무선 인터넷에서 신뢰할 수 있는 과금 시스템

장석철, 박희운, 이임영
순천향대학교 정보기술공학부

The Trustable Billing System for Mobile Internet

Seok-cheol Jang, Hee-un Park, Im-yeong Lee
Division of Information Technology Eng. Soonchunhyang Univ.

요 약

최근 무선 통신 관련 서비스가 활발하게 이루어짐으로써 새로운 종류의 서비스들이 많이 등장하고 있다. 하지만 사업자 측에서 이러한 서비스를 제공하고 사용자로부터 요금을 받을 수 있는 과금 시스템이 아직까지는 미흡한 수준이다.

따라서 본 논문에서는 이러한 상거래 시장 변화에 맞추어 무선 인터넷에서 과금 시스템의 개념을 알아보고, 무선 인터넷 환경에서 안전하고 신뢰할 수 있는 과금 시스템을 제안한다.

1. 서론

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

기술발전과 인터넷에 대한 이용자의 폭발적 증가에 힘입어 간단한 메시지 송수신 단계에 머물던 무선인터넷 서비스는 이제 기업 업무용으로까지 서비스폭이 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 무선 통신 사업자들에게 이러한 사항은 그냥 놔둘수 없는 매력적인 사업 아이템을 제공하고 있다. 따라서 이들 사업자들은 분명히 컨텐츠를 유료화할 것으로 예상된다.

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

* 본연구는 정보통신부의 대학 S/W 연구 센터 지원 사업에 의해 수행된 것임.

구선 이동통신 관련서비스가 활성화되면서 유료 컨텐츠 서비스에 대한 지불을 어떻게 처리할 것인가가 가장 중요한 선결조건이 되고 있다. 컨텐츠 사업자들이 현재 제공하는 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. 무선인터넷에서의 과금 시스템이란?

유선인터넷에서 과금 시스템이란 가스료, 전기료, 수도료, 신문구독료 등 우편으로 배달되는 각종 요금 고지서 내용을 인터넷으로 조회하고 안방에서 전자지불시스템을 이용해 손쉽게 결제할 수 있도록 해주

는 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 진행중이고 있다. 또 무선 이동통신의 2.5세대 기술인 IS95C 서비스 실시 후 데이터 송수신 방법도 현재의 서킷방식에서 패킷방식으로 변환할 것으로 예상됨에 따라 이를 지원하는 과금 시스템도 마련될 것으로 보인다. 서킷방식은 이용자가 이통망에 접속해 있는 동안 이통사업자와 이용자의 단말기가 계속 연결돼 접속시간을 기반으로 요금을 매긴다. 반면 패킷방식은 데이터를 패킷 단위로 보내주므로 사용한 데이터 양만큼 과금할 수 있다. 따라서 이용자들은 무선인터넷 이용시 현재보다 훨씬 더 저렴할 것으로 여겨진다.

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 진행중이다.

이를 기초로 무선 통신에서 사용되는 과금 시스템의 요구사항을 살펴보면 다음과 같다[1][2][3].

- 인증성
  지불 금액은 명시된 사람만이 확인을 해야한다.
- 정확성
  지불 금액의 총계는 지불자가 사용한 내용과 일치해야 한다.
- 유일성
  징수자만이 지불자가 낸 금액을 받을 수 있다.
- 확인성
  징수자 입장에서 보면 징수자는 지불 금액을 정확히 확인을 해야 한다.
- 부인봉쇄
  지불자는 검증된 지불 금액에 대해 부인을 할 수 없어야 한다.

4. 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 프로토콜로 나누어진다. Call-Set-up 프로토콜, Hand-off 프로토콜과 지불 프로토콜이다.

가. 시스템 변수

- M_key : CA에 의해서 생성된 마스터키
- hash() : 안전한 일방향 해쉬함수
- D_ID : 이동통신기기의 식별값
- C_key : CA에 의해서 생성된 통신키
- r' : 사용자에 의해서 선택된 세션 랜덤 수
- S_key : 사용자의 세션키
- ID_M : 사용자 ID
- pw_M : 이동통신기기상에서 사용자의 패스워드
- r_M : 사용자 M에 의해서 생성된 랜덤수
- r_{B_i} : 기지국 BS_i에 의해서 생성된 랜덤수
- T_i : 타임스탬프 (i=1, 2, ..., n)
- BS_i : 기지국 i
- SK : M과 BS_i 사이의 무선 통신 키
- DB_{otp} : BS_i에 대한 이중 구조 one-time 패스워드 DB
- OTP_{i1}, OTP_{i2} : DB_{otp} 연결 패스워드와 세션키 복원 패스워드
- P_{BS_i} : 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
- Cert(*) : *의 인증서

나. 키 분배 및 Call Set-Up 프로토콜 단계

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

- step 1

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

- step 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 BS_i에게 M_key를 보낸다.

• step3

사용자 M은 이동통신기기를 받으면 자신의 ID_M와 pw_M를 입력하여 이동통신기기 안에 저장된 정보와 비교하여 사용자 인증을 수행한다.

• step4

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_{cnt_i}를 다음과 같이 계산하여 저장한다.

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

사용자 M은 랜덤수 r_M을 생성하여 다음과 같이 FS_key를 이용하여 암호화 한다.

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

그러면 사용자는 다음과 같이 계산하여 BS_i에게 보낸다.

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

• step 5

사용자로부터 받은 메시지에서 BS_i는 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.

• step 6

BS_i는 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.

• step 7

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

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

• step 8

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

• step 9

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

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

다. Hand-Off 프로토콜 단계

무선 인터넷 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 프로토콜이 이루어져야 한다. 마찬가지로 과금 시스템에서도 사용자와 새로운 기지국간에 지불에 대한 확인 절차가 필요하다. 다음은 Hand-Off 프로토콜 단계를 설명한 것이다.

• step 1

BS_i는 사용자의 움직임을 확인 후 새로운 기지국 BS_{i+1}을 선택한다. 그리고 새로운 기지국 BS_{i+1}에게 CF, OTP_{i2}, α_0, cnt_i, C_{cnt_i}를 안전한 방법으로 보낸다.

• step 2

BS_{i+1}는 CF를 확인하고, DB_{otp}에서 OTP_{i2}과 $OTP_{(i+1)1}$를 사용하여 SK_i, r', D_ID를 가져온다.

• step 3

BS_{i+1}는 다음과 같이 C_key와 S_key를 계산한다.

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

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

• step 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.

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

• step 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.

$$LS_{key}(Sig_{BS_{i+1}}(r_{Bi+1} || T_{i+1} || SK_{i+1} || cnt_i) || Cert(P_{BSi+1}))$$

• step 6

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

전송되었다는 것을 확인한다.

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

그리고 BS_{i+1}의 서명을 확인한다.

• step 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 프로토콜을 끝맞친다.

라. 지불 프로토콜 단계

• step 1

과금 시스템 키 분배 및 Call Set-up 단계에서, 사용자는 C_{cnt_i}을 다음과 같이 계산하여 CF, α_0, cnt_i, C_{cnt_i}를 전송해 주어야 한다.

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

사용자는 전송하기 전에 α_0와 cnt_i을 저장한다.

• step 2

과금 청구자는 최초 사용 요금에 해당하는 cnt_j를 선택하여 사용자에게 보낸다.

• step 3

사용자는 청구자가 보낸 cnt_j을 $C_{cnt_{i-j}}$를 다음과 같이 계산하여 청구자에게 전달한다.

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

• step 4

청구자는 받은 메시지를 이용하여 C'_{cnt_i}을 다음과 같이 계산한다.

$$\begin{aligned} C_{cnt_{(i-j)+j}} &= hash(\alpha_0 || cnt_{(i-j)+j}) \\ &= hash(\alpha_0 || cnt_i) \\ &= C'_{cnt_i} \end{aligned}$$

그리고 C'_{cnt_i}과 C_{cnt_i}이 일치하는지 확인 후 일치하면 cnt_j를 저장한다.

• step 5

Call-Setup 과정이 끝난 후, 청구자는 현재 프로토콜 수행시 과금 요청을 위해 가장 최근에 수신한 cnt_i값과 사용자에 의해 사용되는 C_{cnt_i}를 저장한다.

마. 제안방식 분석

본 제안방식은 효율성을 높이기 위해 키 분배 및 인증시 2-way 방식을 적용했다. 또한 사용자의 이동성을 고려하여 Hand-off 프로토콜을 적용했다.

과금 수행시 기존 방식은 여러번의 해쉬를 수행해야하지만 본 방식에서는 한번의 해쉬을 함으로써 무선인터넷에서 효율성을 높일 수 있다. 동시에 사용자의 이동성을 고려하지 않은 기존 방식에 비해 본 방식은 기지국의 교환이 있더라도 과금관련 정보를 안전하게 다음 기지국으로 전송할 수 있다.

5. 결론

인터넷의 등장으로 인해 수 많은 변화가 일어났다. 사람들이 자기가 원하는 정보를 찾기 위해 도서관을 찾아가는 것이 아니라 앉은 자리에서 컴퓨터 네트워크를 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 생활속에 일부분이 된 핸드폰에 접목시킴으로써 무선 인터넷이 보편화되었다. 이는 유선에서 행해졌던 모든 일이 무선으로 전환된 것을 말한다.

따라서 상거래 개념도 변화하여 무선에서도 자기가 원하는 컨텐츠를 구입할 수 있게 되었다. 이는 유선에서와 마찬가지로 개인 정보 유출 즉 개인 프라이버시 침해와 과금 관련 기술의 적용이라는 새로운 문제를 야기시켰다.

이에 본 논문은 무선인터넷에서 사용자와 기지국 간의 키 분배와 상호인증을 통해 안전성과 효율성을 높이고 지불관련 기술에서 신뢰할 수 있는 과금 시스템을 제안하였다.

[참고문헌]

[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, 1998, pp. 535-548.

[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, pp115-118 2000