무선 인터넷에서 신뢰할 수 있는 과금 시스템

장석철[†] · 이임영[††]

요 약

무선 이동통신 관련서비스가 활성화되면서 유료 컨텐츠 서비스에 대한 지불을 어떻게 처리할 것인가가 중요한 사안으로 대두되고 있다. 컨텐츠 사업자들은 현재 일부 서비스부터 컨텐츠 유료화를 시작하려 하고 있지만 사용자로부터 결재 금액을 지불 받을 수 있는 시스템을 갖추고 있지 않아 유료화를 시작하는데 어려움이 있다. 또한 사용자와 사업자간의 인증 및 사용자에 대한 개인 프라이버시 보호와 거래에서 발생할 수 있는 보안상의 고려사항들을 어떻게 해결할 것인가에 대한 문제가 있을 수 있다. 따라서 본 논문에서는 이러한 상거래 시장 변화에 맞추어 무선 인터넷에서 과금 시스템의 개념을 알아보고, 데이터 전송시 필요한 키 분배와 통신 상호간의 인증을 어떠한 방법으로 처리 할 것인가 설명한다. 이를 바탕으로 신뢰할 수 있는 과금 시스템을 제안한다.

The Trustable Billing System for Mobile Internet

Seok-Cheol Jang[†] and Im-Yeong Lee[††]

ABSTRACT

As the mobile communication related services are becoming popular, the payment issues on charging for the content services are getting more and more attention. Many contents providers are having difficulties for correctly charging services they provide, because they do not have appropriate payment systems yet. There are also the privacy protection issues, security problems that arise during transactions, and the authentication issues for both the user and the business, to be taken care of. In this paper, the billing system in the mobile internet environment will be discussed. Topics related to the key distribution for exchanging data, and the authentication mechanism for communications will be discussed. Based on this, a trustworthy billing system will be proposed.

Key words: *Mobile Internet, Mobile Commerce, Secure Billing System, Electronic Payment, Authentication*

1. 서 론

현재 무선인터넷은 IT관련업계의 새로운 화두로 부상하고 있다. 인터넷과 이동 통신의 접목을 통해 인터넷의 개념이 유선에서 무선으로 확장되었다. 무선인터넷의 가장 큰 장점은 언제 어디서나 이용할 수 있다는 효용성에 있다. 이러한 장점 때문에 무선 인터넷시장이 급변하고 있다.

기술발전과 인터넷에 대한 이용자의 폭발적 증가에 힘입어 간단한 메시지 송수신 단계에 머물던 무선 인터넷 서비스는 이제 기업 업무용으로까지 서비스 폭이 넓어지고 있다.

국내 이동전화 이용인구는 2800만명으로 이들은 무선인터넷의 거대한 잠재수요층을 형성하고 있다. 따라서 현재 1600만에 달하는 PC기반 인터넷 이용인구를 조만간 능가할 것으로 전망되고 있다. 만약 2800만명이라는 사용자가 무선인터넷을 이용하여 컨텐츠를 구입하려한다면 엄청난 시장이 형성될 것이다. 그리고 현재 컨텐츠를 무료로 제공하고 있는 무선통신 사업자들에게 이러한 사항은 그냥 놔둘 수 없는 매력적인 사업 아이템을 제공하고 있다. 따라서 이들 사업자들은 분명히 컨텐츠를 유료화 할 것으로 예상

[†] 준회원, (주) 인포크립트 연구소 연구원
[††] 정회원, 순천향대학교 정보기술공학부 부교수

된다.

무선인터넷 시장에서 컨텐츠 사업자들의 컨텐츠 유료화에 따른 수익 창출에 대한 기대가 모아지고 있는 가운데 무선상거래(mobile commerce)가 이슈로 부각되고 있다.

무선 이동통신 관련서비스가 활성화되면서 유료 컨텐츠 서비스에 대한 지불을 어떻게 처리할 것인가가 중요한 사안으로 대두되고 있다. 컨텐츠 사업자들은 현재 일부 서비스부터 컨텐츠 유료화를 시작하려 하고 있지만 사용자로부터 결재 금액을 지불 받을 수 있는 시스템을 갖추고 있지 않아 유료화를 시작하는데 어려움이 있다. 또한 사용자와 사업자간의 인증 및 사용자에 대한 개인 프라이버시 보호와 거래에서 발생할 수 있는 보안상의 고려사항들을 어떻게 해결할 것인가에 대한 문제가 있을 수 있다.

따라서 본 논문에서는 이러한 상거래 시장 변화에 맞추어 무선 인터넷에서 과금 시스템의 개념을 알아보고, 데이터 전송시 필요한 키 분배와 통신 상호간의 인증을 어떠한 방법으로 처리 할 것인가 설명한다. 이를 바탕으로 신뢰할 수 있는 과금 시스템을 제안한다.

2. 무선 인터넷에서의 과금 시스템

유선인터넷에서 과금 시스템이란 가스료, 전기료, 수도료, 신문구독료 등 우편으로 배달되는 각종 요금 고지서 내용을 인터넷으로 조회하고 안방에서 전자지불시스템을 이용해 손쉽게 결제할 수 있도록 해주는 서비스를 말한다. 즉 요금 청구 및 결제에 대한 인터넷 원스톱(one-stop) 서비스를 말한다.

무선인터넷에서 과금 시스템이란 유선인터넷에서 과금 시스템 개념을 그대로 무선 인터넷 환경으로 바꾸어 놓은 것이다. 즉 요금 청구 및 결제를 컴퓨터가 아닌 이동통신기기를 이용하여 언제 어디서나 편리하게, 전자지불 시스템을 이용하여 결제를 하는 것을 말한다. 이제까지의 과금 시스템은 사용자가 이동통신망에 접속한 시간을 체크하여 요금을 부과해 왔다. 하지만 현재의 시스템으로는 이용자가 통신망에 접속해 어떤 정보를 얼마동안 이용했는가를 일일이 알아내기 어렵다. 이를 해결하기 위해 많은 연구가 진행중에 있다.

일반적으로 무선인터넷 과금 시스템의 구성은 단말기, 트랜잭션 채널, 어플리케이션 서버, 트랜잭션 수행자, 지급결제 어플리케이션 등으로 구성된다. '트랜잭션 채널'이란 트랜잭션 처리를 위한 데이터 통신을 수행함에 있어 사용되는 물리적 네트워크를 말하는 것으로, 블루투스, 이동통신네트워크, 인터넷 등이 이에 해당한다. '어플리케이션 서버'란 소비자에 대응되는 개념으로 물건이나 서비스를 판매하는 가상 객체를 의미한다. '트랜젝션 수행자'는 거래의 쌍방을 대신에 과금과 대금송부 업무를 수행하는 주체를 의미한다. '지급결제 어플리케이션'은 지급결제 방식으로 e-Purse, Phone Bill, 직불카드 등, 다양한 방식이 존재한다.

무선인터넷 과금 시스템에서는 위와 같은 일반적인 구성요소 이외에 솔루션을 구성하는 다음의 4가지 요소가 존재한다.

• 계좌간 이체모형

일반적으로 유선 인터넷에서 존재하는 신용카드 및 직불카드를 이용한 SSL방식의 지급결제시스템과 유사한 것으로, 소비자는 무선인터넷 상점에서 자신의 신용카드나 직불카드 번호를 입력하면 머천트 서버에서 PG(Payment Gateway)를 통해 과금처리를 수행하는 방식이다.

• WBPP 및 직불카드 모형

WBPP(Wireless Bill Presentation & Payment) 모형은 유선 인터넷에서의 EBPP(Electronic Bill Presentation & Payment)를 이동통신 네트워크를 통해 수행하는 것을 의미한다.

EBPP서버에서 과금정보를 이동통신 네트워크를 통해 소비자에게 보내며, 소비자는 휴대폰 스크린을 통해 이를 확인하며, 결제여부 및 방식을 결정하여 송부하면, EBPP서버는 이를 처리하는 형태를 띈다.

• e-Purse 모형

e-Purse는 휴대폰에 착탈되는 IC카드와 같은 칩(chip)에 실질적인 가치를 저장시킨 다음, 저장된 가치만큼 지불결제에 사용하는 방식을 의미한다. e-Purse를 통해 소비자는 타인에게 가치 이전이 가능하고 기타 상점에서도 직불카드와 비슷하게 지급결제를 수행할 수 있다. 그러나 휴대폰 및 칩을 분실할 경우, 저장된 가치도 분실하게 되는 보안상의 위험이 존재한다.

• Phone Bill 모형

이동통신사업자가 은행 및 신용카드 회사 등, 기존 금융권에 비해 비교우위를 갖는 모형으로서, 이동

통신사업자 대 고객과의 이동통신요금 과금관계를 확장한 것이다. 휴대폰을 통해 물품 구입시 머천트는 과련 정보를 이동통신사업자의 빌링 시스템에 송부하게 되고, 이동통신사업자는 이동전화서비스 사용요금 이외에 별도의 항목을 만들어 이에 대한 과금을 대행한다. 즉, 과거 신용카드가 수행하던 업무를 이동통신사업자가 대신 수행하게 됨을 의미한다. 현재 무선인터넷 과금 시스템으로 가장 많이 확산된 모형이다.

3. 무선 과금을 위한 요구사항

일반적으로 무선 통신에서 사용되는 과금 시스템의 모델은 소액지불 시스템에 기반하고 있다. 이는 무선 통신상에서 적은 연산량과 충분한 안전성을 제공하므로 현재 많은 연구가 진행 중이다.

이를 기초로 무선 통신에서 사용되는 과금 시스템의 요구사항을 살펴보면 다음과 같다[1-3].

• 인증성

지불 금액은 명시된 사람만이 확인을 해야한다.

• 정확성

지불 금액의 총계는 지불자가 사용한 내용과 일치해야 한다.

• 확인성

징수자 입장에서 보면 징수자는 지불 금액을 정확히 확인을 해야 한다.

• 부인봉쇄

지불자는 검증된 지불 금액에 대해 부인을 할 수 없어야 한다.

4. 기존방식

다음에서는 기존에 제시되고 있는 무선 환경에서의 안전한 과금 프로토콜에 대해서 설명한다.

4.1 UMTS 방식

이 방식은 UMTS(Universal Mobile Telecommunications System)와 같은 제 3세대 이동 통신 시스템에서 요구되는 요금 부과 분야를 지원하는 안전한 과금 프로토콜이다. 이 방식은 ASPeCT(Advanced Security for Personal Communications Technologies) 프로젝트에 의해 수행되었으며, 1997년에 실연되었다[3].

UMTS에서 안전한 과금을 수행하기 위한 기본적인 ASPeCT 프로토콜은 이동 사용자와 VASP(Value-Added Service Provider) 간에 일어난다. 이 방식의 궁극적인 목적은 사용자가 통신을 통해 수행한 valued-added 서비스의 총합에 대한 정확한 과금 정보를 설정하는 것이다.

이 방식에서 사용되는 지불 메커니즘의 기본적인 설계 원칙은 value-added 서비스 비용이 매우 적어야하고, 서비스 부과에 따르는 통신 및 프로세싱 비용들은 최소가 되어야 한다. 따라서 적합한 지불 메커니즘으로서 micropayment 기법을 채택하였다. 전자상거래상에서 높은 보안성을 유지하기 위해 사용되는 암호기법은 계산량이 많아서 속도가 느리며 시스템의 부하도 크다. 즉 이것은 거래를 위한 처리비용이 비싸다는 것을 의미한다. 따라서 1달러 미만과 같은 소액 거래에 적합하지 않기 때문에 전자상거래를 위한 최소한의 보안을 유지하고 처리비용을 줄여서 소액 거래가 가능하도록 하는 지불 메커니즘이 micropayment 기법이다. ASPeCT에서 적용되는 micropayment 기법은 tick payment 프로토콜을 이용한다. 여기서 tick개념은 micropayment를 만들기 위해 일방향 해쉬함수 F의 원상(pre-image)을 사슬로 사용하는 것이다. 이를 이용한 응용프로토콜들은 PayWord, NetCard, iKP를 기반으로하는 micropayment와 PayTree이다. 이들 응용프로토콜의 기본 아이디어는 매우 간단하다.

• 과정 1 : 사용자는 안전한 랜덤값 α_0를 선택하여 총 사용할 지불 금액인 α_n를 다음과 같이 계산한다. 여기서 F는 일방향 해쉬함수이고, n은 해쉬를 취한 횟수이다.

$$\alpha_n = F^n(\alpha_0)$$

• 과정 2 : 징수자는 최초로 사용된 요금 d_1을 사용자에게 전달한다.

• 과정 3 : 사용자는 지불 토큰 α을 다음과 같이 계산하여 징수자에게 전달한다.

$$\alpha = F^{n-d_1}(\alpha_0)$$

• 과정 4 : 징수자는 사용자로부터 받은 값을 다음과 같이 확인한다.

$$\alpha^d = F^{(n-d_1)+d_1}(\alpha_0) = \alpha_n$$

마찬가지로 다음 사용 요금을 지불하기 위해서 위

와 같은 방법을 되풀이하면 되며 n을 넘어서지 않는 범위 내에서 지불이 이루어진다. 이 기법을 사용하는 가장 큰 이유는 적용이 용이하며, 제안된 인증 프로세스와 조화를 이룰 수 있기 때문이다.

복잡한 네트워크 상에서 공개키를 적용하기 위해서는 PKI(Public Key Infrastructure)를 필요로 한다. 이 방식에서는 TTP(Trusted Third Party)가 이동통신 사용자들과 VASP와 같은 요소들의 인증을 위해 CA로 활동한다.

본 방식은 크게 2단계로 구성되고 있으며, 다음의 시스템 변수들을 포함한다.

1) 시스템 변수

이 방식에서 사용되는 시스템 변수는 다음과 같다.

- $\{M\}_K$: 키 K를 이용해 M을 암호화
- $h1$, $h2$, $h3$: 128비트 일방향 해쉬 함수
- g: 생성자
- id_U: 사용자 식별값
- id_V: VASP 식별값
- id_{TTP}: TTP 식별값
- cid_U: 사용자에 대한 인증서 식별자
- cid_V: VASP에 대한 인증서 식별자
- $RND_{\{U,V\}}$: 사용자(U)또는 VASP(V)가 선택한 랜덤값
- $CertV$: VASP의 공개키 인증서
- TT: 타임 스탬프
- $CertChain(A, B)$: A가 B의 인증된 공개키를 검증하는 것
- ch_data: 통신정보
- IV 및 α_T: 지불 단계 초기화에 필요한 요소들
- $Sig_{\{U,T\}}(\bullet)$: $\bullet$에 대한 사용자(U) 또는 TTP (T)의 서명

2) 인증과 초기화 단계

이 단계는 두 가지 일반적인 목적을 갖는데 첫 번째는 사용자와 VASP간의 다양한 인증 방식을 허용하는 것이며, 두 번째는 지불 단계를 초기화하는 것이다. (그림 1)은 인증 및 초기화 단계 흐름을 표현하고 있다.

사용자는 랜덤수, TTP의 식별자와 암호화된 사용자 식별자로 구성된 AuthReq를 VASP에게 제공한다. VASP는 TTP에게 사용자에 대한 인증을 요구한다. TTP는 VASP에게 응답 메시지 TTPRes를 전송

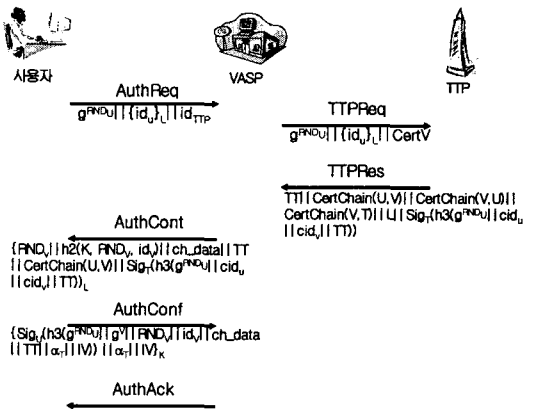


그림 1. 인증과 초기화 단계

한다. 이를 받은 VASP는 사용자에게 랜덤수, 통신정보와 분배키 등으로 구성된 AuthCont를 전송한다. 사용자는 지불단계초기화에서 필요한 요소들과 사용자 서명값으로 구성된 AuthConf를 전송한다. 이를 받은 VASP는 사용자에게 승인 정보 AuthAck을 보낸다.

3) 지불 단계

지불 단계는 value-added 서비스에서 지불 청구를 위한 메커니즘을 기술한다. 이 단계의 목적은 사용자에 대한 VASP가 최종 과금 합계를 완벽하게 생성하는 것이다. 그 외의 부가적인 목적은 사용자가 청구서에 기술된 지불 정보의 총합이 정확함을 확인할 수 있어야 하며, 오직 약정되는 VASP만이 지불을 받을 수 있어야 한다. VASP는 제시된 요청서에 대해 사용자가 부정 할 수 없게끔 해야 하며, 청구서에 기입된 지불금을 받았다는 것을 확인시킬 수 있어야 한다. 마지막으로 UMTS 서비스 제공자는 지불에 있어 투명성을 제공하기 위해 과금 정보가 정확한지 검증할 수 있어야 한다.

이 지불 단계는 초기화 과정에서 VASP는 다음의 정보를 갖는다고 가정한다.

- IV: 해쉬 함수를 정의하기 위해 사용되는 초기 벡터값
- $\alpha_T = F_{IV}^T(\alpha_0)$: 사용자가 랜덤하게 선택한 α_0와 해쉬함수 F_{IV}를 이용하여 tick의 최대수인 T만큼 해쉬를 수행한 값

사용자는 α_T와 관련된 정보를 통해 유닛 서비스에 대한 지불을 수행한다. 그림 2는 지불단계에 대한

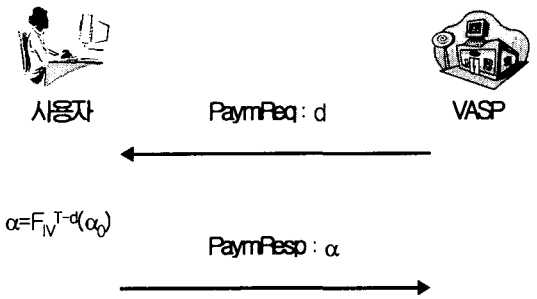


그림 2. 지불 단계

흐름을 기술하고 있다.

VASP는 최초 지불 유닛 d를 사용자에게 전송을 한다. 사용자는 지불 관련 정보 $\alpha = F_{IV}^{T-d}(\alpha_0)$를 계산하여 VASP에게 전달한다.

한 세션이 끝날 경우, VASP는 현재 프로토콜 수행 시 과금 요청을 위해 가장 최근에 수신한 지불관련 정보 α와 사용자에 의해 생성된 tick 수 T를 저장한다.

4) UMTS 분석

UMTS 방식은 통신횟수가 4회로 사용자와 기지국 사이에 통신 횟수에 대해 비효율적이다. 즉, 통신 횟수 측면에서 사용자의 부담을 가중시키고 있다.

지불단계에서는 사전에 사용자가 사용할 수 있는 tick의 최대의 수 인 T만큼 해쉬를 취해야 한다. 이는 처리 능력이 떨어지는 단말기에 부담을 줄 수 있다.

5. 제안방식

본 제안 방식은 사용자의 통신 효율성을 획득하기 위해 2-way 방식을 적용한다[4]. 무선 인터넷 과금 시스템은 사용자(M), 기지국(BSi)과 인증 기관(CA)로 구성된다.

본 제안 방식은 세 개의 단계로 나누어진다. Call-Set-up 단계, Hand-off 단계과 지불 단계이다.

5.1 시스템 변수

본 제안 방식에서 사용되는 시스템 변수는 다음과 같다.

- M_key: CA에 의해서 생성된 마스터키
- hash(): 안전한 일방향 해쉬 함수
- D_ID: 이동통신기기의 식별값
- C_key: CA에 의해서 생성된 통신키
- r': 사용자에 의해서 선택된 세션 랜덤 수
- S_key: 사용자의 세션키
- ID: 사용자 ID
- pw_M: 이동통신기기상에서 사용자의 패스워드
- r_M: 사용자 M에 의해서 생성된 랜덤수
- r_{Bi}: 기지국 BSi에 의해서 생성된 랜덤수
- T_i: 타임스탬프 ($i = 1,\cdots,n$)
- BS_i: 기지국 i
- SK: M과 BSi 사이의 무선 통신 키
- DB_{otp}: BSi에 대한 이중 구조 one-time 패스워드 DB
- OTP_{i1}, OTP_{i2}: DB_{otp} 연결 패스워드와 세션키 복원 패스워드
- P_{BSi}: BS_i의 공개키
- P_{ID_M}: ID_M의 공개키
- CF: 지불 금액 발생 조건
- $Sig_{BS_i}(\ )$: BS_i의 디지털 서명
- cnt_i: 사용자가 스스로 서명을 수행해 전송할 수 있는 지불 시스템 상에서의 최대 unit 수
- C_{cnti}: 지불 단계에서 필요한 지불 토큰
- $Cert(*)$: *의 인증서

5.2 키 분배 및 Call Set-Up 단계

본 단계는 기지국 i에서 무선 인터넷을 수행하기 위해 사용자와 기지국 사이에 키 분배 및 인증을 수행하는 단계이다. 또한, 이 과정을 통해 지불 단계 초기화에 필요한 요소들이 서로 공유한다.

- 과정 1

디바이스를 구입하기 위해 사용자 M은 자신의 ID_M과 패스워드 pw_M을 물리적인 방법으로 인증기관 CA에게 등록한다.

- 과정 2

CA는 M_key를 생성하고 다음과 같이 C_key를 계산한다.

$$C\_key = hash(D\_ID \| M\_key)$$

그리고 C_key, D_ID, ID_M과 pw_M을 사용자 M에 의해서 사용하게 될 이동통신기기에 저장하고, CA는 이동통신기기를 사용자 M에게 주고 안전한 방법으로 BSi에게 M_key를 보낸다.

- 과정 3

사용자 M은 이동통신기기를 받으면 자신의 ID_M

와 pw_M를 입력하여 이동통신기기 안에 저장된 정보와 비교하여 사용자 인증을 수행한다.

• 과정 4

사용자 M은 세션 랜덤수 r'을 생성하여 메시지 암호 세션키 S_key를 다음과 같이 계산한다.

$$S\_key = hash(r' || C\_key)$$

그리고 이것을 반으로 나누어서 첫 번째 부분을 FS_key로 하고 나머지는 LS_key로 한다.

또 지불에 필요한 초기값 α_0을 생성하고 지불 토큰 C_{cnti}를 다음과 같이 계산하여 저장한다.

$$C_{cnt_i} = hash(\alpha_0 || cnt_i)$$

사용자 M은 랜덤수 r_M을 생성하여 다음과 같이 FS_key를 이용하여 암호화한다.

$$FS\_key(D\_ID || r_M || T || CF || \alpha_0 || cnt_i || C_{cnt_i})$$

그러면 사용자는 다음과 같이 계산하여 BSi에게 보낸다.

$$D\_ID || r' || FS\_key(D\_ID || r_M || T || CF || \alpha_0 || cnt_i || C_{cnt_i}) || Cert_M$$

• 과정 5

사용자로부터 받은 메시지에서 BSi는 다음과 같이 C'_key와 S_key를 계산한다.

$$C'\_key = hash(D\_ID || M\_key)$$

$$S\_key = hash(r' || C\_key)$$

그리고 공개보드에 있는 D_ID와 C_key를 위에서 계산한 D_ID와 C'_key을 비교한다. 만약 맞으면 정당한 사용자로 인정한다.

• 과정 6

BSi는 다음과 같이 계산하여 무선통신키 SK_i를 계산한다.

$$r_M || T_i || (r_{B_i} * P_{BS_i})$$

$$SK_i = hash(r_M || T_i || (r_{B_i} * P_{BS_i}))$$

그리고 OTP_{i2}을 가지고 SK_i, r'과 D_ID를 암호화하여 OTP_{i1}을 사용하여 DB_{otp}에 저장한다.

• 과정 7

BSi는 $r_{B_i} || T_i || SK_i$에 서명을 한 후 LS_key를 이용하여 암호화한 다음에 사용자에게 송신한다.

$$LS\_key(Sig_{BS_i}(r_{B_i} || T_i || SK_i) || Cert(P_{BS_i}))$$

• 과정 8

사용자 M은 BSi로부터 받은 메시지를 LS_key로 복호화하고 Sig_{BS_i}과 $Cert(P_{BS_i})$를 이용하여 BSi를 인증한다.

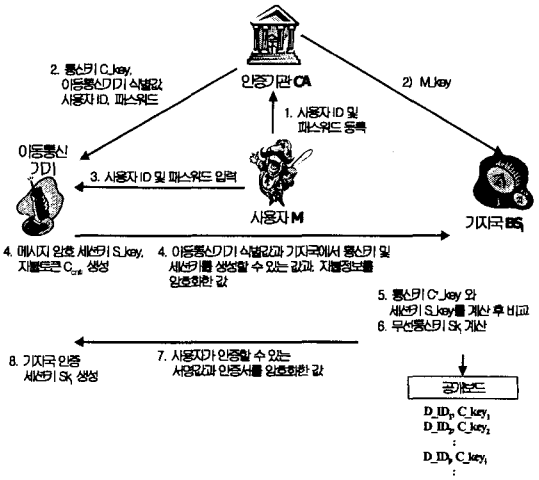


그림 3. 키 분배 및 Call Set-up 단계

• 과정 9

사용자는 다음과 같이 무선 통신 키 SK_i'를 계산하여 SK_i와 비교하여 맞으면 키 분배와 Call Set-up 단계를 종료한다.

$$SK_i' = hash(r_M || T_i || (r_{B_i} * P_{BS_i}))$$

5.3 Hand-Off 단계

무선 인터넷의 특징은 사용자가 이동하면서 사용할 수 있다는 것이다. 즉 사용자가 현재 기지국의 셀 범위에서 다른 기지국의 셀 범위로 이동할 수 있다는 것을 의미한다. 따라서 기지국간의 이동시 인증과 새로운 키를 생성하기 위해 서로 반드시 Hand-Off 단계가 이루어져야 한다. 마찬가지로 과금 시스템에서도 사용자와 새로운 기지국간에 지불에 대한 확인 절차가 필요하다. 다음은 Hand-Off 단계를 설명한 것이다.

• 과정 1

BSi는 사용자의 움직임을 확인 후 새로운 기지국 BS_{i+1}을 선택한다. 그리고 새로운 기지국 BS_{i+1}에게 지불 금액 발생 조건인 CF, DB_{otp} 세션키 복원 패스워드인 OTP_{i2}, 지불 초기값 α_0, 사용자가 스스로 서명을 수행해 전송할 수 있는 지불 시스템 상에서의 최대 unit 수인 cnt_i 와 지불토큰 $Ccnt_i$를 안전한 방법으로 보낸다.

• 과정 2

기지국 BS_{i+1}는 CF를 확인하고, DB_{otp}에서 OTP_{i2}

과 $OTP_{(i+1)1}$를 사용하여 무선 통신키 SK_i, 랜덤값 r'과 이동통신기기 식별값 D_ID를 가져온다.

• 과정 3

BS_{i+1}는 다음과 같이 CA에 의해서 생성된 통신키 C_key와 사용자의 세션키 S_key를 계산한다.

$$C\_key = hash(D\_ID||M\_key)$$

$$S\_key = hash(r'||C\_key)$$

• 과정 4

BS_{i+1}는 $SK_i||T_{i+1}||(r_{B_{i+1}} * P_{BS_{i+1}})$를 생성하고 새로운 무선 통신 키 SK_{i+1}을 계산한다.

$$SK_{i+1} = hash(SK_i||T_{i+1}||(r_{B_{i+1}} * P_{BS_{i+1}}))$$

• 과정 5

BS_{i+1}는 $r_{Bi+1}||T_{i+1}||SK_{i+1}$에 지불과 관련된 정보 cnt_i를 포함해서 서명을 한 후, LS_key를 이용하여 암호화시켜 사용자 M에게 보낸다.

$$LS_{key}(Sig_{BS_{i+1}}(r_{Bi+1}||T_{i+1}$$

$$||SK_{i+1}||cnt_i)||Cert(P_{BSi+1}))$$

• 과정 6

사용자는 BS_{i+1}으로부터 받은 메시지로부터 LS_key를 이용하여 복호화시킨다. 그리고 지불 정보를 이용하여 다음을 계산하고 C_{cnti}과 C'_{cnti}을 비교하여 맞으면 지불에 대한 정보가 정확히 BSi로부터 전송되었다는 것을 확인한다.

$$C'_{cnt_i} = hash(\alpha_0||cnt_i)$$

그리고 BS_{i+1}의 서명을 확인한다.

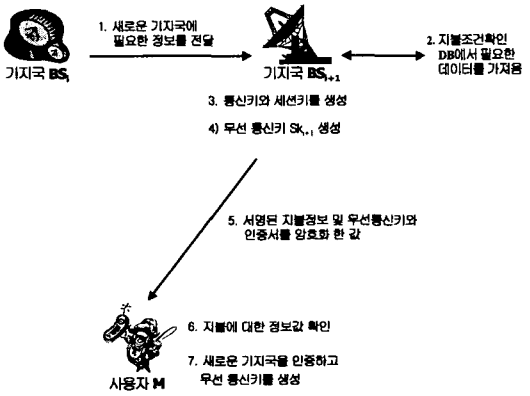


그림 4. Hand-Off 단계

• 과정 7

사용자는 새로운 무선 통신 키를 다음과 같이 만든다.

$$SK'_{i+1} = hash(SK_i||T_{i+1}||(r_{B_{i+1}} * P_{BS_{i+1}}))$$

그리고 SK_{i+1}과 비교하여 맞으면 Hand-Off 단계를 끝맞친다.

5.4 지불 단계

본 단계는 Call Set-up 단계에서 이미 이루어진 지불에 관련된 시스템 변수를 사용하여 과금 시스템과 사용자간에 지불이 이루어지는 단계이다. 지불 단계의 자세한 설명은 다음과 같다.

• 과정 1

과금 시스템 키 분배 및 Call Set-up 단계에서, 사용자는 지불 토큰 $Ccnt_i$을 다음과 같이 계산하여 지불 금액 발생 조건인 CF, 지불 초기값 α_0, 사용자가 스스로 서명을 수행해 전송할 수 있는 지불 시스템 상에서의 최대 unit 수인 cnt_i, C_{cnti}를 전송해 주어야 한다. 사용자는 전송하기 전에 α_0와 cnt_i을 저장한다.

$$C_{cnt_i} = hash(\alpha_0||cnt_i)$$

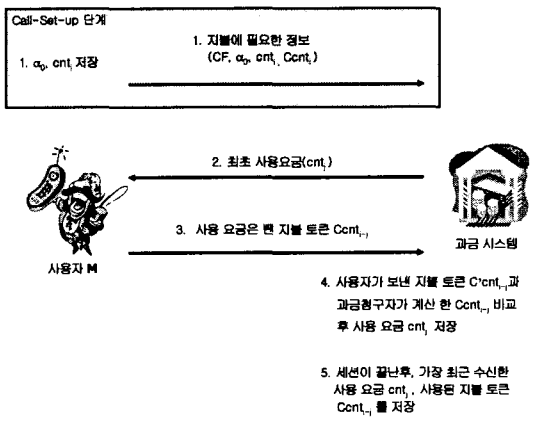


그림 5. 지불 단계

• 과정 2

실질적인 지불 단계가 실행되는 과정으로써, 과금 시스템은 최초 사용 요금에 해당하는 cnt_i를 선택하여 사용자에게 전송한다.

• 과정 3

사용자는 과금 시스템이 보낸 최초 사용 요금 cen_t을 이용하여 지불 토큰 $C_{cnt_{i-j}}$을 다음과 같이 계산하여 과금 시스템에게 전달한다.

$$C_{cnt_{i-j}} = hash(hash(\alpha_0||cnt_i)||hash(cnt_j))$$

• 과정 4

과금 시스템은 메시지를 받은 후에 $C'_{cnt_{i-j}}$을 다음과 같이 계산한다.

$$C'_{cnt_{(i-j)}} = hash(C_{cnt_j} || hash(Ccnt_j))$$

그리고 과금 시스템이 계산한 지불토큰인 $C'_{cnt_{i-j}}$와 사용자로부터 받은 지불토큰인 $C_{cnt_{i-j}}$가 일치하는지 확인 후 일치하면 최초 사용 요금 cnt_j를 저장한다.

• 과정 5

세션이 끝난 후, 과금 시스템은 현재 단계 수행시 과금 요청을 위해 가장 최근에 수신한 사용 요금인 cnt_j값과 사용자에 의해 사용되는 지불 토큰 $C_{cnt_{i-j}}$를 저장한다.

6. 제안방식 분석

본 제안방식은 효율성을 높이기 위해 키 분배 및 인증시 2-way 방식을 적용했다. 또한 사용자의 이동성을 고려하여 Hand-off 단계를 적용했다. 지불단계에서는 UMTS 방식에서 여러번의 해쉬를 수행해야 하는 문제점을 해결하고 있다. 다음은 기존방식과 제안방식을 비교 분석한 결과이다.

• 효율성

UMTS 방식은 통신횟수가 4회로 사용자와 기지국 사이에 통신 횟수에 대해 비효율적이다. 하지만 제안 방식은 UMTS 방식에 비해 통신횟수가 2회로 감소함으로써 효율성이 향상되었다. 또한 지불단계에서 UMTS 방식은 사용자가 스스로 서명을 수행해 전송할 수 있는 지불 시스템 상에서의 최대의 unit 수를 만들기 위해 그만큼에 해쉬를 수행해야하지만 본 방식에서는 두 번에 해쉬를 수행함으로서 지불이 이루어지므로 매우 효율적이라 할 수 있다.

• 인증성

사용자와 과금 시스템은 사전에 인증기관을 통해 인증을 수행하므로, 과금 시스템에서 요구사항인 인증성을 만족한다. 즉, 지불 금액에 명시된 사람인 사용자와 과금 시스템만이 확인을 할 수 있다. 하지만 UMTS 방식의 지불과정에서는 인증을 수행하지 않으므로 인증성을 제공하지 않고 있다.

• 정확성 및 확인성

지불 단계에서 과금 시스템은 사용자로부터 받은 지불 정보로부터 $C'_{cnt_{i-j}}$을 계산하여 $C_{cnt_{i-j}}$과 비교함으로서 과금 시스템은 지불 금액을 정확히 확인을 할 수 있다. 이러한 확인 절차를 통해 지불 금액의 총계는 지불자가 사용한 내용과 반드시 일치한다.

• 신뢰성

제안방식에서의 신뢰성은 크게 두 가지로 나누어질 수 있다. 첫 번째는 무선인터넷에 서의 신뢰성이다. 사용자는 정확한 과금 정보를 제공받아야 하며, 또한 이를 정확하게 확인할 수 있어야 한다. 그리고 사용자와 과금 시스템 사이의 인증을 통해 신뢰된 사용자와 과금 시스템이라는 것은 확인할 수 있어야 한다. 만약 이러한 부분이 확인되지 않을 경우, 사용자와 과금 시스템 사이의 신뢰성은 떨어지게 된다. 두 번째로 지불시스템의 신뢰성이다. 이를 제공하기 위해서는 이중사용방지를 할 수 있어야 한다. 제안방식에서는 무선 과금을 위한 요구사항으로서 인증성, 정확성, 확인성 및 부인봉쇄를 만족하므로 첫 번째 신뢰성에 대해 만족한다. 그리고 지불과정에서 해쉬함수와 과금 시스템의 DB에 저장된 과금 정보의 비교를 통해서 이중사용여부를 판단할 수 있으므로 지불시스템의 신뢰성을 만족한다. 하지만 UMTS 방식에서 지불과정에서는 인증과정을 거치지 않으므로 신뢰성 부분에서 미흡하다. 표 1은 UMTS 방식과 제안방식을 비교 분석한 결과를 보여주고 있다.

7. 결 론

인터넷의 등장으로 인해 수많은 변화가 일어났다. 사람들이 자기가 원하는 정보를 찾기 위해 도서관을 찾아가는 것이 아니라 앉은자리에서 컴퓨터 네트워

표 1. UMTS 방식과 제안방식 비교표

항목 / 방식	효율성		인증성	정확성 및 확인성	부인봉쇄	신뢰성
	통신횟수	해쉬 횟수				
UMTS방식	×(4-way)	×(T번)	×	△	○	△
제안방식	○(2-way)	○(2번)	○	○	○	○

×: 약함, △: 보통, ○: 좋음

크를 이용하여 원하는 정보를 손쉽게 구할 수 있게 되었다. 통신 수단의 변화에 의해서 이제는 각자의 핸드폰을 통해서 의사소통을 하고 있다. 하지만 사람들은 이에 만족하지 않고 인터넷을 생활 속에 일부분이 된 핸드폰에 접목시킴으로써 무선 인터넷이 보편화되었다. 이는 유선에서 행해졌던 모든 일이 무선으로 전환된 것을 말한다.

이러한 흐름 속에서, 상거래 개념도 변화하여 무선에서도 자기가 원하는 컨텐츠를 구입할 수 있는 시대가 도래하였지만, 유선에서와 마찬가지로 개인정보 유출 즉, 개인 프라이버시 침해와 과금 관련 기술의 적용이라는 새로운 문제를 야기시켰다.

이에 본 논문은 무선인터넷에서 사용자와 기지국간의 키 분배와 상호인증을 통해 안전성과 효율성을 높이고 지불관련 기술에서 신뢰할 수 있는 과금 시스템을 제안하였다. 하지만 기지국의 개입으로 사용자의 과금 정보 및 키에 대한 정보를 기지국에 노출됨으로서 악의적인 공격자가 기지국을 공격할 때 사용자의 정보가 누출될 우려가 있다. 향후, 이 분야에 대한 관심 속에서 다각적으로 심도 있는 연구가 진행되리라 본다.

참 고 문 헌

[1] G.Horn and B.Preneel, "Authentication and Payment in Future Mobile Systems", Technical Report ESAT-COSIC Report 98-2, Department of Electrical Engineering, Katholieke, Universiteit Leuven, 1998.

[2] K. Martin, B. Preneel, C. Mitchell, H. Hitz, G. Horn, A. Poliakova, and P. Howard, "Secure billing for mobile information services in UMTS", 5th International Conference in Services and Networks, IS&N'98, LNCS 1430, Springer-Verlag, pp. 535-548, 1998.

[3] G.Horn, P.Howard, K.M.Martin, C.J.Mitchell, B.Preneel and K.Rantos, "Trialling Secure Billing with Trusted Third Party Support for UMTS Application"

[4] Hee-un Park, Im-yeong Lee, Doo-soon Park, "A 2-pass key agreement and authentication for mobile communication", ICEIC2000, pp. 115-118. 2000.

[5] A. Aziz, W.Diffie, "Privacy and Authentication for Wireless Local Area Networks", IEEE Personal Communications, 1st Q 1994, pp. 25-31.

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

[7] ETSI SMG SG DOC 73/95, "A public key based protocol for UMTS providing mutual authentication and key agreement".

[8] R. Hauser, M. Steiner, M. Waidner, "Micro-payments based on iKP", Presented at SECURICOM 96.

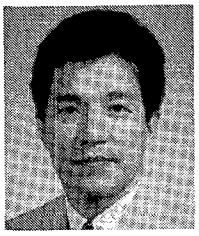
[9] ITU, "Security Principles for Future Public Land Mobile Telecommunication System", Rec. ITU-R M. 1078.

[10] L.R. Knudsen, B. Preneel, "One-way functions for tick payments", in preparation.

[11] H. Lin, L. Harn, "Authentication in Wireless Communications", Proc. GLOBECOM 1993.

장 석 철

1999년 2월 선문대학교 수학과 졸업
2002년 2월 순천향대학교 전산학 전공 석사
2002년 2월~6월 (주)코웰시스넷 부설연구소 연구원
2002년 7월~현재 (주)인포크럽트 연구소 연구원
관심분야 : 암호이론, 네트워크 보안, 전자상거래 보안



이 임 영

1981년 8월 홍익대학교 전자공학과 졸업
1986년 3월 오사카대학 통신공학과 석사
1989년 3월 오사카대학 통신공학과 박사
1989년 1월~1994년 2월 한국전자통신연구원 선임연구원
1994년 3월~현재 순천향대학교 정보기술공학부 부교수
관심분야 : 암호이론, 정보이론, 컴퓨터 보안