Fiat-Shamir 방식을 적용한 디지털 모바일 통신 그룹키 갱신 메카니즘

탁동길* · 정일용*

A Renewal Mechanism of Group Key on Digital Mobile Communication Employing the Fiat-shamir Method

Dong-Kil Tak* · Il-Yong Chung*

요 약

모바일 이동 통신에서 단말기의 분실 또는 단말기의 비밀 정보 유출에 의한 도청이나 통신도용과 같은 경우를 예방하기 위해서 특정 단말기를 배재하고 신속하게 그룹 비밀 키를 갱신할 수 있어야 한다. 본 논문에서 제안된 그룹키 갱신 메카니즘은 Fiat-Shamir 방식을 적용하여 회의장등과 같이 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 오직 사전에 허가된 사용자만이 그룹키를 이용하여 디지털 정보를 얻을 수 있게 한다. 이는 키 갱신을 위해 필요한 비밀 정보가 단말기에 의해서 생성이 되고 상호 통신을 위한 새로운 그룹키가 갱신되므로 단말기의 안전성을 보장할 수 있다.

ABSTRACT

To renew the group key securing on the mobile communication needs that it can be not only re-shared by all members of the group with the exception of members excluded but also prevented from making a fraudulent use of a terminal's registered key because of a leakage of information from the loss of terminal. In this paper, we propose an efficient renewal mechanism of group key in order for all members of the group to be able to get digital information and to perform the renewal of group key in a small-scale conference employing the Fiat-Shamir method. It can guarantee the security of terminals, since a terminal generates security information needed for key renewal, and then renews the group key for mutual communication.

키워드

Group Key, Security, Key distribution, Mobile communication, Fiat-Shamir

* 조선대학교

접수일자 : 2005. 12. 28

Ⅰ. 서 론

모바일 통신의 활용 영역이 다양한 분야로 확대되면서 여러 명의 사용자들에게 동일한 서비스를 제공해주기 위한 그룹 통신에 대한 요구가 증가하고 있다. 따라서 안전한 그룹 통신을 위해 그룹 사용자들에게 전송되는 정보에 대한 여러 가지 그룹 사용자에 대한 보안 요구사항이 만족되어야 한다[1]. 불법 사용에 대한 대책으로 가입자의 인증 절차를 마련하여 불법적인 가입자의 통화 도용을 막고 정당한 가입자를 보호하면서 이동 통신 사업자의 손실을 최소화하는 기술들이 개발되고 있다[2]. 미국의 CDMA(Code Division Multiple Access) 방식이나 유럽의 GSM(Global SYstem for Mobile communication) 등과 같은 이동 통신 표준 방식에서는 이미 인증을 포함함 보안서비스를 권고하여 사용 중이다[8, 9]. 또한 IMT-2000에서도 인증과 암호를 포함한 보안서비스를 표준으로 다루고 있다. 일반적으로 이동 통신 시스템은 그룹 내에 속하는 모든 단말기의 통신을 제어하는 일종의 센터로 구성된 스타형 네트워크를 이루고 있다. 암호 기능을 제공할 경우, 센터와 단말기 간에 비밀리에 사전 분배된 그룹 비밀 키를 이용하여 모든 정보를 암호화하여 동시에 모든 단말기들에 동보 전송하여 특정 그룹 내에서 무선 암호 통신을 수행하고 있다[2]. 그러나 이동 통신에서 신호 교환은 무선 채널을 통해서 대기 중에 수행되므로, 도청이나 그 밖의 신뢰하지 못할 요소들로부터 위조나 불법적인 변경들과 같은 위협들에 대해서는 취약성을 갖고 있다[3].

본 논문의 제안 방식에서는 회의장 등과 같이 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 오직 사전에 허가된 사용자만이 그룹 키를 이용하여 디지털 정보를 얻을 수 있게 하며 사용자가 탈퇴나 새로운 가입 시에 효율적인 키 갱신을 제안한다. 이는 그룹 내의 특정 단말기 또는 불법 단말기를 배제하고자 할 경우, 단말기의 분실 및 단말기의 비밀 정보의 불법적인 유출로 인한 도청이나 통신 도용과 같은 경우를 방지하기 위해서는 센터는 가능한 빨리 도청이나 통신 도용을 감지하고 신속하게 분실 단말기나 비밀 정보 유출 단말기를 제외한 다른 모든 단말기의 그룹 비밀 키를 갱신해야 한다. 이러한 갱신은 일반 통신에 영향을 미치지 않으면서 신속하게 이루어져야 한다. 또한 분실 단말기나 비밀 정보 유출 단말기들이 갱신 시 또는 갱신 이후로는 결코 그룹 비밀 키를 알 수 없게 해야 한다. 본 연구에서는 이러한 조건에 합당하면서 기존 그룹 키 갱신 방법들의 문제점을 해결할 수 있는 효율적인 그룹 비밀 키 갱신 방식을 제안하였다.

본 논문은 5개의 장으로 구분된다. Ⅱ장에서는 기존 연구들에서 제안된 그룹 비밀 키 분배 및 갱신 방식들에 대해서 살펴본다. Ⅲ장에서는 본 연구가 제안하고자하는 그룹 비밀 키 갱신 방식 및 특정 단말기를 배제하고 그룹 비밀 키를 갱신하여 그룹 비밀 키를 재공유하는 절차 및 불법 단말기의 확인을 위한 절차 등을 제안한다. Ⅳ 장에서는 제안 방식의 안전성 분석 및 기존 방식들과 비교 평가 하고 제안 방식의 장점을 분석 기술하였다. Ⅴ장에서 결론을 제시하였다.

Ⅱ. 관련연구

디지털 이동 통신시스템의 특정 그룹 내에서 공유되어 사용되고 있는 비밀 키를 공개된 통신망을 통해 그룹 내의 일부 가입자에 의한 분실 등의 이유로 새로운 그룹 비밀 키를 공유하고자 할 때의 기술은 많이 알려져 있지 않다[11][12]

첫 번째로 고려해볼 수 있는 키를 재분배하는 방식이다. 이러한 방식에는 대칭키 암호화를 이용하는 방식[7]과 비대칭 암호화 기법을 이용하는 방식[8]이 있다. 그러나 이러한 방식은 센터가 많은 회수의 키 분배를 해야 하고 키 전송에 많은 시간이 소요되므로 정상적인 통신을 방해할 수 있고[1, 2], 또한 무선을 기반으로 동보 암호화 통신을 수행하는 하는 디지털 이동 통신 시스템에는 적합하지 않을 수 있다.

다음으로 동보 암호화 통신을 통해 그룹 비밀 키 갱신을 위한 정보를 모든 단말기에 동보 전송하는 방식으로 Matsuzaki-Anzai(MA)방식[4], Sm-Park-Won(SPW)방식[2] 그리고 Park-Lee(PL) 방식[3]이 있다. 이들 방식 중 SPW 방식 및 PL 방식은 스마트 카드를 이용하여 다수의 갱신될 그룹 비밀키 정보와 역수 정보를 은익하여 각 단말기에 배포한다. 그러나 이 방식은 단말기의 경량화가 어려워질 수 있으며 갱신의 횟수가 스마트 카드의 용량에 따라 제한된다. 또한 SPW방식은 사용자간 단합에 의한 그룹 비밀키 유출을 막을 수 없다. 또한 Modular 정보를 미리 제공하기 때문에 2개 이상의 단말기를 동시에 분실 하

였을 때 단말기들이 그룹 비밀키를 생성할 수 있거나, 그들의 단합에 의해 그들 간에 그룹 비밀 키를 공유 할 수 있다[2]. 반면에 PL방식은 Modular 정보는 스마트 카드에 저장하여 배포하지 않고 갱신 시마다 전송함으로써 단합에 의한 그룹 비밀키 생성의 문제및 배제되는 단말기들의 갱신을 위한 정보를 동시에 전송하고 그들의 연산을 통해서 그룹 비밀 키를 생성함으로써 동시 배제의 문제를 해결하였다[3]. 하지만 단말기 경량화의 문제와 갱신의 횟수는 스카트 카드의 용량에 따라 제한되는 문제가 따른다. 그러나 이 방식들은 그룹 비밀 키 갱신을 위해 필요한 통신 횟수가 적고 단말기들이 그룹 비밀 키를 자체적으로 갱신하므로, 디지털 이동 통신 시스템에 적합하다고 할 수 있다.

여기에서 디지털 이동통신 시스템에서 그룹 비밀키 공유 방식 사용을 위해 처음으로 소개된 Matsuzaki-Anzai(MA) 방식을 살펴보면 다음과 같다.

1. Matsuzaki-Anzai(MA) 방식

Matsuzaki-Anzai는 디지털 이동통신 시스템에 적합한 효율적이고 새로운 그룹 비밀키 재 공유 방식을 처음으로 소개하였다[4]. 이 방식은 그룹 비밀 키 갱신 시 사용자의 수에 의존하지 않는 특징을 가지고 있다. 이 방식은 기지국이 복수의 단말기를 관리하는 스타형 이동 통신 시스템에 있어서 그룹 내의 공유 비밀키를 사용해서 동보 암호 통신을 행하는 경우를 말한다. 이 방식은 그룹으로부터 특정 단말기를 배제하고 새로운 그룹 비밀 키를 가능한 빨리 갱신하기 위한 것이다. 먼저 MA 방식 시스템 계수는 [표1]과 같다.

표 1. MA 방식 표기법
Table. 1 Notation of MA method

$T_i\ (1 \le i \le n)$: 각 사용자의 단말기
S_i : 그룹키 갱신을 위한 각 단말기 비밀정보
p, q : 센터가 생성하는 큰 소수
K : 새로 갱신될 그룹 비밀키

1) 준비 단계

① 센터는 $GCD(S_i, S_j) = 1\ (i \ne j)$이 되도록 각 단말기 비밀정보 S_i를 생성하여 비밀리에 보관하고, 각 단말기로 비밀리에 전송한다.

② 센터는 새로 갱신될 그룹 비밀 키 K를 랜덤하게 발생하고 비밀리에 보관한다.

③ 센터는 큰 소수 p, q를 생성한 후, $N = p \times q$를 계산하고 비밀리에 보관한다.

④ 센터는 각 단말기의 비밀 정보를 이용하여 $X_i = K^{S_i}\ (mod\ N)$, $GCD(X_i, N) = 1$을 계산하여 안전하게 보관한 후, 각 단말기 안전하게 전송한다.

⑤ 각 단말기 T_i는 센터로 수신된 S_i, X_i를 비밀리에 보관한다.

2) 그룹 비밀 키 갱신 단계

① 센터가 단말기 T_i를 배제하고자 하는 경우 터미널 T_i와 관련된 정보 (S_i, X_i, N)을 모든 단말기에게 동보 전송한다.

② 단말기 T_j는 수신된 정보를 이용하여 $a \cdot S_i + b \cdot S_j = 1$을 만족하는 a, b 찾는다. 정수 a, b는 확장 유클리드 알고리즘을 이용하여 polynomial time에 계산이 가능하다.

③ 단말기는 다음과 같이 그룹 비밀 키를 갱신한다.

$a < 0$이면, $K = (X_i^{-1})^{-a} \cdot X_j^{\,b} \bmod N$

$b < 0$이면, $K = X_i^{a} \cdot (X_j^{-1})^{-b} \bmod N$

MA 방식은 터미널 T_i의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹 공유키 K를 생성 할 수 없게 된다.

이 방식은 N을 각 단말기가 알게 되는 경우에 단말기들 간의 결탁을 방지 할 수 없다. 즉, 특정 단말기 T_i, T_j가 각각의 비밀 정보 S_i, X_i와 S_j, X_j를 서로 주고 받아 별도의 그룹 비밀 키를 센터의 도움 없이 계산한 후, 모든 다른 단말기들을 배제 할 수 있다[2, 3]. 불법 단말기 T_k가 정당한 단말기 T_i의 비밀 정보 S_i, X_i를 취득하여 불법적인 도청을 하고 있고, 센터가 알게 되었다고 하자. 이 경우 센터는 T_i의 비밀 정보 S_i, X_i를 모든 단말기에 전송함으로써 T_k의 불법적인 도청을 막을 수 있다. 그러나 센터가 또 다른 단말기 T_j를 배제하기 위해서 T_j의 비밀 정보 S_j, X_j를 모든 단말기에 동보전송하게 되면 T_k의 경우 T_i의 비밀 정보를 이용하여 새로운 그룹 비밀 키를 생성

할 수 있다. 이러한 위험에 대처하기 위해서 MA 방식은 RSA 공개키 암호화를 이용한다. 즉 불법 취득한 정보를 이용한 새로운 그룹 비밀 키를 계산하는 어려움은 RSA 안전성에 의존한다[4].

MA 방식은 단 1회의 그룹 공유 비밀 키 갱신만이 가능하다. 2회 이상 연속하여 그룹 비밀 키를 갱신하려면 준비 단계부터 다시 시작해야 한다[2, 3]. 또한 역수 값의 계산이 단말기에서 수행되므로 약간의 계산상의 비효율성이 존재하게 된다[3].

Ⅲ. 새로운 그룹 키 갱신 방식

본 논문에서 제안하는 방식은 디지털 이동 통신 시스템에서 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 키센터에서 관리되는 단말기들 간의 통신의 안전성을 확보하기 위해서 필요한 그룹 비밀 키를 공유하는 방식이다. 본 연구는 그룹 비밀 키 공유 및 분배 방식은 이동 통신의 일반적인 특징인 소형 경량의 이동 단말기와 계산 능력이 큰 키센터를 충분히 고려하였으며, 동보통신을 수행하는 스타형 네트워크를 대상으로 하였다. 키센터를 중심으로 동일한 그룹 내에서 안전한 통신을 하고자하는 경우 먼저 고려해야 할 것은 그룹 내의 비밀 키의 문제이다. 그러나 단말기를 분실하였을 때 이 단말기의 공유 그룹 비밀 키나 비밀 정보를 이용하여 그룹 내의 통신을 쉽게 도청하거나 허위 정보를 유포할 수 있다. 공유 그룹 비밀 키를 이용한 도청이나 허위 정보 유포는 그룹 비밀 키의 갱신을 통해서 예방할 수 있지만, 비밀정보를 이용한 도청이나 허위 정보 유포는 단순한 그룹 비밀 키의 갱신을 통해서 예방하기는 어려운 점이 있다. 특히 동보통신이 이루어지고 있는 상황에서는 더욱 심각하다.

기존 방식들은 특정 단말기 내에 있는 그룹 키를 갱신을 위한 비밀정보를 불법적으로 취득한 불법 사용자를 1회의 그룹 키 갱신을 통해서 배제할 수 있지만, 2회부터는 배제할 수 없다는 문제를 가지고 있다. 따라서 본 연구에서는 이러한 문제점을 해결하고, 소형 경량의 이동 단말기를 위해 스마트카드와 같은 부가적인 장치의 없이 그룹 비밀 키를 갱신할 수 있는 방식을 제안하였다. 제안 방식은 동일한 그룹 내의 가입자가 비밀 키나 비밀 정보를 분실하였을 때, 단말기를 분실하였을 때 또는 키 센터가 불법적인 사용이 의심되는 특정 단말기를 그룹 내의 통신에서 배제하고자 할 때, 그룹 내의 비밀 키를 안전하게 갱신할 수 있는 효율적인 방식이며 최대의 장점은 불법적인 정보에 의한 불법 도청 단말기를 영구적으로 배재할 수 있다는 점이다. 또한 정당하지 않은 센터에 의한 그룹 비밀키 갱신 요청이나 정당하지 않은 사용자의 확인을 위해서 ID기반 디지털 서명 방법을 도입하였다[5][6]. 새로운 그룹키 갱신 방식의 시스템 계수는 [표2]와 같다.

표 2. 제안 그룹 키 갱신 방식 표기법
Table. Notation of a renewal Group key Mechanism

C : 키 분배 센터
$T_i\ (1 \le i \le n)$: 각 사용자의 단말기
GK : 공유 그룹 비밀 키
UK : 새로 갱신될 그룹 비밀 키
$US_i\ (1 \le i \le n)$: 그룹 키 갱신을 위한 각 단말기의 비밀 정보
$UX_i\ (1 \le i \le n)$: 갱신될 그룹 키 은닉한 정보
$ID_i\ (1 \le i \le n)$: 사용자 i 의 ID정보
f, h: 공개된 단 방향 함수
Un: 그룹 키 갱신을 위한 큰 소수
Dn: 디지털 서명을 위한 큰 소수

1. 준비 단계

1) 키 분배 센터

① 키분배 센터(C)는 각 단말기 T_i로부터 식별정보 ID_i를 등록 받은 후 최초 그룹 비밀 키 GK를 랜덤하게 발생한다. 그리고 비밀리에 보관한 후 각 단말기에게 안전하게 배포한다.

② 센터는 커다란 소수 Un을 발생 후, 비밀리 보관한다.

③ $DSc_j\ (1 \le j \le k)$ 를 계산한 후, 안전하게 보관하며 이는 비밀리에 보관하지 않아도 된다.

$DIc_j = f(ID_c, j)$

$DIc_j^{-1} = DSc_j^2 \bmod Dn$

$DIc_j \in QR_{Dn}$,

(QR_{Dn}은 modulus Dn에 대한 이차잉여 집합전체)

④ 그룹 키 갱신을 위한 단말기들의 비밀정보 $US_i\ (1 \le i \le n)$를 발생한 후, 비밀리에 보관하고 각 단말기들에게 안전하게 배포한다.

$GCD(US_i, US_j) = 1, i \neq j$

⑤ 새로 갱신될 그룹 비밀 키 UK를 랜덤하게 발생한 후, 비밀리에 보관한다.

⑥ 그룹 키 갱신을 위한 단말기들의 공개정보 UX_i을 계산한다. 이 단계에서 UX_i는 비밀리에 보관하지 않아도 된다.

$$UX_i = UK^{US_i} \bmod Un$$

⑦ 모든 단말기들에게 다음 정보를 공개적으로 동보전송(broadcasting) 분배

$(Dn, f, h, ID_c, ID_1 \cdots ID_n, UX_1 \cdots UX_n)$

2) 각 단말기

① 센터로부터 수신된 US_i, UX_i와 $Dn, ID_c, ID_i, \cdots ID_n$를 안전하게 보관한다.

② $DSi_j (1 \leq j \leq k)$를 계산한 후, 안전하게 보관한다. 이것은 비밀리에 보관하지 않아도 된다.

$Dh_j = f(IDi, j)$

$Dh_j^{-1} = DSi_j^2 \bmod Dn$

$Dh_j \in QR_{Dn}$,

(QR_{Dn}은 modulus Dn에 대한 이차잉여 집합전체)

2. 그룹 키 갱신 단계

1) 키 분배 센터

① 키 분배 센터가 어떤 사유로 인해 단말기 T_i를 배제하고자 한다.

② 일차 갱신되는 UK 이후, 갱신을 위한 그룹 비밀 키 UK_t를 생성하고 다음 갱신에 사용할 커다란 소수 Un_t을 발생한다.

③ 다음 갱신을 위한 단말기 $T_j (j \neq i)$의 단말기의 정보 UX_j를 은닉한다.

$UX_j = UK^{US_j} \bmod Un_t$

$X_j = US_j^{UK} \cdot UX_j \bmod Un$

④ 서명 정보 X_c, Y_c 생성한다.

ㄱ. 무작위 수 $R_c \in Z_{Dn}$을 생성

ㄴ. $X_c = R_c^2 \bmod Dn$

ㄷ. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

ㄹ. $Y_c = R_c \cdot \prod_{e_{c_j}=1} DSc_j \,(mod)\, Dn$

⑤ 다음 정보를 모든 터미널에 동보 전송 한다.

$(US_i, UX_i, Un, ID_c, ID_1 \| X_1, \cdots \| ID_n \| X_n, X_c, Y_c)$

⑥ 다음의 그룹키 갱신을 위해 정보를 비밀리에 보관한다. $GK = UK, UK = UK_t, Un = Un_t$

2) 각 단말기

① 터미널(T_j)는 아래의 정보를 센터로부터 수신한 후, 정당한 센터로부터 온 정보임을 확인 한다.

$(US_i, UX_i, Un, ID_c, ID_1 \| X_1, \cdots \| ID_n \| X_n, X_c, Y_c)$

ㄱ. $(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$

ㄴ. $DIc_j = f(IDc, j)$

ㄷ. $Z_c = Y_c^2 \cdot \prod_{e_{c_j}=1} DIc_j \,(mod)\, Dn$

ㄹ. $Z_c = X_c$를 만족하는지 검사하여 메시지를 인증한다.

② 그룹 비밀 키를 갱신 한다.

$a \cdot US_i + b \cdot US_j = 1$을 만족하는 a, b 찾는다.

$(a < 0), GK = (UX_i^{-1})^{-a} \cdot UX_j^{\,b} \bmod Un$

$(b < 0), GK = UX_i^{a} \cdot (UX_j^{-1})^{-b} \bmod Un$

③ 다음 그룹 비밀 키 갱신을 위한 단말기의 정보를 갱신한다.

$$\begin{aligned} UX_j &= US_j^{-GK} \cdot X_j \ (mod\ Un) \\ &= US_j^{-GK} \cdot US_j^{GK} \cdot UX_j \ (\bmod Un) \\ &= UX_j \ (mod\ Un) \end{aligned}$$

본 방식은 터미널 T_i의 경우 수신된 정보가 자신의 비밀 키이므로 정확한 a, b를 생성할 수 없게 된다. 즉, 분실 단말기를 불법적으로 취득한 경우는 새로운 그룹 공유키 GK를 생성 할 수 없게 된다. 또한 정당한 그룹 공유키를 생성하지 못한 단말기 T_i는 다음번 그룹 공유키 생성을 위해 필요한 UX_i를 올바르게 생성할 수 없게 되므로, 이후의 그룹 공유키 경신 과정에서 영구히 배제된다. 따라

서 단말기 T_i의 비밀 정보를 취득한 불법 사용자는 영구히 배제된다. 그리고 키 갱신 시마다 새로운 Un값을 배포하고 폐기하므로 단말기들이 서로의 비밀 정보 UX_i와 UX_i를 주고받아 그룹 공유키를 계산한 후 다른 모든 단말기를 배제하는 경우가 없게 된다.

4. 단말기 확인단계

디지털 서명을 이용함으로써 제안 방식은 불법적인 사용을 주기적으로 확인 및 인증하여 임의적으로 배제할 수 있다.

① 키 분배 센터는 서명 정보 X_c, Y_c를 생성 후, 모든 터미널에 동보 전송한다.

② 무작위 수 $R_c \in Z_{Dn}$을 생성한다.

$$X_c = R_c^2 \bmod Dn$$

$$(e_{c_1}, \cdots, e_{c_k}) = h(GK, ID_c \| ID_1 \| \cdots \| ID_n, X_c)$$

$$Y_c = R_c \cdot \prod_{e_{c_j}=1} DSc_j \,(mod)\, Dn$$

③ 각 단말기 T_i은 자신의 서명정보$((e_{i_1}, \cdots, e_{i_K}), Y_i)$를 생성한 후, 센터에게 전송한다.

④ 무작위 수 $R_i \in Z_{N_1}$을 생성한다.

$$X_i = R_i^2 \bmod Dn$$

$$(e_{i_1}, \cdots, e_{i_K}) = h(GK, US_i, ID_c \| ID_1 \| \cdots \| ID_n, X_i)$$

$$Y_i = Y_c \cdot R_i \cdot \prod_{e_{i_j}=1} DSi_j \,(mod)\, Dn$$

⑤ 키 분배 센터 각 단말기 T_i의 서명 정보로부터 정당한 터미널인지를 검사한다.

ㄱ. $DIc_j = f(IDc, j)$

ㄴ. $DIi_j = f(IDi, j)$

ㄷ. $Z_i = Y_i^2 \cdot \prod_{e_{c_j}=1} DIc_j \cdot \prod_{e_{i_j}=1} DIi_j \,(mod)\, Dn$

ㄹ. $(e_{i_1}, \cdots, e_{i_K}) == h(GK, US_i, ID_c \| ID_1 \| \cdots \| ID_n, Z_i)$

를 만족하는지 검사 후 인증한다.

Ⅳ. 제안 방식의 안전성 검토

1. 준비 단계의 안전성

제안 방식에서는 각 단말기가 다른 단말기의 비밀정보를 알아냈거나, 단말기 간의 결탁에 의해 서로의 비밀정보를 알게 될지라도 연산을 위해서 필요한 Un을 알지 못하기 때문에 센터가 그룹 비밀 키 갱신을 위해 Un을 각 단말기에게 전송하기 전까지 각 단말기는 그룹 비밀 키를 알아낼 수 없다. 이것은 이산대수문제를 해결하는 것과 같기 때문이다.

2. 갱신 단계의 안전성

제안한 방식은 키 갱신 단계에서 센터로부터 전송되는 정보는 1회의 갱신을 위해 필요한 배제된 단말기 T_i의 비밀정보 US_i, 은닉 정보 UX_i와 모듈라 연산의 제수 Dn 그리고 다음 번 갱신을 위해 사용될 단말기들의 은닉정보를 은닉한 정보 X_i이다. 먼저, 배제된 단말기는 자신의 비밀 정보 이외에 다른 정보를 알 수 없기 때문에 유클리드 알고리즘에 의한 계산이나 그룹의 새로운 공유키를 계산하는 것은 사실상 불가능하다. 다음으로, 정확한 그룹 비밀 키를 계산하지 못한 단말기는 다음 번 그룹 키 갱신을 위해 필요한 은닉정보 UX_i를 X_i로부터 구할 수 없다. 이것은 이산대수문제에 근거한다.

3. 제안 방식 장점

제안 방식은 그룹 비밀 키의 정당한 갱신이 가능한 단말기만이 다음 번 갱신을 위한 은닉 정보를 알 수 있기 때문에 불법적으로 특정 단말기의 비밀 정보를 취득하여 불법적인 도청을 하는 불법 사용자를 영구히 그룹 내의 통신으로부터 배제할 수 있다. 또한 다음과 같은 장점들이 있다.

첫째, 본 방식 준비 단계 이후 대부분의 정보 전송이 동보통신을 통해서 이루어진다. 둘째, 본 방식은 디지털 서명을 이용함으로써 키센터로 위장한 불법 사용자가 불법적인 키 갱신 정보를 단말기들에게 송신하는 것을 예방할 수 있다. 셋째, 본 방식은 불법적인 사용이 의심되는 사용자를 키센터가 서명을 이용하여 임의적으로 확인하여 배제할 수 있다. 넷째, 본 방식은 스마트카드와 같은 별도의 장치를 사용하여 그룹 키 갱신을 위한 다량의 정보를 미리 분배하는 것이 아니라 단말기가 그룹 키 갱신을 위한 정보를 단말기 내에서 연산을 통해서 갱신 한다. 따라서 소형 경량의 이동 단말기의 특성을 만족한다. 다섯째, 본 방식에서 그룹 키 갱신 시 전달되는 갱신을 위한 정보들은 이산 대수 문제에 의한 안전한 방식을 사용한다. 여섯째, 본 방식은 새로운 그룹 키 갱신 시 별도의 준비 단계를 필요로 하지 않고 연속하여 안전하고 효율적으로 사용 할 수 있으면, 새

로운 단말기가 그룹 내에 진입하는 경우에도 준비과정부터 다시 시작할 필요가 없다. 일곱째, 본 방식은 불법 단말기들이 불법적인 정보로부터 그룹 비밀 키를 계산하는 것을 예방하기위한 추가적인 보호 대책이 필요하지 않다.

V. 결 론

본 제안 방식은 Fiat-Shamir 방식을 적용하여 디지털 서명을 이용함으로써 키센터로 위장한 불법 사용자가 키 갱신 정보를 단말기들에게 송신하는 것을 예방할 수 있으며 이를 이용하여 사용자들을 인증함으로써 불법적인 단말기를 배제할 수 있다. 이는 특정한 공간에서 소규모 그룹회의를 고려한 쉬운 키 생성과 갱신을 위주로 오직 사전에 허가된 사용자만이 그룹키를 이용하여 디지털 정보를 얻을 수 있게 하며 사용자가 탈퇴나 새로운 가입시에 효율적인 키 갱신 메카니즘이다. 또한 그룹 키 갱신을 위해 필요한 비밀 정보가 그룹 키 갱신 시마다 동시에 갱신되므로 단말기의 안전성을 보장할 수 있고 불법 단말기들이 영구적으로 정확한 그룹 비밀 키를 갱신할 수 없게 할 수 있다는 점이다. 이는 그룹 비밀 키 생성을 위한 스마트카드와 같은 부가적인 장치가 필요 없으며 준비단계이후 계속적으로 안전하게 그룹 비밀 키를 갱신하면서 그룹 내의 통신을 수행할 수 있는 효과적인 방식이다.

참고문헌

[1] 박영호, 이경현, "이동 네트워크 환경에서의 그룹키 관리 구조 ", 정보보호학회논문지, Vol.12, No.2. pp. 89-91 , 2002.

[2] 심주걸, 박춘식, 원동호, "디지털 이동통신시스템에 적합한 그룹공유키 경신방식", 한국통신정보보호학회논문지, Vol.10, No.3 pp. 69-76, 2000.

[3] 박희운, 이임영, "효율적인 이동통신 그룹키 갱신 방식 제안", 한국정보과학회논문지, Vol.8, No.1, pp. 367-370, 2001.

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

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

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

[7] T. Hwang, "Scheme for Secure Digital Mobile Communications Based on Symmetric Key Cryptography", Information Processing Letters, Vol.48, pp.35-37, 1993.

[8] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Theory, Vol.22, pp.644-654, 1976.

[9] TIA/EIA Telecommunications Systems Bulletin, Cellular Radio telecommunications Intersystem Operations: Authentication, Signaling Message Encryption and Voice Privacy, TSB 51, 1995.

[10] ETSI-RES, European Telecommunication Standard, ETS 300 175-7, DECT, Common Interface, part 7: Security features, 1992.

[11] 남정현, 이진우, "안전성이 증명 가능한 효율적인 동적 그룹 키 교환 프로토콜" 정보보호 학회 논문지 Vol.14, No,4. pp. 163-165, 2004. 8.

[12] 이덕규, 이임영, "브로드캐스트 암호화에서의 효율적인 키 캥신 방법에 관한 연구" 한국정보보호학회 하계정보보호학술대회 논문집 Vol.13, No.1. pp. 263. 2003

저자소개

탁 동 길(Dong-Kil Tak)

2003년 조선대학교 컴퓨터공학부 박사수료
2000년 1월~2004년 12월 바자울 정보(주) 교육지원실과장
2005년 1월 ~현재 : 도울정보기술(주) 연구원
2003년 3월 ~ 2004년 12월 : 조선대학교 컴퓨터 공학부 겸임교수
2005년 3월~ 현재 : 조선대학교 이공대학 겸임교수
※관심분야 : 네트워크 보안,EC, PKI, PMI,암호학

정 일 용(Il-YongChung)

1983년 한양대학교 공과대학 공학사
1987년 City University of New York 전산학 석사
1991년 City University of New York 전산학 박사
1991년~94년 한국전자통신연구소 선임연구원
1994년~현재 조선대학교 컴퓨터공학부 교수
※관심분야 : 네트워크 보안, 전자상거래, 분산시스템 관리, 코딩이론, 병렬 알고리즘