[6-12] 안전하고 신뢰성 있는 미디어 분배를 위한 멀티캐스트 스트리밍 모델

이승주*, 김종원
광주과학기술원 정보통신공학과 네트워크 미디어 연구실
E-mail: {sjlee, jongwon}@netmedia.gist.ac.kr

Design of Multicast Streaming Model for Secure and Reliable Media Distribution

SeungJoo Lee*, JongWon Kim
Networked Media Lab, Dept. of Information & Communications
GwangJu Institute of Science and Technology (GIST)

요 약

고품질의 멀티캐스트 미디어 스트리밍 서비스를 제공하기 위해서는 패킷의 신뢰성 있는 전송을 보장해야 한다. 또한 전송도중 패킷 내용의 변경 여부나 전송된 패킷의 송신자를 인증할 수 있는 방법을 제공하여 안정성을 확보하는 것이 필요하다. 그러나 멀티캐스트 환경에서 손실된 패킷을 복구하고 각 패킷에 대해서 송신자를 인증하려면 많은 어려움이 있다. 더욱이 스트리밍 환경은 실시간의 특성상 빠르고 효율적인 방법을 요구하지만 기존에 제안된 대부분의 방법들은 이와같은 환경에 적합하지 않다. 본 논문에서는 과거에 제안되었던 방안들과 그 특징을 소개하고 신뢰성 있는 전송을 위해 멀티캐스트 상에서 파일 전송의 용도로 사용되는 FLUTE (File Delivery Unidirectional Transport)와 멀티캐스트 스트리밍 상에서 송신자 인증의 목적으로 사용되는 TESLA (Timed Efficient Stream Loss-tolerant Authentication Protocol)를 이용한 새로운 모델을 제안한다. 제안된 모델은 멀티캐스트 환경에서 전송의 신뢰성을 높이고 실시간에 패킷의 송신자 및 메시지 인증을 가능하게 하여 고품질 스트리밍 서비스를 제공하기위한 효과적인 대안으로 판단된다.

1. 서 론

네트워크의 고속화와 더불어 인프라가 확충되면서 인터넷 영화관, 고화질 VOD 서비스등 대용량 멀티미디어 스트리밍 기술이 널리 이용되고 있다. 그러나 현재 사용되고 있는 유니캐스트 방식으로는 수많은 사용자들을 수용하기에는 한계가 있다. 이에 대한 대안으로 멀티캐스트가 주목을 받고 있다. 멀티캐스트는 대역폭을 효율적으로 사용함으로써 문제를 해결한다. 그러나 멀티캐스트는 유니캐스트와 달리 네트워크 환경이 서로 다른 여러 수신자들이 있기 때문에 송신의 신뢰성을 제공하기가 어렵다. 또한 공격자가 멀티캐스트로 전송되는 패킷을 위조할 경우 파급효과가 크고 알아내기도 힘들므로 수신자가 멀티캐스트로 전송되는 모든 패킷에 대해서 무결성(메시지 인증)과 송신자 인증을 할 수 있도록 제공해야만 한다. 그러나 여러 사람이 동일하게 공유하는 세션키(통신을 위해 임시적으로 공유하는 키)만으로는 송신자를 인증할 수 없다. 게다가 실시간이라는 특성은 더 많은 제약을 가지게 된다[2]. 기본적으로 해결해야 할 문제들을 보면 다음과 같다. 첫째, 전송의 신뢰성을 높여야 한다. 멀티캐스트 방식은 일반적으로 UDP(User Datagram Protocol)를 사용하기 때문에 송신자가 수신자에게 신뢰성 있는 전달을 보장할 수 없다. 따라서 피드백이나 FEC (Forward Error Correction)와 같이 손실이 일어난 패킷을 복구할 수 있는 방법이 필요하다. 둘째는 전송되는 패킷의 무결성과 송신자 인증을 제공해야 한다. 멀티캐스트 상에서 그룹키와 같이 대칭키를 이용해서는 송신자를 인증할 수 없다. 게다가 스트리밍되는 모든 패킷에 대해서 송신자 인증을 하기위해서는 빠르고 효율적인 알고리즘이 필요하다.

멀티캐스트 상에서 신뢰성 있는 전송을 위해서 생각할 수 있는 기술로는 직관적으로 피드백이나 FEC를 이용한 방법이 있다. 보다 진보한 기술로는 수신자 측에서 자체 복구나 계층적인 구조를 이용하는 방법이 있다. 그러나 피드백은 멀티캐스트 기반에서는 트래픽의 집중과 같은 어려움이 있고 더욱이 실시간 스트리밍에는 부적합하다. 이러한 이유로 보통 FEC가 많이 사용되고 있다. FEC는 패킷 손실이 아주 적을때(일반적으로 1%의 손실율 이하일때)는 매우 효과적이다. 그러나 적은 손실이라도 연속적으로 일어나는 경우 효과적이지 못하다. 그러므로 네트워크 상황이 좋지 않을 경우 적절한 해결책이 되지 못한다[6]. 멀티캐스트는 수신자들 사이에 서로 수신시간이 다르다는 특징이 있다. 어떤 수신자는 다른 수신자들에 비해서 빠르게 받을 수 있고 반대로 어떤 수신자는 느릴 수 있다. 그러므로 지연시간을 어느 특정 수신자에 맞추기는 불가능하다. 많은 수신자를 수용하기 위해서는 지연시간을 적당히 길게 잡을 필요가 있다. 이러한 경우 지연시간이 짧은 수신자는 어느 정도 여유 시간이 생긴다. 이러한 면에서 Digital Fountain[6]과 FLUTE[5]에서 접근하는 방식인 반복전송 방법은 유용하게 사용될 수 있다. 즉, 지연시간이 짧은 클라이언트에 대해서는 여러번 전송을 하여 수신율을 높일 수 있다. FLUTE는 원래 멀티캐스트 기반에서 파일을 전송하기 위해 고안되었으므로 실시간성은 떨어지지만 완벽한 수신율을 보장한다. 하지만 수신율을 어느 정도 보장하는 선에서 실시간성의 부여가 가능하다.

인증을 위해서 직관적으로 생각되는 방법으로는 디지털 서명이 있다. 그러나 디지털 서명은 부하가 크기 때문에 실시간으로 전송되는 모든 패킷에 대해서 처리하기에는 어려움이 있다. 이것에 대한 대안으로 모든 패킷이 아닌 패킷을 블록단위로 묶어서 인증하는 방법이 제안되었다[7]. 그러나 이 방법은 블록에서 인증에 필요한 한 패킷만 손실되어도 해당 블록을 모두 버려야 한다는 단점이 있다. 이러한 면에서 TESLA[5]는 좋은 방법을 제공해 준다. 이 기술은 계산상의 부하를 줄여서 스트리밍되는 모든 패킷에 대하여 송신자 인증이 가능하도록 하고 메시지의 무결성을 보장해 준다.

그러므로 본 논문에서는 FEC와 반복 알고리즘을 적용하여 전송의 신뢰성을 높이고, 매 패킷에 대해서 실시간으로 송신자 인증 및 무결성을 보장할 수 있는 멀티캐스