通信情報保護學會論文誌
第 10 券 第 3 號, 2000. 9

디지털 이동통신 시스템에 적합한 그룹 공유키 경신 방식

심 주 걸*, 박 춘 식**, 원 동 호*

Secret Group Key Re-sharing Method Suitable for Digital Mobile Communication

Joo-geol Sim*, Choon-sik Park**, Dong-ho Won*

요 약

본 논문에서는 그룹의 특정 가입자를 제외한 모든 가입자들이 키 분배 센터를 이용하여 그룹의 공유 키를 갖는 이동 통신 시스템에 적합한 새로운 그룹 공유키 경신 방식을 제안하고자 한다. 제안 방식에서의 그룹 공유키 경신은 준비단계 없이 사전에 분배된 스마트 카드를 이용하여 몇 회라도 계속할 수가 있다. 제안 방식은 또한 배제하고자 하는 특정 가입자를 분류한 후, 전송해야 하는 데이터량이 그룹내의 가입자 수와는 무관하게 일정하므로 가입자가 많은 그룹에 적용 가능하다. 제안 방식의 안전성은 이산대수문제의 어려움에 의존하고 있다.

ABSTRACT

In this paper, we propose a new group key renewal scheme suitable for secure mobile communications, in which all members of the group can re-share the new group common key excepted a revoked member using a key distribution center(a trusted center). A renewal group key in the proposed scheme can be shared many times using pre-distributed data by a smart card without a preparation stage.

This scheme is also available for a large group network, because the transmitted data amount, after identifying the revoked member, does not depend on a size of group. The security of this scheme is based on the difficulty of the discrete logarithm problem.

keyword : *group re-sharing key, mobile communication*

Ⅰ. 서 론

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(authentication) 절차를 마련하여 불법적인 가입자의 통화 도용을 막고 정당한 가입자를 보호하면서 이동 통신 사업자의 손실을 최소화하는 기술들이 개발되고 있다. 미국의 CDMA(Code Division Multiple Access) 방식이나 유럽의 GSM(Global System for Mobile communication) 등과 같은 이동 통신 표준 방식에서는 이미 인증을 포함한 시큐리티 서비스를 권고[1,2]하여 현재 사용 중에 있다.

* 성균관대학교 전기전자컴퓨터공학부 통신정보보호연구실(juwangsan@hanmail.net, dhwon@dosan.skku.ac.kr)
** 한국전자통신연구원 부설 국가보안기술연구소(cspark@etri.re.kr)

또한 차세대 이동 통신인 IMT-2000에서도 인증과 암호를 포함한 시큐리티 서비스를 표준으로 다루고 있다.

디지털 이동 통신 시스템의 대표적인 시큐리티 서비스로 가입자의 단말기 복제 등으로 인한 불법 위조 사용을 방지하기 위한 인증 기술, 무선통화 내용을 불법적인 도청으로부터 보호하기 위한 암호 기술 그리고 통신 상대방 또는 그룹내의 비밀키 공유를 위한 키 공유나 분배 기술이 다루어져 왔으며 많은 연구가 이루어지고 있다.[4,5,6,7,8,9,10]

일반적으로 이동 통신 시스템은 그룹 내에 속하는 모든 단말기의 통신을 제어하는 일종의 센터로 구성된 스타형 네트워크를 이루고 있다. 암호 기능을 제공할 경우, 센터와 단말기간에 비밀리에 사전 분배된 그룹 공유 비밀키를 이용하여 모든 정보를 암호화하여 동시에 모든 단말기들에게 전송하여 특정 그룹간의 암호 통신을 행하고 있다.

그러나 특정 그룹간의 비밀키 공유로 인한 암호 통신 기법은 널리 알려져 왔으나 특정 그룹간에 공유하여 사용되고 있는 비밀키의 변경이 필요할 경우, 특히 특정 그룹내의 가입자가 키를 분실하여 새로운 그룹 공유키를 분배하고자 할 때의 기술은 많이 알려져 있지 않다.

그룹 내의 특정 단말기(이동국)를 배제하고자 할 경우, 예를 들면 단말기의 분실로 인한 불법 도청이나 허위의 통신 도용을 방지하기 위하여 분실 단말기를 배제시키고자 할 경우, 센터는 가능하면 빠른 시간 내에 분실된 단말기를 제외한 다른 단말기들을 위한 새로운 그룹 공유 비밀키를 재 공유하여야 한다. 물론, 이러한 방식은 기존의 일반 통신에 아무런 영향을 미치지 않아야 하며, 분실된 단말기만을 배제한 후, 가장 빠른 시간 내에 이루어져야 하고 재 공유시간 동안에 불법 단말기가 새로운 그룹 공유 비밀키를 가지지 못하도록 하여야 한다.

본 논문에서는 디지털 이동 통신 시스템에서 시큐리티 서비스의 일환으로 제공되고 있는 인증이나 암호 기능을 제공하는 데에 기본적으로 필요한 그룹 비밀키 공유 방식을 제안하였다. 특히, 본 논문에서 제안하는 방식은 동일한 그룹 내의 가입자가 비밀키를 분실하였을 때, 또는 비밀 정보가 내장된 스마트 카드를 분실하였거나 단말기를 분실하였을 때 또는 별도의 사유가 있어 특정 가입자를 그룹에서 암호 통신이나 인증 서비스에서 제외시키고자 할 때 새로운 그룹 내 공유 비밀키를 경신할 수 있는 아주 효율적이며 안전한 방식이다.

본 제안 방식의 큰 장점은 먼저 키 분배 센터가 그룹 공유 비밀키 경신시 동시에 송신해야 하는 정보의 양이 적으며, 이산 대수 문제에 의한 안전한 방식을 사용한 점, 그리고 스마트 카드에 의한 각 가입자별 비밀 정보를 미리 분배하여 새로운 비밀키 경신시 별도의 준비 단계를 필요로 하지 않고 계속하여 안전하고 효율적으로 사용할 수 있는 점이다.

이외에도 필요시 키 분배 센터의 디지털 서명 기능을 이용하여 동시 송신하는 정보가 변경되지 않도록 하거나 키 분배 센터로부터 보내진 정보라는 것을 입증하는 기능은 불법 키 경신에 대한 또 다른 효과이며 특징이다.

본 논문은 모두 5개장으로 구성된다. 먼저 Ⅱ장에서는 기존에 제안되어 있는 디지털 이동 통신 시스템용 그룹 비밀키 공유 방식을 소개하고 Ⅲ장에서는 본 논문에서 제안하고자 하는 그룹 비밀키 공유 방식과 특정 가입자의 비밀키를 분실하였을 때 새로운 그룹 비밀키 공유를 경신하는 방식을 제안한다. Ⅳ장에서는 제안 방식에 대한 안전성을 분석하고 문제점들을 검토한다. 그리고 마지막으로 결론부를 Ⅴ장에 언급하고자 한다.

Ⅱ. 기존 방식 고찰

디지털 이동 통신 시스템의 특정 그룹 내에 공유하여 사용되고 있는 비밀키를 그룹내의 일부 가입자에 의한 분실 등의 사유로 새로운 그룹 비밀키를 공유하고자 할 때의 기술은 많이 알려져 있지 않다.

그러나 간단히 고려해 볼 수 있는 가장 기본적인 방식으로는 키를 분실한 이동국만을 제외하고 모든 그룹내 가입자에게 새로운 공유키를 재분배하는 것이다. 즉, 키를 분배하는 센터는 사전에 분배된 각 가입자의 비밀키를 이용하여 키 분실 가입자를 제외한 모든 가입자에게 새로운 그룹 비밀키를 안전하게 전송하는 방식이다. 그러나 이 방식은 센터가 많은 회수의 키 분배와 키 전송에 소요되는 시간으로 인하여 정상적인 통신에 방해를 줄 수 있기 때문에 비효율적인 방식으로 간주될 수 있다.

또 다른 방식으로는 RSA(Rivest, Shamir, Adleman) 공개키 암호법을 활용한 방식으로 공유키를 분실한 특정 단말에 한해서만 새로운 키의 공유를 배제하는 방식이다.[3] 이 방식은 모든 가입자에게 새로운 그룹 비밀키를 새롭게 보내는 방식에

비해서는 전송 데이터량이 그룹의 크기에 의존하지 않는 방식으로 효율적이며 편리하다. 그러나 한번 새로운 그룹 공유키가 설정되고 나면 다음 그룹 비밀키를 분배하기 위해서는 처음부터 관련 정보를 다시 전달해야 하는 불편함이 있어 사실상 처음의 방식에 비해 커다란 이점을 가지지 못한다.

최근에 Matsuzaki와 Anzai[3]는 디지털 이동통신 시스템에 적합한 효율적이고 새로운 그룹 비밀키 재 공유 방식을 처음으로 소개하였다. 이 방식은 기지국이 복수의 단말을 관리하는 스타형 이동체 통신 시스템에 있어서 그룹 내에서 공유 그룹 비밀키를 사용해서 동보 암호 통신을 행하는 경우를 말한다. 이 경우 그룹으로부터 특정의 단말을 배제하고 새로운 그룹 키를 가능한 빨리 경신하고자 하는 방식이다. 본 방식은 RSA 공개키 암호를 이용하며 안전성도 RSA에 의존하고 있다.

여기서는 Matsuzaki와 Anzai의 방식을 소개한다.

[준비 단계]

키 분배 센터는 $GCD(S_i, S_j)=1$, $i \neq j$인 그룹 내의 모든 단말기의 비밀키 S_i를 발생하여 해당 단말기에 비밀리에 분배하며 모든 단말기의 비밀키는 센터가 직접 보관한다. 센터는 그룹의 공유 비밀키 K를 랜덤하게 발생하고 그리고 2개의 소수 p와 q를 발생하여 $n=p\times q$를 계산하여 둔다. 센터는 K와 n을 안전하게 보관한 후, 발생한 p와 q는 소거한다.

센터는 다시 $GCD(X_i, n)=1$ 이 되는

$$X_i = K^{S_i} \bmod n$$

을 계산하여 해당 단말기에 분배한다. 준비 단계가 완료되면 각 단말기는 S_i와 X_i를 안전하게 저장해 둔다. 여기서 X_i는 비밀로 보관하지 않아도 무방하다.

[키 경신 단계]

1. 키 분배 센터가 분실 신고나 내부 정책에 의하여 키를 분실한 가입자를 인지하였을 경우, 즉 그룹으로부터 키를 분실한 가입자의 단말기 T_i를 배제하고자 할 경우, 그룹내의 모든 단말기에 분실 단말기 T_i의 비밀 정보인 S_i, X_i 그리고 공통 정보인 n을 동시에 전송한다.
2. 그룹내의 각 단말기 j는 센터로부터 수신한 S_i 그리고 자신의 비밀키인 S_j를 이용하여 $a\times S_i + b\times S_j = 1$ 인 a와 b를 계산한다. 여기서 a와 b의 계산은 확장 유클리드 알고리즘에 의하여 $GCD(S_i, S_j)=1$ 인 조건을 이용하여 다항식 시간에 언제나 구할 수 있다.[12]
3. 단말기 j는 자신의 고유 정보인 X_j를 이용하여 단계 2에서 계산된 a의 값이 음수이면 X_i^{-1}을 계산하여 $(X_i^{-1})^{-a}\times X_j^{b} \bmod n = K^{a\times S_i + b\times S_j} \bmod n = K$를, a의 값이 양수이면 X_i^{-1}를 계산하여 $X_i^{a}\times (X_j^{-1})^{-b} \bmod n = K^{a\times S_i + b\times S_j} \bmod n = K$를 계산하면 새로운 그룹 공유 비밀키인 K를 구하게 된다. 여기서 X_i^{-1} 또는 X_j^{-1}의 계산은 확장 유클리드 알고리즘(Euclidean Algorithm)에 의하여 $GCD(X_i, n)=1$ 인 조건을 이용하여 다항식 시간에 언제나 구할 수 있다.

그러나 분실된 단말기 T_i는 센터로부터 수신된 정보가 자신의 비밀키인 S_i이기 때문에 타당한 a와 b를 구할 수 가 없다. 즉, 분실 단말기를 불법으로 취득한 경우는 새로운 그룹 공유 비밀키 K를 공유할 수 없어 그룹내의 암호 통신을 복호화 할 수 없게 된다.

Matsuzaki와 Anzai 방식은 준비 단계에서의 n은 각 단말기내에 Tamper-resistant한 상태로 보관되어야 한다. 즉, 정당한 단말기 이용자라 하더라도 n의 정보를 알 수 없어야 한다. (센터로부터 키 경신시 동보 통신이 되기 전까지는 알 수 없어야 한다) 만일, 그룹내의 특정 가입자(단말기) i와 j가 서로 결탁하여 자신들의 비밀 정보인 S_i와 X_i 그리고 S_j와 X_j를 각각 주고받아 별도의 그룹 공유키를 먼저 계산한 후, 다른 모든 단말기 가입자를 배제하는 경우에는 대처할 수가 없기 때문이다. 즉, 센터의 아무런 도움 없이도 특정 단말기 간에 그룹 비밀키를 간단하게 공유하여 다른 단말기를 배제할 수가 있다. Matsuzaki와 Anzai 방식에서는 그룹 내 가입자간의 결탁에 의한 이러한 공격의 대처 방안으로 n의 비밀 보관과 키 경신시 마다 새로운 n값의 변경을 제안하고 있다.

한편, Matsuzaki와 Anzai 방식에서는 특정 단말기가 분실된 경우 비록 S_i, X_i 그리고 공통 정보인 n이 노출된다 할지라도 RSA의 안전성 때문에 새로운 그룹 공유 비밀키를 계산하기가 어렵다. 즉, 분실된 단말기를 이용하여 새로운 그룹 공유키를 계산하는 어려움은 RSA의 안전성에 의존하게 된다. Matsuzaki와 Anzai 방식은 단 1회의 그룹 공유 비밀키 경신으로만 사용 가능하며 2명 이상의 가입

자가 단말기를 분실하여 동시에 그룹으로부터 배제하고 싶을 때나 2회 이상 연속하여 키 경신을 하고자 할 경우에는 그대로 적용할 수가 없어 완전히 새로운 준비 단계부터 다시 시작하여야 하는 문제점이 있다. 또한, RSA 암호를 사용하므로 계산상 효율이 떨어지며 특히 역수의 값을 계산해야 하므로 다소 효율상의 문제점도 있다.

Ⅲ. 제안 방식

본 논문에서 제안하는 방식은 디지털 이동 통신 시스템의 안전성을 제공할 목적으로 암호 또는 인증 기능을 제공할 때에 필요한 비밀키 공유 방식이다. 특히, 제안 방식은 동일한 그룹 내의 가입자가 비밀키를 분실하였을 때, 비밀 정보가 내장된 스마트 카드를 분실하였거나 단말기를 분실하였을 때 또는 별도의 사유가 있어 특정 가입자를 그룹에서 암호 통신이나 인증 서비스에서 배제시키고자 할 때, 그룹 내 새로운 공유 비밀키를 경신할 수 있는 아주 효율적이며 안전한 방식이다.

본 방식의 큰 장점은 먼저 키 분배 센터가 그룹 공유 비밀키 경신시 동시 송신하는 정보의 양이 적으며 이산 대수 문제에 의한 안전한 방식을 사용한 점과 스마트 카드에 의한 각 가입자별 비밀 정보를 미리 분배하여 새로운 비밀키 경신시 별도의 준비 단계를 필요로 하지 않고 계속하여 안전하고 효율적으로 사용할 수 있는 점이다. 즉, 2회 이상 그룹의 공유 비밀키를 연속하여 경신할 수 있다. 이외에도 필요시 키 분배 센터의 디지털 서명 기능을 이용하여 동시 송신하는 정보가 변경되지 않거나 키 분배 센터로부터 보내어진 정보라는 것을 입증하는 기능은 불법 키 경신에 대한 또 다른 효과이며 특징이다.

제안 방식은 이산대수문제(discrete logarithm problem)에 기인한 방식으로 공통 모듈러에 의한 공격법을 활용하여 공유키를 분실한 특정 단말을 배제하고 다른 모든 가입자에게 그룹 공유키를 재분배하는 방식이다. 처음부터 재분배하고자 하는 회수만큼의 정보를 스마트 카드와 같은 매체를 통하여 각 가입자에게 사전에 분배하여 새로운 공유키를 경신하고자 할 경우에는 처음부터 새롭게 시작하는 것이 아니라 저장된 정보의 인덱스를 이용하여 공유키 경신을 계속할 수 있는 효율적이며 편리한 방식이다.

본 논문에서 제안하는 그룹 비밀키 공유 및 경신 방식은 이동 통신의 일반적인 특징인 소형 경량인 이동 단말기와 계산 능력이 큰 기지국 중심의 센터를 충분히 고려하였으며 또한 센터가 많은 단말기를 관리하면서 동보 통신을 행하는 네트워크를 대상으로 하였다. 센터를 중심으로 동일 그룹 내의 안전한 통신을 하고자 하는 경우 먼저 고려되어야 할 것은 그룹내의 비밀키 문제이다. 그러나 공유된 비밀키의 특정 가입자가 단말기를 분실하였을 때는 이것을 이용한 그룹 내의 통신을 쉽게 도청하거나 허위의 정보를 유포할 수 있다. 제안 방식은 이러한 문제점을 해결하고 기존의 방식을 보다 개선하였다. 제안 방식은 안전한 키 분배 센터의 존재와 스마트 카드가 필요하며 크게 준비 단계와 키 경신 단계로 나누어진다.

[준비 단계]

준비 단계에서 먼저 키 분배 센터가 커다란 소수(prime number)인 $P_j, j=1,\ldots,n$ (소수의 크기와 j의 크기는 시스템 파라메터로 안전성과 효율성을 고려하여 임의로 정할 수 있다), $GCD(T_{ij}, T_{ik})=1$, $T_{ij}\neq T_{ik}$인 T_{ij}, 랜덤한 정수 K_j, Y_{ij} $(=K_j^{T_{ij}} \bmod p_j)$, 그리고 $Y_{ij}^{-1} \bmod P_j$를 모두 발생한 후, 가입자 i별로 해당 정보를 해당 가입자의 스마트 카드에 주입하여 안전하게 배포한다.

이때 키 분배 센터는 $P_j, T_{ij}, Y_{ij}, Y_{ij}^{-1}$를 안전하게 관리하여야 하며 스마트 카드 배포시 해당 가입자(단말기)의 신원을 확인한 후 배포하여야 한다. 스마트 카드 배포는 키 분배 센터가 아닌 영업 창구에서도 수행할 수도 있다.

키 분배 센터로부터 각 단말기에 배포된 스마트 카드 내의 정보는 각 단말기별로 서로 다른 정보를 저장하고 있으며 저장된 정보는 그림 1과 같다. 여기서 그룹 공유 비밀키의 경신 회수는 시스템 파라메터인 n(예를 들면 100회 또는 1000회 등) 에 의해 결정된다.

1(=j)	$P_1, T_{i1}, Y_{i1}, Y_{i1}^{-1}$
2	$P_2, T_{i2}, Y_{i2}, Y_{i2}^{-1}$
3	$P_3, T_{i3}, Y_{i3}, Y_{i3}^{-1}$
4	$P_4, T_{i4}, Y_{i4}, Y_{i4}^{-1}$
5	$P_5, T_{i5}, Y_{i5}, Y_{i5}^{-1}$
..	.....
n	$P_n, T_{in}, Y_{in}, Y_{in}^{-1}$

〔그림 1〕 가입자 스마트 카드 저장 정보형태

스마트 카드내의 저장 정보로는 각 가입자 고유의 비밀 정보 T_{ij}(i=가입자, j= 그룹 비밀 공유키 경신 순번), 그룹 공유 비밀키를 자신의 비밀 정보인 T_{ij}로 암호화한 $Y_{ij}(=K_j{}^{T_{ij}} \bmod P_j)$, 그리고 단말기에서 필요한 값을 사전에 센터에서 계산하여 보내준 결과 값인 $Y_{ij}{}^{-1}$가 있다. 이들 정보는 실제로 새로운 비밀키 경신이 일어날 경우 모두 사용되며 다른 가입자 또는 불법 가입자에게 누설되지 않도록 하여야 한다. 카드가 분실될 경우를 대비하여 카드내의 정보를 암호화하여 두거나, 외부에 노출되지 않도록 물리적인 보호 조치가 이루어져야 한다.

〔키 경신 단계〕

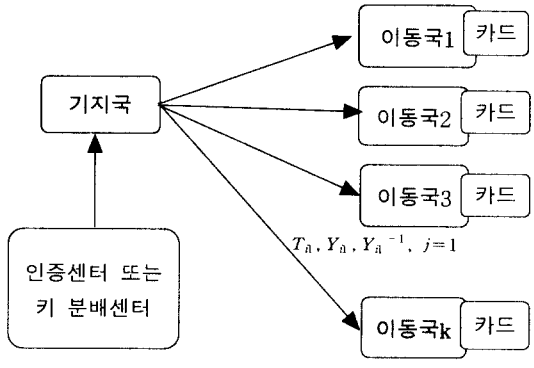
그룹내의 최초의 공유 비밀키는 그룹내의 모든 가입자에게 비밀 정보가 수록된 스마트 카드가 안전하게 배포된 이 후 키 분배 센터로부터 제공받은 카드내의 비밀키가 공유되게 된다. 본 논문에서 제안하는 방식은 최초의 그룹 공유 비밀키의 공유가 완료되어 비밀 통신을 행하고 있는 도중에 그룹내의 특정 가입자가 카드(또는 단말기)를 분실하였거나 또는 다른 특별한 사유로 인하여 특정 가입자를 그룹의 비밀 통신으로부터 배제하여 새로운 그룹 비밀키를 공유하고자 할 경우 적용되는 방식이다.

여기서 각 이동국은 키 분배 센터로부터 스마트 카드를 수령하여 단말기에 장착하여 안전하게 사용중인 것으로 가정한다. 배제 하고자 하는 특정 가입자(이동국)를 i라고 할 때, 가입자 i만을 배제한 상태에서 첫 번째($j=1$) 새로운 그룹 공유 비밀키를 경신하고자 한다. 새로운 그룹 공유 비밀키 공유 절차는 다음과 같다.

1. 키 분배 센터는 그룹내의 공유 비밀키를 경신하기 위하여 배제하고자 하는 특정 가입자의 카드내에 수록된 비밀 정보인 T_{i1}, Y_{i1}, $Y_{i1}{}^{-1}$그리고 P_1을 모든 그룹내의 가입자에게 기지국을 통하여 동보 송신(broadcasting)을 한다.
2. 그룹 내의 각 이동국 j는 키 분배 센터로부터 동보 수신한 정보와 자신의 스마트 카드에 내장되어 있는 자신만의 비밀 정보를 이용하여 그룹내의 새로운 공유 비밀키를 다음과 같이 계산한다.
   ① 이동국 j는 T_{i1}과 T_{j1}을 이용하여 $a\times T_{i1}+b\times T_{j1}=1$ 이 되는 a와 b를 유클리드 알고리즘을 이용하여 계산한다. 계산된 결과인 a와 b는 반드시 어느 한쪽이 음의 정수가 되게 된다.
   ② 만일 $a<0$인 경우는 $(Y_{i1}{}^{-1})^{-a}\times Y_{j1}{}^{b} \bmod P_1 = K_1{}^{T_{i1}\times a}\times K_1{}^{T_{i1}\times b} \bmod P_1 = K_1 \bmod P_1$를 계산하며
   ③ $b<0$인 경우는 $Y_{i1}{}^{a}\times(Y_{j1}{}^{-1})^{-b} \bmod P_1 = K_1{}^{T_{i1}\times a}\times K_1{}^{T_{i1}\times b} \bmod P_1 = K_1 \bmod P_1$을 계산하여 새로운 그룹 공유 비밀키 K_1을 경신하게 된다. 여기서 $Y_{j1}{}^{-1}$은 이미 계산되어 j의 스마트 카드 내에 내장되어 있는 값이므로 별도의 계산이 불필요하다.

그러나 키(카드나 단말)를 분실한 이동국 i는 수신한 정보 T_{i1}이 자신의 비밀 정보인 T_{i1}과 동일하기 때문에 유클리드 알고리즘을 이용하여도 a와 b를 계산할 수 가 없다. 그래서 이동국 i는 그룹내의 새로운 공유 비밀키 K_1을 공유할 수가 없다. 한편, 키를 분실하지 않은 다른 정상적인 가입자는 이동국 j와 마찬가지로 키 분배 센터로부터의 수신 정보, T_{i1}과 자신의 스마트 카드 내에 있는 비밀 정보, T_{j1}을 이용하여 1회 째의 그룹내 공유 비밀키 K_1을 공유할 수가 있다. 제안 그룹 공유키의 경신 방식은 그림 2와 같다.

한편, n회 째의 그룹내 비밀키 공유(단, 키 분실 이동국이 x일 경우)도 상기의 설명과 같이 이루어지나 키 분배 센터에서 보내어져 오는 정보, T_{xn}와 $T_{xn}{}^{-1}$ 그리고 P_n, 각 가입자 카드 내의 비밀 정보, T_{jn}, Y_{jn}와 $Y_{jn}{}^{-1}$을 이용하여 계산한다. 제안 방식은 n회용의 키 공유 관련정보를 스마트 카드에 사전에 보관하고 있기 때문에 준비 단계를 새롭게 수행하지 않고 연속하여 별도의 새로운 그룹 내 공유 비밀키를 경신할 수 있다.



〔그림 2〕 제안 그룹 공유키 경신 방식

제3의 불법자에 의하여 허위의 새로운 공유 비밀키의 경신 정보가 송신되는 것을 방지하기 위하여 키 분배 센터가 보내는 정보 중 T_{xn}의 디지털 서명을 추가하여 전송하면 비밀키 경신시 디지털 서명의 검증을 통하여 정당한 키 분배 센터로부터의 전송 정보임을 확인할 수 있다.

Ⅳ. 제안 방식의 안전성 검토

1. 준비 단계에서의 안전성

준비 단계에서는 어떠한 가입자도 새로운 그룹 공유키를 계산할 수 없어야 한다. 먼저, 키 분배 센터로부터 분배받은 자신의 스마트 카드 내의 P_j, T_{ij}, Y_{ij}, Y_{ij}^{-1} ($j=1,\ldots,n$) 정보를 각 가입자가 알아내었다고 가정해보자. 그러나 각 가입자가 다른 가입자와 결탁하지 않는다면 이들 정보만을 각 가입자가 이용하여 새로운 그룹 공유키 정보인 K_j를 알아낼 수가 없다. 즉, P_j, T_{ij}, Y_{ij}를 이용하여 K_j를 구하는 것은 이산대수문제를 해결하는 것과 같기 때문이다 ($Y_{ij} = K_j^{T_{ij}} \bmod P_j = g^{xT_{ij}} \bmod P_j = h^x \bmod P_j$)

만일, 준비 단계에서 특정 가입자 i와 K가 스마트 카드 내의 정보들을 추출하여 서로 결탁을 행한다면 키 경신 단계에서와 같이 P_j, T_{ij}, Y_{ij}와 P_j, T_{kj}, Y_{kj}정보를 이용하여 동일한 계산 방법으로 새로운 그룹 공유키를 계산할 수가 있다. 그러나 이러한 공격은 가입자들이 안전하게 보관하고 있는 스마트 카드 내의 정보가 쉽게 외부에 노출될 수 있다는 가정 때문이다. 이를 방지하기 위하여서는 카드 내의 정보를 암호화 해 두거나 패스워드 등의 접근 제어 기능을 추가하는 등의 보호 대책과 병행하여 Tamper-resistant 물리적인 보호 조치가 이루어져야 한다.

준비 단계에서 결탁에 의한 공격을 제거하여 보다 높은 안전성을 제공하고자 하는 경우에는 공개 키 P_j의 값을 스마트 카드 내에 저장하여 사전에 배포하는 것을 생략하고 키 경신 단계에서 매번 서로 다른 P_j의 값을 송부하면 된다. 이럴 경우 통신량은 다소 증가되지만 공격자들은 P_j의 값을 사전에 알 수가 없어 결탁에 의한 그룹 공유키 계산이 불가능해지기 때문이다. 물론 준비 단계에서 P_j의 값은 안전하게 보관되어야 한다.

2. 키 경신 단계에서의 안전성

키 경신 단계에서의 안전성은 먼저 배제된 특정 가입자가 기지국을 통하여 키 분배 센터로부터 동보 전송되는 정보를 이용하여 그룹의 새로운 공유 비밀키를 계산할 수 있는지 검토되어야 한다. 본 논문에서 제안된 키 경신 단계에서 키 분배 센터로부터 전송되는 정보는 배제된 특정 가입자의 비밀 정보인 T_{ij}로서 배제된 특정 가입자는 자신의 비밀 정보 외에는 다른 정보를 알 수가 없다. 따라서, 배제된 특정 가입자는 유클리드 알고리즘에 의한 계산이나 그룹의 새로운 공유키 계산을 할 수가 없어 배제된 특정 가입자가 새로운 그룹내의 공유키를 계산하는 것은 사실상 불가능하다.

일반적인 공격 방법으로 가입자 자신의 비밀 정보를 이용하여 다른 가입자의 비밀 정보를 알아내거나 자신의 비밀 정보를 이용하여 그룹 공유키 정보를 알아내는 방법을 생각할 수 있다. 그러나 다른 가입자의 비밀 정보를 알아내는 것은 스마트 카드의 안전성에 의존하게 되며 그리고 자신의 비밀 정보를 이용하여 그룹 공유키를 계산하는 것은 앞에서 설명한 바와 같이 이산대수문제의 어려움과 같게 된다.

Ⅴ. 결 론

본 논문에서는 그룹에서의 특정 가입자를 암호 통신이나 인증 서비스에서 제외시키고자 할 때 새로운 그룹 내 공유 비밀키를 경신할 수 있는 아주 효율적이며 안전한 방식을 제안하였다. 제안 방식은 키 분배 센터가 그룹 공유 비밀키 경신시 전송해야 하는 정보의 양이 적으며, 이산대수문제에 의한 안전한 방식을 사용한 점, 그리고 스마트 카드에 의한 각 가입자별 비밀 정보를 미리 분배하여 새로운 비밀키 경신시 별도의 준비 단계를 필요로 하지 않고 계속하여 안전하고 효율적으로 사용할 수 있는 점이 주요 특징이다. 그러나 그룹 내에서 배제시키고자 하는 특정 가입자가 2명 이상인 경우에는 적용할 수가 없다. 따라서 배제 특정 가입자를 2명 이상인 경우에도 적용 가능한 효율적이고 안전한 방식이 계속 연구될 필요가 있다.

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

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

[5] W.Diffie and M.Hellman, "New Directions in Cryptography", IEEE Trans. Inform. Th., Vol. 22, pp. 644~654, 1976.

[6] M.Tatebayashi, N.Matsuzaki and D.B. Newman, "Key Distribution Protocol for Digital Mobile Communication Systems, Advances in Cryptology", Proceedings of Crypto89, pp. 324~334, 1989.

[7] M.J.Beller, L.Chang, and Y.Yacobi, "Privacy and Authentication on a Portable Communications System", IEEE Global Telecommunications Conference, pp. 1922~1927, 1988.

[8] C.S.Park, K.Kaoru, T.Okamoto and S.Tsujii, "On Key Distribution and Authentication in Mobile Radio Networks, Advances in Cryptology", Proceedings of Eurocrypt93, pp. 461~465, 1993.

[9] T.Hwang, "Scheme for Secure Digital Mobile Communications based on Symmetric Key Cryptography", Information Processing Letters, 48, pp. 35~37, 1993.

[10] W. Adams a nd L.Goldstein, "Introduction to Number Theory", Prentice-Hall, 1976.

〈著者紹介〉

심 주 걸 (Joo-geol Sim) 종신회원
1979년 : 중앙대학교 전자공학과 졸업
1991년 : 건국대학교 전자공학과 석사
1997년3월~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 박사과정
1996년~현재 한국정보보호센터 기술전문위원
〈관심분야〉 정보보안정책, 암호이론

박 춘 식 (Choon-sik Park) 종신회원
광운대학교 전자통신공학과 졸업(학사)
한양대학교 대학원 전자통신공학과 (석사)
일본 동경공업대학 전기전자공학과 졸업 (암호학전공, 공학박사)
1989년 10월~1990년 9월 일본 동경공업대학 객원 연구원
1989년~현재 한국전자통신연구원 부설 국가보안기술연구소 책임연구원, 기반기술연구부장
1999년~현재 한국통신정보보호학회 국제협력이사, 종신회원
〈관심분야〉 암호이론, 이동통신보안

원 동 호 (Dong-ho Won) 종신회원
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학과 박사
1978년 4월~1980년 3월 한국전자통신연구원 연구원
1985년 9월~1986년 8월 일본 동경공대 객원연구원
1982년~현재 성균관대학교 전기전자 및 컴퓨터공학부 정교수
1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부장
〈관심분야〉 암호이론, 정보이론