Journal of Digital Contents Society Vol. 9 No. 1 March. 2008(pp. 69-75)

웹 기반 VOD 시스템을 위한 익명성이 제공되는 Pay-Per-View 서비스

주한규*

요 약

VOD (Video-on-Demand) 서비스는 사용자가 원하는 비디오를 언제든지 볼 수 있도록 해 준다. 고속의 컴퓨터 네트워크의 발달로 웹 기반 VOD 서비스가 가능하게 되었다. VOD 서비스를 지원하기 위해서는 요금 부과 기법이 필요하다. VOD 요금 부과 기법으로 사용자가 시청한 분량에 따라 요금을 부과하는 pay-per-view를 생각할 수 있다.

VOD에서 사용자의 사생활 보호 또한 중요한 이슈가 된다. 사용자는 자신의 시청 정보를 타인에게 노출시키고 싶지 않을 것이다. 이를 위해서 VOD 서비스에 익명성을 제공할 필요가 있다. 익명성 제공은 VOD 서비스 요금 계산을 복잡하게 한다. 익명성 제공과 요금 계산을 함께 지원하는 VOD 기법이 필요하다.

이 논문에서는 익명성이 제공되는 웹 기반 VOD 서비스가 제안된다. 제안된 기법은 사용자의 시청 분량에 따라 요금을 부과하는 pay-per-view 기능을 지원한다.

Anonymous Pay-Per-View Service for Web-Based Video-on-Demand Systems

Hankyu Joo*

Abstract

Video-on-demand (VOD) service allows subscribers to view any video whenever they want. With the development of the high speed computer networks, web-based VOD services are available. To support VOD services, charging scheme is necessary. Pay-per-view is an effective charging scheme for VOD services. Pay-per-view allows the subscribers to pay for what they have viewed.

Privacy is another important attribute for VOD services. The subscribers may not want to reveal what they have viewed to anyone including the VOD provider. Anonymity makes it complicated to calculate charge for the VOD service. An approach that achieves both anonymity and pay-per-view charge calculation is necessary.

In this paper, anonymous web-based VOD service is proposed. The proposed approach also gives pay-per-view capability.

Keywords : 웹 서비스, Video-on-Demand, Pay-Per-View, 익명성

1. 서론

VOD(Video-on-Demand) 서비스는 사용자가 원하는 비디오를 언제든지 볼 수 있도록 해 준다. 고속의 컴퓨터 네트워크의 발달로 웹 기반 VOD 서비스가 가능하게 되었다. VOD 서비스를 유료화할 경우 요금 부과 기법이 필요하다. VOD 요금 부과 기법으로 시청한 분량에 따라 요금을 부과하는 pay-per-view를 생각할 수 있다.

Pay-per-view 는 다시 두 종류로 나누어 생각할 수 있다. 하나는 각 비디오 프로그램에 일정 요금을 부과하는 것이고 다른 하나는 그 프

※ 제일저자(First Author) : 주한규
접수일자:2007년12월04일, 심사완료:2007년12월17일
* 한림대학교 정보통신공학부
hkjoo@hallym.ac.kr
▣ 본 연구는 한림대학교의 연구비 지원에 의하여 수행되었음.

로그램을 시청한 시간에 비례하여 요금을 부과하는 것이다. 비디오 프로그램 당 요금을 부과하는 방법은 간단하나 사용자 중심적이지 못하다. 시청 시간에 비례하는 방법은 사용자 중심적이나 구현하기 복잡하다. 시청 시간에 비례하여 요금을 부과하기 위해서는 사용자의 시청 시간을 정확하게 계산할 수 있어야 한다. 이 방법은 또한 사용자와 비디오 프로그램 제공자 모두가 악용할 수 없어야 한다. 실제 요금은 제공자에 의하여 계산되고 부과된다. 따라서 제공자가 부과된 요금이 정당함을 증명할 의무를 가진다. 동시에 제공자는 사용자의 사용 시간보다 적게 요금을 부과하고 싶지 않을 것이다.

사생활 보호 또한 VOD 서비스에서 제공되어야 할 속성 중의 하나이다. 사용자는 자신의 시청 정보가 VOD 제공자를 포함한 어느 누구에게도 알려지지 않도록 하고 싶을 것이다. 여러 분야에서 사생활 보호를 증진시키기 위한 익명성의 개념이 도입되고 있다[1][2]. 익명성은 자신의 신분을 드러내지 않고 원하는 서비스를 받을 수 있도록 한다. 익명성을 지원하는 경우 사용자는 자신의 신분을 제공자에게도 알리지 않고 비디오 프로그램을 시청하게 되며 이는 요금 계산을 복잡하게 한다. 비디오 프로그램 제공자는 사용자의 신분을 알지 못한 상태에서 사용 요금을 계산해야 한다.

이미 pay-per-view를 위하여 제안된 기법들이 존재한다[3][4]. 제안된 기법들은 사용자의 시청 시간을 정확하게 계산하고 그에 따라 사용 요금을 부과할 수 있도록 한다. 또한 제안된 기법은 임의의 공격자가 사용자의 시청 내용을 확인할 수 없도록 한다. 그러나 제안된 기법에서는 사용자는 시청을 위하여 자신의 정보를 제공자에게 전달하여야 하므로 서비스 제공자는 사용자의 시청 정보를 가질 수 있다.

본 논문에서는 익명성을 지원하는 웹 기반 pay-per-view 기법이 제안된다. 본 논문에서 제안하는 기법은 익명의 서비스 요청을 지원하며 동시에 사용 요금을 시청 시간에 비례하여 정확하게 계산할 수 있도록 한다.

2. 관련 연구

J. Zhou 와 K-Y. Lam에 의하여 pay-per-view 방법이 제안되었고 이 방법은 공정성을 제공한다[3]. Zhou와 Lam의 방법은 반복 해쉬[5]를 사용하여 사용자의 시청 시간을 제공자가 증명할 수 있는 방법이다. 시청 요청을 할 때, 사용자는 랜덤 정수 n 을 선택하고, 다음과 같이 n 을 m 번 반복하여 해쉬한다.

$H^i(n) = H(H^{i-1}(n))$, where $i = 1, 2, \cdots, m$ and $H^0(n) = n$.

사용자는 $H^0(n), H^1(n), \cdots, H^{m-1}(n)$ 은 비밀스럽게 보관하고 $H^m(n)$ 은 제공자에게 전송한다. 비디오를 시청하는 동안, 사용자는 정해진 시간 단위(L)마다 $H^i(n)$ 를 제공자에게 전송한다. 여기에서 i 는 $m-1, m-2, \cdots$ 가 된다. 제공자는 $H(H^i(n)) = H^{i+1}(n)$임을 확인하여 올바르면 다음 프레임 시청 요청을 받은 것으로 간주하여 다음 프레임을 전송한다. 시청을 완료한 후 제공자가 $H^{m-j}(n)$ 을 가지고 있으면 사용자가 j 프레임을 시청하였음을 알 수 있다. 대칭키 암호가 비디오 스트림을 타인으로부터 보호하기 위하여 사용되었다. 이 방법은 사용자의 시청 시간을 올바르게 계산할 수 있다. 그러나 버퍼링을 지원하지 않으므로 사용자의 시청이 매끄럽게 진행되기에 어려움이 있다.

Joo[4]의 방법은 Zhou와 Lam에 의하여 제안된 기법에 버퍼링을 지원하며 시간 동기화의 문제를 제거하였다. Joo가 제안한 방법 또한 반복 해쉬를 사용한다. 그러나 제공자는 시청하고자 하는 비디오의 매 프레임을 자신이 선택한 서로 상이한 세션키(K_i)를 이용하여 암호화 한 후 네트워크 대역이 허용하는 만큼 암호화된 프레임을 사용자에게 전송한다. 사용자는 암호화된 프레임을 자신의 컴퓨터에 저장한다. 비디오를 시청하는 동안, 사용자는 정해진 시간 단위(L)마다 $H^i(n)$ 를 제공자에게 전송한다. 여기에서 i 는 $m-1, m-2, \cdots$ 가 된다. 제공자는 $H(H^i(n)) = H^{i+1}(n)$임을 확인하여 올바르면 다음 프레임에 대한 키(K_i) 를 전송한다. 사용자는 K_i 를 이용하여 해당 프레임을 복호하여 시청한다. 그러나 이 경우에도 사용자의 익명성을 지원하지 못하므로 사용자의 사생활 보호가 충분하지 못하다.

SET(Secure Electronic Transaction)은 인터

넷에서의 신용 카드 지불을 위하여 고안된 프로토콜이다[6]. SET에서는 카드 소지자의 카드 번호를 판매자에게 알리지 않고 물건을 구매할 수 있도록 한다. 카드 소지자는 구매 정보와 지불 정보를 분리하여 구매 정보는 판매자에게만 전송하며 지불 정보는 신용 카드 회사에게만 전송한다.

3. 서비스 모형 및 표기법

3.1 서비스 모형

웹기반 비디오 서비스에는 세 구성원이 존재한다. 사용자, 서비스 제공자, 그리고 결제대행자가 그들이다. 사용자는 VOD 프로그램을 시청하고자하는 사람이다. 제공자는 VOD 서버로서 VOD 프로그램에 대한 서비스 사용권을 가진다. 결제대행자는 사용자에게 VOD 사용에 대한 요금을 부과하고 결제된 요금을 제공자에게 전달하는 역할을 한다.

VOD pay-per-view 서비스 모형은 4 단계로 나누어 생각해 볼 수 있다. 사용자 등록, 서비스 요청 및 시청, 요금 부과 및 결제, 그리고 요금 정산이다.

사용자가 웹기반 pay-per-view 서비스를 원하면 먼저 결제대행자에게 사용자 등록을 한다. 사용자는 자신의 개인 정보, 요금 부과를 위한 주소, 공개키 인증서 등을 결제대행자에게 전송한다. 결제대행자는 새로운 사용자를 위하여 계좌를 개설한다.

사용자가 비디오 프로그램 시청을 원하면 제공자의 웹에 공개된 제목, 가격 등을 참고하여 프로그램을 선택하여 제공자에게 시청을 요청한다. 시청 요청을 받은 제공자는 VOD 프로그램을 제공하며 사용자는 해당 프로그램을 시청한다. 사용자는 언제든 원하는 때 시청을 중지할 수 있다. 경우에 따라 사용자의 컴퓨터 문제, 제공자의 서버 컴퓨터 문제, 또는 네트워크의 문제 등으로 사용자의 의사와 관계없이 시청이 중단될 수도 있다.

결제대행자는 사용자에게 요금 청구를 한다. 요금은 사용자의 이용한 분량에 따른다. 요금에 이의가 없으면 사용자는 요금을 결제대행자에게 지불한다. 사용자는 요금에 동의하지 못하면 이의를 제기한다. 이의가 제기되면 요금을 청구한 결제대행자와 제공자가 올바른 요금임을 증명하여야 한다.

결제대행자는 요금을 받은 후 이를 제공자에게 전달한다. 전달된 요금에 이의가 있는 경우 또한 결제대행자와 제공자간에 이를 해소할 수 있어야 한다.

3.2 표기법

다음의 표기법이 이 논문에서 사용된다.

- P: 서비스 제공자
- C: 사용자
- G: 결제대행자
- Id_A: A(P, C, 또는 G)의 계정이름
- *Title*: 선택된 비디오 제목
- *Pr*: 선택된 비디오 가격
- L: 선택된 비디오의 프레임 길이(1 분, 5 분 등). 요금 부과 단위가 됨.
- m: 선택된 비디오의 프레임 수. *선택된 프로그램 길이* = $m*L$
- $Frame_i$: 선택된 비디오의 i 번째 프레임. i 는 $0, 1, \cdots, m-1$ 이 된다.
- $H(n)$: 메시지 n의 해쉬 함수
- $H^i(n)$: 메시지 n의 반복 해쉬 함수. $H^i(n) = H(H^{i-1}(n))$, 그리고 $H^0(n) = n$
- *Kab*: A와 B 사이의 대칭키
- *Pa*: A(P, C, 또는 G)의 공개키
- *Sa*: A(P, C, 또는 G)의 개인키
- $E_k(X)$: 키 k로 메시지 X 암호화
- $S_k(X)$: 키 k 로 메시지 X 전자서명.
- R_A: A(P, C, 또는 S)에 의하여 생성된 랜덤 정수
- Q: 사용자의 자격(나이, 신뢰도, 유효기간 등)

4. 제안 기법

4.1 접근 방법

실제 사용한 시간에 따라 요금을 부과하며 동시에 익명성을 제공하기 위하여 반복 해쉬 함수와 이중 암호화가 사용된다.

사용자는 시청을 원하면 먼저 결제대행자로부터 임시 계정번호와 자격을 획득한다. 또한 사용

자와 결제대행자간의 세션키를 설정한다.

사용자가 제공자에게 시청 요청을 할 때, 사용자는 랜덤 정수 n 을 선택하고 이에 대하여 m 개의 반복 해쉬 값, $H^1(n)$, $H^2(n)$, …, $H^m(n)$, 을 다음과 같이 생성한다.

$H^i(n) = H(H^{i-1}(n))$, where $i = 1, 2, \cdots, m$ and $H^0(n) = n$.

사용자는 $H^0(n)$, $H^1(n)$, …, $H^{m-1}(n)$ 은 비밀스럽게 보관하고, 임시 계정번호와 자격, 요청하는 비디오에 대한 시청 정보(비디오 제목, 가격, 길이), 그리고 해쉬 값($H^m(n)$), 그리고 사용자와 결제대행자사이에 설정된 키에 의하여 이중 암호화된 지불정보(사용자 계정번호, 요청된 비디오 가격, 길이, 그리고 해쉬 값($H^m(n)$))을 제공자에게 전송한다.

제공자는 자신이 획득한 정보 가운데 가격, 길이, 해쉬 값과 이중 암호화된 지불정보를 결제대행자에게 전송하여 승인 요청을 한다. 결제대행자는 제공자로부터 전송받은 가격, 길이, 해쉬 값과 이중 암호화된 지불정보를 복호화하여 획득한 가격, 길이, 해쉬 값을 비교하여 동일하면 승인 메시지를 제공자에게 전송한다. 제공자는 결제대행자로부터 승인을 받으면, 서비스를 시작한다. 이 경우 제공자는 사용자의 계정번호를 획득할 수 없으며 결제 대행자는 사용자의 시청정보(제목)를 획득할 수 없게 된다.

서비스가 시작되면 제공자는 시청될 프로그램을 m 개의 설정된 시간 단위 길이(L)의 프레임으로 분할한다. 또한 m 개의 대칭키를 생성하여 각 프레임을 암호화한 후 사용자에게 전송한다. 사용자는 수신된 프레임들을 저장할 수 있으나 시청할 수는 없다. 시청을 위해서 사용자는 각 프레임을 암호화한 키를 획득하여야 한다.

비디오를 시청하는 동안, 사용자는 정해진 시간 단위(L)마다 $H^i(n)$ 를 제공자에게 전송한다. 여기에서 i 는 $m-1$, $m-2$, … 가 된다. 제공자는 $H(H^i(n)) = H^{i+1}(n)$ 임을 확인하여 올바르면 다음 프레임 시청 요청을 받은 것으로 간주하여 다음 프레임을 위한 암호화 키를 사용자에게 전송한다. 제공자는 획득한 암호화 키를 이용하여 다음 프레임을 복호화 한 후 이를 시청한다.

시청을 완료한 후 제공자가 $H^{m-j}(n)$ 을 가지고 있으면 사용자가 j 프레임을 시청하였음을 알 수 있다.

4.2 프로토콜

본 프로토콜은 사용자의 시청 시간에 따라 사용 요금을 계산하기 위하여 제안된 프로토콜이다. C 는 먼저 결제대행자로부터 임시 계정 번호와 자격을 획득한다.

1) $C \rightarrow G$: $E_{Pg}(Kcg)$, $E_{Kcg}(Id_C, Id_G, R_C)$
2) $G \rightarrow C$: $E_{Kcg}(Id_C, Id_G, R_G, R_C)$
3) $C \rightarrow G$: $S_{Sc}(Id_C, Id_G, R_G, R_C)$
4) $G \rightarrow C$: $E_{Kcg}(Id_G, R_G, R_C, Q, S_{Sg}(Id_G, R_G, R_C, Q))$

C 는 자신의 계정이름(Id_C)을 자신이 생성한 랜덤 정수(R_C)와 함께 결제대행자(G)에게 전송한다. 이 정보들은 사용자가 생성한 키(Kcg)를 이용한 대칭키 암호를 사용하여 보호되며 Kcg 는 G 의 공개키(Pg)로 암호화되어 결제대행자에게 전송된다. G 는 도전/응답 방식을 이용하여 실제 사용자임을 확인한다. G 는 자신이 생성한 랜덤 정수(R_G)를 C 에게 전송하며 C 는 이를 전자서명($S_{Sc}(Id_C, Id_G, R_G, R_C)$)하여 응답함으로써 자신의 신분을 확인시킨다. G 는 C 의 전자서명을 C 의 공개키(Pc)를 이용하여 확인함으로써 C 의 신분을 확인한다. G 는 C 의 신분이 올바르다고 확인되면 C 의 자격에 전자서명을 첨부하여 C 에게 전송한다. 이 때 교환된 두 랜덤 정수(R_G, R_C,)는 추후에 임시 계정 번호로 사용된다. G 는 사용자의 계정(Id_C)과 임시 계정번호(R_G, R_C)와의 관계를 저장한다.

임시 계정 번호와 자격을 획득한 후, C 는 제공자(P)에게 시청 요청 메시지를 보낸다. C 는 지불 단위 시간(프레임의 길이)인 L 과 m(프레임의 수)을 선택한다. 선택된 비디오 프로그램은 길이가 L 인 m 개의 프레임으로 구성되게 된다. C 가 시청을 요청할 때 C 는 랜덤 정수 n 을 선택하여, 선택된 n 에 대하여 m 번 반복적으로 해쉬 값을 계산한다.

$H^i(n) = H(H^{i-1}(n))$, where $i = 1, 2, \cdots, m$ 그리고 $H^0(n) = n$.

C 는 $H^0(n)$, $H^1(n)$, …, $H^{m-1}(n)$ 를 비밀스럽게 보관하고 다음의 메시지를 P 에게 전송한다.

5) $C \rightarrow P$: $E_{Pp}(Kcp)$, $E_{Kcp}(Id_C, R_G, R_C, Q, S_{Sg}(Id_C, R_G, R_C, Q), Title, Pr, L, m, H^m(n), E_{Kcg}(Id_C, R_G, R_C, Pr, L, m, H^m(n), S_{Sc}(Id_C, R_G, R_C, Pr, L, m, H^m(n))))$

C 는 세션 키 Kcp 를 생성하고 제공자의 공개키(Pp)로 암호화하여 전송한 후 Kcp 를 키로 대칭키 암호화를 사용하여 자신의 전송 내용을 보호한다. C 는 G 에 의하여 전자서명 된 자신의 임시 계좌 번호와 자격(Id_G, R_G, R_C, Q, $S_{Sg}(Id_G, R_G, R_C, Q)$)을 제공자에게 전송한다. 선택된 비디오의 제목 ($Title$), 시간 단위 당 가격 (Pr), 각 프레임의 길이 (L), m 번 해쉬된 값 ($H^m(n)$)이 함께 전송된다. 또한 C 는 지불 관련 정보(Id_C, R_G, R_C, Pr, L, m, $H^m(n)$)와 그에 대한 전자서명($S_{Sc}(Id_C, R_G, R_C, Pr, L, m, H^m(n))$)을 C 와 G 사이의 세션 키인 Kcg를 이용하여 암호화하여 함께 전송한다. 5번 메시지를 받은 제공자(P)는 사용자(C)의 정보를 알지 못하는 상태에서 사용자의 임시 계좌 번호(R_G, R_C), 사용자의 자격(Q), 사용자가 원하는 비디오의 제목($Title$), 프레임의 길이(L), 그리고 프레임 수(m)를 알 수 있다. P 는 다음의 메시지를 G 에게 전송하여 승인 요청을 한다.

6) $P \rightarrow G$: $E_{Pg}(K_{gp})$, $E_{Kgp}(Id_C, R_G, R_C, Pr, L, m, H^m(n), E_{Kcg}(Id_C, R_G, R_C, Pr, L, m, H^m(n), S_{Sc}(Id_C, R_G, R_C, Pr, L, m, H^m(n))))$
7) $G \rightarrow P$: $E_{Kgp}(R_G, R_C, Pr, L, m, H^m(n), S_{Sg}(R_G, R_C, Pr, L, m, H^m(n)))$

P 는 5번의 시청 요청 메시지의 수신 후, 암호화된 지불 관련 정보($E_{Kcg}(Id_C, R_G, R_C, Pr, L, m, H^m(n), S_{Sc}(Id_C, R_G, R_C, Pr, L, m, H^m(n))))$를 결제대행자($G$)에게 전달한다. 이 때에 P 는 자신이 가지고 있는 임시 계좌 번호(R_G, R_C), 가격(Pr), 프레임의 길이(L), 프레임 수(m), 그리고 m 번 반복된 해쉬 값($H^m(n)$)을 함께 전송한다.

6번 메시지를 수신한 결제대행자(G)는 사용자의 정보(Id_C)와 지불 관련 정보 등은 알 수 있으나 사용자가 요청한 비디오의 제목($Title$)은 알지 못한다. G 는 P 로부터 받은 R_G, R_C, Pr, L, m, $H^m(n)$ 과 P 가 C 로부터 받아 전달한 이중 암호화된 내용($E_{Kcg}(Id_C, R_G, R_C, Pr, L, m, H^m(n), S_{Sc}(Id_C, R_G, R_C, Pr, L, m, H^m(n)))$)의 동일함을 확인한다. 또한 그 내용이 C 에 의하여 올바로 서명되었음을 확인한다. G 는 6번 메시지의 올바름을 확인 한 후 7번의 승인 메시지를 보낸다.

P 가 G 로부터 승인 메시지를 받은 후 시청이 이루어진다. P 는 선택된 프로그램을 길이 L 인 m 개의 프레임($Frame_0$, $Frame_1$, …, $Frame_{m-1}$)으로 분할한다. P 는 m 개의 대칭키 (K_0, K_1, …, K_{m-1})를 생성하고, m 개의 프레임 ($Frame_i$)을 각각 생성된 키(K_i)로 암호화한다. P 는 암호화 된 프레임들을 C 에게 전송한다.

8) $P \rightarrow C$: $E_{Ki}(Frame_i)$

C 는 암호화된 프레임($E_{Ki}(Frame_i)$)을 수신하여 저장한다. 시청이 진행되는 동안 C 는 시청 요청 시 생성했던 해쉬 값($H^i(n)$, 여기에서 $i = m-1, m-2, \cdots$)을 매 시간 단위(L)마다 P 에게 전송하여 다음 프레임에 대한 시청 요청을 한다. P 는 $H(H^i(n))$ 과 $H^{i+1}(n)$ 이 동일함을 확인한다. 만약 $H(H^i(n))$ 과 $H^{i+1}(n)$ 이 동일하면 P 는 C 가 다음 프레임에 대한 올바른 시청 요청을 한 것임을 알 수 있다. 다음 프레임에 대한 사용 요청을 받은 P 는 다음 프레임의 암호화 키 (K_{m-i})를 프레임 번호($m-i$)와 함께 C 에게 전송한다. K_{m-i} 와 $m-i$ 는 C 와 P 사이의 세션키 (Kcp)를 이용하여 암호화 되어 있다. 첫 번째 프레임($Frame_0$)에 대한 키(K_0)는 P 가 승인 메시지를 받은 즉시 전송된다. 이는 P 가 이미 $H^m(n)$ 을 가지고 있기 때문이다.

9) $C \rightarrow P$: $E_{Kcp}(H^i(n))$
10) $P \rightarrow C$: $E_{Kcp}(m-i, K_{m-i})$

C 는 $E_{Kcp}(m-i, K_{m-i})$ 를 수신한 후, K_{m-i} 를 복원하고 K_{m-i} 를 이용하여 저장되어 있는 $E_{Km-i}(Frame_{m-i})$ 로부터 $Frame_{m-i}$ 를 복원하여 이를 시청한다.

C 로부터 일정 시간 요청이 없으면 P 는 시

청이 완료된 것으로 간주한다. 시청이 완료되면 P 는 다음의 메시지를 G 에게 전송하여 시청한 분량을 통보한다.

11) $P \rightarrow G$: $E_{Kgp}(Id_G, R_G, R_C, j, H^{m-j}(n))$

만약 C 가 j 개의 프레임을 시청하였으면 마지막으로 P 가 수신한 해쉬 값은 $H^{m-j}(n)$ 가 된다. P 는 j 와 $H^{m-j}(n)$ 을 G 에게 전송한다. 결제대행자(G)는 사용자(C)에게 j 프레임만큼의 요금을 청구한다.

만약 시청한 분량에 대하여 사용자가 이의를 제기하면 결제대행자는 초기에 사용자로부터 $H^m(n)$ 을 전자서명과 함께 수신하였음과 자신이 $H^{m-j}(n)$ 을 수신하였으며 $H^j(H^{m-j}(n)) = H^m(n)$ 임을 보임으로써 사용자가 최소한 j 프레임 이상 시청하였음을 증명할 수 있다.

5. 토론

제안된 프로토콜은 사용자의 사생활을 보호하여 준다. 비디오 제목을 비롯한 시청 정보는 사용자와 제공자 사이에 설립된 세션 키(Kcp)에 의하여 암호화되어 외부인으로부터 보호된다. 세션키 Kcp 는 사용자에 의하여 생성되며 제공자에게 전송될 때 제공자의 공개키(Pp)에 의하여 암호화되어 전송된다. 시청되는 내용 또한 암호화되며 이는 사용자가 제공자로부터 획득한 세션키(K_i)에 의해서만 복호화 될 수 있다. 세션키(K_i)는 다시 사용자와 제공자 사이에 설립된 세션 키(Kcp)에 의하여 암호화되어 보호된다. 따라서 사용자가 요청하는 모든 정보와 시청하는 내용은 외부로 누출되지 않는다.

사용자는 또한 익명으로 시청요청을 할 수 있다. 사용자가 제공자에게 시청 요청을 할 때, 사용자는 결제대행자로부터 획득한 임시 계정번호를 이용하여 시청 요청을 한다. 그리고 시청 정보와 지불 정보를 분리하여 시청 정보는 제공자만이 볼 수 있고 지불 정보는 결제대행자만이 볼 수 있도록 한다. 사용자의 실제 계정 번호를 포함하는 지불정보에는 시청하는 비디오의 제목은 포함하지 않고 사용자 계정번호, 요청된 비디오 가격, 길이, 그리고 해쉬 값($H^m(n)$) 등의 요금 부과와 관계된 정보만을 포함한다. 시청 정보에는 사용자의 계정 번호를 포함하지 않고 임시 계정번호와 자격, 요청하는 비디오에 대한 시청 정보(비디오 제목, 가격, 길이), 그리고 해쉬 값($H^m(n)$) 등의 시청에 관계되는 정보만 포함한다. 따라서 제공자와 결제대행자가 공모하지 않는 한, 사용자의 시청 정보는 누구에게도 알려지지 않을 수 있다.

제안된 프로토콜은 시청 시간을 정확하게 계산하며 사용자가 부인할 수 없는 증거를 제시하는 기능을 제공한다. 결제대행자가 제공자를 통하여 초기에 사용자로부터 $H^m(n)$ 을 전자서명과 함께 수신하였고 마지막으로 $H^{m-j}(n)$ 을 수신하였으면 사용자가 최소한 j 프레임 이상 시청하였음을 증명할 수 있다. 해쉬 함수는 일방향 함수이므로, x < y 인 경우, 사용자를 제외한 누구도 $H^{m-x}(n)$ 으로부터 $H^{m-y}(n)$ 를 생성할 수 없다. 따라서 $H^j(H^{m-j}(n)) = H^m(n)$ 임을 보임으로써 사용자가 최소한 j 프레임 이상 시청하였음을 증명할 수 있다.

또한 사용자는 제공자에게 알리지 않고 원하는 프레임을 시청할 수는 없다. 각 프레임은 제공자가 선택한 상이한 키에 의하여 암호화 되었으며 제공자는 사용자로부터 올바른 해쉬 값을 이용한 요청을 받은 경우에만 다음 프레임을 위한 암호화 키를 전송하기 때문이다.

제안된 프로토콜은 정밀도의 문제점을 가진다. 제안된 프로토콜은 언제나 시간 단위(L)의 수로 시간을 측정한다. 만약 결제 대행자가 $H^{m-j}(n)$ 를 마지막 해쉬 값으로 가지고 있고 $H^m(n)$ 을 초기 해쉬 값으로 가지고 있는 경우, 사용자는 j 프레임을 이미 시청하였으며 $j+1$ 프레임을 현재 시청 중임을 알 수 있다. 따라서 j 프레임에 대한 요금을 부과하면 조금 적게 요금을 부과한 것이며 $j+1$ 프레임에 대한 요금을 부과하면 너무 많은 요금을 부과한 것이다.

6. 결론

웹 기반의 VOD 서비스는 고속 네트워크의 발전과 함께 더욱 활성화 될 것으로 여겨진다. 요금 계산 및 부과 방법은 VOD 서비스에서의 중요한 이슈이다. 그리고 개인의 사생활 보호 또

한 VOD 서비스의 중요한 이슈가 된다.

본 논문에서는 사용자의 익명성을 지원하는 웹기반 pay-per-view 기법이 제안되었다. 제안된 기법은 사용자의 사생활 보호를 위하여 익명으로 VOD 시청을 요청할 수 있다. 또한 사용자의 시청 시간에 비례하여 요금을 부과하며 이의 제기 시 시청 시간을 증명하여 부인을 할 수 없도록 하는 기능을 제공한다.

참 고 문 헌

[1] T. S. Hyedt-Benjamin, H. Chae, B. Defend, and K. Fu, "Privacy for public transportation," Proceedings of the Sixth Workshop on Privacy Enhancing Technologies, pp. 1-19, 2006.

[2] R. Dingledine and A. Mathewson, "Anonymity loves company: Usability and the network effect," Proceedings of the Fifth Workshop on Economics of Information Security, 2006.

[3] J. Zhou and K. Lam, "A secure pay-per view scheme for web-based video service," Proceedings of the Second International Workshop on Practice and Theory in Public Key Cryptography, LNCS 1560, pp. 315-326, 1999.

[4] H. Joo, "Private and fair pay-per-view scheme for web-based video-on-demand systems," IEEE Trans. Consumer Electronics, vol. 49, no. 2, pp. 403-407, May 2003.

[5] T. Pedersen, "Electronic payments of small amounts," Proceedings of the Cambridge Workshop on Security Protocols, LNCS 1189, pp. 59-68, 1996, U.K.

[6] G. N. Drew, Using SET for Secure Electronic Commerce, Prentice Hall, 1998.

주 한 규

1988년 : 한림대학교 전자계산학과 (학사)

1994년 : Arizona State Univ. Computer Science and Engineering (석사)

1998년 : Arizona State Univ. Computer Science and Engineering (박사)

1999년~2000년 : 한국전자통신연구원 선임연구원

2000년~현 재 : 한림대학교 정보통신공학부 부교수

관심분야 : 정보보호, 소프트웨어공학