이동 통신에 적용 가능한 대리서명방식

이명희, 박지환
부경대학교 전산정보학과
부경대학교 컴퓨터멀티미디어공학전공

Proxy Signatures Scheme for Mobile Communication

Myoung-Hee Lee, Ji-Hwan Park
Dept. of Computer & Information Science, PuKyong Nat'l University
Div. of Computer & Multimedia Engineering, PuKyoung Nat'l University

요 약

최근 무선 이동 통신의 발전을 기반으로 많은 사용자들에게 현재보다 더 나은 서비스를 제공하기 위해 많은 기술적 응용분야들이 고려되고 있으며, 특히 보안 관련 분야의 도입을 통해 기밀성 및 안전성을 획득하려 하고 있다. 이와 관련하여 무선 이동 통신상에서 상대적으로 계산능력이 뛰어난 Agent의 도움을 통해 사용자의 전자서명을 수행할 수 있는 대리서명방식을 제안하고 있다. 본 논문에서는 무선통신에서 대리서명자의 비밀 서명키에 대한 Forward Secrecy의 성질을 제공하면서 대리서명 수행 시 발생 할 수 있는 사용자 및 대리서명자의 부정서명 생성 방지, 부인봉쇄 및 기밀성을 제공할 수 있도록 제안하였다.

1. 서론

최근 네트워크의 발전과 함께 컴퓨터를 이용한 전자상거래가 활성화되고 있다. 또한 이동통신 및 Mobile IP(Internet Protocol)분야는 IT(Information Technology)산업계에서 가장 빠른 성장을 나타내는 분야 중에 하나로서 많은 사람들이 이동 통신서비스를 통해 그 편리성과 유효성을 인지하고 있다. 이러한 유.무선 통신상에서 통신 상대방을 인증하고 메시지의 무결성을 보장하는데 있어 가장 각광을 받고 있는 방식 중에 하나가 "전자서명"이다. 그러나 공개키 암호화 기법에 기초하는 전자 서명 방식을 무선통신에 적용하는 것은 상대적으로 많은 시간을 필요로 한다.

또한, 이동통신에서 도청자나 그 밖의 인증되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있고, 사용자 인증 및 부인봉쇄 등과 같은 문제는 이동통신에서 발생할 수 있는 안전성과 관련하여 여러 가지 문제를 발생시킬 수 있다 그리고 무선통신에서 대리서명자가 비밀서명 정보를 사고로 분실하였거나, 공격자가 침입함으로써 대리서명자의 비밀 서명키를 알게되는 경우 이전에 생성되었던 자료는 기밀성과 인증성을 제공하지 못한다.

본 논문의 내용은 다음과 같다. 먼저 2장에서는 무선통신 이동 상에서 인증성과 안전성을 제공하는데 필요한 요구사항을 살펴보고 3장에서는 이와 관련된 대리서명 방식과 Proxy-Signcryption방식에 대해 설명하고 4장에서는 사용자의 불법적 행위로부터 사용자 및 대리 서명 Agent를 보호하기 위한 기법과 Forward Secrecy를 제공하는 서명방식을 제안하고 5장에서 결론을 맺는다.

2. 요구사항 분석

본 장에서는 무선 이동 통신상에서 수행되는 다양한 응용분야에서 신뢰성과 효율성을 제공하기 위한 요구사항과 특징을 살펴본다[5].

1) 사용자 기밀성

무선 이동 통신을 통해 송신자가 메시지를 송신할 경우 제3자의 도청으로부터 자신의 신원을 보장하기 위하여 안전하고 정확한 방법으로 정당한 수신자에게 전송되어야 한다.

2) 인증성

메시지 송.수신시 출처가 누구이며, 전송 도중 불법적인 제3자로부터 위조 및 변경되지 않았음을 보증하는 것으로 전자 서명 기법이 적용된다.

3) 부인 봉쇄

메시지의 송.수신 여부에 대하여 무선 이동 통신 당사자간에 부인은 방지되어야 하며 이를 위해 전자 서명 기법을 사용한다.

4) 유효성

무선 이동 통신은 메시지 송.수신을 위하여 일반 네트워크에 비해 상대적으로 계산 능력이 떨어지는 무선 단말기를 사용한다. 따라서 사용자 측면에서도 충분히 사용 가능해야 한다.

5) 안전성

무선 이동 통신에서 메시지 송.수신에 참여하는 개체들이라 할지라도 위조 및 변조가 불가능해야 한다.

3. 관련연구

1) 대리서명(proxy signature)방식[1][2]

본인이 부재 중 자신을 대신하여 서명을 수행 할 수 있도록 하는 방식이다. 이는 무선 통신 상에서 계산 능력이 부족한 사용자 단말기의 한계를 극복하기 위해 대리Agent에서 서명을 수행할 수 있도록 확장될 수 있다.

[기호 및 표기]

- p : 512비트 이상의 큰 소수
- q : $q|p-1$인 큰 소수
- g : 위수가 q인 Z_p상의 원소
- x_A : 위임서명자의 비밀키
- y_A : $y_A = g^{x_A} \bmod p$, 위임서명자의 공개키
- $h()$: 해쉬 함수
- X_{AP} : 대리서명자의 비밀 서명용 키
- Y_{AP} : $Y_{AP} = g^{X_{AP}} \bmod p$, 대리서명용 공개키
- M : 서명문(메세지)

(1) 위임서명자 A

위임서명자는 $x \in Z_q$ 를 선택하여 다음과 같이 K와 대리서명자의 비밀서명 키 X_{AP}를 생성하여 (X_{AP}, K)를 대리서명자에게 비밀리에 전송한다.

$$K \equiv g^x \bmod p$$

$$X_{AP} \equiv x_A + x \cdot K \cdot \bmod q$$

(2) 대리서명자 P(Proxy Agent)

대리서명자는 자신이 받은 (X_{AP}, K)이 정당한 키인지 다음의 관계식에 의하여 확인한다.

$$g^{X_{AP}} \equiv y_A \cdot K^K \bmod p$$

맞으면 정당한 대리서명용 키로 받아들이고 아니면 다시 요구하던지 이 프로토콜을 멈춘다. 정당하면 비밀 랜덤수 $x' \in Z_q$ 를 선택하여 다음과 같이 중간값 r 과 서명문 M을 압축하기 위해 해쉬함수를 계산하고 서명 $S_{X_{AP}}$를 생성하여 검증자에게 $(K, S_{X_{AP}}, r, M)$를 전송한다.

$$r = g^{x'} \bmod p \bmod q$$

$$H = h(M)$$

$$S_{X_{AP}} \equiv (x' - r \cdot X_{AP} \cdot H) \bmod q$$

(3) 검증자 B

검증자는 위임서명 $S_{X_{AP}}$를 검증하기 위해 먼저 다음과 같이 계산한다.

$$Y_{AP} \equiv y_A \cdot K^K \bmod p$$

$$H = h(M)$$

검증과정은 다음과 같은 식의 성립여부로 대리서명의 정당성을 확인하게 된다.

$$r \equiv g^{S_{X_{AP}}} y_{AP}^{r H} \bmod p \bmod q$$

(4) 특성분석

이동 통신상의 전자 상거래 수행시 사용자의 서명을 계산능력이 뛰어난 대리서명 Agent가 대신하여 서명하므로 계산량을 줄여주는 장점이 있지만 대리서명자가 이전의 서명 정보로부터 서명을 생성할 수 있기 때문에 위임 서명자가 서명 사실에 대한 부인이 가능하다. 그리고 대리 서명자로부터 수신된 서명 정보에 대해 누구나 확인 가능하므로 전자상거래에서 사용할 경우 위임 서명자의 정보 노출이 가능하다는 단점이 발생한다[5].

2) Proxy-Signcryption방식[3]

서명자가 지정한 대리인으로 하여금 자신을 대신하

여 정당한 signcryption메세지를 생성할 수 있도록 하는 방식 방식으로 통신양자간의 안전한 정보교환을 위하여 부분위임 대리서명 방식과 방식의 장점을 이용하여 제안한 방식이다. 본 장에서는 "대리서명"방식과 "수신자지정성"을 제공하기 위해 제시된 signcrypt-ion방식을 설명한다.

[기호 및 표기]

- x_B : 검증자의 비밀키
- y_B : $y_B = g^{x_B} \bmod p$, 검증자의 공개키
- h_k : k를 키로 하는 Keyed 해쉬 함수
- $E()$ /$D()$: 관용암호/ 복호 알고리즘

(1) 위임서명자 A

위임서명자는 $x \in Z_q$ 를 선택하여 다음과 같이 K와 대리서명자의 비밀서명 키 X_{AP}를 생성하여 (X_{AP}, K)를 대리서명자에게 비밀리에 전송한다.

$$K \equiv g^x \bmod p$$
$$X_{AP} \equiv x_A + x \cdot K \bmod q$$

(2) 대리서명자 P(Proxy Agent)

대리서명자는 자신이 받은 (X_{AP}, K)이 정당한 키인지 다음의 관계식에 의하여 확인한다.

$$g^{X_{AP}} \equiv y_A \cdot K^K \bmod p$$

정당하면 비밀 랜덤수 $x' \in Z_q$ 를 선택하고 다음과 같이 계산하여 검증자에게 (c, S, H, K)를 전송한다.

$$K' \equiv Y_B^{x'} \bmod p$$
$$K' = K_1 \| K_2$$
$$H = h_{K_2}(M)$$
$$S \equiv (x'/H + X_{AP}) \bmod q$$
$$c \equiv E_{K_1}(M)$$

(3) 검증자 B

검증자는 $Y_{AP} \equiv y_A \cdot K^K \bmod p$를 계산한 후, 자신의 비밀키를 이용하여 다음을 구한다.

$$K' \equiv (y_{AP} \cdot g^H)^{S \cdot X_B} \bmod p$$

$K' = K_1 \| K_2$를 나누고 다음과 같이 메시지를 복호한다.

$$M \equiv D_{K_1}(c)$$

단, $h_{K_2}(M) = H$ 인 경우에만 정확하게 서명된 것으로 받아 들인다.

(4) 특성분석

본 방식은 무선 통신에서 요구되는 기밀성 및 인증성을 확보하고 있고 계산량이 뛰어난 대리Agent를 이용하므로 유효성 또한 확보하고 있다. 그러나 이 방식은 메시지 송신 시 서명자와 대리서명자간의 대리서명용 키를 이용하므로 서명자가 원할 경우 자신이 대리서명자를 대신하여 서명을 생성할 수 있고 대리서명 역시 서명자의 동의 없이 서명생성 가능하다. 그리고 서명자가 메시지 서명에 대한 부인봉쇄가 불가능하다[4]. 아울러 송신자와 대리서명자 사이의 비밀키인 X_{AP}가 드러날 경우 K'값을 계산할 수 있으므로 Forward Secrecy를 제공하지 못한다. X_{AP}는 특정인의 개인키가 아니므로 대리서명인의 부주의로 각 개인의 비밀키보다 노출될 확률이 높다[6][7].

$$(y_{AP} \cdot g^r)^{S \cdot X_B} = (y_B^{x_{AP}+r})^S$$

4. 제안하는 대리서명방식

본 제안방식은 기밀성 및 인증성을 만족하기 위해 대리서명 메시지를 검증자의 공개키로 암호화하여 전송하고 위임서명자와 대리서명자간의 부인봉쇄 및 안전성을 확보하기 위해 대리인 보호형 대리서명 방식과 수정된 blind Nyberg-Rueppel방식으로 제안한다[8][9].

[기호 및 표기]

- x_P : 대리서명자의 비밀키
- y_P : $y_P = g^{x_P} \bmod p$, 대리서명자의 공개키

1) 위임서명자A

(1) 위임 정보 생성

① 위임서명자A는 $x \in Z_q$ 를 선택하고 다음과 같이 계산하여 대리서명자에게 K 를 보낸다.

$$K \equiv g^x \bmod p$$

② 대리서명자는 비밀 랜덤수 $x' \in Z_q$를 선택하고 다음과 같이 계산한다.

$$R \equiv g^{x'} K \bmod p$$

※ 대리서명자는 계산 한 $R \in Z_q^*$이면 R을 위임서

명자에게 보내고 아니면 ②을 다시 수행한다.

③ 위임서명자는 대리 서명용 키를 다음과 같이 생성한다.

$$X_{AP} \equiv x_A \cdot R + x \bmod p-1$$

여기서 대리 서명용 키는 위임 서명자와 대리 서명자의 키를 같이 이용하여 생성하므로 위임 서명자는 이를 부인할 수 없다.

(2) 위임 정보 전송

위임 서명자A는 위임서명정보 X_{AP}를 비밀리에 대리서명 Agent에게 전송한다.

2)대리서명자

(1) 위임정보 확인

대리서명자는 $g^{X_{AP}} = y_A^R \cdot K \bmod p$ 를 이용하여 위임 서명자의 정당성을 확인한다. 만약 수식이 정확하다면, 전송 정보 및 위임 서명자의 정당성이 인증된다.

(2) 대리서명 수행

위임서명자의 부정행위를 막기 위해 X_{AP}'를 생성한다.

$$X_{AP}' \equiv X_{AP} + x_P y_P \bmod q$$

그리고 대리서명자는 다음과 같이 계산한다.

$$K' = y_B^{x'} \bmod p$$

$$Z = h(y_B \| K' \| M)$$

$$S(Z) \equiv (x' - x_P - X_{AP}' \cdot Z) \bmod q$$

(3) 대리서명 정보 전송

대리서명자는 서명검증을 위해 검증자B에게 $(M, K, K', R, S(Z))$ 를 전송한다.

3)검증자B

(1) 서명 검증

검증자B는 위임서명 $S(Z)$를 검증하기 위해 먼저 다음과 같이 계산한다

$$h(y_B \| K' \| M) \equiv H$$

$$Y_{AP}' \equiv y_A{}^R \cdot y_P^{y_P} \cdot K \bmod p$$

검증과정은 자신의 비밀키를 이용하여 다음과 같은 식의 성립여부로 대리서명의 정당성을 확인하게 된다.

$(g^{S(Z)} \cdot y_{AP}{}^H \cdot y_P)^{x_B} \bmod p \equiv K'$ 를 검증한다

서명검증 정보는 다음과 같은 과정을 통해 입증할 수 있다

$$(g^{S(Z)} \cdot Y_{AP}{}^H \cdot y_P)^{x_B} \bmod p$$

$$\equiv (g^{x'-x_P - X_{AP}'} \cdot {}^H(y_A^R \cdot y_P^{y_P} K)^H \cdot y_P)^{x_B} \bmod p$$

$$\equiv (g^{x'-x_P-X_{AP}'} \cdot {}^H(g^{x_A} \cdot R \cdot g^{x_P y_P} g^x)^H \cdot y_P)^{x_B} \bmod p$$

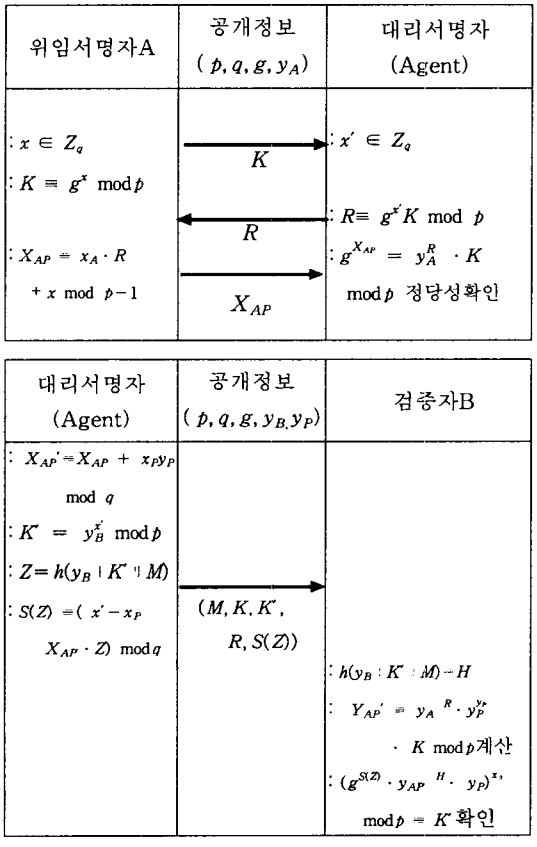
$$\equiv (g^{x'-x_P-X_{AP}'} \cdot {}^H(g^{x_A} \cdot R + x_P y_P + x)^H \cdot y_P)^{x_B} \bmod p$$

$$\equiv (g^{x'-x_P-X_{AP}'} \cdot {}^H(g^{X_{AP}'})^H \cdot g^{x_P})^{x_B} \bmod p$$

$$\equiv (g^{x'-x_P-X_{AP}'} \cdot {}^H + X_{AP}' \cdot {}^H + x_P)^{x_B} \bmod p$$

$$\equiv (g^{x'})^{x_B} \bmod p \equiv K'$$

[그림1]은 제안된 방식에 대한 전체 흐름도를 나타내었다.



[그림 1] 제안방식 흐름도

[제안 방식 고찰]

(1) 서명자 기밀성 확보

검증자만이 서명자의 서명을 확인할 수 있으므로 제3자의 도청에 의한 서명자 기밀성을 확보할 수 있다

(2) 인증성 제공

수신자 지정서명방식을 이용함으로써 인증성을 제공하고 있다

(3) 유효성 획득

서명생성 시 계산능력이 뛰어난 대리서명Agent를 이용하므로 유효성을 확보하고 있다

(4) 부인 봉쇄 가능

서명생성 시 자신의 비밀정보와 서명자의 위임정보를 함께 포함하여 수행하므로 위임서명자의 서명생성 의뢰에 대한 부인을 방지한다.

(5) 안전성 제공

서명생성 시 대리 서명자 역시 자신의 비밀정보를 생성하여 전송하고 위임서명자 역시 비밀서명정보를 위임서명자와 대리 서명자의 키로 생성되므로 위임서명자 및 대리 서명 Agent의 불법적인 서명생성이 불가능하여 안정성을 제공한다.

(6) Forward Secrecy 제공

X_{AP}가 노출되더라도 대리서명자의 비밀키 x_P를 알지 못하면 키를 계산할 수 없으므로 정당성을 확인할 수 없다.

$$(g^{S(Z)} \cdot y_{AP}{}^{H} \cdot y_P)^{x_H} \bmod p$$

$$= y_B^{S(Z)} \cdot y_B{}^{x_{AP}} \cdot {}^{H} \cdot y_B^{x_I} \bmod p$$

X_{AP}와 X_P가 모두 드러나면 키를 계산할 수 있지만, 두 키가 모두 드러날 경우는 X_{AP}만 드러날 경우에 비하여 매우 낮은 확률로 발생한다.

[각 방식의 비교분석]

방식 / 특성	대리서명 [1,2]	Proxy-Signcryption[7]	제안방식
서명자 기밀성	×	○	○
인증성	○	○	○
부인봉쇄	×	×	○
유효성	○	○	○
안전성	×	×	○
Forward Secrecy제공	×	○	○

5. 결 론

컴퓨터 네트워크 및 이동통신의 발전을 통해 향후 정보화 사회는 전자 상거래 서비스들을 비롯하여 더욱 다양한 응용 서비스들이 제공될 것이다. 이러한 환경하에서 이동통신 상의 기밀성 및 인증성을 제공하는 효율적인 전자 서명방식에 대한 연구는 매우 중요한 주제가 되고 있다.

기존의 대리 서명 방식의 경우 대리 서명자를 도입해서 유효성을 확보하고 있으나 기밀성 및 서명자 부인봉쇄가 불가능한 경우가 발생한다. 이에 본 제안 방식은 이러한 문제점을 해결하고 동시에 Forward Secrecy를 제공하는 새로운 대리 서명 방식을 제안하였다. 이를 통해 제안 방식은 기밀성과 효율성을 획득하고 있으며 동시에 인증성, 부인봉쇄 , 안전성 및 Forward Secrecy를 만족하고 있다.

향후 기존에 제안된 많은 서명방식들을 포함하여 더욱 효율적이고 안전한 대리 서명방식의 연구가 필요하리라 판단된다.

[참고문헌]

[1] M.Mambo, K. Usuda and E. Okamoto, "Proxy signature : Delegation of the power to sign message", IEICE Transaction on Fundamentals, E79-A(9):1338-1354, 1996

[2] M.Mambo, K. Usuda and E. Okamoto, "Proxy signatures for Delegation Signing Operation", Proc. Third ACM Conference on Computer and Communications Security, pp.48-57, 1996

[3] C.Gamage, J.Leiwo and Y.Zheng, "An Efficient scheme for Secure Message Transmission using Procy-Signcryption", Proceeding of the Twenty Second Australasian Comprter Science Conference, Auckland, New Zealand. January 18-21, 1999

[4] 오수현, 김현주, 원동호, "이동통신 환경에서의 전자 상거래에 적용할 수 있는 Proxy-Signctyption 방식",통신정보보호학회논문지,제10권2호,pp43-52,2000.6

[5] 박희운, 이임영 , "이동통신에서 적용 가능한 수신자 지정 대리서명 방식 "통신정보보호학회논문지, 제11권2호, pp27-34,2001.4

[6] D.Park, C.Boyd and S.Moon, "Forward Secrecy and its Application to Future Mobile Communication Security" Proc.of PKC 2000,

[7] 정희윤, 이동훈, 임종인, "Forward Secrecy를 제공하는 Signcryption" ITRC Forum 2001. pp (D1)11-14

[8] 김승주, 박상준, 원동호, "보증 부분 위임 과 역치 위임에 의한 대리 서명방식", 통신정보보호학회논문지, 제8권2호, 1998.6

[9] J.L.Camenisch, J-M.Piveteau, and M.A.Stadler, "Blind Signatures Based on the Discrete Logarithm Problem", Proc.EUROCRYPT'94, Springer Verlag, 1994, pp428-432.