BcN 멀티캐스트 기능 구조

A Functional Architecture of Multicast in BcN

광대역통합망기술 특집

박 혁 (H. Park) BcN설계팀 선임연구원
송종태 (J.T. Song) BcN설계팀 선임연구원
전경규 (K.G. Chun) BcN설계팀 책임연구원
이순석 (S.S. Lee) BcN설계팀 팀장

목 차

BcN에서의 멀티캐스트 특히 IPTV 방송서비스의 서비스 및 네트워크의 요구 사항을 살펴보고 기능 구조를 도출하였다. 방송서비스의 수익은 시청률에 민감하다. 특히 접속제어를 바탕으로 하는 BcN에서 IPTV 방송서비스를 제공한다면, 표본추출 방식의 기존 방송과 달리 시청자의 거동을 전수 조사할 수 있어 수익과 시청률의 관계는 더욱 밀착될 것이다. 품질 문제로 시청자를 잃지 않기 위해서는 전달망은 패킷의 손실을 최대한 막아야 하며, 네트워크 장애 발생시 서비스의 장애가 최소한으로 억제되도록 설계되어야 한다. 따라서 망은 OAM 기능 및 경로 보호 기능을 가져야 하며, 악의적인 사용자의 공격에 대한 대비책도 갖추어야 한다. 본 고에서 논의한 기능 구조에서는 서비스 인증 후 개별 채널 변환을 L2 스위치에서 접속제어하여 적법하지 않은 사용자의 접근을 막도록 하였으며, 코어 네트워크에서는 Multicast MPLS를 사용하여 OAM 및 경로보호를 제공할 수 있도록 하였다. 또한 채널 변환에 대한 정보를 파악함으로써, 자원의 사용 및 개별 사용자의 거동을 파악할 수 있도록 하였다.

Ⅰ. 서론

멀티캐스트는 다수의 수신자에게 동일한 정보를 일대일 방식으로 보내고자 할 때 부딪히게 되는 대역폭의 낭비, 확장성 제한, 수신자 간 지연 등의 문제를 해결할 수 있는 방법이다. 멀티캐스트 서비스는 크게 실시간 서비스와 비실시간 서비스로 나눌 수 있다. 실시간 서비스로는 E-learning, 화상회의, interactive game 등을 들 수 있으며, 비실시간 서비스로는 다수의 서버 혹은 PC를 대상으로 하는 데이터 분배 서비스, 즉 소프트웨어 분배, 데이터베이스 복제 등이 있다[1].

IPTV의 방송 서비스는 멀티캐스트를 대규모로 사용하는 최초의 서비스가 될 것으로 보인다. IPTV는 통신 채널로 방송서비스와 VOD 서비스 그리고 그 외 부가 서비스를 제공하는 서비스를 말한다. VOD 서비스는 주문에 따라 영상을 송출하는 방식이므로 유니캐스트 방식에 의하여 서비스가 제공되지만 방송 서비스는 다중에게 동일한 내용의 콘텐츠를 전달하여야 하므로 멀티캐스트 통신을 이용하여 서비스가 제공된다. 방송 서비스는 신호 손실의 검출 및 네트워크의 보수가 매우 어려울 뿐 아니라 손실이 발생했을 때 사용자의 반응도 일반적인 통신서비스와 다르다. 웹 서핑과 같은 애플리케이션에서는 일시적으로 통신이 중단되더라도 사용자들이 느끼지 못하고 지나갈 수 있으나, TV 시청자는 TV 화면의 끊김 및 화질의 저하에 매우 민감하다. 방송서비스는 기존의 공중파 및 케이블 방송 등과 경쟁하여야 하므로 실시간성 및 안정성 그리고 화질에 있어서 기존의 방송과 최소한 유사하거나 더 나은 품질을 제공하여야 할 것이다. 방송서비스는 실시간으로 공공을 대상으로 하는 서비스로 사용자의 수가 많고 요구하는 QoS 및 대역폭이 높으므로 단방향 멀티캐스트 서비스 중에서 가장 까다로운 요구조건을 가지는 서비스로 볼 수 있다.

BcN 망에서 멀티캐스트 특히 그 중에서도 IPTV의 방송서비스를 지원하기 위해서는 먼저 그 기능구조의 설계가 필요할 것이다. 본 고에서는 멀티캐스트 애플리케이션 중 특히 가장 가까운 시일에 전개될 것으로 보이는 IPTV 서비스를 BcN에서 제공하기 위하여 추가되어야 할 요소 및 그 기능을 기술하였다. 기능구조를 설계하기 위해서 상위 요구사항으로부터 하위 요구사항을 도출하는 방식을 택하였다. 먼저 Ⅱ장에서 서비스 요구사항을 살펴보고 이를 기반으로 네트워크 요구사항을 Ⅲ장에서 정리하였다. Ⅳ장에서는 네트워크 및 서비스 주요 요구사항을 충족할 수 있도록 설계한 기능 구조를 설명하였다.

● 용 어 해 설 ●

IPTV: ITU-T의 FG IPTV는 "필요한 레벨의 QoS/QoE, 보안, 상호작용성(interactivity), 신뢰성을 제공하도록 관리되는 IP 기반의 망을 통하여 전달되는 텔레비전/비디오/오디오/텍스트/그래픽스/데이터와 같은 멀티미디어 서비스"로 정의하고 있다. 이 정의는 유선 및 무선 구간을 모두 포함하는 것으로 해석할 수 있다.

Ⅱ. 서비스 요구사항

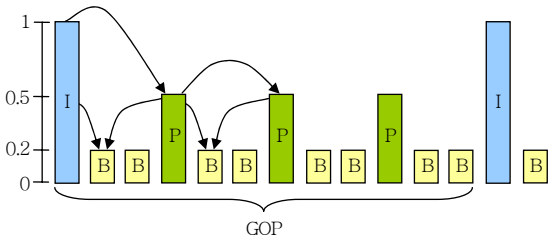
1. 압축된 영상 트래픽 특성

압축되지 않은 영상 트래픽은 화면의 손상이 해당 화면에만 국한된다. 보통 사람들은 한 두 개의 화면이 빠지거나 혹은 손상된 경우에 이를 감지하기 어렵다. 그러나 SD급의 경우 통상 270Mbps, HD급은 통상 1.5Gbps 정도의 대역폭을 요구하므로 이를 그대로 통신망에서 서비스 할 수 없다. 따라서 압축 기술을 사용하게 된다. 현재의 가장 앞선 압축기술인 H.264 혹은 MPEG-4는 200:1 이상의 압축률을 보이고 있어 SD급은 2~3Mbps, HD급은 8~10Mbps의 대역폭으로 전송이 가능하다[2]. 반면 압축된 영상에서는 각 화면이 연관되어 있으므로 화면이 손상되거나 혹은 특정 화면이 빠진 경우에 이 영향이 눈으로 감지하기에 충분한 시간 동안 지속될 수 있으므로 화면의 손상 및 누락에 민감하다.

압축된 영상은 독립적으로 재생할 수 있는 I (Intra) 화면을 주기적으로 배치하여 손상 누적을 방지

한다. 이 주기를 GOP라고 부른다. (그림 1)은 15개의 화면으로 이루어진 GOP의 예를 보여주고 있다. (참고로 국내에서 사용되고 있는 북미규격 TV 방송의 경우 초당 약 30 화면을 사용하므로 이 길이는 약 0.5초에 해당된다.) P 화면은 하나의 I 혹은 다른 P 화면을 참조하며, B 화면은 두 개의 I 혹은 P 화면을 참조한다. (그림 1)에서 볼 수 있는 바와 같이 하나의 GOP 내에 있는 모든 화면은 I 화면을 직, 간접으로 참조한다[2]. 따라서 I 혹은 P 화면에서 손상이 발생하면 다음의 I 화면이 올 때까지 이 손상이 계속 누적될 수 있다. B 화면은 이를 참조하는 화면이 없으므로 손상이 하나의 화면으로 국한된다. 최근의 압축 기술에서는 B 화면을 참조하는 구조도 거론되고 있다. 이러한 영상 구조는 디코딩에도 영향을 미친다. 디코더는 I 화면이 있어야 재생을 시작할 수 있으므로 평균적으로 하나의 GOP가 재생되는 시간의 절반에 해당하는 시간을 디코딩의 시작을 위하여 기다려야 한다.

하나의 GOP의 길이에 대한 특정한 규정은 없으나 GOP의 길이에 따른 장단점은 있다. GOP를 구성하는 화면 수가 늘어나면 전송에 필요한 대역폭은 작아지지만 I 화면 간의 간격이 길어지므로 ① 채널 전환시 I 화면을 기다리는 시간이 길어지므로 전환이 느리다. ② I 화면 손실시 영향을 받는 시간이 길어진다. ③ 빠른 화면 변환이 있는 비디오에서는 P, B 화면이 길게 이어질 경우 누적되는 에러가 커져서 화질이 상대적으로 나쁘다. 기존의 TV에 익숙해 있는 시청자에게 긴 채널 변경 시간은 큰 저항요소이다. 또한 I 화면이 손실되었을 때 수 초 동안 방송이



(그림 1) GOP의 구성 예(각 화면을 표시하는 막대의 높이는 대략적인 대역폭 요구량을 표시)

중단된다면 이 역시 큰 문제가 된다. 화면이 빠르게 전환되면 압축에 의한 손상 누적이 커져서 화면이 나빠질 수 있다는 점도 고려되어야 한다. 일반적인 드라마류는 화면 전환이 느리므로 큰 문제가 되지 않지만 SF, 뮤직비디오, 전쟁이나 액션 장면이 많이 등장하는 콘텐츠에서는 문제가 될 수 있다.

2. 화질 유지

비디오 트래픽 전송 중 잡음에 의하여 bit 단위의 에러가 발생하거나, 네트워크의 혼잡에 의하여 패킷을 잃어버릴 수 있으며, 네트워크의 장애로 다수의 화면을 전송 받지 못할 수도 있다. Bit 에러 혹은 패킷 손실이 발생하면 시청중이던 화면의 일부가 사라지거나, 화면 전체에 잡음이 발생할 수도 있으며 중요 정보가 있는 부분이 손상되면 화면이 정지할 수도 있다. 화질은 TV 시청자들이 민감하게 반응하는 사항이고 통신사업자들은 TV 방송서비스에서 CATV 사업자들과 경쟁해야 하는 상황이므로 화질의 유지는 필수적이다.

네트워크에서 장애가 발생하면 다수의 화면이 없어지게 되므로 복구시간에 따라서는 수 분 이상 화면이 정지할 수 있다. 지상파 방송의 경우 이런 사고는 중대한 방송사고로 취급되며 언론 매체에서 보도하고 있는 것을 볼 수 있다. IPTV 서비스에서는 이 문제가 더 심각할 수 있다. Pay TV, 시청률과 광고비의 연계, 드라마에 나오는 물품을 바로 클릭하여 구매할 수 있게 하는 서비스 등은 IPTV의 TV 방송서비스에서 자주 언급되는 주요 비즈니스 모델들이다. 만약 pay TV로 중요 스포츠 이벤트를 관람중 화면이 수 분간 끊어지거나, 다수의 광고가 계획된 프로그램에서 화면 끊김이 발생하여 TV를 끄거나 다른 매체를 이용함으로써 시청률이 하락하거나, 드라마에 나오는 상품을 협찬하여 T-commerce 계약을 한 경우에 패킷 손실 등으로 상품에 대한 정보가 사라지거나 혹은 계약한 화면 전체가 사라지는 경우 네트워크 제공자가 재정적인 책임을 져야 하는 경우도 발생할 것이다.

3. 채널 변환 시간

표준화가 필요한 사안이지만 대략 1초 이내에는 채널 변경이 가능해야 할 것으로 보인다[3]. 네덜란드의 TNO는 최근 채널 변환 시간에 대한 모델 및 측정 결과를 ITU SG12에 기고하였다[4]. 이 기고서는 채널 변환 시간과 사용자가 인지하는 만족도 사이의 관계를 MOS로 표현하였다. 채널 변환 시간과 MOS 관계의 경험적인 모델을 제안하고 13명의 피실험자를 대상으로 실험하였다. 실험 결과는 모델에 잘 일치하였으며 MOS 3.5 이상을 만족하기 위해서는 채널 변경 시간이 0.43초 이하이어야 한다는 결과를 얻었다.

Cisco는 두 종류의 STB에 대하여 채널 변환 시간을 측정한 결과 30 화면으로 이루어진 GOP를 사용했을 때 1~2초 정도의 값을 얻었다[5]. 이 값은 IGMP[6] JOIN/LEAVE 지연, 네트워크 JOIN 시간, 지터 버퍼, I 화면 대기, 디코더의 성능 등 다양한 요인에 기인한다. GOP의 시작 부분에 있는 I 화면을 받아야 디코딩이 시작되므로 이를 기다리는 시간은 0부터 GOP의 길이까지 임의의 시간이 될 수 있으며 확률밀도는 균일하다. GOP의 길이가 0.5~수 초 정도이므로 이 시간이 큰 부분을 차지하지만 이는 압축을 위한 인코딩/디코딩과 관련 있으며, 네트워크의 성능과 직접적인 관련은 없다. 채널 변환 시간 중 네트워크 관련 부분은 ① 네트워크에서 발생하는 지터를 흡수하기 위한 지터 버퍼 시간 ② IGMP JOIN/LEAVE 지연 ③ 네트워크 JOIN 시간의 세 가지이다. 네트워크에서 소비되는 시간이 차지하는 비율이 작기는 하지만 요구되는 채널 변환 시간이 매우 짧으므로 이 부분을 최대한 줄여야 한다.

4. 서비스 이용 상황 정보 파악

맞춤형 광고, 시청률에 따른 광고료의 연동 등 시청자의 행동에 따른 수익 모델은 IPTV의 방송서비스에서 수익 모델을 논의할 때는 많이 거론되는 것들이다. 이를 위하여 요구되는 것은 개별 시청자의 콘텐츠 및 광고에 대한 반응을 파악하는 것이다. IPTV 방송서비스에서 제공할 수 있는 양방향성은 이에 대한 기초를 마련해 줄 수 있다. IPTV 방송서비스에서는 광고 및 본 콘텐츠의 화면에 노출되는 상품을 클릭하여 특징, 가격 등의 정보를 제공받고 구매까지 할 수 있는 서비스가 등장할 것으로 보인다. 서비스 제공자가 시청자가 어떠한 콘텐츠를 즐겨 보는지, 이때 제공되는 양방향 서비스에 대하여 어떤 반응을 보이는지, 그리고 실제로 어떤 상품들을 구매하는지 파악할 수 있다면, 이를 기반으로 개인별 맞춤광고 등과 같은 새로운 비즈니스 모델을 계획할 수 있는 토대를 마련할 수 있을 것이다.

Ⅲ. 네트워크 요구사항

네트워크에 대한 요구사항은 서비스 요구사항과 네트워크의 효율성 추구라는 두 축으로부터 도출할 수 있다. 서비스의 요구사항은 중단 없이 계약된 화질의 영상을 사용자에게 제공할 수 있도록 해달라는 것으로 요약할 수 있다. 네트워크에서 이를 방해하는 것으로는 노드나 링크에서 발생할 수 있는 사고, 네트워크의 혼잡, 악의적인 공격 등을 들 수 있다. 본 고에서는 네트워크에 대한 요구사항을 액세스 네트워크와 코어 네트워크로 나누어 기술하였다. 액세스 네트워크는 가격에 대한 압력이 높은 부분으로 대역폭이 제한되어 있고, 제어가 어려운 구간이지만 액세스 네트워크에서의 사고는 지역적으로 국한된다. 코어 네트워크에서는 개별 장비에 대한 가격 압력은 액세스 네트워크보다 높지 않지만 코어 네트워크에서의 사고는 다수의 액세스 네트워크에 미치게 되므로 이에 대한 대비책이 필요하다.

1. 액세스 네트워크

액세스 네트워크에서 멀티캐스트 서비스를 하고자 할 때는 자원관리를 효율적으로 할 필요가 있다. 액세스 구간에서 특정 장비부터 점대점 방식의 유니캐스트를 사용하여 멀티캐스트를 지원하는 방법도 가능하지만 이 경우 다수의 수신자가 동일한 채널을

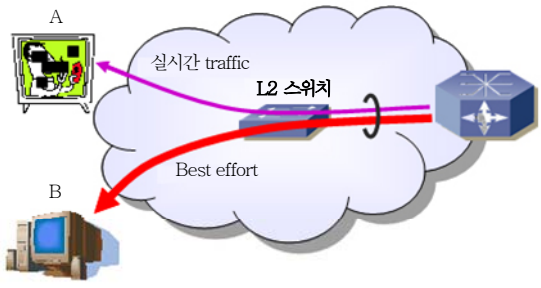
시청하고자 하는 경우 하나의 물리적 링크에 동일한 멀티캐스트 패킷이 수신자 수만큼 중복되어 흘러가게 되므로 그만큼 대역폭을 낭비하게 되며 수신자의 수가 늘어날 때 대처할 수 없다. 자원이 부족한 액세스 네트워크에서 요청하지 않은 수신자에게 멀티캐스트 패킷을 흘려 보내면 그 수신자가 요청한 다른 서비스의 질을 떨어뜨릴 수 있다. 이더넷 스위치는 source MAC learning을 통하여 수신자의 MAC 주소와 위치를 확인하고 이 주소를 수신 주소로 하는 프레임이 입력되면 해당 포트로 송신하게 된다. 그러나 멀티캐스트 수신자는 송신 주소로 멀티캐스트 MAC 주소를 사용하지 않으므로 멀티캐스트 주소를 수신 주소로 하는 프레임은 항상 모든 포트로 송신되게 된다. 이를 막기 위하여 IGMP snooping[7] 혹은 GMRP[8]가 사용될 수 있다.

채널 변경 시간을 줄이기 위하여 그룹 멤버십에 대한 JOIN 및 LEAVE 시간을 최소화하여야 한다. 멀티캐스트는 일대다 통신이므로 수신자들은 하나의 그룹으로 생각할 수 있다. 그룹에 가입되어 있는 멤버만 수신을 할 수 있다. 따라서 특정 멀티캐스트 주소를 가지는 패킷을 수신할 것을 요청하는 것은 해당 멀티캐스트 주소의 수신자 그룹에 합류(JOIN)하는 것으로 볼 수 있으며, 수신을 거부하는 것은 그룹에서 탈퇴(LEAVE)하는 것으로 볼 수 있다. 그룹 멤버십에 대한 JOIN 시간은 채널 변경 시간에 직접적으로 영향을 미치지만 일반적으로 JOIN 시간은 크지 않다. 그러나 IGMP를 사용하는 경우에는 LEAVE 시간이 길어질 수 있다. IGMP는 그룹 멤버십을 집합 개념으로 관리하므로 개별 그룹 구성원의 상태를 꼭 알아야 하는 것은 아니다. 따라서 LEAVE 메시지를 받으면 이 그룹에 남아 있는 사용자가 있는지를 다시 한 번 확인한다. 이에 걸리는 시간은 조절이 가능하기는 하지만 초기 설정값을 사용하면 약 2초 정도가 필요하다. 만약 LEAVE 요청을 한 사용자가 그 그룹의 마지막 구성원이라면 이 그룹에 대한 송신을 중지하여야 하지만 IGMP를 사용하면 이것이 2초 정도 유예된다. 채널을 계속 바꾸면서 마음에 드는 채널을 찾는 수신자는 일반적으로 흔하다. 이 경우 기존의 채널을 해제한 후 JOIN을 허용한다면 2초의 유예가 채널 변환 시간에 더해지게 되며 채널 해제 전에 JOIN을 허용한다면 해제되지 않은 채널이 계속 대역폭을 점유하게 되므로 주어진 대역폭을 사용하지 않는 트래픽이 점유하여 새로운 JOIN이 불가능해지는 상황이 발생할 수 있다. 따라서 그룹에 대한 LEAVE 처리가 늦어지면 JOIN 메시지 발송 간격도 늘이는 것이 안전하다. 이를 방지하기 위하여 LEAVE 메시지를 송신한 단말의 ID (MAC 주소, IP 주소 등)를 확인하여 그룹 구성원을 관리하는 방법도 있다[9].

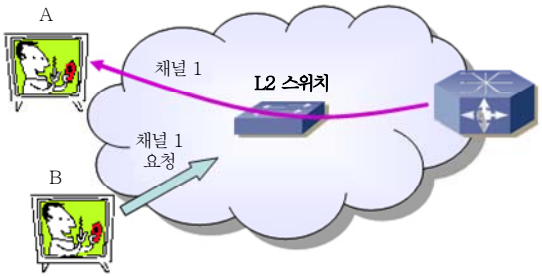
액세스 구간의 L2 스위치는 프레임에 대한 classification을 지원해 줄 필요가 있다. (그림 2)에서와 같이 best effort 트래픽이 많아지는 경우 실시간 트래픽과 링크를 공유하는 부분에서 혼잡에 의하여 실시간 트래픽의 손상이 발생할 수 있다. 이를 위하여 IPTV와 같이 민감한 서비스를 제공하기 위한 트래픽은 best effort 트래픽이 범람하더라도 영향을 받지 않도록 보호해 줄 필요가 있다.

● 용 어 해 설 ●

IGMP: IGMP는 IPv4에서 멀티캐스트 데이터 수신자를 관리하기 위하여 IETF에서 정의한 프로토콜로 현재 IGMPv3가 RFC로 채택되어 있다. 수신자를 관리하는 라우터는 인터페이스별로 각각의 멀티캐스트 주소에 대하여 소스 관련 정보로 이루어진 수신상태를 관리하고 이 정보를 상위의 멀티캐스트 라우팅 프로토콜에 제공한다. IPv6를 위해서는 MLD가 정의되어 있으며 MLDv1은 IGMPv2에, MLDv2는 IGMPv3에 각각 대응된다.



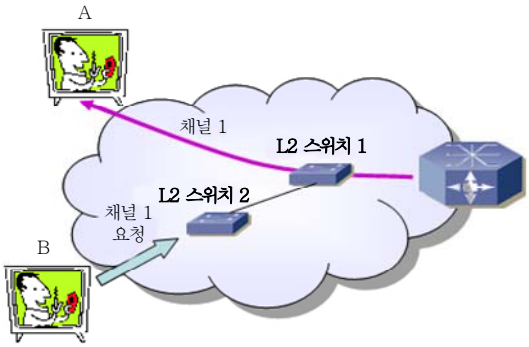
(그림 2) Best Effort 트래픽에 의한 실시간 트래픽의 장애 발생



(그림 3) L2 스위치에서 접속제어 필요성

액세스 네트워크에서 사용되는 L2 스위치가 가져야 할 중요한 기능 중의 하나로 접속제어를 들 수 있다. 유니캐스트 통신의 경우에는 접속제어를 에지 라우터에서 수행하는 것도 가능하다. 그러나 멀티캐스트의 경우에는 에지 라우터에서 접속제어를 하면 권한이 없는 수신자가 수신하는 것을 막을 수 없는 경우가 발생한다. (그림 3)에서와 같이 권한이 있는 수신자가 먼저 특정 채널에 대하여 수신을 요구하여 멀티캐스트 스트림이 이미 L2 스위치까지 내려와 있는 경우에 권한 없는 수신자 B가 같은 채널을 요청한다면 이 요청은 접속제어를 받지 않고 수신자 B에게 전달될 수 있다. 따라서 L2 스위치는 하위에 있는 수신자에 대한 권한 정보를 알고 있어야 하며 이에 따라 접속제어를 할 수 있어야 한다.

실제 IPTV의 방송서비스에서는 콘텐츠를 암호화하여 권한 없는 수신자가 멀티캐스트 스트림을 수신하더라도 시청을 할 수 없도록 막는 방법을 사용할 것이다. 그러나 암호는 언제나 풀릴 수 있는 개연성이 있으며 이보다 더 중요한 것은 이것이 네트워크에 대한 일종의 DQoS[10] 공격으로 사용될 수 있다는 점이다. 다단의 L2 스위치가 계층적으로 연결되어 있는 망에서는 다수의 채널이 최상층 L2 스위치까지 내려와 있을 가능성이 높다. 이 경우 (그림 4)의 B와 같은 악의적인 사용자가 최상층 L2 스위치에 내려와 있는 채널에 대하여 요청을 발송하면 이 채널은 사용자가 없는 L2 스위치 1과 L2 스위치 2 구간을 채우게 된다. 특히 IPTV 방송서비스에서는 모든 방송원에 대한 정보가 노출될 가능성이 많으므로 악의적인 사용자가 바이러스 등을 사용하여

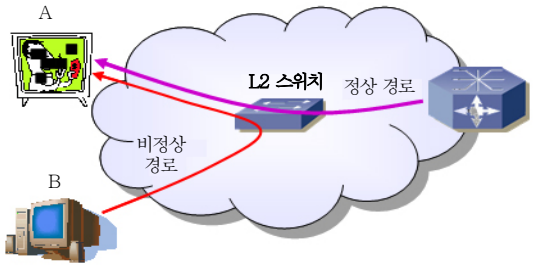


(그림 4) 불법적인 수신 요청에 의한 공격

모든 IPTV 방송 채널에 대하여 요청을 발송하도록 하면 망의 대역폭을 모두 의미 없는 데이터로 채울 수 있는 가능성이 있다. 만약 이 공격을 동기화하면 전국적으로 망의 성능 저하를 가져올 수 있는 가능성도 배제할 수 없다. 따라서 L2 스위치에서 접속제어를 수행하는 것이 반드시 필요하다.

이러한 공격은 접속제어 위치에 관계없이 IGMP snooping이나 GMRP를 사용하는 L2 스위치에 있어서 제어계에 대한 직접적인 DDoS 타입 공격의 수단이 될 수도 있다. 다수의 수신자 단말에서 동시에 채널에 대한 요청을 발송하여 계획된 처리 용량을 초과하도록 하면 L2 스위치의 제어계를 마비시킬 수 있는 가능성이 있다. IGMP snooping 혹은 GMRP를 제어계의 소프트웨어로 구현하여 사용하는 경우 처리 속도가 느리므로 특히 취약할 수 있다. 이 역시 동기화될 경우 전국적으로 채널 변환이 불가능해지는 등 서비스 질을 현저하게 떨어뜨려 사업자에게 타격을 줄 수 있는 가능성이 있다. 이 공격에 대응하기 위해서는 비정상적인 JOIN 요청의 패턴을 분석하고 이를 처리하는 과정에 들어가기 전에 막는 방법이 필요하다.

최전방 L2 스위치에서는 JOIN 요청뿐 아니라 멀티캐스트 프레임에 대한 접속제어도 수행해야 한다. (그림 5)에서 허용된 수신자 A가 특정 채널에 대하여 수신 요청하면, L2 스위치는 해당 멀티캐스트 주소를 가지는 프레임을 A가 연결된 포트로 보내도록 필터링 데이터베이스를 갱신한다. 만약 이 때 다른 사용자 B가 같은 멀티캐스트 주소를 가지는 프레임



(그림 5) 위조된 패킷을 사용한 공격

을 발송하면 이에 대한 대비가 없는 L2 스위치는 이 프레임을 A가 연결된 포트로 발송하게 된다. STB가 발송자의 MAC 주소를 인식하여 필터링하는 기능을 가지고 있지 않다면 조작된 패킷은 화질을 떨어뜨릴 수 있는 가능성이 있다. STB가 이 기능을 가지고 있다 해도 조작된 멀티캐스트 프레임의 양이 많아지면 서비스를 방해할 수 있다. 이러한 공격은 특정 시간에 동시에 현재 수신하고 있는 패킷을 재발송하도록 조작하는 것만으로도 목적을 달성할 수 있다. 따라서 L2 스위치는 허가된 경로 이외의 포트에서 들어오는 멀티캐스트 프레임을 차단하는 기능을 가져야 한다.

2. 코어 네트워크

코어 네트워크에서의 사고는 다수의 사용자에게 영향을 미칠 수 있으므로 코어 네트워크에서는 무엇보다 네트워크의 안정성이 중요하다. 코어 네트워크는 다수의 전송장비와 라우터 등으로 이루어져 있으므로 개별 장비의 사고 확률이 낮더라도 전체 망에서의 사고는 자주 일어날 수 있다. 이러한 사고는 아무리 짧더라도 비디오를 구성하는 프레임의 손실을 수반하게 되므로 그 영향이 클 수 있다. 따라서 이를 감지하고 보호할 수 있는 방법이 필요하다. 특히 라우터의 장애는 이를 검출하는 데만 수십 초의 시간이 걸릴 수 있어 이에 대한 대응책이 필요하다.

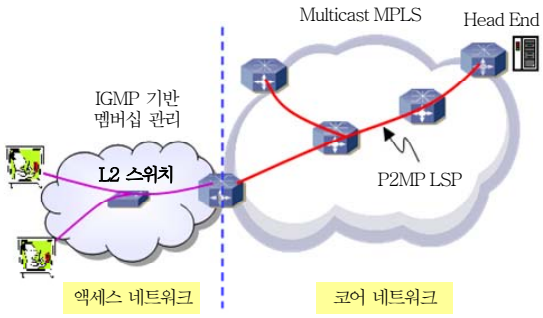
패킷의 손실 및 패킷 지터를 최소화해야 한다. 패킷의 손실은 곧 화질의 저하로 이어진다. 압축된 비디오에서 I 화면이나 P 화면의 패킷이 손실되면 이 손실에 의한 피해는 해당 GOP의 끝, 즉 새로운 I 화면에 의하여 갱신되는 시점까지 영향을 미치므로 시청자에게 쉽게 감지된다. AT&T의 IPTV 서비스인 U-verse는 출범에 앞서 시범서비스 중 분당 약 2개꼴의 패킷 손실이 발생하여 화질이 떨어져서 시청자들의 불만을 초래한 예가 있다[11]. 시청자는 화질의 저하에 민감하며 특히 T-commerce와 연계된 콘텐츠나 광고에서는 화질이 상품에 대한 선호도를 결정할 수 있으므로 패킷 손실 관리는 매우 중요하다. 화질에 대한 평가가 광고 계약 가격의 결정요인이 되는 상황도 배제할 수 없다. 패킷의 도착 시간의 지연 편차가 커지면 STB는 이를 재조합하기 위한 버퍼링 시간을 충분히 확보해야 하므로 채널 변경시 이를 위한 시간이 추가된다. 즉 패킷 지터를 최소화하여야 한다.

코어 네트워크에서도 역시 네트워크에 대한 악의적인 공격을 막을 수 있는 방법이 필요하다. 공격은 제어 패킷의 조작, 위조된 멀티캐스트 패킷의 발송과 같은 형태로 이루어질 수 있다. 제어 패킷의 조작에 대한 대응은 주로 암호화 방법을 사용한다. 위조된 멀티캐스트 패킷이 유입되면 전 네트워크에 영향을 미칠 수 있어 이에 대한 대비도 필요하다.

Ⅳ. 멀티캐스트 기능 구조

1. 개관

BcN에서 멀티캐스트를 지원하기 위한 구조는 매우 다양할 수 있다. 코어 네트워크에서는 PIM-SM과 같은 IP 멀티캐스트 프로토콜을 사용할 수 있으며, 최근 개발되고 있는 multicast MPLS를 사용할 수도 있다. 액세스 네트워크에서의 그룹 멤버십 관리는 제어평면에서 수행하거나, IGMP 혹은 GMRP와 같은 프로토콜을 사용할 수도 있다. 본 논문에서는 액세스 네트워크에서의 멤버십 관리는 IGMP 프로토콜을 사용하고, 코어 네트워크에서는 multicast MPLS[12]를 사용하는 구조를 고려하였다((그림 6) 참조). NCP[13]가 직접 L2 스위치의 필터링 데이터베이스를 제어하는 방식은 채널 변경시 시간이 많



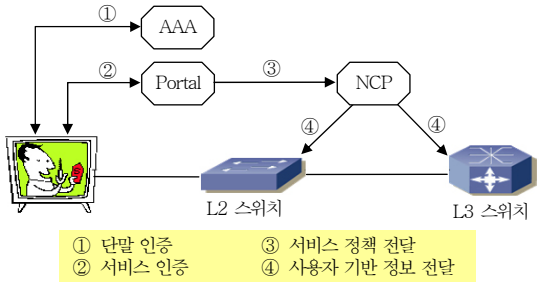
(그림 6) 고려하고 있는 멀티캐스트 망의 개략도

이 걸릴 수 있고, 채널 변경 요청을 사용한 DDoS 공격시 모든 채널 변경 요청이 한 곳으로 몰리므로 서비스 전체를 마비시킬 수 있는 문제점이 있다. 따라서 분산하여 처리할 수 있는 방식 중 현재 많이 이용되고 있는 IGMP를 고려하였다. 코어 네트워크에서 IP 멀티캐스트는 링크나 노드의 장애 시에 실시간으로 검출할 수 있는 방법이 없어 multicast MPLS의 사용을 고려하였다. Multicast MPLS는 아직 IETF에서 draft 상태에 있으나, MPLS의 OAM 및 보호절체 기능을 사용하여 제어 가능한 네트워크를 구현할 수 있을 것으로 기대하고 있다.

2. 최초 접속 시나리오

단말이 네트워크에 최초로 접속할 때의 과정을 (그림 7)에 나타내었다. STB는 전원을 켠 후 최초 접속할 때 인증 서버인 AAA 서버로부터 단말 인증을 받게 된다. 단말 인증을 받은 STB는 서비스 포털(IPTV의 경우에는 IPTV 포털)로부터 서비스에 대한 접속인증을 받는다. 서비스 포털은 인증을 요청한 사용자의 서비스 등록에 관한 정보, 즉 사용자가 접속할 수 있는 채널 및 서비스에 관련된 정보를 NCP로 넘겨준다. NCP는 이를 바탕으로 사용자와 연결된 L2 스위치에 서비스 관련 정책 정보를 넘겨준다. 이 정보는 사용자가 가입할 수 있는 멀티캐스트 그룹에 대한 정보, 즉 사용자가 IGMP를 통하여 JOIN을 신청하여 시청할 수 있는 채널의 멀티캐스트 주소에 대한 정보이다.

앞에서 언급한 바와 같이 그룹 멤버십의 관리는

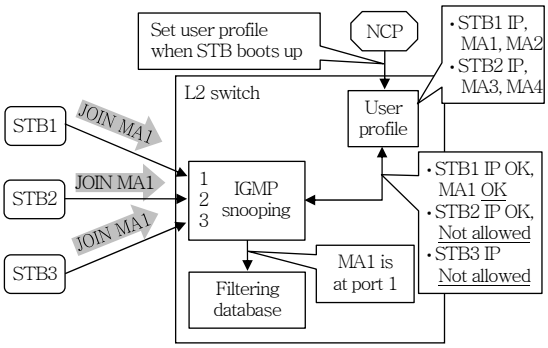


(그림 7) 단말 최초 접속 시나리오

IGMP를 사용하는 것을 고려하였으나 IGMP는 L3 프로토콜이므로 L2 스위치에서는 이를 인식할 수 없다. 따라서 서비스 관련 정책 정보를 받더라도 L2 스위치만으로는 이것을 적용할 수 없다. 그러므로 L2 스위치에 IGMP 프록시를 두어 IGMP 패킷을 읽어보는 것(snooping)을 고려하였다. IGMP 프록시는 IGMP 메시지에 대한 snooping시 사용자 기반 정보를 참조하여 요청을 수락하거나 거절하게 된다.

3. 채널 변경 시나리오

(그림 8)에 채널 변경 시의 L2 스위치의 동작을 예시하였다. 최초 접속 시에 NCP는 L2 스위치에 서비스와 관련한 사용자의 프로파일을 내려준다. 이 프로파일은 사용자의 IP와 가입할 수 있는 group address와 같은 정보를 가질 수 있다. 그림의 예에서는 세 개의 STB 중 STB1과 STB2만 인증이 되어 있으며, STB1은 멀티캐스트 주소 MA1 및 MA2, 그리고 STB2는 MA3 및 MA4에 대해서만 인증이 되어 있는 것을 가정하였다. 세 개의 STB (STB1,

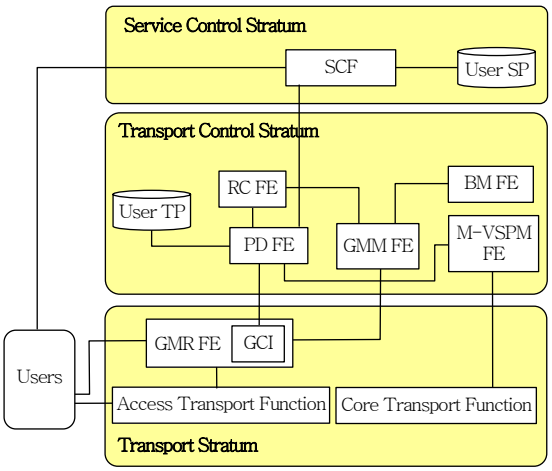


(그림 8) 사용자 정보에 따른 채널 변경 처리

STB2, STB3)가 IPTV의 특정 채널, 즉 멀티캐스트 주소 MA1에 대하여 IGMP 메시지를 사용하여 가입 요청을 하면 L2 스위치의 IGMP 프록시는 이 패킷의 내부를 읽어보고 이 내용을 알게 된다. 사용자 프로파일을 참고해 보면 STB1만이 멀티캐스트 주소 MA1에 접속하는 것이 인증되어 있으므로 IGMP 프록시는 STB1이 연결되어 있는 1번 포트로만 멀티캐스트 프레임이 전달되도록 필터링 데이터베이스를 갱신해 준다. L2 스위치에서는 이 외에도 비정상적인 IGMP JOIN 메시지, 즉 DDoS 공격을 위한 메시지를 IGMP 프록시에 전달되기 전에 차단하는 기능이 필요하다. 이를 위해서는 DDoS 공격에 의한 메시지 패턴을 인지하는 것이 필요할 것으로 보인다. 이 기능을 어떠한 방식으로 구현할 것인지, 그리고 이를 위하여 필요한 기능이 무엇이며 이 기능이 어디에 위치하는 것이 좋은지에 대해서는 더 많은 연구가 필요하다.

4. 기능 구조

앞에서 기술한 요구사항을 만족하기 위한 BcN [14] 멀티캐스트의 기능구조를 (그림 9)에 나타내었다. 기존의 BcN 기능구조에서 추가되는 부분은 GMM FE와 M-VSPM FE 그리고 GMR FE이다. GMR FE에는 GCI가 포함되어 있다. GMR FE는 사



(그림 9) 멀티캐스트 기능 구조

용자가 보내온 멀티캐스트 그룹 가입 요청, 즉 멀티캐스트 수신 요청을 처리하는 역할을 한다. IGMP snooping을 사용한다면 L2 스위치의 IGMP 프록시 및 에지 라우터의 IGMP 프로세스가 이에 대응된다. GCI는 각 개별 사용자에 대한 서비스 허가 사항에 대한 정보를 가지고 있다. GMR FE는 GCI의 정보를 바탕으로 사용자의 멀티캐스트 그룹 가입 요청을 처리한다. (그림 8)에서 사용자 프로파일을 가지고 있는 부분이 이에 대응된다. GMM FE는 멀티캐스트 그룹 가입 현황, 즉 각 가입자가 시청한 채널에 대한 정보를 수집하고 처리하는 기능을 한다. BcN에서 이미 정의되어 있는 기능들은 기본적으로는 같은 역할을 수행하지만 멀티캐스트 서비스를 제공하기 위해서는 역할의 확장이 필요한 경우도 있다.

BcN에서 SCF는 단말과의 시그널링을 제공하며 QoS 요구사항을 transport stratum으로 전달하는 역할을 한다. IPTV 멀티캐스트 서비스를 제공하려면 SCF는 transport control stratum에 사용자의 서비스 가입 현황, 즉 사용자가 시청할 수 있는 채널 및 제한사항 등을 알려줘야 할 것이다. IPTV와 같이 방송원에 대한 특성이 잘 알려져 있는 서비스에 있어서는 채널별 QoS 요구사항을 서비스 신청 시마다 내려주는 것보다는 미리 transport control stratum이 알고 있는 것이 적절할 것으로 보인다. PD FE는 SCF로부터 받은 사용자 정보와 RC FE로부터 받은 망의 자원에 대한 정보를 바탕으로 사용자에 대한 정보를 정리하여 transport stratum의 GCI로 보내준다. GMR FE는 GCI를 참조하여 그룹 가입 요청을 수락하거나 거절할 수 있다. GMR FE에서 발생한 그룹 가입 및 현황은 GMM FE가 취합한다. GMM FE에서 취합하는 정보는 서비스 가입 정보와는 달리 사용자가 실제로 어떤 채널을 어느 시간대에 얼마나 오랜 시간 동안 시청했는지에 대한 구체적인 정보를 줄 수 있다. GMM FE의 정보는 RC FE에 제공되어 망에서 멀티캐스트 트래픽에 의한 망의 자원 점유 상황을 파악하는 데 쓰일 수 있으며, BM에 제공되어 정산에 사용될 수도 있다. 또한 서비스 제공자나 콘텐츠 제공자 혹은 광고주들은 이

정보를 바탕으로 전략을 세울 수도 있을 것이다. M-VSPM FE는 코어 네트워크의 멀티캐스트 LSP 경로를 계산하고 provisioning 하는 기능을 한다.

제시한 기능 구조의 모델에서는 사용자가 가입한 채널군 내에서 채널을 변경할 때는 이것을 새로운 서비스로 보지 않는다. 채널 변환을 새로운 서비스로 보는 모델을 사용한다면 사용자가 새로운 채널을 요청할 때마다 이를 SCF로 알려주고 서비스에 대한 인증을 받아야 한다. 따라서 L2 스위치의 필터링 데이터베이스의 갱신도 RACF를 통하여 제어계에서 직접 수행하는 것이 적절할 것이다. 만약 필터링 데이터베이스의 갱신을 IGMP snooping을 통하여 수행한다면 동일한 메시지를 다른 경로로 두 번 보내는 셈이 되므로 L2 스위치에 부담을 주면서 IGMP 프록시를 두는 이유가 불분명해질 수 있다. 후자의 모델은 앞에서 언급한 바와 같이 채널 변경을 공격의 수단으로 삼는 DDoS 공격이 있을 때 SCF의 과부하로 서비스 자체가 불가능해 질 수 있고 서비스 인증 절차로 인하여 채널 변경 시간이 오래 걸릴 가능성이 있어 고려하지 않았다.

V. 결론

본 고에서는 BcN에서의 멀티캐스트 서비스 특히 그 중 IPTV 방송 서비스를 위한 기능 구조를 제시하였다. 기능 구조의 설계를 위하여 서비스 요구사항 및 네트워크 요구사항을 먼저 살펴 보았으며 이를 지원할 수 있도록 기능구조를 설계하였다. 이 기능 구조에서는 상위에서의 요구사항에 따라 L2 스위치에서의 접속 제어를 지원하며, 사용자들의 멀티캐스트 서비스 이용 실태를 기록하여 파악할 수 있도록 하였다. L2 스위치에서의 접속제어를 지원함으로써, 채널에 대한 권한이 없는 사용자가 멀티캐스트 스트림을 내려 받는 것을 차단할 수 있다. 또한 악의적인 사용자가 액세스망에 내려와 있는 멀티캐스트 스트림을 끌어옴으로써 망의 성능을 저하시키는 DQoS 공격을 무력화할 수 있다. 사용자의 멀티캐스트 서비스 이용 실태를 transport stratum으로부터 보고받아 기록함으로써 이를 정산에 사용할 수 있다. 이 데이터를 개인이 양방향 부가 서비스, 즉 상품에 대한 정보 수집 및 구매 이력 등과 연결하면 개인별 맞춤형 광고도 가능하다. 또한 사용자가 특정 콘텐츠를 얼마만큼의 시간 동안 이용했는지 알 수 있으므로 이는 시청률에 대한 전수조사 데이터의 의미를 가진다. 이 데이터는 미디어에 대한 시청자의 반응에 대한 연구를 함에 있어서 마치 청진에 의존하던 진료체계에 X-ray가 도입된 것과 같은 영향을 줄 것으로 예상된다. 이러한 연구는 새로운 비즈니스 모델이 출현할 수 있는 바탕을 제공할 것으로 기대된다.

현 기능구조에서는 아직 액세스 네트워크 부분에서 위조된 소스 패킷을 이용한 공격 및 IGMP JOIN 패킷을 이용한 DDoS 공격에 대한 대책과, 코어 네트워크에서 multicast MPLS에 대한 OAM 및 protection switching 지원 구조에 대한 추가적인 연구가 필요하다.

약 어 정 리

AAA	Authentication, Authorization, Account
BcN	Broadband convergence Network
DDoS	Distributed Denial of Service
DQoS	Denial of Quality of Service
FE	Functional Entity
GARP	Generic Attribute Registration Protocol
GCI	Gate Control Information
GMM FE	Group Membership Management FE
GMR FE	Group Membership Registration FE
GMRP	GARP Multicast Registration Protocol
GOP	Group of Pictures
IGMP	Internet Group Management Protocol
IPTV	Internet Protocol TV
M-VSPM FE	Multicast Virtual Switched Path Management FE
MAC	Media Access Control
MOS	Mean Opinion Score
NCP	Network Control Platform
PD FE	Policy Decision FE

RACF	Resource and Admission Control Functional entity
RC FE	Resource Control FE
RPF	Reverse Path Forwarding
SCF	Service Control Function
SP	Service Profile
STB	Set-Top Box
TP	Transport Profile

참 고 문 헌

[1] C. Kenneth Miller, "Multicast Networking and Applicastions," Addison Wesley, 1999.

[2] Wes Simpson, "Video over IP," Focal Press, 2006.

[3] 명령을 내렸을 때 반응 시간이 1초가 넘으면 사용자는 기기가 명령을 수행하고 있다는 느낌을 잃기 시작한다. http://www.useit.com/papers/responsetime.html 참조

[4] Robert E. Kooij, Kamal Ahmed, and Kjell Brunnstrom, "Perceived Quality of Channel Zapping," ITU-T Study Group 12, COM12-C24-E, Feb. 2006.

[5] "Managing Delay in IP Video Networks Version 1.0," Cisco, white paper, 2005.

[6] B. Cain, S. Deering, I. Kouvelas, B. Fenner, and A. Thyagarajah, "Internet Group Management Protocol, Version 3," IETF RFC 3376, Oct. 2002.

[7] M. Christensen, K. Kimball, and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches," IETF RFC 4541, May 2006.

[8] IEEE 802.1DTM-2004, "Media Access Control (MAC) Bridges," *IEEE Computer Society*, 2004.

[9] Dat Ba Nguyen, Bakri Aboukarr, and Gregory Erich Gyetko, "IGMP Expedited LEAVE Triggered by MAC Address," US Patent US2004/0117503, 2004.

[10] Thomas Hardjono and Lakshminath R. Dondeti, "Multicast Group Security," Artech House, 2003.

[11] "AT&T Still has IPTV 'Jitters'," http://www.light-reading.com/document.asp?doc_id=101056, Aug. 11, 2006.

[12] R. Aggrawal, D. Papadimitriou, and S. Yasukawa, "Extentions to RSVP-TE for Point-to-Multipoint TE LSPs," IETF draft, draft-ietf-mpls-rsvp-te-p2mp-06.txt, July 2006.

[13] NCP는 네트워크의 자원 현황을 모니터링하고 관리하는 제어 플랫폼. ITU-T NGN-GSI에서 정의하는 RACF의 superset, ITU-T, Draft Recommendation Y.2012, 2006.

[14] Jong Tae Song, Soon Seok Lee, and Young Sun Kim, "DiffProbe: One Way Delay Measurement for Asynchronous Network and Control Mechanism in BcN Architecture," ICACT 2006, Feb. 2006, p.677.