

이동단말의 그룹 비밀키 관리를 위한 효율적인 프로토콜

김성열[°], 오명옥, 정일용
울산과학대학 컴퓨터정보학부[°], 조선대학교 전자계산학과

Efficient protocol for group security key management of mobile terminal

Seong-yeol Kim[°], Myung-ok Oh, Il-yong Chung
School of Computer Information, Ulsan College[°]
Dept. of Computer Science, Chosun University

E-mail : kimsy@mail.ulsan-c.ac.kr, sugar@hyun.chosun.ac.kr, iyc@mail.chosun.ac.kr

요약

본 논문에서는 신분확인 프로토콜에 기반을 둔 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 이산대수 문제에 근거하고 있으며 단말기의 저장능력과 처리 능력이 적을 경우도 적절하게 운영될 수 있고, 그룹 내에서 제외하고자 하는 단말기가 동시에 여러 대일 경우에도 적용할 수 있다. 또한 센터가 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계되었다.

1. 서론

컴퓨터를 이용한 원격회의의 증가 및 이동 단말기의 보급 증대와 이동 무선통신의 확대로 인하여 통화 참여자간의 안전한 통신채널의 확보가 필수적으로 요구되고 있다. 일 예로 불법 도청과 침해, 이동통신 시스템에서의 복제 단말을 이용한 통화 도용이나 도청 등이 매년 증가하고 있는 추세이다. 이러한 불법적 사용으로부터 단말기를 보호하기 위하여 인증 절차를 통한 통화 도용을 막고 정당한 단말기를 보호하려는 기술들이 개발되고 있다.

CDMA(Code Division Multiple Access)방식, GSM(Global System for Mobile Communication) 등의 이동 통신 서비스들도 이미 보안 서비스 권고안을 제시하여 현재 사용 중에 있다[1,2]. 또한, 차세대 통신 서비스로 주목받고 있는 IMT-2000에서도 보안 서비스를 표준으로 다루고 있다. 이러한 이동 통신 시스템의 보안 서비스는 단말기 복제 등으로 인한 불법 위조 사용을 방지하기 위한 인증기술, 불법적인 도청으로부터 무선통화 내용을 보호하기 위한 암호기술, 통신 상대방 또는 그룹내의 비밀키 공유를 위한 키관리[3,4,5].

그룹 비밀키를 이용한 암호방식은 센터와 단말기가

사전에 비밀키를 분배하여 특정 그룹 안에서의 통화를 보호하는 방식으로 널리 알려져 있다. 그러나 공유하여 사용되고 있는 그룹 비밀키의 변경이 필요할 경우, 특히 특정 그룹내의 단말기가 키를 분실하여 새로운 그룹 비밀키를 분배하고자 할 때의 기술은 많이 알려져 있지 않다[8].

본 논문에서는 다자간 원격회의 및 디지털 이동통신시스템에서 필수적으로 요구되는 그룹 비밀키 관리를 위한 프로토콜을 제안한다. 제안한 그룹 비밀키 관리를 위한 프로토콜은 센터가 필요에 의해 그룹 비밀키를 갱신하고자 할 때, 단말기가 그룹 비밀키를 분실하였을 때 또는 비밀 정보를 분실하였거나 단말기를 분실하였을 때, 그리고 불법적 의도가 있는 특정 단말기를 보안 서비스에서 제외시키고자 할 때 적용될 수 있도록 설계되었다.

제안 방식은 이산 대수 문제에 근거한 ID 보안 기법을 사용하고 있다. 제안된 프로토콜은 단말기가 유지해야하는 비밀 정보의 양이 적고, 별도의 변경 사항 없이 센터의 필요에 의해 그룹 비밀키를 변경할 수 있으며, 동시에 여러 단말기의 변동 사항을 처리할 수 있다는 점이 특징이다.

본 논문에서 제안한 그룹 비밀키 관리 프로토콜은

디지털 서명을 추가함으로써, 여러 공격들에 대처할 수 있는 이점을 가지고 있고, 송신 정보의 불법적 변경과 불법적 키 갱신에 대한 보호 능력을 가진다.

2. 관련연구

기존의 그룹 비밀키 갱신 방식에는 대칭키 암호 기법을 이용한 방식[6], RSA 공개키 암호법을 활용한 방식[3], Matsuzaki-Anzai(MA)방식[7], Sim-Park-Won(SPW)방식[8]이 있으며, 첫째로 대칭키 암호 기법을 이용한 방식은 특정 그룹 내에 사용되고 있는 비밀키를 새로운 그룹 비밀키로 공유하고자 할 때의 기술로서 키를 분실한 단말기만을 제외하고 모든 그룹 내 단말기에 새로운 공유기를 재분배하는 방식이다. 이 방식은 키를 분배하는 센터는 사전에 분배된 각 단말기의 비밀키를 이용하여 키 분실 단말기를 제외한 모든 단말기에 새로운 그룹 비밀키를 안전하게 전송하는 방식이다. 하지만, 단말기가 키를 분실할 때마다 센터가 그룹 비밀키를 분배해야하기 때문에 많은 회수의 키 분배를 해야 하며, 키 전송에 소요되는 시간이 많이 걸려 정상적인 통신에 방해를 줄 수 있어 비효율적인 방식으로 간주될 수 있다. 둘째, RSA 공개키 암호법을 활용한 방식은 공유기를 분실한 단말기에 한해서만 새로운 키의 공유를 배제하는 방식이다. 이 방식은 그룹 내 모든 단말기에 새로운 그룹 비밀키를 새롭게 보내는 방식에 비해서는 효율적이며 편리하다. 그러나, 한번 새로운 그룹 비밀키가 설정하고 난 후, 새로운 그룹 비밀키를 분배하기 위해서는 처음부터 관련 정보를 다시 전달해야하므로 사실상 처음의 방식에 비해 효율성을 가지지 못한다.

셋째, Matsuzaki-Anzai(MA)방식은 디지털 이동통신 시스템에 적합한 효율적인 그룹 비밀키의 재 공유 방식이다. 이 방식은 기지국이 복수의 단말을 관리하는 스타형 이동체 통신 시스템에 있어서 그룹 내에서 공유 그룹 비밀키를 사용해서 동보 암호 통신을 행하는 경우를 가정하고 있다. 그러나 이 방식은 그룹 비밀키 갱신 시 정상적인 통신을 방해할 수 있으며, 단 1회의 그룹 비밀키 갱신에서만 사용 가능하며, 2대 이상의 단말기를 분실한 경우 2대 이상의 단말기를 그룹으로부터 동시에 제외하고자 할 경우 혹은 2회 이상 연속하여 키를 갱신하고자 할 경우에 적용할 수 없다는 단점이 있다. 넷째, Sim-Park-Won(SPW)방식은 Matsuzaki-Anzai방식을 개선하여 안전하고 효율적인 방식을 제안하였다. 이 방식은 스마트 카드를 이용하여 2회 이상 그룹의 공유키를 연속하여 갱신할

수 있게 하였다. 그러나, 그룹 내에서 제외하고자 하는 단말기가 2대 이상인 경우 적용할 수 없다. 또한, 단말기의 변동 없이 그룹 비밀키를 변경하고자 하는 경우 용이하지 않다는 단점이 있다.

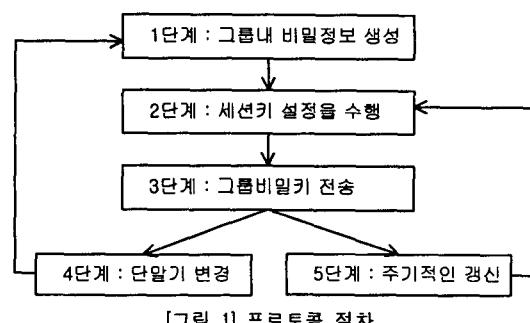
이러한 단점을 보완하기 위하여 본 논문에서는 Okamoto가 제안한 Diffie-Hellman의 키 분배 방식을 변형시킨 ID 기반의 키 분배 방식을 이용하여 그룹 비밀키의 암호화 및 분배에 사용하는 세션키를 생성하였으며, 안전하고 효율적인 그룹 비밀키 분배 및 갱신 프로토콜을 설계하기 위하여 Fiat-Shamir[10]의 ID 기반의 디지털 서명 방식을 사용하였다.

3. 그룹키 분배 및 갱신 프로토콜 설계

3.1 개요

ID 보안 기술[8,9]에 기반을 둔 디지털 서명, 키분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안한다.

제안된 프로토콜의 안전성은 이산대수 어려움에 근거하고 있으며 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있고, 그룹 내에서 제외하고자 하는 통화자가 동시에 여러 명일 경우에도 적용할 수 있다. 또한 통화자의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계하였다. 프로토콜은 [그림 1]과 같은 절차를 거쳐 수행된다.



1단계에서 센터는 본 프로토콜에서 사용되어질 센터와 통화자간의 비밀정보를 생성하여 발급하고, 2단계에서 센터와 통화자사이의 세션키를 생성하여 3단계에서 세션키를 이용하여 그룹 비밀키를 모든 통화자에게 전달하고 통화자는 센터로부터의 정보임을 검증할 수 있으며 센터는 모든 통화자에게 올바르게 그룹 비밀키가 전송되었는지를 검증할 수 있다. 4단계에

서는 통화자가 그룹 비밀키를 분실하였거나 단말기를 분실하였을 때 또는 보안상의 위협사항이 있는 통화자를 그룹에서 제외시키고자 할 때 새로운 그룹 내 비밀정보를 갱신한다. 통화자가 변경되면 2단계에서 세션키 설정을 수행한 후 1단계의 그룹 내 비밀정보를 전송하고 3단계에서 그룹 비밀키를 전송한다. 5단계에서 주기적으로 그룹 비밀키를 갱신하고자 할 때 2단계에서 세션키를 생성하고 4단계에서 세션키를 이용하여 새로운 그룹 비밀키를 전송한다.

3.2 프로토콜 절차

본 논문에서 제안되는 프로토콜은 ID 방식에 기반한 디지털서명 및 키분배 기법을 이용하여 설계되어 이산대수 문제의 어려움에 근거하고 있다. [표 1]은 본 프로토콜에서 사용되는 표기법이다.

<표 1> 프로토콜 표기

표기	의미
f, h	공개된 단방향 함수
ID_i	통화자 i 의 개인식별정보 $i = c, 1, 2, \dots, m$
ID_{cm}	식별정보의 연접(= $ID_c \ ID_1 \ ID_2 \ \dots \ ID_m$) ID_c : Center의 ID ID_1 : 첫 번째 통화자의 ID ID_m : 최종 통화자의 ID
SK	세션키
GK	그룹공유키
I_{ij}	통화자 i 의 공개키
V_i	통화자 i 의 비밀키
S_{ij}	이차임여류의 역수
e	공개키
d	비밀키
g	$GF(p)$ 과 $GF(q)$ 에 포함되는 원시근
R_i	통화자 i 가 발생하는 랜덤수

3.2.1 비밀정보 생성

통화자 i 가 개인식별정보 ID_i 를 키 발급센터에 등록하면 키 발급센터는 다음 절차에 의해 비밀정보를 생성하여 배포한다.

센터는 두 개의 서로 다른 큰 소수 p, q 를 랜덤하게 생성하고 그들을 비밀리에 유지하고, p 와 q 의 곱 $N = p \cdot q$ 를 계산하여 공개한다.

그리고, $\varphi(N) = (p-1)(q-1)$, $\gcd(e, \varphi(N)) = 1$ 과 $ed = 1 \pmod{\varphi(N)}$ 를 만족하는 e, d 를 구한다. 또한, 센터는 $GF(p)$ 과 $GF(q)$ 에 포함되는 원시근 g 를 구하여, 키발급센터는 통화자 i 에 대하여 V_i, S_{ij} 를

다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j), \quad i = c, 1, \dots, k \quad j = 1, 2, \dots, k$$

$$V_i = ID_i^d \pmod{N}, \quad I_{ij}^{-1} = S_{ij}^2 \pmod{N}$$

여기서, I_i 는 $I_i \in QR_N$ 이고, QR_N 은 modulus N 에 대하여 이차 잉여인 집합 전체를 만족해야 한다.

키 발급센터는 최초 등록 통화자 i 에 대하여 물리적 식별을 한 후, 비밀정보 ($N, ID_{cm}, e, g, f, h, V_i, S_{1i}, \dots, S_{ki}$)를 배포해준다. 하지만 최초 등록을 마친 통화자들은 비밀정보를 전달받게 된다.

3.2.2 세션키 설정

센터가 랜덤수 $R_c \in Z_N$ 을 선택하여, $C_c = V_c \cdot g^{R_c} \pmod{N}$ 를 계산해 통화자 i 에게 보낸다. 통화자는 $R_i \in Z_N$ 을 선택하여, $C_i = V_i \cdot g^{R_i} \pmod{N}$ 를 계산하여 센터에게 보내고, $SK = (C_c^e / ID_c)^{R_i} \pmod{N} = g^{e \cdot R_i \cdot R_c} \pmod{N}$ 를 계산한다. 센터도 같은 방법으로 $g^{e \cdot R_i \cdot R_c}$ 를 얻는다.

이런 방법으로 센터와 통화자 i 는 $g^{e \cdot R_i \cdot R_c}$ 를 세션키로 한다.

3.2.3 비밀키 전송

(1) 디지털 서명 및 전송

센터는 그룹 비밀키 GK 를 생성하여 세션키 SK 를 이용하여 모든 통화자들에게 GK 와 다음과 같이 서명 정보를 기록하여 비밀정보를 받은 통화자들에게 전달한다.

센터는 랜덤수 $R_c \in Z_N$ 을 선택하여 다음을 계산한다.

$$X_c = R_c^2 \pmod{N}$$

$$(e_{c1}, \dots, e_{ck}) = h(GK, ID_{cm}, X_c)$$

$$Y_c = R_c \cdot \prod_{e_{cj}=1} S_{cj} \pmod{N}, \quad j = 1, 2, \dots, k$$

센터는 모든 통화자들에게 (GK, X_c, Y_c) 을 동시에 전송한다.

(2) 통화자의 그룹 비밀키 획득

통화자 i 는 센터로부터 전송받은 메시지 (GK, X_c, Y_c) 를 다음과 같이 검증한다.

통화자는 X_c 와 식 $(e_{c1}, \dots, e_{ck}) = h(GK, ID_{cm}, X_c)$ 을 이용하여 (e_{c1}, \dots, e_{ck}) 를 계산하고, ID_c 와 식 $I_{ci} =$

$f(ID_c, j)$, $j = 1, 2, \dots, k$ 을 이용하여 I_{cj} 을 계산한다. 그리고, Z_c 를 다음과 같이 계산한다.

$$Z_c = Y_c^2 \cdot \prod_{e_{cj}=1} I_{cj} \pmod{N}$$

통화자 i 는 $Z_c = X_c$ 이 만족되는지를 점검하여, 만약, $Z_c = X_c$ 이면 그 메시지는 유효한 것으로 간주하고 센터에 의해서 서명되었음을 확인할 수 있다.

그룹 비밀키를 센터가 보낸 것임을 확인한 통화자는 GK 를 채택한다.

(3) 통화자 i 의 서명정보 전송

통화자 i 는 센터로부터 전송받은 메시지 (GK, X_c, Y_c) 를 검증한 후, 랜덤수 $R_i \in Z_N$ 선택하여 다음을 계산한다.

$$X_i = R_c^2 \cdot X_c \pmod{N}, \quad i = 1, 2, \dots, m \quad j = 1, 2, \dots, k$$

$$(e_{il}, \dots, e_{ik}) = h(GK, ID_{cm}, X_i)$$

$$Y_i = Y_c \cdot R_i \cdot \prod_{e_{ij}=1} S_{ij} \pmod{N}$$

이렇게 하여 얻은 $((e_{il}, \dots, e_{ik}), Y_i)$ 를 센터에 전송한다.

(4) 센터의 검증

센터는 통화자 i 로부터 메시지 $((e_{il}, \dots, e_{ik}), Y_i)$ 을 수신하면 다음과 같은 절차에 의해 메시지를 검증한다.

센터는 ID_{cm} 와 식 $I_{ij} = f(ID_i, j)$, $i = 1, 2, \dots, m$ $j = 1, 2, \dots, k$ 를 이용하여 각 통화자에 대한 I_{ij} 를 계산한다. 그리고, Y_i , (e_{il}, \dots, e_{ik}) 및 I_{ij} 로부터 다음과 같이 Z_i 를 계산한다.

$$Z_i = Y_i^2 \cdot \prod_{e_{ij}=1} I_{ij} \pmod{N}$$

센터는 $h(GK, ID_{cm}, Z_i)$ 를 계산하여 다음식이 성립하는지를 점검한다.

$$(e_{il}, \dots, e_{ik}) = h(GK, ID_{cm}, Z_i)$$

만약, $(e_{il}, \dots, e_{ik}) = h(GK, ID_{cm}, Z_i)$ 가 만족하면 그 서명 메시지는 유효한 것으로 간주한다.

이렇게 그룹 비밀키를 이용하여 그룹 내 통화자들 간에 정보를 주고받다가 특정 통화자가 그룹 비밀키를 분실하였거나 단말기를 분실하였을 때 또는 보안상의 위협 사항이 있는 통화자를 그룹에서 제외시키

고자 할 때 새로운 그룹 내 비밀정보를 생성하기 위하여 센터와 통화자들 사이에 새로운 세션키를 생성한 후, 센터는 세션키를 이용하여 비밀정보를 안전하게 전달하게 되고, 새로운 그룹 비밀키를 통화자들에게 전송하여 새로운 그룹 비밀키를 전달받은 통화자들은 그룹 내 통화자들과 서로간의 정보를 주고받을 수 있게 된다.

이러한 분배 방법에 따라 배제 통화자가 여러 명일 경우에도 다른 부하없이 효율적이고 안전하게 새로운 비밀정보를 분배하고 그룹 비밀키를 생성할 수 있다.

4. 결론

본 논문에서는 다자간 원격회의 및 디지털 이동통신시스템에서 안전성을 제공할 목적으로 암호 또는 인증 기능을 제공할 때에 필요한 그룹 비밀키를 이용한 보안 서비스를 위한 그룹 비밀키 관리 프로토콜을 제안하였다. 제안한 방식은 ID 보안 기술에 기반을 둔 디지털 서명, 키 분배 기법을 이용하여 그룹 비밀키 관리를 위한 효율적이고 안전한 방식이다.

본 논문은 보안 위협에 대처하기 위하여 ID 기반의 키 분배 기법과 Fiat-Shamir 디지털 서명 방식에 기초한 안전한 방식을 사용하여 송신 정보의 불법적 변경과 불법적 키 생성에 대한 보호 능력을 가지고 있다. 특히, 디지털 서명을 추가함으로써, 기존의 방식이 여러 공격에 노출되어 있는 것에 비해 공격들에 대처할 수 있는 이점을 가지고 있다. 또한, 키 분배 센터의 디지털 서명 기능을 이용하여 송신하는 정보가 변경되지 않도록 하거나 키 분배 센터로부터 보내진 정보라는 것을 입증할 수 있다.

본 논문은 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있으며, 2회 이상 그룹의 비밀키를 연속하여 생성할 수 있다는 장점을 가지고 있고, 그룹 내에서 제외하고자하는 단말기가 동시에 여러 대일 경우에도 센터가 변동사항을 반영하여 일괄적으로 비밀정보를 생성함으로써 여러 변동사항을 한번에 처리할 수 있다. 또한 단말기의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 생성할 수 있어 효율적인 보안정책 운영이 가능하다.

[참고문헌]

- [1] TIA/EIA Telecommunications Systems Bulletin, Cellular Radio telecommunications Intersystem Operations: Authentication, Signaling Message

- Encryption and Voice Privacy, TSB 51, 1995.
- [2] ETSI-RES, European Telecommunication Standard, ETS 300 175-7, DECT, Common Interface, part 7: Security features, 1992.
- [3] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Th., Vol.22, pp.644-654, 1976.
- [4] M. Tatebayashi, N. Matsuzaki, and D. B. Newman, Jr., "Key distribution Protocol for digital mobile communication systems." Proc. Crypto 1989, pp.324-333, 1990.
- [5] 문태숙, 박상우, 이정숙, 조성준, "디지털 이동통신 시스템에서 스마트 카드를 이용하는 키 분배 프로토콜", 한국통신정보보호학회논문지, 제4권, 제2호, pp.3-16. 1994.
- [6] T. Hwang, "Scheme for Secure Digital Mobile Communications Based on Symmetric Key Cryptography", Information Processing Letters, 48, pp.35-37, 1993.
- [7] N. Matsuzaki and J. Anzai, "A Group Key Renewal Method Suitable for Mobile Telecommunications", Proceedings of SCIS98, 5.2.E. 1998.
- [8] 심주걸, 박춘식, 원동호, "디지털 이동통신시스템에 적합한 그룹 공유키 경신방식", 한국통신정보보호학회논문지, 제10권, 제3호, pp.69-76, 2000.
- [9] 박희운, 이임영, "효율적인 이동통신 그룹키 갱신 방식 제안", 한국정보과학회논문지, 제28권 제1호, pp.832-834, 2001.
- [10] A. Fiat and A. Shamir, "How to prove yourself : Practical Solutions to identification and signature problems." proc. Crypto 1986, pp.186-194, 1986.