효율적인 이동통신 그룹키 갱신 방식 제안

박희운°, 이임영
순천향대학교 정보기술공학부
hceun@cse.sch.ac.kr, imylee@sch.ac.kr

A Efficient Mobile Communication Group Key Reforming Method

Hee-Un Park° Im-Yeong Lee
Division of Information Technology Engineering Soonchunhyang University

요 약

무선 이동 통신 시스템의 발전으로 인해 사회의 전반적인 모습들 역시 새로운 형태로 변화하고 있다. 그러나 이러한 변화는 무선 단말기의 불법 사용 또는 제 3자에 의한 불법적 도청으로 인해 취약성이 존재할 수밖에 없다. 현재 이를 해결하기 위한 방법으로서 암호학적 해결책들이 제시되고 있다. 이에 대해 본 고에서는 특정 그룹을 대상으로 무선 이동 통신에서 적용 가능한 기존의 그룹 키 갱신 방법을 알아보고, 이들의 문제점을 고찰한다. 동시에 기존의 방식에서 발생되는 문제점을 해결할 수 있는 안전하면서 효율적인 이동 통신 그룹 키 갱신 방식을 제안한다.

1. 서론

정보 사회의 발전을 통해 인간 문명 전반에 획기적인 변환의 시대가 도래하고 있다. 현대 사회의 정보화 현상은 산업 구조 및 사회 일반에 광범위한 컴퓨터의 보급 확산과 통신 서비스의 발전을 통해 확대되고 있다.

이 중에서 이동 통신 분야는 IT(Internet Technology) 산업계에서 가장 빨리 성장하는 분야 중에 하나로서, 많은 사람들이 이동 통신 서비스를 통해 그 편리성과 유용성을 인지하고 있다.

이러한 이동 통신 발전의 이면에는 사용자들의 다양한 서비스가 요구되고 있다. 즉, 단순한 의사 교환의 범위를 넘어서 동영상 그리고 이들을 포함해 그룹을 대상으로 하는 인터넷 서비스까지 포괄적으로 확대되고 있다.

그러나 무선 이동 통신상에서 제공되어질 이와 같은 그룹 서비스들은 많은 문제점에 노출될 수 있다. 이동 통신에서의 신호 교환은 무선 채널을 통해 대기 중에서 수행되므로, 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 동시에 무선 단말기의 분실 등은 그룹 소속원들의 공유 정보의 노출뿐 아니라 불법적 시스템 사용 등을 야기시키므로 특히 주의해야 할 사항이다. 따라서 그룹에 가입된 사용자를 제외한 다른 불법적 사용자들로부터 기밀성과 안전성을 확보하기 위해 암호 시스템의 연구가 활발히 진행되고 있다.

그러나 무선 통신 상에서 사용되는 암호 기법들을 고려해보면, 특정 그룹간의 비밀키 공유로 인한 암호 통신 기법은 널리 알려져 왔으나, 그룹 키의 분실 및 유용으로 인한 변경 및 갱신에 대해서는 연구가 미흡한 실정이다.

본 고에서는 특정 그룹을 대상으로 무선 이동 통신 시스템 상에서 적용 가능한 기존의 그룹 키 갱신 방법을 살펴보고, 이들의 문제점을 고찰한다. 또한 제시된 기존 방식들의 문제점을 해결할 수 있는 안전하면서 효율적인 이동 통신 그룹 키 갱신 방식을 제안한다.

2. 기존 방식 연구

무선 이동 통신 상의 그룹 서비스를 위해 현재 다양한 암호 방식들이 연구되고 있다. 그룹의 특성상 키 갱신을 위해서는 센터와 그를 중심으로 하는 성형 네트워크를 기본 조건으로 가정한다. 다음은 기존의 무선 이동 통신 그룹 키 갱신 방식들을 기술한 것이다.

2.1 대칭키 암호 기법 이용 방식

각 사용자 i(i = {0, 1, ..., n})는 그들의 비밀키 K_i를 가지고 있으며, 그룹 키 생성 및 분배를 담당하는 센터 C는 모든 사용자의 비밀키들을 비밀리에 보관한다. 단말기 분실이 발생할 경우, 센터는 사용자 U_i를 제외하고 각 사용자들을 위한 새로운 그룹 키 K_{G_NEW}를 자신이 보유하고 있는 각 사용자의 비밀키를 사용해 개별적으로 암호화 및 분배한다[1].

단, 이때 폐지된 사용자 U_i를 식별한 다음 새로운 그룹 키 K_{G_NEW}를 암호화하고 분배하는데 n-1번 정도의 시간을 필요로 하게된다. 만약 센터가 많은 수의 사용자들

을 관리하는 경우, 키 갱신을 위한 데이터 전송에 많은 시간이 요구되기 때문에 정상적인 통신을 방해할 수 있다는 문제점을 갖는다.

2.2 비대칭 암호 기법 이용 방식

이 방식은 기본적으로 공개키를 전제로 하고 있기 때문에 다음과 같은 과정을 통해 그룹 키 갱신이 수행되어진다[2].

1) 각 사용자 i(i={1,2, ..., n})는 자신의 공개키 e_i 및 개인키 d_i를 다음과 같이 생성한 다음, e_i를 공개한다.

$e_i * d_i = 1 \bmod (p-1)$ (단, p는 큰 소수)

2) 센터는 다음의 정보를 생성하여 안전하게 저장한다.

$Y_i = g^{e_i} \bmod p$

3) 키 갱신이 필요할 경우 센터는 랜덤 값 R을 생성하여 사용자 U_i를 제외한 모든 사용자에게 다음을 전송한다.

$Z_j = Y_j^R \bmod p$ (단, $j \neq i$, $j=\{1,2, ..., n\}$)

4) 새로운 그룹 키 K_{G_NEW}는 다음과 같은 과정을 통해 갱신된다.

$K_{G\_NEW} = Z_i^{dj} \bmod p = (Y_j^R)^{aj} = g^{ej*dj*R} = g^R \bmod p$

센터가 각 사용자의 비밀키를 알지 못하기 때문에 보안 측면에서 이 방법이 바람직할 것이다. 그러나 센터는 새로운 그룹 키를 암호화하고 분배하는데 (n-1)번 정도의 시간이 필요하다는 단점이 있다.

2.3 Matsuzaki-Anzai(MA) 방식

본 방식은 상기 방식들과는 달리 그룹 키 갱신시 가입된 사용자의 수에 의존하지 않는다는 특징을 가지고 있다[3]. 다음은 본 방식의 프로토콜을 간결하게 기술한 것이다.

1) 시스템 계수

본 방식에서 사용되는 시스템 계수는 다음과 같다.

- T_i : 각 사용자의 터미널 ($i=\{1, 2, ..., n\}$)
- s_i : 각 사용자 i의 비밀키
  : $i \neq j$일 경우 $GCD(s_i, s_j) = 1$
  : 센터는 모든 사용자의 비밀키를 보관한다.
- p, q : 센터가 생성하는 큰 소수
- K : 새로 갱신될 그룹 키

2) 준비 단계(Preparation phase)

가) 센터

- $GCD(s_i, s_j) = 1$, $i \neq j$가 되도록 각 사용자의 비밀키 s_i를 생성하고, 각 사용자의 터미널로 안전하게 전송 및 저장한다.
- 랜덤하게 새로운 그룹 키 K를 생성한다.
- 큰 소수 p, q를 생성한 다음, $n = p * q$를 계산한다.
  : 센터는 안전하게 s_i, K 및 n을 보관한다.
- 센터는 각 사용자의 비밀키를 이용하여 다음을 계산한 다음, 모든 T_i에게 분배한다.

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

: X_i의 역수가 존재함을 보증하고, 분배된 X_i를 이용하여 modular n을 인수 분해 하지 못하게 하기 위해 modular n은 다음의 조건을 만족한다.

$gcd(X_i, n) = 1$

나) 각 사용자

- 각 사용자는 센터로부터 수신된 X_i를 자신의 터미널에 저장한다.

3) 키 갱신 단계

가) 센터

- 터미널의 분실 또는 정책에 의해, 센터에서 터미널 T_i를 폐지해야 할 경우, 다음과 같이 터미널 T_i와 관련된 정보를 모든 사용자에게 보내야 한다.
  : $(s_i, X_i(= K^{si} \bmod n), n(= p * q))$

나) 각 사용자

T_i를 제외한 모든 사용자들은 수신된 정보를 이용하여 다음과 같은 과정을 수행한다.

- 1 단계
  : T_i는 $a * s_i + b * s_j = 1$을 만족하는 a, b를 계산한다. (단, s_i와 s_j는 공통 제수를 가지고 있지 않음)
  : 터미널 T_i는 정수 a와 b를 확장된 유클리드 알고리즘을 이용하여 polynomial time안에 계산가능하다.
- 2 단계
  : $a < 0$일 때, 터미널 T_i는 다음을 계산한다.

$(X_i^{-1})^{-a} * X_j^b \bmod n$
$= K^{a*si+b*sj} \bmod n = K$ (X_i, n, X_j를 이용)

  : $b < 0$ 이면,

$X_i^a * (X_j^{-1})^{-b} \bmod n$
$= K^{a*si+b*sj} \bmod n = K$ (X_i, n, X_j를 이용)

본 방식은 터미널 T_i에 대해서 수신된 정보가 자신의 비밀키이므로 합당한 a와 b를 생성할 수 없게 된다. 따라서 터미널을 불법적으로 취득하거나 기존의 그룹 키를 안다 하더라도, 새로운 그룹 키 K를 얻을 수 없다는 특징을 가지고 있다. 그러나, 본 방식은 2회 연속 그룹 키 갱신을 수행할 경우 새로이 준비 단계를 수행해야하며, 역수 값 계산이 사용자 단말에서 수행되므로 계산상 비효율적이라는 문제점을 드러내고 있다.

2.4 Sim-Park-Won(SPW)방식

상기 방식의 문제점을 개선하기 위해 SPW 방식이 제안되었다[4]. 이 방식은 준비 단계의 문제점을 개선하기 위해 스마트 카드를 이용하여 다수의 그룹 키 정보와 역수 정보를 은닉해 사용자에게 제공하고 있다. 그러나 modular 정보를 미리 제공함으로서 2개 이상의 단말기를 동시에 분실하거나, 사용자들의 단합에 의한 그룹 키 유출을 방지 못하는 특징을 가지고 있다.

3. 새로운 방식 제안

본 장에서는 상기 두 방식-MA 및 SPW-의 문제점을 해결하는 새로운 그룹 키 갱신 방식을 제안한다.

3.1 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

- P_j : 센터가 생성하는 큰 소수(j는 키 갱신 순번)
- K_j : 그룹 키 생성 정보
- T_i : 각 사용자의 터미널 (i={1, 2, ..., n})
- Y_{ij}, Y_{ij}^{-1}: 그룹 키 은닉 정보 및 역수
- S_{ij} : 사용자 i의 비밀키

3.2 프로토콜

1) System setup 및 준비 단계

가) 센터

- 큰 소수 P_j(j={1, ..., m})를 생성하여 안전하게 저장하고, 다음과 같이 사용자 비밀키 정보를 계산한다.
  $GCD(S_{ij}, S_{ik}) = 1$ (단, $S_{ij} \neq S_{ik}$)
- 그룹 키 생성 정보 K_j를 생성하고, 그룹 키 은닉 정보 및 역수를 계산한다.
  $Y_{ij} = K_j^{Sij} \bmod P_j$, Y_{ij}^{-1}
  : 이를 통해 사용자는 별도의 역수 계산이 필요없게 되므로 계산상 효율성을 얻을 수 있다.
- 센터는 해당 사용자 i에게 (S_{i1}, Y_{i1}, Y_{i1}^{-1}, ..., S_{im}, Y_{im}, Y_{im}^{-1})을 스마트 카드에 저장하여 안전하게 전송한다.

2) 키 갱신 단계

본 과정에서는 2명의 사용자가 각각 단말기 T_i 및 T_j'를 분실한 것으로 가정하고 기술한다.

가) 센터

- 폐지 대상 단말기들을 확인하고 기지국을 통하여 스마트 카드 정보를 모든 사용자에게 동보 전송한다.
  : (P_1, S_{i1}, Y_{i1}, Y_{i1}^{-1}), (P_2, S_{i2}', Y_{i2}', $Y_{i2}'^{-1}$)
  이때, 키 갱신시 P_j를 제공함으로서 사용자 단말에 대한 그룹 키 유출을 막을 수 있다.

나) 각 사용자

- 1 단계
  : 사용자 e는 수신된 정보를 이용하여 다음을 만족하는 a_t, b_t(t∈{1, 2})를 계산한다.
  $a_1 * S_{i1} + b_1 * S_{e1} = 1$
  $a_2 * S_{i2}' + b_2 * S_{e2} = 1$
- 2 단계
  : $a_t < 0$일 때, 터미널 j는 다음을 계산한다.
  $(Y_{i1}^{-1})^{-a1} * Y_{e1}^{b1} \bmod P_1$
  $= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$
  $(Y_{i2}'^{-1})^{-a2} * Y_{e2}^{b2} \bmod P_2$
  $= K_2^{a2*Si2'+b2*Se2} \bmod P_2 = K_2$
  : $b_t < 0$ 이면, 터미널 j는 다음을 계산한다.
  $Y_{i1}^{a1} * (Y_{e1}^{-1})^{-b1} \bmod P_1$
  $= K_1^{a1*Si1+b1*Se1} \bmod P_1 = K_1$
  $Y_{i2}'^{a2} * (Y_{e2}^{-1})^{-b2} \bmod P_2$
  $= K_2^{a2*Si2'+b2*Se2} \bmod P_2 = K_2$
- 3 단계
  : 각 사용자는 계산된 정보를 통해 새로운 그룹 키 K를 갱신한다.

$$K = \left(\prod_{i=1}^{t} K_i\right) \bmod n$$

4. 각 방식별 비교 분석

기존의 대칭/비대칭 암호 기법의 경우 효율성 및 단합에 의한 부정을 극복하지 못하였으며, MA 방식은 준비 단계 및 2명 이상의 터미널이 분실시 비효율성을 낳고 있다. 동시에 SPW 방식은 사용자간 단합 및 2명 이상의 터미널 분실에 대한 대책이 미비하였다. 다음은 기존 방식들에 대해 제안 방식의 특징을 표로 기술한 것이다.

<표 1> 각 방식별 비교 분석 결과

항목 \ 방식	대칭키 방식	공개키 방식	MA 방식	SPW 방식	제안 방식
통신 병목현상해결	X	X	O	O	O
키 갱신 준비 단계 overhead 해결	X	X	X	O	O
사용자간 단합 해결	X	X	O	X	O
2명 이상의 키 갱신 해결	O	O	X	X	O

5. 결론

이동 통신 분야의 고속 성장은 음성 서비스의 차원을 넘어서 그룹을 대상으로 하는 인터넷 서비스까지 포괄적으로 적용되고 있다. 그러나 무선 이동 통신상에서 그룹 서비스를 지원할 경우, 보안적 위협에 대해서 취약성을 지니고 있으며, 그룹 키의 분실 및 유용으로 인한 변경 및 갱신에 대해서는 연구가 미흡한 실정이다.

본 고에서는 기존의 그룹 키 갱신 방법을 살펴보고, 이들의 문제점을 고찰하였다. 동시에 제시된 기존 방식들의 문제점을 해결할 수 있는 안전하면서 효율적인 이동 통신 그룹 키 갱신 방식을 제안하였다.

6. 참고 문헌

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

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

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

[4]. 심주걸, 박춘식, 원동호, "디지털 이동통신 시스템에 적합한 그룹 공유키 경신 방식," 한국통신정보보호학회논문지, 제 10권, 제 3호, pp.69~75, 2000. 9. 30.

[5]. 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.