DOI: 10.3745/KIPSTC.2009.16-C.1.21

해쉬 트리 기반의 효율적인 IPTV 소스 인증 프로토콜

신 기 은[†] · 최 형 기[††]

요 약

최근 소비자들의 다양한 요구로 인하여 IPTV에 대한 수요가 폭발적으로 증가하고 있다. IPTV는 트리플 플레이(음성, 인터넷, 비디오)를 소비자에게 전달하며, IP 컨버전스 네트워크의 킬러 어플리케이션으로 주목 받고 있다. IPTV는 서비스 공급자의 이익을 위하여 수신자 접근 제어 수단으로 CAS를 이용한다. 현재 CAS는 수신자 인증을 통하여 접근 제어를 제공하지만, 서비스 공급자로부터 전달되는 컨텐츠에 대해서는 어떠한 인증도 제공하지 않는다. 그러므로, 공격자가 서비스 공급자로부터 전달되는 컨텐츠를 조작하여 해로운 정보를 수신자에게 전달할 수 있는 보안 취약점이 존재한다. 본 논문은 해쉬 트리 스킴에 기반하여 현재 IPTV 시스템의 취약점을 제거하는 효율적이고 강력한 소스 인증 프로토콜을 제안한다. 또한, IPTV의 요구사항 관점에서 제안한 프로토콜을 평가한다.

키워드 : 수신자 제어 시스템, IPTV, 소스 인증

Efficient Source Authentication Protocol for IPTV Based on Hash Tree Scheme

Ki-Eun Shin[†] · Hyoung-Kee Choi[††]

ABSTRACT

Presently, the demand for IPTV, to satisfy a variety of goals, is exploding. IPTV is coming into the spotlight as a killer application in upcoming IP convergence networks such as triple play which is the delivery of voice, internet, and video service to a subscriber. IPTV utilizes CAS, which controls the subscriber access to content for a profit. Although the current CAS scheme provides access control via subscriber authentication, there is no authentication scheme for the content transmitted from service providers. Thus, there is a vulnerability of security, through which an adversary can forge content between the service provider and subscribers and distribute malicious content to subscribers. In this paper, based on a hash tree scheme, we proposed efficient and strong source authentication protocols which remove the vulnerability of the current IPTV system. We also evaluate our protocol from a view of IPTV requirements.

Keywords : Conditional Access System, IPTV, Source Authentication

1. 서 론

현재 엔터테이먼트는 전 세계적으로 큰 비즈니스이다. 매년 케이블 TV 수익과 가입자의 수가 급격하게 증가하고 있으며, VDSL, FTTH와 같은 광대역 IP 인프라의 전파로 인하여 하이 퀄리티의 다양한 서비스를 제공할 수 있는 상황이 되었다. 2007년 9월을 기준으로 국내 IPTV 가입자 수는 65만명을 초과하였으며 현재 빠른 증가세를 보이고 있다. [1]

IPTV는 음성, 인터넷, 비디오 서비스를 가입자에게 전달하는 소위 트리플 플레이(Triple play)라고 불리는 다양한 서비스를 제공한다. 또한 IPTV는 기존 TV의 단방향 서비스의 단점을 극복하여 양방향 서비스를 제공하며, 실시간 방송 서비스의 요구사항인 QoS(Quality of Service) 와 QoE(Quality of Experience)를 만족하면서 IP 네트워크망을 통하여 SD와 HD급의 컨텐츠를 제공한다. 수신자의 다양한 요구사항을 만족시키기 위하여 IPTV 서비스 공급자는 다양하고 세분화된 컨텐츠를 전달하며, 자신들의 수익을 위하여 유료 컨텐츠 또한 제공한다. 서비스 공급자는 CAS(Conditional Access System)를 사용하여 수신자의 컨텐츠 접근을 제어한다. [2][3] 즉, 권한을 부여 받은 수신자는 수신자 인증을 통하여 컨텐츠에 접근할 수 있다. 예를 들면, 어떤 컨텐츠에 대하여 요금을 지불한 수신자만이 해당 컨텐츠에 접근하여 이용할 수 있다.

CAS는 스크램블링 알고리즘을 이용하여 컨텐츠를 보호한다. 스크램블링 알고리즘은 권한이 있는 수신자 그룹이 정상적인 프로세스를 통하여 얻을 수 있는 CW(Control Word)라고 불리는 암호화 키를 시드(Seed)로 사용한다. 따라서, 권한이 있는 그룹의 멤버는 CW를 얻을 수 있기 때문에 내부 공격자가 될 수 있으며, 조작된 컨텐츠를 다른 정

† 준 회 원 : 성균관대학교 휴대폰학과 석사과정
†† 정 회 원 : 성균관대학교 정보통신공학부 조교수(교신저자)

논문접수 : 2008년 8월 14일
수 정 일 : 1차 2008년 9월 26일
심사완료 : 2008년 10월 6일

상적인 수신자에게 전송할 수 있다. 그러므로, 현재 IPTV 시스템은 위와 같은 보안 취약점이 존재하며, 공격자는 서비스 공급자에 의해서 전송되는 컨텐츠를 악의적으로 변경하여 정상적인 컨텐츠 사이에 끼워 넣을 수 있다. 예를 들면, 공격자는 자신의 이익을 위하여 주식 정보를 의도적으로 조작할 수 있으며, 이는 사회적으로 큰 문제를 야기시킬 수 있다. 본 논문에서는, 해쉬 트리 스킴에 기반하여 서비스 공급자가 전송하는 라이브 스트리밍 또는 VoD와 같은 데이터 스트림에 대한 소스 인증 프로토콜을 제안한다. 제안된 프로토콜은 짧은 인증 지연시간을 제공하며 패킷 손실과 DoS 공격에 강하다. 또한, 추후에 분쟁이 발생하였을 경우 부인방지 서비스를 바탕으로 법적 근거를 제시할 수 있다. 본 논문의 나머지 부분은 다음과 같이 구성되어 있다. 2장에서는 소스 인증에 관한 기존 연구와 IPTV 시스템을 위한 소스 인증 요구사항을 알아보고, 3장에서는 제안한 프로토콜을 위한 CAS의 구조와 중요한 시그널링 메시지에 대하여 자세히 알아본다. 4장에서는 Merkle Tree(MT)와 [4] 제안한 프로토콜을 자세히 설명한다. 5장에서는 보안 측면과 IPTV 시스템 요구사항 측면에서 성능을 분석하며 측정한다. 마지막으로, 6장에서 본 논문의 결론을 내린다.

2. 관련 연구

멀티캐스팅은 제한된 네트워크 자원 상황하에서 유니케스팅보다 실시간 비디오나 주식 정보와 같은 데이터를 수신자 그룹에게 전달하는데 효율적인 방법이다. 소스 인증은 수신자가 수신한 메시지 중 변조된 패킷을 필터링할 수 있다. 멀티캐스팅에서의 소스 인증은 현재까지 중요한 연구 주제였지만, 멀티미디어 스트리밍을 위한 소스 인증은 전송과 연산 오버헤드로 인하여 효과적인 해결책을 찾기 힘들었다.

현재까지 멀티캐스팅 소스 인증을 위한 많은 연구가 진행되었다. 서명 분산을 통하여 패킷 손실에도 강력한 소스 인증을 제공하는 프로토콜인 SAIDA [5]와 데이터 스트림 중 적은 수의 패킷을 서명함으로써 소스 인증을 제공하는 EMSS [6] 등이 제안되었다. 또한, 대칭키의 해쉬 체인과 대칭키의 공개를 통하여 빠르고 가벼운 연산의 검증을 제공하는 소스 인증 프로토콜인 TESLA [7]도 제안되었다. 하지만, 이러한 프로토콜은 IPTV에 적용하기 적합하지 않다. SAIDA는 수신자 측면에서 분산된 서명을 재생성하기 위해서는 전송되는 패킷의 버퍼링, 높은 연산 오버헤드, 그리고 긴 프로세스 지연이 필요하다. 또한 EMSS는 비교적 긴 서명 검증 지연 시간 때문에 IPTV의 중요한 요구사항인 실시간 서비스 제공에 부적합하다. TESLA는 전자서명을 이용하지 않기 때문에 부인방지 서비스를 제공할 수 없으며, 송신자와 수신자 사이에 시간 동기화가 필요하다. 더불어, 해쉬 충돌로 인하여 해쉬 체인의 길이가 한정되기 때문에 무한한 길이의 실시간 방송과 같은 서비스에 적합하지 않다.

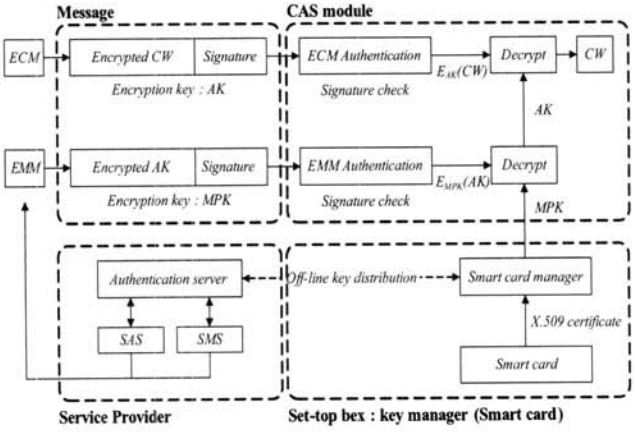
IPTV는 라이브 스트리밍과 주식 정보와 같은 실시간 서비스를 제공해야만 한다. 하지만 SAIDA와 EMSS는 수신자가 TV를 보기 위하여 기다려야만 하는 프로세싱(인증) 지연으로 인하여 실시간 서비스를 제공할 수 없으며, 정상적인 스트림 사이에 악의적으로 삽입된 변조된 패킷으로 인하여 전체 스트림 인증에 실패할 수 있다. 또한 TESLA는 이후에 서비스 공급자와 수신자 사이에 분쟁이 발생하였을 경우, 서비스 공급자가 전달한 패킷에 대한 증거를 제공하는 소스 인증의 중요한 기능 중의 하나인 부인 방지 서비스를 제공하지 못한다.

3. CAS, IPTV 요구 사항

IPTV는 DRM과 CAS와 같은 보안 요소를 갖고 있다. DRM은 컨텐츠 공급자의 이익을 보호하기 위하여 디지털 미디어의 사용 제한하는 기술이다. 반면에, CAS는 서비스 공급자의 이익을 보호하기 위하여 권한에 따라 수신자의 디지털 미디어 접근을 제안하는 시스템이다. CAS는 서비스를 이용할 수 있는 권한을 수신자에 부여함으로써 서비스 공급자의 이익을 보호하며, 서비스 공급자는 수신자의 서비스 구매에 따라 권한을 제어한다. 현재까지 CAS 표준이 없었기 때문에, 각 서비스 공급자들은 자신만의 CAS를 개발해 왔다. 하지만, 각 서비스 공급자의 CAS는 프레임워크와 기본 개념은 거의 유사하다.

CAS의 보안 요소는 접근 제어를 위한 스크램블링과 암호화로 이루어진다. CAS는 스크램블링과 디스크램블링을 통하여 데이터 스트림을 보호한다. (그림 1)은 CAS의 구조를 나타낸다.

서비스 공급자는 MPEG-2 TS(Transport Stream) 타입의 데이터 스트림(즉, 비디오나 오디오)을 스크램블링하여 유효한 수신자만이 데이터 스트림을 이용할 수 있게 한다. 권한이 있는 수신자만이 스크램블링된 스트림의 디스크램블링 과정을 통하여 본래의 데이터 스트림을 생성할 수 있다. CAS는 이러한 수신자 접근 제어를 위하여 다음과 같은 계층적인 키를 사용한다: MPK(Master Private Key), AK(Autorization Key), CW(Control Word). CW는 TS의 스크램블링과 디스크램블링에 사용되는 키의 씨드로서 임의의 숫자이다. CW는 불법적인 시청을 막기 위하여 일종의 그룹키인 AK를 이용하여 암호화되며 브로드케스트를 통하여 자주 업데이트 된다. AK로 암호화된 CW는 ECM(Entitlement Control Message)



(그림 1) 접근 제어 시스템

와 함께 전송된다. AK는 MPK로 암호화되며, 유니케스트를 통하여 EMM(Entitlement Management Message)과 함께 수신자에게 전송된다. EMM은 각 수신자의 계약 정보를 포함하고 있으며 ECM과 비교하여 상대적으로 긴 주기로 전송이 된다. 서비스 공급자는 각 수신자의 셋톱박스 내 스마트 카드에 오프라인을 통하여 MPK를 저장한다. 예를 들어, MPK는 셋톱박스가 출하될 때나, 수신자가 IPTV 서비스에 가입하여 셋톱박스를 설치할 때에 스마트 카드 내에 저장된다.

CAS는 수신자의 접근을 제어하기 위하여, ECM과 EMM과 같은 제어 메시지가 전송이 된다. 수신자에게 권한 정보를 전달하며, 키 업데이트 스케쥴에 따라 CW를 업데이트 하기 위하여 ECM은 TS 스트림 사이에 삽입된다. 수신자는 각각 ECM과 EMM에 포함되어 전송된 CW와 AK를 획득하며, 이를 통하여 스크램블링된 컨텐츠를 디스크램블링할 수 있다.

일반적으로, ECM과 EMM은 수신자에게 서비스 이용 권한을 부여하는 중요한 시그널링 메시지이다. 따라서, 서비스 공급자는 메시지에 대하여 무결성과 신뢰성을 제공하기 위하여 전자 서명 방식을 이용하여 이 메시지에 서명을 한다. 수신자는 서명 검증 과정을 통하여 이 메시지의 유효성을 체크할 수 있으며 지불한 컨텐츠에 대하여 수신할 수 있는 권리를 부여 받는다.

하지만, 수신자에게 전송되는 스트림에 대한 소스 인증은 제공하지 않는다. 본질적으로 그룹 키를 이용한 그룹 통신에서 발생하는 메시지의 소스를 확인할 수 없는 문제가 IPTV 시스템에서도 발생하게 된다. 따라서 권한이 있는 수신자(AK를 합법적으로 얻는 수신자)는 스트림을 스크램블링하는데 쓰이는 CW를 얻을 수 있으며, CW를 이용하여 불법적인 스트림을 재스크램블링하여 다른 수신자에게 전송할 수 있다. 스트림에 대한 소스 인증을 제공하지 않기 때문에 수신자는 전송 받은 데이터의 출처를 확인할 수 없다. 현재 IPTV 시스템은 위와 같은 보안 취약점을 내포하고 있기 때문에, 이러한 공격을 막기 위하여 IPTV 시스템은 서비스 공급자에 의해서 전송되는 스트림에 대하여 소스 인증 서비스를 제공해야만 한다.

또한, 컨텐츠를 제공할 권한이 있는 정당한 서비스 공급자도 불법적인 이익을 위하여 변조된 컨텐츠를 전송할 수 있다. 예를 들면, 서비스 공급자는 잘못된 주식 정보를 브로드케스팅할 수 있다. 따라서, IPTV 소스 인증 프로토콜은 서비스 공급자가 전송한 컨텐츠에 대하여 이후에 전송을 부인 하는 것을 방지할 수 있는 부인방지 서비스를 제공해야만 한다.

IPTV 요구사항을 만족시키기 위하여 2장에서 언급하였던 소스 인증 프로토콜을 대신 할 새로운 소스 인증 프로토콜이 필요하다. IPTV를 위한 소스 인증 프로토콜의 중요한 요소는 다음과 같다.

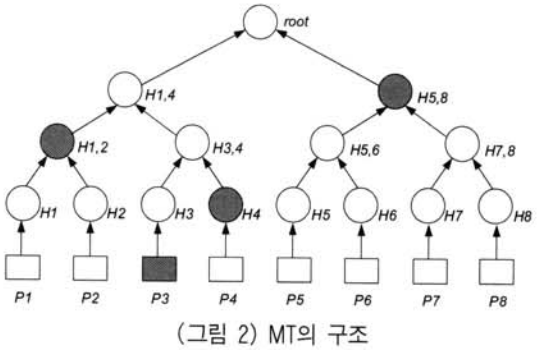
1) 스트림 내의 각 패킷은 전송 받자마자 이용되어야 한다.
2) 패킷 손실이 있더라도, 수신자는 나머지 패킷에 대하여 검증할 수 있어야 한다.
3) 공격자로부터 DoS 공격이 있더라도, 수신자는 정상적인 서비스 이용이 가능해야만 한다.
4) 컨텐츠 전송 부인을 막기 위하여 부인 방지 서비스를 제공해야만 한다.
5) 휴대폰과 같은 이동 단말로의 방송과 같이 유연한 서비스를 제공하기 위하여 전송과 연산 오버헤드를 최소화 해야만 한다.

4. IPTV 소스 인증 프로토콜

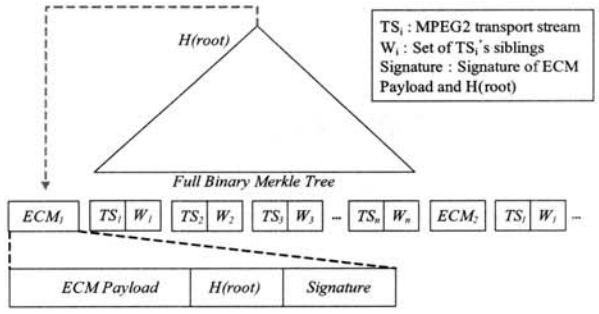
IPTV 소스 인증 프로토콜은 실시간 방송을 위하여 서비스 공급자와 수신자 측면에서 모두 효율적이어야만 한다. 특히, 셋톱박스의 연산 능력은 일반적으로 뛰어나지 않기 때문에 수신자 측에서 서명 인증과정의 효율성은 서비스 공급자 측에서 서명을 생성하는 효율성보다 더욱 중요하다. 서비스 공급자와 수신자는 공격자로부터 공격이 있더라도 안정된 서비스를 제공하기 위하여 DoS 공격에 강력해야만 하며, 추후 분쟁이 발생했을 경우를 대비하여 부인방지 서비스를 제공해야만 한다.

일반적으로 소스 인증을 위해서는 송신자와 수신자가 공유하고 있는 대칭키를 사용하거나, 비대칭 키를 이용한 전자서명 방식을 사용한다. 대칭키 연산은 비대칭키 연산보다 더 빠르다. 하지만 그룹통신에서 소스 인증을 위해서는 한명의 송신자와 나머지 n명의 그룹 멤버 사이에서 n개의 PSK(Pre Shared Key)를 공유해야 하며, 송신자는 n개의 MAC(Message Authentication Codes)을 생성해야만 한다. 이러한 방식으로 브로드캐스팅 메시지를 전송할 경우에는 MAC 연산과 전송 오버헤드가 $O(n)$이므로 효율적이지 못하다. 따라서, 일반적으로 브로드캐스트 메시지에 대한 소스인증을 위하여 전자서명을 이용한다. 전자서명은 메시지 무결성과 소스인증 및 부인방지 서비스를 포함하는 적절한 인증 서비스를 제공할 수 있다. 하지만 전자서명을 통한 인증방법은 서명자와 검증자 모두 많은 연산을 필요로 하기 때문에, 데이터 스트림을 검증하는데 있어서 많은 지연이 발생하며 이는 서비스의 QoS를 떨어뜨린다. 그러므로 IPTV와 같은 실시간 방송의 경우 효율적인 소스 인증 프로토콜이 필요하다. 이를 위하여 최소한의 전자서명을 하여 서명에 대한 검증 횟수를 최소화함으로써 실시간 서비스를 제공할 수 있다.

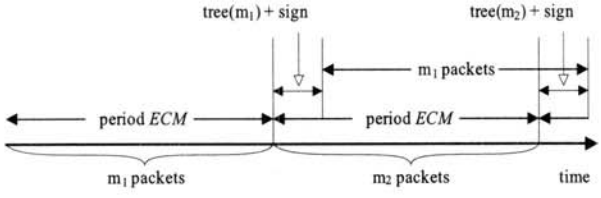
본 논문에서는 3장에서 언급한 요구사항을 만족시키기 위하여 MT(Merkle Tree) [4]를 수정하여 서비스 공급자로부터 공급되는 데이터 스트림에 대한 소스 인증을 제공한다. 일반적으로, MT는 송신자가 전송한 패킷에 대하여 수신자가 패킷 전송자를 확인할 수 있도록 트리를 생성하여, 소스 인증을 제공한다. (그림 2)는 MT의 예이다. 송신자는 8개의 패킷(P)에 대하여 해쉬 함수와 연결(Concatenation)을 이용



(그림 2) MT의 구조



(그림 3) 제안한 프로토콜의 스트림



(그림 4) 제안한 프로토콜의 스트리밍 플로우

하여 이진트리를 생성한다. 다음은 MT를 생성하는 과정이다. 각 패킷의 해쉬 값을 구하고, 이 값들을 트리의 종단 노드로 구성을 한다. 각 종단 노드 쌍을 연결한 후 다시 해쉬 값을 구한다. 이 값은 노드 쌍의 부모 노드가 되고, 이러한 방식을 반복적으로 적용하여 트리의 루트 값을 계산한다. 메시지 송신자는 이 루트 값에 대하여 서명을 하고, 형제 노드 쌍과 루트의 서명을 수신자에게 전달한다. 예를 들면, *P3*에 대한 형제 노드 쌍들은 (그림 2)의 빗금 친 원 $\{H_4, H_{1,2}, H_{5,8}\}$이다. 따라서, *P3*와 해당 형제 노드 쌍들, 그리고 루트에 대한 서명값이 함께 수신자에게 전송된다. 수신자는 다음과 같은 식을 통하여 루트 값을 복원할 수 있다.

$$root = H((H_{1,2}, (H(P3), H_4)), H_{5,8})$$

수신자는 루트 값을 복원하여 서명을 검증함으로써 전송한 패킷의 소스를 확인할 수 있다. 한번 트리에 대한 서명이 검증되면, 해당 트리의 종단 노드를 구성하는 나머지 패킷들은 루트를 재생성하고 기존에 인증 받은 루트와 비교를 통하여 전송 받은 패킷을 인증할 수 있다. 만약 비교 결과 같으면, 해당 패킷은 정당한 송신자로부터 전송된 패킷이며, 같지 않을 경우는 해당 패킷을 버린다.

MT를 통하여 소스 인증을 제공할 경우 각 패킷은 형제 노드 쌍과 함께 전송이 되기 때문에, 패킷 손실이 있더라도 수신자는 루트 값을 복원할 수 있다. 따라서, SAIDA [5]와 같이 패킷을 검증하기 위한 버퍼링이 필요 없으며, 수신자는 패킷을 전송 받자마자 패킷의 신뢰성을 검증할 수 있다. 이러한 MT의 속성은 DoS나 Pollution 공격에 수신자가 잘 견딜 수 있게 해준다. 그러므로 MT는 IPTV와 같은 실시간 방송 서비스 소스 인증에 적합하다. 하지만, 각 패킷과 함께 전송되는 서명 값과 형제 노드 쌍들로 인하여 각 패킷 당 전송 오버헤드가 높다. 따라서, 우리는 전송 오버헤드와 인증 딜레이를 줄이기 위하여 MT를 수정하였다.

3장에서 언급하였듯이, CAS 시그널링 메시지라 불리는 ECM과 EMM은 메시지에 대한 신뢰성과 무결성을 보장하기 위하여 서비스 공급자에 의해서 서명된다. 따라서, 만약 MT의 루트 값과 CAS 시그널링 메시지가 함께 서명된다면, 수신자는 한번의 서명 검증을 통하여 CAS 시그널링 메시지와 루트를 검증할 수 있다. 전송 오버헤드를 줄이기 위하여 각 패킷과 함께 전송되는 루트의 서명 값 또한 보내지 않으며, 대신 CAS 시그널링 메시지는 MT의 루트 값과 MT의 루트 값을 포함하는 메시지의 서명 값을 포함한다. 또한 기존 MT와 마찬가지로 각 데이터 스트림 패킷(TS)는 형제 노드 쌍들을 포함한다. 이러한 과정을 통해서, 서비스 공급자는 기존 CAS와 비교하였을 때 추가적인 서명과정이 필요 없으며, 수신자 측면에서도 마찬가지로 추가적인 서명 검증 과정이 필요 없다. 또한, 각 패킷에 루트에 대한 서명 값이 포함되지 않으므로, MT를 IPTV에 직접 적용한 방법보다 전송 오버헤드를 줄일 수 있다.

ECM의 전송 주기는 EMM의 전송 주기보다 짧으며, ECM은 브로드케스트로 수신자에게 전송이 된다. 따라서, 서비스 공급자가 전송하는 TS에 대하여 인증을 제공하고 전송 오버헤드를 줄이기 위하여, EMM을 이용하는 것보다 ECM을 이용하는 것이 더욱 적합하다. ECM 손실이 있을 수 있으므로, 수신자는 CW를 얻기 위하여 다음 ECM을 기다려야만 한다. 일반적으로, 시청자는 TV를 시청하기 위하여 오랜 시간 동안 기다리는 것에 인색하기 때문에, 현재 국내 IPTV 시스템의 ECM 전송 주기는 약 0.1초이다.

송신자는 TS의 해쉬 값을 MT의 종단 노드로 하여 MT를 생성하며, MT의 루트를 ECM의 페이로드와 함께 서명한다. 이 루트 값은 MT를 구성하는 모든 TS의 대표값으로 볼 수 있다. 즉, MT의 루트를 서명함으로써 각 TS를 서명한 효과를 얻을 수 있다. 서비스 공급자는 각 패킷에 대한 종단 노드로부터 MT의 루트 경로까지의 형제 노드들을 연결하여 형제 노드 쌍을 만들며, 이 형제 노드 쌍을 TS와 함께 전송한다. (그림 3)은 제안한 프로토콜의 스트림을 나타내며, W_i는 TS_i에 대한 형제 노드 쌍이다. ECM과 TS(즉, 기존 TS와 형제 노드 쌍)은 수신자에게 전송된다. 예를 들어, ECM_1과 ECM_2 사이에 8개의 TS 패킷이 존재한다면, W_1은 $\{H_2, H_{3,4}, H_{5,8}\}$이다.

수신자는 ECM내의 서명을 검증함으로써 ECM 페이로드의 신뢰성을 확인할 수 있으며, 이를 통하여 ECM 페이로드 내의 루트 값의 신뢰성 또한 확인할 수 있다. 이 후에 전송되는 TS에 대하여 수신자는 루트 값을 재생성하고 이 값을 신뢰성을 확인한 루트 값과 비교함으로써 TS의 신뢰성과 무결성을 확인할 수 있다. 만약 비교 결과 값이 같지 않을 경우, 수신자는 TS를 버퍼링 없이 바로 버린다.

수신자는 TS를 검증하기 위하여 MT당 한번의 서명 검증과 해쉬 연산이 필요하다. (그림 4)는 제안한 프로토콜의 스트리밍 플로우를 나타낸다. $tree(m_i)$는 m_i 스트림에 대하여 MT를 생성하는데 걸리는 시간을 나타낸다. MT를 생성하고 서명한 후에, 서비스 공급자는 스트림을 수신자에게 전달하기 시작한다.

〈표 1〉 송신자 측에서의 연산 회수와 지연 시간

Stream	Hash (188Bytes)	Hash (32Bytes)	Concatenation	Delay (ms)
5Mbps	256	255	255	0.55
10Mbps	512	511	511	1.1121
20Mbps	1024	1023	1023	2.2217

〈표 2〉 수신자 측에서의 연산 회수와 지연 시간

Stream	Hash (188Bytes)	Hash (32Bytes)	Concatenation	Delay (μs)
5Mbps	1	8	8	5.696
10Mbps	1	9	9	6.548
20Mbps	1	10	10	6.599

5. 보안 및 성능 분석

5.1 인증 지연시간(Authentication latency)

일반적으로, 수신자 측에서 서명 검증 회수를 줄이기 위한 블록 기반의 소스 인증 방식은 검증 프로세스 전에 모든 패킷을 받아야 하기 때문에, 인증 지연시간은 길다. 또한 SAIDA [5]와 같은 (m, n) 코딩 프로토콜은 패킷의 소스를 인증하기 위해서 n개 이상의 패킷을 수집해야만 한다.

하지만, 본 논문에서 제안한 프로토콜은 매우 가볍고 빠른 해쉬 연산을 통해 생성된 루트를 서비스 공급자에 의해서 서명된 ECM 내의 루트와 비교하기 때문에 인증 지연시간이 짧다. 현재 CAS의 기본적인 ECM을 서명하는 프로세스를 이용하기 때문에, 수신자 측에서 추가적인 서명 검증 과정이 필요하지 않다. 즉, ECM과 MT의 루트를 함께 서명하였기 때문에 서비스 공급자 측에서는 추가적인 서명과정이 필요하지 않으며, 수신자는 루트를 재생성함으로써 스트림을 검증할 수 있다. 따라서, 수신자는 효율적인 해쉬 연산만을 이용하여 멀티미디어 스트림을 검증할 수 있다.

우리는 IPTV 소스 인증을 현 IPTV 시스템에 적용하였을 경우 서비스 공급자와 수신자 측면에서 발생하는 추가적인 지연을 측정하기 위하여 시뮬레이션을 수행했다. 시뮬레이션 프로그램은 C언어로 구현되었으며, 1.6 GHz 펜티엄 듀얼코어 리눅스 PC에서 구동되었으며, 암호화 라이브러리로는 XySSL 0.9 [9]가 사용되었다. MD5-128이 해쉬 함수로 이용되었으며, 전자서명 방식으로 1024비트의 키를 이용한 RSA를 사용하였다. <표 1>은 비트레이트에 따른 신뢰성 있는 패킷을 생성(즉, MT 생성)하기 위하여 필요한 연산 회수와 지연시간이며, <표 2>는 비트레이트에 따른 수신자 측에서 MT를 재생성하는데 필요한 연산 회수와 지연시간이다. 제안한 프로토콜은 시뮬레이션 결과에서 확인할 수 있듯이, 수신자 측의 지연시간보다 송신자 측의 지연시간이 더욱 길다. 하지만, 실제 CAS 서버의 연산 능력은 셋톱박스의 연산 능력보다 뛰어나기 때문에 송신자 측의 지연시간은 단축될 수 있다.

ITU-T에서 제안한 Y.1540과 Y.1541 [10]은 IPTD (IP Packet Transfer Delay), IPDV (IP Packet Delay Variation), IPLR (IP Packet Loss Ratio), IPER (IP Packet Error Ratio)과 같은 QoS 요소와 5가지의 QoS 클래스를 제공한다. Y.1541에 따르면 IPTV 서비스는 클래스 4에 속한다. 본 논문에서 제안한 프로토콜은 단지 IPTD에만 영향을 미치기 때문에, 우리는 ITU-T의 표준과 비교하여 프로토콜의 적합성을 확인했다. 클래스 4의 IPTD는 1초이며, 제안한 프로토콜의 소스 인증을 처리하기 위한 추가적인 지연시간은 IPTD의 값과 비교하여 미미하기 때문에 IPTV의 QoS는 추가적인 인증 지연시간에 영향을 받지 않는다.

5.2 패킷 손실에 강함(Resilience to packet loss)

블록기반의 소스 인증이나 해쉬 체인 기반의 소스 인증은 각 패킷간의 상관관계를 갖는다. 그러므로, 패킷 손실이 있을 경우, 블록을 구성하는 나머지 패킷이나 해쉬 체인이 영향을 받는다. 그러나, 본 논문에서 제안한 프로토콜은 패킷간의 상관관계를 제거하였으며, 패킷과 형제 노드 쌍들을 함께 보냄으로써 패킷 손실에도 불구하고 ECM 내의 신뢰성 있는 루트 값과 비교함으로써 나머지 패킷을 신뢰성을 검증할 수 있다. 제안한 프로토콜의 이러한 속성에도 불구하고 만약 ECM이 손실되었을 경우, 해당 트리를 구성하는 패킷을 검증할 수 없다. 현 CAS에서 ECM이 손실되었을 경우, 수신자는 CW를 획득할 수 없으므로 멀티미디어 스트림을 디스크램블링할 수 없다. 따라서, 본 논문에서는 ECM 손실에 관하여 고려하지 않는다.

5.3 DoS 공격에 강함(DoS resilience)

현 IPTV 시스템에서 공격자는 변조된 스트림(또는 임의적으로 생성된 스트림)을 수신자에게 전송할 수 있으며, 이로 인하여 수신자는 서비스 공급자에게 전송받은 스트림 검증에 방해를 받을 수 있으며, 추가적인 연산 오버헤드를 겪을 수 있다.

해쉬 체인을 이용한 소스 인증 프로토콜의 경우는 공격자가 블록 서명 없이 변조된 패킷을 정상 패킷 사이에 섞을 수 있으며, 수신자는 블록 서명을 받을 때까지 전송 받은 패킷의 버퍼링이 필요하기 때문에 오버플로우가 발생할 수 있다.

제안한 프로토콜은 MT를 이용하여 전송 받은 패킷의 신뢰성을 검증하며, 공격자가 의도적으로 변조하여 전송한 패킷에 대하여 ECM내의 신뢰성 있는 루트 값과 비교함으로써 필터링할 수 있다.

5.4 부인 방지(Non-repudiation)

서비스 공급자는 전자서명을 통하여 패킷에 서명을 하기 때문에 수신자에게 전송한 패킷에 대하여 송신에 대한 부인을 할 수 없다. 따라서, 서비스 공급자와 수신자 사이에 분쟁이 발생할 경우, 부인 방지 서비스는 전송한 패킷에 대하여 법적인 근거를 제시할 수 있다.

5.5 연산 오버헤드(Computation overhead)

연산 오버헤드는 송신자 측(서비스 공급자)과 수신자 측의 두 측면으로 나눌 수 있다. 송신자는 MT를 생성하기 위하여 $O(nlogn)$ 해쉬 연산이 필요하며, 루트 값 서명에 대한 추가적인 프로세스는 필요하지 않다. 현재 CAS 시스템은 ECM을 서명하며 제안한 프로토콜은 ECM과 MT의 루

〈표 3〉 같은 해쉬 값을 갖는 입력값 찾는데 걸리는 시간 및 연산 회수

Operation	Hash output (8bit)	Hash output (16bit)	Hash output (32bit)
Number of Operation	256	65536	4294967296
Time (s)	0.00067	0.17391	3.16595

트를 함께 서명하기 때문이다. 일반적으로, 서비스 공급자의 서버는 데이터 스트림을 멀티플랙스하고 스크램블링하기 위하여 연산 능력이 뛰어난 장치이다. 그러므로 본 논문에서 우리의 초점은 수신자 측면에서 연산 오버헤드와 인증 지연 딜레이를 줄이는데 있다. 반면에, 수신자는 MT의 루트 값을 포함하는 ECM의 서명을 검증한 이 후에 신뢰성 있는 루트 값과 $O(logn)$의 해쉬 연산을 통하여 재생성된 루트 값을 비교함으로써 전송받은 패킷의 소스를 확인할 수 있다.

5.6 전송 오버헤드(Communication overhead)

제안한 프로토콜에서 TS와 함께 전송되는 형제 노드 쌍의 수는 $O(logn)$이다. n 값은 ECM의 전송 주기와 멀티미디어 스트림의 비트 레이트에 따라 결정된다. 제안한 프로토콜의 전송 오버헤드를 줄이기 위하여 해쉬 값의 일부분만을 사용하는 것이 가능하다. 해쉬의 암호학적인 강도는 해쉬 값의 크기에 따르기 때문에, 해쉬 값의 크기를 줄이는 것은 브루트포스(brute force)공격에 취약할 수 있다. 따라서, 서비스 공급자는 상황에 맞게 해쉬 값의 크기를 결정해야 한다.

공격자는 TS가 수신자에게 전송되기 이전에 TS를 받아 TS의 해쉬 값과 동일한 해쉬 값을 갖는 TS를 찾은 후, 정상적인 TS가 아닌 신뢰성 없는 TS를 수신자에게 전송할 수 있다. 이러한 공격을 막기 위하여, 서비스 공급자는 IPTV 서비스 내의 최대 RTT(Round-Trip Time) 값의 1/2 이내에 공격자가 동일한 해쉬 값을 찾는 것을 불가능하게 해야 한다. <표 3>은 해쉬 값의 크기에 따라 같은 해쉬 결과 값을 갖는 입력값을 찾는데 걸리는 평균시간이다. 해쉬 값의 크기와 보안 강도는 트레이드오프 관계이므로 데이터 스트림의 중요성에 따라 적절히 해쉬 값의 크기를 선택해야만 한다.

6. 결 론

본 논문에서는 IPTV 시스템을 위한 소스 인증 프로토콜을 제안하였다. 우리가 조사한 결과, 현재까지 IPTV의 스트림에 대한 소스 인증 프로토콜을 없었다. IPTV를 위해 제안된 대부분의 프로토콜은 수신자가 아닌 서비스 공급자와 컨텐츠 공급자의 이익을 위한 것이었다. 제안한 프로토콜은 전송받은 스트림에 대하여 수신자가 신뢰성 있는 컨텐츠를 즐길 수 있는 권리를 제공하며, 서비스 공급자와 수신자 사이에 분쟁이 있을 경우 법적인 근거를 제공한다. 제안한 프로토콜은 서비스 공급자와 수신자 측 모두에 효율적이며, 특히 수신자 측에서 추가적인 서명검증이 필요 없기 때문에 실시간 서비스의 QoS를 만족시키며 DoS 공격을 예방할 수 있다.

이러한 장점에도 불구하고 제안한 프로토콜은 단점을 갖는다. 5장에서 언급하였듯이, 제안한 프로토콜의 전송 오버헤드는 TS와 함께 전송되는 형제 노드 쌍으로 인하여 경미하게 높다. 해쉬 값의 크기와 보안 강도는 트레이드오프 관계 이므로, 서비스 공급자는 상황과 컨텐츠의 중요도에 따라서 적합한 해쉬 값의 크기를 선택함으로써, 전송 오버헤드를 조절할 수 있다. 이러한 트레이드오프에 관한 연구는 향후 과제로 남겨둘 것이다.

참 고 문 헌

[1] Won. Young J. et al., "End-user IPTV traffic measurement of residential of broadband access networks," Proc. of IEEE NOMS Workshops, pp.95-100, Apr., 2008.

[2] T. Yoshimura, "Conditional access system for digital broadcasting in Japan," Proc. of IEEE, pp.318-322, Jan., 2006.

[3] B. Lu et al., "A scalable key distribution for conditional access system in digital pay-tv sys-tem," IEEE Trans. On Consumer Electronics, pp.632-637, May, 2004.

[4] R. C. Merkle, "A digital signature based on a conventional encryption function," Advances in Cryptography, CRYPTO'87, 1987, pp.369-378

[5] J. M. Park et al., "Efficient multicast packet authentication using signature amortization," Proc. IEEE Symp. Security and Privacy, pp.227-240, May, 2002.

[6] A. Perrig et al., "Efficient authentication and signing of multicast streams over lossy channels," Proc. IEEE Symp. Security and Privacy, pp.56-73, May, 2000.

[7] A. Perrig et al., "Efficient and secure source authentication for multicast," Net. and Distrib. Sys. Sec. Symp., pp.35-46, Feb. 2001.

[8] ITU-T, "Security architecture for systems providing end-to-end communications," ITU-T Rec. X.805, 2003.

[9] XySSL Project, http://www.xyssl.org

[10] Neal Seitz, "ITU-T QoS Standards for IP-Based Networks," IEEE Communications Maga-zine, pp.82-89, Jun., 2003.

신 기 은

e-mail : keshin@hit.skku.edu

2008년 고려대학교 컴퓨터학과(이학사)

2008년~현 재 성균관대학교 휴대폰학과 석사과정

관심분야 : 프라이버시 보호, 그룹 커뮤니케이션, 인증 프로토콜 등

최 형 기

e-mail : hkchoi@ece.skku.ac.kr

1992년 성균관대학교 전자공학과(공학사)

1996년 Polytechnique University 전기전자(공학석사)

2001년 Georgia Institute of Technology 전기전자(공학박사)

2001년~2004년 미국 Lancope. Inc. 연구원

2004년~2006년 성균관대학교 정보통신공학부 전임강사

2006년~현 재 성균관대학교 정보통신공학부 조교수

관심분야 : 인터넷 보안, 모바일 커뮤니케이션 등