論文 96-21-3-15

디지털 이동 통신을 위한 안전 대책

正會員 박 춘 식*

Security Planning for Digital Mobile Communications

Choon Sik Park* *Regular Member*

요 약

본 논문에서는 미국의 EIA/TIA의 표준인 CMDA 관련 security와 유럽의 ETSI의 표준인 GSM 관련 secuirty 그리고 공개키 암호 방식을 이용한 security 방식들에서 제공되는 디지털 이동 통신을 위한 안전 대책들을 다루고자 한다. 이들 각 방식들에 대하여, 통신 사업자가 고려하여야 하는 security 서비스 그리고 키 관리 방안들을 중심으로 한 비교 분석을 하고자 한다. 이러한 분석을 토대로 하여 국내 디지털 이동 통신에 적용가능한 체계적인 안전 대책을 제안한다.

ABSTRACT

This paper deals with the security planning for digital mobile communications provided in CDMA and GSM security standards and the public key cryptosystem security methods. In this paper, we provide a comparison of these methods with respect to security services and key management. Based upon this analysis, we also present a security planning which is applicable to the domestic digital mobile communications.

I. 서 론

자동차 전화, 무선 호출기, 휴대용 전화 등의 이동 통신 서비스를 이용하는 이용자의 수는 앞으로도 계속해서 늘어날 전망이다. 특히 우리나라에서는 1996년의 CMS(CDMA Mobile System) 상용화를 계기로 세계 최초로 CDMA(Code Division Multiple Access) 방식을 이용한 이동 통신 서비스를 제공하는 나라가 될 것이다.

한편, 이러한 이동 통신 서비스의 수요가 폭발적으로 증가하는 일면에 무선 통신망을 이용하는 이동 통신의 특성때문에, 불법적인 사용이나 도청 또는 추적을 통한 불법적인 행위나 각종 통신 범죄 행위 등도 늘어나게 된다. 이러한 행위들은, 통신 사업자의 수익 감소로 인한 경영상의 압박과 가입자에 대한 서비스의 저하, 그리고 개인의 프라이버시 침해 등의 역기능적인 문제를 가져오게 된다. 예로써, 이동 통신의 불법 사용에 대한 문제가 미국 사회에서 심각하게 대두되고 있다. 1994년 한 해 동안의 뉴욕에서 이동 통신

*한국전자통신연구소 책임연구원
論文番號:95334-0925
接受日字:1995年 9月 25日

사업자가 위조로 인하여 손해를 입은 총액이 5천만불($50 million)이며, 미국 전역에서는 5억불($500 million)에 상당한다[1]. 또 다른 보고인 뉴욕의 셀룰라 코퍼레이션사에 의하면, 전파스캐너를 이용하여 해당전화 번호를 알아낸 후, 이를 무선전화기에 주입하여 암거래하는 전화도둑들이 늘어나고 있으며, 가입비를 내지 않고도 무제한으로 사용할 수 있다는 점때문에 유학생이나 영세 수출입자로 부터 폭발적인 인기를 끌고 있다고 한다. 이 보고에서, 이 같은 도용전화비 규모는 하루 평균 3백만달러가 넘는 것으로 덧붙이고 있으며, 월 1백달러 정도를 사용하던 가입자가 어느날 갑자기 2만달러의 전화요금고지서를 받게 되는 일도 발생하고 있다고 한다[2].

최근, 이러한 불법 사용에 대한 대책과 안전한 이동 통신 서비스를 마련하기 위하여 각국의 이동 통신 업무의 표준화에 인증 기능등을 추가하여 권고하고 있다. 미국의 TIA/EIA(Telecommunications Industry Association/Electronic Industries Association)에서 무선 인터페이스 표준안[3]으로 권고 하고 있는 CDMA용 인증 및 암호화 기능이나, 유럽 국가에서 ETSI(European Telecommunications Standards Institute)의 표준화로 추진하고 있는 GSM(Global System for Mobile Communications)[4]이나 DECT(Digital European Cordless Telecommunications)[5] 표준에서도 인증을 포함한 security 서비스를 권고하고 있다. 이들 표준들은 PCS(Personal Communications System)나 FPLMTS (Future Public Land Mobile Telecommunications System) 등을 비롯한 디지털 이동 통신을 위한 안전 대책으로도 널리 검토되어 왔으며, 이와 관련한 많은 연구도 행하여 지고 있다[6], [7], [8], [9], [10], [11], [19]. 우리나라에서도 아날로그 및 CDMA 방식 차량 전화 시스템의 이동국과 기지국간의 분계점인 무선 인터페이스에 관한 TTA(Telecommunications Technology Association)표준[14]에서도 인증 기능의 제공을 권고하고 있다.

이들 표준들은 인증 및 암호 기능을 제공하기 위해서 모두 비밀키 암호 방식(Conventional or Private Key Cryptosystem)[12], [13]을 채택하고 있다. 이는 security 서비스의 제공으로 인한 시스템에 미치는 부하의 증가, 단말기 소형화에 따른 계산 능력의 문제점 등을 고려하여 선정한 것으로 추정된다. 그러나 거대한 데이터 베이스의 안전 관리, 기지국에서 인증센터로의 인증 및 암호 관련 정보 요구에 따른 트래픽 증가와 집중화 현상은 시스템 전체의 부하에 크게 영향을 미치게 되는 방식이다.

반면, 비밀키 암호 방식에 의한 security 서비스의 제공에 대한 취약점을 개선하기 위하여, 공개키 암호 방식[15], [20]을 이용한 각종 방안들이 제시되고 있다[16], [17], [18]. 이들은 비록 시스템의 부하(공개키 암호를 이용한 인증 프로토콜은 비밀키 암호 방식을 이용한 프로토콜보다는 단순화될 수 있으나 공개키 암호의 사용으로 인한 많은 양의 데이타가 증가된다.)를 증대시키는 등 실현이 용이하지 않은 부분도 있으나, 앞으로의 반도체 칩의 기술 발달이나 소형화 기술, 그리고 계산 능력의 향상에 따라 표준으로의 검토도 이루어지고 있다.

본 논문에서는 먼저 이들의 security 서비스를 검토하여 보고, 국내 이동 통신 서비스의 security 서비스 정책을 수립하는 데 적용될 수 있는 방안을 제시하고자 한다. 제안 방안은 먼저 1단계와 2단계로 구분하여 서비스를 제공하는 방안으로, 기존의 각종 방식에서 구체적으로 제시되고 있지 않는 키 관리 시스템을 포함하므로써, 보다 실용적인 security planning이 가능하도록 하였다.

본 논문은 모두 Ⅵ개장으로 구성된다. 먼저, 이동 통신에 있어서 예상 security 위협요소와 이들에 대한 대책으로서의 security 서비스를 2장에서 정의한다. 3장에서는 이동 통신에서의 대표적인 표준들인 미국의 CDMA용 표준과 유럽의 GSM용 표준에서 제공되고 있는 security 서비스들을 살펴본다. 4장에서는 표준으로는 채택되지 않았지만 공개키 암호를 이용하는 대표적인 2가지 방식을 소개하고, 그들이 제공하는 security 서비스들을 중심으로 정리하고자 한다. 5장에서는 검토한 방식들을 참고로 하여 security 서비스와 키 관리 방안을 중심으로 하는 새로운 security planning을 제안하고자 하며 결론은 6장에 언급하고자 한다.

Ⅱ. Security 위협요소와 Security 서비스

2.1 Security 위협요소

디지털 이동 통신에 있어서의 secuity 위협 요소로

는 다음 사항들이 고려될 수 있다.

- 불법 사용
  정당한 사용자의 번호를 도용하거나, 분실 및 도난에 의한 단말기를 불법으로 사용하여 통신 사업자와 합법적인 가입자에게 과금의 혼란으로 인한 막대한 피해를 주게 된다.

- 가입자정보(데이터와 signalling 정보)의 도청(eavesdropping) 및 가로채기(interception)
  무선 통신의 취약성 때문에 누구든지 쉽게 다른 사용자의 통화 내용을 청취할 수 있다. 비록 암호화가 되었을 경우라도, 암호 알고리즘의 안전성이 취약하거나 관련 프로토콜이 안전하지 못할 경우도 통화내용이 도청될 수 있다.

- 추적(tracing)에 의한 프라이버시 침해
  이동 통신에서는 단말기 사용자에 관한 정보 및 위치 정보가 억세스 채널에서 평문 형태로 무선 구간에 전달될 수 있다. 이러한 정보들은 누가 언제 통화를 했는지 그리고 단말기 사용자의 위치 정보를 이용하여 사용자의 행방을 쉽게 추적하는 데 이용될 수 있다. 제3자 외에도 네트워크 내의 인증 센터나 기지국 등이 결탁하거나, 불법 행위를 할 경우, 특정 단말기 사용자의 추적은 쉽게 행하여 질 수 있다.

2.2 Security 서비스

Security 정책 수립에서 다루어야 하는 security 서비스는 무선 통신 구간을 이용하는 이동 통신의 상황을 고려하여 제공되어야 한다. 디지털 이동 통신에 있어서의 security 위협 요소에 대처하기 위한 기본적인 security 서비스로써 고려될 수 있는 사항들은 다음과 같다.

- 인 증
  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 사업자에 대해서는 반드시 고려하여야 할 security 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 단말기 사용자의 신분 확인이 반드시 이루어져야 한다. 이러한 인증 작업은 인증 알고리즘과 인증 프로토콜에 의해서 이루어 질 수 있다.

- 암 호
  이동 통신은 무선 구간을 통한 이동 통신의 특성 때문에 불법 도청이 가장 용이하여 안전성 측면에서 가장 취약하다. 즉 누구든지 통화중의 내용을 쉽게 그리고 발각되지 않고 도청할 수 있다. 이러한 관점에서 무선 구간의 통화 내용은 반드시 암호화되어 보내어져야 한다. 단말기 사용자의 음성 정보 및 신호 정보는 도청 및 가로채기에 대한 대책으로써 암호화가 이루어져야한다. 이러한 암호화는 암호화에 사용될 키(세션 키)가 선행되어 공유되어야 하며, 반드시 인증 절차가 완료된 후에 수행되어져야 한다.

- 추적 불가능성(party anonymity)
  추적 불가능성은 단말기 사용자의 프라이버시를 제공해주는 기능이다. 송수신자의 위치정보나 통화당사자에 대한 정보가 제3자에게 노출되어 추적되는 것을 방지하기 위해서는, 공개 키 암호를 사용하면 쉽게 해결할 수 있다. 그러나, 공개 키 암호의 사용도 인증센터나 기지국 등의 결탁에는 효과가 없으므로, 이때에는, 익명통신로(Anonymous Communication Network)[23], [24]를 이용한 방식[25], [26]을 활용하여 안전성을 증가시킬 수 있다.

Security 서비스와 관련하여 security 정책 수립에서 고려하여야 할 사항으로 키 관리 문제가 있다. 이는 대부분의 방식에서 거의 언급되지 않고 있는 부분으로 security 서비스와 밀접한 관계가 있다.

• 키 관리

인증, 암호 그리고 추적 불가능의 서비스를 제공하기 위해서는 암호 알고리즘의 사용이 필수적이다. 이러한 알고리즘이나 각종 방식에 사용되는 주요한 변수나 키들을 어떻게 관리하는 지에 따라 시스템 전체의 안전이 위태롭게 될 수가 있다. 또한, 인증 센터가 별도의 키 관리 센터를 필요로 하는 지, 또는 인증 센터 자체가 키 관리 센터를 겸하는지 등의 시스템의 안전을 제공하기 위한 키 관리 기능이 제공되어야 한다.

Ⅲ. 비밀키 암호를 이용한 Security Policies

이동 통신의 인증 및 암호 기능의 제공을 위하여 비밀 키 암호 방식을 채택한 방식들이 널리 알려져 있다[3], [4], [5], [7], [10], [19]. 본장에서는 이중에서 미국과 유럽의 표준으로 각각 알려져 있는 CDMA 이동 통신 표준 방식[3]과 GSM 표준 방식[4]에 대해서, 제공되고 있는 security 서비스와 키 관리면을 중심으로 살펴보고자 한다.

3.1 CDMA Security 서비스

3.1.1 인 증

CDMA 가입자 인증은 가입자 이동국의 등록, 발호 및 착호시에 사용자의 정당성을 확인한다. 이때 인증이 실패할 경우, 유일시도응답절차(Unique Challenge Response Procedure)가 수행되며 이것마저 실패할 경우는 진행중인 호를 중지하거나 SSD(Shared Secret Data)를 새롭게 갱신하여 사용한다. 등록, 발호 및 착호시의 인증 프로토콜은 서로 유사하므로, 이동국의 발호시 사용자의 정당성을 확인하는 이동국 발호 인증 프로토콜만을 설명하면 다음과 같다.(그림 1 참조)

(step 1) 가입자 *B*와의 통화를 원하는 이동국 가입자 *A*는 시스템에 대하여 통화 시도를 행한다.

(step 2) 시스템의 인증 센터(또는 기지국 등)는 32비트 난수 데이터 RAND를 *A*에게 전송한다.

(step 3) *A*는 수신한 RAND, 이동국의 장치 일련번호 ESN(Electronic Serial Number), 상대방 통화자 *B*의 전화번호 그리고 공유 비밀 데이터 SSD_A를 해쉬 함수(CAVE(Cellular Authentication and Voice Encryption) 또는 인증절차로 표기됨)에 입력하여 18비트 인증 부호 AUTHR를 생성한다. *A*는 인증 부호 AUTHR, 수신한 RAND의 상위 8비트인 RANDC, ESN, 상대방 통화자의 전화번호 관련 DIGITS 그리고 COUNT 정보를 인증 센터에 보낸다.

(step 4) 인증 센터는 수신된 정보중 먼저 자신의 저장 정보 RAND의 상위 8비트와 수신한 RANDC를 비교한다. 비교가 일치할 경우는 RAND, 수신한 ESN과 상대방 통화자의 전화번호 그리고 *A*에 해당하는 데이터 베이스에 등록되어 있는 *A*의 비밀 공유 데이터, SSD_A를 입력으로 한 해쉬함수의 값 AUTHR을 생성하여 수신된 *A*로 부터의 AUTHR 값과 비교한다. 또한 수신된 COUNT값과 인증 센터가 저장하고 있는 가입자 *A*의 COUNT값을 비교하여 최종적으로 인증을 완료하여 채널 할당을 승인하며 아울러 COUNT값을 갱신하고 *A*에게 통보한다.

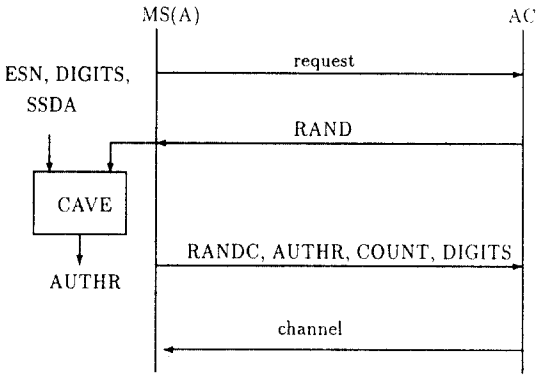

그림 1. CDMA에서의 발호 인증

단말기 사용자가 방문 네트워크(Visiting Network)에 위치하여 통화를 시도할 경우의 인증을 고려하면, 방문 네트워크에서는 사용자의 홈 네트워크(Home Network)에 인증 관련 정보(SSD_A, SSD_B, Count 정보, 사용자 관련 정보 등)를 요청하여 위의 인증 절차를 수행하게된다. 이러한 방식은 GSM방식 보다는 적은 양의 트래픽으로 가능하며, count 정보의 사용으로

인한 불법 복사 단말기 사용에 대한 구별이 가능하나, 방문 네트워크와 홈 네트워크 사이의 가입자 비밀 정보 전송으로 인한 취약점이 있으므로, 중간 경로에 대한 암호화 대책이 필요하다.

3.1.2 암 호

CDMA에서 보호 대상이 되는 것은 음성 정보와 신호 정보로서, 스크램블링(Scrambling)이나 암호화(Ciphering)에 의해서 암호 기능이 제공되고 있다. 스크램블링을 위해서는 공용 긴 코드 마스크(Public Long Code Mask)와 개별 긴 코드 마스크(Private Long Code Mask)가 공용 그리고 특정 개인용 키로써 사용되며, 암호화(Ciphering)에 비하여 안전도가 떨어지는 방식이다. 암호화에 의한 방식은 표준 자료에는 언급되어 있지 않다. 그러나 암호화용의 키로써는 SSD_B가 사용되리라 추정되며 단말기와 인증 센터가 이를 보관 관리하게 된다. 이러한 암호 기능은 반드시 인증 기능이 수행된 후에 행하여진다.

3.1.3 추적 불가능성

이동국은 통화를 요구할 시 네트워크측에 자신의 Identity나 통화하고자 하는 상대방의 전화번호 등을 평문으로 인증관련 정보와 함께 보내게 되어 제3자에게 발호 이동국의 위치가 노출되어, 추적이 가능하게 된다. 또한, 상대방의 전화번호를 이용하여 누가 누구와 통화를 시도하고 있는지의 내용도 알 수 있게 된다. 이는 인증센터가 발호 이동국에 해당하는 비밀 공유 테이터를 알기 위해서는 발호 이동국이 평문 형태로 자신의 정보를 보내지 않으면 안되기 때문에, CDMA 표준에서는 추적 불가능의 security 서비스가 제공되지 못하고 있다.

3.1.4 키 관리

인증 및 암호에 사용되는 키 SSD_A와 SSD_B는 인증 키 A_key에 의해 발생되며, 이 인증 키 A_key는 인증 센터에 의해 발생되어, 이동국과 인증 센터에 의해 각각 보관된다. 인증 센터에서 이동국으로의 키 분배는 이동국이 등록 신청을 행할 경우, 등기 우편에 의하여 전달한다. 키를 수령한 이동국은 키 패드(keypad)를 이용하여 직접 주입한다. 이 방식은 키 분배에 따른 비용 절감이 있으나, 키 패드에 의한 주입을 사용자가 직접 주입해야 하는 불변함이 있다. 또한 인증이 단말기 소유자가 아니라 단말기 그 자체이며, GSM 방식에 비해서는 유연성(flexibility)이 떨어지지만 스마트 카드에 따른 경제적 부담은 고려되지 않는다. 인증용 키인 SSD_A의 변경이 필요한 경우는 갱신 프로토콜에 의해서 이동국과 인증 센터간에 행하여진다.

3.2 GSM Security 서비스

3.2.1 인 증

GSM 표준에서의 인증은, 기본적으로는 CDMA 표준의 Challenge Response 인증 방식과 유사하나 가입자 Identity 정보와 인증용 알고리즘 및 키가 내장된 스마트 카드를 단말기에 주입하여 네트워크와의 인증을 행하는 것이 특징이다. 인증 프로토콜은 IMSI (International Mobile Subscriber Identity) 또는 TMSI (Temporary Mobile Subscriber Identifiers) 정보를 이용한 가입자 확인이 선행되어 이루어지는 것으로 먼저 가입자 A가 통화 요구를 네트워크측에 TMSI정보를 전송함으로써 네트워크측의 인증 센터(또는 기지국)가 가입자의 인증용 키를 데이터 베이스로 부터 수령하여 준비된 상태에서 시작하는 것으로 프로토콜은 다음과 같다.(그림 2 참조)

(step 1) 인증 센터는 A로 부터의 통화 요구가 있을 경우, 먼저 난수 RAND를 발생하여 A에게 보낸다.

(step 2) A는 수신한 RAND와 자신의 인증 키 K_A를 입력으로 인증 알고리즘 A3를 이용하여 출력 SRES를 계산한다. 계산된 SRES를 응답으로서 인증 센터에 전송한다.

(step 3) 인증 센터는 가입자 A의 인증 키 K_A와 자신이 발생한 난수를 입력으로 한 A3의 출력값과 수신한 SRES 값을 비교한다. 이 값이 일치할 경우 정당한 가입자로 판단한다.

단말기 사용자가 방문 네트워크에 위치하여 통화를 시도할 경우의 인증을 고려하면, 위 프로토콜에서 인증 센터는 방문 네트워크이 되어 홈 네트워크에 난수, 출력 응답 SRES 및 사용자 관련 정보를 요청하여 위와 같은 절차를 수행한다. 이러한 방식은 사용자의 비밀 정보가 홈 네트워크이외는 노출되지 않으므로

(그러나, K_C 정보는 별도 전달이 필요하므로 노출됨.) 안전성이 아주 좋으나 전체적인 트래픽이 증가하게 된다.

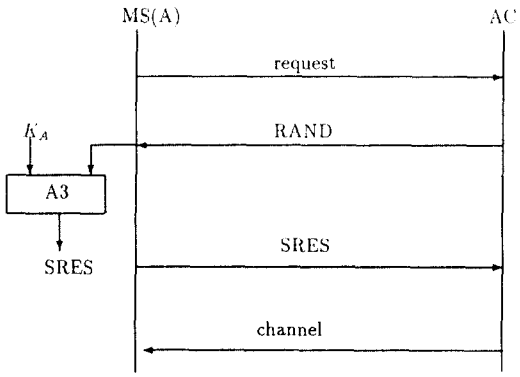

그림 2. GSM에서의 발호 인증

3.2.2 암 호

GSM 표준의 암호화 대상은 CDMA 표준의 경우와 동일하나 부가적으로 가입자 Identity 정보도 대상이 되고 있다. 암호를 수행하는 데 필요한 세션 키는 인증 절차 완료후에 생성하며 키 변경 및 암호화 수행은 네트워크측(기지국)에서 결정하여 수행한다. 기지국은 인증 절차에 사용된 난수 RAND와 인증용 키를 세션 키 발생기 A8에 입력하여 세션 키 K_C를 발생한다. 세션 키 K_C를 키 스트림 발생기 A5의 입력으로 하여 발생되는 키 스트림을 암호화 하고자 하는 음성 또는 신호정보와의 배타적 논리합(Exclusive-or)을 행하여 암호화한다. 이러한 절차는 이동국의 가입자도 동일하게 수행한다.

3.2.3 추적 불가능성

GSM 표준은 단말기의 신분을 보호하기 위하여 등록시 부여되는 IMSI 대신에 TMSI를 사용한다. 이 기능은 매번 호출시 마다 새로운 TMSI가 사용되며, 암호화 되어 각 단말기에 보내어지므로 어떤 단말기가 누구와 교신을 하고 있는지의 여부를 알 수 없게 한다.

3.2.4 키 관리

인증이나 암호에 사용되는 각 가입자의 인증 키들은 인증 센터가 발생하여 등록시에, SIM(Subscriber Identity Module) 이라는 스마트 카드를 통하여, 각 가입자에게 안전하게 분배하며 또한 관리 운영된다.

표 1. CDMA와 GSM 제공 security 서비스의 비교

구분		CDMA	GSM
표준		TIA/EIA(IS-95)	ETS
인증	인증 방식	Challenge Response 방식	Challenge Response 방식
	인증 알고리즘	CAVE(?)	A3
	보조 인증기능	유일 시도 응답 절차	없음
	제공 인증	단방향 인증	단방향 인증
암호	암호 대상	음성 및 Signalling 정보	음성, Signalling 정보, ID 정보
	암호 방식	비밀 키 암호	비밀 키 암호
	암호 알고리즘	비공개	A5, A8
추적 불가능성		미제공	제공(TMSI)
키 관리	키 발생	통신사업자인증센터(A_key)	통신사업자인증센터(K_i)
	키 분배	우편(A_key)	스마트카드(K_i)
	인증용 키	SSD_A	K_i
	암호용 키	SSD_B	K_C
Secure Database		필요	필요
시스템 부하(트래픽)		크다	크다

주1. A3(Algorithm 3, authentication algorithm used for authenticating the subscriber)
주2. A5(Algorithm 5, cipher algorithm ; used for enciphering/deciphering data)
주3. A8(Algorithm 8, cipher key generator ; used to generate K_c)

SIM내에는 인증 알고리즘 A3와 세션 키 발생 알고리즘 A8 그리고 가입자 관련 정보도 인증 센터에서 발생되어 함께 저장 되어진다.

가입자의 등록시에 인증 센터는 스마트 카드에 인증용 키를 주입하여 분배하며 인증 센터는 가입자 Identity 정보와 해당 인증 키를 데이타 베이스화하여 안전하게 관리한다. 이 방안은 카드 소지자가 카드 소지만으로 GSM용 단말기의 어떠한 종류, 예를 들면 공중 이동 단말기 또는 대여 단말기 등과도, 자유로히 이용할 수 있어 편리하다. 반면, 카드 사용에 따른 단말기 측의 제작 및 카드 제작 관리에 따른 별도의 부담이 추가되는 것이 단점이다.

3.3 CDMA와 GSM 제공 security 서비스의 비교

본 절에서는 디지털 이동 통신의 대표적 표준인 CDMA 방식과 GSM 방식의 security 서비스에 대한 비교를 표 1에 나타내었다. CDMA의 security 서비스 중 보조인증기능으로는 유일 시도 응답 절차가 인증 실패시나 망운용상의 필요에 의해 기지국(또는 인증 센터)에 의해서 행하여 지는 것외에 count 정보를 이용해서 불법 사용자를 찾을 수도 있다. GSM의 security 서비스중 단방향 인증이 제공되고 있으나, 또 다른 표준인 DECT[5]에서는 양방향 인증(Mutual Authentication)이 제공되고 있다.

Ⅳ. 공개 키 암호를 이용한 Security 서비스

본 장에서는 표준으로는 권고되지 않았지만, 이동 통신의 안전을 제공하기 위하여 연구 발표된 내용들을 검토한다. 기본적으로 비밀키 암호 방식을 사용한 표준안들에 비해 공개키 암호 방식을 사용하는 점이 크게 다르다. 비밀키 암호를 이용한 security 서비스는 인증이나 암호에 사용된 비밀키나 관련 비밀 정보가 수록된 데이터 베이스가 노출되게 되면, 시스템에 대한 영향이 치명적이 되고 만다. 다시말해서 데이터 베이스를 관리하는 인증 센터의 의존도가 심각하며 키 관리상의 문제 또한 어려운 방식이다. 더욱 곤란한 문제는 서로 다른 통신 사업자간에 동일한 사용자의 키를 어떻게 관리할 것인가 하는 것이다.

이를 근본적으로 해결하기 위한 수단중의 하나가 공개키 암호를 도입하는 방식이나 이는 기존의 표준 프로토콜을 변경하여야 하는 점외에도 이동국의 알고리즘 수행에 따른 S/W나 H/W의 증가로 인한 문제점도 제기된다. 이러한 관점에서 본 장에서는 공개키 암호를 이용하여 이동 통신의 인증 및 암호 기능을 제공하고 있는 대표적인 방식들인 TMN[16]방식과 BCY[17]방식을 표준안과 비교하여 검토한다.

4.1 TMN 방식 [16]

4.1.1 인 증

TMN의 인증 방식은 센터가 각 단말기 사용자의 신분 및 정당성을 확인하는 방식이다. 그러므로 시스템의 안전성이 센터에 의존하게 되므로, 센터는 네트워크의 신뢰할 만한 곳에서 담당하여야 한다. 기존의 이동 통신 인증 표준과 관련하여서는 인증 센터가 이에 해당될 수 있다. 본 방식은 단말기 사용자의 계산 능력을 고려하여 가장 단순한 계산 방식을 수행하도록 하였고, 센터는 계산 능력을 가진 곳으로 고려하여 좀더 복잡한 계산을 수행하도록 하므로써 단말기 사용자의 H/W 제약 문제를 해결하고 있다. 또한 단말기 사용자가 센터에게 단 1회의 전송만으로 인증을 행할 수 있으므로 적은 트래픽으로 그리고 기존 네트워크에 부하를 최소화할 수 있는 방식이다.

ID_a를 단말기 사용자 A의 Identity 정보 그리고 ID_b를 단말기 사용자 B의 Identity 정보라 하고 프로토콜 중에 사용되는 f를 센터의 비밀인 pseudo-random 함수로 한다.

준비 단계로 센터 C는 다음을 계산하여,

$S_a = f(ID_a)$와 $S_b = f(ID_b)$

S_a는 단말기 사용자 A에게 그리고 S_b는 단말기 사용자 B에게 각각 비밀로 안전하게 보낸다. 사용자의 인증을 행하기 위한 프로토콜은 다음과 같다.

(step 1) B와의 통화를 하고자 원하는 A는 먼저 랜덤수 r_1를 발생하여 $Z_a = E(S_a \| r_1)$를 계산한다. A는 Z_a와 ID_a를 센터 C에게 보낸다. 여기서 암호화 함수 E는 공개키가($e=3$, N)인 RSA 공개키 암호 방식[20]이며 ‖는 연접(concatenation)을 의미한다.

(step 2) 센터 C는 Z_a를 복호화 하여 복호화된 결과중의

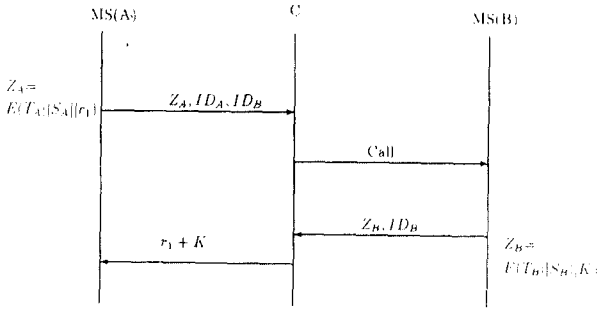

그림 3. TMN 방식의 인증 및 키 공유

S_a와 수신된 ID_a를 이용하여 계산된 $f(ID_a)$의 값을 비교한다. 만일 비교해 본 결과 서로 같을 때는 정당한 단말기 사용자로 간주하고 다음 서비스를 제공한다.

(step 3) B에 대해서도 동일하게 수행한다.

4.1.2 암 호

TMN의 암호 서비스는 암호화에 사용될 세션키를 인증 프로토콜의 수행시 동시에 수행되는 것으로 암호 알고리즘은 비밀키 암호를 사용한다. 즉, TMN의 방식은 인증과 세션키 공유가 동시에 수행되는 방식이다. TMN의 인증 방식에서 설명한 초기 인증 프로토콜은 무선 채널상에서 취득한 암호문을 재차 사용하여 공격하는 Simmons의 replay attack[21]이 가능하므로 TMN의 최종 프로토콜에서는, 이를 방지하기 위하여 센터와 단말기 사용자가 공유하는 timestamp 정보를 이용한다. 그러나 모든 단말기가 센터와 동일한 시각 정보를 공유하는 방안은 실제적으로 실현하기는 쉽지 않을 것으로 예상된다. 더우기, 최종 프로토콜에 대한 공격[18]도 존재하므로 안전성 측면에서는 취약한 방식이다. 그들이 제안한 효율적인 프로토콜은 다음과 같다.(그림 3 참조)

(step 1) B와의 안전한 통화를 하고자 원하는 단말기 사용자 A는 먼저 랜덤수 r_1를 발생하여 암호문 $Z_a = E(T_a \| S_a \| r_1)$를 계산한다. A는 Z_a와 ID_a 그리고 통신 상대방의 ID_b를 센터 C에게 보낸다. 여기서 T_a는 A의 timestamp 정보이다.

(step 2) 센터 C는 Z_a를 복호화 하여 인증을 행한다. 인증에서 정당한 단말기 사용자 A임이 확인되었을 경우 센터 C는 상대방 통화자 B를 호출한다.

(step 3) B는 A와 유사한 동작으로 암호문 $Z_b = E(T_b \| S_b \| K)$를 계산한다. 여기서 T_b는 B의 timestamp 정보이며 S_b는 B의 비밀 정보 그리고 K는 세션키로 사용될 B가 발생한 랜덤 수이다. B 또한 Z_b와 자신의 Identity 정보 ID_b를 센터에게 보낸다.

(step 4) 센터 C는 A와 동일하게 timestamp 정보의 확인과 인증을 행하여 복호화 된 결과중의 데이터를 이용하여 $u = r_1 + K$를 계산하여 A에게 보내어 준다.

(step 5) A는 센터로 부터 받은 u로 부터 $K = u - r_1$를 계산하여 B와의 비밀 통신용키로써 사용하여 안전한 통화를 행할 수가 있다.

4.1.3 추적 불가능성

공개키 암호를 이용한 암호문이 보내어지므로 기본적으로는 추적 불가능성을 만족하나, 중계 센터는 단말기 사용자의 정보를 이용하여 추적할 수 있다. 각 단말기 사용자가 통화 요구시 자신과 상대방의 Identity 정보를 평문 형태로 보내기 때문에 기존 방식만으로는 추적 불가능성을 만족하지 않으나, Identity 정보 마져 암호화하면 추적 불가능 서비스를 제공할 수 있다.

4.1.4 키 관리

인증 센터와 키 관리 센터를 겸한 센터가 센터 자신의 비밀키들, d와 pseudo-random 함수 f를 발생 안전하게 보관한다. 이동국의 등록이 행하여 질 경우 센터는 각 가입자의 Identity 정보를 이용하여 $S_i = f$ (*Identity* 정보)를 계산하여 안전하게 분배한다.

키 관리는 단일 센터를 활용하는 방안으로 모든 기지국이나 통신 사업자가 다를 경우에도 모두 동일한 비밀 키들을 사용해야 한다.

4.2 BCY 방식 [17]

4.2.1 인 증

BCY[17]의 인증 방식은 인증 센터 CA(Certification Authority)가 각 단말기 사용자나 네트워크의 RCE (Radio Control Equipment)에게 인증서(Certificate)를

발행하며, 각 단말기 사용자와 RCE는 CA로 부터 수령한 인증서를 이용하여 상호 신분 및 정당성을 확인하는 방식이다.

준비 단계로 인증 센터 CA는 단말기 사용자나 RCE들로 부터의 인증서 요청이 있는 경우, 그들의 신분을 확인한 후 단말기 사용자에게는 $A_i=(h(i, P_i))^{1/2} \bmod N_u$, $P_i=g^{S_i} \bmod N$와 비밀 키 S_i를, RCE에게는 $(A_j=h(j, N_j, P_j))^{1/2} \bmod N_u$, $P_j=g^{S_j} \bmod N$와 비밀 키 S_j를 안전하게 분배한다. 여기서, h는 one-way hash 함수이며 N과 N_u는 각각 두 소수의 합성수들이며 g는 mod N에 대한 원시근이다. 사용자 인증에 대한 프로토콜은 발신 사용자나 착호 사용자의 경우 동일하며 발신 사용자의 인증을 위한 프로토콜은 다음과 같다. (그림 4 참조)

(step 1) 발신자 i로 부터의 서비스 요청을 받은 네트워크측의 RCE_j는 인증 센터로 부터 수령한 A_j와 함께 공개 정보 j, N_j, P_j를 발신자 i에게 전송한다.

(step 2) i는 인증 센터의 공개키 N_u를 이용하여 $A_j^2 \bmod N_u$를 계산하여 다음 식이 만족하는 지를 확인한다.

$$A_j^2 = h(j, N_j, P_j) \bmod N_u$$

(step 3) RCE_j의 정당성이 확인이 된경우, i는 $C_1=x^2 \bmod N_j$, $C_2=f(x, m)$를 각각 계산한다. 여기서 x는 랜덤수이며 f는 비밀키 암호 방식(DES [12] 또는 FEAL[13] 등)을 나타내며 $m=i \| P_i \| A_i$을 의미한다. 계산된 C_1, C_2를 i는 RCE_j에게 전송한다.

(step 4) RCE_j는 $x=C_1^{1/2} \bmod N_j$와 $m=f^{-1}(x, C_2)$를 계산한다. 계산된 값으로 부터 $h(i, P_i)$와 $A_i^2 \bmod N_u$를 계산하여 비교 검토한다. 일치할 경우 정당한 사용자임을 확인할 수 있다.

4.2.2 암 호

암호 기능은 인증 기능이 선행된 후에 이루어지며, 암호 기능의 실현을 위해서는 세션키의 공유가 이루어져야 한다. 위의 프로토콜은 상호간의 인증은 이루어지나 발신자 i로 부터 받은 발신자의 인증서를 RCE_j가 남용할 수 있으므로 다음의 프로토콜은 키 공유도 수행하면서 인증서의 남용 문제도 해결할 수 있다. 공유된 세션키의 정확성을 확인하기 위하여 공개 된 표준 정보 M을 이용한다.(그림 4 참조)

(step 1) i는 $K=(P_j)^{S_i} \bmod N$를 계산한 후 세션 키 $S_K=f(K, x)$를 계산하여 $C_M=f(S_K, M)$와 함께 RCE_j에게 전송한다.

(step 2) RCE_j도 $K=(P_i)^{S_j} \bmod N$를 계산한 후 세션 키 $S_K=f(K, x)$를 계산하여 $C_M=f(S_K, M)$와 함께 i에게 전송한다.

(step 3) i와 RCE_j는 각각 수신한 C_M의 정당성을 확인한다.

4.2.3 추적 불가능성

세션키 설정 이후에 주요한 정보들이 교환되며, 공개키 암호화에 의해 특정 가입자의 추적은 곤란하다.

4.2.4 키 관리

통신 사업자의 인증 센터(또는 키 관리 센터)와는 별개의 신뢰할 만한 인증 센터가 존재하여 각 이동국이나 기지국에 인증 센터의 인증서(Certificate) 및 해당 비밀키를 안전하게 분배한다. 이동국이나 기지국은 수령한 인증서의 정당성 여부를 확인한 후 사용한다. 세션키의 공유는 Diffie-Hellman의 키 공유 프로토콜[15]에 의해 이루어진다.

4.3 TMN 방식과 BCY 방식의 비교

기존에 알려져 있는 공개키 암호를 이용한 디지털 이동통신용의 인증 및 키 공유 방식으로는 TMN 방식과 BCY 방식이 주로 알려져 있다. TMN 방식은 주

표 2. TMN 방식과 BCY 방식의 비교

구 분		TMN 방식	BCY 방식
인증	인증 방식	인증서 제공	인증서 제공
	인증용 알고리즘	RSA[20]	Rabin[22]+DH[15]
	제공 인증	단방향 인증	상호 인증
	인증 프로토콜	단순	복잡
암호	암호 알고리즘	비밀키 암호	비밀키 암호
추적 불가능성		미제공	제공
키 관리	키 발생 및 분배	인증 센터	키 관리 센터
	세션 키 공유	송수신자 공유	중계국과 송(수)신자 별개

로 단일 통신 사업자의 단일 센터에 의한 방식으로 이를 복수 센터로 구성할 경우는 다소 검토할 여지가 많은 방식이다. 한편, BCY 방식은 복수 통신 사업자와 복수 센터를 고려한 방식으로 안전성면에서는 TMN 방식보다는 다소 우수하나 효율면에서는 미흡하다. 이 절에서는 이들 두 방식, TMN 방식과 BCY 방식의 security 서비스에 대한 비교를 표 2에 나타내었다.

V. 제안 Security 서비스 제공 정책

5.1 기본 수립 원칙

디지털 이동 통신의 security 서비스로 인증, 암호 및 추적 불가능성이 기본적으로 고려되며, 단말기나 네트워크 전체에 대한 부하를 최소화하는 방안에서 마련되어져야 한다. 또한 앞으로의 기술 발전 추세를 고려하여 비밀키 암호 방식보다는 공개키 암호 방식을(비밀키 암호 이용 방식과 공개키 암호 이용 방식의 비교는 표 3 참조), 단말기 자체 인증 보다는 스마트 카드를 이용하여 단말기를 인증하는 방안으로 검토되어져야 한다. 그러나, 현 단계(CDMA나 TDMA)에서의 정책으로는 공개키 암호 사용에 따른 계산량과 트래픽의 증가를 고려하여, 비밀키 암호와 단말기 자체 인증을 행하는 것이 바람직 하며, PCS나 FPLMTS 단계에서는 공개키 암호와 고성능 스마트 카드를 이용하여 security 서비스를 제공하는 것이 좋을 것으로 생각된다.

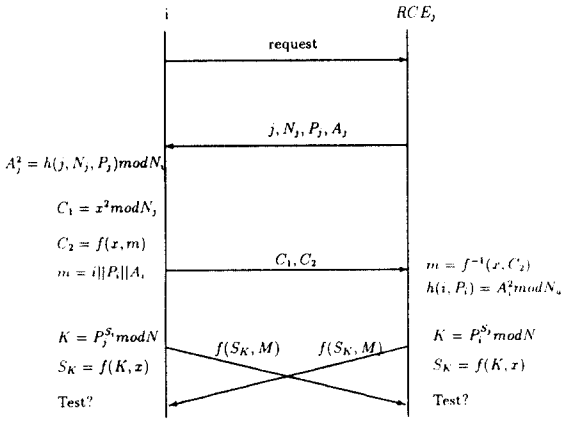

그림 4. BCY 방식의 인증 및 키 공유

표 3. 비밀키 암호와 공개키 암호를 이용한 방식 비교

구 분		비밀키 암호 이용 방식	공개키 암호 이용 방식
인증	인증 방식	Challenge Response 방식	인증서 제공
	인증용 알고리즘	해쉬 함수	공개키 암호
	제공 인증	단방향 인증	상호 인증
암호	암호 알고리즘	비밀키 암호	비밀키 암호
인증과 세션 키 공유		별도 수행	동시 수행
추적 불가능성		미제공	제공
키 관리		인증 센터	키 관리 센터
Secure Database		필요	불필요
계산 복잡도		적다	크다
트래픽		적다	크다

비밀키 암호 방식이 security 서비스 제공의 기본이 될 경우에는, 비밀키 암호를 이용한 CDMA나 GSM의 security 서비스에서 살펴본 바와 같이, 비밀키나 가입자의 해당 정보가 수록되어 있는 데이터 베이스의 안전한 관리가 커다란 문제점이 될 수 있다. 특히, 통신 사업자가 복수개 존재하는 상황에서는 이러한 데이터베이스의 관리는 심각한 문제가 된다. 각 통신 사업자가 모든 단말기 사용자의 비밀 정보가 저장된 공통의 데이터베이스들을 관리할 경우에는 문제 발생시의 책임 소재가 불분명하여 지며, 각 통신 사업자가 공통의 데이터베이스를 관리하지 않을 경우에는, 각 단말기 사용자가 각 통신 사업자가 관리하고 있는 자신의 해당 비밀 정보를 모두 보관하여야 하는 불편함이 있다. 또한, 각 통신 사업자가 security 서비스의 안전성에 대한 핵심 부분인 이러한 데이터베이스를 안전하게 그리고 신뢰성 있게 관리하는 것은 결코 쉬운 일이 아니며, 실제적으로, 인증 업무 수행시에 데이터베이스까지의 악세스로 인한 트래픽이 크게 증가하는 요인이 된다. 이러한 문제는 키 관리 부분에서 충분히 고려하여 대책을 마련하여야 한다.

다른 문제점으로는 추적 불가능성을 제공하기가 곤란한 점이다. 비밀 키 암호 사용시에는, 모든 단말기는 통화 시도시 네트워크에 자신의 정보(Identity 등) 및 통화를 하고자 하는 상대방의 호출번호등의 정보를 암호화하지 않은 채, 전송하고 있기 때문에 도청자 등에 의해서 쉽게 발신자의 위치등이 알려지기 때문이다. 비밀키 암호를 이용하여 추적 불가능성 서비스를 제공하고자 할 경우에는, 현재로써는, GSM

의 문제점을 개선한 방식[8]을 검토하는 것이 좋을 것 같다.

암호 기능을 제공하는 구간으로는 단말기와 중계기를 경유한 단말기간의 무선 구간과 단말기와 PSTN (Public Switch Telephone Network) 가입자 간의 유선 구간으로 구분할 수 있으나, 1차적으로는 무선 구간만을 대상으로 서비스를 제공하는 것으로 하고, 향후 필요시 유선 구간까지의 서비스도 고려하는 것으로 정책을 수립하는 것이 타당하다고 생각된다.

이러한 내용을 중심으로한 디지털 이동 통신을 위한 안전 대책 수립의 기본 원칙은 다음과 같다.

- 디지털 이동 통신의 security 서비스로 인증, 암호 및 추적 불가능을 고려한다.
- security 서비스를 제공하는 데 필요한 암호 방식으로는 TDMA나 CDMA 단계(1차 단계)에서는 비밀키 암호 방식을, PCS나 FPLMTS 단계(2차 단계)에서는 공개키 암호 방식을 사용한다.
- 1차 단계에서는 인증에 있어서 단말기 가입자의 정당성만을 인증하나, 2차 단계에서는 단말기와 시스템의 중계국 상호간의 인증도 수행한다.
- 인증 서비스는 1차 단계에서는 단말기 자체 인증이나 2차 단계에서는 고성능의 스마트 카드를 이용한 인증을 고려한다.
- 인증 서비스에 있어서 보조 인증 기능인 count 정보 활용 방안이나 유일 시도 응답 절차를 고려하여 보다 정확하고 질 높은 서비스를 제공하도록 한다.
- 암호 서비스는 반드시 인증 작업이 완료된 후에 제공하여야 한다.
- 암호 서비스의 제공 범위는 무선 구간만으로 하되, 향후 필요시 유선 구간까지도 제공할 수 있도록 한다.
- 발착호의 인증과 세션키 공유는 동시에 수행하도록 하며, 중계 센터와 발착신자 사이의 세션키는 동일하여야 하나 경우에 따라서는 중계 센터와 발신자, 중계 센터와 착신자 사이의 공유 세션키가 서로 다르게 할 수 도 있다.
- 암호용 비밀키는 별도로 관리할 필요없이 인증용 비밀키와 인증시 사용된 난수 그리고 기타 정보를 이용하여 매회 서로 다른 암호화 키가 사용되도록 한다.
- 1 단계에서 부터 추적 불가능 서비스를 제공하고자 할 경우에는 TMSI를 이용하는 GSM 방식을 개선 사용하는 것으로 한다.
- 각 통신 사업자의 인증 센터는 일반 가입자와의 결탁 등의 부정한 행위를 하지 않아야 하며 신뢰성을 높이기 위해 데이터베이스의 안전 관리를 철저히 하여야 한다.
- 1차 단계에서는 시스템의 제작 완료 후 security 서비스를 고려하나, 2차 단계에서는 시스템의 제작 초기시 부터 security 서비스를 고려하여야 한다.

제공할 서비스에 대한 기본적인 수립 원칙을 표 4에 요약하여 나타내었다.

5.2 서비스별 우선순위

위에서 살펴본 바와 같이, 디지털 이동 통신의 security 서비스로 고려한 사항은 인증, 암호 및 추적 불가능이었다. 이들 서비스들은 사용 환경이나 시기 등에 의해서 서비스 제공의 완급을 정의할 수 있다. 본 절에서는 서비스별 우선 순위에 대한 방안을 제안하고자 한다. 앞절에서 설명한 1단계/2단계별 서비스 제공 방안과는 달리 여기서는 제공 서비스의 우선 순위만을 고려한다.

먼저, 인증은 가장 기본적인 security 서비스로 최우선적으로 제공되어야 한다. 단말기의 불법 사용에 따른 과금상의 혼란으로 통신 사업자의 경영에 심각한

표 4. 단계별 제공 security 서비스

구분	1 단 계	2 단 계
범위	CDMA/TDMA	PCS/FPLMTS
인증	-비밀키 암호 -단방향 인증 -Challenge Response -보조인증기능	-공개키 암호 -양방향 인증
암호	-인증 완료후 제공 -무선구간 -인증과 동시 세션 키 공유	-인증완료 후 제공 -유선구간 -인증과 동시 세션 키 공유
추적 불가능		-제공(제3자 범행) -option(내부 범행)
키 관리	-키패드에 의한 비밀 키 주입 -데이터 베이스관리 -인증 및 키 관리센터	-스마트 카드 -인증 및 키관리 센터 분리

장애를 줄 수 있는 문제를 사전에 막을 수 있다는 측면에서 서비스라기 보다는 통신 사업자가 절대적으로 필요로하는 시스템의 기본 기능으로 간주되기 때문이다. 즉, 다시말해서 시스템의 개발 단계에서 부터 인증 서비스를 고려하여 제작하여야 한다는 의미이다. 또한 부당한 사용료 징수에 대한 정당한 사용자의 불편을 해소하여, 사용자에 대한 통신 사업자의 신뢰성을 확보하는 차원에서도 인증이 필요하기 때문이다.

다음으로 제공하여야 할 서비스는 암호로 이는 인증 기능이 제공된다는 전제하의 서비스이다. 기본적으로는 제공하도록 하여야 하나, 필요에 따라서는 조건부 형태(서비스 제공료는 가입자 부담)로, 서비스를 받기를 원하는 가입자에 한해서 제공할 수 있다. 암호 기능의 제공은 사전에 단말기에 암호 모듈을 장착 준비하는 것으로, 세션키는 인증키와 난수 정보를 이용하여 매번 사용되는 키가 달라지도록 하여야 한다.

추적 불가능 서비스는 1단계에서는 제공 곤란하나 2단계에서는 공개키 암호의 사용으로 기본적인 서비스는 제공할 수가 있다. 이 또한 조건부 서비스로 가능하며 제3자에 의한 불법 추적에 대해서는 GSM의 방식을 사용하거나 공개키 암호를 사용함으로써 쉽게 해결할 수 있으므로, 중계국 등의 내부인에 의한 불법 추적에 대한 대책보다는 먼저 제공할 수가 있다. 내부인의 불법 추적에 대한 대책 까지도 고려하여야 하는 경우는 아주 특수한 고급 서비스로써 현 단계에서는 이론적인 방안들만 제안되어 있는 실정이므로, 고려하지 않아도 무방하리라 예상된다. 가장 우선 순위가 낮은 서비스이지만, 서비스가 제공되지 않아 생기는 문제는 통신 사업자에 대한 신뢰성 저하는 물론이고 사회적인 문제로 대두되리라 예상된다.

이동 통신 사업자가 security 서비스를 제공하는 데 있어서의 우선순위는 다음과 같다.

(1) 인증 서비스
- 단방향 인증(Unilateral Authentication)
- 양방향 인증(Mutual Authentication)

(2) 암호 서비스

(3) 추적 불가능 서비스

5.3 Security 서비스

5.3.1 인 증

[비밀키 암호를 이용한 인증 서비스]

1 단계에서는 인증 프로토콜은 Challenge Response 방식으로 수행하며 인증 알고리즘은 국내 표준으로 제작하도록 한다. 이는 외국의 인증 알고리즘이 비공개이며 특허 문제가 거론될 소지가 있으므로 국내 제작이 필요하다. 국내 표준 인증 알고리즘이 가져야 할 최소한의 암호학적 요구 사항으로는 일방향(onewayness) 성질을 만족하여야 하며, 입력의 모든 비트가 출력 생성에 영향을 주어야 하며, 또한 알려져 있는 해쉬함수나 블럭 암호에 대한 공격에 취약하지 않도록 하여야 한다. 인증 프로토콜의 보조 인증 기능은 CDMA 표준의 기능을 참고로 하되 우리나라 실정에 맞게 수정하여 사용하도록 한다.

[공개키 암호를 이용한 인증 서비스]

2단계에서 필요한 인증 서비스는 다수의 통신 사업자가 존재할 경우를 고려하고 모든 가입자의 비밀 정보를 보관하는 데이터 베이스와의 트래픽을 줄이거나 전반적인 인증 관련 프로토콜이 시스템에 미치는 부하를 줄이기 위해서 공개키 암호 방식과 스마트 카드 활용 방식을 고려한다. 이러한 방식은 단말기나 중계 센터의 H/W 부담을 가중하거나 인증을 위해 주고 받는 정보량의 증가로 인하여 시스템에 부담을 주게된다. H/W 부담에 관해서는 소형화를 해야하는 단말기의 경우가 특히 문제가 되므로 Rabin 공개키 암호[22]나 $e \equiv 3 \bmod 6$인 RSA 공개키 암호[20]를 사용하여 단말기의 계산량을 최소화하여 단말기의 부담을 최소화한다. 안전성면에서는 Rabin 공개키 암호는 소인수 분해의 어려움에 의존하고 있으며[22], $e \equiv 3 \bmod 6$인 변형된 RSA 공개키 암호에 대해서도 소인수 분해의 어려움에 의존하고 있음이 증명되어 있으므로[27] 안전하게 사용할 수 가 있다. 그러나 중계 센터나 인증 센터의 경우는 어느 정도(Workstation 급)의 계산 능력을 갖고 있다고 가정할 수 있으므로, 다소 계산량이 많은 경우라도 문제가 되지 않으리라 생각된다. 또한, 반도체 제조 기술과 컴퓨터의 계산 능력의 추이를 감안할 경우, 이러한 부담은 점차 개선되리라 생각된다. 각 통신 사업자의 기지국용 공개키에 대한 인증서는 키 관리 센터를 통해서 발급 받

을 수 있으며 또는 독자적으로 각 사업자에 의해 발생하여 사용할 수도 있다. pseudo-random 함수인 f는 키 관리 센터에 의하여 발생되며, 모든 기지국이 공통으로 사용한다. 함수 f는 각 가입자의 비밀 정보, S_i $(=f(ID_i))$를 발생하는 것으로 필요시는 직접 각 통신 사업자의 인증 센터가 발생하여 각 가입자의 스마트 카드에 주입하도록 한다. 인증 프로토콜은 TMN 방식을 보완하여 활용할 수도 있다.

5.3.2 암 호

인증단계에서 세션키의 공유를 동시에 행하기 때문에 암호는 크게 문제가 되지 않는다. 그러나 사용될 알고리즘은 통신 사업자간에 공통으로 사용될 수 있는 표준 알고리즘을 채택하는 것이 바람직하며, 암호화의 처리 속도를 고려하여 암호 알고리즘은 비밀키 암호 방식을 사용하도록 한다. 표준 알고리즘은 보호하고자 하는 내용의 중요도에 따라 선정되어야 하며 기존에 알려져 있는 입·출력 변화 공격법(Differential Cryptanalysis)[28]과 선형 근사 공격법(Linear Cryptanalysis)[29] 등을 최소한 고려하여야 하며, S/W 구현에도 용이한 형태의 알고리즘이 되어야 한다. 암호 알고리즘은 단말기나 중계국 등의 장치에 제작 단계에서 제작업체 등에 의해 미리 장착되어 제공되도록 할 필요가 있다. 이렇게 함으로써, 서로 다른 통신 사업자간의 사용자 사이에도 아무런 문제없이 암호 통신을 행할 수가 있다. 또한 유선 구간으로의 암호 구간의 확대가 필요할 경우에도 쉽게 대처할 수 있다.

5.3.3 추적 불가능성

인증 프로토콜에서 본바와 같이 가입자 관련 모든 정보는 암호화 되어 전송되므로 제3자에 의한 불법 추적을 손쉽게 막을 수가 있다.

5.3.4 키 관리 시스템

본 논문에서 고려하고 있는 센터들의 분류는 다음과 같다.

- 인증 센터 : 통신 사업자가 제공하는 시스템내의 모든 가입자의 인증 및 비밀 정보를 관리하는 센터로 대부분 단 한개의 센터로 구성된다. 필요시 복수개로 구성할 수도 있다.
- 키 관리 센터 : 여러 통신 사업자가 공존할 경우 가입자와 통신 사업자간의 상호 인증을 위한 인증서 발행이나 모든 키 관리를 수행하는 곳으로 모든 가입자나 통신 사업자가 신뢰할 수 있는 기관이어야 한다.

키 관리 시스템에서 고려하여야 할 가장 기본적인 사항은 키의 생성, 분배, 주입 및 파기에 대한 것으로 다음과 같다.

- 1개의 키 관리 센터와 복수개의 인증 센터로 구성함을 기본으로 한다. 키 관리 센터는 인증서 발행, 시스템 관련 비밀 정보 발행 및 관리 등을 담당하며 각 인증 센터는 인증 및 암호 기능을 수행한다. 각 통신 사업자는 1개의 인증 센터를 설치 운영하며 키 관리 센터는 각 통신 사업자로부터 신뢰될 수 있어야 한다. 키 관리 센터의 설치는 다소 검토의 여지가 있으나 2단계에서는 키 관리 센터를 설치하는 것으로 한다. 그러나 이러한 키 관리 센터의 설치가 곤란한 경우, 서로 다른 통신 사업자간의 상호 승인에 의해서 인증 및 암호 기능을 행할 수 있으나 많은 양의 트래픽 증가가 예상되어 비효율적이다. 특히 비밀키 암호에 의한 경우는 비밀키 정보가 수록된 데이타 베이스의 공유 또는 사용자가 모든 통신 사업자와의 공유 비밀 정보를 보관하여야 한다.
- 키 생성은 기본적으로 인증 센터(또는 키 관리 센터)가 수행하도록 하여야 하며, 인증 센터는 security 서비스의 안전성 측면에서 가장 핵심적인 부분이므로 물리적 안전성이 확보되어야 한다.
- 키 분배 및 주입은 1단계에서는 인증 센터와 가입자(또는 영업 전화국)간의 데이터 통신 네트워크(예를들면 PSDN)를 통하여 전달된 키 정보를 키 패드에 의해 자동 주입되도록 하며, 2단계에서는, 키 관리 센터가 각 통신 사업자에게 분배하는 것으로 하고 각 통신 사업자가 해당 단말기 사용자에게 스마트 카드를 이용하여 키를 분배하는 것으로 한다. 이때 키 관리 센터와 각 통신 사업자간의 네트워크 구축에 의하여 키 분배가 이루어지며 최종 스마트 카드의 발급은 각 통신

사업자의 인증 센터가 수행한다.

- 키 교체 및 파기는 필요시 통신 사업자의 인증 센터가 주로 수행하도록 한다.

Ⅵ. 결 론

본 논문에서는 비밀키 암호 방식을 이용하여 security 서비스를 제공하는 CDMA나 GSM 관련 표준들과 공개키 암호를 이용하여 security 서비스를 제공하는 방식들을 비교 분석하였다. 그리고 우리나라의 디지털 이동 통신에서 제공하여야 할 security 서비스를 1단계(CDMA/TDMA)와 2단계(PCS/FPLMTS)로 구분하여 제안하였다. 이러한 security 서비스를 제공하기 위한 기본 정책의 수립을 위해 서비스 제공의 우선 순위, 기본 원칙 그리고 키 관리 방안을 중심으로 한 정책 방향을 제시하였다. 제안된 내용들은 디지털 이동 통신의 security 서비스 정책에 관한 기본적인 내용에 불과하며, 필요시는 안전성이나 실용성 측면에서의 많은 연구가 더욱 더 이루어져야한다. 마지막으로 본 논문이 이동 통신 사업자의 security 정책 수립 및 국내의 이동 통신 security 정책 수립의 기초 자료로써 활용되기를 기대한다.

참 고 문 헌

1. Cellular One's Fraud Protection for New Customers. NewsBytes News Service, Jan. 31. 1995.
2. 동아일보, 뉴욕 도둑전화 비상, Jul. 25, 1995.
3. TIA/EIA Telecommunications Systems Bulletin, Cellular Radiotelecommunications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy, TSB51, May, 1993.
4. European Telecommunications Standards Institute (ETSI), "European Digital Cellular Telecommunications System(phase1); GSM 3.20, Security Related Network Functions", Version 3.3.2, Jan. 1991.
5. ETSI-RES, European Telecommunication Standard, Final Draft, ETS 300 175-7, DECT, Common interface, part 7: Security features, May, 1992.
6. K.Vedder, "Security Aspects of Mobile Communications", Spring-Verlag, Computer Security and Industrial Cryptography, ESAT Course, pp.193-210, 1991.
7. M.Walker, "Security in Mobile and Cordless Telecommunications", CompEuro'92, U.S.A., pp. 493-496, 1992.
8. J.C.Cooke and R.L.Brewster, "Cryptographic Security Techniques for Digital Mobile Telephones", Int'. conf. on selected Topics in Wireless Com., pp. 425-428, 1992.
9. D.Brown, "Security Planning for Personal Communication", 1st ACM conf. Computer and Communication Security, pp.107-111, 1993.
10. R.Akiyama and S.Sasaki, "Authentication and Encryption in a Mobile Communication System", Proc. 43rd. IEEE VT conf., pp.927-930, 1993.
11. 오현서, 이홍섭, 이대기, "GSM시스템의 Security 특성에 관한 고찰", 한국통신정보보호학회지, 제3권, 제4호, pp.57-61, Dec., 1993.
12. FIPS Pub. 46-1, U.S. Department of Commerce, Data Encryption Standard, Federal Information Processing Standards Publications 46-1, 1988.
13. A.Shimizu and S.Miyaguchi, "Fast Data Encipherment Algorithm FEAL", Advances in Cryptology, Proceedings of Eurocrypt'87, pp.267-278, 1987.
14. 한국통신기술협회, TTA Interim Standard; 800MHz 대 디지털 이동 전화 무선 인터페이스, 제1판, 1994.
15. W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, Vol.22, pp.644-654, 1976.
16. M.Tatebayashi, N.Matsuzaki and D.B.Newman, "Key Distribution Protocol for Digital Mobile Communication Systems", Advances in Cryptology, Proceedings of Crypto'89, pp.324-334, 1989.
17. M.J.Beller, L.Chang, and Y.Yacobi, "Privacy and Authentication on a Portable Communications System", IEEE Global Telecommunications Conference, pp.1922-1927, Dec., 1988.
18. C.S. Park, K.Kaoru, T.Okamoto and S.Tsujii, "On Key Distribution and Authentication in Mobile Radio Networks", Advances in Cryptology,

Proceedings of Eurocrypt'93, pp.461-465, 1993.

19. T.Hwang, "Scheme for Secure Digital Mobile Communications based on Symmetric Key Cryptography", Information Processing Letters, 48, pp. 35-37, 1993.
20. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the Association for Computing Machinery, Vol. 21, No.2, pp.120-126, 1978.
21. G.J. Simmons, "Proof of Soundness(Integrity) of Cryptographics Protocols", Journal of Cryptology, Vol.7, No.2, pp.69-77, 1994.
22. M.O.Rabin, "Digitalized Signatures and Public Key Functions as Intractable as Factorization", MIT Lab. for Computer Science, TR.212, Jan. 1979.
23. D. Chaum, "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84-88, Feb., 1981.
24. C.S. Park, K. Itoh and K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology, Eurocrypt'93, pp.248-259, May, 1993.
25. D.A. Cooper and K.P. Birman, "Preserving Privacy in a Network of Mobile Computers", Proceedings of IEEE Symposium on Security and Privacy, pp.26-38. 1995.
26. S.Houmura, R.Sakai and M.Kasahara, "Schemes of Anonymous Channel on Communication Networks", Technical Report of IEICE, IT93-64, pp. 7-11. 1993.
27. J.H.Loxton, D.S.P. Khoo, G.J.Bird and J.Seberry, "A Cubic RSA Code Equivalent to Factorization", Journal of CRYPTOLOGY, Vol.5, No.2, pp.139-150, 1992.
28. E.Biham and A.Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology, Proceedings of Crypto'90, pp.2-21, 1990.
29. M.Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology, Proceedings of Eurocrypt'93, pp.386-397, 1993.

박 춘 식(Choon Sik Park) 정회원
광운대학교 전자통신공학과 졸업 (학사)
한양대학교 대학원 전자통신공학과 졸업 (석사)
일본 동경공업대학 전기전자공학과 졸업 (암호학 전공, 공학박사)
1989년 10월~1990년 9월:일본 동경공업대학 객원연구원
1982년~현재:한국전자통신연구소 책임연구원
※주관심분야:암호이론 및 응용, 정보이론, 통신이론