USIM 기반 무선 네트워크 연동 보안 인증 시스템에 관한 연구

정병근
고려대학교 컴퓨터정보통신대학원
forest@korea.ac.kr

A Study of Interworking Security Authentication System for the Wireless Networks of based on USIM

ByungKeun Jeong,
Graduate School of Computer and Information Technology, Korea University

요 약

최근의 다양한 무선 네트워크 서비스의 장단점을 상호 보완하기 위해, 3G/WLAN/WiBRO 등을 포괄하는 통합 무선 네트워크 서비스 체계를 구축하고자 하는 노력이 활발히 이루어지고 있다. 현재 무선 네트워크 기술은 단순한 Ethernet 접속 수단이었던 초기와는 달리 공중망 서비스 지원을 위한 인증, 보안, QoS(Quality of Service), 주파수 간섭 등에 대한 기술이 추가로 개발되어 접목되고 있으며, 3세대 이동통신과의 상호 보완적 서비스 개념 형태의 진보된 초고속 무선 이동 서비스로 변화되어 가고 있다.이 때, 각 네트워크 간의 연동은 필연적이며 따라서 기존의 개별 네트워크를 넘어 연동되는 네트워크 상에서의 인증, 키 교환 및 데이터 암호화 등을 가능하게 하는 연동 보안 기술이 요구된다. 본 논문에서는 국제 표준에서 제안되고 있는 무선 네트워크 간의 연동 기술을 소개하고, 효율적인 무선 네트워크 연동 보안을 위하여 USIM 을 통한 인증시스템이 보다 안전한 인증을 할 수 있음을 확인하였다.

1. 서 론

USIM(Universal Subscriber Identity Module) 카드는 WCDMA/HSDPA 네트워크상에서 가입자를 인증하기 위해 가입자의 개인정보를 스마트카드에 저장한 전세계적 WCDMA/HSDPA 표준 가입자 인증 방식이다. 무선 통신 기술의 발전과 무선 네트워크 서비스에 대한 수요의 다변화로 인해, 현재 3G 와 WLAN 이 주도하는 무선 네트워크 서비스가 최근 휴대인터넷(WiBro)이 새로운 서비스로서 추가되는 등 점차 다양화됨에 따라 이종 무선 네트워크 간의 연동(interworking)을 통한 통합 무선 서비스가 활성화되고 있다. 무선 네트워크 연동 시스템이 부각되는 이유는 각각의 시스템이 가지는 성능 제약의 극복이라는 문제가 개별적인 비용을 추가하지 않고도 이종 네트워크와의 연동을 통해 상호 보완적으로 가능하게 되며, 아울러 환경 특성에 따라 효율적으로 대역폭을 관리할 수 있는 등 무선 네트워크 인프라 구축이 보다 용이해질 것이라는 것과 다양한 무선 네트워크 서비스를 이용하기 위해서 각각의 서비스를 개별적으로 이용해야 되는 것이 아니라 네트워크 간의 연동만으로 이종 네트워크의 서비스를 이용할 수 있을 것이라는 기대 때문이다. 이러한 기대를 충족시키기 위해 통합 무선 네트워크 서비스는 먼저 인증/과금/로밍 서비스에 있어 기존의 개별화된 방식을 넘어 상호 협약을 통한 통합된 형태로 가능해야 하며 궁극적으로는 단일화된 방식으로 처리할 수 있어야 한다. 또한 이종 네트워크로 연동하는 과정에서도 끊어짐이 없이(seamless) 음성, 데이터, 멀티미디어 서비스를 제공할 수 있어야 하며 아울러 QoS 나 mobility 등의 서비스도 가능해야 한다. 이를 위해 반드시 제공되어야 할 서비스가 바로 " seamless & invisible security"를 통해 안전한 서비스를 제공하도록 하는 보안 서비스이다. 보안 서비스의 제공을 위한 기술적 해결 과제가 바로 연동 보안 기술이며, 이는 기존의 개별 네트워크에 대한 보안의 수준을 넘어 연동되는 네트워크 상에서 보안을 제공할 수 있는 새로운 보안 기술 체계의 구축을 의미한다. 연동 네트워크 상에서 보안 기술의 구현을 위해서는 개별 네트워크의 보안 체계가 가지는 취약성, 이종 네트워크 간의 상이한 보안 체계의 연동 과정에서 발생 가능한 취약성, 그리고 예상 가능한 각종 보안 위협에 대한 대응책 등을 고려하여 보다 강화된 보안 기술로 개발되어야 한다. 이러한 연동 보안 체계가 지향하는 기술로서 단일인증 및 사용자와 망간의 상호 인증을 통한 강화된 인증 방식, 보다 안전한 프로토콜을 이용한 키 관리기법, 그리고 향상된 데이터의 기밀성 및 무결성을 제공하기 위한 비도 높은 암호화 기술의 활용 등이 매우 중요하기에 본 논문에서는 효율적인 무선 네트워크 연동 보안을 위한 인증 시스템을 연구하고자 한다. 2 장에서는 관련연구에 대한 표준 구조를 설명하고, 3 장에서는 관련연구에 대한 연동 보안의 문제점을, 4 장에서는 제안모델을 설명하고, 5 장에서는 본 논문의 결론을 맺고 향후 연구에 대해서 설명한다.

2. 관련 연구

3G-WLAN-WiBro 연동을 위한 보안 구조는 ETSI BRAN(Broadband Radio Access Network) TR 101 957 에서 HIPERLAN/2 기반 WLAN 망과 3G UMTS(Universal Mobile Telecommunications Systems) 망간의 연동을 위해 제시하고 있는 loose 연동 및 tight 연동 구조를 토대로 현재는 WiBro 까지 포함되며, 추후에는 더 많은 영역으로 확대 될 것으로 예상된다[1].

2.1 Loosely Coupled 구조

그림 1. 에서처럼 loose 연동구조에서는 WLAN 망이 별도로 존재하면서 단지 UMTS 핵심망(core network)과의 연동을 위해 IWU 가 추가된다. IWU(Inter-Working Unit)는 두 시스템의 연동을 위해 필요한 이동성, 인증 및 과금 등의 관련 기능을 수행하는 장비이다. Loose 연동구조는 다시 USIM(UMTS Subscriber Identity Module) 기반 사용자 식별 및 인증 시나리오와, 다이얼업 인터넷 접속에서 사용하는 NAI(Network Access Identifier) 기반 사용자 식별 및 인증 시나리오로 분류할 수 있다. NAI 기반 인증에서는 WLAN 의 AAA 서버와 UMTS 의 AAA 서버간의 연동이 요구되며, USIM 기반 인증에서는 필요에 따라 HLR(Home Location Register) 혹은 HSS(Home Subscriber System)과의 연동도 요구된다. AAA 간 연동을 위해서 IETF 에서 개발중인 RADIUS 혹은 Diameter 프로토콜이 사용되며, USIM 기반 IWU 와 HLR 과의 연동은 기존 MAP(Mobile Application Part) 프로토콜이 사용된다.

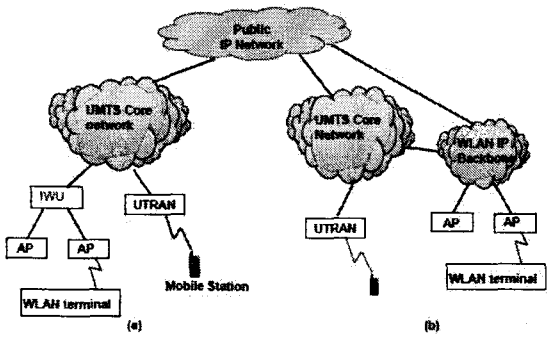

그림 1. WLAN 과 3G 시스템간의 연동구조

2.2 Tightly Coupled 구조

Tight 연동방식은 UMTS 핵심망에 WLAN 접속망이 연결되는 형태로써, WLAN 망은 UTRAN 처럼 하나의 접속망으로 동작한다. 각 가입자는 망 접속환경에 따라 UTRAN(UMTS Terrestrial Radio Access Network) 혹은 WLAN 망을통해 UMTS 서비스를 이용하게 된다.이 시나리오 에서는 UMTS 핵심망과 WLAN 망간 연동을 위해 IWU 장비가 필요하게 되며, 기본적인 서비스제어 및 관리기능은 UMTS 핵심망에서 담당하게 된다.

2.3 Loosely 와 Tightly 의 장단점 비교

Loose 연동방식은 IP layer 상에서 연동이 가능하여 UMTS 의 PSDN(Packet Switched Data Network)을 core 로 통합이 가능하다. 또한 WLAN terminal 에 WCDMA 프로토콜을 구현할 필요가 없으며 다양한 WLAN 규격의 수용이 가능한 반면 mobility, QoS, security 기능의 제공에 어려움이 있다.Tight 연동방식은 WCDMA 망의 security, QoS, mobility mechanism 의 사용이 가능한 반면 WLAN terminal 에 WCDMA 프로토콜의 구현을 요구하고 표준화에 많은 시간을 요구하는 어려움을 가지고 있다. 따라서, tight 연동방식은 보다 장기적인 관점에서 접근할 수 있는 망 구조라 할수있다.

2.4 3G-WLAN-WiBro 연동보안 참조 모델

3GPP-WLAN Interworking 참조모델을 기반으로 3GPP 와 WLAN/WiBro 연동 참조 모델을 제시할 수 있다[2]-[4]. 로밍이 지원되는 모델과 로밍이 지원되지 않는 모델을 구분하여 기술을 설명한다.

2.4.1 로밍이 지원되지 않는 참조모델

그림 2. 는 로밍이 지원되지 않는 참조 모델로 홈네트워크가 접근제어와 터널 설정을 책임진다.

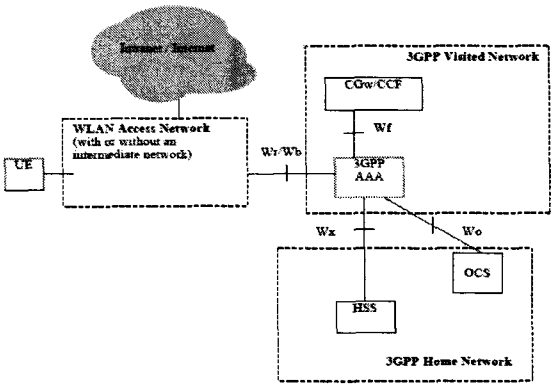

그림 2. 로밍이 지원되지 않는 참조모델

2.4.2 로밍이 지원되는 참조 모델

그림 3. 은 로밍이 지원되는 참조 모델을 나타내고 있다. 홈네트워크는 접근제어의 책임이 있고 과금기록은 방문 혹은 홈 3GPP 네트워크에서 생성될 수 있다.

3GPP AAA proxy 는 접근제어 신호와 계정정보를 홈 3GPP AAA 서버에 전달하게 된다.

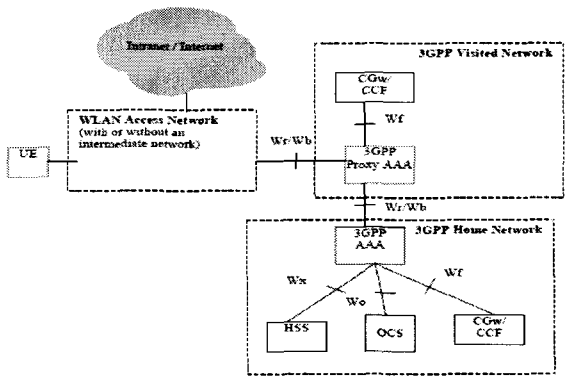

그림 3. 로밍이 지원되는 참조모델

3. 연동 보안의 문제점

3G-WLAN-WiBro 연동은 서비스 제공자가 사용자들에게 어디서나 자유롭게 저렴하고 빠른 인터넷 서비스 및 다양한 응용들을 사용할 수 있도록 하는 서비스기술로서 3G, WLAN, 그리고 WiBro 가 가지는 각각의 장점을 접목시켜서 하나의 새로운 서비스 모델을 만들 수 있음을 의미한다. 하지만 이를 위해 고려해야 할 보안관련 문제점들은 여전히 해결되어야 할 기술적 과제로 남아 있다. 우선, 3G-WLAN-WiBro 연동을 위해서는 기본적으로 도메인별 security 가 보장 되어야 하며, 망간 연동에 따른 도메인간 security 역시 반드시 보장 되어야 한다. 도메인별 혹은 도메인 간 security 는 일반적으로 local PIN(Personal Identification Number)이나 global PIN 을 이용하여 제공될 수 있으며 UICC 혹은 SIM 카드에 PIN 값을 저장하는 방법을 이용함으로써 사용자에게 보다 안전한 보안성을 제공해줄 수 있게된다. 그리고 취약한 인증 방식에서 벗어날 수 있도록 인증에 사용되는 키 길이를 늘리고, IV(Initial Vector) 값에 대한 취약성을 보완하는 한편 키관리 기능(키 분배, 키 저장, 주기적인 키 갱신)을 인증 알고리즘에 포함함으로써 보다 견고한 인증방식을 구축해야 한다. 더불어, 네트워크상에서 주고 받는 데이터는 반드시 암호키를 이용하여 평문이 아닌 암호문 형태로 암호화하여 송수신 하도록 한다. 3G-WLAN-WiBro 세 가지 종류의 무선 네트워크는 각기 다른 인증 알고리즘을 정의하여 사용하고 있기 때문에 연동시 서로 다른 인증 프로토콜 변환과정 에서 발생될 수 있는 보안문제점 들도 고려되어야 할 것이다. 이밖에 해결되어야 할 보안문제점들로 replayattack, man-in-the-middle attack, 무선구간 트래픽 도청, 링크레벨 sniffing 방지 및 물리계층 보안 등이 있을 수 있는데, 우선 replay attack 의 경우 재전송 공격방지를 위해 디폴트로 송신측에서 순차번호(sequence number)를 증가시키고 수신측에서 이를 검사하여 순차 번호가 적절한 값을 갖고 있지 않으면 서비스를 거부할 수 있도록 하는 방안을 고려해볼 수 있고, 중간에서 통신데이터를 가로채거나 수정하는 공격방법인 man-in-the-middle 공격의 경우 애플리케이션 레벨에서 취할 수 있는 방법으로 PKI(Public Key Infrastructure) 기반 디지털 인증서를 이용하여 송신측과 수신측이 서로 상호인증을 수행함으로써 제 3 자에 의한 개입 공격을 방지할 수 있는 방안과 송신측과 수신측간에 데이터를 주고 받기에 앞서 secure channel 을 설정하여 링크 레벨계층의 보안을 강화 할 수 있는 방안으로 나누어 생각해 볼 수 있다. 이때, 송수신되는 데이터는 물론 평문이 아닌 암호문 형태로 전송하도록 해야 할 것이다. 무선 구간 트래픽 도청 방지를 위해서는 무선구간으로 전송되는 모든 데이터를 암호화하여 전송하고,암호 알고리즘에 사용되는 키 값을 주기적으로 서버로 부터 할당 받아 갱신해 주는 방법을 적용할 수 있고, 물리계층 보호를 위해서는 안전하게 데이터를 저장하고 관리할 수 있는 방안으로 안전한 하드웨어 토큰의 필요성이 대두되고 있다. 마지막으로 sniffer 는 컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치를 의미하며, sniffing 이란 이러한 sniffer 를 이용하여 네트워크상의 데이터를 도청하는 행위를 말한다. 링크레벨에서 발생될 수 있는 sniffing 을 방지하기 위해서는 네트워크 트래픽의 암호화, 스위칭 환경의 네트워크구성, 주기적인 sniffer 탐지 등의 다양한 방법을 적용시킬 수 있다. 지금까지 연동 보안 문제점으로 지적한 항목들은 외부로 유출되지 않아야 할 사용자의 비밀 데이터(사용자 identity, IMSI(International Mobile Subscriber Identity), PIN 등)가 보안구조가 취약한 연동시스템 및 다양한 공격법에 의해 제 3 자에게 유입될 수 있는 상황을 고려하여 기술된 것이며, 사용자의 비밀 데이터를 가장 안전하게 저장하고 관리할 수 있는 대안으로 UICC 또는 USIM 카드를 연동시스템에 적용시키는 방법을 채택하였다.

4. 제안 모델

4.1 통합 인증 과정

서로 다른 무선 네트워크의 연동보안은 사용자의 편의성과 친밀성, 그리고 강화된 보안서비스에 초점을 맞추어 서비스 제공을 위한 통합 인증방법과 그 과정을 살펴보도록 한다. IETF 의 표준인 EAP-AKA 인증은 3 세대 이동통신망(WCDMA)의 사용자가 표준인증인 AKA 알고리즘을 이용하여 WLAN 망에서 동일하게 인증될 수 있는 모델을 보여준다[5],[6]. 그림 4. 는 USIM 에서 AUTH 를 검증하고 RES 로 응답하는 과정은 아래 순서로 이루어진다.

1) AK=f 5K(RAND), SQN=(SQN ⊕ AK) ⊕ AK

2) XMAC=f1K(SQN || RAND || AMF)을 계산해서 AUTN 내의 MAC 과 비교한다. 만약 일치하지 않는다면 user authentication reject 메시지를 보내서 인증절차에 실패한다. 3) SQN 이 적합한 범위에 속하는지 확인하고 그렇지 않다면 synchronization failure 메시지를 보낸다. 사용자로부터 synchronization failure 를 받으면 VLR/SGSN 는 HE/AuC 에게 synchronization failure indication 을 포함한 인증 데이터 요구 메시지를 보내서 새로운 AV 에 기초한 인증을 다시 시도한다.

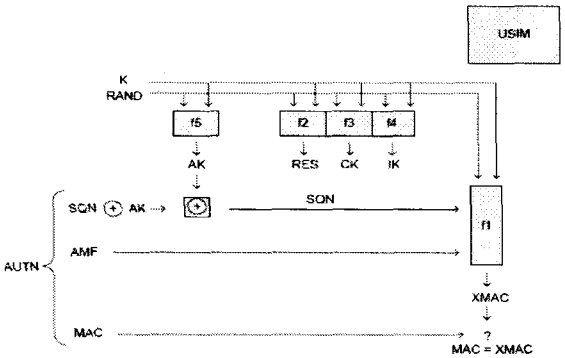

그림 4. USIM Authentication Protocol

4.2 USIM 인증 시스템 구조

EAP-AKA 인증은 기존 AKA 인증에 EAP 개념을 도입함으로써 사용자의 단일인증을 통한 편의성, 호환성 및 보안이 한층 강화될 수 있는 장점은 있으나, 프로토콜의 오버헤드가 증가하는 단점을 지닌다. 무선네트워크와의 연동시스템에 EAP-AKA 를 사용하였을 때, 단일 인증을 통해 이동통신 망사용자가 WLAN 에 접속하는 과정은 그림 5. 에 나타나 있다. USIM 카드를 이용한 EAP-AKA 를 위한 구성요소는 AKA 의사용자 인증을 위한 USIM 카드, 사용자의 단말기(client), AP(Access Point), WLAN 과 이동통신 망간의 연결고리인 AC(Access Controller), EAP 인증 및 사용자 인증을 위한 AAA 서버, 그리고 사용자 인증 데이터가 저장된 HLR(Home Location Register) 등으로 이루어져 있다. 이동통신 가입자가 자신의 USIM 카드와 단말기를 이용하여 WLAN 을 접근하려 하였을 때 인증이 이루어지는 과정은 다음과 같다. AC 는 사용자의 identity(IMSI)를 EAP-request/AKA-identity 를 통하여 요구한다. 단말기와 USIM 카드는 자신의 identity 를 EAP-response/AKA-identity 에 실어 보내고, 이는 AC 와 AAA proxy 를 거쳐 HLR 에서 IMSI 에 해당하는 인증 벡터를 추출할 수 있는 기본 벡터로 활용된다. 인증 벡터는 다시 EAP-request / AKAchallenge 를 통하여 AAA 서버로부터 USIM 카드에 전달되고, 카드는 메시지에 포함된 MAC (Message Authentication Code) 값을 검증하여 검증 결과가 성공적일 경우 결과값(RES)을 AAA 서버에게 전달한다.

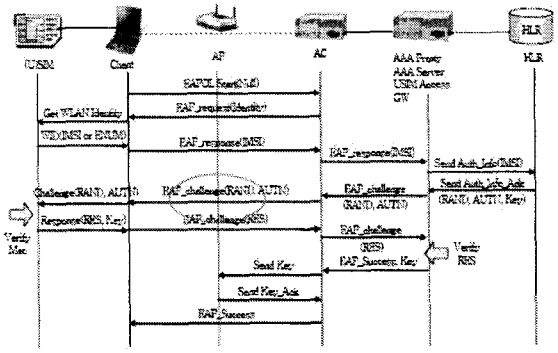

그림 5. USIM Based Authentication Flow

인증관계의 마지막 단계로 AAA 서버는 수신된 RES 값을 자신이 가지고 있는 값과 비교하여 사용자 인증을 수행한다[7]. 이러한 일련의 과정이 모두 성공적으로 수행될 경우에만 사용자는 비로소 WLAN 을 접근할 수 있는 권한을 갖게 된다.

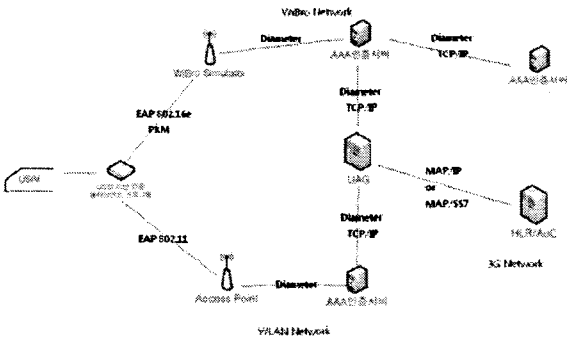

그림 6. USIM 기반 통합 인증 시스템 구성도

그림 6.은 USIM을 통한 무선네트워크 통합 인증 시스템 구성도이다. AAA인증서버는 Diameter 메시지, 암호 알고리즘 처리, 세션키의 생성 및 분배를 한다. UAG(USIM Access Gateway)는 이종 무선네트워크의 연동과 인증을 가능하게 하며, RADIUS<->Diameter 와 Diameter <-> MAP 프로토콜 변환을 하게 된다. USIM기반 연동 보안 구조는 가입자 정보 및 안전한 무선 데이터 서비스를 가능하게 한다.

5. 결론 및 향후 연구

본 논문에서는 무선 네트워크 연동 보안 시스템의 구축은 앞으로 다양한 무선 네트워크를 넘나드는 통합 무선서비스를 안전하게 제공하기 위해 가장 우선되어야 할 전제 조건으로 USIM 인증 시스템을 구현하였다. 현재 대표적인 무선네트워크라 할 수 있는 3G-WLAN-

WiBro 를 중심으로 한 연동 및 보안 기술에서 살펴 보았듯이 무선 네트워크 연동보안 기술 개발은 개별 네트워크를 위한 단일 보안기술 개발이 아닌 연동되는 네트워크 상에서 상이한 보안체계를 효과적으로 연동하는 보안기술을 구현하는 것이므로 현재 각 개별 네트워크의 보안취약성, 연동과정에서 발생할 수 있는 보안취약성, 그리고 예상 가능한 보안위협에 대한 대응책을 모두 고려하여 보다 강화된 보안기술로의 개발을 지향해야 할 것이다. 그리고, 현재 무선네트워크의 연동 기술은 계속 진화되는 과정에 있으며, 앞으로 새로운 무선네트워크 서비스의 추가 등으로 인해 보다 다양한 네트워크 간의 연동을 예상할 수 있으므로, 이에 맞추어 효율적인 USIM 기반 통합 연동 보안 인증시스템을 구현하고 적용할 수 있는 방안을 추진해 보고자 한다.

참고문헌

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

[2] 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)," June 2004.

[3] 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)," Aug. 2002.

[4] 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)," June 2004.

[5] RFC 3748 "Extensible Authentication Protocol (EAP)," June 2004.

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

[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)," June 2002.