IMT-2000환경에서 Symmetric Balanced Incomplete Block Design을 응용한 회의용 인증메커니즘의 설계

배용근[†] · 정일용[††]

요 약

본 논문은 IMT-2000환경에서 대수학적 방법을 적용하여 회의용 키 인증 메커니즘을 제안한다. 이를 위해서 symmetric balanced incomplete block design 기법을 응용하여 회의용 키를 생성하고, 참여한 사용자들에 생성된 키를 분배한다. 회의용 키 생성 기술과 ID 정보를 기반으로 하여 수행된 상호 인증을 통하여 통신 프로토콜은 설계한다. 제안된 프로토콜에서 회의용 전송키를 생성하기 위한 통신 복잡도를 최소화시키며, 특별한 경우에 복잡도는 $O(v\sqrt{v})$이 되는데 여기에서 v는 참여자의 수이다. 보안 시스템의 구축에 있어서 중요한 문제인 본 프로토콜의 안전도는 이산 대수를 찾아내는 것은 hard 문제이기 때문에 보장할 수 있다.

The Design of Conference-based Authentication Mechanism Employing the Symmetric Balanced Incomplete Block Design on IMT-2000 Environment

Yongeun Bae[†] and Ilyong Chung[††]

ABSTRACT

In this paper, we present a conference key authentication mechanism by employing an algebraic method on IMT-2000 environment. To accomplish this, the symmetric balanced incomplete block design is applied for generating a conference key and then this key is distributed to participants. Through the technique for creation of a conference key and mutual authentications performed based on identification information, a communication protocol is designed. The protocol proposed minimizes the communication complexity for generating a conference key. On a special case the complexity is $O(v\sqrt{v})$, where v is the number of participants. The security of the mechanism, which is a significant problem in construction of secure systems, can be assured since finding discrete logarithms is generally a hard problem.

Key words: Symmetric Balanced Incomplete Block Design, 인증, 회의용 키분배 시스템

1. 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 종합정보통신망으로 발전하고 있으며, 전송방식의 디지털화, 고속화, 서비스 종합화를 추구하고 있다. 또한 현재 세계적으로 급속하게 보급되고 있는 이동통신 서비스를 위한 무선통신망도 음성서비스 위주의 아날로그방식에서 디지털방식으로, 그리고 개인휴대통신을 거쳐 고속데이터, 영상 등의 멀티미디어 서비스까지 지원할 수 있는 IMT-2000[1,2]으로 진화하고 있다.

접수일 : 2003년 2월 24일, 완료일 : 2003년 6월 3일
[†] 정회원, 조선대학교 컴퓨터공학부 부교수
[††] 종신회원, 조선대학교 컴퓨터공학부 부교수

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 위치 갱신시에 방문망의 전송로를 경유하여 단말기가 등록된 홈 망의 인증센터에서 인증과정을 수행하여 통보한다. 이를 위해 단말과 사용자, 그리고 인증센터는 인증에 필요한 비밀 데이터를 보유 및 관리하고 있다. 그러나 현재 제시된 인증과정은 단말과 인증센터간에 비밀 데이터를 평문으로 전송하기 때문에 외부에 노출되기 쉽다.

IMT-2000의 보안원칙에 관련하여 ITU-R에서는 서비스 관련, 접근제어 관련, 이동단말 관련, 사용자 관련, 네트워크 운용 관련, 그리고 보안관리 관련 등에 대해 최소한의 기본 요구사항을 제시하고 있는데, 무선통신시스템의 보안위협에 대적할 수 있는 구체적인 방안이나 조치는 제시되지 않고 있다. 또한 무선망을 통한 비밀 데이터의 전송과 전자상거래 서비스 제공을 위해 필요한 인증[3-5] 및 회의용 그룹통신에 관한 연구가 절실한 상태이다.

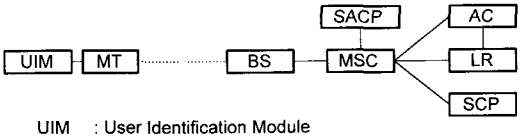
본 논문에서는 IMT-2000에서 사용자 인증시 단말과 홈 망의 인증센터 간에 교환되는 데이터를 암호화함으로서 전송로에서의 정보를 보호하고, 회의용 키분배 시스템을 위한 회의용 키생성 및 ID기반[6]으로 하여 효율적인 회의용 키분배 프로토콜을 제안한다. Ingemarssory[7]이 Ring Network상에서 다자간 회의용 키를 생성하는 방법을 제안하고 Koyama[8]는 인증을 고려한 키분배 방식(Identity-based Conference Key Distribution System:ICKDS)을 Ring Network, 완전 그래프 네트워크와 스타 네트워크 상에서 제안하였다. 그리고 Shimbo[9]는 기 발표된 회의용 키분배 시스템을 분석하였다. Koyama가 제안한 ICKDS가 완전그래프 네트워크 상에서 수행할 때 회의용 키분배 시스템을 위해서 가입자의 수가 v일 때 $O(v^2)$의 통신 복잡도가 필요하지만, 본 연구에서는 symmetric balanced incomplete block design을 응용하여 회의용 전송키를 생성하는 메카니즘을 설계하여 기존의 방식보다는 복잡도를 감소시키고, 특수한 경우에는 $O(v\sqrt{v})$로 향상시킬 수 있다.

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

2. IMT-2000의 인증 및 보안체계

IMT-2000의 보안요구사항은 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 분산되어 구성된다. 그림에서 사용자는 UIM(User identification Module)으로 표현되고, UIM의 기능에 의해 사용자 이동성이 보장된다. AC(Authentication Center)는 홈 망에 등록한 모든 사용자와 단말기들의



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

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 망간의 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.

인증은 상대방을 확인하는 절차로 매우 중요한 통신서비스로서 UIM과 홈 망의 인증센터간에 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. 인증 알고리즘의 수행하는 UIM은 스마트 카드 형태를 가지면서 사용자 이동성에 관련된 정보와 알고리즘을 관리하고 인증 파라메터를 생성하여 관리한다. 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 인증키와 암호화키를 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. SSD_A는 CDMA 인증기능을 위하여 인증서명절차에 사용되는 알고리즘의 입력, 즉, 인증키로 사용하고 SSD_B는 CDMA 음성 프라이버시와 신호 메시지의 기밀성을 위한 암호화키를 계산하는 데에 사용된다. 따라서 동일한 난수 값을 가지고 단말과 망에서 각각 SSD 생성과 암호화 통신용 키를 생성하는 과정을 수행함으로서 공통키를 보유할 수 있게 된다.

IMT-2000에서 수행하는 인증절차는 이동단말이 기지국에 등록을 하고자 할 때 수행하는 이동단말 등록시, 이동단말의 발호와 착호시, 이동단말 등록 인증절차나 이동단말 발호 인증절차가 실패할 때 수행되는 유일 도전 응답절차 수행시, 이동단말의 유일 도전 응답인증절차가 실패한 경우 수행되는 비밀 공유 데이터 갱신절차시 등에 수행한다.

인증과정은 이동망에서 난수 값을 제시하고, 이동단말에서는 난수를 입력으로 인증알고리즘을 수행한 결과 값을 이동망에 제출하여 비교함으로서 수행하게 되는데, 망의 상황에 따라 유일시도/응답(Unique Challenge/Response Mechanism)과 전체시도(Global Challenge Mechanism)라는 2 가지 방식이 선택적으로 사용될 수 있다. 유일시도/응답방식은 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 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 전해

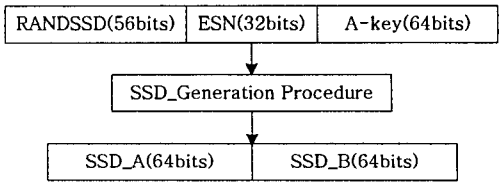


그림 2. SSD 생성과정

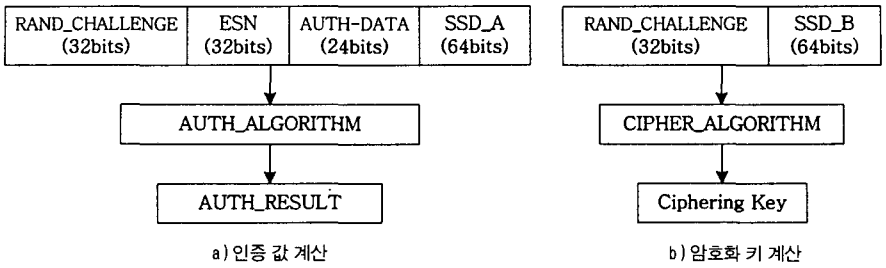


그림 3. SSD를 사용한 인증 및 비밀키 계산

진다. 인증센터에서는 수신된 파라메터와 보유하고 있는 SSD_A 등을 가지고 단말에서와 동일한 인증 알고리즘을 수행하여 단말에서 전송한 인증 값과 일치여부를 검사함으로서 인증과정이 수행된다.

3. 인증 및 회의용 키분배 시스템의 설계

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. 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 암호화 통신을 위한 키 관리 및 키 공유 프로토콜에 대한 구체적인 연구가 필요하다.

본 논문에서는 인증에 입력되는 데이터나 결과 값을 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 분배시에 상대단말임을 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 통신 키 분배방식을 설명하기 위해 사용하는 기호는 다음과 같다.

- AC_i : 인증센터 i의 ID
- MS_i : 이동단말 i의 ID
- r_i : SSD_B에 의해 생성된 이동단말 i와 홈 인증센터의 공통 키
- R_u, R_v, R_h : 사용자, 방문 망, 홈 망에서 제시한 난수
- $E_K[M]$: 메시지 M을 키 K로 암호화
- CAVE() : CDMA에서 적용하는 인증 계산 알고리즘
- ARES, ARES′ : 망과 이동단말 각각에서 CAVE()에 의해 계산된 인증 값

3.1 사용자 인증

기존의 유일시도 응답방식에서는 방문망이 난수 값을 단말에 제시하였는데 반하여 제안한 방식에서는 이동단말이나 사용자가 인증에 필요한 난수 값(R_u)을 생성하고, 저장된 인증관련 파라메터와 함께 인증 알고리즘을 수행하도록 함으로서 데이터 전송단계를 줄일 수 있으며 인증 프로토콜은 다음과 같다.

[1단계]

MS_i : $ARES_i' = CAVE(R_u, ESN, ID_i, SSD\_A)$

$C_i = E_{ri}[ID_i, ARES_i, R_u]$

유일시도 응답방식의 제 1단계에서는 인증을 필요로 하는 사용자나 단말에서 난수를 생성하여 ESN, 단말번호, SSD_A와 함께 인증계산을 한다. 결과 값은 홈 인증센터와 공유하는 비밀키인 r_i를 사용하여 암호화한다.

[2단계] $MS_i \rightarrow VLR \rightarrow AC$: ID_i, C_i

제 2단계에서는 암호화된 인증 값과 난수 값이 이동단말에서 방문망을 거쳐 홈 망의 인증센터로 전한다.

[3단계] AC : $[ID_i, ARES_i', R_u] = D_{ri}[C_i]$

$ARES_i = CAVE(R_u, ESN, ID_i, SSD\_A)$

$ARES_i = ARES_i'$?

제 3단계에서는 홈 망의 인증센터에서 발신단말의 비밀키를 찾아 암호문을 복호화하고, 발신단말이 보낸 난수 값을 입력으로 인증계산 한 결과와 수신한 인증 값을 비교한다.

[4단계] $AC \rightarrow VLR \rightarrow MS_i$: 인증결과

제 4단계에서는 인증 결과를 방문망과 이동단말에 통보한다.

전체시도 방식에서도 인증계산에 관련된 데이터를 비밀키로 암호화하여 전송함으로서 이동단말과 홈 망의 인증센터 간에 이루어지는 인증과정이 기존 방식에 비해 안전성을 보장할 수 있다.

3.2 Symmetric Balanced Incomplete Block Design을 이용한 회의용 키분배 시스템의 설계

이동단말과 홈 망간의 인증 메커니즘을 이용하여 홈 망이 상이한 n개의 이동단말이 서로 정보 교환하여 회의용 키분배 시스템을 구축하려 한다. 본 논문에서는 이동단말과 사용자는 동일한 개념으로 이용된다. 이를 위해서 서로간 공통의 키를 각 사이트의 키를 이용하여 통신키를 빠른 시간 안에 생성하여야 하고 이 키의 생성에 필요한 시간 복잡도와 공간 복잡도는 최대한 보장이 되어야 한다. algebraic 방법의 하나인 에러수정 코드가 갖는 이온적인 특징을 이용하여 회의용 키를 생성하기 위한 메시지 전송량을 최소화하고자 한다. 이 코딩 기법[10,11]은 최적의 코드워드가 주어졌을 때 어떤 특정 코드워드가 속한 coset를 찾아가서, 만일 코드 워드에 에러가 발생했다고 하더라도 원래의 데이터 값을 갖는 것이다. 이것을 메시지의 경로 설정에 적용한다면 대단히 효율적인 분산 경로방법을 선택할 수 있을 것이다. 본 연구에서는 symmetric balanced incomplete block design(SBIBD)[12]을 적용하고 있어 회의용 키를 생성 및 분배하고 있다.

정의 1: X가 v개의 객체 $x_1,x_2,...,x_v$를 가진 집합일 때, X의 balanced incomplete block design(BIBD)은 다음의 조건을 만족하는 b개의 부분집합(블럭)으로 구성되며, 각 부분집합의 크기는 k이다.

1. 각 객체는 b개의 블럭에서 r개가 나타난다.
2. 각각의 두 객체는 b개의 블럭에서 λ개가 나타난다.(Every two objects appears simultaneously in exactly λ of the b blocks)
3. $k < v$.

예를 들어 $B_1=\{x_1,x_2,x_3\}$, $B_2=\{x_4,x_5,x_6\}$, $B_3=\{x_7,x_8,x_9\}$, $B_4=\{x_1,x_4,x_7\}$, $B_5=\{x_2,x_5,x_8\}$, $B_6=\{x_3,x_6,x_9\}$, $B_7=\{x_1,x_5,x_9\}$, $B_8=\{x_2,x_6,x_7\}$, $B_9=\{x_3,x_4,x_8\}$, $B_{10}=\{x_1,x_6,x_8\}$, $B_{11}=\{x_2,x_4,x_9\}$, $B_{12}=\{x_3,x_5,x_7\}$일 때 $X=\{x_1,x_2,...,x_9\}$, b=12, v=9, r=4, k=3, λ=1가 되고 이것은 다섯 개의 파라메터 b,v,r,k, λ를 사용하여 (12,9,4,3,1)-configuration로 표현되며 BIBD를 만족하는 이들 파라메터들의 관계는 정리 1에 있으며[12]에서 증명하고 있다.

정리 1: BIBD에서 $bk = vr$이고 $r(k-1) = \lambda(v-1)$이다.

k-subset 대신에 BIBD는 원소가 0과 1로 구성된 $(b \times v)$ 접합 행렬(incidence matrix) Q로 표현할 수 있는데 행렬의 열은 $x_1,x_2,..,x_9$으로, 행렬의 행은 $B_1,B_2,...,B_{12}$으로 대응되어 아래에 나타난다. 만일 x_j가 B_i에 있다면 $Q_{i,j}$=1이고 아니면 $Q_{i,j}$=0으로 표시된다. 위의 예를 접합 행렬로 나타내면 아래와 같다.

$$Q = \begin{bmatrix} 1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&1 \\ 1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&0&1 \\ 1&0&0&0&1&0&0&0&1 \\ 0&1&0&0&0&1&1&0&0 \\ 0&0&1&1&0&0&0&1&0 \\ 1&0&0&0&0&1&0&1&0 \\ 0&1&0&1&0&0&0&0&1 \\ 0&0&1&0&1&0&1&0&0 \end{bmatrix}$$

그림 4. (12×9) incidence matrix

인증 메카니즘에서 사용되는 키는 SBIBD를 적용하는데 여기에서 B_i는 $object_i$로, x_i는 key_i로 대응되어 블럭의 개수와 |X|의 값은 동일해야 한다.

정의 2: 만일 b=v, r=k이면, BIBD는 SBIBD라 정의한다.

SBIBD에서는 어떤 두 block은 공통으로 λ개가 들어있다는 것을 알 수 있고, 이는 (v,k,λ)-configuration로 표현하며 정리 1을 만족하고 있다. 예를 들어서 $B_1=\{x_1,x_2,x_4,x_7,x_{11}\}$,$B_2=\{x_1,x_2,x_3,x_5,x_8\}$, $B_3=\{x_2,x_3,x_4,x_6,x_9\}$, $B_4=\{x_3,x_4,x_5,x_7,x_{10}\}$,$B_5=\{x_4,x_5,x_6,x_8,x_{11}\}$, $B_6=\{x_5,x_6,x_7,x_9,x_1\}$,$B_7=\{x_6,x_7,x_8,x_{10},x_2\}$, $B_8=\{x_7,x_8,x_9,x_{11},x_3\}$,$B_9=\{x_8,x_9,x_{10},x_1,x_4\}$, $B_{10}=\{x_9,x_{10},x_{11},x_2,x_5\}$, $B_{11}=\{x_{10},x_{11},x_1,x_3,x_6\}$일 때 b=v=11, r=k=5, λ=2이 되어 (11,5,2)-configuration이 된다.

통신에 참여하는 각 사용자는 (v,k,λ)-configuration를 이용하여 효율적인 메시지 전송량을 가지고 회의용 키를 얻을 수가 있다. 예를 들어서 7명의 사용자가 화상회의를 할 때 (7,4,2)-configuration을 사용하고 각 사용자는 비밀키 r_i를 가지고 있다. 먼저 접합 행렬을 아래와 같이 구한다.

각 사용자는 상대방으로부터 비밀키를 받아서 회의용 키를 생성하는데 본 논문에서는 두단계를 이용하여 계산한다. 먼저 사용자 i는 i번째의 행에서 원소의 값이 1인 사용자 j로부터 키값 r_j을 받고 다음에는

$$Q = \begin{bmatrix} 1&1&0&1&0&0&1 \\ 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 0&0&1&1&1&0&1 \\ 1&0&0&1&1&1&0 \\ 0&1&0&0&1&1&1 \\ 1&0&1&0&0&1&1 \end{bmatrix}$$

그림 5. (7×7) incidence matrix

k번째의 행(i≠k)에서 키값을 받아 회의용 키를 계산한다. 위의 행렬에서는 사용자 1은 1번째의 행에서 원소의 값이 1인 사용자 2,4,7로부터 키값를, 2,5,7행에서 키값을 받아 계산한다. Block 1에서는 $k_{11}=r_2*r_4*r_7$, $k_{12}=r_1*r_4*r_7$, $k_{14}=r_1*r_2*r_7$, $k_{17}=r_1*r_2*r_4$을 계산한다. Block 2에서 $k_{21}=r_2*r_3*r_5$, Block 5에서 $k_{51}=r_5*r_6*r_4$, Block 7에서 $k_{71}=r_7*r_3*r_6$를 받아 회의용 키 K를 얻는다; $K = r_1^2 * (k_{11}*k_{21}*k_{51}*k_{71})$.

정리 2: (v,k,λ)-configuration을 기반으로 하는 회의용 키는 다음과 같이 계산한다.

$$K = r_i^{\lambda} \times \left(\prod_{Q_{ji}=1} k_{ji}\right)$$

증명 : (v,k,λ)-configuration의 정의에 의해서 (v x v) 접합 행렬의 각 행과 열에는 k개의 1이 존재한다. 각 사용자는 화상회의를 위해서 회의용 키가 만들어져야 하는데 값은 $r_1*r_2*...*r_v$이다. 회의용 키는 두단계를 거쳐서 얻어지는데 첫 번째 단계에서 (k-1)개의 키의 곱이 주어지고 두 번째 단계에서 (k-1)행에서 (k-1)개의 키의 곱이 주어지므로 이를 계산하면(k-1)+(k-1)*(k-1)=k^2-k가 된다. 정리 1을 적용하면 k(k-1)=λ(v-1)가 되어 k(k-1)개의 곱에는 자신의 비밀키를 제외한 상이한 (v-1)개의 비밀키가 λ개씩 들어있음을 알 수 있다. 그러므로 각 사용자는 자신의 비밀키를 λ 멱승한 값과 (k^2-k) 비밀키를 곱하면 회의용 키를 계산한다.

각 사용자들이 (7,4,2)-configuration에서 정리 2을 사용하여 동일한 회의용 키를 구하는데 일련의 과정이 (표 1)에서 표현된다.

표 1. (7,4,2)-configuration에서 회의용 키 생성단계

사용자 ID	단계 1	단계 2
1	$k_{11}=r_2*r_4*r_7$, $k_{12}=r_1*r_4*r_7$, $k_{14}=r_1*r_2*r_7$, $k_{17}=r_1*r_2*r_4$	$r_1^2 * (k_{11}*k_{21}*k_{51}*k_{71})$
2	$k_{22}=r_1*r_3*r_5$, $k_{21}=r_2*r_3*r_5$, $k_{23}=r_2*r_5*r_1$, $k_{25}=r_2*r_3*r_1$	$r_2^2 * (k_{22}*k_{12}*k_{32}*k_{62})$
3	$k_{33}=r_2*r_4*r_6$, $k_{34}=r_2*r_3*r_6$, $k_{36}=r_2*r_4*r_3$, $k_{32}=r_3*r_4*r_6$	$r_3^2 * (k_{33}*k_{23}*k_{43}*k_{73})$
4	$k_{44}=r_3*r_5*r_7$, $k_{45}=r_3*r_4*r_7$, $k_{47}=r_3*r_5*r_4$, $k_{43}=r_4*r_5*r_7$	$r_4^2 * (k_{44}*k_{14}*k_{34}*k_{54})$
5	$k_{55}=r_4*r_6*r_1$, $k_{56}=r_4*r_5*r_1$, $k_{51}=r_4*r_6*r_5$, $k_{54}=r_5*r_6*r_1$	$r_5^2 * (k_{55}*k_{25}*k_{45}*k_{65})$
6	$k_{66}=r_2*r_5*r_7$, $k_{67}=r_2*r_5*r_6$, $k_{62}=r_6*r_5*r_7$, $k_{65}=r_2*r_6*r_7$	$r_6^2 * (k_{66}*k_{36}*k_{56}*k_{76})$
7	$k_{77}=r_1*r_3*r_6$, $k_{71}=r_7*r_3*r_6$, $k_{73}=r_1*r_7*r_6$, $k_{76}=r_1*r_3*r_7$,	$r_7^2 * (k_{77}*k_{17}*k_{47}*k_{67})$

위의 방법은 회의를 참여하는 사용자가 메시지를 전송하기 위한 회의용 키를 생성하는 과정을 살펴보았지만 이 과정에서는 회의용 키를 생성하기 위해 필요한 전송된 상대방의 키가 적법한 가에 대한 확신은 없다. 이를 위해 우리는 인증을 위해서 사용자의 ID 정보를 활용하여 다음과 같이 비밀정보를 생성한다. 여기에서 ID 정보의 크기는 256bit 미만으로 한다.

(1) 홈 망은 256비트이상의 자릿수를 가진 p, q를 생성하고 n=p*q를 계산한다.

(2) 조건을 만족하는 e와 d를 계산한다.

e. $d = 1 \bmod (p-1)*(q-1)$

(3) GF(p)와 GF(q)에 포함되는 정수 g를 얻는다.

(4) 각 사용자에게 비밀정보 S_i를 계산하다.

$S_i = ID_i^d$

각 사용자는 e,g,n,ID_i,S_i와 같은 정보를 갖고 있으며 공개정보로는 e,g,n이 있다. 이제 사용자를 효율적으로 인증하고 메시지 전송을 위한 회의용 키 생성 프로토콜은 다음과 같다.

[1단계] i → j : (ID_i, X_{ij}, Y_{ij}, $time_1$)

$X_{ij} = g^{e \cdot r_i} \bmod n,\ Y_{ij} = S_i \times g^{C1 \cdot r_i} \bmod n,$

$where\ C1 = h(X_{ij}, time_1)$ and $i, j \in B_j$

제 1 단계에서는 B_j에 속한 사용자 i는 인증을 위한 두가지 정보 X_{ij}와 Y_{ij}를 생성하여 사용자 j에게 (ID_i, X_{ij}, Y_{ij}, $time_1$)을 보내며 이때 h는 모든 사용자가 공통으로 가지고 있는 해쉬 함수이다.

[2단계] j :

$ID_i = Y_{ij}^e / X_{ij}^{C2},\ where\ C2 = h(X_{ij}, time_1)$

제 2 단계에서는 사용자 j는 전송된 정보와 보유하고 있는 해쉬 함수를 이용하여 사용자 i를 인증하는데 만일 $ID_i = Y_{ij}^e / X_{ij}^{C2}$ 이라면 인증한다.

[3단계] j → p : (ID_j, X_{jp}, Y_{jp}, $time_2$)

$X_{jp} = \prod_{i \in B_j - p} X_{ij}$

$Y_{jp} = S_j \times g^{C3 \cdot r_j} \bmod n,\ where\ C3 = h(X_{jp}, time_2)$

제 3 단계에서는 j는 B_j에 속한 사용자들로부터 받은 X_{jp}와 Y_{jp}를 계산하여 사용자 p에게 (ID_j, X_{jp}, Y_{jp}, $time_2$)를 보낸다. 여기에서 X_{jp}는 회의용 키를 생성하기 위한 중간단계의 키가 된다.

[4단계] p :

$ID_j = Y_{jp}^e / X_{jp}^{C4},\ where\ C4 = h(X_{jp}, time_2)$

$K = \prod_{i=1}^{k-1} X_{j,p} \cdot X_{pp} \cdot g^{e^{\lambda} \cdot r_p^{\lambda}}$

제 4 단계에서는 사용자 p는 사용자 j로부터 받은 정보를 이용하여 사용자 j를 인증하는데 만일 $ID_j = Y_{jp}^e / X_{jp}^{C4}$ 이라면 메시지가 사용자 j로부터 전송되었음을 확인하고 이 정보들을 이용하여 공통의 회의용 키 K를 생성한다. 사용자 p는 전송받은 (k-1)개의 키, X_{pp}와 자신의 비밀키를 이용하여 계산하는데 이들 k개의 키에는 사용자 p를 제외한 각 사용자의 비밀키가 λ번씩, e는 λ(v-1)번이 멱승으로 되어 있다. 그러므로 모든 사용자가 동일한 키를 갖기 위해서 사용자 p는 자신의 비밀키와 e를 λ로 각각 멱승한다.

정리 3: 사용자 j는 만일 ID_i가 Y_{ij}^e / X_{ij}^{C2}이라면 회의용 키를 생성하기 위한 정보가 사용자 i로부터 전송된 것임을 인증한다.

증명 :

$Y_{ij}^e / X_{ij}^{C2} = (S_i \cdot g^{C1 \cdot r_i})^e / (g^{e \cdot r_i})^{C2} \equiv S_i^e$, if $C1 = C2$

이 되어 S_i는 ID_i^d이므로 $(ID_i^d)^e$는 Fermat의 정리에 의해 ID_i가 된다.

3.3 인증 메커니즘의 분석

제안된 프로토콜에서 회의용 키 생성을 위한 통신 복잡도를 고찰하도록 한다. 이 방식은 (v,k,λ)-configuration을 응용하여 설계된 것으로 정리 2에서 증명하는 과정과 같이 1단계에서 v*(k-1)의 전송이 발생하고 2단계에서도 동일하게 v*(k-1)의 전송량이 필요하게 되어 전체 복잡도는 O(v*k)이 된다. 정리 2을 통하여 알 수 있듯이 k는 v와 λ의 값에 의해서 결정되며 λ=1인 특별한 경우에는 k가 $\sqrt{v}$의 근사값으로 되어 복잡도는 O($v\sqrt{v}$)이다.

프로토콜의 안전도 측면에서는 비밀 정보 S_i를 알아내기 위해서는 공개정보 e와 n을 가지고 d를 구해야 하는데 이를 위해 n을 소인수 분해를 수행해야 하는데 265bit 이상의 p,q를 선택하므로 이는 불가능하다. 그리고 인증과 회의용 키 생성을 위한 메시지인 X_{ij}로부터 비밀키 r_i를 계산해야 하는데 이는

GF(r)상의 이산 대수문제의 어려움 때문에 비밀키를 찾아낼 수 없어 안전성을 보장받는다.

4. 결 론

이동통신 서비스의 수요가 증가함에 따라 무선통신망의 특성에 기인한 불법적인 도용이나 도청 또는 추적을 통한 개인 프라이버시 침해 등의 범죄행위도 늘어나게 된다. 더구나 향후 제공될 전자상거래를 고려할 때 이동의 자유가 있는 무선망 사용자의 인증이나 전송 데이터의 암호화기술은 중요한 핵심기술이다.

본 논문은 이동통신 시스템에서 인증 및 암호화통신을 위해 전송은 데이터를 암호화함으로서 사용자 데이터의 비밀성을 보장하고, 각각의 키가 인증센터에 분산되어 있는 송수신 단말이 인증센터의 ID를 기반으로 하여 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.

회의용 키관리 시스템을 설계하기 위해서 block design중의 하나인 (v,k,λ)-configuration 기법을 응용하여 회의용 키를 생성하여 참여한 사용자들이 키를 분배한다. 이런 키 생성 기술과 ID 정보를 기반으로 하여 수행된 상호 인증을 통하여 통신 프로토콜은 설계한다. 제안된 프로토콜에서 프로토콜의 효율성 측면에서는 회의용 전송키를 생성하기 위한 통신 복잡도를 최소화시키고, 특히 λ=1인 경우에는 복잡도는 $O(v\sqrt{v})$이 된다. 보안 시스템의 구축에 있어서 중요한 문제인 본 프로토콜의 안전도는 이산 대수를 찾아내는 것은 hard 문제이기 때문에 보장할 수 있다.

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] D. Lee and I. Lee, "Security Protocols for IMT-2000-Based Contents Services," SAM'02, pp. 113-119, 2002.

[3] W. Stallings, Cryptography and Network Security, Prentice-Hall, 1999.

[4] 김은환, 전문석, "공개키를 이용한 커버러스기반의 강력한 인증 메커니즘의 설계," 한국통신정보보호학회논문지, 제12권, 제4호, pp. 67-76, 2002. 8.

[5] 박호상, 정수환, "패스워드 기반의 상호인증 및 키 교환 프로토콜," 한국통신정보보호학회논문지, 제12권, 제5호, pp. 37-44, 2002. 10.

[6] A.Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature schemes", Proc. of Crypto'86, Lecture Notes in Computer Science no. 263, Springer-Verlag, pp. 186~194, 1987.

[7] I. Ingemarsson, D. T. Tang and C. K. Wong, "A Conference Key Distribution system", IEEE Trans. on Information Theory, IT-28, pp.714~720, 1982.

[8] K. Koyama and K. Ohta, "Security of Improved Identity-Based Conference Key Distribution system", EUROCRYPT88, pp.11~19, 1988.

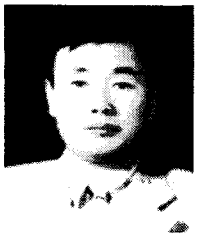
[9] A. Shimbo and S. I. Kawamura, "Cryptanalysis of Several Conference Key Distribution Schemes", Proc. of Asiacrypt91, pp.115~160, 1991.

[10] M. Rhee, Error-Correcting Coding Theory, McGraw-Hill, New York, 1989.

[11] D. Welsh, Codes and Cryptography, Oxford Science Pub., Oxford, 1988.

[12] C. Liu, Introduction to Combinatorial Mathematics, McGraw-Hill, New York, 1968.

[13] A. Menezes, P. Oorchot and S. Vanstone, Handbook of Applied Cryptography, CRC, New York, 1996.



배 용 근

1984년 조선대학교 컴퓨터공학과 졸업(공학사)
1986년 조선대학교 컴퓨터공학과 졸업(공학석사)
2002년 원광대학교 전자공학과 졸업(공학박사)
1988년~현재 조선대학교 컴퓨터공학부 부교수
관심분야 : 전자상거래, 병렬처리, 마이크로 프로세서 응용, 멀티미디어

정 일 용

1983년 한양대학교 공과대학 졸업(공학사)
1987년 City University of New York 전산학과(전산학석사)
1991년 City University of New York 전산학과(전산학박사)
1991년~1994년 한국전자통신연구소 선임연구원
1994년~현재 조선대학교 컴퓨터공학부 부교수
관심분야 : 네트워크 보안, 전자상거래, 분산시스템 관리, 코딩이론, 병렬 알고리즘

교 신 저 자

정 일 용 501-759 광주시 동구 서석동 조선대학교 컴퓨터공학부