ID보안 시스템에 기반한 그룹 비밀키 분배 및 갱신 프로토콜

오명옥[0] 김성열* 정일용
조선대학교 전자계산학과
*울산과학대학 컴퓨터정보학부
omo77[0]@hanmail.net sykim@mina.chosun.ac.kr iyc@mail.chosun.ac.kr

Secret Group Key Distribution and Re-sharing Protocol Based on the Identity Security System.

Myung-ok Oh[0] Seong-yeol Kim Il-ong Chung
Major in Computer Science Education, Chosun University

요 약

본 논문에서는 ID 보안 기술에 기반을 둔 디지털서명, 키분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안한다. 제안된 프로토콜의 안전성은 이산대수 문제에 근거하고 있으며 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있고, 그룹 내에서 제외하고자하는 통화자가 동시에 여러 명일 경우에도 적용할 수 있다. 또한 통화자의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계되었다.

1. 서 론

컴퓨터를 이용한 원격회의의 증가 및 이동 단말기의 보급 증대와 이동 무선통신의 확대로 인한 불법 사용, 복제 단말을 이용한 통화 도용이나 무선 통화의 도청 등이 크게 늘어나고 있다. 이러한 불법 사용에 대한 대책으로 가입자의 인증 절차를 마련하여 불법적인 가입자의 통화 도용을 막고 정당한 가입자를 보호하면서 이동통신 사업자의 손실을 최소화하는 기술이 개발되고 있다[1,2]. 가입자의 단말기 복제 등으로 인한 불법 위조 사용을 방지하기 위한 인증기술, 무선 통화 내용을 불법적인 도청으로부터 보호하기 위한 암호기술 그리고 통화 상대방 또는 그룹내의 비밀키 공유를 위한 키 공유나 분배 기술이 다루어져 왔으며 많은 연구가 이루어지고 있다[3,4,5].

그룹 비밀키를 이용한 암호방식은 센터와 단말기간에 비밀리에 사전에 분배된 그룹 공유 비밀키를 이용하여 모든 정보를 암호화하여 동시에 모든 단말기들에게 전송하여 특정 그룹간의 암호통신을 행하는 방식으로 알려져 있다. 그러나 공유하여 사용되고 있는 그룹 비밀키의 변경이 필요할 경우, 특히 특정 그룹내의 통화자가 키를 분실하여 새로운 그룹 비밀키를 분배하고자 할 때의 기술은 많이 알려져 있지 않다.

본 논문에서는 그룹 비밀키를 이용한 보안 서비스를 위한 분배 및 갱신 방법을 제안한다. 제안한 그룹 비밀키 분배 및 갱신 프로토콜은 센터가 필요에 의해 그룹 비밀키를 갱신하고자 할 때, 통화자가 그룹 비밀키를 분실하였을 때, 비밀 정보를 분실하였거나 단말기를 분실하였을 때 또는 불법적 의도가 있는 특정 통화자를 보안서비스에서 제외시키고자 할 때 적용될 수 있도록 설계하였다.

제안 방식은 이산 대수 문제에 근거한 ID 보안 기법을 사용하고 있다. 제안된 프로토콜은 통화자가 유지해야하는 비밀정보의 양이 적고, 별도의 변경 사항 없이 센터의 필요에 의해 그룹 비밀키를 변경할 수 있으며, 동시에 여러 통화자의 변동 사항을 처리할 수 있다는 점이 특징이다. 또한 디지털 서명 기능을 이용하여 송신 정보의 불법적 변경과 불법적 키 갱신에 대한 보호 능력을 가진다.

본 논문은 2장에서 기존에 제안되어 있는 그룹 비밀키 공유 방식에 대하여 살펴보고 프로토콜 설계에 반영된 기초이론에 대하여 살펴본다. 3장에서는 그룹 비밀키 분배 및 갱신을 위한 프로토콜을 제안한다. 4장에서 결론를 맺는다.

2. 관련연구

특정 그룹 내에 사용되고 있는 비밀키를 새로운 그룹 비밀키로 공유하고자 할 때의 기술은 키를 분실한 이동국만을 제외하고 모든 그룹내 통화자에게 새로운 공유키를 재분배하는 방법, RSA 공개키 암호법을 활용한 방식, 디지털 이동통신 시스템에 적합한 효율적인 그룹 비밀키의 재 공유 방식인 Matsuzaki-Anzai방식[7]이 있다. 그러나 이 방식들은 정상적인 통신을 방해하거나 단 1회의 그룹 비밀키 갱신으로만 사용 가능하며, 2명 이상의 통화자가 단말기를 분실하여 동시에 그룹으로부터 배제하고 싶을 때나 2회 이상 연속하여 키를 갱신하고자 할 경우에 적용할 수 없다는 단점이 있다[6].

또한 [6]는 Matsuzaki-Anzai방식을 개선하여 안전하고 효율적인 방식을 제안하였으나 단말기의 저장능력과 처리의 능력의 부하를 요구하며, 그룹 내에서 제외하고자하는 통화자가 2명 이상인 경우 적용할 수 없으며, 통화자의 변동없이 그룹 비밀키를 변경하고자 하는 경우 용이하지 않다는 단점이 있다.

3. 그룹키 분배 및 갱신 프로토콜 설계

3.1 개요

본 장에서는 ID 보안 기술[8,9]에 기반을 둔 디지털 서

명, 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 다음 절차를 거쳐 수행된다.

1단계 : 그룹내 비밀정보 생성
2단계 : 세션키 설정을 수행
3단계 : 세션키를 이용하여 그룹 비밀키를 전송
4단계 : 통화자가 변경되면 1단계에서 비밀정보를 생성하고 2단계에서 세션키 생성하여 3단계에서 비밀정보와 그룹 비밀키를 전송
5단계 : 주기적인 그룹 비밀키 갱신 수행시 2단계에서 세션키 설정을 수행한 후 3단계에서 그룹 비밀키를 전송
4, 5단계의 이벤트 발생 전까지 그룹 비밀키 유지

<그림 1> 프로토콜 절차

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. 4단계에서는 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 갱신하고자할 때 2단계에서 세션키를 생성하고 4단계에서 세션키를 이용하여 새로운 그룹 비밀키를 전송한다.

3.2 프로토콜 절차

본 논문에서 제안되는 프로콜은 ID 방식에 기반한 디지털 서명 및 키분배 기법을 이용하여 설계되어 이산대수 문제의 어려움에 근거하고 있다. [표 1]는 본 프로토콜에서 사용되는 표기법이다.

3.2.1 비밀정보 생성

통화자 i가 개인식별정보 ID_i를 키 발급센터에 등록하면 키 발급센터는 다음 절차에 의해 비밀정보를 생성하여 배포한다.

센터는 두 개의 서로 다른 큰 소수 p, q를 랜덤하게 생성하고 그들을 비밀리에 유지하고, p와 q의 곱 $N=p\cdot q$를 계산하여 공개한다. 그리고, $\varphi(N)=(p-1)(q-1)$이고, $\gcd(e,\varphi(N))=1$과 $ed=1 \bmod \varphi(N)$를 만족하는 e,d를 구한다. 또한, 센터는 GF(p)와 GF(q)에 포함되는 원시근 g를 구하여, 키발급센터는 통화자 i에 대하여 V_i, S_{ij}를 다음과 같이 계산한다.

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

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

여기서, I_i는 $I_i \in QR_N$ 이고, QR_N은 modulus N에 대하여 이차 잉여인 집합 전체를 만족해야 한다.

키 발급센터는 최초 등록 통화자 i에 대하여 물리적 식별을 한 후, 비밀정보 (N, ID_{cm}, e, g, f, h, V_i, S_{i1}, …, S_{ik})를 배포해준다. 하지만 최초 등록을 마친 통화자들은 비밀정보를 전달받게 된다.

<표 1> 프로토콜 표기

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

3.2.2 세션키 설정

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

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

3.2.3 비밀키 전송

3.2.3.1 디지털 서명 및 전송

센터는 그룹 비밀키 GK를 생성하여 세션키 SK를 이용하여 모든 통화자들에게 GK와 다음과 같이 서명 정보를 기록하여 비밀정보를 받은 통화자들에게 전달한다.

센터는 랜덤수 $R_c \in Z_N$을 선택하여 다음을 계산한다.

$$X_c = R_c^{\,2} \bmod N$$

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

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

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

3.2.3.2 통화자의 그룹 비밀키 획득

통화자 i는 센터로부터 전송받은 메시지 (GK, X_c, Y_c)를

다음과 같이 검증한다.

통화자는 X_c와 식 $(e_{c1}, \cdots, e_{ck}) = h(GK, ID_{cm}, X_c)$을 이용하여 $(e_{c1}, \cdots, e_{ck})$를 계산하고, ID_c와 식 $I_{cj} = f(ID_c, j)$, $j = 1,2,\cdots,k$을 이용하여 I_{cj}을 계산한다. 그리고, Z_c를 다음과 같이 계산한다.

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

통화자 i는 $Z_c = X_c$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 GK를 채택한다.

3.2.3.3 통화자 i의 서명정보 전송

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

$$X_i = R_c^2 \cdot X_c \bmod N, \quad i = 1,2,\cdots,m \quad j = 1,2,\cdots,k$$

$$(e_{i1}, \cdots, e_{ik}) = h(GK, ID_{cm}, X_i)$$

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

이렇게 하여 얻은 $((e_{i1}, \cdots, e_{ik}), Y_i)$을 센터에 전송한다.

3.2.3.4 센터의 검증

센터는 통화자 i로부터 메시지 $((e_{i1}, \cdots, e_{ik}), Y_i)$을 수신하면 다음과 같은 절차에 의해 메시지를 검증한다.

센터는 ID_{cm}와 식 $I_{ij} = f(ID_i, j)$, $i = 1,2,\cdots,m$ $j = 1,2,\cdots,k$를 이용하여 각 통화자에 대한 I_{ij}를 계산한다. 그리고, Y_i, $(e_{i1}, \cdots, e_{ik})$ 및 I_{ij}로부터 다음과 같이 Z_i를 계산한다.

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

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

$$(e_{i1}, \cdots, e_{ik}) = h(GK, ID_{cm}, Z_i)$$

만약, $(e_{i1}, \cdots, e_{ik}) = h(GK, ID_{cm}, Z_i)$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 제외시키고자 할 때 새로운 그룹 내 비밀정보를 갱신하기 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 갱신할 수 있다.

4. 결 론

본 논문에서 제안한 프로토콜은 ID 보안 기술에 기반을 둔 디지털서명[10], 키분배 기법을 이용한 그룹 비밀키의 분배와 갱신을 위한 효율적이고 안전한 방식으로, 센터가 필요에 의해 그룹 비밀키를 갱신하고자 할 때, 통화자가 그룹 비밀키를 분실하였을 때, 비밀 정보를 분실하였거나 단말기를 분실하였을 때 또는 불법적 의도가 있는 특정 통화자를 보안 서비스에서 제외시키고자 할 때 적용될 수 있도록 설계되었다.

보안 위협에 대처하기 위하여 ID를 이용한 키 분배 기법과 Fiat-Shamir 디지털 서명 방식에 기초한 안전한 방식을 사용하여 송신 정보의 불법적 변경과 불법적 키 갱신에 대한 보호 능력을 가지고 있다. 또한 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있으며, 그룹 내에서 제외하고자하는 통화자가 동시에 여러 명일 경우에도 센터가 변동사항을 반영하여 일괄적으로 비밀정보를 생성함으로써 여러 변동사항을 한번에 처리할 수 있다. 또한 통화자의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있다는 점이 특징이다.

참 고 문 헌

[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] 문태욱, 박상우, 이정숙, 조성준. "디지털 이동통신 시스템에서 스마트 카드를 이용하는 키 분배 프로토콜", 한국통신정보보호학회논문지, 제4권, 제2호, pp.3-16. 1994.

[6] 심주걸, 박춘식, 원동호. "디지털 이동통신시스템에 적합한 그룹 공유키 경신방식", 한국통신정보보호학회논문지, 제10권, 제3호, pp.69-76, 2000.

[7] N. Matsuzaki and J. Anzai, "A Group Key Renewal Method Suitable for Mobile Telecommunications", Proceedings of SCIS98, 5.2.E. 1998.

[8] A. Fiat and A. Shamir, "How to prove yourself : Practical Solutions to identification and signature problems." proc. Crypto 1986, pp.186-194, 1986.

[9] 김성열, "ID기반의 디지털 서명 기술을 이용한 이동 에이전트 보안 시스템에 관한 연구", 조선대학교: 이학박사학위논문, 2000.

[10] 강창구, "디지털 다중서명 방식과 응용에 관한 연구", 충남대학교: 공학박사학위논문, 1993.