무선 인터넷 서비스를 위한 효율적인 지불 프로토콜

김선형, 이윤정, 김정범, 김태윤
*고려대학교 컴퓨터학과
e-mail : shaklim@netlab.korea.ac.kr

An Efficient Payment Protocol for Wireless Internet Services

Sun-Hyoung Kim, Yoon-Jung Rhee, Jeong-Beom Kim, Tai-Yun Kim
Dept. of Computer Science & Engineering, Korea University

요 약

본 논문은 무선 인터넷 상에서 서비스 제공자로부터 제공되는 정보나 서비스의 지불 메커니즘에 관한 것이다. 본 논문에서는 사용자로 하여금 무선 인터넷이 가능한 단말기를 사용하여 획득한 정보나 서비스를 은행과 같은 중간 매개 기관을 거치지 않고 직접 서비스 제공자에게 지불하는 효율적인 메커니즘을 제안한다. 이는 무선 인터넷 상에서의 프로토콜 참여자 사이에 신속하고 안전한 전자상거래의 실현을 가능하게 한다. 본 논문에서는 무선 단말기가 브로커로부터 지불 권한을 부여받아 직접 전자 화폐를 생성하는 PayWord[5] 기법을 도입한다. 본 논문에서 제안하는 지불 프로토콜은 무선 인터넷 단말기를 소지한 사용자가 구입에 필요한 전자화폐를 인출하는 단계, 사용자가 실제 서비스 받은 항목에 대해 전자화폐를 무선 네트워크 상으로 전송하는 지불 단계, 서비스 제공업자가 자신이 받은 전자 화폐를 하기 상환하기 위한 브로커와의 결제 단계로 구성되어 있다.

1. 서론

무선 인터넷 서비스를 이용하기 위한 이동 통신 시스템의 설계 시 전송 채널의 불안전성과 사용자 단말기의 제한된 성능을 충분히 고려하여야 한다. 특히 UMTS(Universal Mobile Telecommunications System)와 같은 제 3세대 무선 이동 시스템에서는 이동 사용자가 이러한 무선 인터넷 서비스를 이용하기 위해 기존에 구축된 지불 시스템보다 더 안전하고 효율적인 메커니즘이 요구된다.

티켓 기반의 인증 및 지불 프로토콜[2]에서는 기존의 지불 방식을 탈피하여 사용자가 티켓 서버로부터 발급받는 티켓을 이용하여 서비스를 제공받는다. 티켓 안에 서비스를 이용할 수 있는 최대 사용 횟수를 설정함으로써 여러 VASP(Value-Added Service Provider)와의 거래가 가능하고, 티켓이 지불 수단이 되므로 지불이 매우 용이하다는 장점을 가진다. 그러나 제공되는 서비스의 종류와 금액에 따라 티켓의 종류와 수가 증가되어야 하며 사용자가 특정한 서비스에 대한 티켓을 소유하고 있지 않을 경우 이에 대한 새로운 티켓을 발급받아야 한다.

본 논문에서는 UMTS와 같은 제 3세대 이동 통신 시스템에서 PayWord 기법을 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 AIP 프로토콜[1,3]을 기반으로 한 티켓 기반의 인증 및 지불 프로토콜에 대하여 살펴본다. 3장에서는 본 논문에서 제안하는 다중 지불 메커니즘에 대하여 기술한다. 4장에서는 이를 바탕으로 한 프로토콜을 제안하고, 5장에서는 이에 대한 성능 평가를 한다. 6장에서 결론을 맺는다.

2. 티켓 기반의 인증 및 지불 프로토콜

2.1. 티켓 구조

티켓 기반 지불 모델의 구성원들은 이동 사용자와 VASP, 티켓 서버이다. 티켓 기반의 인증 및 지불 프로토콜은 사용자가 티켓 서버로부터 티켓을 획득하는 단계와 티켓을 사용하여 서비스나 정보를 얻는 단계로 구분된다. 티켓 서버는 사용자의 정보를 유지하는 신뢰기관으로서 사용자에게 다음과 같은 구조를 갖는 티켓을 발행한다.

$Ticket=$
$\{Sig_T(h(sn \| idT \| g^u \| PK_U \| TT \| data)) \| sn \| idT \| g^u \| PK_U \| TT \| data\}$

티켓은 서비스나 정보를 위해 사용자에게 발급되는 특별한 인증서로 티켓 서버의 서명으로써 그 정당성이 입증된다.

2.2. 티켓 획득 프로토콜

사용자는 티켓 서버로부터 티켓을 획득하기 위해 아래 그림 1과 같이 티켓 획득 프로토콜을 수행한다. 사용자와 티켓 서버는 각각 U와 T로 나타내고, 이미 비밀 세션키 L을 공유하고 있다고 가정한다.

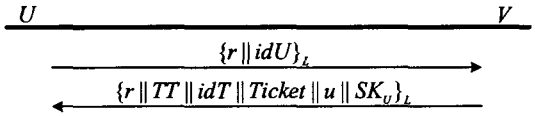

그림 1. 티켓 획득 프로토콜

U는 난수 r을 생성하고 idU와 함께 비밀 세션키 L로 암호화하여 T에게 전송한다. T는 전달받은 메시지를 복호화하여 티켓을 요청하는 idU와 r을 얻는다. T는 U의 인증서 취소 여부를 파악하여 티켓과 idU, r, TT, 그리고 비밀키 u와 SK_U를 L로 암호화하여 U에게 전송한다.

U는 T로부터 전달받은 메시지를 복호화하여 티켓과 개인키 u와 서명용 키 SK_U를 획득한다. U는 T의 서명을 검증하여 티켓의 정당성을 보장받는다.

2.3. 티켓 기반의 인증 및 지불 프로토콜

아래 그림 2는 티켓 기반의 인증 및 지불 프로토콜을 나타낸다. VASP는 티켓의 정당성과 사용자가 티켓의 소유주라는 사실을 확인한다. 아래에서 U와 V는 각각 사용자와 VASP를 나타낸다.

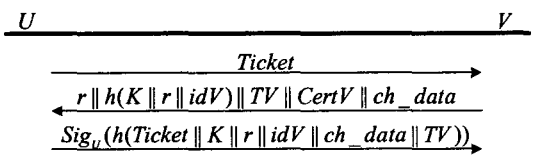

그림 2. 티켓 기반의 인증 및 지불 프로토콜

프로토콜이 시작되면 U는 티켓 획득 프로토콜에서 얻은 $Ticket$을 V에게 전송한다. V는 $Ticket$으로부터 g^u와 키 설정용 비밀키 v를 얻고, 이를 이용하여 비밀 세션키 $K=h(g^{uv} \| r)$을 계산한다. 그런 후에 V는 난수 r을 생성하여 두 번째 메시지를 U에게 전송한다.

메시지를 전송받은 U는 $CertV$로부터 g^v를 획득하여 V와 동일한 세션키 K를 계산한다. 그리고 해쉬 값을 검사하여 V가 실제로 비밀 세션키를 소유하고 있는지를 확인한다. V는 이렇게 획득한 값들에 자신의 비밀키로 서명하여 U에게 전송한다.

마지막 메시지를 전달받은 V는 비밀 세션키 K를 이용해서 메시지를 복호화하고 사용자의 서명을 검증한 후 U에게 서비스 제공을 시작한다. V는 티켓 서버에게 U의 서명이 기재된 티켓을 제출하고 제공한 서비스에 대한 지불을 얻는다.

3. 다중 지불 메커니즘

본 논문에서는 사용자에 의한 한 번의 해쉬 체인의 생성으로 여러 서비스 제공자와 거래를 할 수 있는 메커니즘을 제안한다. 다음 표 1은 프로토콜을 기술하기 위해 사용되는 기호들을 나타낸다.

표 1. 프로토콜에 사용되는 기호

기 호	설 명
g	이산 대수 문제에서의 곱셈군 생성원
idX	참여자 X의 신원
TX	X에 의해 생성된 타임스탬프
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

3.1. *PayRoot*

브로커는 사용자와의 상호 보안 협상을 통해 거래 가능한 서비스 제공자의 최대값인 N개만큼의 새로운 해쉬 체인 $PayRoot$를 $TN_U=h(idU \| r \| K)$와 함께 다음과 같이 생성한다.

$$T_i=h(T_{i+1}, TN_U), \quad i=N,\ldots,0$$

3.2. *PayCert*

사용자는 $PayRoot$와는 별도로 자신이 생성한 해

쉬값들의 정당성을 보장받기 위해 브로커로부터 다음과 같은 구조를 갖는 *PayCert*를 발급받는다.

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

*PayCert*는 브로커가 사용자에게 지불을 생성할 수 있는 권한을 부여하기 위해 발급하는 지불 권한 인증서이다.

4. 무선 인터넷 서비스를 위한 지불 프로토콜

4.1. 시스템 모델

본 논문에서 제안하는 지불 모델에서는 이동 사용자, 서비스 제공자, 그리고 브로커의 세 참여자들이 시스템을 구성하고 있다.

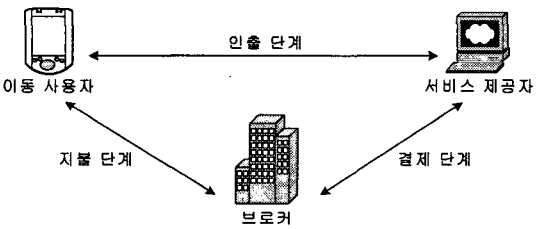

그림 3. 시스템 모델

4.2. 인출 프로토콜

제안하는 인출 프로토콜은 이동 사용자와 브로커 사이에 비밀 세션키 L을 공유하고 있다고 가정한다.

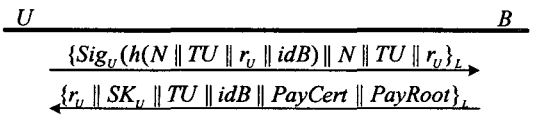

그림 4. 인출 프로토콜

*U*는 프로토콜의 시작 전에 N과 난수 r_U를 설정한다. 설정된 값들을 TU, idB와 함께 해쉬 함수로 처리하고 서명한 후 비밀 세션키 L로 암호화하여 B에게 전송한다.

*B*는 전달받은 메시지를 복호화하고 서명을 검증한다. 그런 후에 TN_U를 계산하여 *PayRoot*를 생성한다. 또한 서명용 키 쌍 PK_U, SK_U를 생성하고, 지불 권한 인증서 *PayCert*를 만들어낸다. *B*는 r_U와 SK_U, TS, idB를 *PayCert*, *PayRoot*와 함께 비밀 세션키 L로 암호화하여 *U*에게 전송한다.

*U*는 *B*로부터 메시지를 전달받아 복호화하고 r_U와 TS를 확인한다. 확인이 완료되면 *U*는 *PayCert*와 *PayRoot*, SK_U를 획득하게 된다.

4.3. 지불 프로토콜

그림 5는 서비스 제공자와의 지불 프로토콜을 나타낸다. *U*는 프로토콜의 시작 전에 지불값의 root값과 *PayRoot*가 삽입된 메시지를 서명해야 한다. 전자화폐의 생성은 PayWord 기법을 따른다.

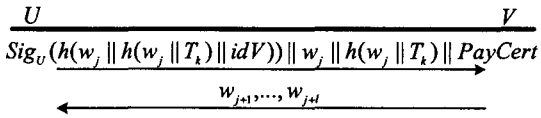

그림 5. 지불 프로토콜

*U*는 이전까지 $k-1$까지 *V*와의 거래에서 $j-1$개의 전자 화폐를 소비하였다고 가정한다. 새로운 k 번째 *V*와의 거래에서 w_j는 지불값의 root값으로 설정되고 T_k는 이에 대한 증거요소인 *PayRoot*이다. *U*는 이를 idV와 함께 SK_U로 서명한 후 *PayCert*와 함께 *V*에게 전송한다.

*V*는 *PayCert*를 검증하고 *U*의 공개키 PK_U로 서명을 검증함으로써 지불받을 전자 화폐에 대한 정당성을 보장받는다. *V*는 이후부터 지불되는 전자화폐에 대하여 해쉬 함수를 통하여 인증하며 브로커에게 지불을 받기 위해 $w_j \| h(w_j \| T_k) \| PayCert \| P_{j+1}$을 저장한다.

4.4. 결제 프로토콜

일정 마감 시점이 되면 서비스 제공자는 브로커와 결제 프로토콜을 수행한다. 브로커는 자신이 발행한 *PayCert*를 검증함으로써 서비스 제공자가 요구하는 지불에 대한 정당성을 확인할 수 있다.

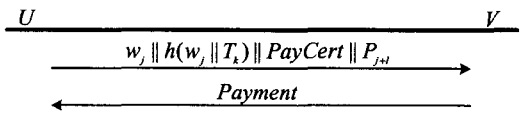

그림 6. 결제 프로토콜

*PayCert*에 포함된 TN_U는 *U*와의 인출 프로토콜에서 *PayRoot*를 계산하기 위해 특정한 *U*에게 사용된 식별자이므로 idU, r_U, K를 해쉬 함수를 수행하여 TN_U이 위조되지 않았음을 검증한다. 검증이 완

료되면 *PayRoot* 테이블에서 T_k에 대한 지불값들을 찾아내고 이에 해당하는 금액을 V에게 보낸다.

B가 V와의 결제 단계에서 T_k에 대한 지불값 w_j에서 w_{j+l}값까지만 검증할 수 있다. 즉 마지막 지불값 w_{j+l}을 l번 해쉬 수행하여 w_j와 같은지에 대해서만 확인하면 된다.

5. 성능 평가

5.1. 안전성 분석

- 이중 지불 탐지 : *PayCert* 에는 TN_U가 포함되어 있고 $h(w_j \| T_k)$는 *PayRoot*와 묶여 있다. 결제 시에 브로커는 이 값을 전달받으므로 사용자의 이중 지불을 브로커가 탐지할 수 있다.
- 위조 방지 : *PayCert*는 비밀 세션키 L로 암호화되어 발급되고, 정당한 사용자만이 이를 소유하므로 전자 화폐에 대한 위조가 불가능하다.
- 부인 방지 : *PayCert*는 지불의 정당성을 보장할 뿐 아니라 사용자의 서명으로써 부인 방지를 제공한다. 사용자는 지불 단계에서 이를 함께 전송하므로 서비스에 대한 부인을 방지한다.
- 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.
- 기밀성 : 사용자와 브로커 사이에서 교환되는 정보는 비밀 세션키 L에 의해 암호화되어 전송되되므로 기밀성이 보장된다.

5.2. 효율성 분석 및 성능 평가

아래의 표 2와 표 3은 각각 제시된 프로토콜들의 계산량을 비교한 것이다. 티켓 기반 프로토콜이 비밀 세션키 설정을 위해 공개키 암호화 연산을 수행하는 반면 제안한 프로토콜은 이를 배제함으로써 뛰어난 효율성을 나타낸다.

표 2. 사용자의 계산량 비교

항목 \ 프로토콜	티켓 기반 프로토콜	제안한 프로토콜
사전 계산	0	0
온라인 계산	1	0
공개키 암호화	1	0
공개키 복호화	0	0
서명 생성	1	1
검증	1	0

표 3. 서비스 제공자의 계산량 비교

항목 \ 프로토콜	티켓 기반 프로토콜	제안한 프로토콜
사전 계산	0	0
온라인 계산	1	0
공개키 암호화	0	0
공개키 복호화	0	0
서명 생성	0	0
검증	2	2

아래 표 4는 제시된 프로토콜들의 특성을 비교한 것이다. 제안한 프로토콜은 한 번의 해쉬 체인의 생성으로 다중 거래가 가능하며 나머지 지불값들을 충분히 이용할 수 있기 때문에 사용자의 공개키 연산을 필요로 하는 인출 과정을 최소화함으로써 사용자 단말기의 제한된 성능을 고려하고 있다.

표 4. 프로토콜들의 특성 비교

항목 \ 프로토콜	티켓 기반 프로토콜	제안한 프로토콜
익명성 제공	○	○
다중 거래	○	○
용이한 서비스 이용	×	○
서비스 계약기간	중기/장기	단기
지불 방식	후지불	선지불

[×: 제공하지 않음 ○: 제공함]

6. 결론

본 논문에서는 무선 인터넷 서비스를 이용하기 위한 지불 프로토콜을 제안하였다. 제안한 프로토콜은 다수의 서비스 제공자와의 거래가 가능하도록 설계되었으며 이동 단말기를 소지한 사용자의 제한된 상황을 충분히 고려하고 있다[4]. 또한 공개키 연산을 최소화함으로써 효율성을 극대화하였다.

참고문헌

[1] ACTS AC095, ASPeCT Deliverable D20, Project final report and results of trials, 1998.
[2] B.R.Lee, S.S.Kang, T.Y.Kim, "Ticket-Based Authentication and Payment Protocol for Mobile Telecommunications Systems," PRDC, 2001.
[3] G.Horn, B.Preneel, "Authentication and payment in future mobile systems," LNCS, Vol.1485, 1998.
[4] M.Satyanarayanan, "Fundamental Challenges in Mobile Computing," Proc. of the ACM, 1996.
[5] R.Rivest, A.Shamir, "PayWord and MicroMint: two simple micropayment schemes," LNCS, 1996.