IMT-2000 인증 프로토콜 설계

강 형 우[†]·윤 이 중[††]·이 수 연[†††]·박 창 섭[††††]·이 동 훈[†††††]

요 약

2000년대 초반에 서비스가 개시될 것으로 예상되는 IMT-2000 시스템은 전세계적으로 단일 표준을 결정하여 하나의 단말기로 세계적인 고품질 서비스를 목적으로 하고 있다. 본 논문에서는 IMT-2000 시스템의 가입자 인증 프로토콜을 설계할 때 고려해야 할 보안 사항을 살펴보며 IMT-2000 시스템을 위한 보안 고려사항을 만족하는 효율적인 가입자 인증 프로토콜을 제안한다. 제안된 프로토콜은 가입자 인증, 가입자의 위치정보 보호와 안전한 통신을 제공하며 IMT-2000 시스템의 서비스 목표인 글로벌 로밍을 제공한다.

Design of Authentication Protocol for IMT-2000

Hyung-Woo Kang[†]·E-Joong Yoon[††]·Su-Yoon Lee[†††]·
Chang-Seop Park[††††]·Dong-Hoon Lee[†††††]

ABSTRACT

IMT-2000 system is expected to start its service at the beginning of 2000 on the purpose of providing with the highest qualitative service through one mobile terminal. In this paper, we investigate some of the important issues which need to be addressed in designing an authentication protocol for IMT-2000. Also proposed is an authentication protocol which addresses the above issues, and we design a correct and efficient authentication protocol to establish secure communication channel. Our protocol provides an authentication of the communicating entities, location privacy, and secure messaging as well as global roaming service.

1. 서 론

최근에 늘어나는 이동 통신의 수요를 충족시키고 저렴한 서비스를 제공하기 위하여 각 나라마다 차세대 디지털 이동 통신 시스템인 IMT-2000 개발을 서두르고 있다. 차세대 디지털 이동 통신이란 2000년대 고기능, 고품질의 다양한 통신욕구를 충족시킬 수 있는 이동 통신 서비스를 제공하기 위하여 기존의 셀룰러 서비스나 개인통신서비스가 제공할 수 없는 2Mbps급의 고속 무선 멀티미디어 서비스를 제공함을 의미한다. 또한, 기존에 사용하고 있는 주파수대에서의 2000년대 가입자 수용 포화 상태를 극복하여 새로운 주파수대의 다양한 저가, 고성능 이동 통신 서비스를 제공하며 기존의 개별적인 서비스를 통합하여 유·무선 통합서비스를 실현하기 위한 지능형 광대역 종합 이동 통신 시스템인 IMT-2000 환경에서 이루어지는 통신을 의미한다. 따라서, IMT-2000은 기존의 2세대 이동전화 서비스의 기능을 만족시키는 것 이외에, 전세계 이동 전화망의 접속 표준화, 이종 무선 통신 서비스의 통합화,

† 준 회 원 : 고려대학교 대학원 전산학과
†† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부 선임연구원
††† 정 회 원 : 천안외국어대학 사무자동화과 교수
†††† 정 회 원 : 단국대학교 전자계산학과 교수
††††† 정 회 원 : 고려대학교 전산학과 교수
논문접수 : 1998년 11월 21일, 심사완료 : 1999년 6월 23일

그리고 무선 데이터 서비스의 광역화로 그 범위를 확장시킬 수 있다. 더불어 IMT-2000은 고정망의 지능화에 따라 추진되는 UPT(Universal Personal Telecommuncation) 서비스를 무선 휴대전화 영역까지 확대 적용하는 개념을 포함하는 제 3세대 이동 통신 시스템으로써 서비스 환경은 누구나 언제 어디서나 하나의 단말기로 통화를 할 수 있는 단말기 이동성, 개인 이동성, 서비스 이동성을 제공한다. IMT-2000 환경에서는 무선 통신망을 이용하는 이동 통신의 특성 때문에, 불법적인 사용, 도청, 추적을 통한 불법적인 행위 등 각종 통신 범죄 행위도 늘어나게 된다. 이러한 행위들은 가입자에 대한 서비스의 저하, 개인의 프라이버시 침해 등의 역기능적인 문제를 가져오게 된다.

최근, 이런 문제들을 해결하기 위하여 각국의 이동 통신 업무의 표준화에 인증 기능 등이 추가되어 권고되고 있다. 미국의 TIA/EIA(Telecommunications Industry Association/ Electronic Industries Association)에서 무선 인터페이스 표준안이나, 유럽 국가에서 ETSI (European Telecommunications Standards Institute)의 표준화로 추진하고 있는 GSM(Global System for Mobile Communications), DECT(Digital European Cordless Telecommunications) 표준에서도 인증을 포함한 보안 서비스를 권고하고 있다. 이들 표준들은 인증 및 암호기능을 제공하기 위해서 모두 비밀키 암호 방식을 채택하고 있다. 이 방식은 보안 서비스의 제공으로 인한 시스템에 미치는 부하의 증가, 단말기 소형화에 따른 계산능력의 문제점 등을 고려하여 선정된 것이다. 그러나, 거대한 데이터 베이스의 안전 관리가 문제로 남게 된다. 이러한, 비밀키 암호 방식에 의한 보안 서비스 제공에 대한 취약점을 개선하기 위하여 공개키 암호 방식을 이용한 각종 방안들이 제시되고 있다. 하지만 제안된 방식들은 비록 비밀키의 단점인 안전한 데이터베이스 관리 문제를 해결할 수 있으나, 시스템의 부하를 증대시키는 등의 문제가 있다.

본 논문에서는 비밀키 암호 방식을 이용하여 시스템 부하와 단말기의 계산 능력을 고려하고, 비밀키 인증서를 사용하여 가입자의 비밀정보를 저장하는 데이터베이스의 안전한 관리 문제를 해결하고 IMT-2000 시스템이 최종적으로 목표로 하고 있는 글로벌 로밍 서비스를 제공하기 위해 기존의 다른 무선망과의 연동이 가능한 새로운 인증 프로토콜을 제안한다. 2장에서는 이동 통신 보안의 특징을 살펴보고, 3장에서는 기존의 연구를 살펴보며, 4장에서는 IMT-2000 시스템에 대해서 살펴보며, 5장에서는 IMT-2000 시스템 환경에 맞는 보안 프로토콜을 제안하며, 마지막으로 6장에서는 결론을 논한다.

2. 이동 통신 보안의 특징

이동 통신에 있어서 보안 위협 요소로는 다음 사항들이 고려될 수 있다. 첫째는 불법 사용이다. 불법 사용은 정당한 가입자의 번호를 도용하거나, 도난·분실된 단말기를 불법으로 사용하여 통신 사업자와 합법적인 가입자에게 과금의 혼란으로 인한 막대한 피해를 주게 하는 것이다. 둘째는 가입자 정보의 도청 및 가로채기이다. 무선 통신의 취약성 때문에 누구든지 쉽게 다른 가입자의 통화 내용을 청취할 수 있고 비록 암호화가 되었을 경우에도, 암호 알고리즘의 안전성이 취약하거나 관련 프로토콜이 안전하지 못할 경우 통화 내용이 도청될 수 있다. 셋째로는 추적에 의한 프라이버시의 침해이다. 이동 통신에서는 이동 가입자에 관한 정보 및 위치 정보가 엑세스 채널에서 평문 형태로 무선 구간에 전달될 수 있다. 이런 정보들은 누가 언제 어디서 통화를 했는가를 쉽게 추적하는 데 이용될 수 있다. 제3자 외에도 네트워크 내의 인증 센터나 기지국 등이 결탁하거나 불법행위를 할 경우, 특정 이동 가입자의 추적은 쉽게 행하여 질 위험이 있다.

보안 정책 수립에서 다루어야 하는 보안 서비스는 무선 통신 구간을 이용하는 이동 통신의 상황을 고려하여 제공되어야 한다. 이동 통신에 있어서의 보안 위협요소에 대처하기 위한 기본적인 보안 서비스로서 고려될 수 있는 사항들은 다음과 같다. 첫째는 인증 서비스이다. 이동 통신에서 인증이란 통화 초기에 설정된 비밀 정보를 가입자 즉, 단말기를 소지한 자가 서비스 제공자인 네트워크에 증명하여 정당한 가입자임을 밝히는 절차이다. 이는 단말기의 불법 사용을 방지하기 위한 대책으로서 이동 통신 서비스 제공자인 통신 사업자가 반드시 고려하여야 할 보안 서비스이다. 모든 공중 통신망에서는 사용에 따른 과금이 가입자에게 징수되어야 하지만, 제공된 통화나 서비스에 대한 과금이 제대로 수행되지 않게 되거나, 다른 사람에게 과금이 되도록 하는 불법 행위들이 일어날 수 있다. 이러한 위조나 불법 사용에 대한 보호 대책을 위해 이동 가입자의 신분 확인이 반드시 이루어져야 한다. 이

러한 인증 작업은 인증 프로토콜에 의해서 이루어 질 수 있다. 둘째는 데이터를 암호하는 암호 서비스이다. 이동 통신은 무선 구간을 통한 이동 통신의 특성 때문에 불법 도청이 가장 용이하여 안전성 측면에서 가장 취약하다. 즉, 누구든지 통화중의 내용을 발각되지 않고 쉽게 도청할 수 있다. 이러한 관점에서 무선 구간의 통화 내용은 반드시 암호화되어 보내져야 한다. 이동 가입자의 음성 정보 및 신호 정보는 도청 및 가로채기에 대한 대책으로서 암호화가 이루어져야 한다. 이런 암호화는 암호화에 사용될 키(세션키)의 공유가 선행되어야 하며 반드시 인증 절차가 완료된 후에 수행되어져야 한다. 셋째는 익명성(anonymity)과 추적 불가능성(untraceability) 서비스이다. 익명성과 추적 불가능성은 이동 가입자의 프라이버시를 제공해 주는 기능이다. 송수신자의 위치 정보나 통화당사자에 대한 정보가 제 3자에게 노출되어 추적되는 것을 방지하기 위해서는 공개키 암호를 사용하면 쉽게 해결할 수 있다. 그러나 공개키 암호방식은 단말기에게 많은 계산능력을 요구한다.

마지막으로 이동 통신에서 인증 프로토콜 설계시 고려할 사항은 단말기의 낮은 계산능력과 적은 배터리 용량이다. 이동 통신에서 인증 프로토콜은 작은 시스템인 단말기와 큰 시스템인 인증 서버와의 통신이기 때문에 프로토콜 설계시 작은 시스템인 단말기에게는 낮은 연산을 수행하도록 설계해야 한다.

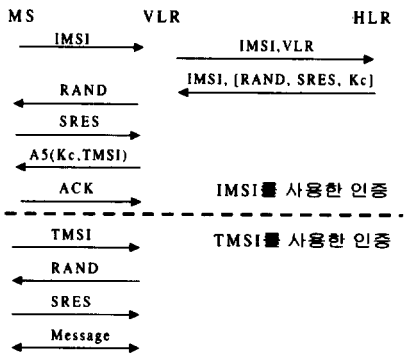
3. 기존의 연구

이 장에서는 이동 통신 가입자의 프라이버시를 제공하기 위한 기존의 연구를 비밀키 방식과 공개키 방식으로 분류하여 살펴본다.

3.1 비밀키 방식의 가입자 인증 프로토콜

이동 통신 환경에서의 비밀키 방식의 가입자 인증 프로토콜은 GSM과 CDPD를 들 수 있다. CDPD에서는 Diffie-Hellman 키 교환 프로토콜을 수행하여 세션키를 공유하지만 가입자 인증과 프라이버시 제공을 위해서 비밀키 방식을 사용하기 때문에 비밀키 방식으로 분류하였다. GSM(Global System for Mobile Communication)은 가입자의 프라이버시를 제공하기 위한 최초의 디지털 셀룰라 네트웍이다. 다음은 GSM에서 사용되는 기호들이다.

- MS(Mobile Station) : GSM 가입자의 단말기
- VLR(Visitor Location Register) : 방문 지역에 있는 인증을 위한 데이터베이스
- HLR(Home Location Register) : 홈 지역에 있는 인증을 위한 데이터베이스
- IMSI(International Mobile Subscriber Identity) : MS의 고유번호
- A3, A8 : 일방향 함수
- A5 : 비밀키(Symmetric Key) 암호 알고리즘
- RAND : 도전(challenge)에 해당하는 난수열
- SRES = A3(K_i, RAND) : RAND에 대한 응답(response)
- Kc = A8(Ki, RAND) : RAND와 K_i를 통해 만들어진 세션키



(그림 1) GSM 인증 프로토콜

모든 GSM 가입자들은 단말기의 스마트카드 안에 HLR과 공유하는 비밀키 K_i를 저장하고 있다.

가입자는 홈이 아닌 방문 지역에 위치하였을 경우 이동 통신 서비스를 받기 위하여 다음과 같은 인증 프로토콜(그림 1)을 시작한다. 먼저 IMSI를 VLR에 전송하면 VLR은 그것을 HLR에 전송한다. HLR은 MS를 인증하기 위하여 도전/응답(challenge/response) 메시지(RAND, SRES, Kc)를 VLR에게 전송한다. VLR은 HLR로부터 받은 RAND와 SRES를 가지고 도전/응답 프로토콜을 수행하여 MS를 인증한다.

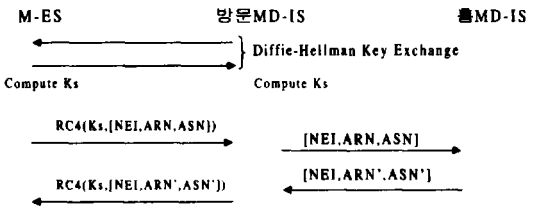
GSM에서 프라이버시는 TMSI(Temporary Mobile Subscriber Identifiers)로 알려진 가명을 이용하여 제공되는데, 가입자의 단말기에 전원이 들어갈 때 IMSI (International Mobile Subscriber Identity)로 알려진 가입자의 ID가 전송되고, 그 다음 단계부터는 TMSI가

가입자의 가명으로 전송된다. GSM의 문제는 TMSI를 반복적으로 사용할 경우 도청자가 가입자의 IMSI는 알지 못할 지라도 TMSI를 추적할 수 있다. 또한, 가입자와 홈 지역 사이에 TMSI의 동기화가 끊어졌을 경우에는 가입자가 다시 홈 지역에게 IMSI를 보내야 한다. 이런 점은 가입자의 프라이버시에 문제가 생길 수 있다.

GSM의 또 다른 문제점은 홈 지역과 방문 지역사이의 네트웍은 안전하다고 가정을 하였기 때문에 방문 지역이 홈 지역에게 가입자의 IMSI와 위치정보를 평문 상태로 보내게 된다. 하지만 이런 일들은 가입자의 프라이버시를 해치기 쉬운 일들이다.

CDPD(Cellular Digital Packet Data)는 셀룰라 음성 통신에서의 비어있는 슬롯을 이용하여 데이터를 전송하는 것이다. CDPD 각각의 서비스 지역에는 이동 MD-IS(Mobile Data Intermediate System)와 같이 위치한다. 단말기 M-ES(Mobile End-System)의 인증은 단말기의 홈 지역상에 있는 인증 서버를 통해서 이루어진다.

인증의 시작은 먼저 MD-IS와 M-ES 사이에 수행되는 Diffie-Hellman 키 분배 프로토콜[4]로부터 이루어진다. 이 프로토콜의 결과로 이동 단말기 M-ES와 MD-IS는 공통의 세션 키 Ks를 공유하게 된다.



(그림 2) CDPD 인증 프로토콜

(그림 2)는 이동 단말기 M-ES가 방문 MD-IS를 경유하여 홈 MD-IS에게 자신에 대한 신분을 확인시키는 인증 프로토콜을 보여주고 있다. M-ES는 자신의 credential [NEI, ARN, ASN]을 RC4 알고리즘에 세션 키 Ks를 적용시켜 암호화한 후에 방문 MD-IS로 보내고, 방문 MD-IS는 복호화한 후에 credential을 홈 MD-IS로 보낸다. 이때 NEI(Network Equipment Identifier)는 등록된 단말기 번호이고, ARN(Authentication Random Number)과 ASN(Authentication Serial Number)에는 매 세션마다 상이한 값을 부여하여 불법 복제 단말기에 의한 접속 도전을 방지하거나 또는 사후적으로 검출할 목적으로 사용된다. 홈 MD-IS는 수신된 credential [NEI, ARN, ASN]의 유효성에 따라서 M-ES에 대한 위치 등록 요청을 결정한다. 선택적으로 MD-IS는 다음에 사용될 ARN'과 ASN'을 생성하여 방문 MD-IS를 경유하여 M-ES에게 전송한다.

GSM과는 달리 CDPD는 좀 더 안전한 방법을 취한다. CDPD는 인증 과정이 일어나기 전에 먼저 가입자와 방문 지역사이의 Diffie-Hellman 키 교환 프로토콜을 이용하여 세션키를 공유하고 그 다음에 가입자는 자신의 ID를 세션키로 암호화하여 방문 지역에게 전송한다. 즉, 키 교환 후에 인증을 수행하여 가입자의 익명성을 유지하는 방법이다. 이 방법에서 첫 번째 문제점은 방문 지역이 가입자의 ID를 알 수 있다는 것이다. 이것은 가입자의 프라이버시 보호 차원에서 문제가 될 수 있다. 두 번째 문제점은 Diffie-Hellman 키 분배 프로토콜의 문제점에 기인한다[15]. 즉, 세션 키의 분배가 방문 MD-IS에 대한 인증 메커니즘이 결여된 상태에서 이루어지기 때문에 불법적인 제3자가 MD-IS로 가장하여 프로토콜에 적극적으로 개입한다면 이동 단말기 비밀 정보의 노출이 가능하게 된다.

3.2 공개키 방식의 가입자 인증 프로토콜

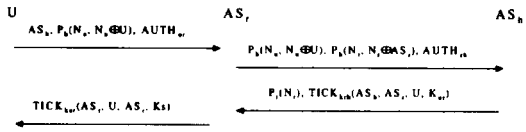
이 절에서는 Samfat, Molva 그리고 Asokan[9]이 제안한 공개키 방식의 가명을 이용하여 이동 통신 가입자의 프라이버시를 제공하는 인증 프로토콜을 보겠다.

이 프로토콜의 특징은 가입자가 인증 프로토콜을 수행할 때 매번 다른 가명을 사용하여 가입자의 익명성과 추적불가능성을 제공한다. 다음은 Samfat, Molva 그리고 Asokan이 제안한 프로토콜에서 사용되는 기호이다.

- U : 이동 통신 가입자의 ID
- AS_h : 홈 지역 인증 서버의 ID
- AS_r : 방문 지역 인증 서버의 ID
- K_u : U와 AS_h의 공유키
- K_{rh} : AS_r과 AS_h의 공유키
- $K_{ur} = h(U, AS_r, K_u)$, h는 일방향 해쉬 함수
- P_x, S_x : AS_x의 공개키 개인키 쌍
- N_x : X에 의해 발생된 난수
- $P_x(M)$: AS_x의 공개키 P_x로 메시지 M을 암호화한 형태
- $AUTH_{XY}$: X가 Y에게 자신을 인증시키기 위해서

보내는 X와 Y의 비밀키로 암호화된 메시지[3]

- $TICK_{Kx}(Ks)$: 세션 키 Ks를 분배하기 위한 메시지로서 키 Kx로 암호화되어 전송되는 메시지[3]



(그림 3) Samfat, Molva, Asokan이 제안한 인증 프로토콜

이 프로토콜(그림 3)은 가입자가 홈 지역이 아닌 방문 지역에 위치하였을 경우 위치등록을 하는 인증 프로토콜에서 자신의 ID를 그대로 사용하지 않고 공개키 방식의 가명 Ph(Nu, Nu⊕U)을 사용하여 ASr과 ASh만이 자신의 ID를 알 수 있도록 가입자의 프라이버시를 보장하는 것이다. 첫 번째 메시지를 받은 ASr은 Kur이 없기 때문에 가입자에 대한 인증은 나중으로 미루고 먼저 ASh에게 가입자의 ID인 U, 자신의 가명인 Ph(Nr, Nr⊕ASr), 그리고 자신을 ASh에게 인증시키기 위한 메시지 AUTHrh를 전송한다. 그러면 ASh는 먼저 ASr을 인증하고 그 다음에 가입자 U에 해당하는 Kur을 계산하여 ASr에게 Kur이 포함되어 있는 TICK을 전송한다. 세 번째 메시지에서 Pr(Nr)은 ASh의 가명 역할을 한다. 여기서 ASh의 가명을 사용한 이유는 가입자의 홈 지역을 외부로 드러나지 않게 함으로써 가입자의 프라이버시를 더욱 높일 수 있기 때문이다. 세 번째 메시지를 받은 ASr은 Kur을 TICK으로부터 뽑아내어 첫 번째 메시지의 AUTHur을 복호화하고 ASr은 이동 통신 가입자 U를 비로소 인증할 수 있게 된다. 여기서 마지막 네 번째 메시지는 옵션으로 보내어지는 것으로 U와 ASr 사이의 세션 키를 ASr이 전달하는 것이다. 가입자 U는 이 메시지를 받음으로써 ASr과 ASh를 인증하게 된다.

위에서 보인 프로토콜은 가입자의 프라이버시를 보장하는 인증 프로토콜이다. 하지만 현재 사용중인 이동 통신 단말기의 계산적인 능력으로 보아서 공개키 방식은 이동 통신에서 인증 과정으로 사용하기에는 적절하지 않은 것으로 보인다.

4. IMT-2000(FPLMTS) 시스템

FPLMTS(Future Public Land Mobile Telecommunications)에서 명칭이 변경된 IMT-2000(International Mobile Telecommunication)[12,13,14]은 2000년대에 서비스 개시를 계획하고 있는 차세대 이동 통신 시스템으로서 다음과 같은 개념을 포함하는 것으로 정의되고 있다. 첫째, 기존 이동전화 서비스 기능을 만족시키며, 둘째, 전세계 이동 전화망의 접속표준화, 셋째, 이기종 무선통신 서비스의 통합화, 넷째, 무선 데이터 서비스의 광역화로 집약될 수 있으며, 고정망의 지능화에 따라 추진되는 UPT(Universal Personal Telecommunication) 서비스를 무선 휴대전화 영역에까지 확대 적용하는 개념 등이다.

IMT-2000은 1.8~2.2GHz의 주파수대역을 사용할 시스템으로서 다음과 같은 특징을 가지고 있다. 첫째, 세계적으로 고도의 공통성을 가진 구조이다. IMT-2000 서비스는 상용화되면 위성과 연계되고, 국제로밍을 제공하여 단말기 및 개인 이동성이 보장되어 "언제, 어디서나, 누구나"의 서비스를 실현하고 내용도 음성에서 멀티미디어에 이르기까지 모든 형태를 수용할 수 있게 될 것이다. 둘째, 내부적으로 고정망과의 호환성이다. 셋째, 다양한 무선시스템의 결합기능이다. IMT-2000에서는 여러 종류의 서비스를 다양한 무선운용 환경하에서 제공하기 위해 요구되는 서비스를 수용할 것이다. 넷째, 이동관리 및 서비스제어를 위한 지능망 기능의 활용이다. 다섯째, 높은 보안성 및 프라이버시의 제공이다. 여섯째, 고품질 및 세계적으로 로밍이 가능한 휴대용 단말기의 사용이다. IMT-2000이 유선계의 초고속망과 연동되고, 무선접속방식이 광대역화되어 고속으로 데이터를 처리함으로써 음성뿐만 아니라 데이터, 화상 및 영상 등의 고품질 서비스를 제공하게 된다. 서비스 내용 중에서 가장 중요한 요소는 데이터 전송률로 동화상의 멀티미디어를 처리하려면 데이터 전송률이 2Mbps 정도는 되어야 한다. 따라서 고속으로 데이터를 전송하려면 무선 접속칩의 수용률도 커져야 하기 때문에 W-CDMA방식의 개발이 요구되고 있다. 또한 IMT-2000은 무선망뿐만 아니라 광대역 데이터 전송을 처리할 수 있는 ATM망과 연동이 되어야 하고, 이동성과 부가서비스를 위한 차세대 지능망이 추진되어야 한다.

IMT-2000 시스템에서 위치등록에 따른 가입자 인증 방식은 기존의 이동 통신 시스템에서 채택하고 있는 바와 같이 위치관리를 담당하는 LR(Location Register)을 VLR(Visitor Location Register)과 HLR(Home

Location Register)로 나누는 구조가 그대로 적용될 것이며, 사업자간 또는 국가간의 글로벌 로밍을 위해서는 로밍 사용자의 위치관리를 수행하는 GLR(Global Location Register)이 추가될 것이다. GLR은 방문 망에 대해서는 홈 망의 기능을 대리수행하고, 홈 망에 대해서는 방문 망의 기능을 수행함으로써 빈번한 위치등록과 인증 등으로 인한 국제회선의 비효율적인 사용을 감소시킬 수 있다. 현재 ITU(International Telecommunication Union)에서 IMT-2000 시스템의 표준화 작업을 진행하고 있으며 정보보호 서비스를 위한 2개의 권고안(M.1078, M.1223)을 승인하였다. 하지만 두 개의 권고안에는 구체적인 알고리즘이나 가입자 인증 프로토콜이 없는 상황이며 본 논문에서는 아직 제안되지 않은 IMT-2000 시스템 환경 하에서의 가입자 인증 프로토콜을 제안한다.

5. 제안된 IMT-2000 환경에서의 인증 프로토콜

본 장에서는 박창섭 등[7]이 제안한 오류수정부호를 이용하여 IMT-2000 환경에서 가입자의 익명성과 추적 불가능성을 제공하는 가입자 인증 프로토콜을 제안한다.

5.1 가입자 익명성과 추적 불가능성을 제공하는 인증 프로토콜

박창섭 등[7]은 오류수정부호와 비밀키 인증서를 이용하여 이동 가입자 MU(Mobile User)를 인증서버 AS(Authentication Server)가 인증하는 도전/응답 인증 프로토콜을 제안하였다.

오류수정부호는 채널오류나 잡음을 가진 통신망 내에서 신뢰성을 제공하기 위해 사용되어진다. 암호학에 적용된 오류수정부호의 응용은 McEliece[11]에 의해 처음 소개되었다. 이것은 Berlekamp, McEliece, Van Tilborg에 의해 작성된 선형블록코드의 일반적인 복호화 문제가 NP-complete라는 초기 논문의 결과이다. 길이가 N, 차원이 K, 그리고 최소거리가 D인 선형 오류수정부호는 (N, K, D)로 표기되어진다. 이진 k-tuple의 메시지 m은 $c = m \cdot G$에 의해 N 비트의 코드워드로 부호화 되어지고 오류벡터 e가 추가되어 $c' = c + e$ 벡터의 결과가 되어진다. 여기서, G는 $K \times N$의 생성행렬이다. 만약, e의 해밍 가중치가 $t = \lfloor (D-1)/2 \rfloor$ 보다 작거나 같다면 c'는 신드롬 벡터 $s = c' \cdot H^T$를 사용하여 c로 복호화될 수 있다. 여기서, H는 $G \cdot H^T = 0$이 되는 $(N-K) \times N$ 패리티 검사행렬이다.

사전 단계로 AS는 적합한 가입자로서 MU를 등록시키고 비밀키 k와 부호화된 비밀키 인증서 $c = m \cdot G$를 제공한다. 여기서, 메시지 $m = f(k_{AS}, [id, k])$은 실제 신분 id와 MU의 비밀키 k를 AS 자신만이 알고 있는 비밀키 k_{AS}를 사용하여 암호화한 비밀키 인증서이다. 여기서 $f()$는 대칭형 암호 알고리즘이다. 다음은 박창섭 등[7]의 인증 프로토콜을 나타내고 있다.

[프로토콜]
MU ← AS : r
MU → AS : $m \cdot G + e$

AS에 의해 생성되어진 난수 r을 이용하여 MU는 응답으로 $h(k, [r, id])$를 계산한다, 여기서, $h()$는 키를 이용하는 해쉬 함수이고 k는 MU의 비밀키이다. 다음으로 해쉬 값 $h(k, [r, id])$을 길이 N, 해밍가중치 $t = \lfloor (D-1)/2 \rfloor$인 오류 벡터 e로 변형시키고 이 오류 벡터 e를 추가한 부호화 된 비밀키 인증서 $m \cdot G + e$를 AS에게 보낸다. 여기서 해쉬 값 $h(k, [r, id])$는 [10]의 알고리즘을 이용하여 오류 벡터 e로 변형시킬 수 있다.

$m \cdot G + e$를 수신한 후 AS는 복호화 과정을 수행하고 m과 마찬가지로 오류벡터 e를 식별한다. 이동 가입자의 실제 신분 id와 대응되는 비밀키 k는 $m = f(k_{AS}, [id, k])$을 AS의 비밀키 k_{AS}로 복호화하여 얻을 수 있다. 이제, AS가 MU의 신분을 확인하면 합법적인 가입자로 간주되어진다. 그 후 해쉬 값 $h(k, [r, id])$는 AS에 의해 계산된다. 만약, 계산된 해쉬 값이 e로부터 유도된 값과 같다면 AS는 MU를 인증한다.

5.2 제안된 인증 프로토콜

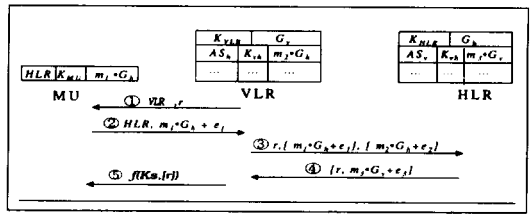
IMT-2000을 위한 가입자 인증 프로토콜 설계시 글로벌 로밍 서비스를 제공하기 위하여 단말기의 위치에 따라서 고려할 사항은 다음과 같다. 첫째, 자신이 가입한 IMT-2000 망 안에 단말기가 있을 경우, 둘째, 다른 지역(국가)의 IMT-2000망 안에 단말기가 있을 경우이다. 이 경우는 외부의 IMT-2000망에서도 동일한 서비스를 받도록 IMT-2000망간의 호환성을 유지시켜 주는 것이다. 셋째, 다른 외부 망(GSM, CDMA 등) 안에 단

말기가 있을 경우이다. 이 경우는 IMT-2000에서 목표로 정하고 있는 글로벌 로밍 서비스를 제공하기 위하여 전 세계의 모든 이동 통신 시스템과의 호환성을 유지시켜 주는 것이다. <표 1>은 본 논문에서 제안하는 프로토콜에서 사용되는 기호들이다.

5.2.1 자신이 가입한 IMT-2000 망 안에 단말기가 있을 경우

가입자의 단말기가 자신이 가입한 IMT-2000망 안에 있을 경우에 위치등록을 하는 인증 프로토콜 I을 제안한다. 인증 프로토콜 I에서는 홈 지역(HLR)을 제외한 어느 누구도 가입자 MU의 신원(ID)과 방문 지역(VLR)의 신원을 알 수 없다. 이 프로토콜의 기본적인 요구사항은 가입자 MU는 가입 신청시 그의 단말기 안에 홈 지역이 제공한 비밀키 K_{MU}와 비밀키 인증서 ($c = m_1 \cdot G_h$)를 저장하고 있고 각각의 LR들은 다른 LR들에게 발행한 비밀키 인증서를 생성하는 데 사용한 비밀키 K_{LR}과 생성행렬 G를 갖고 있고, 또한 각각의 LR들과 공유하는 공유키와 각각의 LR들이 발행한 비밀키 인증서를 저장하고 있는 데이터베이스를 가지고 있어야 한다. 하지만 각각의 LR들은 자신을 홈 지역으로 가지고 있는 가입자들의 비밀정보(공유키)에 대한 데이터베이스는 필요로 하지 않는다.

(그림 4)는 제안된 프로토콜 I의 수행과정을 나타낸 것이고 <표 2>는 프로토콜 I에서 사용된 기호이다.



(그림 4) 제안된 프로토콜 I

〈표 2〉 프로토콜 I에서 사용되는 기호

$m_1 = f(K_{HLR}, [MU, K_{MU}])$	$e_1 = Ks, h(K_{MU}, [r, MU])$
$m_2 = f(K_{HLR}, [VLR, K_{vh}])$	$e_2 = h(K_{vh}, [r, VLR])$
$m_3 = f(K_{VLR}, [HLR, K_{vh}])$	$e_3 = Ks, h(K_{vh}, [r, HLR])$

1. 이동 통신 가입자가 방문 지역으로 지역을 이동하였을 경우 VLR은 먼저 자신의 지역 내에 있는 단말기에게 VLR과 r을 시스템 방송한다.
2. 이 메시지를 받은 단말기는 자신이 홈 지역에 있지 않고 외부지역에 있다는 것을 인지하고 방문 지역(외부지역)에서 이동 통신 서비스를 얻기 위한 인증 프로토콜을 시작한다. 가입자의 단말기는 자신의 단말기내에 있는 비밀키 K_{MU}와 VLR로부터 받은 r을 이용하여 해쉬값 $h(K_{MU}, [r, MU])$를 구하고 나중에 VLR과 통신하기 위한 세션키 Ks를 생성해서 해쉬값과 함께 길이 N, 해밍가중치 t인 오류 벡터 e_1으로 변형시켜 오류 벡터 e_1을 추가한 부

〈표 1〉 제안된 프로토콜에서 사용되는 기호

MU	이동 통신 가입자(Mobile User)의 ID
VLR	(Visiting Location Register) 방문 지역에 있는 위치등록 DB(Data Base)의 ID
HLR	(Home Location Register) 홈 지역에 있는 위치등록 DB의 ID
GLR	(Global Location Register) 외부 네트워의 위치등록을 위한 DB의 ID
r	도전(Challenge)로 사용되는 난수열
K_{MU}	가입자 MU와 홈 지역의 위치등록 DB인 HLR과 공유하는 long-term key
$h(M)$	MAC 해쉬 함수
Ks	가입자 MU가 생성하는 MU와 VLR사이의 세션키
K_{vh}	VLR과 HLR이 공유하는 long-term key
K_{gh}	GLR과 HLR이 공유하는 long-term key
K_{gv}	GLR과 VLR이 공유하는 long-term key
$K_{HLR}, K_{VLR}, K_{GLR}$	각각 HLR, VLR, 그리고 GLR이 비밀키 인증서를 생성하는 master key
G_h, G_v, G_g	각각 HLR, VLR, 그리고 GLR의 생성행렬

* 각각의 LR에는 인증서버가 포함되어 있으므로 LR이 인증서버 역할을 한다고 표기함.

호화된 비밀키 인증서 $m_1 \cdot G_h + e_1$를 HLR과 함께 VLR에게 보낸다.

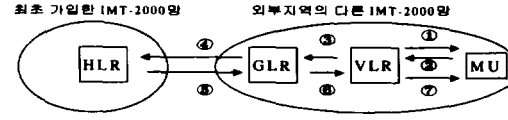
3. MU로부터 메시지②를 받은 VLR은 HLR이 MU를 인증하기 위한 메시지인 도전 값 r에 대한 응답 값 $m_1 \cdot G_h + e_1$과 자신의 신분을 HLR에게 인증시키기 위하여 난수열 r을 도전 값으로 하는 응답 값 $m_2 \cdot G_h + e_2$를 HLR에게 보낸다. $m_2 \cdot G_h$는 HLR이 VLR에게 발행한 부호화된 비밀키 인증서이다.
4. VLR으로부터 메시지③을 받은 HLR은 생성행렬(G_h)과 $G_h \cdot H^T$=0의 관계가 있는 패리티-검사 행렬 H를 이용하여 MU와 VLR의 각각의 오류가 추가된 부호화된 비밀키 인증서인 $m_1 \cdot G_h + e_1$과 $m_2 \cdot G_h + e_2$를 복호화하여 m_1, m_2, e_1, e_2를 식별한다. 그 다음 비밀키 인증서 m_1, m_2를 HLR 자신만이 알고 있는 비밀키인 K_{HLR}을 사용하여 복호화 함으로서 MU와 VLR의 신원을 확인하고 가입자 MU의 키인 K_{MU}를 뽑아낸다. 이제, HLR은 e_1의 해쉬값을 점검하여 가입자 MU가 합법적인 가입자인지를 인증(확인)하고 또한 e_2의 해쉬값을 점검하여 VLR을 인증한다. 다음 HLR는 자신의 데이터베이스의 $m_3 \cdot G_v$를 이용하여 VLR이 생성한 난수열 r을 도전 값으로 하는 응답 값 $m_3 \cdot G_v + e_3$ 쌍을 VLR에게 보낸다. $m_3 \cdot G_v$는 VLR이 HLR에게 발행한 부호화된 비밀키 인증서이다. e_3에는 HLR이 메시지③의 e_1에서 뽑아낸 가입자 MU와 VLR의 세션키 Ks가 포함되어 있다. 여기서 세션키 Ks는 가입자 MU와 VLR이 공유하며 데이터를 암•복호화하는 데 사용하게 될 키이다.
5. HLR으로부터 메시지④를 받은 VLR은 e_3의 해쉬값을 점검하여 HLR을 인증하고 또한, e_3에서 Ks를 뽑아내어서 MU와의 세션키로 사용한다. VLR은 비로소 HLR을 통해서 가입자 MU를 인증하게 된다. 그리고 VLR은 MU에게 $f(Ks,[r])$를 보낸다. 이 메시지를 받은 MU는 HLR과 VLR만이 Ks를 얻을 수 있으므로 HLR과 VLR을 인증할 수 있다.

5.2.2 다른 지역(국가)의 IMT-2000망 안에 단말기가 있을 경우

단말기가 다른 지역(국가)의 IMT-2000망 안에 있을 경우 위치등록을 하는 프로토콜을 제안한다. 본 논문에서 제안하는 프로토콜에서는 지역이 서로 다른 IMT-2000망들의 LR들이 위치등록 시 같은 인증 알고리즘을 사용한다고 가정한다. 단말기가 다른 IMT-2000망 안에 있을 경우에는 현재 단말기가 위치한 IMT-2000망의 VLR과 자신이 가입한 IMT-2000망의 HLR이 직접 위치등록을 위한 인증 프로토콜을 수행하지 않고 중간에 GLR을 두어서 계속적으로 일어나는 위치등록 필요시 GLR이 HLR의 역할을 하게 된다. 즉, GLR은 단말기가 가입한 IMT-2000망에 대해서는 VLR의 역할을 하고 현재 위치한 IMT-2000망에 대해서는 HLR 역할을 하게 된다.

i) 다른 IMT-2000망에서 최초의 위치등록

먼저 단말기가 다른 IMT-2000망에서 최초의 위치등록을 할 때 수행되는 인증 프로토콜 II(그림 5)를 살펴보겠다. <표 3>은 프로토콜 II에서 사용된 메시지와 기호들이다.



(그림 5) 제안된 프로토콜 II

〈표 3〉 프로토콜 II에서 사용된 메시지와 기호

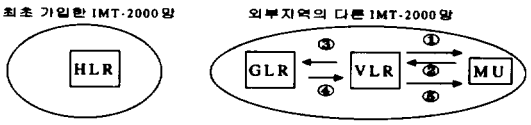
① VLR, r	
② HLR, $m_1 \cdot G_h + e_1$	
③ HLR, r, $[m_1 \cdot G_h + e_1]$, $[m_2 \cdot G_g + e_2]$	
④ HLR, r, $[m_1 \cdot G_h + e_1]$, $[m_3 \cdot G_h + e_3]$	
⑤ r, $m_4 \cdot G_g + e_4$, $f(K_{gh}, [Ks, K_{MU}, MU])$	
⑥ r, $m_5 \cdot G_v + e_5$, $m_6 \cdot G_g$	
⑦ $f(Ks, [r])$, $m_6 \cdot G_g$	
$m_1 = f(K_{HLR}, [MU, K_{MU}])$	$e_1 = Ks, h(K_{MU}, [r, MU])$
$m_2 = f(K_{GLR}, [VLR, K_{gv}])$	$e_2 = h(K_{gv}, [r, VLR])$
$m_3 = f(K_{HLR}, [GLR, K_{gh}])$	$e_3 = h(K_{gh}, [r, GLR])$
$m_4 = f(K_{GLR}, [HLR, K_{gh}])$	$e_4 = h(K_{gh}, [r, HLR])$
$m_5 = f(K_{VLR}, [GLR, K_{gv}])$	$e_5 = Ks, h(K_{gv}, [r, GLR])$
$m_6 = f(K_{GLR}, [MU, K_{MU}])$	

제안된 프로토콜 II에서 인증과 익명성 및 추적 불가능성을 제공하는 방식은 5.2.1의 프로토콜 I과 같은 방식으로 제공하며, 이 프로토콜에서 GLR은 메시지⑤를 받을 때 HLR으로부터 MU에 대한 비밀정보인

K_{MU}를 제공받아서 현재 위치해있는 IMT-2000망의 또 다른 지역에서 위치등록을 도전할 경우에 대비하여 메시지⑥에서 MU에게 줄 새로운 비밀키 인증서($m_6 \cdot G_g$)를 발급해서 VLR에게 전달해준다. 그러면 VLR은 메시지⑦에서 GLR로부터 받은 MU의 새로운 비밀키 인증서를 MU에게 전달한다. 새로운 비밀키 인증서를 받은 MU는 다음 위치등록을 위하여 이 인증서를 현재의 IMT-2000망에 있는 동안에는 저장하고 있어야 한다.

ii) 다른 IMT-2000망에서 첫 번째 이후의 위치등록

i)의 방법으로 위치등록을 위한 인증 프로토콜을 수행하고 현재의 IMT-2000망에 속하는 또 다른 지역으로 이동하여 위치등록을 할 경우의 인증 프로토콜 III (그림 6)은 다음과 같다.



(그림 6) 제안된 프로토콜 III

<표 4>는 프로토콜 III에서 사용된 메시지와 기호들이다.

〈표 4〉 프로토콜 III에서 사용된 메시지와 기호

① VLR, r ② $HLR, m_1 \cdot G_g + e_1$ ③ $HLR, r, [m_1 \cdot G_g + e_1], [m_2 \cdot G_g + e_2]$ ④ $r, [m_3 \cdot G_v + e_3]$ ⑤ $f(Ks, [r])$

$m_1 = f(K_{GLR}, [MU, K_{MU}])$	$e_1 = Ks, h(K_{MU}, [r, MU])$
$m_2 = f(K_{GLR}, [VLR, K_{gv}])$	$e_2 = h(K_{gv}, [r, VLR])$
$m_3 = f(K_{VLR}, [HLR, K_{gv}])$	$e_3 = Ks, h(K_{gv}, [r, GLR])$

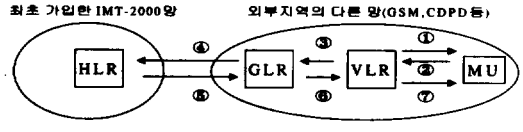
프로토콜 III는 다른 IMT-2000망에서 첫 번째 위치등록 이후의 두 번째 위치등록부터 해당되는 인증 프로토콜이다. 이 프로토콜에서는 GLR이 완전히 HLR의 역할을 수행하며 5.2.1의 프로토콜 I과 똑같은 형태를 띄며 인증과 익명성 및 추적 불가능성 또한 같은 방식으로 제공된다. MU는 첫 번째 위치등록 시 GLR로부터 받은 비밀키 인증서($m_1 \cdot G_g$)를 사용하여 GLR로부터 자신을 합법적인 가입자로 인증받는다.

5.2.3 다른 외부 망 안에 단말기가 있을 경우

IMT-2000 시스템은 글로벌 로밍을 목표로 하고 있기 때문에, 다른 외부망(CDMA, GSM 등)과의 연동을 필요로 하고 있다. 하지만 종류가 다른 망들은 각각이 다른 인증 프로토콜을 사용하기 때문에 각 망에 속한 LR들 또한 서로 다른 암호 알고리즘을 사용한다고 가정할 수 있다. 여기서 제안하는 프로토콜은 5.2.2의 프로토콜 II, III와 동일한 형태를 가지게 되나 VLR은 IMT-2000망과는 다른 종류의 외부 망이므로 오류수정부호와 비밀키 인증서 시스템을 갖추고 있지 않으며 제안하는 프로토콜은 다른 외부 망에 GLR을 두어서 IMT-2000망과 연동을 할 수 있게 하는 방식을 채택하였다. 여기서 GLR은 IMT-2000망과 같이 오류수정부호와 비밀키 인증서를 사용할 수 있게 설계를 하여 GLR이 HLR의 역할을 할 수 있도록 하였고 5.2.2의 프로토콜들과 다른 차이점은 VLR이 오류수정부호와 비밀키 인증서 시스템을 갖고 있지 않기 때문에 VLR과 GLR이 상호 인증하는 부분은 오류수정부호와 비밀키 인증서를 사용하지 않고 현재 그 망에서 사용하고 있는 인증 알고리즘을 사용하는 것이다. 여기서는 "인증 메시지"로 표현을 한다.

i) 다른 외부 망에서 최초의 위치등록

다른 외부 망 안에 IMT-2000 단말기가 있을 경우에 일어나는 인증 프로토콜 IV(그림 7)를 보겠다. <표 5>는 프로토콜 IV에서 사용된 메시지와 기호들이다.



(그림 7) 제안된 프로토콜 IV

〈표 5〉 프로토콜 IV에서 사용된 메시지와 기호

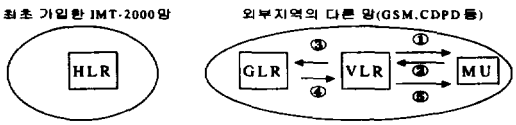
① VLR, r ② $HLR, m_1 \cdot G_h + e_1$ ③ $HLR, r, [m_1 \cdot G_h + e_1]$, 인증 메시지 ④ $HLR, r, [m_1 \cdot G_h + e_1], [m_3 \cdot G_h + e_3]$ ⑤ $r, m_4 \cdot G_g + e_4, f(K_{gh}, [Ks, K_{MU}, MU])$ ⑥ 인증 메시지, $m_6 \cdot G_g$ ⑦ $f(Ks, [r]), m_6 \cdot G_g$

$m_1 = f(K_{HLR}, [MU, K_{MU}])$	$e_1 = Ks, h(K_{MU}, [r, MU])$
$m_3 = f(K_{HLR}, [GLR, K_{gh}])$	$e_3 = h(K_{gh}, [r, GLR])$
$m_4 = f(K_{GLR}, [HLR, K_{gh}])$	$e_4 = h(K_{gh}, [r, HLR])$
$m_6 = f(K_{GLR}, [MU, K_{MU}])$	

제안된 프로토콜 IV에서 인증과 익명성 및 추적 불가능성을 제공하는 방식은 5.2.2의 프로토콜 II와 같은 방식으로 제공하며, VLR이 인증을 위하여 사용하는 알고리즘이 IMT-2000 시스템의 LR들과 다르므로 VLR과 GLR의 상호 인증에 대해서는 현재 그 망에서 사용 중인 인증 알고리즘을 이용한 메시지란 뜻에서 "인증 메시지"라고 표현하였다.

ii) 다른 외부 망에서 첫 번째 이후의 위치등록

i)의 방법으로 위치등록을 위한 인증 프로토콜을 수행하고 현재의 다른 외부 망에 속하는 또 다른 지역으로 이동하여 위치등록을 할 경우의 인증 프로토콜 V (그림 8)은 다음과 같다. <표 6>은 프로토콜 V에서 사용된 메시지와 기호들이다.



(그림 8) 제안된 프로토콜 V

〈표 6〉 프로토콜 V에서 사용된 메시지와 기호

① *VLR, r*	
② *HLR,* $m_1 \cdot G_g + e_1$	
③ *HLR, r,* $[m_1 \cdot G_g + e_1]$*, 인증 메시지*	
④ *인증 메시지*	
⑤ $f(Ks, [r])$	
$m_1 = f(K_{GLR}, [MU, K_{MU}])$	$e_1 = Ks, h(K_{MU}, [r, MU])$

제안된 프로토콜 V는 다른 IMT-2000망에서 첫 번째 위치등록 이후의 두 번째 위치등록부터 해당되는 인증 프로토콜이다. 이 프로토콜에서는 GLR이 완전히 HLR의 역할을 수행하며 5.2.2의 프로토콜 III와 똑같은 형태를 가지며 인증과 익명성 및 추적 불가능성 또한 같은 방식으로 제공된다. MU는 첫 번째 위치등록 시 GLR로부터 받은 비밀키 인증서($m_1 \cdot G_g$)를 사용하여 GLR으로부터 자신을 합법적인 가입자로 인증받고 프로토콜 IV와 같이 GLR과 VLR의 상호 인증을 위한 메시지는 현재 그 망에서 사용 중인 인증 알고리즘을 이용한 메시지란 뜻에서 "인증 메시지"라고 표현하였다.

5.3 제안된 프로토콜들의 분석 및 평가

제안된 인증 프로토콜들(I, II, III, IV, V)은 도전/응답(Challenge/Response) 메시지를 주고받으면서 가입자의 인증 서비스를 제공하여 부정당한 가입자의 불법 사용 문제를 해결하고 MU와 VLR이 세션키를 공유하여 메시지 암호를 통한 도청 문제를 해결한다. 그리고 박창섭 등[7]이 제안한 비밀키 인증서를 사용하여 가입자 익명성을 제공하며 매 세션마다 오류수정부호의 가변적인 오류벡터로 인한 가입자의 추적 불가능성 서비스를 제공해 준다.

기존의 인증 프로토콜들은 크게 비밀키 방식과 공개키 방식으로 나눌 수 있다. 비밀키 암호 알고리즘을 사용한 기존의 인증 프로토콜[3]은 단말기에 적은 계산능력을 요구하는 이동 통신 환경의 인증 프로토콜에 적당한 방식이다. 하지만 비밀키 방식을 사용할 때 모든 인증 서버들은 자신을 홈 지역으로 등록한 가입자들의 비밀정보(공유키)들을 안전하게 관리해야하는 방대한 데이터베이스의 안전성 문제가 생기게 된다. 이런 문제점은 공개키 방식[9]을 사용하면 쉽게 해결할 수 있으나 공개키 연산은 비밀키 연산에 비해 단말기에 매우 많은 계산능력을 요구하고 있다. 하지만 단말기 안에 있는 스마트 카드는 공개키 연산을 하기에는 계산능력에 한계가 있으므로 공개키 암호 방식은 이동 통신 환경의 인증 프로토콜에 적합하지 않다. 제안된 인증 프로토콜들은 비밀키 방식의 문제점인 방대한 데이터베이스 문제점을 비밀키 인증서를 사용하여 해결하고 인증 프로토콜 수행 시 오류수정부호, 해쉬 함수 그리고 비밀키 암호 알고리즘을 사용하여 공개키 암호 알고리즘을 사용한 프로토콜의 문제점인 단말기에 과중한 계산능력을 요구하는 문제점을 해결하였다. 기존의 프로토콜들에서 단말기가 자신을 인증 서버에 인증시키기 위해서는 비밀키 알고리즘 연산 또는 공개키 알고리즘 연산 등을 필요로 했는데, 제안된 프로토콜들은 빠른 해쉬 알고리즘과 오류수정부호를 사용하고 비밀키 알고리즘 연산의 회수도 최소로 사용하게 된다. 즉, 기존의 어떤 프로토콜보다도 단말기에 가장 적은 암호학적 연산이 요구되는 프로토콜이다.

제안된 프로토콜들에서 각각의 지역 인증 서버들은 상대편에 대한 비밀키 인증서를 저장하는 데이터베이스를 갖는 것을 전제로 하고 있다. 인증 서버들간의 인증을 제공하는 기존의 프로토콜들[3,9]에서도 마찬가지로 인증 서버들간의 인증을 위하여 공유키를 저장하는 데이터베이스를 갖고 있으므로 기존 프로토콜[3,9]의 데이터베이스에 인증서 필드항목을 하나 추가 시켜

서 보관하면 보안상에 문제점이 증가된 것은 없고 단지 이동 통신 사업을 시작할 때 각각의 인증 서버들간의 공유키를 생성함과 함께 인증서를 같이 생성해서 각각의 인증서버들의 데이터베이스에 저장하면 된다. 제안된 프로토콜들은 인증서버들간의 인증을 제공하는 기존의 프로토콜[3,9]보다 이동 단말기뿐만이 아니라 LR(VLR, HLR)들이 수행해야 하는 암호학적 연산이 줄어들었다. [3,9]의 프로토콜에서 인증 서버들은 서로 자기자신을 인증시키기 위해서 비밀키 암호 알고리즘과 해쉬 알고리즘을 수행한다. 하지만 제안된 프로토콜들에서는 오류수정부호와 해쉬 알고리즘을 사용하므로 인증서버 측면에서 [3,9]의 프로토콜보다 효율적이다.

GSM과 CDPD에서 인증서버가 단말기를 인증하는 일방향 인증만을 제공하고 VLR과 HLR간의 보안 서비스가 불완전한 단점을 제안된 가입자 인증 프로토콜들은 MU, VLR 그리고 HLR 모두의 상호 인증을 제공하여 보안을 강화하였다. 이런 점은 제안된 프로토콜들이 로밍 환경에서의 보안 서비스를 충분히 제공할 수 있음을 나타낸다. 제안된 프로토콜은 GSM과 CDPD의 인증 프로토콜이 비밀키 방식을 사용하기 때문에 발생하는 가입자의 방대한 데이터베이스 관리의 안전성 문제를 비밀키 인증서를 이용하여 해결하였다. 또한 제안된 프로토콜은 GSM과 CDPD에서 가입자의 신원을 방문 지역의 인증 서버가 알 수 있는 단점을 비밀키 인증서를 이용하여 해결하였다. 즉, 제안된 프로토콜들은 가입자의 신원을 홈 지역의 인증 서버만이 알 수 있도록 하여 GSM과 CDPD보다 더 높은 익명성을 제공한다. 제안된 프로토콜들은 GSM의 문제점인 추적 불가능성을 오류 수정부호를 이용하여 해결하였고 공개키 방식의 가입자 인증 프로토콜의 문제점인 단말기의 낮은 계산능력과 적은 배터리 용량을 고려하여 가장 적은 암호학적 연산이 요구되는 프로토콜들을 제안하였다.

6. 결 론

본 논문에서는 박창섭 등[7]이 제안한 비밀키 인증서와 오류수정부호의 개념을 IMT-2000 시스템 환경에 맞게 설정하여 이동 통신 가입자의 프라이버시를 보장하고 IMT-2000 시스템의 목표 중의 하나인 글로벌 로밍을 지원하기 위한 가입자 인증 프로토콜들을 제안하였다. 기존의 이동 통신 인증 프로토콜인 GSM과 CDPD의 문제점을 지적하고 그 문제점을 해결하는 새로운 방향을 제시하였다. 제안된 프로토콜들은 가입자의 익명성을 제공하기 위하여 비밀키 인증서를 가입자의 단말기에 저장하여 인증 프로토콜의 수행시 가입자가 자신의 신분확인을 위하여 이 비밀키 인증서를 인증 서버에 전송하는 방식을 채택하여 인증서버들이 가입자들의 비밀정보(공유키)들을 관리하는 방대한 데이터베이스 문제를 해결하였고, 오류 수정부호를 이용하여 가입자의 익명성과 추적 불가능성을 제공하였다. 기존의 프로토콜이 익명성을 제공하기 위하여 공개키 방식의 가명을 사용함으로써 단말기에 과중한 계산능력을 요구하는 반면, 제안된 프로토콜들은 비밀키 암호 알고리즘과 오류수정부호 그리고 해쉬 함수만을 사용하여 단말기의 낮은 계산능력을 고려하여 설계하였다.

참 고 문 헌

[1] M. Rahnema, "Overview of the GSM System and Protocol Architecture," IEEE Communications Magazine, April 1993.

[2] R. Rivest. "The MD5 message-digest algorithm," RFC 1321, Network Working Group, 1992.

[3] R. Molva, D. Samfat, G. Tsudik, "Authentication of Mobile Users," IEEE Network Magazine, Special Issue on Mobile Communications, March/April 1994.

[4] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol.22, pp.644-655, 1976.

[5] Cellular Digital Packet Data(CDPD) System Specification, Release 1.0, July 19, 1993.

[6] European Telecommunications Standards Institute, Universal Personal Telecommunications, ETSI NA7 WP1, November 1992.

[7] 박창섭, 이수연, 이동훈, "오류수정부호를 이용한 익명성과 인증의 통합", WISC'98, pp.405-412, 1998.

[8] M J. Beller, L F. Chang, Y. Yacobi, "Security for Personal Communications Services : Public-Key vs. Private Key Approaches," Proceedings of 2nd International Symposium on Personal, Indoor and Mobile Radio Communications, October 1992.

[9] D. Samfat, R. Molva, N. Asokan, "Anonymity and Untraceability in Mobile Networks," Proc. of

the ACM International Conference on Mobile Computing and Networking, Nov. 1995, Berkeley, Ca.

[10] C. S. Park, "Improving Code Rate of the McEliece Public-Key Cryptosystem," Electronics Letters, Vol.25, No.21, pp.1466-1467, 1989.

[11] R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory," DSN Progress Report, Jet Propulsion Lab., Ca., pp.42-44, Jan. and Feb. 1978.

[12] Ken Buchanan et al., "IMT-2000 Standards : Service Provider's Perspective," IEEE Personal Communications, Vol.4 pp.8-13, August 1997.

[13] Rah Pandya et al., "IMT-2000 Standards : Network Aspects," IEEE Personal Communications, Vol.4, pp.20-29, August 1997.

[14] Richard D. Carsello et al., "IMT-2000 Standards : Radio Aspects," IEEE Personal Communications, Vol.4, pp.30-40, August 1997.

[15] Y. Frankel, A. Herzberg, P. A. Karger, H. Krawczyk, C. A. Kunzinger, and M. Young, "Security Issues in a CDPD Wireless Network," IEEE Personal Communications, Vol.2, No.4, pp.16-27, August 1995.

강 형 우

e-mail : kanghw@etri.re.kr

1997년 고려대학교 전산학과 졸업(학사)

1999년 고려대학교 대학원 전산학과(이학석사)

1999년~현재 한국전자통신연구원 정보보호기술연구본부 연구원

관심분야 : 정보보호, 알고리즘 등

윤 이 중

e-mail : yej@etri.re.kr

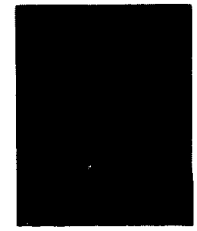
1988년 인하대학교 전자계산학과 졸업

1990년 인하대학교 전자계산학과 석사 졸업

1997년~현재 충남대학교 전산전공 박사과정

1990년~현재 한국전자통신연구원 정보보호기술연구본부 선임연구원

관심분야 : 정보보호



이 수 연

e-mail : sylee@mail.chonan-c.ac.kr

1990년 2월 단국대학교 전자계산학과(이학사)

1993년 2월 단국대학교 전산통계학과(이학석사)

1996년 2월 성균관대학교 정보공학과 박사과정 수료

1997년 3월~현재 천안외국어대학 사무자동화과 전임강사

관심분야 : 암호와 부호이론, 정보보호기술, 무선통신망 프로토콜 설계 및 성능분석

박 창 섭

e-mail : csp0@unitel.co.kr

1983년 연세대학교 경제학과 졸업

1983년 1983년 한국 IBM System Administration 근무

1985년~1987년 미국 LEHIGH Univ. 전산학 석사

1987년~1990년 미국 LEHIGH Univ, 전산학 박사

1990년~현재 단국대학교 전자계산학과 부교수

관심분야 : 암호이론 부호이론, 네트워크 보안

이 동 훈

e-mail : donghlee@tiger.korea.ac.kr

1984년 고려대학교 경제학과 졸업

1985년~1988년 미국 Univ. of Oklahoma 전산학 석사

1988년~1992 미국 Univ. of Oklahoma 전산학 박사

1992년~1993 단국대학교 전자계산학과 전임강사

1993년~현재 고려대학교 전산학과 부교수

관심분야 : 암호이론, 계산이론