효율적인 그룹키 분배 및 갱신을 위한 보안 프로토콜의 설계

오 명 옥[†] · 김 성 열[††] · 배 용 근[†††] · 정 일 용[††††]

요 약

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 제외하고자하는 단말기가 동시에 여러 대일 경우에도 적용할 수 있다. 또한 센터가 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계되었다.

The Design of Security Protocol for An Efficient Distribution and Renewal Method of Group Key

Myungok Oh[†] · Seongyeol Kim[††] · Yonggeun Bae[†††] · Ilyong Chung[††††]

ABSTRACT

In this paper, we propose a new distribution and renewal scheme for a group key suitable for secure mobile communications based on identification protocol, in which all members of the group can reshare the new group common key except revoked members by using a key distribution center (a trusted center). The security of this scheme is based on the difficulty of the discrete logarithm problem. The proposed scheme can be appropriately managed in case that terminal's capability of storage and computing power is relatively small and more than one caller are revoked. It also renews a group key easily when the center changes this key intervally for security.

키워드 : 신분확인 프로토콜(Identification Protocol), 그룹키 분배 및 갱신(Distribution and Renewal of Group Key)

1. 서 론

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, 이동 통신 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 사용중에 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 키 공유나 키 분배 기술이 다루어지고 있다[3-5].

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.

본 논문에서는 다자간 원격회의 및 디지털 이동통신시스템에서 필수적으로 요구되는 그룹 비밀키 분배 및 갱신 방법을 제안한다. 제안한 그룹 비밀키 분배 및 갱신 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

† 준 회 원 : 조선대학교 대학원 전자계산학과
†† 정 회 원 : 울산과학대학 컴퓨터정보학부 전임강사
††† 정 회 원 : 조선대학교 컴퓨터공학부 교수
†††† 종신회원 : 조선대학교 컴퓨터공학부 교수
논문접수 : 2001년 12월 20일, 심사완료 : 2002년 5월 2일

단말기의 변동 사항을 처리할 수 있다는 점이 특징이다.

본 논문에서 제안한 그룹 비밀키 갱신 방식은 디지털 서명을 추가함으로써, 기존의 방식이 여러 공격에 노출되어 있는 것에 비해 공격들에 대처할 수 있는 이점을 가지고 있고, 송신 정보의 불법적 변경과 불법적 키 갱신에 대한 보호 능력을 가진다.

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

2. 관련 연구

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]등이 제안되어 있다. 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 공유키를 재분배하는 방식이 있다. 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 공유키를 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 내의 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 가능하고, 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 제외하고자하는 단말기가 2대 이상인 경우 적용할 수 없다. 또한, 단말기의 변동없이 그룹 비밀키를 변경하고자 하는 경우 용이하지 않다는 단점이 있다.

이러한 단점을 보안하기 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 기반 디지털 서명 방식을 사용하였다.

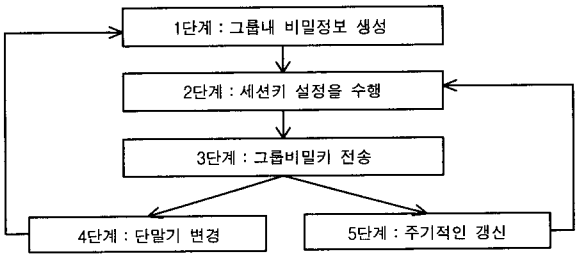
3. 그룹키 분배 및 갱신 프로토콜 설계

3.1 프로토콜 개요

본 장에서는 ID 기반 디지털 서명[11] 및 키 분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적인 프로토콜을 제안하고자 한다.

제안된 프로토콜의 안전성은 Fiat-Shamir의 ID 기반의 디지털 서명과 Diffie-Hellman의 키 분배 방식을 이용하여 이산대수 어려움에 근거하고 있으며 단말기의 저장능력과 처리 능력이 적을 경우도 적절하게 운영될 수 있고, 그룹 내에서 제외시키고자 하는 단말기가 동시에 여러 대일 경우에도 적용할 수 있다. 또한 단말기의 변동 없이 그룹 비밀키를 변경하고자 하는 경우에도 용이하게 키를 갱신할 수 있도록 설계하였다.

본 논문에서 설계된 프로토콜은 (그림 1)과 같은 절차를 거쳐 수행된다.



(그림 1) 프로토콜 절차

1단계에서, 센터는 본 프로토콜에서 사용되어질 센터와 단말기간의 비밀정보를 생성하여 발급한다. 2단계에서는 센터와 단말기사이의 세션키를 생성하고, 3단계에서 세션키를 이용하여 그룹 비밀키를 모든 단말기에 전달하고 단말기는 센터로부터의 정보임을 검증할 수 있으며, 센터는 모든 단말기에 그룹 비밀키가 올바르게 전송되었는지를 검증한다.

4단계에서는 단말기가 그룹 비밀키를 분실하였거나 비밀정보가 내장된 스마트 카드를 분실하였을 경우, 단말기를 분실하였을 경우 또는 악의적인 단말기를 그룹에서 제외시키고자 할 경우에 그룹 내 비밀정보를 새로운 내용으로 갱신한다. 단말기가 변경되면 1단계에서 새로운 그룹 비밀키를 생성하고 2단계에서 세션키 설정을 수행한 후 세션키를 이

용하여 1단계에서 생성한 그룹 내 비밀정보와 3단계에서 생성한 그룹 비밀키를 전송한다. 5단계에서 주기적으로 그룹 비밀키를 갱신하고자할 때 2단계에서 세션키를 설정하고 4단계에서 세션키를 이용하여 새로운 그룹 비밀키를 전송한다.

3.2 프로토콜 설계

본 논문에서 제안되는 프로콜은 ID 방식에 기반한 디지털서명 및 키 분배 기법을 이용하여 설계되었으므로 이산대수 문제의 어려움에 근거하고 있다. <표 1>은 본 프로토콜에서 사용되는 표기법을 나타낸다.

〈표 1〉 프로토콜 표기

표 기	의 미
p, q	512bit이상의 소수
f, h	공개된 단방향 함수
ID_i	단말기 i의 개인식별정보 i=c,1,2,…,m
ID_{cm}	식별정보의 연접($=ID_c \| ID_1 \| ID_2 \| \cdots \| ID_m$) ID_c : Center의 ID ID_1 : 첫 번째 단말기의 ID ID_m : 최종 단말기의 ID
SK	세션키
GK	그룹공유키
I_{ij}	단말기 i의 공개키
V_i	단말기 i의 비밀키
S_{ij}	이차잉여류의 역수
e	공개키
d	비밀키
g	GF(p)와 GF(q)에 포함되는 원시근
R_i	단말기 i가 발생하는 랜덤수

3.2.1 비밀정보 생성

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

① 두 개의 서로 다른 큰 소수 p, q를 랜덤하게 생성하고 그들을 비밀리에 유지한다.

② p와 q의 곱 $N = p \cdot q$를 계산하여 공개한다.
$\varphi(N)=(p-1)(q-1)$이다.

③ $\gcd(e, \varphi(N))=1$과 $ed=1 \bmod \varphi(N)$를 만족하는 e, d를 구한다.

④ GF(p)와 GF(q)에 포함되는 원시근 g를 구한다.

⑤ 키발급센터는 단말기 i에 대하여 V_i, S_{ij}를 다음과 같이 계산한다.

$$I_{ij} = f(ID_i, j), \quad i=c,1,\cdots,k \quad j=1,2,\cdots,k$$
$$V_i = ID_i^{\,d} \bmod N$$
$$I_{ij}^{-1} = S_{ij}^{\,2} \pmod N$$

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

⑥ 키 발급센터는 최초 등록 단말기 i에 대하여 물리적 식별을 한 후, 비밀정보 (N, ID_{cm}, e, g, f, h, V_i, S_{i1}, …, S_{ik})를 배포한다. 이 과정을 통해 최초 등록을 마친 그룹 내 모든 단말기들은 비밀정보를 보유하게 된다.

3.2.2 세션키 설정

Okamoto가 제안한 Diffie-Hellman의 키 분배 방식을 변형시킨 ID 기반의 키 분배 방식을 이용하여 세션키를 생성한다.

① 센터가 랜덤수 $R_c \in Z_N$을 선택하여, $C_c = V_c \cdot g^{R_c} \bmod N$를 계산해 단말기 i에게 보낸다.

② 단말기 i는 $R_i \in Z_N$을 선택하여, $C_i = V_i \cdot g^{R_i} \bmod N$를 계산하여 센터에게 보낸다.

③ 단말기 i는 $SK = (C_c^e / ID_c)^{R_i} \bmod N \equiv g^{e \cdot R_i \cdot R_c} \bmod N$을 계산한다.

〈표 2〉 세션키 생성

$$\begin{aligned} SK &= (C_c^e / ID_c)^{R_i} \bmod N \\ &= (V_c \cdot g^{R_c e \cdot R_i} / ID_c^{R_i}) \bmod N \\ &= (V_c^{e \cdot R_i} \cdot g^{e \cdot R_c \cdot R_i} / ID_c^{R_i}) \bmod N \\ &= (ID_c^{e \cdot d \cdot R_i} \cdot g^{e \cdot R_i \cdot R_c} / ID_c^{R_i}) \bmod N \\ &\equiv g^{e \cdot R_i \cdot R_c} \bmod N \end{aligned}$$

④ 센터도 같은 방법으로 $g^{e \cdot R_i \cdot R_c}$ 를 얻는다.

⑤ 센터와 단말기 i는 $g^{e \cdot R_i \cdot R_c}$ 를 세션키로 한다.
이렇게 만든 세션키를 이용하여 그룹 내 모든 단말기에 그룹 비밀키를 암호화하여 전달한다.

3.2.3 비밀키 전송

a. 디지털 서명 및 전송

센터는 그룹 비밀키 GK를 생성한 다음 세션키 SK를 이용하여 그룹 내 모든 단말기들에 GK와 다음과 같이 서명정보를 기록하여 비밀정보를 전달한다.

① 센터는 랜덤수 $R_c \in Z_N$을 선택하여 다음을 계산한다.

$$X_c = R_c^{\,2} \bmod N$$
$$(e_{c1}, \cdots, e_{ck}) = h(GK, ID_{cm}, X_c)$$
$$Y_c = R_c \cdot \prod_{e_{cj}=1} S_{cj} \pmod N, \quad j=1,2,\cdots,k$$

② 센터는 그룹 내 모든 단말기들에 (GK, X_c, Y_c)를 동시에 전송한다.

b. 단말기의 그룹 비밀키 획득

단말기 i는 센터로부터 전송받은 메시지 (GK, X_c, Y_c)를 다음과 같이 검증한다.

① 단말기는 X_c로부터 (e_{c1}, …, e_{ck})를 계산한다.
$(e_{c1}, \cdots, e_{ck}) = h(GK, ID_{cm}, X_c)$

② 단말기는 ID_c를 이용하여 I_{ci}를 계산한다.

$I_{cj} = f(ID_c, j), \quad j=1,2,\cdots,k$

③ 단말기는 Z_c를 다음과 같이 계산한다.

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

④ 단말기는 $Z_c = X_c$이 만족되는지를 검사한다.

만약, $Z_c = X_c$이면 그 메시지는 유효한 것으로 간주하고 센터에 의해서 서명되었음을 <표 3>에서와 같이 확인할 수 있으며 그룹 비밀키를 센터가 보낸 것임을 확인한 단말기는 GK를 채택한다.

〈표 3〉 서명 검증

$I_{cj}^{-1} = S_{cj}^2 \bmod N, \quad j=1,2,\cdots,k$ 이고,
Z_c는 다음과 같이 X_c가 된다.

$$\begin{aligned} Z_c &= Y_c^2 \cdot \prod_{e_{cj}=1} I_{cj} \pmod N \\ &= (R_c^2 \cdot \prod_{e_{cj}=1} S_{cj}^2) \prod_{e_{cj}=1} I_{cj} \pmod N \\ &= R_c^2 \prod_{e_{cj}=1} S_{cj}^2 I_{cj} \pmod N \\ &= R_c^2 \pmod N \\ &= X_c \end{aligned}$$

c. 단말기 i의 서명정보 전송

단말기는 센터로부터 전송받은 메시지 (GK, X_c, Y_c)를 검증한 후, 다음을 수행한다.

① 단말기 i는 랜덤수 $R_i \in Z_N$ 선택하여 다음을 계산한다.

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

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

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

② 단말기 i는 $((e_{i1}, \cdots, e_{ik}), Y_i)$를 센터에 전송한다.

d. 센터의 검증

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

① 센터는 ID_{cm}으로부터 각 단말기에 대한 I_{ij}를 계산한다.

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

② 센터는 Y_i, $(e_{i1}, \cdots, e_{ik})$ 및 I_{ij}로부터 다음과 같이 Z_i를 계산한다.

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

③ 센터는 $h(GK, ID_{cm}, Z_i)$를 계산하여 다음 식이 성립하는지를 검사한다.

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

만약, $(e_{i1}, \cdots, e_{ik}) = h(GK, ID_{cm}, Z_i)$가 만족하면 그 서명 메시지는 유효한 것으로 간주한다.

그룹 비밀키를 이용하여 그룹 내 단말기들 간에 정보를 주고받다가 특정 단말기가 그룹 비밀키를 분실하였거나 비밀 정보가 내장된 스마트 카드를 분실하였을 경우, 단말기를 분실하였을 경우 또는 보안상의 위협 사항이 있는 단말기를 그룹에서 제외시키고자 할 경우에 그룹 내 비밀정보를 갱신하기 위하여 센터와 단말기들 사이에 새로운 세션키를 생성한 후, 센터는 세션키를 이용하여 비밀정보를 안전하게 전달하게 되고, 새로운 그룹 비밀키를 그룹 내 단말기에 전송한다. 이러한 새로운 그룹 비밀키를 전달받은 단말기들은 그룹 내 단말기들과 서로간의 정보를 주고받을 수 있게 된다. 이러한 분배 방법에 따라 배제 단말기가 여러 대일 경우에도 다른 부하없이 효율적이고 안전하게 새로운 비밀정보를 분배하고 그룹 비밀키를 갱신할 수 있다.

3.3 프로토콜 분석

제안한 논문을 단계별로 공격에 대처할 수 있음을 분석해 보았다[12].

3.3.1 비밀정보 생성단계 분석

비밀정보 생성단계에서 Unknown key share 공격[13]을 막을 수 있다. 이 공격은 공개키 등록과정에서 Center의 부주의로 인해 사용자들간에 동일한 공개키가 존재할 경우 공격이 가능하다. 이는 비밀 정보 생성의 준비단계에서 공개키로 사용되어지는 ID를 각각의 단말기가 모두 서로 다른 ID를 발급 받음으로써 대처할 수 있다.

Subgroup confinement 공격[14]을 막을 수 있다. 이 공격은 잘못된 공개 파라미터의 선택에 의해서 발생하는 공격이다. 이는 비밀 정보 생성단계에서 p, q를 512bit이상의 소수를 선택함으로써 공개 파라미터 N, e, I_{ij}는 안전하며, 안정성이 보장된 단방향 함수 f를 선택함으로써 대처할 수 있다.

3.3.2 세션키 설정단계 분석

Diffie-Hellman의 키 분배 방식을 변형시킨 ID를 이용한 키 분배 방식을 이용하여 세션키를 생성한다. Center는 비밀정보와 그룹 비밀키를 세션키로 암호화하여 모든 단말기들에 전달해준다.

세션키 설정단계에서 무결성, 기밀성, 익명성을 보장할 수 있다. 이는 도청의 가능성으로부터 그룹 비밀키를 비밀로 공유할 수 있고, 센터와 단말기 사이에 세션키를 생성하여 인증 정보를 암호화하여 전송함으로써 가능하다.

Unknown key share 공격을 막을 수 있다. 이는 서명으로 센터와 단말기 사이에 동일한 세션키를 가지고 있는지를 확인함으로써 대처할 수 있다.

3.3.3 그룹 비밀키 전송단계 분석

3단계 그룹 비밀키 전송단계에서는 이산대수 문제에 근거를 둔 Fiat-Shamir의 ID를 이용한 디지털 서명 방식을 이용한 인증과정이다.

그룹 비밀키 전송단계에서는 Impersonation 공격[15]을 막을 수 있다. 이 공격은 공격자가 정당한 사용자인 것처럼 행동하는 공격이다. 이는 키 생성시 전송되는 각 정보에 대한 디지털 서명기법을 사용함으로써 부인봉쇄가 가능하므

로써 대처할 수 있다.

Replay 공격도 막을 수 있다. 이 공격은 공격자가 합법적인 사용자로 위장하여 정당한 사용자와 세션키를 설정하기 위하여 이전 프로토콜에서 사용된 메시지를 재사용하는 공격이다. 이는 이전 프로토콜에 사용한 메시지와는 무관하게 센터가 랜덤수를 이용하여 세션키를 설정함으로써 Replay 공격에 대처할 수 있고, 공격자의 전송정보에 대한 내용변경, 순서변경, 삭제여부 등을 확인하여 메시지의 변경에 의한 공격을 막는다.

Known key 공격[15]을 막을 수도 있다. 이 공격은 키 분배 프로토콜 수행 후의 공격인 기한이 만료되어 공개되거나 부주의로 인해 노출된 이전 세션의 세션키를 이용하여 해당 세션키를 얻어내는 공격이다. 이는 디지털 서명과 그룹 비밀키를 생성할 때 랜덤수를 사용함으로써 공격자가 유효한 전송정보를 생성할 수 없도록 함으로써 이를 막을 수 있다.

Intruder-in-middle 공격[16]을 막을 수 있다. 이 공격은 통신 선로상의 중간에 위치한 공격자가 합법적인 사용자들 사이에 전송되는 정보들을 불법으로 도청·변경하여 전송하여 세션키를 구하는 공격이다. 이는 전송정보에 서명을 이용함으로써 대처할 수 있다.

Oracle session 공격[17]을 막을 수 있다. 이 공격은 공격자 E가 사용자 B에게 자신을 사용자 A로 위장하기 위해 필요한 전송정보를 A로부터 얻어내는 공격이다. 이는 직접적인 인증을 수행하여 대처할 수 있다.

3.3.4 기존 프로토콜과 연산량 및 통신횟수 비교 분석

본 논문은 이동 통신의 일반적인 특징인 소형 경량인 이동 단말기와 계산 능력이 큰 기지국 중심의 센터를 충분히 고려하여 제안하였다.

기존의 방식들은 디지털 서명에 대해 언급하고 있지 않아 디지털 서명에 관련하여 연산을 행하지 않고, 단말기는 그룹 비밀키를 생성하기 위해 연산을 행한다. 하지만, 제안한 방식은 디지털 서명을 추가함으로써, 센터는 비밀정보와 세션키를 생성하기 위하여 연산을 행하고, 단말기는 그룹 비밀키를 생성하기 위한 연산은 하지 않고 세션키를 생성하여 그룹 비밀키를 모든 단말기들에게 전송해주기 위해 세션키를 생성하는 연산을 한다. <표 4>에서는 디지털 서명을 제외시킨 연산량을 계산하였다.

<표 4>에서는 기존의 논문과 통신횟수와 그룹 비밀키 생성시의 연산량을 비교 분석하였다.

〈표 4〉 기존 논문과 통신횟수와 그룹 비밀키 생성시 연산량 비교

분류 / 방식	통신 횟수	그룹 비밀키 생성시 연산량		비 고
		센 터	단말기	
MA방식	1회	Exp(2)	Exp(2)+M(3)	n : 비밀키 갱신 횟수 t : 분실 단말 대수
SPW방식	1회	Exp(2) * n	Exp(2)+M(3)	
PL방식	1회	Exp(2) * n	{Exp(2)+M(3)} * t+M(t-1)	
제안한 방식	2회	Exp(3)+M(3)	Exp(2)+M(1)	

MA방식은 연산량은 적지만 많은 문제점을 가지고 있다. 2대 이상의 단말기를 분실하였을 경우, 2대 이상의 단말기를 그룹으로부터 동시에 제외하고자 할 경우 혹은 2회 이상 연속하여 그룹 비밀키를 갱신하고자 하는 경우에도 적용할 수 없다는 단점을 가지고 있다.

SPW방식은 2회 이상 연속하여 키를 갱신하기 위해 미리 비밀정보들을 연산하여 스마트카드에 저장해두므로 센터의 연산량이 갱신횟수에 비례하여 커진다. 또한, 2회 이상 그룹의 공유키를 연속하여 갱신할 수 있으나, 그룹 내에서 제외하고자하는 단말기가 2대 이상인 경우 적용할 수 없다는 단점을 가지고 있다.

PL방식[9]은 2회 이상 연속하여 키를 갱신할 수 있고, 그룹 내에서 제외하고자 하는 단말기가 2대 이상인 경우 적용이 가능하지만, 단말기에서 수행해야할 연산량이 배제하고자 하는 단말 대수에 비례하므로 비효율적이고, 디지털 서명을 하고 있지 않으므로 제3자에게 공격당할 수 있다는 문제점이 있다.

본 논문에서 제안한 그룹 비밀키 갱신 방식은 디지털 서명을 추가함으로써, 기존의 방식이 여러 공격에 노출되어 있는 것에 비해 공격들에 대처할 수 있는 이점을 가지고 있다. 또한, MA방식과 SPW방식이 가지고 있는 단점을 개선하여, 제외하고자하는 단말기가 여러 대 이상인 경우에도 적용가능하며, 2회 이상 그룹의 공유키를 연속하여 갱신할 수도 있다는 큰 장점을 가지고 있다.

4. 결 론

본 논문에서는 다자간 원격회의 및 디지털 이동통신시스템에서 안전성을 제공할 목적으로 암호 또는 인증 기능을 제공할 때에 필요한 그룹 비밀키를 이용한 보안 서비스를 위한 분배 및 갱신 방법을 제안하였다. 제안한 방식은 ID 보안 기술에 기반을 둔 디지털서명, 키 분배 기법을 이용하여 그룹 비밀키의 분배와 갱신을 위한 효율적이고 안전한 방식이다.

제안 프로토콜은 센터가 필요에 의해 그룹 비밀키를 갱신하고자 할 때, 단말기가 그룹 비밀키를 분실하였을 때, 비밀 정보를 분실하였거나 단말기를 분실하였을 때 또는 불법적 의도가 있는 특정 단말기를 보안 서비스에서 제외시키고자 할 때 그룹 내 새로운 비밀키를 갱신할 수 있도록 설계되었다. 특히, 그룹 내의 특정 단말기를 배제하고자 할 경우, 예를 들면 단말기의 분실로 인한 불법 도청이나 허위의 통신 도용을 방지하기 위하여 키 분배 센터는 가능하면 빠른 시간 내에 그룹 비밀키를 재 공유하여 통신이 가능하도록 하여 기존의 일반 통신에 아무런 영향을 미치지 않아야 하며, 재 공유시간동안 불법 단말기가 새로운 그룹 비밀키를 가지지 못하도록 하여야 한다.

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 갱신에 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 동시 송신하는 정보가 변경되지 않도록 하거나 키 분배 센터로부터 보내진 정보라는 것을 입증하는 효과를 가지고 있다.

본 논문은 통신횟수와 연산량은 기존의 논문에 비해 커다란 이점은 없지만, 단말기의 저장능력과 처리의 능력이 적을 경우도 적절하게 운영될 수 있으며, 2회 이상 그룹의 비밀키를 연속하여 갱신할 수 있다는 장점을 가지고 있다.

또한 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 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 1986, 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] 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.

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

[12] 조동욱, 최연이, 김희도, 원동호. "이동통신환경에 적합한 상호 인증을 제공하는 키 분배 프로토콜의 설계", 한국통신정보보호학회논문지, 제10권 제2호, pp.21-29, 2000.

[13] W. Diffie, P. C. Oorschot, M. J. Wiener, "Authentication and Authenticated Key Exchange," Designs, Codes and Cryptography, 2, pp.107-125, 1992.

[14] C. H. Lim, P. J. Lee, "A Key Recovery Attack on discrete log-based schemes using a prime order subgroup," Advances in Cryptologycypto 97, Springer-verlag, LNCS 1294, pp.249-263, 1977.

[15] 이필중, 임채훈, "일반화된 Diffie-Hellman 키분배 방식의 안전성 분석", 한국정보통신학회논문지 '97-7 Vol.16, No.7, pp.575-597, 1997.

[16] R. L. Rivest, A. Shamir, "How to expose an eavesdropper," Communications of the ACM, 27, pp.393-395, 1984.

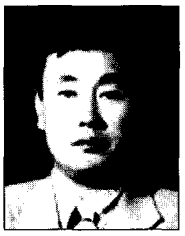
[17] M. Burmester, "On the risk of opening distribution keys," Advances in Cryptology-Crypto '94, Springer-verlag, LNCS 839, 1994.

오 명 옥

e-mail : sugar@hyun.chosun.ac.kr
1999년 조선대학교 전산통계학과 졸업 (학사)
2002년 조선대학교 교육대학원 전자계산 교육전공 졸업(교육학석사)
2002년~현재 조선대학교 대학원 전자계산학과 박사과정
관심분야 : 정보보안, 전자상거래

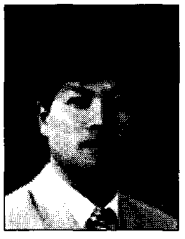
김 성 열

e-mail : kimsy@ulsan-c.ac.kr
1994년 조선대학교 전자계산학과 졸업 (학사)
1996년 조선대학교 대학원 전자계산학과 (이학석사)
2000년 조선대학교 대학원 전자계산학과 (이학박사)
2002년~현재 울산과학대학 컴퓨터정보학부 전임강사
관심분야 : 정보보안, 전자상거래



배 용 근

e-mail : ygbae@chosun.ac.kr
1984년 조선대학교 컴퓨터공학과 졸업 (학사)
1986년 조선대학교 컴퓨터 공학과 졸업 (석사)
1988년~현재 조선대학교 컴퓨터공학부 조교수
관심분야 : 전자상거래, 병렬처리, 마이크로프로세서 응용, 멀티미디어



정 일 용

e-mail : iyc@mail.chosun.ac.kr
1983년 한양대학교 공과대학(학사)
1983년 City University of New York in U.S.A(전산학석사)
1991년 City University of New York in U.S.A(전산학박사)
1991년~1994년 한국전자통신연구소 선임연구원
1994년~현재 조선대학교 컴퓨터공학부 부교수
1997년~1999년 조선대학교 정보과학대학 학장보
1999년~2000년 조선대학교 정보전산원장
관심분야 : 네트워크 보안, 전자상거래, 분산 시스템 관리, 코딩이론, 병렬 알고리즘