CCN TV 서비스를 위한 컨텐츠 권한 설정 및 제어 메커니즘

조응준○ 홍충선
경희대학교 컴퓨터공학과
d2o2mask@khu.ac.kr, cshong@khu.ac.kr

Contents Authorization and Control Mechanism for CCN TV Service

Eung Jun Cho○ Choong Seon Hong
Department of Computer Engineering, Kyung Hee University

요 약

인터넷을 통해 제공되는 서비스 중 스트리밍 서비스의 비중은 점점 증가하고 있다. 그리고 현재 FHD 수준의 영상 서비스를 넘어 차세대 표준으로 기대되는 UHD 영상의 시대가 도래할 경우 지금의 케이블 방식의 TV 서비스로는 충분한 대역폭을 확보할 수가 없다. 이미 상용화되어 있는 IPTV의 경우도 IP의 많은 기술적인 한계로 인해 기본 대역폭 요구량이 현재의 FHD의 수 십배에 이르는 UHD 영상의 경우 보다 효율적으로 데이터를 전송할 필요가 있다. CCN은 현재의 IP기반의 인터넷 구조를 보다 효율적으로 대체할 수 있는 미래인터넷 기술로서 최근 많은 연구가 진행되고 있다. 그러나 CCN의 경우 CCN 라우터간의 단일 홉간에 데이터를 전송하는 구조로 종단 간의 컨텐츠 전송 시 권한 설정, 그리고 컨텐츠 제공자가 자신의 컨텐츠를 완벽하게 제어할 수 없는 문제점이 있다. 본 논문에서는 현재 IPTV 기술을 CCN 기반의 TV 서비스로 적용시 문제가 될 수 있는 컨텐츠의 권한 설정 및 제어를 해결하기 위한 변경된 CCN 메커니즘을 제안한다.

1. 서 론

인터넷을 통한 스트리밍 서비스의 수요는 폭발적으로 증가하고 있다. 특히 스마트폰의 등장과 IPTV 서비스 수요의 증가에 따라 전체 인터넷 트래픽 중 스트리밍 서비스의 대역폭은 2010년에 이미 약 50%를 넘어서고 있다. 그리고 TV 서비스가 디지털로 전환되면서 HD 화질의 채널 서비스가 늘어나고 있으며 이로 인해 기존 케이블을 이용한 서비스 제공은 한계에 다다르고 있다. 실제 유선 케이블을 통해 제공되는 HD화질의 TV 서비스의 수는 매우 제한적이며 IPTV의 경우 상대적으로 보다 많은 HD 화질의 채널 서비스를 제공하고 있다. 그러나 현재 기술의 HD를 넘어 UHD 화질로 발전하고 있으며 실제 LG와 삼성에서 UHD 해상도를 지원하는 TV를 상용화 하였다.

HD 채널의 경우 약 7~ 10Mbps의 대역폭을 요구하는 반면 UHD의 경우 기존 HD 채널보다 최소 4배에서 최대 96배의 대역폭을 필요로 한다. 실제 UHD의 경우 그 해상도가 4K(2160P)와 8K(4320P)의 두 가지 규격이 존재하며 현재 표준화가 진행 중에 있다. 이런 상황에서 IP기반의 스트리밍 서비스를 수행할 경우 멀티캐스트 서비스를 수행하지 않는 이상 중복된 데이터의 수신을 방지할 수 없으며 이는 네트워크상의 대역폭 낭비로 이어지게 된다.

본 논문에서는 이런 문제점을 해결하기 위하여 CCN (Content Centric Networking) 기반의 TV 스트리밍 서비스를 위한 메커니즘을 제안한다. 현재 연구가 진행 중인 CCN 메커니즘을 그대로 적용할 경우 실제 상용화 서비스에 부족한 부분들이 존재하는데 이런 문제점을 살펴보고 이를 해결하기 위한 메커니즘을 제안하도록 한다.

"본 연구는 미래창조과학부 및 정보통신산업진흥원의 IT융합 고급인력과정 지원사업의 연구결과로 수행되었음" (NIPA-2013-H0301-13-3007) Dr. CS Hong is corresponding author

2. 관련 연구 및 문제점

1) CCN

CCN[1]은 현재 IP 주소기반의 데이터 전송 방법을 컨텐츠 중심의 전달 방법으로 변경하여 보다 효율적으로 데이터를 전달하기 위한 기술이다. 실제 이런 컨텐츠 중심의 연구는 CCN 외에도 NDN(Named data networking), CBN (Content-Based Networking), DON(Data Oriented Networking), ICN(Information Centric Networking) 등의 다양한 이름으로 연구가 되고 있다. CCN은 PARC의 Van Jacobson을 중심으로 연구가 진행되고 있으며 자신들의 연구로 개발된 메커니즘을 CCNx[2]라는 이름의 프로젝트로 문서화 및 코드를 공개하고 있다.

CCN 프로토콜의 경우 크게 두 가지의 메시지를 통해 데이터를 송수신하고 있다. 하나는 데이터 요청에 사용되는 Interest 패킷이고 다른 하나는 실제 데이터를 포함하는 Data 패킷이다. 실제 CCN은 데이터를 전송하기 위해 특정 프로토콜을 지정하고 있지 않으며 IP, UDP, TCP, 혹은 2계층 MAC 기술만을 통해 데이터 전송이 가능하도록 설계되어 있다. 모든 통신은 청크(chuunk)로 불리는 데이터 단위로 이루어진다.

2) CCN의 문제점

현재 CCN 메커니즘의 경우 그 특성 상 컨텐츠에 대한

권한을 설정할 수 없는 문제점이 있다. 즉 기존 IP 기반의 전송 메커니즘의 경우 모든 전달이 종단 간에 이루어지기 때문에 컨텐츠 소스에서 클라이언트의 정보를 확인한 후 정책에 따라 데이터를 전송하는 것이 가능하였다. 그러나 CCN의 경우 CCN 라우터 상의 CS에 컨텐츠가 저장되어 이를 홉 단위로 전달을 한다. 즉 CCN 라우터는 특정 컨텐츠를 요청한 사용자를 확인할 수 없으며 컨텐츠 요청 패킷인 Interest packet이 들어온 face로 data packet을 전달한다. 이는 해당 컨텐츠를 컨텐츠 제공자가 완벽하게 제어할 수 없는 것을 의미할 뿐만 아니라 컨텐츠에 접근하기 위한 사용자의 권한 제어가 불가능한 것을 의미한다. 이는 [3]의 연구에서도 CCN의 문제점으로 지적되고 있다.

TV 스트리밍 서비스의 경우 기본 제공 채널뿐만 아니라 유료 가입 채널도 존재한다. 즉 사용자 별로 차별화된 컨텐츠를 제공할 수 있어야 하며 허가받지 않은 사용자는 해당 채널의 시청이 불가능 해야 한다. 그러나 현재 CCN 메커니즘을 그대로 TV 스트리밍 서비스에 적용할 경우 중복된 데이터의 전송을 줄여 망 효율성은 좋아지겠지만 TV 서비스 제공자나 컨텐츠 제공자에게 보다 많은 수익을 줄 수 있는 유료 채널링 서비스를 제공할 수 없는 문제점이 있다.

3. 제안 사항

본 논문의 제안사항은 기존 CCN과 호환성을 가지면서 컨텐츠에 대한 권한 부여 및 제어가 가능하도록 하는 것이다. 이를 위하여 본 논문에서는 새로운 유형의 CCN data와 Interest 패킷을 정의하고 이를 활용하도록 한다. 그리고 컨텐츠별 권한부여 및 관리를 위하여 인증서버를 추가한다. 인증서버의 경우 CCN의 기본적인 컨텐츠 인증 외에 사용자의 권한 인증을 위한 서버이다. 해당 인증서버의 경우 정보 업데이트는 컨텐츠 제공자만 가능하며 인증 요청은 해당 컨텐츠를 가진 CCN 라우터가 수행할 수 있다. 이런 기능을 수행하기 위하여 본 논문에서는 Interest 패킷에 새로운 필드를 추가하고 Data 패킷의 type 영역에 스트리밍 데이터를 구분하기 위한 새로운 유형을 정의한다.

표 1은 본 논문에서 사용되는 기호의 의미를 정의한다.

표 1 사용된 기호와 그 의미

기호	설명
$[A]_B$	B로 A를 암호화
UK	사용자 키
K_{pri}	개인키
K_{pub}	공개키

1) 컨텐츠에 권한을 부여하기 위한 메커니즘

a. 컨텐츠 및 사용자 등록 단계

컨텐츠 제공자는 자신의 컨텐츠를 인증서버에 등록한다. 이 때 컨텐츠 제공자는 해당 컨텐츠를 사용할 수 있는 사용자의 공개키를 인증 서버에 함께 제공한다. 이 사용자의 공개키는 컨텐츠 제공자가 필요시 업데이트 할 수 있다. 그리고 컨텐츠 제공자는 사용자에게 인증 시 사용한 사용자의 키쌍(UK_{pri}, UK_{pub})을 전달한다.

b. 인증 및 데이터 전달

사용자가 권한이 필요한 컨텐츠를 Interest 패킷을 통해 요청하는 경우 다음과 같은 절차를 통하여 인증을 거쳐 data 패킷을 수신하게 된다.

① Interest 패킷 생성 및 전달

사용자는 컨텐츠 제공자로부터 받은 대칭키 쌍을 이용하여 원하는 data에 대한 Interest 패킷을 생성한다. 이 때 Interest 패킷에 *Authentication* 필드를 추가하고 해당 필드에 $[nounce|UK_{pub}]_{UK_{pri}}|UK_{pub}$ 값을 입력하여 전송한다. 이때 *nounce*는 CCN에서 Interest 패킷을 생성할 때 임의로 생성하는 숫자이다.

② Interest 패킷의 전달

Interest 패킷을 수신한 CCN 라우터는 자신의 CS에서 해당 컨텐츠를 검색한 후 데이터가 존재하지 않을 경우 기본 CCN 메커니즘에 따라 Interest 패킷을 전달한다. 만약 자신의 CS에서 일치하는 데이터가 발견될 경우 인증절차를 시작한다.

③ 사용자 인증

사용자가 전송한 Interest 패킷에 *Authentication* 필드가 존재할 경우 해당 필드의 암호화 되지 않은 사용자 공개키(UK_{pub})를 사용하여 데이터를 복호화하여 *nounce*와 UK_{pub}값을 얻는다. 이 값이 Interest 패킷의 *nounce* 값과 사용자의 공개키값(UK_{pub})과 일치할 경우 권한 인증을 시작한다.

④ 사용자 권한 인증

사용자가 요청한 컨텐츠의 유형이 스트리밍 데이터 이면서 인증이 필요한 컨텐츠일 경우 CCN 라우터는 전달해야 할 컨텐츠 data 패킷의 *KeyLocator* 필드를 확인하여 인증서버의 주소를 알아낸다. 그리고 해당 인증서버에 컨텐츠를 요청한 사용자의 공개키(UK_{pub})와 컨텐츠의 서명비트, 그리고 Interest 패킷의 *nounce*를 전송하여 해당 컨텐츠의 유효성과 사용자의 권한을 검증 받는다.

⑤ data 패킷의 전달

인증 서버로부터 확인 메시지를 수신한 CCN 라우터는 해당 컨텐츠를 interest 패킷을 수신한 face로 전달하여 사용자가 데이터를 수신할 수 있도록 한다.

2) 라이브 스트리밍 데이터의 전달 메커니즘

CCN의 경우 하나의 Interest 패킷에 하나의 청크만을 전송하도록 설계되어 있다. 그러나 이런 데이터 전송의 경우 연속적으로 큰 데이터의 전송이 필요한 스트리밍 서비스 형태에는 적합하지 않다. 무엇보다 실시간 스트리밍 서비스의 경우 사용자가 새롭게 전송되는 컨텐츠에 상응하는 Interest 패킷을 지속적으로 만들어 전송해야 하는 문제점이 있다. 이를 해결하기 위하여 본 논문에서는 다음과 같이 스트리밍 데이터 전송을 위한 알고리즘을 기존 CCN 라우터에 추가하였다.

우선 특정 Data 패킷이 라이브 스트리밍 패킷이라는 것을 구분하기 위하여 data 패킷의 컨텐츠의 유형을 알려주는 type 필드에 라이브 스트리밍 컨텐츠의 유형을 추가한다. 다음 표는 CCNx 문서[2] 상의 Type의 정의 상태이다.

표 2 Type 필드의 유형과 설명

Base64	Hex	설명
DATA	0x0C04C0	Type의 값이 없는 경우로 기본
ENCR	0x10D091	컨텐츠가 암호화된 경우
GONE	0x18E344	whiteout marker
KEY/	0x28463F	공개 키
LINK	0x2C834A	링크
NACK	0x34008A	현재 컨텐츠가 없음
STRM	*0xFFxxxx*	*라이브 스트리밍 xxxx 채널*

상기 표의 가장 마지막에 있는 STRM은 본 논문에서 새롭게 정의한 유형으로 3byte의 크기 중 처음 바이트의 값은 0xFF로 설정하여 해당 컨텐츠가 라이브 스트리밍형 컨텐츠 임을 알리고 뒤의 두 바이트는 채널 ID를 의미한다.

한 사용자가 라이브 스트리밍의 컨텐츠를 요청할 경우 CCN 라우터의 동작은 다음과 같이 이루어진다. 제안사항을 위해 CCN 라우터 상에 기존 PIT(Pending Interest Table)과 FIB(Forwarding Inforamtion Base)외에 라이브 스트리밍을 관리하기 위한 SIT(Streaming Information Table)를 추가한다. SIT에서 보관하는 정보는 표 2에서 정의한 STRM의 채널 ID와 해당 채널을 전달할 out-going face 정보이다. 하나의 채널 ID 정보에 여러 face가 할당 될 수 있다.

CCN 라우터의에서 기본적인 data 패킷의 전달은 기존 CCN 메커니즘에서 정의한 것처럼 PIT와 FIB를 기반으로 이루어진다. 단 CCN 라우터가 전달받은 data 패킷의 유형이 위에서 정의한 라이브 스트리밍일 경우에는 알고리즘 1과 같이 추가적인 동작이 이루어진다. 사용자와 CCN 라우터는 지속적으로 라이브 스트리밍 data 패킷을 수신하고자 하는 경우 주기적으로 해당 라이브 스트리밍 data 패킷을 수신하기 위한 Interest 패킷을 전송하여 데이터 요청을 갱신한다.

알고리즘 1을 통하여 사용자는 하나의 data 패킷 마다 Interest 패킷을 전송할 필요 없이 주기적인 Interest 패킷의 전송을 통하여 라이브 스트리밍 데이터를 수신할 수 있다.

알고리즘 1 라이브스트리밍을 위한 메커니즘

STRM*n* : 채널 ID *n*의 라이브 스트리밍 데이터
PIT*m* : PIT에 저장되어 있는 Interest 패킷이 도착한 *m* face
if received data packet type is STRM*n* **then**
  if received data packet is in PIT*m* **then**
    Renewal Timer for channel *n*/face *m*.
    Register face *m* on channel *n* of SIT and forward data packet to faces listed in SIT.
    Remove interest packet in PIT.
  else if received data packet type is STRM*n* and it is in SIT but not in PIT **then** Forward data packet to all face listed in SIT and reduce the Timer for channel *n*
if Timer for channel *n*/face *m* is expired **then** remove face *m* from channel *n* in SIT

4. 제안된 메커니즘의 평가

제안 사항 중 컨텐츠에 권한을 부여는 메커니즘의 경우 다음과 같은 장점을 지니고 있다.

① 인가된 사용자의 경우 Authentication 필드에 nounce 값을 사용자의 개인키로 암호화 하여 전송하기 때문에 공격자가 이 값을 복사하여 사용할 경우 CCN 라우터에서 같은 *nounce*가 사용되었기 때문에 이 값을 폐기하여 재연공격이 불가능
② Authentication 필드의 값은 사용자의 개인키로 암호화되어 있으며 이 값은 오직 사용자만이 생성 가능

라이브 스트리밍을 위한 알고리즘의 경우 기존 IP 멀티캐스팅 방식보다 다음과 같은 장점을 지닌다.

① 복잡한 그룹 가입 및 그룹 탈퇴 과정의 불필요
② 복잡한 라우팅 알고리즘이 불필요
③ TCP/IP 기반의 오버레이 형태의 CCN 토폴로지 구성을 통해 보다 적은 수의 라우터에 제안된 CCN 알고리즘을 적용하여 서비스 가능

5. 결론 및 향후 계획

본 제안사항을 통하여 CCN 환경에서 보다 효율적인 라이브 스트밍 서비스가 가능하며 컨텐츠의 권한 설정을 통하여 제한된 사용자에게만 컨텐츠를 공개하는 것이 가능하다. 본 논문의 제안사항을 활용할 경우 현재 IPTV 수준의 라이브 스트리밍과 VOD 서비스를 CCN환경에서 보다 효율적으로 제공할 수 있다.

앞으로 본 논문에서 제안한 메커니즘의 성능상의 이점을 분석하기 위해 기존 CCN 기반의 스트리밍 연구와 비교 및 분석을 수행하고 CCNx 기반의 구현을 통하여 제안사항을 입증할 것이다.

참고문헌

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking named content," in Proceedings of the 5th international conference on Emerging networking experiments and technologies, ser. CoNEXT '09. New York, NY, USA: ACM, 2009, pp. 1-12

[2] CCNx, available on online : http://www.ccnx.org/

[3] D. Goergen, T. Cholez, J. Francois, and T. Engel, "Security monitoring for content-centric networking," in International Workshop on Autonomous and Spontaneous Security, ser. SETOP. Springer-Verlag, 2012.