제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

제 3세대 이동 통신 시스템을 위한 인증 및 지불 기법

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

Authentication and Payment Scheme for 3G Mobile Telecommunications System

Sun-Hyoung Kim*, Tai-Yun Kim*
*Dept. of Computer Science & Engineering, Korea University

요 약

본 논문에서는 제 3세대 이동 통신 시스템에서 안전한 전자상거래의 구현을 위한 인증 및 지불 메커니즘을 제안한다. 제 3세대 이동 통신 환경에서는 GSM이나 DECT와 같은 제 2세대 이동 통신 시스템에서 사용되지 못했던 공개키 기반 구조를 도입하여 각 이동 단말기 사이에 공개키 암호 시스템을 이용한 통신이 가능하게 되었다. 이동 사용자는 TTP(Trusted Third Party)로부터 획득한 공개키 인증서를 사용하여 외부 도메인에서도 종단간의 통신을 할 수 있으며 디지털 콘텐츠를 제공하는 사이트에 접속하여 안전한 서비스를 제공받을 수 있다. 본 논문은 이동 통신 환경에 적합한 소액지불 기법을 기반으로 하여 이동 사용자와 VASP간의 상호 인증 및 지불에 관한 기법을 제안한다.

1. 서론

이동 통신 시스템의 가장 큰 장점은 사용자의 이동성(mobility)와 편재성(ubiquity)이다. 즉 이동 사용자는 시간과 장소에 구애받지 않고 원하는 사이트에 접속하여 서비스를 받거나 다른 사용자와의 통신을 할 수 있다는 점이다. 최근 무선 인터넷을 지원하는 서비스 제공업체들이 증가하고 단말기의 성능이 향상됨에 따라 이동 통신 시스템에서 안전한 통신에 대한 연구가 활발해지고 있다. 또한 UMTS(Universal Mobile Telecommunications System)[1]와 같은 제 3세대 이동 통신 시스템에서는 이동 사용자의 음성 통신뿐만 아니라 고용량의 데이터 통신을 위한 무선 인터넷 서비스를 이용하기 위해 더 안전하고 효율적인 시스템이 요구된다.

제 3세대 이동 통신 시스템이 공개키 암호 시스템을 제공함에 따라 TTP로부터 공개키 인증서를 획득한 이동 사용자는 네트워크 상에 존재하는 다양한 VASP와의 안전한 전자상거래가 가능해졌다.

티켓 기반의 인증 및 지불 프로토콜[2]은 UMTS에서 인증 및 지불 메커니즘을 제공하는 ASPeCT (Advanced Security for Personal Communications Technologies) 프로젝트의 AIP(Authentication and Initialisation of Payments) 프로토콜[3]을 기반으로 하여 이동 통신 환경에서 공개키 암호를 이용한 지불 시스템을 제시하고 있다. 이 시스템에서는 기존의 지불 방식을 탈피하여 사용자가 티켓 서버로부터 발급받는 티켓을 이용하여 서비스를 제공받을 수 있다. 티켓이 지불 수단이 되므로 지불이 용이하다는 장점이 있지만 제공되는 서비스의 종류와 금액에 따라 티켓의 종류와 수가 증가되어야 하고, 특정 서비스에 대한 티켓이 없을 경우 새로운 티켓을 발급받아야 한다.

본 논문에서는 제 3세대 이동 통신 시스템에 적합한 소액지불 프로토콜을 제안한다. 제안한 프로토콜은 공개키 암호 시스템을 사용하는 PayWord 시스템[4]을 기반으로 하여 이동 사용자가 한 번 생

성한 지불 정보를 여러 VASP에게 사용할 수 있는 효율적인 방법을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 AIP 프로토콜을 살펴보고, 3장에서는 이를 기반으로 하는 티켓 기반의 지불 프로토콜을 살펴본다. 4장에서는 본 논문에서 제안하는 종단간의 인증 및 지불 메커니즘에 대하여 설명하고, 5장에서 본 논문에 제시된 프로토콜의 안전성과 효율성을 평가한다. 6장에서 본 논문의 결론을 맺는다.

2. AIP 프로토콜

AIP 프로토콜은 사용자와 VASP간의 상호 인증과 세션키 설정을 위한 단계와 Pederson의 "tick"을 사용하는 지불 단계로 구분된다. 표 1은 본 논문의 프로토콜에 사용되는 기호를 나타낸다.

표 1. 프로토콜의 표기에 사용되는 기호

기 호	설 명
id_X	참여자 X의 신원
r_X	X에 의해 생성된 난수
TS_X	X가 생성한 타임스탬프
PK_U	사용자의 서명 검증 공개키
SK_U	사용자의 비밀 서명키
$h(x)$	x에 대하여 일방향 해수 함수를 적용
$\{M\}_K$	메시지 M을 키 K를 사용하여 암호화
$Sig_X\{M\}$	메시지 M을 X가 서명

U는 VASP와의 통신을 개시하기 위해 난수 u를 생성하고 g^u를 계산하여 이를 자신의 인증기관 신원인 id_{CA}와 함께 V에게 전송한다.

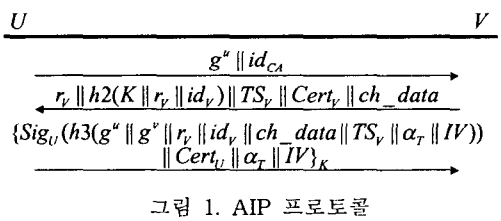

그림 1. AIP 프로토콜

메시지를 수신한 V는 난수 r_V를 생성하고, U와 비밀 세션키 $K = h1(g^{uv} \| r_V)$을 계산한다. 그런 후에 $Cert_V$와 지불 관련 정보 ch_data, TS_V, 난수 r_V와 id_V를 K와 함께 해쉬 함수를 수행하고 이를 전송한다. U는 V가 K를 수립하고 있음을 알게 된다.

두 번째 메시지를 전달받은 U는 V의 인증서 $Cert_V$를 검증하고 V와 동일한 K를 계산한다. 그런 후에 ch_data, g^u, g^v, r을 id_V와 TS_V, α_T, 지불 초기화 벡터 IV를 함께 서명한 후 K로 암호화하여 V에게 전송한다.

마지막 메시지를 수신한 V는 U의 인증서를 이용하여 서명을 검증하고 지불 관련 요소을 얻는다. 검증이 완료되면 V는 U에게 서비스를 제공한다. U는 제공받은 서비스에 대하여 tick 지불 프로토콜을 사용하여 지불한다.

3. 티켓 기반의 인증 및 지불 프로토콜

3.1 티켓 구조

티켓 기반의 지불 시스템은 이동 사용자, VASP, 티켓 서버로 구성되어 있다. 이 시스템은 사용자가 티켓 서버로부터 티켓을 획득하는 단계와 티켓을 사용하여 서비스나 정보를 얻는 단계로 구분된다. 티켓 서버는 신뢰기관의 역할을 하며 사용자에게 다음과 같은 티켓을 발행한다.

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

3.2 티켓 획득 프로토콜

사용자는 티켓 서버로부터 티켓을 획득하기 위해 아래 그림과 같은 티켓 획득 프로토콜을 수행한다. 사용자와 티켓 서버는 각각 U와 T로 나타내고, 비밀 세션키 L을 공유하고 있다고 가정한다.

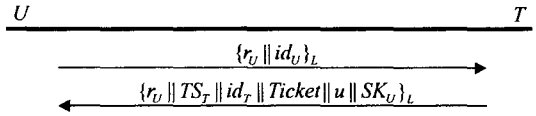

그림 2. 티켓 획득 프로토콜

U는 난수 r_U를 생성하고 id_U와 함께 비밀 세션키 L로 암호화하여 T에게 전송한다. T는 전달받은 메시지를 복호화하여 티켓을 요청하는 id_U와 r_U를 얻는다. T는 U의 인증서 취소 여부를 파악하여 티켓과 id_U, r_U, TS_T, 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.

3.3 티켓 기반의 인증 및 지불 프로토콜

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

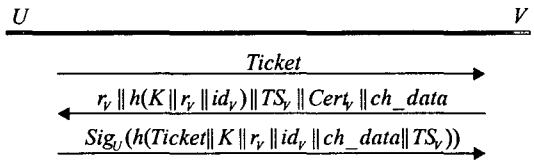

그림 3. 티켓 지불 프로토콜

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 $K=h(g^{uv} \| r_V)$을 계산한다. 그런 후에 V는 난수 r_V을 생성하여 두 번째 메시지를 U에게 전송한다. 메시지를 전송받은 U는 $Cert_V$로부터 g^v를 획득하여 V와 동일한 세션키 K를 계산한다. 그리고 해쉬값을 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 서비에게 U의 서명이 기재된 티켓을 제출하고 제공한 서비스에 대한 지불을 얻는다.

4. 제안하는 인증 및 지불 프로토콜

4.1 시스템 구성 모델

본 논문에서는 제안하는 시스템은 이동 사용자, VASP, 브로커로 구성되어 있다. 이들은 아래 그림과 같이 인증서 발급 단계, 지불/정보 전달 단계, 결제 단계를 수행하면서 m-Commerce를 실현한다.

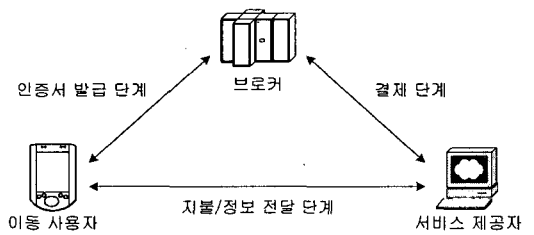

그림 4. 시스템 구성 모델

4.2 인증서 발급 단계

U는 키 설정 공개키 g^u, 서명 관련 키 쌍인 PK_U, SK_U를 생성하여 B에게 상호 인증된 안전한 채널로 전송한다. B는 U에게 지불 생성의 권한을 부여하는 인증서 $PayCert$를 발급한다.

$$PayCert=\{Sig_U(h(id_B \| TN_U \| g^u \| PK_U)) \| id_B \| TN_U \| TS_B \| g^u \| PK_U\}$$

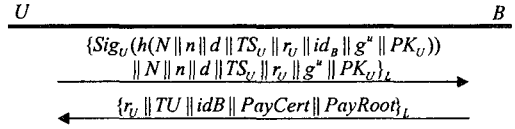

그림 5. 인증서 발급 프로토콜

B는 U와 수립하고 있는 비밀 세션키 L을 이용하여 $TN_U=h(L \| r_B \| id_V)$를 계산하고 아래와 같이 임의의 T_N을 선택하여 $i=N-1,\ldots,0$에 대한 해쉬 체인을 수행한다. 이와 같이 생성된 $PayRoot$는 U가 생성한 지불되지 않은 첫 번째 해쉬 체인 값과 연동하여 root 값으로 사용함으로써 $PayRoot$의 수만큼 다중 지불을 할 수 있게 한다.

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

4.3 지불 및 결제 단계

제안하는 지불 프로토콜은 U와 B간의 상호 인증 및 지불 정보를 교환하는 지불 초기화 프로토콜과 해쉬 체인을 사용하는 소액지불 기법을 이용하여 지불 정보를 전송하는 지불 프로토콜로 구분된다.

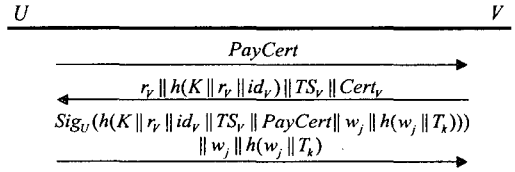

그림 5. 지불 초기화 프로토콜

인증서를 전달받은 V는 사용자와의 비밀 세션키 $K=h(g^{uv} \| r_V)$를 계산하고 r_V, K, id_V를 해쉬 함수로 처리하여 이를 TS_V와 $Cert_V$와 함께 U에게 전송한다. 메시지를 수신한 U는 V의 인증서를 검증하고 V와의 비밀 세션키 K를 계산한다. U가 이전까지 거래한 $k-1$ 번째 V에게 지불한 전자 화폐가 w_{j-1}이라고 가정하면 현재 거래 중인 k 번째 V와의 거래에서 지불되지 않은 첫 번째 해쉬 값인 w_j가 새로운

root 값으로 설정된다. *PayRoot*와 해쉬 함수를 수행한 $h(w_j \| T_k)$는 w_j가 k 번째 VASP에게 사용되는 root 값임을 나타낸다. U는 이러한 지불 요소들과 *PayCert*, r_V, K, id_V가 포함된 메시지를 비밀 서명키 SK_U로 서명하여 V에게 전송한다. 메시지를 전달받은 V는 *PayCert*를 검증하고, PK_U로 U의 서명을 검증하여 이후에 U가 지불할 전자 화폐에 대한 정당성을 확보하고, 해쉬 함수를 통해 이를 인증한다.

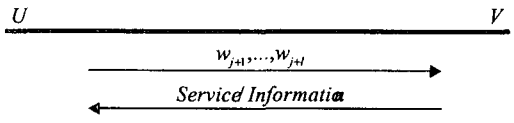

그림 6. 지불 프로토콜

V는 마지막 지불 값인 $P_{j+l}=(w_{j+l}, j+l)$과 *PayCert*, w_j, $h(w_j \| T_k)$를 저장하고 결제 단계에서 브로커에 이를 제출하여 지불 요구한다.

5. 성능 평가

5.1 안전성 분석

- 상호 인증 : U에게 전송되는 $h(K \| r_V \| id_V)$는 V에 대한 함축적 키 인증성과 개체 인증성에 대한 요구사항을 만족시킨다.
- 부인 방지 : 사용자는 공개키 인증서에 자신의 서명을 증명할 수 있는 공개키를 넣고 이를 root 값과 함께 전송하기 때문에 사용자는 제공받은 서비스에 대하여 부인할 수 없다.
- 익명성 : *PayCert*의 TN_U는 사용자의 익명성을 제공한다. 이는 브로커만이 알고 있기 때문에 제3자가 이를 획득한다 할지라도 사용자의 신원을 확인할 수 없다. VASP는 단지 PK_U로 사용자의 서명을 검증할 뿐이다.
- 이중 지불 탐지 :사용자가 생성하는 전자 화폐의 root 값으로서 w_j가 사용되며 이것은 거래 중인 VASP에 대한 *PayRoot*와 연동되어 있기 때문에 사용자가 이를 이중으로 지불하게 된다면 브로커가 이를 탐지할 수 있다.
- 위조 방지 : 사용자가 생성하는 전자 화폐는 오직 브로커만이 생성할 수 있는 *PayCert*로부터 인증받기 때문에 이를 위조할 수 없다.

5.2 효율성 분석

지불 과정에서 사용자와 VASP가 수행하는 지수 연산의 횟수로 프로토콜의 효율성을 평가한다. 이러한 결과가 표 2와 표 3에 나타나 있다.

표 2. 사용자의 계산량 비교

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

표 3. 서비스 제공자의 계산량 비교

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

6. 결론

본 논문에서는 종단간의 이동 사용자와 VASP와의 안전한 통신을 위한 인증 및 지불 프로토콜을 제안하였다. AIP 프로토콜은 VASP와 거래할 때마다 새로운 지불 정보를 생성하여야 하며, 티켓 기반의 프로토콜은 사용자의 비밀 서명키 쌍을 티켓 서버가 생성하기 때문에 보안상의 큰 문제점을 야기시킬 수 있다. 제안한 논문에서는 이러한 문제점을 해결하는 효율적인 방법을 제시하고 있으며 이는 이동 통신 시스템에 적합한 메커니즘을 제공한다.

참고문헌

[1] UMTS Forum, "A Regulatory Framework for UMTS," Report No.1, 1997.

[2] B.R.Lee, S.S.Kang, T.Y.Kim, "Ticket-Based Authentication and Payment Protocol for Mobile Telecommunications Systems," PRDC, 2001.

[3] ACTS AC095, ASPeCT Deliverable D20, Project final report and results of trials, Dec. 1998.

[4] R.Rivest, A.Shamir, "PayWord and MicroMint: two simple micropayment schemes," LNCS, Vol.1189, pp.69-87 Springer-Verlag, 1996.