모바일 통신에서 상호 신뢰할 수 있는 과금 시스템에 관한 연구†

신제용*, 김순석*, 김성권*

*중앙대학교, 컴퓨터공학과

Study on Trusted Billing System in Mobile Communication

Je-Yong Shin*, Soon-Seok Kim*, Sung-Kwon Kim*

*Department of Computer Science & Engineering, Chung-Ang Univ.

요 약

이동 통신 기술의 발달로 시공간을 초월하여 인터넷에 접속할 수 있게 되었다. 그리고 현재 국내에서도 무선 인터넷 사용이 가능한 단말기의 보급이 크게 늘어나면서 새로운 다양한 서비스를 제공받을 수 있다. 기존의 문자, 벨소리 혹은 이미지를 전송 받을 수 있는 기술을 넘어 이제는 게임을 즐기거나 음악, 동영상 등의 서비스를 제공받을 수 있는 수준에 있다. 따라서 서비스를 제공하는 콘텐츠 제공자와 무선 단말기로 서비스를 이용하는 사용자 사이에 서비스 이용에 따른 과금의 필요성이 대두되고 있다. 그러나 현재와 같이 콘텐츠 제공자나 네트웍 제공자의 로그 정보만으로 요금을 부과하는 것은 문제가 있다. 따라서 사용자에게 부과된 요금에 대해서 사용자와 콘텐츠 제공자가 상호 신뢰할 수 있는 과금 시스템의 개발이 절실히 요구된다.

I. 서론

1. 등장 배경

인터넷은 이미 사회, 문화, 경제 등 여러 가지 측면에서 인류의 삶에 큰 영향을 미쳤다. 이러한 인터넷은 현재 우리 생활과 떨어져서는 상상할 수 없는 위치에 있다. 또 90년대 초반부터 널리 보급된 호출기에서 시작하여 핸드폰, PCS를 거쳐 상용화될 IMT2000[1]과 같은 이동 통신 기술의 발달로 언제, 어디서나 인터넷의 접근이 가능하게 되었다.

무선 단말기의 발전은 무선 인터넷 서비스를 앞당기는 견인차 역할을 담당했다. 무선 단말기를 통해 여러 가지 부가 서비스를 이용할 수 있는 방향으로 발전하고 있으며, 이동 통신 단말기를 이용하여 PDA나 네트웍 연결을 필요로 하는 많은 기기에 연결이 가능하게 되었다. 그리고 단순히 음성 메시지를 송수신하는 획일적인 이동 통신 단말기가 아닌 음성과 영상을 함께 사용 가능하게 해주는 멀티미디어 단말기, 자료의 처리와 저장을 가능하도록 해주는 고성능의 단말기, 네트웍을 이용해 실시간으로 게임을 즐길 수 있는 단말기 등이 개발되고 있다.

2. 연구의 필요성

위에서 살펴본 바와 같이 무선 단말기의 보급이 확대되고 또 이를 활용할 수 있는 서비스의 개발이 활발히 진행되고 있다. 그리고 서비스를 제공하는 콘텐츠 제공자와 무선 단말기로 서비스를 이용하는 사용자 사이에 일어나는 서비스 이용에 따른 과금에 대한 필요성이 대두되고 있다. 현재와 같이 일방적으로 콘텐츠 제공자의 로그 정보에만 의존해서 작성되는 요금 통지는 바람직하지 않다. 실제로 사용자가 이용한 시간이나 횟수와 다르게 과금이 되는 경우가 있기 때문이다. 만약 악의를 가진 콘텐츠 제공자에 의해서 로그 정보가 조작될 수 있다. 이런 경우 사용자는 자신이 이용한 서비

† 본 연구는 한국과학재단 목적기초연구 R01-2000-00401 지원으로 수행되었음.

1) 국가별로 개별 운영되고 있는 다양한 이동전화 시스템의 규격의 통일

스에 대해서 어떤 증거를 어떻게 제시해야하는가 하는 문제가 발생한다. 만약 증거를 제시하기 위해서도 많은 노력이 필요하다. 따라서 서비스 이용자와 콘텐츠 제공자 사이에 신뢰할 수 있는 과금 시스템이 필요하다. 또 무선 단말기를 이용한다는 특수한 상황에 알맞은 과금 시스템을 제안하는 것이 중요하다.

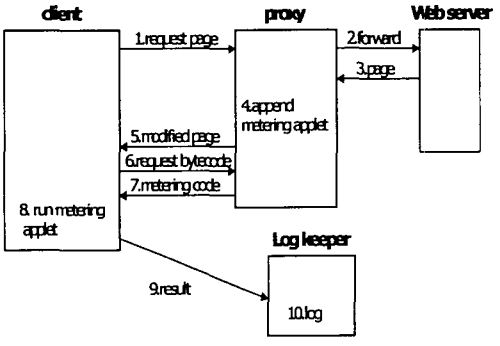
II. 본문

1. 관련 연구

본 논문에서 제안하는 방법과 관련된 연구는 무선 인터넷과 관련된 프로토콜, 인터넷과 관련된 방문자에 대한 측정, 무선 단말기를 이용하여 외부 도메인에서 통신을 할 경우에 대한 과금 시스템에 관련된 논문들이 있다. 아직까지 콘텐츠 제공자와 무선 단말기를 이용한 서비스 사용자 사이에서 발생하는 과금 문제에 대한 연구가 미비한 상태이다. 따라서 위에서 언급한 여러 연구들을 통해서 콘텐츠 제공자와 무선 단말기를 이용해서 서비스를 이용하는 사용자 사이에 신뢰할 수 있는 과금 시스템을 제안하기로 한다.

1) 인터넷에서 방문자 측정에 관한 연구

방문자를 측정하는 방법으로서 가장 기본적인 방법은 전자서명을 이용하는 방법이다. 제 3의 신뢰할 수 있는 기관이 방문할 고객과 방문자 수를 측정하는 서버 각각에게 서명키와 공개키를 분배한다. 그리고 방문자가 해당 서버를 방문했을 경우에 전자서명 프로토콜을 수행한다. 그리고 서버는 방문자들로부터 받은 서명 목록을 가지고 광구주에게 확인을 받는다. 이 방법은 서명을 이용하므로 정확하게 방문자 수를 측정할 수는 있지만 전자서명을 이용하므로 방문자에게 많은 계산량을 필요로 하게 된다. 다른 방법으로는 방문자가 서버에 접속했을 때 일정 시간 동안 주어진 계산을 수행하고 그 수행에 대한 결과값을 서버에게 전달하는 방법이다. 이러한 방법은 Dwork와 Naor[1]가 제안한 방법과 Franklin과 Malkhi[2]가 제안한 방법이다. 이 중에서 Franklin과 Malkhi[2]가 제안한 방법은 일정 시간 동안 계산을 수행하는 *timing function*을 이용하는데, 이 결과값으로 방문 사실과 이용 시간도 측정이 가능하다.



[그림 1] Franklin과 Malkhi[2]가 제안한 방법

2) 외부 도메인에서 무선 통신할 때 과금에 관한 연구

이동 통신을 이용하는 사용자와 통신 서비스 제공자 사이에서 사용자 자신에게 부과된 요금이 실제 사용량에 맞게 과금이 되었는지에 대해 분쟁이 일어날 수 있다. 이것을 좀더 확정해서 이동 통신 사용자가 외부 도메인에서 통신을 시도할 경우에 일어날 수 있는 요금 분쟁이 있다. 사용자는 자신이 등록된 도메인이 아닌 외부 도메인에서 로밍 서비스를 받을 경우에도 사용자에게 올바른 과금을 되도록 하는 방법이 필요하다. 사용자는 자신이 외부 도메인에 있더라도 통신을 할 수 있고, 자신이 등록된 도메인과 외부 도메인 사이의 통신을 통해서 올바른 사용자인지를 확인 할 수 있으며 또 사용자는 자신이 사용한 통화에 대한 증거를 외부 도메인에게 보낸다. 외부 도메인은 일정하게 서비스에 대한 요청을 하고 사용자는 이에 대한 증거를 계속 생성하여 전달한다. 이러한 메시지의 교환으로 나중에 요금에 대해서 사용자와 외부 도메인 사이에 상호 부인을 방지할 수 있는 방법을 제안했다.[3]

2. 업계 동향

유무선 콘텐츠에 대한 과금 시스템에 대한 중요성이 부각되면서 여러 업체들이 과금 시스템을 내놓고 있다. 대표적인 회사로서 티비 소프트[4], 퓨처테크[5], 애드빌 소프트[6] 등이 있다. 기존에는 인터넷에서 방문자 측정 및 통계에 관련된 연구를 해오던 회사들이며 현재는 콘텐츠 과금에 관심을 기울이고 있다.

3. 요구사항

무선 단말기를 이용한 과금 시스템은 다음과 같은 요구 사항을 가진다.

1) 단말기 브라우저에서 사용이 가능해야한다.

2) 사용자의 계산량을 최소화해야 한다.

3) 사용자는 콘텐츠 제공자가 제출한 사용 내역에 대해 판별 가능해야한다.

4) 여러 가지 과금 방법에 대한 지원이 가능해야한다.

5) 사용자의 익명성을 지원해야한다.

4. 제안하는 과금 방법

제안하는 방법이 안전하게 수행하기 위해서 다음과 같은 가정을 한다. 첫째, 무선 단말기의 내부에는 임의의 접근이나 변경이 불가능해야 한다. 둘째, 제 3의 신뢰할 수 있는 기관이 존재한다. 이 기관은 사용자의 개인키와 공개키를 저장하고 분배하는 역할을 한다. 셋째로는 사전에 신뢰할 수 있는 기관으로부터 사용자와 콘텐츠 제공자 사이에 키분배가 일어났다고 가정한다. 따라서 사용자와 콘텐츠 제공자 사이에 일어나는 일에 관심을 둔다.

[Notation]

User : 무선 단말기를 이용하여 콘텐츠 제공자가 제공하는 서비스를 이용하는 사용자

CP : 콘텐츠 제공자(Contents Provider)

UID : 사용자 ID

U_{sk} : 서명을 위한 사용자의 서명키

Time : 처음 서비스를 요구할 때의 시간

Service : 사용자가 콘텐츠 제공자에게 요구하는 서비스 명세

isAccepted : 콘텐츠 제공자가 사용자의 서비스 요구를 받아들일지를 나타냄.

S(X) : 메시지 X를 사용자의 서명키로 서명

f(X) : 메시지 X를 입력으로 해쉬(hash) 연산 수행. 사용하는 해쉬함수로는 MD5, SHA를 사용.

cur_time : CP가 User에게 전달하는 현재 시간

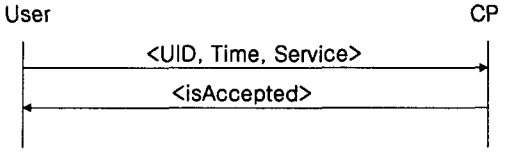
Proof Request : 일정시간이 지났을 때 콘텐츠 제공자가 사용자에게 사용에 대한 증거 요구

Data : 사용자가 콘텐츠 제공자에게 요청한 Service에 대해서 콘텐츠 제공자가 제공하는 자료

제안하는 방법은 다음과 같이 3단계로 구성된다.

[단계 1 Initialization]

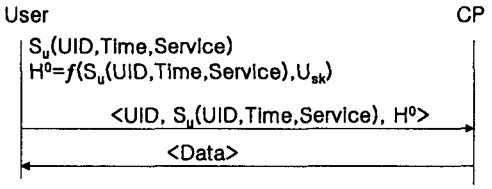
사용자는 자신의 UID, 서비스 시작 시간, 그리고 자신이 콘텐츠 제공자로부터 제공받을 서비스에 대한 명세를 생성하여 콘텐츠 제공자에게 보낸다. 콘텐츠 제공자는 사용자의 ID를 확인하고 서비스 제공 여부를 판단하여 사용자에게 전달한다.



[그림 2] 단계 1

[단계 2 Setup]

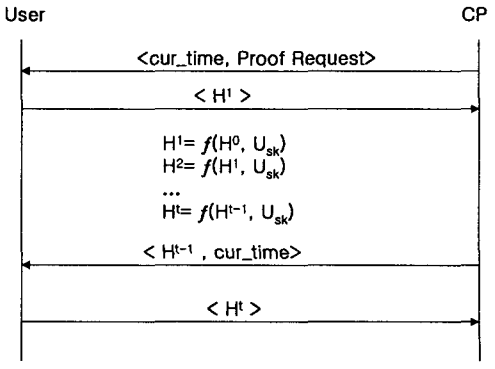
사용자는 UID와 서비스 시간 그리고 서비스 명세에 대해서 서명한다. 그리고 서명한 결과와 자신의 서명키를 연결하여 해쉬 연산을 수행한다. 콘텐츠 제공자에게 UID, 서명과 해쉬 결과를 함께 전달한다. 콘텐츠 제공자는 UID를 확인하고 사용자의 공개키로 서명을 확인한다. 받은 메시지에 이상이 없다면 사용자가 요구한 데이터를 전송한다. 그리고 사용자의 서명과 해쉬 값을 저장한다.



[그림 3] 단계 2

[단계 3 Regular]

일정 시간이 경과하면 콘텐츠 제공자는 사용자에게 이용에 대한 증거를 요구한다. 증거를 요구할 때는 현재 시간을 함께 보낸다. 사용자의 단말



[그림 4] 단계 3

기에서 현재 시간을 확인하고 해쉬 연산을 수행한다. 해쉬 연산은 이전 단계에서 생성한 해쉬값과 자신의 서명키와 함께 수행한다. 또 일정한 시간이 지나면 콘텐츠 제공자는 이용에 대한 증거를 다시 요구하게 된다. 이렇게 일정시간 단위로 반복적으로 수행된다. 마지막으로 콘텐츠 제공자는 마지막 해쉬값을 저장한다.

요금에 대한 분쟁이 일어났을 경우에 콘텐츠 제공자는 사용자로부터 받은 서명과 해쉬의 초기값과 마지막 값을 제시한다. 사용자는 서명을 확인하고 해쉬의 초기값과 마지막 값을 가지고 자신이 사용한 시간을 계산해 낼 수 있다.

5. 비교 분석

• 계산량

일정한 시간마다 증거를 생성하기 위해서 서명을 수행하는 경우와 비교해 보자. 단계 3에서 제안한 방법이 k번의 해쉬 연산을 한다면 서명을 이용한 방법은 k회의 서명을 수행해야 한다. Palm에서 암호 알고리즘을 수행한 결과가 표 1과 같다.[7] 따라서 사용자의 계산량이 줄어들어, 배터리 소모량도 줄일 수 있는 장점이 있다.

표 1: Palm에서 시간 측정

Algorithm	Time	Comment
DES encryption	4.9ms/blocks	4900ms for 1000 encryptions
SHA-1	2.7ms/blocks	2780ms for a 1000 long hash chain
512bit RSA sig. generation	7028ms	
512bit RSA sig. verify	438ms	e=3

• 효율성

MD5를 사용할 경우 일정하게 128 bit의 결과값을 생성하지만 RSA를 이용한 서명은 결과의 길이가 일정하지 못하다. 해쉬값의 작은 길이는 사용자와 콘텐츠 제공자 사이에 일어나는 통신량을 줄일 수 있다. 서명을 이용한다면 증거의 모든 자료를 콘텐츠 제공자와 사용자의 단말기에 저장해야하는 단점이 있다. 해쉬를 이용하여 초기 해쉬값과 마지막 값을 가지고 확인하는 것이 콘텐츠 제공자와 사용자 모두에게 효율적이다.

• 안전성

제안한 방법의 안전성은 사용하는 해쉬함수에 의존한다. 제안한 방법에서는 계산 속도 및 기타 조건에 따라서 MD5를 사용하거나 SHA를 사용해서 수행 할 수 있으므로 각 해쉬 함수의 안전성에 의존한다.

III. 결론

본 논문에서 사용자와 콘텐츠 제공자 사이에 믿을 수 있는 과금 시스템을 위해서 해쉬 함수를 이용하여 효율성과 안전성을 가지는 과금 방법을 제안하였다. 서명보다 빠른 연산으로 사용자의 계산량을 줄이고 또 콘텐츠 제공자에게 빠른 응답이 가능하도록 하였다. 그러나 자주 콘텐츠를 이용한다면 무선 단말기의 메모리 한계로 인해서 장기적인 사용에 많은 메모리가 필요하다. 그리고 사용자의 증거 요구가 빈번하게 일어난다면 단말기의 배터리 소모량에도 영향을 끼친다. 따라서 향후 연구 방향으로는 증거 생산과 저장을 믿을 수 있는 기관에게 위임하여 콘텐츠 제공자와 통신을 이루어지도록 하는 것이다. 이렇게 한다면 무선 단말기의 부담을 줄일 수 있다.

참고문헌

[1] C. Dwork and M. Naor, Pricing via Processing or Combating Junk Mail, *Crypto '92,* LNCS 576, pp. 114-128 1992.

[2] M. K. Franklin and D. Malkhi, Auditable metering with lightweight security, *Financial Cryptography '97,* LNCS 1318 pp. 151-160, 1997.

[3] Jianying Zhou and Kwok-Yan Lam, Undeniable Billing in Mobile Communication , *Mobile Computing and Networking*, pp. 284-290, 1998

[4] http://www.tobest.com

[5] http://www.futec.com

[6] http://www.adbillsoft.com

[7] Neil Daswani and Dan Boneh, Experimenting with Electronic Commerce on the PalmPilot, *Financial Cryptography*, pp. 1-16, 1999

[9] Horn and Preneel, Authentication and Payment in Future Mobile Systems, *ESORICS '98*, Springer-Verlag, 1998