P2P 기반의 미디어 스트리밍 보안 고려사항

권혁찬*, 김상춘**, 나재훈*
*한국전자통신연구원 정보보호연구본부
**강원대학교 전자정보통신공학부
e-mail : hckwon@etri.re.kr

Security Considerations for P2P-based Media Streaming

Hyeokchan Kwon*, Sangchoon Kim**, Jaehoon Nah*
*Electronics and Telecommunications Research Institute
**Gangwon National University

요 약

최근 들어 미디어 스트리밍 서비스 제공 시 서버의 부하 및 비용을 줄이기 위해 P2P 기반의 오버레이 네트워크를 이용하여 미디어 스트리밍 콘텐츠를 분배하는 방안이 등장하고 있다. 하지만 이 방안은 그 효율성만큼이나 보안 취약성도 많이 존재하는 방안이다. 본 논문에서는 P2P 기반의 미디어 스트리밍 서비스에 대한 보안 위협과 이에 대응하기 위한 보안 고려사항을 분석하였다.

1. 서론

최근 들어 IPTV, VoD 등 미디어 스트리밍 서비스 제공시 서버의 부하 및 비용을 줄이기 위해 P2P 기반의 오버레이 네트워크를 이용하여 분배하는 방안이 등장하고 있다. 실제로 Joost[1] 등은 P2P 를 기반으로 스트리밍 서비스를 제공하고 있다.

일반적으로 P2P 기반의 오버레이 네트워크를 이용하여 미디어를 분배하는 구조는 동일 채널을 시청하는 피어간에 가상의 오버레이 트리(Virtual Overlay Tree)를 구축하며, 각 피어는 미디어 데이터를 상영하면서 다음 피어 – child peer – 에게 데이터를 전달하는 방식으로 동작을 하게 된다. 오버레이 트리의 구축을 위해 DHT(Distributed Hash Table) 기반의 Chord[2], Pastry[3] 등의 알고리즘을 사용할 수도 있으며 별도의 오버레이 트리 관리를 위한 메커니즘을 자체 사용할 수도 있다.

그러나 P2P 기반의 오버레이 네트워크를 미디어 스트리밍에 이용하는 경우 중간 피어의 콘텐츠 불법 취득, 악의적인 노드의 오버레이 네트워크 참여를 통한 미디어 데이터 전달 방해, 키 유출, DoS 공격 등 다양한 형태의 보안 위협이 존재한다.

본 논문은 P2P 기반의 미디어 스트리밍 서비스 구축을 위한 보안 위협에 대해 분석해보고 이에 대응하기 위한 보안 고려사항 등을 논의해 보고자 한다. 본 논문에서는 채널단위의 미디어 스트리밍 서비스에 대해 주로 초점을 맞추고 있으며 VoD 형태의 서비스의 경우는 고려하지 않았다.

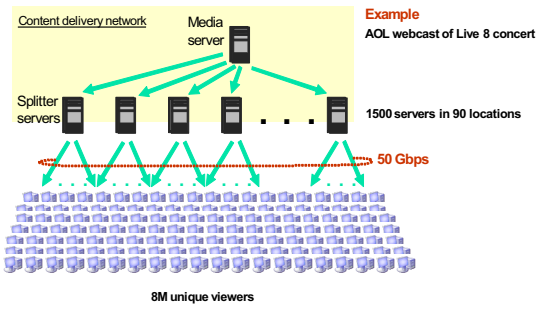
* 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2008-S-001-01, “유무선 환경의 개방형 IPTV(IPTV2.0) 정보보호 기술개발”]

본 논문의 구성은 다음과 같다. 2 장에서는 P2P 기반의 미디어 스트리밍 서비스의 개요를 살펴보고, 3 장에서는 이에 대한 보안 위협을 분석하고 이에 대한 보안 고려사항을 논의한다. 4 장에서는 결론을 맺는다.

2. P2P 기반의 미디어 스트리밍 서비스 개요

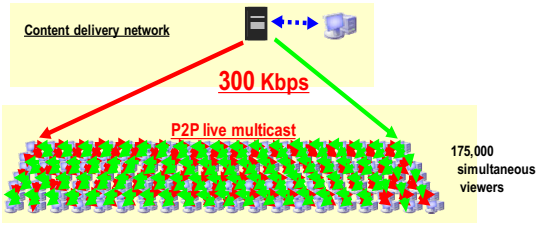
P2P 기반의 미디어 스트리밍 서비스가 등장한 것은 서버의 부하와 비용을 줄이기 위한 목적이다. 또한 KT 나 하나로 통신을 인수한 SKT 와 같이 자체 보유한 프리미엄 망을 통해 IPTV 서비스를 제공하는 경우를 제외하고는 보통 오픈 망을 통해 미디어 스트리밍 서비스를 제공하기 때문에 이 경우 충분한 대역폭 확보의 어려움도 P2P 기반의 스트리밍을 도입하게 된 배경이라 할 수 있다.

서버 기반의 일반적인 미디어 스트리밍의 예로 AOL webcast Live 8 concert 의 구조는 (그림 1)과 같다.[4]



(그림 1) 서버 기반의 미디어 스트리밍
(AOL Webcast Live 8 concert)

(그림 1)은 미디어 서버와 미디어 스트리밍을 위해 1500 개의 분배서버로 이루어진 CDN(Content Delivery Network)이 구축된 경우이다. 만약 이 때 175,000 명의 동시 청취자가 있는 채널이 있고 각 300Kbps 의 미디어 스트리밍을 제공하고 있다면, CDN 과 청취자 사이의 대역폭은 50Gbps 가 필요하게 된다. 또한 분배서버 구축을 위한 비용도 만만치가 않을 것이다.

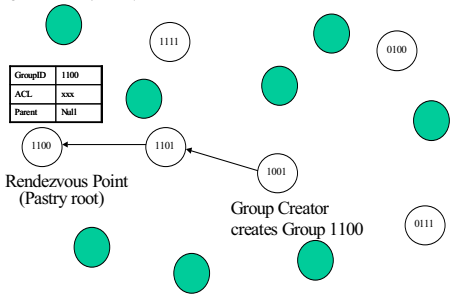


(그림 2) P2P 오버레이 망을 이용한 미디어 스트리밍

(그림 2)는 미디어 분배를 위해 P2P 망을 이용하는 경우를 보여준다. 서버는 단지 300Kbps 의 대역폭만 사용하고 나머지 분배는 피어간의 통신에 의한 P2P live multicast 방식에 의해 처리가 진행된다. 당연히 분배서버 구축을 위한 비용 및 서버의 부하가 줄어들게 된다.

P2P 기반의 미디어 분배를 위해 중요한 기술 중 하나는 P2P 오버레이 네트워크를 어떻게 구축하는가 하는 것이다. 미디어 스트리밍 서비스 가입자의 접속과 종료가 불규칙적으로 발생하기 때문에 효율적으로 이를 처리하기 위한 방법이 매우 중요하다. 기본적으로는 가상 오버레이 트리를 구성하는 방식이 사용되는데, 각 피어는 자신의 parent peer 로부터 미디어 데이터를 수신하고 이를 자신의 child peer 로 전달하는 구조이다. 이를 위해 동일 채널을 시청하는 peer 들간의 오버레이 트리가 구축되게 된다.

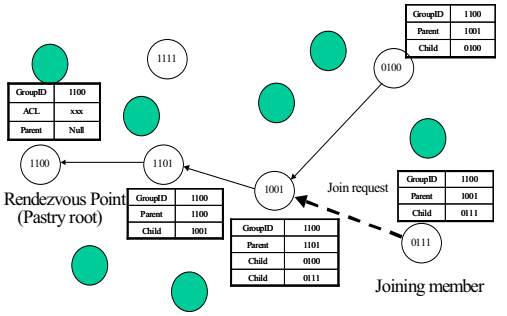
대표적인 P2P 기반의 응용계층의 오버레이 멀티캐스트 구조로 Castro 가 제안한 SCRIBE[5]가 있다. SCRIBE 는 객체의 위치 지정과 라우팅을 위해 Pastry[3]를 사용하였다. Pastry 는 DHT 기반의 오버레이 네트워크로 Prefix matching 기반으로 동작하는 특징을 갖는다. SCRIBE 는 그룹관리를 위해 Rendezvous Point(RP)를 두고 있다. (그림 3)은 SCRIBE 의 그룹 생성 과정을 보여준다.



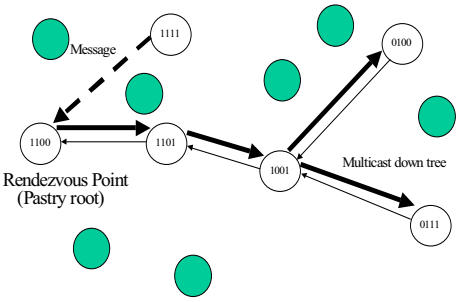
(그림 3) 그룹 생성 과정 (SCRIBE)

(그림 3)은 1001 이라는 ID 를 가진 피어가 1100 이라는 그룹을 생성하는 과정이다. 이 1100 이라는 그룹 ID 와 동일한 ID 를 소유한 피어가 Rendezvous Point 가 되는 것이며, Pastry 라우팅을 위한 Root 역할도 하게 되는 것이다. (그림 3)에서 1001 피어가 생성한 그룹 생성 메시지가 1101 피어를 통해 1100 으로 전달되는 것을 볼 수 있다. 이는 Prefix matching 기반의 Pastry 라우팅 테이블에 의해 결정된 경로이며, 이 경로에 포함되는 피어는 트리의 멤버로 참여하게 된다. 각 피어는 이 메시지 전달과정에서 자신의 parent peer, child peer 정보를 별도의 테이블에 저장하게 된다.

(그림 4)는 SCRIBE 의 그룹 Join 과정을 보여준다. 그룹에 Join 할 때도 동일하게 그룹 ID 로 라우팅 하는 과정이 필요하며, 라우팅 과정에서 트리가 구성된다. 이 것이 가능한 것은 Prefix matching 기반의 Pastry 의 특성 때문이다.



(그림 4) 그룹 Join 과정 (SCRIBE)



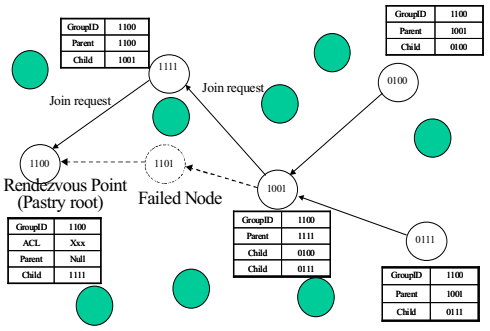
(그림 5) 멀티캐스팅 과정 (SCRIBE)

(그림 5)는 멀티캐스팅 과정을 보여준다. 1111 이라는 피어가 1100 이라는 그룹으로 멀티캐스팅을 요청하면 1100 을 root 하는 오버레이 트리로 데이터가 멀티캐스트 된다.

SCRIBE 에서 트리의 관리를 위해 각 child 피어는 자신의 parent 피어가 살아있는지 주기적인 메시지 전송을 통해 확인하고, 만약 parent 피어에 fail 이 발생한 경우 다시 그룹 ID 를 이용하여 Join 메시지를 전송한다. (그림 6)은 피어의 fail 발생시 트리 재구성 과정을 보여준다.

SCRIBE 외에도 미디어 스트리밍의 특성이나 요구사항에 따라 다양한 방식의 P2P 오버레이 망의 구축

이 가능할 것이다. 하지만 기본적으로 오버레이 트리를 구성하고 이를 통해 미디어를 배포하는 방식은 유사할 것으로 보인다.



(그림 6) 트리 재구성 과정 (SCRIBE)

3. 보안 고려사항

본 절에서는 P2P 기반의 오버레이 트리를 이용한 미디어 스트리밍 서비스 적용시에 발생할 수 잇는 보안 위협과 이에 대응하기 위한 보안 고려사항에 대해 논의한다.

P2P 기반 구조에서는 스트리밍 되는 미디어 데이터를 각 피어가 직접 전달하기 때문에 다양한 형태의 보안 위협이 존재할 수 있다. 특히 SCRIBE 와 같은 경우는 미디어에 대한 접근 권한이 없는 피어도 Pastry 라우팅 경로에 존재하면 오버레이 트리의 멤버로 참여가 되기 때문에 더 큰 위협이 존재한다. <표 1>에서 보안 위협을 정리하였다.

<표 1> P2P 기반의 미디어 스트리밍에 대한 보안 위협

보안 위협	설명
중간 피어의 콘텐츠 불법 취득	콘텐츠를 전달하는 중간 피어가 불법적으로 콘텐츠를 복제/취득
피어의 콘텐츠 전달 방해 공격	중간 피어가 콘텐츠를 엉뚱한 피어로 전달하거나, 전달을 중지. 이 경우 하위에 존재하는 피어들은 정상적인 콘텐츠 수신이 불가능
라우팅 방해 공격	중간 피어가 오버레이 트리 구축을 위한 제어 메시지를 위변조하여 전달. 라우팅 체계 붕괴.
DoS 공격	악의적인 피어들이 오버레이 트리 구축을 위한 제어 메시지를 위변조하여 특정 피어로 트래픽을 집중. DoS 공격 가능.
오버레이 망 성능 저하 공격	의도적으로 오버레이 트리에 가입(Join) 및 탈퇴(Leave)를 반복. 오버레이 트리 재구성 트래픽 폭주.
키 유출 문제	그룹 키 및 콘텐츠 복호화 키의 유출
ID spoofing 공격	다른 피어로 위장하여 상대 노드를 속이는 ID spoofing 공격

<표 1>의 보안 위협 중 대다수는 오버레이 트리에 참여하는 각 피어를 신뢰할 수 없기 때문에 발생하는 것이다. 피어의 콘텐츠 전달 방해공격, 라우팅 방해 공격, DoS 공격, 오버레이 망 성능 공격 등을 방지하기 위해서는 전체 라우팅 전달과정을 모니터링 할 수 있는 장치가 필요하다. SCRIBE 의 경우라면 Rendezvous Point 가 전체 tree 의 정보를 보유하도록 하고 각 피어와의 통신을 통해 주기적으로 정상적인 라우팅 수행 여부를 모니터링 할 수 있을 것이다.

또한 평판(Reputation)을 기반으로 하는 신뢰 관리(Trust management) 방법도 사용이 가능할 것이다. 평판 점수에 따라 오버레이 트리에 참여에 차등을 두는 방안도 가능하다.

P2P 는 그 특성상 참여와 탈퇴가 자유롭기 때문에 의도적으로 가입(또는 채널 접속), 탈퇴(또는 채널 접속 중단)을 통한 오버레이 망 성능 저하 공격이 가능하다. 이러한 공격은 가입과 탈퇴를 위한 시간 제한을 두는 방법으로 해결이 가능할 것이다. 예를 들어 채널접속/차단을 위한 사용자의 행위를 모니터링 하고 차단 이후 접속이 가능한 시간에 차등을 둘 수 있을 것이다.

그 밖에 그룹키 생성, 분배, rekeying 등의 그룹키 관리 방법과 오버레이 트리 관리를 위한 제어메시지 보호 및 이를 위한 키 관리 방법 등에 대한 고려가 필요할 것이다. 또한 오버레이 트리 구축을 위해 구축된 각 피어의 라우팅 테이블의 정상 구축 여부를 확인하고 무결성을 보장하기 위한 방안도 마련이 필요할 것이다.

4. 결론

P2P 기반의 미디어 스트리밍 서비스는 서버의 비용 및 대역폭 절감 측면에서 매우 큰 장점을 가지고 있지만, 보안성 측면에서는 많은 위협이 존재하는 서비스 중 하나이다. 본 논문에서는 이러한 보안 위협에 대해 분석하고 이에 대응하기 위해 필요한 보안 고려사항들을 논의하였다. 신뢰성이 확보된다면 P2P 기반의 미디어 스트리밍 서비스는 IPTV, VoD 서비스 등 다양한 응용에 활용이 가능할 것이다.

참고문헌

[1] http://www.joost.com/
[2] Ion Stoica, Robert Morris, David Karger, M.Frans Kaashoek, Hari Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," ACM SIGCOMM'01, 2001
[3] A. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems," Proc. of the 18th IFIP/ACM Int'l Conf. on Distributed Systems Platforms (Middleware 2001). Heidelberg, Germany, Nov. 2001
[4] B.Girod, Transport of Real-Time Traffic over The Internet, Presentation slides, 2005
[5] M.Castro, P.Druschel, A.Kermarrec, and A. Rowstron, SCRIBE: A large-scale and decentralized application-level multicast infrastructure, IEEE Journal on Selected Areas in Communications, Vol.20, No.8, Oct 2002