IP-TV 시스템을 위한 소스 인증 프로토콜+

신기은*, 최형기*
*성균관대학교 정보통신공학부
e-mail:keshin@hit.skku.edu, hkchoi@ece.skku.ac.kr

Source Authentication Protocol for IP-TV System

Ki-Eun Shin*, Hyoung-Kee Choi*
*School of Information and Communication Engineering, Sungkyunkwan University

요 약

최근 고객의 다양한 요구를 충족시키는 IP-TV 시스템에 대한 수요가 크게 증가하고 있다. IP-TV는 IP 기반 인프라를 이용하여 다양한 서비스를 제공하며, 가입자의 콘텐츠에 대한 접근을 제어하기 위하여 CAS(Conditional Access System)를 이용한다. 현재의 CAS는 가입자 인증을 통한 콘텐츠 접근 제어를 지원하지만, 서비스 공급자가 제공하는 데이터에 대해서는 어떠한 인증도 제공하지 않는다. 그러므로 공격자는 데이터를 변조할 수 있으며, 이로 인하여 IP-TV 시스템은 심각한 보안 위협에 노출된다. 따라서 본 논문은 서비스 공급자의 데이터 스트림에 대한 소스인증 메커니즘을 제안한다. 소스인증은 해쉬 트리를 적용한 메커니즘을 사용하며, 이를 통해 기존 CAS 시스템에서 발생하는 문제점을 해결할 수 있다.

1. 서론

최근 고객의 다양한 요구를 충족시키기 위하여 다양한 서비스가 제공되고 있다. 특히 방송과 통신의 융합 시스템인 IP-TV에 대한 수요가 크게 증가하고 있다. 통신과 방송의 융합으로 인하여 방송, 음성, 데이터 서비스를 아우르는 서비스를 제공한다.

IP-TV는 단방향 서비스의 기존 방송 서비스 단점을 개선하여 양방향 서비스를 제공하며 광대역 IP망을 기반으로 하여 고화질 / 고음질의 데이터를 전달한다. IP-TV 서비스는 가입자가 원하는 채널과 콘텐츠를 선택하여 이용할 수 있으며, 세분화되고 다양한 장르를 전달한다. 따라서 서비스 공급자는 자신의 수익 모델을 위한 유료 콘텐츠를 제공하며, 이에 대한 가입자의 접근을 제어하기 위하여 CAS(Conditional Access System)[1][2]의 필요성이 요구되었다. 즉 콘텐츠에 대한 정당한 사용료를 지불한 가입자만이 해당 프로그램을 이용할 수 있다.

CAS는 가입자에 대한 인증은 제공하지만, 제공하는 콘텐츠에 대한 소스 인증은 제공하지 않는다. 가입자는 자신이 받은 콘텐츠가 정당한 서비스 공급자로부터 제공받은 것이지 확인할 방법이 없다. 이로 인하여, 서비스 공급자와 가입자 사이에 공격자가 변조된 데이터를 끼워 넣음으로써 정상적인 서비스를 막을 수 있으며, 심각하게는 증권 정보와 같은 중요한 정보를 공격자가 의도한 방향으로 변조시킴으로써 사회적으로 큰 문제를 일으킬 수 있다.

따라서 본 논문에서는 서비스 공급자로부터 제공되는 데이터에 대한 효율적인 소스 인증 제공 방법을 제시하며, 또한 부인 방지를 통하여 향후에 문제가 발생하였을 때, 법적 근거 자료를 제공할 수 있다.

2장에서는 브로드캐스트 소스 인증에 대한 기존 연구에 대하여 알아보고, 3장에서는 기존 CAS의 구조를 알아본다. 4장에서는 본 논문이 제안하는 IP-TV 소스 인증 프로토콜에 대하여 소개를 하고, 제안된 프로토콜의 분석과 본 논문의 결론을 각 각 5장과 6장에서 소개한다.

2. 관련 연구

일반적으로 브로드캐스트 인증은 <표 1>과 같은 서비스가 요구 된다 :

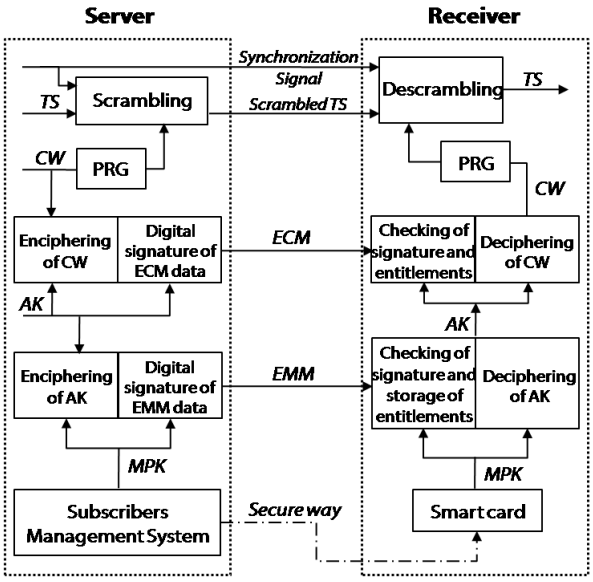
<표 1> 브로드캐스트 인증의 서비스 종류[3]

서비스	설명
데이터 무결성	각 수신자는 수신한 데이터에 대한 변조 유무를 확인할 수 있어야 한다.
데이터 소스 인증	각 수신자는 데이터가 적법한 송신자로부터 전송된 것인지 확인할 수 있어야 한다.
송신 부인 방지	분쟁이 있을 경우, 데이터 송신자는 데이터 보낸 것에 대하여 부인할 수 있어서는 안 된다.

현재까지 브로드캐스트 소스 인증을 위한 다양한 연구들이 진행되었다. 데이터 패킷의 손실이 있음에도 불구하고 소스 인증이 가능한 EMS[4]와, 소스 인증을 좀 더 효

+ "본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2008-C1090-0801-0028)

율적으로 하기 위한 TESLA[5] 등이 제안되었다. 특히 EMS는 송신자가 소스 코딩 알고리즘을 이용하여 패킷집합에 대한 서명을 각 패킷에 분산키고 이를 수신자에게



(그림 1) CAS의 구조

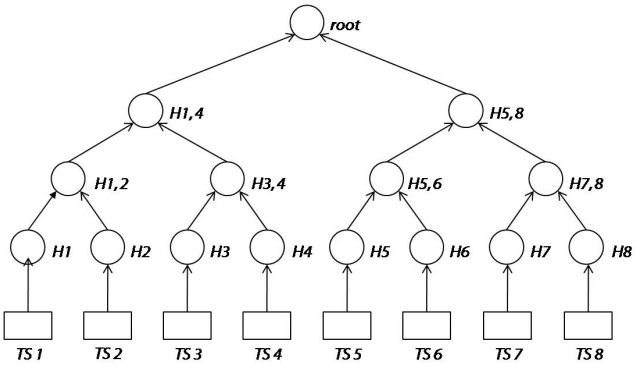
전달하며 수신자는 받은 패킷을 이용하여 서명을 복원함으로써 소스를 인증한다. 하지만 송신자와 수신자가 데이터를 처리하는 데 있어서 많은 연산과 시간이 요구되어 IP-TV와 같은 실시간 데이터를 전송하는데 적합하지 않다. 또한 TESLA는 키에 대한 해쉬 체인과 지연된 키를 이용하여 각 패킷의 소스를 인증하는 방식으로 분쟁 발생 시 법적 근거를 제공할 수 있는 부인방지를 지원하지 않으며, 이로 인하여 IP-TV 콘텐츠 소스 인증에 적합하지 않다.

3. CAS

CAS는 사용자의 콘텐츠에 대한 접근 제어를 위하여 스크램블링과 디스크램블링을 통하여 데이터 스트림을 보호하며, 따라서 유효한 가입자만이 콘텐츠를 이용을 할 수 있다. CAS는 인증 되지 않은 수신기로부터 서비스를 보호하기 위한 암호화 기술과 불법적인 사용자를 막기 위한 스크램블링 기술로 구성되어 있다. (그림 1)은 CAS의 구조이다.

일반적으로 서비스 공급자는 콘텐츠 공급자로부터 콘텐츠를 받아 데이터 스트림, 즉 TS(Transport Stream)를 수신권한이 있는 가입자만 이용할 수 있도록 원래의 신호를 변형시키는 스크램블링을 수행한다. 수신권한이 있는 가입자는 전송받은 스크램블된 TS로부터 원래의 신호를 생성해 낸다. 이 과정을 디스크램블링이라 한다. 스크램블링과 디스크램블링을 위해서는 CW(Control Word)라는 랜덤값이 이용된다. CW를 통하여 보안을 제공하기 때문에 이 값은 매우 빠른 주기로 갱신이 된다.

또한 불법적인 사용자가 CW를 얻지 못하게 하기 위하여 AK(Authorization Key)로 CW값이 암호화되며, 이 값은 ECM(Entitlement Control Message)와 함께 보내지게 된다. AK는 MPK(Master Private Key)로 암호화되어, EMM(Entitlement Management Message)에 포함되어 가



(그림 2) Merkle Tree의 구조

입자에게 전달이 된다. 이 EMM의 값은 상대적으로 긴 주기로 가입자에 보내어 진다. 서비스 공급자는 가입자에 대하여 해당 MPK를 생성하여 가입자 셋탑박스의 스마트카드에 이 값을 저장한다. 실제 데이터 스트림 사이에 ECM이 끼워져 전달된다. 일반적으로 ECM과 EMM은 서비스 보안을 위한 중요한 메시지이므로 서비스 공급자가 전자서명을 해서 함께 보내며, 가입자는 서명을 검증함으로써 ECM과 EMM의 유효성을 확인한다[1].

4. IP-TV 시스템을 위한 소스 인증

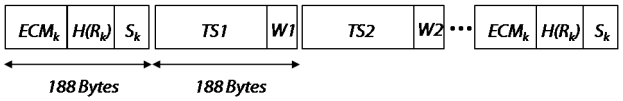
일반적으로 소스 인증을 위해서는 송신자와 수신자가 공유하고 있는 대칭키를 사용하거나, 비대칭 키를 이용한 전자서명 방식을 사용한다. 하지만 그룹통신에서 소스 인증을 위해서는 하나의 송신자와 나머지 n명의 그룹 멤버 사이에서 n개의 PSK(Pre Shared Key)를 공유해야 한다. 이러한 방식은 브로드캐스팅을 통하여 메시지를 전송할 경우에는 적용할 수 없다는 문제점이 있다. 따라서 일반적으로 브로드캐스트 메시지에 대한 소스인증을 위하여 전자서명을 이용한다.

하지만 전자서명을 통한 인증방법은 서명자와 검증자 모두 많은 계산을 필요로 하기 때문에, 데이터 스트림을 검증하는데 있어서 많은 지연이 발생한다. 그러므로 IP-TV와 같은 실시간 방송의 경우 이러한 지연은 서비스의 질을 떨어뜨리는 결과를 낳기 때문에 효율적인 소스 인증 방법이 필요하다. 이를 위하여 최소한의 전자서명을 함으로써 서명에 대한 검증 횟수를 최소화함으로써 실시간 서비스를 제공할 수 있어야 한다. 또한 패킷 손실의 여부와 관계없이 패킷 인증을 제공해야하며, 데이터 전송 이후에 분쟁이 생겼을 경우, 데이터 전송에 대한 부인 방지를 위한 부인 방지 서비스가 제공이 되어야 한다.

따라서 본 논문에서는 위에서 언급한 요구사항을 만족시키기 위하여 MT(Merkle Tree)[6]를 이용하여 서비스 공급자로부터 공급되는 데이터 스트림에 대한 소스 인증

을 제공한다. (그림 2)는 일반적인 MT의 구조이다.

MT는 종단 노드에 대한 인증을 제공하는 이진트리로써 해쉬 함수와 연결(Concatenation)을 이용하여 트리를



(그림 3) 제안한 프로토콜의 스트림

구성한다. 각 패킷의 해쉬 값을 구하고, 이 값들을 트리의 종단 노드로 구성을 한다. 각 종단 노드 쌍들을 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, 루트 값과 서명을 수신자에게 전달한다. 송신자는 루트 경로로의 형제 노드를 해당 패킷과 함께 보내주며, 수신자는 이 패킷과 형제 노드를 이용하여 트리의 루트를 생성한다. 이 값을 송신자로부터 받은 루트 값과 비교하여 패킷의 소스를 검증한다. MT는 연산이 빠른 해쉬 함수를 사용하였기 때문에, 패킷을 인증하는데 필요한 시간을 최소화 할 수 있으며, 패킷 손실이 있더라도 나머지 패킷에 대한 인증이 가능한 장점을 갖고 있다. 하지만 각 패킷과 함께 보내어지는 해당 형제 노드들로 인하여 통신 오버헤드가 증가하게 된다.

예를 들면 (그림 2)에서 송신자는 보낼 패킷 집단에 대하여 트리를 구성하고 해당 트리의 루트를 ECM, 그리고 서명과 함께 전송한다. 송신자가 TS1을 전송하는 경우, 실제 데이터 패킷인 TS1과 루트 경로로의 형제 노드인 H2, H34, H58을 함께 보낸다. 수신자는 전송 받은 이 값들을 이용하여 루트를 복원한다. 이 값을 먼저 수신한 ECM과 함께 보내어진 루트 값과 비교한다. 이를 통하여 소스를 인증할 수 있다.

앞에서 언급하였듯이 ECM과 EMM은 서비스 공급자에 의하여 서명을 한다. 또한 ECM의 주기가 EMM의 주기보다 훨씬 짧기 때문에, ECM을 이용하여 데이터 스트림을 인증하는 것이 더욱 적합하다. 이를 위하여 ECM과 ECM 사이의 전달할 TS의 해쉬 값을 종단 노드로 하여 MT를 구성한다. 그리고 MT의 루트를 인증하기 위하여, 루트의 해쉬 값을 ECM의 패킷과 함께 보내고, 이 값들에 서명함으로써 ECM과 ECM사이의 모든 패킷에 서명한 효과를 얻을 수 있다. 서비스 공급자는 ECM 사이의 데이터 스트림, 즉 TS에 루트를 복원할 수 있도록, 루트 경로로의 형제 노드들을 붙여준다. 이를 받은 각 가입자는 자신이 받은 TS과 해당 형제노드들을 이용하여 루트를 다시 복원하여 해쉬 값을 계산하고, ECM을 통해 전달된 루트의 해쉬 값을 비교하여 같을 경우, 공격자가 아닌 인증된 서비스 공급자로부터 데이터 스트림이 온 것인지를 확인할 수 있다. 만약 같지 않을 경우는, 해당 TS를 버퍼링할 필요 없이 버린다.

(그림 3)은 제안된 프로토콜의 데이터 스트림이다. 그림에서 $H(R_k)$는 루트에 대한 해쉬 값, S_k는 ECM_k와 $H(R_k)$에 대한 서명, 그리고 W_n은 n번째 TS대한 형제 노들들 값이다. 최소한의 서명을 통하여 전체 패킷을 서명한 효과를 얻을 수 있으며, 패킷의 손실 여부와 상관없이 받은 모든 패킷에 대하여 소스 인증을 할 수 있다. 또한 인증을 위한 버퍼링이 필요 없기 때문에 DoS(Denial of Service) 공격을 막을 수 있다.

5. 제안하는 프로토콜의 분석

가장 확실한 소스 인증 방법은 전달되는 모든 패킷에 서명을 하는 것이다. 하지만 앞에서 언급하였듯이 이는 실시간 서비스에 적합하지 않다. 본 논문에서 제안하는 프로토콜은 기존 CAS의 ECM에 서명하는 것을 그대로 이용하기 때문에, 추가적으로 서명을 하는데 필요로 하는 자원을 최소화 하였으며, 해쉬 함수를 이용하여 패킷을 인증하기 위한 오버헤드를 최소화 하였다. 또한 각 패킷에 형제 노드들을 붙여줌으로써, 패킷 스트림의 일부분의 손실이 있더라도 나머지 패킷의 인증을 할 수 있다.

제안된 프로토콜은 ECM과 함께 해당 트리의 루트에 대한 해쉬 값을 받기 때문에 가입자가 받은 패킷에 대하여 몇 번의 연산 후에 소스 인증을 할 수 있기 때문에 버퍼링이 필요 없어 DoS공격을 막을 수 있다.

IP-TV에 TESLA 프로토콜을 적용시킬 경우 시간동기화(Time Synchronization)가 필수적이지만, IP-TV 시스템의 특성상 빠르게 변하는 가입자로 인하여 시간동기화를 계속적으로 갱신해야만 하며, 데이터 스트림을 전송중인 가운데 TESLA를 위한 시간동기화를 맞추기는 쉽지 않다. 하지만 제안된 프로토콜은 시간동기화가 전혀 필요하지 않으며, 빠르게 변화하는 가입자 수와 관계없이 소스 인증을 제공할 수 있기 때문에 확장성이 좋으며, 이는 IP-TV에 대한 수요가 증가함에 따라 제안된 프로토콜이 갖는 큰 장점이다.

6. 결론

현재 IP-TV시스템은 데이터 스트림에 대한 소스 인증을 하지 않기 때문에, 가입자들은 공격자에 의해 변조된 데이터 스트림 전송에 무방비 상태로 노출되어 있다.

본 논문에서는 기존 CAS의 보안 취약성으로 인한 문제점을 분석하고, 데이터 스트림에 대한 소스 인증을 제공함으로써 이 문제점을 해결하였다. 최소한의 서명 검증 회수와 효율적인 해쉬 함수 사용을 통하여 IP-TV의 필수적인 실시간 서비스를 가능하게 하였다. 또한 패킷 손실이 있을 경우, TS와 함께 보내어지는 형제 노드들로 인하여 나머지 패킷에 대한 소스 인증이 가능하다. 따라서 완벽한 소스 인증과 부인방지를 제공함으로써, 공격자의 DoS 공격을 완벽히 방지하고, 추후에 분쟁이 생겼을 경우 법적 근거를 제시할 수 있다.

마지막으로, 본 프로토콜에서는 TESLA 프로토콜에서의 필수적인 시간 동기화가 필요하지 않다. 따라서 사용자

의 수와 관계없이 소스 인증 서비스를 제공할 수 있으므로, IP-TV 수요의 폭발적인 증가에 대처할 수 있는 적합한 프로토콜이다.

하지만 각 데이터 패킷과 함께 보내는 형제 노드는 통신 오버헤드를 증가시킬 수 있다. 따라서 해쉬 값의 크기를 적당히 조절함으로써 적절한 보안 강도와 적합한 통신 오버헤드를 제공할 수 있다. 이러한 트레이드오프에 관한 연구는 향후 과제로 남겨둘 것이다.

참고문헌

[1] T. Yoshimura, "Conditional Access System for Digital Broadcasting in Japan" Proc. of IEEE, Jan. 2006

[2] B. Liu et al., "A Scalable Key Distribution for Conditional Access System in Digital Pay-TV system" IEEE Trans. on Consumer Electronics, May. 2004

[3] Y. Zhou et al., "Multimedia Broadcast Authentication Based on Batch Signature" IEEE Communications Magazine, Aug. 2007

[4] J. M. Park et al., "Efficient Multicast Packet Authentication using Signature amortization" Proc. of 2002 IEEE Symposium on Security and Privacy

[5] A. Perrig et al., "Efficient and Secure Source Autehtication for Multicast" Net. and Distrib. Sys. Sec. Symp., Feb. 2001

[6] R. Merkle, "Protocols for Public Key Cryptosystems," Pro. IEEE Symp. Security and Privacy, Apr. 1980