워크 인터페이스 카드를 포함한 펜티엄 III 500MHz 리눅스 OS 기반에서 네트워크 인터페이스 카드 드라이버를 AP 모드로 동작할 수 있도록 드라이버를 수정하고 보안 로밍 관련 과정을 구현하였다. 그리고 이동 노드는 같은 무선랜 네트워크 인터페이스 카드와 CDMA 무선랜 듀얼 모드 네트워크 카드가 장치된 랩톱을 사용하였다. 이동 노드의 플랫폼은 펜티엄 III 800MHz, 256MB 램의 윈도우 XP OS이다. 그러나 USIM을 사용한 셀룰러 인증 플랫폼을 시뮬레이션 하기 위해서는 대부분의 USIM이 ARM7에 기반을 둔 프로세서를 사용하기 때문에 3G 네트워크와 WLAN 모두 사용되는 인증 정보를 획득하기 위해 상호 전달하는 USIM 시뮬레이터 타겟 보드로 써 441FX 보드(ARM7TDMI)를 사용하였다. 사용된 프로그래밍 언어는 GNU C(Cross Compiler), C, C++ Compiler와 ADS(ARM Developer Suite) v1.2이다. 또한 이동 노드의 GUI를 위해 Visual C++ 6.0을 사용하였다. 사용된 암호 라이브러리는 OpenSSL 0.9.7c[17]이고 토큰 검증에서 데이터 사이즈는 1KB, 로밍 컨텍스트 전송에서 10KB이다.

5.2. 시스템 적용 및 논의 사항

로밍 이슈를 바탕으로 본 논문에서는 서비스 도메인이 다르거나 같은 경우 서로간의 EAP-TLS, EAP-AKA 같은 실제 로밍 서비스 모두에서 대부분 적용되는 보안 프로토콜의 성능 평가를 수행하였다. 또한 사용된 USIM 타켓 보드에서 구현된 가벼운 로밍 컨트롤과 TCP/IP 모듈은 32비트 프로세서와 31.28 KByte의 사이즈의 일반적인 스마트카드와 호환성이 있도록 구현하



(a) 이동통신-공중무선랜 로밍 테스트베드 구조



(b) 프로토콜 스택

〔그림 6〕 모바일 네트워크에서 제안된 보안 로밍 관리를 위한 테스트베드

였기 때문에 성능을 미리 예상하는데 아무런 문제가 없다. 〔그림 6〕은 보안 프로토콜이 동작하는 USIM 타겟 보드에서 인증 처리 상태와 모듈 사이즈를 보여준다. 우리의 로밍 방식은 핸드오버가 발생되기 이전에 앞서서 AAA 컨텍스트를 설정하고, 그 다음 로밍 코디네이터가 성공적으로 수행한 다음 로밍 네트워크를 제공한 후 토큰 검증을 수행한다. 다음 핸드오버를 위한 AR는 사용자의 인증 정보를 갖는다. 사용자는 핸드오버를 위한 각 인증을 AAA 서버로부터 얻지 않기 때문에 제안된 로밍 메커니즘은 부가적인 재인증 지연을 피한다. 그러므로 이동 노드는 로밍 코디네이터를 가진 보안 지식기반 핸드오버 프로토콜을 사용할 때 비교적 낮은 지연시간을 제공한다. 또한 AAA 서비스 관리의 강도는 로밍 코디네이터에 기반하며, 로밍 코디네이터를 사용함으로써 증가하는 자원 소비 대신에 보안 QoS를 제공하는 USIM에서 프로파일을 분류함으로 로밍 코디네이터에 걸리는 서비스 부하를 감소시킨다. 〔표 2〕는 실제 동작 시나리오에 기반한 테스트 베드에서 측정한 결과이다.

물론 실험한 테스트베드 실제 시스템에 비교하여 다양한 환경 요소가 고려되지 않았으며, 시스템 환경 역시 제한적이다. 그러나 실험 결과를 검토해 보면 상호연동이 되는 네트워크에서 이동 노드의 이동에 따라 성능에 많은 영향을 주지 않을 정도의 충분한 로밍 제어 기능을 수행할 수 있음을 보여준다. 〔표 2〕에서 보듯이 기존 EAP-SIM 인증을 이용해 핸드오버를 수행한 경우 3,313ms정도의 시간이 필요하지만 제안된 로밍 코디네이터를 통한 AAA 과정의 단축 및 위임이 가능하다면 1,153ms정도의 지연시간만이 필요할 뿐이다. 따라서 제안된 보안 프레임워크에서 지식기반 로밍 메커니즘은 퍼베이시브 서비스에서 다양한 서비스 도메인 간 로밍이 활발한 서비스 구조에서 사용하는 것이 가능할 것이다.

Ⅵ. 결 론

본 논문에서는 퍼베이시브 로밍 서비스(Pervasive roaming service)에서 사용자 인증 및 신뢰성 확보를 위한 구체적인 요구사항들을 도출하고 로밍을 위한 보안 컨텍스트를 USIM 기반의 사용자 프로파일을 이용하고 보안 컨텍스트를 관리하기 위한 로밍 코디네이터를 도입하여 보안 프레임워크 구조를 설계하였다. 또한 스마

〔표 2〕 테스트 베드에서의 성능 측정 결과

장치	동작 시나리오	성능
인증 과정 (Association, Authentication)		
이동 노드-AP	무선랜에서 AP를 찾기 위한 지연시간	40~300ms
이동 노드-AP	무선랜에서의 IAPP를 사용한 재인증 지연시간	40ms
이동 노드-AAA	802.1X 기반의 EAP-TLS를 사용한 인증 지연시간	1,600ms
다중 분할 다중 접속(CDMA)	CDMA 장치에서의 사용자 인증을 위한 최종 지연시간	4,300ms
컨텍스트 전송과 핸드오버		
이동 노드-AP	무선랜에서의 4-way handshake를 이용한 빠른 핸드오버	60ms
이동 노드	무선랜에서의 USIM 의 인증 토큰을 통한 로밍 요청 시 발생한 지연시간	30.34 ms
로밍	인증 토큰을 통한 상황정보 전달 트리거 전송 지연시간	27.4 ms
접근	파라미터를 이용하여 인증 토큰 처리 (512비트 키를 사용한 RSA 암호화)	31.201 KB/s
접근	AAA 컨텍스트 설치	200 ms
접근	3DES 대칭키 암호화를 사용한 토큰 검증	1.090 MB/s
무선랜(WLAN)/ 다중 분할 다중 접속(CDMA)	무선랜과 CDMA 망에서의 로밍을 위한 TCP 파라미터 조정	5,000ms
AAA 프록시/AAA 서버	AAA 상황정보 전달 응답	25ms
로밍 딜레이		
UMTS-무선랜	단일 UMTS 도메인에서 EAP-SIM 인증을 통해 무선랜 핸드오버 지연시간	3,313ms
UMTS-무선랜	단일 UMTS 도메인에서 인증 기반 USIM과 로밍 코디네이터를 통한 무선랜 핸드오버 지연시간	1,153ms

트카드와 같은 매체를 이용하여 사용자 프로파일들을 분류하는 로밍 코디네이터를 제안하고, 이를 이용해 자동 상황 관리(Autonomic Context Management)가 가능한 구조를 제안하였다. 그리고 이종 네트워크에서의 다양한 네트워크 도메인을 이용하여 자동적인 보안 등록(Association)의 로밍을 가능하게 하였다.

또한, 본 논문의 보안 프레임워크는 USIM 기반의 사용자 프로파일을 이용하여 모바일 노드들의 통신 및 계산 처리량을 최소화하면서, 로밍 서비스에서 보안관계들의 관리와 연계 문제를 해결하였다. 그리고 본 논문에서는 성능 분석 결과를 기반으로 제안한 퍼베이시브 로밍 서비스를 위한 보안 프레임워크에 대한 시스템 및 서비스 측면에서의 성능 향상을 검증했다. 이는 기존 시스템에서 지능적 모델의 추가 구현이 가능함을 보여준다.

앞으로 제안한 보안 구조를 기반으로 보안 웹 서비스 인프라[10]와 새로운 상호 작용 시스템[18][19]과 같은 기존의 제안된 보안 및 이동 메커니즘을 통합하여 퍼베이시브 서비스를 위한 보안 관리 프레임워크를 확장할 계획이다.

참고문헌

〔1〕 Keith Mayes, Konstantinos Markantonakis, F.P.: Smart card based authentication- any future? Computers & Security 24 (2005) 188-191.

〔2〕 Nicolas Montavont, e.a.: Handover management for mobile nodes in ipv6 networks. IEEE Commun. Mag. 40 (2002) 38-43.

〔3〕 김미연,김계진,이동훈, "VoWLAN 보안 및 로밍 설계," 정보보호학회논문지, 2005.

〔4〕 Feng, V. W.-S., e.a.: Wgsn: Wlan-based gprs environment support node with push mecha-

nism. The Computer Journal 47 (2004) 405-417.

[5] Salkintzis, A.K.: Interworking techniques and architectures for wlan/3g integration toward 4g mobile data networks. IEEE Wireless Commun. Mag. 11 (2004) 50-61.

[6] Minghui Shi, Xuemin Shen, M.J.: Ieee 802.11 roaming and authentication in wireless lan/cellular mobile networks. IEEE Wireless Commun. Mag. 11 (2004) 66-75.

[7] 3rd Generation Partnership Project (3GPP): Feasibility study on 3GPP system to wireless local area network (WLAN) interworking. Technical Report TR 22.934, 3rd Generation Partnership Project (3GPP) (2003).

[8] Jenq-Shiou Leu, Rong-Horng Lai, H.I.L.W.K.S.: Running cellular/pwlan services: practical considerations for cellular/pwlan architecture supporting interoperator roaming. IEEE Commun. Mag. 44 (2006) 111-122

[9] Sasitharan Balasubramaniam, e.a.: Vertical handover supporting pervasive computing in future wireless networks. Computer Communications (2004).

[10] Lee, M., Kim, J., Park, S., Lee, J., Lee, S.: A secure web services for location based services in wireless networks. In Mitrou, N., Kontovasilis, K.P., Rouskas, G.N., Iliadis, I., Merakos, L.F., eds.: NETWORKING 2004. Volume 3042 of Lecture Notes in Computer Science., Springer (2004) 332-344.

[11] 3rd Generation Partnership Project (3GPP): 3gpp system to wireless local area network (wlan) interworking;system description (release 6). Technical Report TR 23.234, 3rd Generation Partnership Project (3GPP) (2005).

[12] Prehofer, C., Wei, Q.: Active networks for 4g mobile communication: Motivation, architecture and application scenarios. In: Proc. IWAN 2002. (2002)

[13] 3rd Generation Partnership Project (3GPP): Functional stage 2 description of location services (lcs) (release 7). Technical Report TS 23.271, 3rd Generation Partnership Project (3GPP) (2005).

[14] 3rd Generation Partnership Project (3GPP): Feasibility study on location services (lcs) for wireles local area network (wlan) interworking (release 7). Technical Report TR 22.935, 3rd Generation Partnership Project (3GPP) (2005).

[15] McNair, J., F.Z.: Vertical hando®s in fourth-generation multinetwork environments. IEEE Wireless Commun. Mag. 11 (2004) 8-15.

[16] FreeRADIUS: (http://www.freeradius.org)

[17] OpenSSL: (http://www.openssl.org)

[18] Lee, M., Kim, G., Park, S., Jun, S., Nah, J., Song, O.: E±cient 3G/WLAN interworking techniques for seamless roaming services with location-aware authentication. In: NETWORKING 2005. Volume 3462 of Lecture Notes in Computer Science., Springer (2005) 370-381.

[19] Lee, M., Kim, G., Park, S.: Seamless and secure mobility management with location aware service (LAS) broker for future mobile interworking networks. Journal of Communications and Networks 7 (2005) 207-221.

〈著者紹介〉

김 관 연 (Gwanyeon Kim) 학생회원
2001년 2월 : 중앙대학교 전자공학과 졸업
2003년 2월 : 중앙대학교 전자공학과 석사
2007년 2월~현재 : 중앙대학교 전자전기공학부 박사과정
<관심분야> 홈네트워크, 정보보호, 유비쿼터스컴퓨팅

황 지 온 (Zion Hwang) 학생회원
2003년 2월 : 중앙대학교 정보 시스템학과 졸업
2005년 2월 : 중앙대학교 전자전기공학부 석사
2005년 9월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크, 지식기반 서비스 아키텍쳐 등

김 용 (Yong Kim) 학생회원
2004년 2월 : 중앙대학교 전자전기공학부 졸업
2006년 2월 : 중앙대학교 전자전기공학부 석사
2006년 3월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크, 유비쿼터스 상황인지, 홈네트워크 보안 등

엄 윤 식 (Yoonsik Uhm) 학생회원
2004년 2월 : 중앙대학교 전자전기공학부 졸업
2006년 2월 : 중앙대학교 전자전기공학부 석사
2006년 3월~현재 : 중앙대학교 전자전기공학부 박사과정
관심분야 : 홈네트워크 미들웨어, 지식기반 서비스 아키텍쳐, 홈네트워크 보안 등

박 세 현 (Se Hyun Park) 종신회원
1999년 3월~현재 : 중앙대학교 부교수
2004년 8월~현재 : 홈네트워크 연구센터 센터장
관심분야 : 홈네트워크, 유비쿼터스 컴퓨팅, 인터넷 보안 및 정책 관리 등