이동 통신에서 적용 가능한 수신자 지정 대리 서명 방식에 관한 연구

박희운, 이임영
순천향대학교 정보기술공학부

A study of digital nominative proxy signature for mobile communication

Hee-Un Park, Im-Yeong Lee
Division of Information Technology Eng,
Soonchunhyang University

요 약

최근 무선 이동 통신의 발전을 기반으로 향후 이동 통신 시스템은 많은 사용자들에게 현재보다 더 나은 고품질의 멀티미디어 서비스를 제공할 것으로 기대된다. 따라서 이와 관련된 많은 기술적 응용 분야들이 고려되고 있으며, 특히 보안 관련 분야의 도입을 통해 기밀성 및 안전성을 획득하려 하고 있다.

본 연구에서는 이와 관련하여 이동 통신상에서 상대적으로 계산 능력이 뛰어난 agent의 도움을 통해 사용자의 디지털 서명 및 암호화를 수행할 수 있는 수신자 지정 대리 서명 방식을 제안한다. 제안 방식은 대리 서명을 수행할 경우 발생할 수 있는 사용자의 대리 서명 생성 및 부인 행위를 해결하도록 구성되어 있다. 동시에 정당한 수신자가 서명을 확인하도록 함으로서 이동 통신상에서 기밀성을 획득하는 안전한 방식이라 하겠다.

1. 서론

정보화 사회의 발전은 우리의 일반적인 생활 양식에 있어 획기적인 변화의 흐름을 일으키고 있다. 이러한 현대 사회의 정보화 현상은 산업 구조 및 사회 일반에 광범위한 컴퓨터의 보급 확산과 통신 서비스의 발전을 통해 더욱 확대되고 있다. 최근 이러한 조류에 한 흐름으로 네트워크와 컴퓨터를 이용한 전자 상거래가 활성화되고 있다.

동시에 이동 통신 및 Mobile IP(Internet Protocol) 분야의 발전은 많은 사용자들에게 네트워크에 직접 연결된 컴퓨터를 사용하지 않고도 이동 중에 Hand PC나 PDA와 같은 휴대용 단말기를 이용하여 인터넷에 접속하고 상품 주문 및 계약 등과 같은 서비스를 지원하고 있다.[1][2][3][4][5]

그러나 이러한 이동 통신 인터넷 전자 상거래 서비스들은 많은 문제점에 노출될 수 있다. 즉, 이동 통신에서 신호 교환은 무선 채널을 통해 대기 중에서 수행되므로, 도청자나 그 밖의 신뢰되지 못한 요소들로부터 위조나 불법적 변경 등과 같은 위협들에 대해서는 취약성을 지니고 있다. 뿐만 아니라 사용자 인증 및 부인 봉쇄 등과 같은 문제는 이동 통신상에서 발생할 수 있는 안전성과 관련하여 여러 가지 문제를 발생시킬 수 있다. 따라서 가입자를 제외한 다른 불법적 가입자들로부터 기밀성과 안전성을 확보하고, 사용자의 인증성을 제공하기 위한 방법 중에 하나로서 수신자 지정 서명 기법이 제시되었다.[6][7] 이 기법은 네트워크 상에서 기밀성과 사용자 인증성을 동시에 제공하기 위해서 디지털 서명을 수행하고 그 결과에 공개키 암호 방식을 사용하여 전송하게 된다. 그러나 이 방식은 모듈러 멱승과 같은 많은 계산량을 소요하게 되므로 상대적으로 계산 능력이 적은 휴대용 단말기상에서는 사용하기 힘들게 된다.

따라서 본 연구에서는 적은 계산량으로 디지털 서명을 수행하면서 안전성을 제공하기 위해 대리 서명 agent를 도입한 수신자 지정 대리 서명 기법을 제안한다. 동시에 본 방식은 사용자의 불법적 행위로부터 agent를 보호하기 위한 기법을 제공함으로서 안전성을 확보하고 있다.

2. 연구 배경

가. 대리 서명 방식[8]

1) 시스템 계수

- g : 원시 원소
- p, q : 소수 (p ≥ 512 bits, q | p-1)
- X_A : 서명자의 비밀 서명 정보
- $Y_A = g^{XA} \bmod p$: 가입자 A의 공개 검증정보
- σ : 대리 서명자의 비밀 서명 정보

2) 프로토콜

위임 서명자 A	공개 정보 (g, p, q, Y_A)	대리 서명자 B
· $k \in {}_RZ_p$ · $K = g^k \bmod p$ · $\sigma = X_A + kK \bmod p-1$	σ, K →	$g^{\sigma} = Y_A K^K \bmod p$

대리 서명자 B	공개정보 (g, p, q, Y_A)	검증자 C
· $r \in {}_RZ_n$ 선택 · $R = g^r \bmod p \bmod q$ · $H = h(M)$ · $S_\sigma(M) = r - R\sigma H \bmod q$	K, $S_\sigma(M)$, R, M →	
		· $H = h(M)$ · $\nu = Y_A K^k \bmod p$ · $R = g^{S\sigma(M)} \nu^{RH} \bmod p \bmod q$ 확인

그림 1. 부분 위임 대리 서명 방식 흐름도

3) 특성 분석

: 본인의 부재 중 자신을 대신하여 다른 사람이 자신의 서명을 수행할 수 있도록 하는 서명 방식으로 검증자는 대리 서명자가 서명자의 위임 사실을 확인할 수 있다는 특징을 가지고 있다. 이 방식은 이동 통신상의 전자 상거래 수행시 사용자의 계산량 부담을 줄여주는 장점을 가지고 있지만 위임 서명자 A가 서명을 수행한 다음 서명 사실에 대한 부인이 가능하다. 따라서 본 방식은 기밀성 및 대리 서명자의 안전성 부분에서는 취약점을 나타내고 있다.

나. 수신자 지정 서명 방식[6][7]

1) 시스템 계수

- p : 소수 p ≥ 512 bits
- q : 소수 q | p-1
- g : 원시 원소
- X_A : 서명자의 비밀 서명 정보
- $Y_A = g^{XA} \bmod p$: 가입자 A의 공개 검증정보
- $Y_B = g^{XB} \bmod p$: 가입자 B의 공개 검증정보

2) 프로토콜

이 방식의 프로토콜을 그림 2와 같이 나타내었다.

서명자 A	공개정보 (Y_A, Y_B, g, p, q)	검증자 B
· $r, R \in {}_RZ_p$ · $K = g^{R-r} \bmod p$ · $D = Y_B{}^R \bmod p$ · $e = h(Y_B, K, D, M)$ · $S = r - X_A e \bmod q$	M, K, D, S →	
		· $h(Y_B, K, D, M) = e$ · $(g^S Y_A{}^e K)^{XB} = D \bmod p$

그림 2. 수신자 지정 서명 방식 흐름도

3) 특성 분석

: 네트워크를 통해 두 명의 사용자가 메시지의 기밀성을 유지하면서 당사자간에는 메시지의 출처를 확인할 수 있도록 하기 위해 제안된 방식이다. 이 방식은 메시지의 기밀성 유지 및 송신자 인증에는 적합하나 서명 생성 및 암호화를 위해 공개키 암호 방식을 사용하게 되므로 많은 계산 능력을 필요로 한다는 문제점을 가지고 있다.

3. 수신자 지정 대리 서명 방식

본 장에서는 이동 통신 인터넷상에서 안전한 전자 상거래를 수행하려 할 경우, 서명자와 수신자 사이에 기밀성을 보장하면서, 무선 이동 단말기 상에서도 충분히 인증성을 제공하는 새로운 디지털 서명 방식을 제안한다. 그렇다면 과연 어떠한 요소들이 요구되며, 그 특징은 무엇인지 살펴본다. 다음은 그에 대한 요구 사항을 기술한 것이다.

가. 요구 사항

1) 기밀성

: 정당한 수신자에게 메시지를 정확하게 보내기 위해서는 기밀성이 요구되며 이를 위해 공개키 암호화 방식을 사용한다.

2) 인증성

: 메시지의 출처가 누구이며, 전송 도중 위조 및 변경되지 않았음을 보증하는 것으로서 디지털 서명 기법이 적용된다.

3) 부인 봉쇄

: 메시지의 송·수신 여부에 대한 부인은 방지되어야 하며 이를 위해 디지털 서명 기법을 도입한다.

4) 유효성

: 상대적으로 계산 능력이 떨어지는 사용자 측면에서도 충분히 사용 가능해야 한다.

5) 안전성

: 대리 서명 agent가 생성한 서명을 제 3자가 위조할 수 없어야 한다.

나. 수신자 지정 대리 서명 방식 제안

상기 요구 사항을 만족하는 디지털 서명을 위하여 본 연구에서는 다음과 같은 해결책을 제시한다.

1) 시스템 계수

- p : 소수 $p \geq 512$ bits
- q : 소수 $q \mid p-1$
- g : 원시 원소
- X_A, X_B, X_G : 서명자, 검증자 및 agent의 비밀 서명 정보
- $Y_A = g^{X_A} \bmod p$: 가입자 A의 공개 검증정보
- $Y_B = g^{X_B} \bmod p$: 검증자 B의 공개 검증정보
- $Y_G = g^{-X_G} \bmod p$: 대리 서명 agent의 공개 검증 정보
- a : 대리 서명자의 비밀 서명 정보

2) 프로토콜

(1) 위임 정보 생성

이동 통신 단말기를 보유한 사용자(위임 서명자)는 대리 서명 agent에게 서명 생성을 위한 위임 정보를 다음과 같이 생성한다.

- $k \in {}_RZ_p$
- $K = g^k \bmod p$
- $a = X_A + kK \bmod p$

(2) 위임 정보 전송

사용자는 생성된 정보 a, K 그리고 서명을 수행할 메시지 M을 대리 서명 agent에게 전송한다.

(3) 위임 정보 확인

대리 서명 agent는 다음과 같이 수신된 정보를 기초로 위임 서명자의 정당성을 확인한다. 만약 수식이 정확하다면, 전송 정보 및 위임 서명자의 정당성이 인증된다.

- $g^a = Y_A K^K \bmod p$

(4) 수신자 지정 대리 서명 수행

대리 서명 agent는 랜덤 수 r 및 R을 다음과 같이 선택하고, 위임 서명자의 부정 행위를 방지하기 위한 K''을 생성한다. 이를 통해 위임 서명자가 대리 서명 agent를 가장해 수신자 지정 서명을 생성하는 것을 막을 수 있으며, 차후 분쟁이 발생할 경우 위임 서명자의 부정으로부터 대리 서명 agent를 보호하게 된다.

- $r, R \in {}_RZ_p$
- $K'' = g^{R-rXG} \bmod p$

대리 서명 agent는 서명 수행을 위해 다음과 같이 D, e를 계산한 다음 수신자 지정 서명 Sa(Z)를 생성한다. D 및 e를 생성할 때 검증자 B의 공개키를 사용하는 이유는 제 3자의 도청이 있다 하더라도 검증자만이 서명을 확인할 수 있도록 하기 위함이다. 이를 통해 대리 서명 agent와 검증자간에 기밀성을 제공하게 된다.

- $D = Y_B^R \bmod p$
- $e = h(Z(= Y_B, K'', D, M))$
- $Sa(Z) = X_G r - Rae \bmod q$

(5) 수신자 지정 대리 서명 정보 전송

대리 서명 agent는 서명 검증을 위해 검증자 B에게 M, K'', D, R, Sa(Z)를 전송한다.

(6) 서명 검증

검증자 B는 다음과 같이 수신된 정보를 통해 서명 검증을 위한 정보 e와 b를 생성한다.

- $h(Y_B, K'', D, M) = e$
- $b = Y_A K^K \bmod p$

생성된 정보를 통해 다음과 같이 수신자 지정 대리 서명을 검증한다.

- $(g^{Sa(Z)} b^{Re} K'')^{XB} \bmod p = D$

그림 3은 제안된 방식에 대한 개략적인 흐름도를 나타낸 것이다.

위임 서명자 A	공개정보 (g, p, q, Y_A)	대리 서명 agent
· $k \in {}_RZ_p$ · $K = g^k \bmod p$ · $a = X_A + kK \bmod p$	a, K, M →	$g^a = Y_A K^K \bmod p$ 정당성 확인

대리 서명 agent	공개정보 (g, p, q, Y_B)	검증자 B
· $r, R \in {}_RZ_p$ · $K'' = g^{R-rXG} \bmod p$ · $D = Y_B^R \bmod p$ · $e = h(Z = Y_B, K'', D, M)$ · $Sa(Z) = X_G r - Rae \bmod q$	M, K'', D, R, Sa(Z) →	
		· $h(Y_B, K'', D, M) = e$ · $b = Y_A K^K \bmod p$ · $(g^{Sa(Z)} b^{Re} K'')^{XB} \bmod p = D$

그림 3. 제안 방식 흐름도

3) 서명 프로토콜 검증

서명 프로토콜 검증은 다음과 같은 과정을 통해 그 유효성을 입증할 수 있다.

$$
\begin{aligned}
&(g^{Sa(Z)} b^{Re} K'')^{XB} \\
&= (g^{rXG-Rae} (Y_A K^K)^{Re} g^{R-rXG})^{XB} \\
&= (g^{rXG-Rae} (g^{XA} g^{Kk})^{Re} g^{R-rXG})^{XB} \\
&= (g^{rXG-Rae} (g^{Kk+XA})^{Re} g^{R-rXG})^{XB} \\
&= (g^{rXG-Rae} g^{aRe} g^{R-rXG})^{XB} \\
&= (g^R)^{XB} \\
&= Y_B^R \\
&= D
\end{aligned}
$$

4) 제안 방식 고찰

기존에 제시되었던 디지털 서명 방식들을 고려할

경우, 본 방식은 다음과 같은 특징을 보유하고 있다.

(1) 기밀성 확보

본 제안 방식은 수신자 지정 서명 방식을 적용함으로서 제 3자에 대한 도청 공격에 대해 기밀성을 확보하고 있다.

(2) 인증성 제공

이동 통신에서 전자상거래를 수행할 경우 투명성을 높이기 위해 인증성 제공은 필수적이다. 본 방식은 수신자 지정 서명 방식을 이용함으로서 인증성을 제공하고 있다.

(3) 부인 봉쇄 가능

서명 생성시 대리 서명 agent는 자신의 비밀 정보를 생성하여 위임 서명 정보와 함께 서명을 수행하게 된다. 따라서 위임 서명자의 서명 생성 의뢰에 대한 부인을 방지할 수 있다.

(4) 유효성 획득

서명 생성시 위임 서명자는 상대적으로 계산 능력이 뛰어난 대리 서명 agent를 이용하여 서명을 수행하게 되므로 이동 통신 단말기를 가정하더라도 충분히 유효성을 확보하고 있다.

(5) 안전성 제공

대리 서명 agent가 서명을 수행할 때, 자신의 비밀 정보를 생성하여 서명을 수행하게 된다. 따라서 위임 서명자를 포함하여 제 3자에 의한 불법적인 서명 생성은 불가능하게 되므로 안전성을 제공하게 된다.

표 1은 상기 고려 사항을 살펴 볼 때, 기존의 몇몇 방식과 제안 방식의 기능을 비교 분석한 것이다.

표 1. 각 방식별 특성 비교 분석

특성 / 방식	기밀성	인증성	부인봉쇄	유효성	안전성
수신자 지정 서명	O	O	O	X	X
대리 서명	X	O	X	O	X
제안 방식	O	O	O	O	O

4. 결론

네트워크 및 이동 통신의 발전을 통해 향후 정보화 사회는 더욱 다양한 전자 상거래 서비스들이 제공될 것이다. 이러한 환경하에서 이동 통신상에서 인증성을 제공하는 효율적인 디지털 서명 방식의 연구는 매우 중요한 주제가 되고 있다.

기존의 수신자 지정 서명 방식의 경우 기밀성 확보를 통해 서명자와 검증자간에 안전한 채널이 형성되어 무선 통신상의 취약성은 극복하고 있다. 그러나 서명 수행시 모듈러 멱승 계산이 서명자의 무선 단말기를 통해 이뤄져야 하므로 효율성은 없다. 또한 대리 서명 방식의 경우 대리 서명자를 도입해 유효성은 확보하고 있으나, 기밀성 및 서명자 부인봉쇄가 불가능한 경우가 발생된다.

이에 본 제안 방식은 기존의 방식들이 안고 있던 문제점을 해결하는 새로운 수신자 지정 대리 서명 방식을 제안하였다. 이를 통해 제안 방식은 기밀성과 효율성을 획득하고 있으며 동시에 인증성, 부인봉쇄 및 안전성을 동시에 만족하고 있다. 향후 기존에 제안된 많은 서명 방식들을 응용해 더욱 효율적이고 안전한 수신자 지정 대리 서명 방식의 연구가 필요하리라 판단된다.

[참고문헌]

[1] ETSI ETS GSM 02.09, "European Digital Cellular Telecommunications System(Phase 2); Security Aspects," Version 4.2.4, September 1994.

[2] ETSI ETS 3000175-7, "DECT Common Interface, Part 7: Security Features," October 1992.

[3] UMTS Forum, "A regulatory framework for UMTS," Report no. 1, 1997.

[4] ETSI ETR 33.20, "Security Principles for the Universal Mobile Telecommunications System (UMTS)," Draft 1, 1997.

[5] ITU, "Security Principles for Future Public Land Mobile Telecommunication Systems," Rec. ITU-R M. 1998.

[6] Y. Zheng, "Signcryption and Its Applications in Efficient Public key Solutions," Proc. ISW'97, LNCS 1397, pp.291-312, 1998.

[7] S. J. Kim, S. J. Park and D. H. Won, "Nominative Signatures," Proc. ICEIC'95, pp.II-68 ~ II-71, 1995.

[8] M. Mambo, K. Usuda, and E. Okamoto, "Proxy Signatures," Proceedings of the 1995 Symposium on Cryptography and Information Security (SCIS 95), Inuyama, Japan, 24-27 Jan 1995, pp. B1.1.1-17.