논문 98-23-12-17 한국통신학회논문지 '98-12 Vol. 23 No.12

IMT-2000에서 안전한 전송을 위한 ID 정보기반 인증 메카니즘의 설계

정회원 이 태 훈*, 정 일 용**, 김 용 득***

A Design of IMT-2000 Authentication Mechanism based on Identification Information for Secure Communications

Taehoon Lee*, Ilyong Chung**, Yongdeak Kim*** *Regular Members*

요 약

본 논문은 IMT-2000에서 제 3자로부터 불법 사용을 방지하기 위한 인증 메카니즘을 제시한다. 기존 방식에서는 인증에 필요한 비밀 데이터를 평문으로 전송하는 것에 비해 제안된 방식은 암호화하여 전송함으로서 기밀성을 유지하면서 기존 프로토콜과 비교하여 최소의 정보흐름을 유지한다. 또한 이동단말 간에 데이터를 전송하는 데에 필요한 비밀키를 생성하고 상호 공유하는 프로토콜을 제안한다. 제안한 방식은 각 단말의 홈 인증센터 사이에 단말의 ID를 기반으로 인증센터간 상호 신분을 확인하면서 단말의 암호화 통신용 비밀 키를 공유하는 키 분배 프로토콜로써 단말이 가지고 있는 비밀키를 이용하여 중간단계의 침입을 방지할 수 있고 키 공유에 소요되는 정보의 흐름을 최소화하였으며 복잡한 계산을 인증센터에서 수행하도록 함으로서 단말에서의 계산부하를 줄일 수 있도록 하였다.

ABSTRACT

In this paper, we present IMT-2000 Authentication mechanism for accomplishing information security and protecting illegitimate access from an adversary. According to methods previously proposed, security data requisite for authentication is transmitted on plaintext form. However, the presented method ensures data confidentiality by sending data encrypted with a secret key, and additionally decreases the information flow for secure communications. It also provides the protocol that two mobile terminals keep the same secret key in order to transmit data encrypted with this key. The method authenticates communication entities mutually based on identification information on an authentication center in HLR a terminal belongs to. At the same time it interrupts an interim attack by applying the secret key a mobile terminal utilizes. In terms of efficiency, it minimizes the information flow for distributing keys and decreases the computational time for a terminal by performing the complex computation on an authentication center.

* 광주대학교 컴퓨터학과, ** 조선대학교 전자계산학과, *** 아주대학교 전자공학과
논문번호 : 98423-0923, 접수일자 : 1998년 9월 23일

I. 서 론

정보통신 서비스의 목표는 언제, 어디서나, 누구와도, 그리고 어떠한 서비스 유형이든지 서비스가 가능하도록 하는 것이다. 이를 위해서 통신망에서는 사용자 단말기가 가입되어 있는 통신망과 무관하게 원하는 상대 단말에 연결하는 기능과 단말기에서 발생하는 데이터를 전송할 수 있는 전송능력을 제공하여야 한다. 현재 유선망은 기존의 일반전화망에서 영상정보를 포함하는 멀티미디어 서비스 제공이 가능한 초고속 정보통신망으로 발전하고 있으며, 전송방식의 디지틀화, 고속화, 서비스 종합화를 추구하고 있다. 또한 현재 세계적으로 급속하게 보급되고 있는 이동통신 서비스를 위한 무선통신망도 음성서비스 위주의 아날로그방식에서 디지틀방식으로, 그리고 개인휴대통신(PCS)을 거쳐 고속데이터, 영상 등의 멀티미디어 서비스까지 지원할 수 있는 IMT-2000망으로 진화하고 있다[12].

무선 이동통신망은 타 지역에서도 통신 서비스에 접근할 수 있는 단말의 능력과 해당 단말을 식별하고 위치를 인식하는 망의 능력을 가지고 있기 때문에 단말의 이동성을 보장할 뿐 아니라 사용자 식별정보를 통하여 임의의 이동단말을 자신의 이동단말로 인식시킴으로서 사용자가 어떠한 이동단말을 사용하더라도 자신의 서비스 프로파일에 따라 통신서비스에 접근하는 사용자의 이동성을 제공하려 한다. 그러나 무선망은 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제 3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 등의 문제가 있다. 따라서 무선통신의 안전성을 유지하기 위해서는 가입자에 대한 신분확인, 통화 및 메시지 내용의 암호화 그리고 가입자에 대한 추적 불가능성 등의 보안기능이 요구된다. IMT-2000에서는 이동단말의 발호나 착호시, 위치등록이나 위치갱신시에 방문망의 전송로를 경유하여 단말기가 등록된 홈 망의 인증센터에서 인증과정을 수행하여 통보한다. 이를 위해 단말과 사용자, 그리고 인증센터는 인증에 필요한 비밀 데이터를 보유, 관리하고 있다. 그러나 현재 제시되어 있는 인증과정은 단말과 인증센터 간에 비밀 데이터를 평문으로 전송하기 때문에 외부에 노출되기 쉽다.

IMT-2000의 보안원칙에 관련하여 ITU-R M1078(IMT-2000, 1994)[8]에서는 서비스 관련, 접근제어 관련, 이동단말 관련, 사용자 관련, 네트워크 운용 관련, 그리고 보안관리 관련 등에 대해 최소한의 기본 요구사항을 제시하고 있는 데, 무선통신시스템의 보안위협에 대적할 수 있는 구체적인 방안이나 조치는 제시되지 않고 있다. 또한 무선망을 통한 비밀 데이터의 전송과 전자상거래 서비스 제공을 위해 필요한 암호화 통신 및 프로토콜에 관한 연구가 절실한 상태이다.

본 논문에서는 IMT-2000에서 단말 및 사용자 인증시 단말과 홈 망의 인증센터 간에 교환되는 데이터를 암호화함으로서 전송로에서의 정보를 보호하고, 인증센터로부터 인증을 마친 두 이동단말이 암호화 통신을 하기 위해 키를 공유하는 효율적인 비밀키 분배 프로토콜을 제안한다.

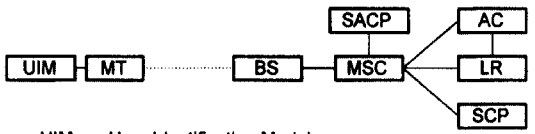
본 논문의 II장에서는 IMT-2000에서 제시하고 있는 인증 및 보안체계에 대해 기술하고, III장에서는 암호화 통신을 이용한 인증방식과 두 단말 간 암호화 통신을 위한 키 분배 프로토콜에 대해 제안한다. IV장에서는 제안한 방식에 대해 분석과 평가를 하며 V장에서 결론을 맺는다.

II. IMT-2000의 인증 및 보안체계

IMT-2000의 보안요구사항은 ITU-R M1078에 제시하고 있는데, 이동 단말기의 도난, 단말기 복제, 가장 등의 위협으로부터 사용자를 보호하는 기능과 사용자 신분과 위치, 그리고 사용자 통신의 도청 등 비밀성, 기밀성, 익명성 등에 대한 위협으로부터 사용자를 보호하는 기본적인 사항을 포함하고 있으며, IMT-2000의 사용자와 서비스 제공자, 그리고 망 운용자 각각이 고정망에서 제공하는 수준의 보안기능을 제공할 수 있도록 목표로 하고 있다.

IMT-2000 망은 그림 1과 같이 UIM, MT, BS, MSC, LR, AC, SCP 등 여러 개의 기능개체들로 분

산되어 구성된다[1]. 그림에서 사용자는 UIM(User identification Module)으로 표현되고, UIM의 기능에 의해 사용자 이동성이 보장된다. 인증센터(AC:Authentication Center)는 홈 망에 등록한 모든 사용자와 단말기들의 인증관련 정보와 인증 알고리즘을 저장하며, 다른 기능개체의 요구에 의해 인증 알고리즘을 수행한 후 결과를 통보해 주는 기능을 수행한다. 가입자 데이터와 서비스 프로필 데이터 등 인증관련 정보는 처음 등록시 홈 망의 인증센터에 저장되고 등록 해지시 삭제된다. BS는 이동단말의 망에 대한 접근을 제공하며 이동단말과 망 간의 연결 및 이에 관련되는 무선자원 할당, 핸드오버 제어 등의 전반적인 제어를 수행한다. MSC(Mobile Switching Center)는 이동교환기이며 SCP(Service Control Point)는 지능망 서비스 관련기능을 수행하며, 호 처리와 다른 흐름을 갖는 특수 호를 제어한다. 또한 서비스 로직을 관리하며, 서비스 요구에 대하여 해당 서비스 로직을 구동한다. LR(Location Register)은 단말기의 위치정보를 관리하며 VLR(Visiting LR)과 HLR(Home LR)로 구분하여 많은 수의 단말위치를 계층적으로 분산하여 관리한다.



UIM : User Identification Module
MT : Mobile Termination
BS : Base Station
MSC : Mobile Switching Center
SACP : Service Access Control Point
AC : Authentication Center
LR : Location Register
SCP : Service Control Point

그림 1. IMT-2000 망 모델

인증은 UIM과 홈 망의 인증센터 간에 이루어지며 따라서 방문망에서 인증을 수행할 경우에는 SCP를 통해 홈 망의 인증센터까지 연결이 필요하다. 즉, 그림 1에서 MT, BS, MSC, SCP 등은 인증시에는 단순한 정보전달 경로로 생각할 수 있다.

사용자 이동성에 관련된 정보와 알고리즘을 관리하고 인증 파라메터를 생성하여 관리하며 이를 사용하여 인증 알고리즘의 수행하는 UIM은 스마트카드 형태를 가진다. 인증을 위해 UIM의 내부기능인 UIMF(User Identification Management Function)는 프로그램과 단말기 제조시 부여되며 각 이동단말에 대해 유일한 값을 갖는 ESN(Electronic Serial Number), 인증 알고리즘에 관련된 파라메터, 등록시 서비스 제공자가 결정하여 망과 이동단말에 저장하는 비밀 데이터(Secret Data, A-Key), 방문국에서 이동단말에 잠정적으로 부여하는 임시 신분번호인 TMUI(Temporary Mobile User Identity), 단말기 등록시 부여되는 사용자 정보인 IMUI(International Mobile User Identity), 카드의 소유자를 확인하기 위한 PIN(Personal Identity Number), 이동단말이 위치하고 있는 지역의 네트워크 식별번호인 LAI(Location Area Identity) 등의 정보를 보유한다.

단말과 홈 망의 인증센터는 보유하고 있는 인증관련 정보로부터 상호 동일한 인증 키와 암호화 키를 갖기 위해서 그림 2와 같이 망에서 제공하는 56비트의 난수 값인 RANDSSD와 함께 공유 비밀데이터(SSD: Shared Secret Data) 생성과정을 통해 각각 64비트의 SSD_A와 SSD_B를 생성한다. SSD는 하나의 임시 키라고 할 수 있는 데, 현재 사용 중인 비밀 데이터가 망 측에서 보안도가 떨어진다고 판단되면 새로운 RANDSSD를 단말에 제공하여 값을 변경한다.

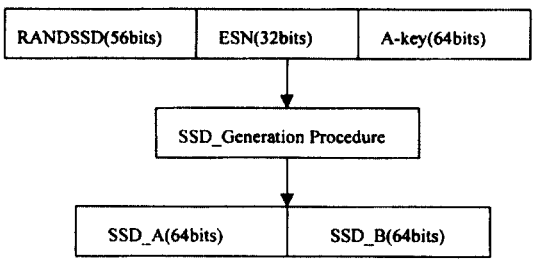


그림 2. SSD 생성과정

SSD_A는 그림 3의 a)와 같이 CDMA 인증서명절차에 사용되는 알고리즘의 입력, 즉, 인증 키로 사용하는 비밀 키이고, SSD_B는 그림 3의 b)와 같이 CDMA 음성 프라이버시와 신호 메시지의 기밀성을 위한 암호화 키를 계산하는 데에 사용되는 비밀키이다. 단말과 망은 똑 같은 비밀 데이터 값과 비밀키 생성 알고리즘을 가지고 있으므로 동일한 난수 값의 입력에 의해 각각 동일한 임시 비밀 키를 보유할 수 있게 된다.

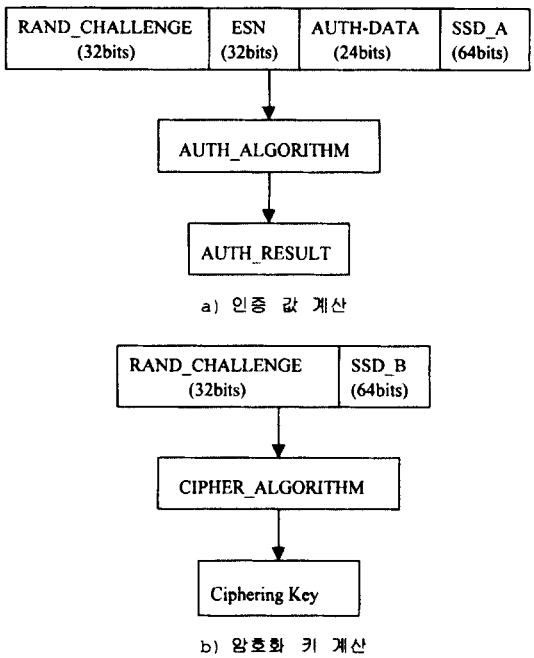


그림 3. SSD를 사용한 인증 및 비밀키 계산

IMT-2000에서 인증절차는 이동단말 등록시, 이동단말의 발호와 착호시, 그리고 이동단말 등록 인증절차나 이동단말 발호 인증절차가 실패할 때 수행되는 유일시도/응답절차(Unique Challenge/Response Mechanism) 수행시, 이동단말의 유일시도/응답인증절차가 실패한 경우 수행되는 비밀 공유 데이터 갱신절차시 등에 수행한다.

인증과정은 이동망에서 먼저 이동단말에 난수 값을 제시하고, 이동단말에서는 수신된 난수를 입력으로 인증알고리즘을 수행한 결과 값을 이동망에 제출하여 이동망에서 자신이 계산한 값과 비교함으로서 수행된다. 인증은 망의 상황에 따라 그림 4와 같은 유일시도/응답과 전체시도(Global Challenge Mechanism)방식이 선택적으로 사용될 수 있다[5].

유일시도/응답방식은 그림 4의 a)와 같이 망측에서 난수 값을 특정 단말에 제시하고, 이를 SSD_A와 함께 입력 파라메터로 하여 인증 알고리즘에 의해 계산한 결과 값과 홈망의 인증센터에서 계산한 값과의 일치여부를 비교함으로서 인증을 수행한다.

전체시도 방식은 그림 4의 b)와 같이 방문망 측에서 난수 값이 포함한 전체시도 메시지를 제어채널을 통해 방송형태로 단말에 보내고, 등록절차나 발호 등을 하고자 하는 단말은 ESN, SSD_A 및 망측에서 제시한 난수 값 등을 입력으로 인증 알고리즘을 수행한다. 결과 값은 인증계산에 사용되었던 파라메터와 함께 홈 망의 인증센터에 전해진다.

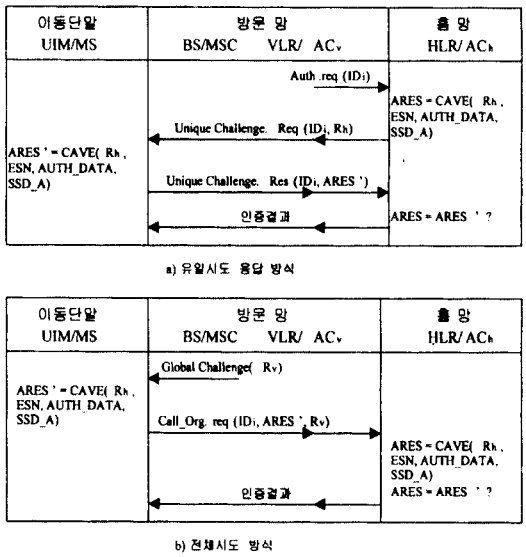


그림 4. IMT-2000 사용자 인증방식

인증센터에서는 수신된 파라메터와 보유하고있는 SSD_A 등을 가지고 단말에서와 동일한 인증 알

고리즘을 수행하여 단말에서 전송한 인증 값과 일치여부를 검사함으로서 인증과정이 수행된다.

III. 인증 및 암호화 통신 프로토콜 제안

모든 표준안이나 권고는 상호 호환성에 목적을 두고 있으므로 주로 접속형태와 절차에 대하여 규정하고 있다. IMT-2000의 서비스 관련 보안요구사항과 접근관련 보안요구사항에 관한 표준안도 마찬가지이며, 호환성에 관련하지 않은 부분은 그 구현방법을 규정하지 않는다. 즉, 현재 규정된 표준안에는 사용자와 서비스 제공자 혹은 네트워크 운용자 사이의 보안기능 및 행위만을 언급하고 있으며, 구체적인 방법과 절차는 규정하지 않고 있다. 그런데 인증을 위한 보안관련 키의 생성 및 관리, 보관, 분배, 전송방법 등과 인증 알고리즘과 인증시기 등은 그 구현이 적절하지 않을 경우 보안기능 전체가 무의미할 수도 있으며, 망의 부하와 제어에 필요한 시간이 크게 증가될 수 있다. 따라서 시스템의 규모와 기능구성, 보안정책 등에 따라 적절한 인증 알고리즘과 인증시기, 그리고 암호화 방식 등을 채택하여 인증 및 암호화 통신 프로토콜을 적용할 필요가 있다. 또한 전송 데이터의 비밀성을 유지하는 암호화 통신에 대한 방안이 없다면 향후 제공될 전자 상거래나 전자결재 등에 이동성이 자유로운 무선단말을 사용하는 것이 문제가 될 수 있다.

IMT-2000에서 보안기능의 주 역할은 인증과 비밀성 두 범주로 나눌 수 있다[16]. 적법한 사용자인가를 확인하는 인증기능은, 단말에 따라 고유한 값을 인증센터와 단말이 보유하고 있는 상황에서, 망에서 인증알고리즘의 입력으로 사용될 값을 단말에 제공하고 단말은 인증계산 결과 값을 망에 회신하여 인증센터에서 계산한 인증 값과 비교하는 것이다. 그러나 인증을 위해 망과 단말 사이에 전송되는 파라메터와 인증계산 값이 평문이므로 쉽게 노출되어 공격당할 수 있는 문제점을 내포하고 있다. 또한 단말 대 단말 간 안전한 통신을 위해서는 암호화 기능이 필요하나, 다수의 불특정 가입자간 암호화 통신을 하기 위한 효율적인 키 분배 프로토콜이 요구된다.

본 논문에서는 인증에 입력되는 데이터나 결과값을 암호화하여 전송함으로서 기존의 인증시스템의 안전도를 높일 수 있는 인증방안을 제안한다. 또한 사용자 ID를 기반으로 하여 통신하는 단말간에 암호화 통신용 비밀키를 공유하는 프로토콜을 제안한다. 이 방식은 공개키와 비밀키 방식을 혼용하여 사용하고, 암호화 키 생성 및 분배 시에 상대 단말임을 확인하면서 키 공유 데이터를 전송하며, 단말기의 계산능력에 한계가 있다고 보고 단말에서의 계산부하를 줄이고 시간이 많이 소요되는 복잡한 계산은 인증서버에서 수행하도록 고려한다. 또한 단말의 인증과 암호화 통신 키 분배 시 홈망과 방문망 사이의 메시지 전송을 최소로 함으로서 시그널링 트래픽에 의한 오버헤드를 줄이도록 한다.

제안하는 사용자 인증과 암호화 통신용 키 분배 프로토콜을 설명하기 위해 사용하는 기호는 다음과 같다.

- AC_i : 인증센터 i의 ID
- MS_i : 이동단말 i의 ID
- CK_i : SSD_B에 의해 생성된 이동단말 i와 홈 인증센터의 공통 키
- SK_A : 인증센터 A의 비밀 키
- PK_A : 인증센터 A의 공개 키
- R_u, R_v, R_h : 사용자, 방문 망, 홈 망에서 제시한 난수
- CK_{ij} : 이동단말 MS_i가 MS_j로 통신하는 데 사용하는 공통 키
- CAVE() : CDMA에서 적용하는 인증 계산 알고리즘
- ARES, ARES' : 망과 이동단말 각각에서 CAVE()에 의해 계산된 인증 값
- E[CK: M], D[CK: C] : 공통 키 CK로 관용 키 알고리즘을 사용하여 암호화, 복호화
- E[PK: M], D[SK: C] : 공개 키 알고리즘을 사용하여 암호화, 복호화

1. 사용자 인증

그림 5는 인증계산에 사용되는 비밀정보들을 암호화하여 전송함으로서 기존의 인증기능의 안전도

를 높이는 방안을 나타낸다. 그림 5의 a)는 개선된 유일시도/응답 방식을, b)는 개선된 전체시도방식을 나타낸다.

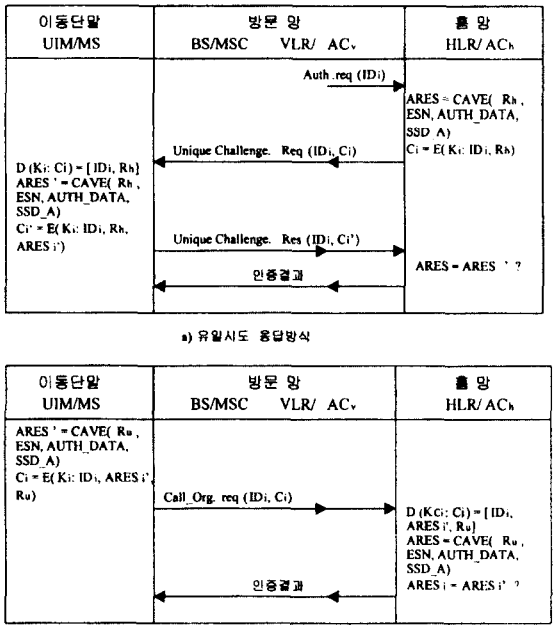


그림 5. 제안한 사용자 인증방식

기존의 유일시도/응답방식에서는 방문망이 난수 값을 단말에 제시한 것에 반하여 제안한 방식에서는 이동단말이나 사용자가 인증에 필요한 난수 값(R_u)을 생성하고, 저장된 인증관련 파라메터와 함께 인증 알고리즘을 수행하도록 함으로서 데이터 전송단계를 줄이도록 한다.

유일시도/응답방식의 단계 1은 인증을 필요로하는 사용자나 단말에서 난수를 생성하여 ESN, 단말번호, SSD_A와 함께 인증계산을 한다. 결과 값은 홈 인증센터와 공유하는 비밀 키인 CK_i를 사용하여 암호화한다.

[단계 1] MS_i : $ARES_i' = CAVE(R_u, ESN, ID_i, AUTH\_DATA, SSD\_A)$ (1)

$C1 = E[CKi: IDi, ARESi, Ru]$ (2)

단계 2는 암호화된 인증 값과 난수 값이 이동단말에서 방문망을 거쳐 홈 망의 인증센터로 전해진다.

[단계 2] MS_i --> VLR --> AC : ID_i, C1

단계 3은 홈망의 인증센터에서 발신단말의 비밀키를 찾아 암호문을 복호화하고, 발신단말이 보낸 난수 값을 입력으로 인증계산 한 결과와 수신한 인증 값을 비교한다.

[단계 3] AC : $D(CK_i: C1) = [ID_i, ARES_i', R_u]$ (3)

$ARES_i = CAVE(R_u, ESN, AUTH\_DATA, SSD\_A)$ (4)

$ARES_i = ARES_i'$? (5)

단계 4는 인증 결과를 방문망과 이동단말에 통보한다.

[단계 4] AC --> VLR --> MS_i : 인증결과

그림5의 b)에 나타난 바와 같이 전체시도 방식에서도 인증계산에 관련된 데이터를 비밀키로 암호화하여 전송함으로서 이동단말과 홈 망의 인증센터 간에 이루어 지는 인증과정이 기존방식에 비해 안전성을 보장할 수 있다.

2. 안전한 인증을 포함한 ID 기반 키 공유 프로토콜

비밀키 암호화방식은 사용자의 수가 많아질수록 키관리 및 분배에 어려움이 있으나, 비교적 빠른 속도로 계산할 수 있어서 보안기능에 소요되는 시스템의 부하 증가를 줄일 수 있다는 장점이 있다. 반면에, 공개 키 방식은 계산시간이 많이 소요되나 키 관리가 용이하고 이에 따른 안전성이 보장되는 장점이 있다. 따라서 세션 키를 분배하기 위한 마스터 키의 적용은 공개 키 방식을, 세션 내에서 통신되는 메시지의 암호화에는 비밀 키 방식을 사용함으로써 두 암호화 방식의 장점을 이용한 암호화 통신 프로토콜에 관한 연구가 많이 수행되고 있다[15].

이동통신 시스템에서 안전한 데이터 전송을 위한 암호화 기능을 갖도록하기 위해서는 인증기능 외에 불특정한 다수의 단말 간에 암호화 통신용 키를 효율적으로 분배하는 프로토콜이 요구된다. 키 분배 프로토콜은 이동통신 시스템이 갖는 보안 및 인증기능을 기반으로 이루어져야 하고, 키 분배 프로토콜의 추가로 인한 시스템의 부하가 가능한한 최소가 되도록 하며, 단말의 계산능력을 고려하여

복잡한 계산은 인증서버에서 수행되도록 할 필요가 있다.

본 논문에서는 이러한 요구사항을 고려하여 IMT-2000에서 사용자와 인증센터 ID를 기반으로 암호화 통신을 하기 위한 효율적인 키 공유 프로토콜을 제안한다. IMT-2000의 기능모델 내에는 인증을 수행하는 인증센터를 포함하고 있으며, 인증센터는 홈 망에 속한 각 단말기에 대해 인증과 암호화 통신에 필요한 비밀 데이터와 비밀 키를 관리한다.

암호화 통신은 호 설정 후에 시작되며, 호 설정시에는 발신단말과 발신단말의 홈 인증센터, 착신단말과 착신단말의 홈 인증센터간에 비밀 데이터를 이용하여 인증이 이루어진다. 따라서 암호화 통신을 위한 키 분배 프로토콜이 수행되기 전에 인증과정을 통해서 각 단말과 홈 인증센터에는 항상 동일한 비밀 데이터와 비밀 키가 저장되어 있다고 할 수 있다. 따라서 암호화 통신용 키 분배 프로토콜에서는 발착신 단말에 보유하고 있는 비밀 키를 사용하여 키를 분배하는 대신에, 단말의 홈 인증센터에 보유하고 있는 비밀 키를 기반으로 각 단말에 동일한 비밀 키를 갖도록 함으로써 키 분배 절차를 간략화 할 수 있다.

암호화 통신용 키 분배 프로토콜을 설명하기 위해 다음과 같은 가정을 한다.

- 이동단말과 인증센터는 각각 고유의 ID를 가지고 있다.
- 각 이동단말은 홈 망의 인증센터 사이에 비밀 키를 공유하고 있다.
- 단말 간 암호화 통신 키를 공유하는 과정이 수행되기 전에 발착신 단말은 호설정 과정 중에 각각 홈 망의 인증센터와의 사이에 인증과정이 수행된다.
- 모든 이동단말은 같은 암호화 알고리즘을 사용한다.
- 각 단말과 홈 인증센터 사이의 통신은 공유하고 있는 비밀 키를 사용한 관용 키 알고리즘을 적용한다.
- 인증센터 사이의 통신은 공개 키를 기반으로한 암호화 통신을 하기 위한 준비는 다음과 같다.

1) 큰 소수 p,q를 생성하고 두 소수의 곱 $n = p * q$를 계산하여 n을 공개정보로 한다.
2) $e * d = 1 \bmod (p-1)(q-1)$을 만족하는 소수 e와 정수 d를 결정하고 e를 공개정보로 한다.
3) GF(p)와 GF(q)에 포함된 정수 g를 선택하여 공개정보로 한다.
4) 인증센터 N은 자신의 ID_N를 기반으로 $S_N = ID_N^d \bmod n$을 계산하여 비밀 정보로 보관한다.

그림 6은 호 설정 과정 이후에 수행되는 사용자와 인증센터의 ID 정보에 의한 암호화 통신용 키 공유과정을 나타내고 있다. 발신단말 MS_1과 홈 인증센터 AC_A는 공통 키 CK_1을 공유하고 있으며, 착신단말 MS_2와 홈 인증센터 AC_B는 공통 키 CK_2를 공유하고 있다. ID_1과 ID_2는, ID_A와 ID_B는각각 발착신측 단말과 홈 인증센터의 ID를 의미한다.

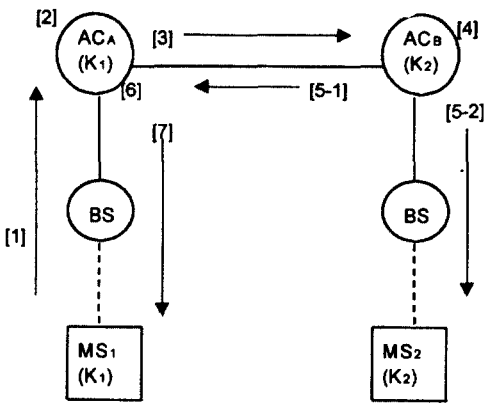


그림 6. 암호화 키 분배 과정

제 1단계는 암호화 통신을 원하는 발신단말 MS_1이 홈 인증센터와 공유하고 있는 공통 키인 CK_1을 가지고 자신과 통신을 원하는 착신 단말번호를 암호화하여 '암호화 통신요구' 메시지에 실어 자신의 홈 인증센터인 AC_A에 보낸다.

[1단계] $MS_1 \rightarrow AC_A : C1 = E[CK_1 : ID_1, ID_2]$ (6)
암호화 통신요구 메시지(ID_1, C1)

제 2단계에서는 홈 망의 인증서버가 암호화 통신

요구 메시지 내에 있는 발신단말 ID_1으로부터 공통 키 CK_1을 찾아서 수신 메시지를 복호화함으로서 착신단말 번호 ID_2와 해당 홈 인증센터를 알 수 있다. ID_2가 속한 홈 망의 인증센터에서 송신지 인증을 위해 X_A와 Y_A를 생성해 낸다. H_A를 계산하는 데에 사용된 h는 사용자 인증과 메시지 무결성을 위해 모든 인증센터가 공통으로 가지고 있는 해쉬함수이다. ID_A, ID_1, ID_2, time 정보는 수신측 인증센터의 공개 키로 암호화한다.

[2단계] AC_A : ID_1의 공통 키 CK_1을 찾음

$$(ID_1, ID_2) = D[CK_1: C1] \quad (7)$$

$$X_A = g^{e*CK_1} \bmod n \quad (8)$$

$$H_A = h(X_A, time, ID_1, ID_2) \quad (9)$$

$$Y_A = S_A * g^{H_A*CK_1} \bmod n \quad (10)$$

$$C2 = E[PK_B : ID_A, ID_1, ID_2, time] \quad (11)$$

제 3단계에서 AC_A는 제 2단계에서 생성한 X_A, Y_A, C2를 자신의 ID를 AC_B에 전송한다.

[3단계] AC_A ---> AC_B : X_A, Y_A, C2

제 4단계에서 AC_B는 자신의 비밀 키로 C2를 복호화하고, 수신한 정보 중 X_A, time, ID_1, ID_2를 자신이 가지고 있는 해쉬함수의 입력변수로 사용하여 H_A 값을 계산하고, $Y_A^e / X_A^{H_A}$를 계산하여 그 결과가 AC_A가 전송한 ID_A와 같은지를 검사한다. 일치하지 않으면 프로토콜 진행을 중단하고, 일치하면 두 개의 메시지 X_B, Y_B를 생성한다. 착신단말 MS_2에서 암호화 통신용 키로 사용될 비밀키 CK_{21}을 계산하여 통신단말 ID와 함께 MS_2와 AC_B의 공유 키인 CK_2로 암호화한다.

[4단계] AC_B : $(ID_A, ID_1, ID_2, time) = D[SK_B: C2]$ (12)

$$H_A = h(X_A, time, ID_1, ID_2) \quad (13)$$

$$ID_A = Y_A^e / X_A^{H_A} ? \quad (14)$$

$$X_B = g^{e*CK_2} \bmod n \quad (15)$$

$$H_B = h(X_B, time, ID_1, ID_2) \quad (16)$$

$$Y_B = S_B * g^{H_B*CK_2} \bmod n \quad (17)$$

$$C3 = E[PK_A: ID_B, ID_1, ID_2, time] \quad (18)$$

$$CK_{21} = X_A^{CK_2} \bmod n \quad (19)$$

$$C4 = E[CK_2: ID_1, ID_2, CK_{21}] \quad (20)$$

제 5-1단계와 5-2단계는 각각 독립적으로 수행될 수 있는 데, 5-1단계는 AC_B에서 AC_A로 제 4단계에서 생성한 X_B, Y_B와 인증센터와 단말의 ID정보를 암호화한 C3를 AC_A에 보내고 5-2단계는 AC_B에서 착신단말 MS_2로 통신용 암호화 키와 발착신 통신단말 번호를 암호화한 메시지 C4를 보낸다.

[5-1단계] AC_B ---> AC_A : X_B, Y_B, C3

[5-2단계] AC_B ---> MS_2 : C4

제 6단계에서 발신단말 홈 인증센터 AC_A는 수신한 C3을 자신의 비밀 키로 복호화하여 X_A, time, ID_1, ID_2를 자신이 가지고 있는 해쉬함수의 입력 매개변수로 사용하여 H_B 값을 계산하고, $Y_B^e / X_B^{H_B}$를 계산하여 그 결과가 AC_B가 전송한 ID_B와 같은지를 검사한다. 일치하면 발신단말 MS_1이 착신단말 MS_2로 암호화하는 데 사용할 비밀 키 CK_{12}를 계산하고, 전송을 위하여 AC_A와 MS_1의 공유 키 CK_1을 사용하여 암호화 한다.

[6단계] AC_A : $(ID_B, ID_1, ID_2, time) = D[SK_A: C3]$ (21)

$$H_B = h(X_B, time, ID_1, ID_2) \quad (22)$$

$$ID_B = Y_B^e / X_B^{H_B} ? \quad (23)$$

$$CK_{12} = X_B^{CK_1} \bmod n \quad (24)$$

$$C5 = E[CK_1: ID_1, ID_2, CK_{12}] \quad (25)$$

제 7단계에는 AC_A에서 MS_1로 암호화 통신용 키를 보내고 MS_1에서 이를 복호화함으로서 $CK_{12} = CK_{21}$인 공유 키를 MS_1과 MS_2사이에 공유하게 된다.

[7단계] AC_A ---> MS_1 : C5

이 프로토콜의 단계 4와 단계 6이 맞게 실행한 경우 g와 p가 공개된 값이기 때문에 AC_A와 AC_B가 각각 $CK_{12} = CK_{21}$인 CK_{12}, CK_{21}를 계산할 수 있다는 것을 알 수 있다. AC_B는 단계 4에서 $Y_A^e / X_A^{H_A}$를 계산하고 이 값이 수신한 ID_A와 일치하는 지를 확인함으로서, 메시지의 송신지가 AC_A 인지를 확인할 수 있다. AC_B에 대해서도 단계 6에서 마찬가지 사실을 확인할 수 있다.

IV. 검 증

제안한 인증 및 ID 기반 암호화 통신용 키분배 프로토콜에 대해 사용자 정보보안, 통신상대 인증, 암호화 효율, 암호화 프로토콜의 단순화 측면에서 검토한다.

제안한 인증방식에서 망에 전송되는 난수 값, 인증계산 결과 값 등을 단말의 비밀키로 암호화함으로서 해당 단말을 관리하는 홈 인증센터에서만 비밀 데이터를 해석하여 알 수 있도록 하였다. 따라서 방문망이나 홈 망까지 전달하는 중간단계에서 데이터의 절취에 의한 도용이나 가장 등을 방지할 수 있다. 또한 전체시도 방식의 경우 망에서 제공하는 난수 값을 수신하여 인증 값을 계산하는 대신에, 각 단말에서 난수를 발생하여 계산하도록 함으로서 정보전송 단계를 줄일 수 있고, 인증이 필요한 단말에서 인증 값을 미리 계산해 놓을 수도 있기 때문에 인증시간을 단축시킬 수 있다.

암호화 통신용 키 분배 프로토콜은 이산 대수 문제의 어려운 점을 이용하고 있기 때문에 X_A나 X_B가 공개되어도 각 단말의 비밀 키인 CK_1 또는 CK_2를 구하는 데 걸리는 계산시간이 커지게 되어 이에 근거한 암호시스템은 안전하다. 즉, n의 길이가 1000비트일 때 CK_1으로부터 X_A를 계산하거나 X_B와 CK_1을 이용하여 CK_{12}나 CK_{21}을 계산하는 데는 1000비트 길이의 수를 약 2000번 곱하는 연산이 필요하지만, 역으로 log 계산을 하기 위해서는 2^{100}, 약 10^{30}번 이상의 연산이 필요하기 때문이다.

단말에 관한 비밀 데이터와 암호화 키가 홈 인증센터에서 관리되고 있는 IMT-2000에 본 논문에서 제안하고 있는 키 분배 방식을 사용하면 첫째, 프로토콜에 따른 데이터 교환의 회수를 줄일 수 있고, 둘째, 암호화 통신을 하고자 하는 상대를 확인함으로서 안전한 통신이 가능하며, 셋째, 암호화 프로토콜 중 시간이 많이 걸리는 계산은 단말보다는 서버에서 수행하도록 함으로서 계산 시간과 단말기의 부하를 줄일 수 있다. 암호화통신을 요구하는 시점에 이미 각 단말은 발착신 호설정 과정에서 홈 인증센터와의 사이에 인증을 받은 상태이며, 인증센터에는 공유하는 비밀 데이터와 비밀 키가 있다. 따라서 나머지 전달 구간인 두 인증센터 간에 ID를 이용하여 상대를 확인함과 동시에 암호화 통신용 키를 공유하여 각 단말에 전송함으로서, 발착신단말 간에 직접 비밀 키를 공유하도록 시도하는 것에 비해 데이터 교환 회수가 줄고 안전한 통신을 보장할 수 있다. 만일 두 단말의 홈 인증센터가 동일하다면 인증센터 간 키공유 과정은 2단계부터 6단계까지 부분적 또는 전체적으로 생략되기 때문에 키 공유 과정은 더욱 간단해 진다. 또한 프로토콜 과정 중 지수승 계산과 같이 부담이 많이 되는 작업은 인증센터의 서버에서 수행하기 때문에 단말의 부하를 줄일 수 있다.

V. 결 론

이동통신 서비스의 수요가 증가함에 따라 무선통신망의 특성에 기인한 불법적인 도용이나 도청 또는 추적을 통한 개인 프라이버시 침해 등의 범죄행위도 늘어나게 된다. 이를 해결하는 방법의 하나로 사용자나 단말의 인증기능이 요구되며, 더구나 향후 제공될 전자상거래를 고려할 때 이동의 자유가 있는 무선망 사용자의 인증이나 전송 데이터의 암호화기술은 중요한 핵심기술이라 하겠다.

본 논문은 IMT-2000 시스템에서 인증 및 암호화 통신을 위해 전송되는 데이터를 암호화함으로서 사용자 데이터의 비밀성을 보장하고, 각각의 키가 인증센터에 분산되어 있는 송수신 단말이 가입자의 ID를 기반으로하여 홈 인증센터를 경유한 통신용 비밀키를 분배받는 방안을 제안하고 이에 대한 안전성 및 효율성을 분석한 것이다.

인증에서 안전성의 경우, 단말의 비밀 데이터나 인증에 관련된 데이터를 평문으로 전송하는 기존의 방식에 비해 이를 비밀키로 암호화하여 보낼 수 있게 함으로서 침입자에 대한 도용을 방지할 수 있다.

IMT-2000의 호 설정과정을 고려할 때, 암호화통신 요구 메시지가 전송되기 전에 발착신 과정에서 각 단말은 홈 망의 인증센터와 인증과정을 마친 상태이므로, 인증센터에서 발착신 단말의 ID와 공개키방식을 기반으로 상대 인증센터를 확인함과 동

시에 단말의 암호화 통신용 키를 분배하도록 함으로서, 키 분배 프로토콜이 간략화되며 이에 따른 처리속도의 개선 등을 기대될 뿐만 아니라 키 분배과정에서 필요한 복잡한 계산과정을 계산능력에 한계가 있는 이동단말에서 수행하지 않고 인증센터의 서버에서 수행하도록 함으로써 키의 안전성 향상을 기대할 수 있다.

향후, 제안한 방식을 기본으로해서 무선망을 통한 전자상거래에의 적용방안, IMT-2000이 제공해야하는 글로벌 로밍 서비스의 사용자 인증 및 암호화 통신 프로토콜 등에 관한 연구도 진행 될 수 있으리라 본다.

참 고 문 헌

1. ITU-T SG11, Draft New Recommendation of Q.FNA, Network Functional Model for IMT-2000, Version 8.0, Question 8/11 Rapporteur Meeting, Bath, U.K., June 1997.
2. ITU-T Baseline Document of Q.8/11(former SWP1/3-11) on IMT- 2000 Standardization(version 2), New York, April 1997.
3. ITU-T Draft Recommendation F.115 - Service Objectives and Principles for Future Public Land Mobile Telecommunications Systems(version 9), Question 8/1 Rapporteur Meeting, London, May 1995.
4. ITU-R M.816 Framework for Service Supported on FPLMTS, 1995.
5. ITU-T Draft Recommendation Q.FIF - Information Flows, (version 7.1), New York, April 1997.
6. ITU-T F.sfea Service Features in FPLMTS, Geneva, September 1994.
7. ITU-T Draft New Recommendation Q.FSR - FPLMTS Signaling Requirements for Radio Interface(General Aspect Ver. 1.2), Geneva, January 1997.
8. ITU-R Recommendation M.1078, Security Principles for Future Public Land Mobile Telecommunication Systems(FPLMTS)
9. W. Stallings, Network and Internetwork Security Principles and practice, Prentice-Hall, 1995.
10. TIA/EIA IS-95, Mobile Station - Base Station Compatibility Standard for Dual-Mode Wideband spread Spectrum Cellular System, TIA, July 1993.
11. Hak S. Jeong, Dong K. Kim, "An authenticated key distribution protocol for the CDMA mobile communication network", , June 1997.
12. S. Hirose, S. Yoshida, "A Secure authenticated Diffie-Hellman key agreement protocol and its application to conference key distribution", ISEC97-37, Sep. 1997.
13. Teag H. Lee, Yeong J. Kim, "Performance of Authentication for Digital Mobile Comm. Networks based on Public key Cryptographic Technology", CICE, Oct. 1997.
14. 박순, "CDMA 무선 데이터 서비스", 텔레콤, 제 11권 2호, pp. 13-22, 1995. 12.
15. "통신망 데이터 보호기술", 한국전자통신연구원 보고서, 1992.

이 태 훈(Taehoon Lee)정회원
현재:광주대학교 컴퓨터학과

정 일 용(Ilyong Chung)정회원
현재:조선대학교 전자계산학과

김 용 득(Yongdeak Kim)정회원
현재:아주대학교 전자공학과