이동 통신 시스템에서의 효율적인 소액지불 기법

김선형°, 임수철, 김태윤
고려대학교 컴퓨터학과
{shaklim, causal, tykim}@netlab.korea.ac.kr

An Efficient Micropayment Scheme in Mobile Telecommunications System

Sun-Hyoung Kim°, Soo-Chul Lim, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

이동 통신 시스템에 적합한 지불 프로토콜의 설계 시 네트워크의 적은 대역폭과 사용자 단말기의 제한된 성능을 고려하여 서비스 제공자와의 지불 단계에서 수행되는 온라인 계산이 최소화되어야 한다. 이는 대부분의 소액지불 프로토콜에서 해쉬 체인 기법을 사용함으로써 해결하고 있다. 그러나 기존의 소액지불 기법에서는 이동 통신 시스템에 존재하는 수많은 서비스 제공자와 거래를 하기 위해서 각 서비스 제공자에 대한 해쉬 체인을 새로 생성해야 하는 문제점이 있다. 본 논문에서는 UMTS와 같은 차세대 이동 통신 시스템에서 제공되는 서비스를 위한 개선된 소액지불 기법을 제안한다. 제안한 기법은 사용자의 추가적인 계산량의 부담없이 네트워크에 존재하는 여러 서비스 제공자와의 거래를 가능하게 하는 효율적인 방법을 제공한다.

1. 서론

무선 인터넷 단말기를 소유한 이동 사용자는 편리하고 다양한 수단으로 정보를 획득하고 있다. 이제는 사용자의 단말기가 단순히 정보 획득을 위한 도구로서 뿐만 아니라 정보에 대한 지불 수단으로 이용될 것이다. 이에 따라 UMTS(Universal Mobile Telecommunications System)[5]와 같은 제 3세대 이동 통신 시스템에 존재하는 수많은 서비스 제공자들로부터 다양한 서비스와 정보를 이용하기 위해서 지불의 안전성과 효율성이 보장되는 새로운 지불 메커니즘의 필요성이 제시되고 있다.

ACTS 프로젝트인 ASPeCT(Advanced Security for Personal Communications Technologies)에서 개발된 AIP(Authentication and Initialisation of Payments) 프로토콜[1,2]은 공개키 암호 시스템을 기반으로 이동 통신 환경에서의 인증 및 지불 메커니즘을 제시하고 있다. 그러나 AIP 프로토콜에서는 사용자가 생성한 지불값들을 하나의 VASP(Value-Added Service Provider)에게만 사용할 수 있으며 각 VASP에 대한 지불값들을 새로 생성해야 하는 문제점이 있다.

본 논문에서는 UMTS와 같은 제 3세대 이동 통신 시스템에서 PayWord 기법[3]을 기반으로 하여 이동 사용자에 의한 한 번의 해쉬 체인의 생성으로 여러 서비스 제공자와 거래가 가능한 효율적인 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구로서 ASPeCT에서 개발된 AIP 프로토콜에 대하여 살펴본다. 3장에서는 본 논문에서 제안하는 지불 프로토콜에 대하여 기술한다. 4장에서는 제안한 프로토콜에 대하여 안전성을 분석하고, 5장에서는 성능을 평가한다. 6장에서 결론을 맺는다.

2. AIP 프로토콜

AIP 프로토콜은 사용자와 VASP간의 상호 인증 방법과 적절한 지불 메커니즘을 제공한다. AIP 프로토콜에서는 사용자와 VASP간의 지불 메커니즘으로 "tick"을 사용하는 소액지불 프로토콜[4]을 사용한다. 다음 기호들은 본 논문에서 프로토콜을 기술하기 위해 사용된다.

g : 이산 대수를 풀기 어려운 곱셈군의 생성원
idX : 참여자 X의 신원
u : 사용자의 비밀키
v : VASP의 비밀키
PK_U : 사용자의 인증된 서명 검증용 공개키
SK_U : 사용자의 서명 생성용 비밀키
$\{M\}_K$: 키 K를 사용하여 메시지 M을 암호화
$Sig_X\{M\}$: X에 의해 서명된 메시지 M

AIP 프로토콜을 개시하기 전에 U는 난수 u를 생성하고 비밀 세션키를 수립하기 위한 g^u를 계산하여 사용자 인증기관의 신원인 $idCA$와 함께 V에게 전송한다.

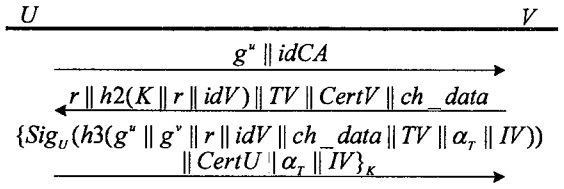

그림 1. AIP 프로토콜

첫 번째 메시지를 수신한 V는 난수 r을 생성하고 g^{uv}를 계산하여 U와 Diffie-Hellman 방식의 비밀 세션키 $K = h1(g^{uv} \| r)$을 확립한다. 그런 후에 $CertV$와 지불에 대한 정보를 포함하는 ch_data, 타임스탬프 TV, 난수 r과 더불어 r과 idV를 K와 함께 해쉬 처리하여 보냄으로써 U로 하여금 V가 K를 수립하고 있음을 알게 한다.

두 번째 메시지를 전달받게 되면 U는 V의 공개키 인증서 $CertV$를 검증하고 V가 생성한 것과 같이 비밀 세션키 K를 계산한다. U는 ch_data, g^u, g^v, r을 idV와 TV, α_T, 지불 초기화 벡터 IV를 함께 서명한 후 K로 암호화하여 V에게 전송한다.

마지막 메시지를 전달받은 V는 U의 공개키 인증서를 이용하여 서명을 검증하고 지불에 관련된 파라미터들을 획득한다. 검증이 완료되면 V는 U에게 서비스를 제공하기 시작한다.

3. 이동 통신 서비스를 위한 지불 프로토콜

3.1. 시스템 구성

본 논문에서 제안하는 지불 프로토콜에서는 이동 사용자, 서비스 제공자 그리고 브로커의 세 참여자들이 시스템을 구성하고 있다. 아래 그림 2는 이들 사이의 관계를 보여주고 있다.

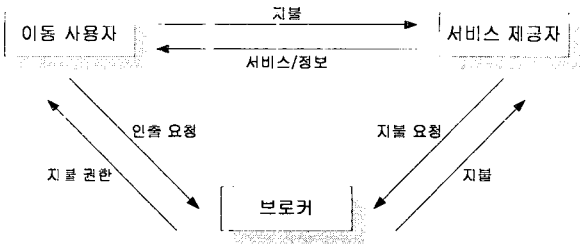

그림 2. 시스템 구성

3.2. 제안하는 인출 프로토콜

제안하는 인출 프로토콜은 이동 사용자가 이미 브로커와 비밀 세션키 L을 공유하고 있다고 가정한다.

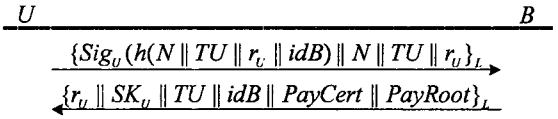

그림 3. 인출 프로토콜

프로토콜을 개시하기 전에 U는 서비스 제공자의 최대값 N과 난수 r_U를 설정한다. 이렇게 설정된 값들을 타임스탬프 TU, idB와 함께 해쉬 함수로 처리하고 서명을 한 후 비밀 세션키 L로 암호화하여 B에게 전송한다.

B는 U로부터 전달받은 메시지를 복호화하고 서명을 검증한다. 검증이 완료되면 B는 $TN_U = h(idU \| r_U \| K)$를 생성하고 $PayRoot$를 계산한다. 그런 후에 B는 키 쌍 PK_U, SK_U를 생성하고, 특정한 사용자에 유효한 지불 권한 인증서 $PayCert$를 만들어낸다. $PayCert$는 다음과 같은 구조를 갖는다.

$$\{Sig_B(h(idB \| TN_U \| PK_U)) \| idB \| TN_U \| PK_U\}$$

B는 난수 r_U와 사용자의 비밀 서명키 SK_U, 타임스탬프 TS와 idB를 $PayCert$, $PayRoot$와 함께 비밀 세션키 L로 암호화하여 U에게 전송한다.

U는 B로부터 메시지를 전달받아 복호화하고 r_U와 TS를 확인한다. U는 $PayCert$와 $PayRoot$, SK_U를 획득한다.

3.3. 제안하는 지불 프로토콜

U는 프로토콜을 개시하기 전에 root값과 $PayRoot$의 인자를 포함시킨 메시지를 서명해야 한다. U가 전자 화폐를 생성하는 과정은 PayWord[2]기법을 따른다.

U는 이전까지 $k-1$까지 V와의 거래에서 $j-1$개의 전자 화폐를 소비하였다고 가정한다. 새로운 k 번째 V와의

거래에서 w_j는 해쉬값의 새로운 root값으로 설정되고 T_k는 이에 대한 증거 요소로 작용한다. T_k는 $i=N,\ldots,0$에 대하여 다음과 같이 생성된다.

$$T_i = h(T_{i+1}, TN_U)$$

U는 이 메시지를 idV와 함께 비밀 서명키 SK_U로 서명한 후 $PayCert$와 함께 V에게 전송한다.

메시지를 전달받은 V는 $PayCert$를 검증하고 여기에서 추출된 U의 공개키 PK_U로 U의 서명을 검증함으로써 가지불할 전자 화폐에 대한 정당성을 보장받는다. V는 이후부터 지불값에 대하여 해쉬 함수를 통하여 인증한다.

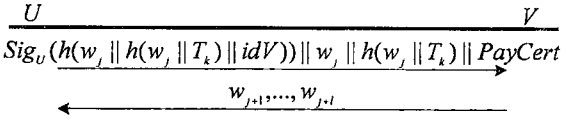

그림 4. 지불 프로토콜

V는 $w_j \| h(w_j \| T_k) \| PayCert \| P_{j+1}$을 저장하고 결제 단계에서 브로커에게 이를 제출하여 지불을 요구한다.

4. 안전성 분석

- 기밀성 : 사용자와 브로커 사이에서 교환되는 정보는 비밀 세션키 L에 의해 암호화되어 안전하게 전송되기 때문에 기밀성이 보장된다.
- 부인 방지 : 사용자는 지불 단계에서 자신의 서명이 포함된 메시지와 더불어 서명의 정당성을 보장하는 PK_U가 포함된 $PayCert$를 함께 전송하므로 서비스에 대한 부인을 방지할 수 있다.
- 익명성 : 지불 단계에서 서비스 제공자에게 전송하는 메시지에는 사용자를 인식할 만한 정보가 포함되지 않는다. 또한 브로커와의 결제에 필요한 $PayCert$와 $root$값, 지불값만 저장하므로 익명성이 보장된다.
- 이중 지불 탐지 : $PayCert$ 에는 TN_U가 포함되어 있고 $h(w_j \| T_k)$는 $PayRoot$와 묶여 있다. 이 값들은 결제 시에 브로커에게 전달되므로 사용자가 이중으로 지불하면 브로커가 이를 탐지할 수 있다.
- 위조 방지 : $PayCert$는 비밀 세션키 L로 암호화되어 발급되고 이를 소유한 정당한 사용자만이 전자 화폐를 생성할 수 있으므로 위조가 불가능하다.

5. 성능 평가

제안한 프로토콜의 가장 큰 특징은 같은 계산량으로 여러 서비스 제공자와의 거래가 가능하다는 점이다. 사용자의 공개키 연산을 필요로 하는 인출 과정을 최대한 줄임으로써 무선 환경에 적합한 특성을 나타내고 있다.

표 1. 프로토콜들의 특성 비교

항목 \ 프로토콜	AIP 프로토콜	제안한 프로토콜
익명성 제공	×	○
다중 거래	×	○
서비스 계약기간	중기/장기	단기
지불 방식	후지불	선지불
지불 규모	소액	소액/고액

[×: 제공하지 않음 ○: 제공함]

아래의 표 2는 제시된 프로토콜들에서 사용자와 서비스 제공자가 수행하는 계산량을 비교한 것이다. API 프로토콜이 비밀 세션키 설정을 위해 공개키 암호화 연산을 수행하는 반면 제안한 프로토콜은 한 번의 메시지 전송으로 이를 완료함으로써 우수한 효율성을 나타낸다.

표 2. 제시된 프로토콜들의 계산량 비교

항목 \ 프로토콜	AIP 프로토콜		제안한 프로토콜	
	U	V	U	V
사전 계산	1	0	0	0
온라인 계산	1	1	0	0
공개키 암호화	1	0	0	0
공개키 복호화	0	0	0	0
서명 생성	1	0	1	0
검증	1	2	0	2

6. 결론

본 논문에서는 이동 통신 시스템에 적합한 효율적인 지불 프로토콜을 제안하였다. 제안한 지불 메커니즘은 사용자에 의한 한 번의 해쉬 체인의 생성으로 여러 서비스 제공자와의 거래를 할 수 있으며, 지불 단계에서 공개키 연산을 배제함으로써 우수한 효율성을 나타내었다.

참고문헌

[1] ACTS AC095, ASPeCT Deliverable D20, Project final report and results of trials, 1998.
[2] G.Horn, B.Preneel, "Authentication and payment in future mobiel systems," LNCS, Vol.1485, 1998.
[3] R.Rivest, A.Shamir, "PayWord and MicroMint: two simple micropayment schemes," LNCS, Vol.1189, 1996.
[4] T.P.Pederson, "Electronic payments of small amounts," LNCS Vol.1351, 1997.
[5] UMTS Forum, "A Regulatory Framework for UMTS," Report No.1, 1997.