이동 통신 사용자의 컨텐츠 교환을 위한 권한 관리 서비스

장경아° 이병래
삼성전자 소프트웨어센터
{kachang, byungrae.lee}@samsung.com

Rights Management Service for Contents Transfer of Mobile Users

Kyung-Ah Chang° Byung-Rae Lee
Software Center, Samsung Electronics

요 약

본 논문에서는 이동 통신 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 디지털 컨텐츠 제공자와의 연결을 고려하여 선택적 Proxy 서비스를 수용한 컨텐츠 교환 목적의 권한 관리 서비스 프로토콜을 제안하였다.

제안한 서비스는 이동 통신 사용자 기기의 한계적 능력에 대해 해당 도메인의 Proxy와 공개키를 기반으로 인증 서비스를 수행하도록 하였으며, 이후 종단 사용자는 해당 인증 결과를 기반으로 인터넷 기반의 디지털 컨텐츠 제공자와의 메시지 교환을 수행하도록 하였다.

또한 사전에 인터넷 기반 구조에 대한 컨텐츠 교환 서비스 요청에 한하여 Proxy의 부분적 서비스를 수행하도록 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다.

1. 서론

인터넷의 확장은 가정 내의 가전 기기와 자동화 기기에 대한 개인 정보 네트워크에 대해 정보 공유 및 외부의 제어가 가능한 형태로 발전하고 있으며, 이것은 근거리 무선 통신 기술의 실용화로 이동 통신 기기 기반 다종 기기간의 디지털 컨텐츠 교환을 활성화 시키게 되었다.

이에 대해 DRM(Digital Rights Management)의 대상이 되는 디지털 컨텐츠는 음악, 영화, 게임과 같은 멀티미디어 형식을 기반으로 'One-Source Multi-Use', 'Media Mix'로 대표되는 유형의 가공을 통한 다양한 효용성을 제어 해야만 한다.

가전 기기 또는 자동화 기기에 대한 네트워크를 통해 보다 강력한 사용자 편리성으로 PC, TV, Audio 등의 가정 기기를 하나로 통합한 개인 정보 네트워크에서 활용 가능하며, 이동 통신으로 자유로운 장소와 시간에 대해 디지털 컨텐츠 사용을 확산시키게 되었다. 또한 유선과 무선, 다양한 네트워크 구조를 통합한 엔터프라이즈 환경에서도 마찬가지로 B-2-B 컨텐츠의 사용이 활발히 진행중이다.

본 연구에서는 이동 통신 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 기존 네트워크와의 연결을 고려하여 선택적 Proxy 서비스를 수용한 권한 관리 서비스 프로토콜을 제안하였다.

제안한 서비스는 이동 통신 사용자 기기의 한계적 능력에 대해 해당 네트워크와 공개키를 기반으로 인증 서비스를 수행하도록 하였으며, 이후 사용자는 해당 인증 결과를 기반으로 디지털 컨텐츠 제공자와의 상호 메시지 교환을 위한 권한 관리 서비스 프로토콜을 수행하도록 하였다.

또한 사전에 디지털 컨텐츠 제공자에 대한 서비스 요청에 한하여 Proxy의 부분적 서비스를 수행하도록 허용하여 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다.

본 연구의 구성은 다음과 같다. 2장에서 이동 통신에서의 사용자 애플리케이션 플랫폼 및 Mobile DRM 관련 환경을 살펴본다. 3장에서는 해당 네트워크의 선택적 Proxy 서비스 구조를 수용하여 인증 수행 및 이후 인증 결과 정보를 기반으로 권한 관리 서비스 프로토콜을 제안한다. 마지막으로 4장에서 결론을 내리고 향후 과제를

제시한다.

2. 관련 연구

2.1 이동 통신에서의 사용자 플랫폼

이동 통신 기기에 대한 플랫폼은 사용자의 네트워크 기기 상에서 제공되는 서비스를 가능하게 한다. 이것은 이동 통신 플랫폼이 기기 내에서 구동하는 애플리케이션 뿐만 아니라, 서비스 제공 Back-End 시스템을 함께 포함한다고 할 수 있다. 또한 유/ 무선 통합 솔루션을 대상으로 이동 통신 기기 뿐만 아니라 유선 인터넷의 주요 플랫폼이라 할 수 있는 PC까지 포함하여 확장할 수 있다.

이러한 플랫폼은 기존 인터넷과는 차별화된 제한된 이동 통신 환경에 대한 지원 기술 및 비즈니스 모델을 적용하게 되며, 이동 통신 애플리케이션에서 보다 강조된 개인화(Personalization) 솔루션을 요구하게 된다. 또한 개인 사용자 대상의 플랫폼은 엔터테인먼트, 개인 정보 관리, 커뮤니케이션, 전자상거래 등을 제공하게 된다. 또한 대형 엔터프라이즈 어플리케이션들의 유/ 무선 통합 지원 확대와 다양한 기기와의 연결로 유/ 무선 인터넷 서비스 및 애플리케이션과의 통합을 가능하게 한다.

- 무선 메시징 서비스

  AOL-time warner는 Microsoft의 Mobile MSN에 대응하는 AOL Alerts 서비스를 통해 AOL 사이트에 접속 가능한 Mobile Communicator eMail 장비를 기반으로 스포츠 상황, 일기 예보, 주식 정보, 주요 뉴스 등을 eMail 또는 Instant Messenger로 이동중인 원격 사용자에게 제공하도록 하였다.

  또한 Mobile MSN과 AOL Alerts 서비스는 공통적으로 'Anywhere Anytime' 정책을 반영하며, 사용자의 main PC가 아닌 다른 장비로 interactive 서비스를 제공을 목표로 하고 있다.

- Mobile P-2-P(peer-to-peer)

  기존의 단순 메시지 전송 서비스는 Mobile MSN과 AOL Alerts 와 같은 인스턴트 메시징(IM)을 기반으로 무선 원격 제어 및 무선 컨텐츠 교환을 가능하게 할 것이다.

  따라서, 개인의 위치정보 및 신상 데이터 등 개인의 프라이버시와 관련된 PIMS가 악용될 수 있으며, 구조적인 네트워크 환경으로 인한 바이러스 감염이 가능하다. 또한 기존 인터넷의 Napster, Gnutella 등 P-2-P를 통한 컨텐츠의 불법 유통에 대한 DRM 시스템의 Mobile Network에 대한 적절한 적용 모델이 제시되어야 할 것이다.

2.2 Mobile DRM

이동 통신 환경은 유선 인터넷과는 다른 성격으로, 디지털 컨텐츠 사용에 대해 일반적으로 유선 인터넷에서는 유료 디지털 컨텐츠 이용에 적대적인 반면, 이동 통신에서는 원하는 디지털 컨텐츠에 대해 긍정적인 경향이 나타나고 있다.

그러나, MMS(Multimedia Messaging Service)가 가능해지면서 Rich Content에 대한 다양한 모델이 DRM을 기반으로 제시되어야 하며, 다양한 디지털 컨텐츠 교환 및 사용에 대한 표준의 제정이 필요하다.

이에 대해 3GPP 및 OMA(Open Mobile Alliance)에서는 이미 Mobile DRM의 중요성을 파악하여 표준화를 진행 중에 있다.

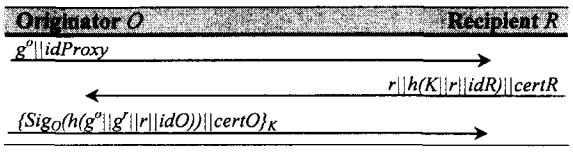
3. 이동 통신 사용자의 권한 관리 서비스

3.1 제안한 프로토콜의 개요

본 연구에서 제안하는 이동 통신 사용자의 권한 관리 서비스는 상호 인증 및 메시지 교환 과정으로 구성된다. 선택적 Proxy 서비스 수행을 기반으로 이동 통신 사용자 기기의 컴퓨팅 능력 및 대역폭에 대한 오버헤드에 대한 대단위 계산의 효율성을 증가시키도록 하였다.

본 논문에서는 이동 통신 환경에 대해 사용자의 컨텐츠 교환에 대한 관련 정보를 Proxy에 위탁하도록 하며, 인터넷 상의 디지털 컨텐츠 제공자와의 서비스 요청으로 초기화된다.

이동 통신 사용자 기기의 한계적인 컴퓨팅 능력을 고려하였을 때, 선택적 Proxy 서비스는 효율적이며, 이동 통신 사용자와 Proxy는 세션키를 공유하므로, 서비스 프로토콜의 종료 후, 단지 결과를 통보 받기만 하면 된다.



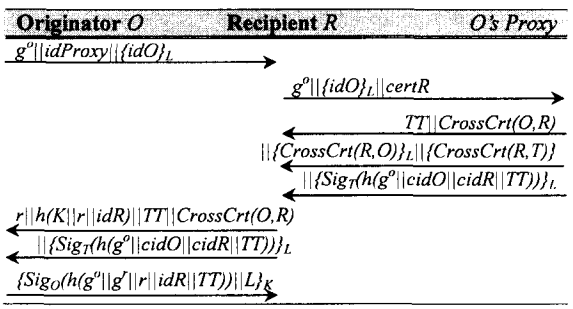
<그림 1> 기본 인증 프로토콜

본 논문에서 제안하는 보안 관리 서비스의 기본 인증 구조는 O가 난수 o를 생성하여 공개키 동의 키(public key agreement key) g^o와 함께 메시지를 교환하고자 하는 R의 해당 인증 기관 정보 id_caR를 R에게 전송하면서 시작된다.

이 메시지로는 R은 아직 통신 대상을 파악할 수 없으나 난수 r을 생성하여 전송 받은 정보를 $(g^o)^r$로 연산하여 세션키 K를 생성하여 해쉬화(h)한 후 R의 인증서 $certR$와 함께 전송한다. O는 $certR$를 통해 R의 공개키 정보 등을 파악할 수 있으며 자신의 신분 정보 idO와 함께 인증서 $certO$를 자신의 공개키로 서명한 후 다시 K로 암호화하여 전송하게 된다. 이후 R은 $certO$를 통해 O의 서명을 검증하게 되고 이 정보는 차후 서비스에 반영하도록 한다.

3.2 인증 수행 프로토콜

인증 프로토콜은 주체 O와 R이 상대방의 인증서 검증을 위해 해당 Proxy의 공개키 보유 및 해당 Proxy에 자신의 공개키에 대한 인증서 식별 정보($cidO$, $cidR$)를 인지하고 있음을 가정한다.



<그림 2> 제안한 인증 수행 프로토콜

인증 수행 프로토콜은 해당 도메인의 이동 통신 사용자로부터 위탁 받은 정보를 통해 Proxy O가 인터넷 상의 디지털 컨텐츠 제공자 R에게 자신의 네트워크 영역에 대한 Proxy 식별 정보 및 Proxy와의 공유 비밀키 L로 암호화된 자신의 식별 정보를 전송한다. 이 메시지를 R은 자신의 인증서($certR$)와 함께 O's $Proxy$에게 전달(forwarding)한다. 이때 O's $Proxy$는 $\{idO\}_L$를 복호화하여 현재 유용성을 확인하고 R의 인증서 적합성 역시 검증하여 인증을 수행하도록 한다.

인증서의 유용성이 검증된 경우, O's $Proxy$는 타임스탬프 TT와 O에 대한 범용 인증서($CrossCrt$)들과 검증된 인증서에 대한 고유 식별 정보 $cidO$, $cidR$를 서명하여 암호화한 후 R에게 전송한다. $CrossCrt$는 해당 도메인의 Proxy가 그 인증서에 서명하여 일반 인증서를 확장한 형태이다.

마지막으로 O가 받은 메시지의 서명을 검증하여 올바르다고 판단되었다면 O는 R에게 비밀키 L을 포함한 메시지를 세션키 K로 암호화하여 전송한다. R은 비밀키 L을 사용하여 O의 마지막 전송 단계 이후 Proxy로부터 받은 메시지를 복호화하고 그 서명을 검증할 수 있다.

3.3 메시지 교환 프로토콜

인증 이후 메시지 교환 프로토콜은 *Exchange*, *Abort*, *Resolve* 단계로 구성하였다. 정상적인 메시지 교환시 양자간 프로토콜로 구성된 *Exchange* 프로토콜만 실행되며, 서비스 주체 간의 프로토콜 수행에 대한 오류 판단으로 강제적 종료 및 검증을 요청할 경우, 선택적 Proxy 서비스를 실행하도록 하여 상대 주체의 정당성 여부를 결정한 후 프로토콜의 진행 여부를 결정하도록 하였다.

4. 결론 및 향후 과제

본 연구에서는 이동 통신 사용자 기기의 한계적 계산 능력 및 무선 링크의 대역폭과 기존 인터넷과의 연결을 고려하여 선택적 Proxy 서비스를 수용한 권한 관리 서비스 프로토콜을 제안하였다. 사전 인터넷 기반 구조에 대한 컨텐츠 교환 서비스 요청에 대한 Proxy의 부분적 서비스 수행은 시스템의 대단위 계산 능력에 대한 효율성을 보장할 수 있다

향후 본 논문에서 제안한 서비스에 대한 Mobile P2P로의 확장 연구 및 분석이 진행되어야 할 것이다.

참 고 문 헌

[1] N. Asokan and Victor Shoup, "Optimistic fair exchange of digital signatures",*EUROCRYPT '98, Springer-Verlag*, 1998.