인터넷 기반의 유료 방송에서 IGMP를 개선한 그룹 관리 기법*

김정훈[1†], 이훈정[1], 김상진[2], 오희국[1]
[1]한양대학교 컴퓨터공학과
[2]한국기술교육대학교 컴퓨터공학과

Enhanced Internet Group Management Protocol for Pay-TV Service in IP Network

Junghoon Kim[1†], Hoonjung Lee[1], Sangjin Kim[2], Heekuck Oh[1]
[1]Dept. of Computer Science and Engineering, Hanyang University
[2]Dept. of Computer Science and Engineering, Korea University of Technology and Education

요 약

위성이나 케이블을 통해서 이루어지던 유료 방송 서비스가 최근에는 IPTV 라는 이름 아래 인터넷을 통해서 이루어지고 있다. IP 네트워크를 통해 콘텐츠가 전송되면서 네트워크의 대역폭을 효율적으로 사용하기 위해 멀티캐스트를 통해 이루어진다. 멀티캐스트는 IP 환경에서 동일한 내용의 데이터를 여러명의 특정한 그룹의 수신자에게 동시에 전송하는 것을 말하며, 이때 그룹을 관리하기 위해 인터넷 그룹 관리 프로토콜(Internet Group Management Protocol, IGMP)이 사용된다. IGMP에는 접근제어와 같은 보안 기능을 제공하지 않고 있으며, IPTV와 같은 유료 방송 서비스에서는 멀티캐스트를 통해 전송되는 콘텐츠를 보호하기위해 접근제어시스템(Conditional Access System, CAS)을 사용한다. 그러나 CAS를 통해 콘텐츠를 보호 하더라도, IGMP에는 보안 기능이 없다는 근본적인 문제에 의해 사용자의 TV 시청을 방해할 수 있다는 가능성이 남아있다. 본 논문에서는 이러한 문제를 해결하기 위해 CAS가 운영되면서 교환된 키를 사용해 IGMP메시지에 보안기능을 추가한 기법을 제안한다.

1. 서론

위성이나 케이블을 통해서 이루어지던 유료 방송 서비스가 최근에는 IPTV 라는 이름 아래 인터넷을 통해서 이루어지고 있다. IPTV는 광대역 연결 상에서 인터넷 프로토콜을 사용하여 소비자에게 디지털 텔레비전 서비스를 제공하는 시스템을 말한다. 케이블이나 위성 방송은 단방향 통신을 기본으로 하지만 IPTV는 양방향 통신이 가능하다는 인터넷의 특성을 이용할 수 있기 때문에 기존의 방송 매체와 비교했을 때, 사용자와의 활발한 상호작용이 가능하다는 장점이 있다. 이러한 장점을 이용하여 VoD는 물론 기존 웹에서 이루어지던 정보검색, 쇼핑, 뱅킹 서비스는 물론이고, VoIP등과 같은 인터넷 서비스를 부가적으로 제공할 수 있게 된다. IPTV는 다양한 서비스 제공과 더불어 멀티미디어 및 맞춤형 방송 서비스에 대한 소비자들의 욕구를 충족시킬 수 있어 그 사용자의 수는 나날이 증가하고 있는 추세이다.

IPTV에서는 IP 네트워크를 통해 콘텐츠를 전송한다. 이때 사용되는 네트워크의 대역폭을 효율적으로 사용하기 위해 실시간 방송은 멀티캐스트를 통해 이루어진다. 멀티캐스트는 IP 환경에서 동일한 내용의 데이터를 여러 명의 특정한 그룹의 수신자에게 동시에 전송하는 것을 말하며, 이는 하나의 수신자에게 데이터를 전송하는 유니캐스트와 대응되는 개념이다. 멀티캐스트에서 말하는 그룹은 IGMP(Internet Group Management Protocol)를 통해 관리된다[1][2][3]. IGMP에는 접근제어와 같은 보안 기능을 제공하지 않고 있다. 따라서 멀티캐스트를 통해 전송되는 데이터는 기밀성을 보장할 수 없다. 이러한 문제를 해결하기 위해 정당한 사용자들 간에 안전하게 키를 공유하기 위한 그룹 키 개념을 도입한 연구가 활발하게 진행되고 있다[4][5]. 다른 한편으로는 IGMP에 접근제어 기능을 추가하는 연구가 이루어지고 있지만 그룹 키에 관한 연구보다는 활발하지 않게 진행되고 있다[6][7].

IPTV에서는 콘텐츠를 전송하기 위해 IGMP를 사용해 멀티캐스트를 하고 있으며, 콘텐츠를 보호하기 위해 CAS(Conditional Access System)를 사용하고 있다. 그러나 IGMP의 보안 기능이 없다는 근본적인 문제는 대용량의 유료 콘텐츠가 전송되는 IPTV 서비스에서 예상하지

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2011-C1090-1111 - 0010).
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2011-0000189).
† 주저자, jhkim@infosec.hanyang.ac.kr

못한 문제를 발생하게 한다. 기존의 위성이나 케이블 방송은 단방향 통신을 기반으로 하기 있기 때문에 모든 콘텐츠가 하나의 스트림으로 전송되던 환경에서는 생각하지 않아도 되었던 문제가 IP상에서 IGMP를 통해 선택적으로 방송 스트림을 수신하게 되면서 사용자의 시청을 방해할 수 있게 한다. 이러한 문제를 해결하기 위해 CAS에서 제공하는 보안기능을 바탕으로 IGMP에 최소한의 기능을 추가하면 위와 같은 문제를 해결할 수 있다.

이어지는 논문의 구성은 다음과 같다. 2장에서는 연구의 배경이 되는 CAS와 IGMP에 대해서 살펴본 뒤, 3장에서는 IPTV를 위해 IGMP를 개선한 기법을 제안하고 4장에서 제안하는 기법을 분석한 뒤, 5장에서 결론을 짓는다.

2. 연구배경

이 장에서는 유료 방송에서 콘텐츠 보호를 위해 사용하는 CAS에 대해 살펴보고, 멀티캐스트를 위해 사용되는 IGMP에 대해 알아본다.

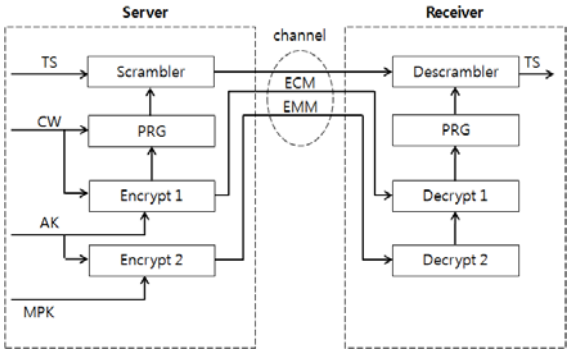
2.1 Conditional Access System(CAS)

CAS는 방송 사업자들이 요금을 지불한 정당한 가입자에 대해서만 콘텐츠를 시청할 수 있도록 하기 위해 사용하는 접근제어 기술로 CSA(Common Scrambling Algorithms)에 의해 콘텐츠를 스크램블링/디스크램블링하는 기능과 이때 사용하는 여러 키들을 계층적으로 관리하는 기능을 한다. [그림 1]은 CAS의 구조를 나타낸다[8][9].

CAS에서 사용되는 키들을 계층적으로 관리하는 기능은 사용자의 셋톱박스에 내장된 스마트카드를 바탕으로 이루어진다. 스마트카드는 서비스 제공자가 발급하는 것으로 권한이 있는 사용자라면 스마트카드에 저장된 공개키 기반의 MPK(Master Private Key)를 통해 스크램블링에 사용되는 키를 얻을 수 있다. 스크램블링에 사용되는 키는 CW(Control Word)라 하며 대칭키 기반의 AK(Authorization Key)를 통해 암호화 되어 ECM(Entitlement Control Message)의 형태로 전송된다. AK는 사용자의 스마트카드에 내장된 MPK를 통해 암호화 되어 EMM(Entitlement Management Message)의 형태로 따라서 권한이 있는 사용자는 스마트카드의 내장된 MPK를 통해 EMM을 복호화 하여 AK를 얻고, AK를 통해 ECM을 복호화 하여 CW를 얻을 수 있게 된다. 이때 사용되는 키들은 모두 스마트카드 내부에서만 사용되며 외부로 노출되지 않는다. 또한 CAS에서 사용되는 키는 스마트카드를 소유하고 있는 사용자도 알 수 없다. 만약 스마트카드에 저장된 MPK가 노출되어 유포된다면 노출된 키를 통해 AK와 CW를 얻어, 정당하지 않은 방법으로 방송을 시청할 수 있게 되는 문제가 발생한다. 따라서 CAS의 안전성은 스마트카드에 의존한다고 할 수 있다.

2.2 Internet Group Management Protocol(IGMP)

IGMP는 IETF(Internet Engineering Task Force)에서

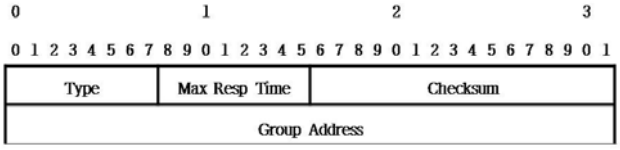


(그림 1) CAS의 구조

제정한 국제 표준으로 IPv4 환경에서 멀티캐스트 그룹을 관리하기 위해 사용되는 라우터와 호스트간의 시그널링 기술이다. 각 호스트는 라우터에게 report/leave 메시지를 전송하여 멀티캐스트 그룹에 가입/탈퇴를 하고 라우터는 호스트에 query 메시지를 전송하여 멀티캐스트 그룹에 계속 참여할지를 질의하게 된다. 특정 그룹에 대해 멀티캐스트 된 데이터는 라우터에게 전달되며 라우터는 해당 그룹에 참여하고 있는 호스트가 있으면 데이터를 라우터와 직접 연결된 모든 호스트에게 전송한다. 이때 그룹에 참여하고 있지 않은 호스트에게 멀티캐스트 데이터를 전송하는 것은 대역폭을 의미 없이 낭비한다고 할 수 있으며, 이를 막기 위해 스위치에서 IGMP 메시지를 해석하고, 해당하는 포트에만 멀티캐스트 데이터를 전송하는 IGMP Snooping 기술이 사용된다[10].

IGMP는 현재 IGMPv1, IGMPv2, IGMPv3 세 가지의 버전이 있으며, 상위 버전에서는 이전 버전과의 호환성을 지원한다. 호스트는 라우터에게 IGMP report 메시지를 전송하여 멀티캐스트 그룹에 가입하고, 라우터는 호스트들에게 주기적으로 IGMP query 메시지를 전송하여 호스트가 멀티캐스트 그룹에 계속 참여할 것인지를 확인한다. IGMPv1의 특징은 탈퇴메시지가 없다는 점이다. IGMPv1에서 탈퇴는 라우터의 query에 대한 응답이 하나도 없을 경우 그룹 내에 수신자가 하나도 없는 것으로 간주하고 데이터 전송을 중단하는 형태로 이루어진다. 실제 호스트에서 더 이상 멀티캐스트되는 데이터의 수신을 원하지 않는 시점부터 라우터가 이를 파악하기 까지 발생하는 대역폭의 낭비를 막기 위해 IGMPv2에서는 leave 메시지가 추가되었다. IGMPv3에서는 그룹 내에서 특정 소스로부터 전송되는 데이터를 선택적으로 수신할 수 있게 하는 기능이 추가되었다.

IPTV에서는 모든 방송 데이터를 서비스 제공자가 전송하는 것이기 때문에 IGMPv3의 기능은 필요로 하지 않



(그림 2) IGMPv2 메시지 포맷

는다. 또한 IGMPv1에서 발생하는 대역폭의 손실은 IPTV에서 크게 작용하기 때문에 IGMPv2를 사용해야 한다. (그림 2)는 IGMP의 메시지 포맷을 나타낸다.

2.3 IPTV에서 IGMP의 역할과 문제점

IGMP는 IP 네트워크 상에서 수신자가 원하는 멀티캐스트 그룹에 가입/탈퇴하기 위해 사용하는 프로토콜이다. IPTV의 실시간 방송 채널은 각각의 멀티캐스트 그룹을 형성하고 있다. IPTV에서 IGMP는 채널을 변경하면서 사용된다. 사용자가 원래 시청하고 있던 채널에서 다른 채널의 시청을 원하게 되면 IGMP를 통해 기존에 시청하고 있던 채널의 그룹에서 탈퇴를 하고, 이어서 시청할 채널의 그룹에 가입을 하게 된다. 새로운 채널 그룹에 가입하면 즉각 해당 채널의 방송 데이터가 전송되어 결과적으로 사용자는 원하는 채널을 시청할 수 있게 된다. 이때 IGMP에서 제공하는 보안기능이 없기 때문에 발생하는 문제는 다음과 같다.

- IGMP 메시지는 다른 사용자가 보낸 것처럼 위장하여 해당 사용자가 시청하고 있는, 현재 가입되어 있는 멀티캐스트 그룹에서 탈퇴시키는 것이 가능하다. 이러한 공격은 IGMP Snooping 기능이 사용되고 있는 경우에만 가능하다. 라우터는 탈퇴 메시지를 받으면 해당 그룹의 데이터를 계속 상위 라우터로부터 수신할지를 결정하기 위해 호스트에게 query 메시지를 보내 판단한다. IGMP Snooping 기능이 사용되지 않는다면 사용자는 query에 대한 응답으로 repot 메시지를 다시 보내기 때문에 문제가 발생하지 않는다. IGMP Snooping 기능이 사용되는 경우 탈퇴를 하게 되면 사용자에게 더 이상 해당 그룹의 메시지가 전달되지 않아, query 메시지를 수신하지 못하게 되고 응답 역시 하지 못해 라우터는 자연스럽게 탈퇴로 인식하게 된다.
- 여러 채널에 가입한 것으로 위장하여 네트워크의 대역폭을 의미 없이 소비하게 하는 경우도 발생할 수 있다. IPTV는 CAS에 의해 콘텐츠가 보호되고 있다. 따라서 권한 여부에 상관 없이 채널의 멀티캐스트 그룹에 쉽게 가입할 수 있다. 만약 공격자가 여러 멀티캐스트 그룹에 가입하게 되면 해당 그룹의 방송 데이터를 수신하게 되는데 방송 데이터는 동영상 정보이기 때문에 많은 대역폭을 필요로 하게 된다. 만약 다른 사용자가 멀티캐스트 그룹에 가입하는 것으로 위장하여 라우터에게 report 메시지를 전송한다면 해당 사용자는 의미 없이 대역폭을 소비하게 될 것이다.

3. 제안하는 기법

이 장에서는 IP 네트워크 상에서 CAS에 의해 서비스되는 방송 서비스를 안전하게 지원하기 위해 IGMP에 보안 기능을 추가한 기법을 제안한다. 제안하는 기법은 기존에 사용되는 IGMP와 동일한 역할을 한다. 기존 IGMP와 다른 점은 CAS에서 사용되는 키를 사용해서 스마트카드가 생성한 메시지임을 확인하는 기능을 추가하였다는 점이다.

<표 1> 표기법

표기	설명
TS	Transport Stream
AK	Autorization Key
MPK	Master Private Key
TK	Token Key
IP	소스의 IP
T	토큰을 생성한 시간, 타임스탬프
R	랜덤 값
EMM	Entitlement Management Message
ECM	Entitlement Control Message

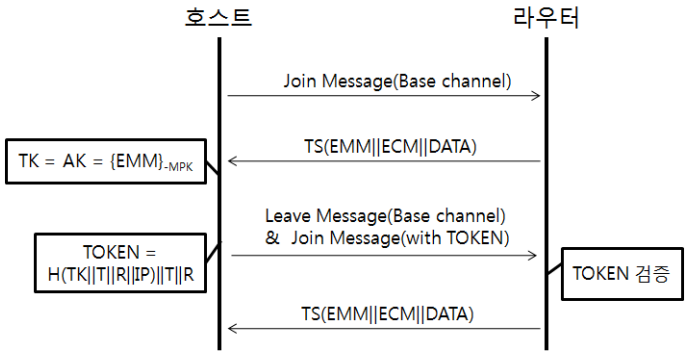
3.1 환경정의

제안하는 기법은 유료 콘텐츠에 대한 보호를 위해 CAS를 사용하는 방송 서비스를 IP 네트워크 상에서 제공하는 환경을 바탕으로 하고 있다. 기존 시스템과 마찬가지로 CAS에서 보안 기능과 관련된 모든 연산은 스마트카드 내부에서 이루어지며, 키는 외부로 유출되지 않는다. 또한 방송 서비스를 제공하는 사업자는 네트워크 또한 제공하며, 라우터에는 조작 불가능한 하드웨어(Tamper Resist Hardware, TRH)를 통해 CAS에서 사용하는 키를 획득할 수 있는 환경이라고 가정한다.

3.2 강화된 인터넷 그룹 관리 프로토콜

제안하는 기법은 기존 시스템에서 권한에 상관없이 모든 그룹에 참여할 수 있으며, 다른 사용자가 보낸 메시지로 위장하는 것을 막기 위해 CAS에서 사용하는 키를 사용하였다. 이를 통해 제안하는 기법은 스마트카드에서 생성한 IGMP 메시지임을 인증 할 수 있게 되고 불법적인 목적으로 다른 사용자가 생성한 것처럼 IGMP 메시지를 위조할 수 없게 하였다. <표 1>은 제안하는 기법의 표기법을 나타낸다.

제안하는 기법은 기존의 IGMP가 수행하는 역할을 그대로 수행한다. 호스트에서 메시지를 생성하는 것과 라우



(그림 3) 제안하는 기법

터에서 메시지를 생성하는 것 역시 모두 동일하다. 다만 스마트카드에서 생성한 인증 토큰이 추가된다는 점이 다르다. 스마트카드에서는 인증 토큰을 생성하기 위해 CAS의 AK를 사용한다. AK를 얻기 위해서는 먼저 멀티캐스트 그룹에 가입해야 하는데, 그룹에 가입하려면 AK를 얻어야 한다. 따라서 인증 토큰에 상관 없이 가입할 수 있는 그룹을 지정해서 스마트카드에서 AK를 얻을 수 있도록 한다. IPTV의 경우 서비스가 시작되면 무조건 광고채널부터 시작하는데, 해당 채널의 그룹은 인증 토큰에 상관 없이 가입할 수 있게 하고 나머지 다른 채널은 인증 토큰을 확인하여 스마트카드에서 생성한 메시지인지 여부를 검증한다.

(그림 3)은 제안하는 기법을 나타낸다. 인증 토큰을 생성할 때 사용하는 키는 TK라 하며, 기본 채널의 AK와 같다. 인증 토큰은 TK와 토큰을 생성한 시점의 타임스탬프 T, 랜덤 값 R, 소스의 IP주소, 네 값의 해쉬 값과 T, R로 이루어져 있다. 랜덤 값 R은 소스별로 정해진 시간 내에 다시 사용할 수 없도록 해야 하며, 토큰을 생성하기 전에 R값을 확인해야 한다. 라우터에서 이를 검증할 때에는 먼저 T를 통해 최신성을 판별하고, R과 IP를 통해 토큰이 재사용 되는것인지 판별한다. 검증이 완료되면 라우터는 해당 메시지의 내용대로 그룹에 가입/탈퇴를 수행한다.

4. 분석

4.1 보안 요구사항

제안하는 기법은 CAS에서 사용하는 키를 사용하여 스마트카드에서만 생성할 수 있는 인증 토큰을 바탕으로 그룹에 대한 가입/탈퇴 메시지의 유효성을 판별한다. 제안하는 기법은 특정 사용자를 인증하는 것이 아닌, 방송 사업자가 제공한 스마트카드를 통해서 메시지가 생성된 것인지 만을 판단한다. 이 때문에 다른 스마트카드에서 사용한 인증 토큰을 다시 재사용할 수 없어야 하며, 임의로 생성할 수 없어야 한다.

4.2 안전성 분석

제안하는 기법은 CAS의 안전성에 기반한다. 먼저 메시지에 사용되는 TK는 기본채널의 AK이다. AK는 스마트카드에서 관리되고 사용되며, 외부로 절대 유출되지 않는다. 따라서 공격자는 인증 토큰을 임의로 생성할 수 없다. 또한 이미 사용된 인증 토큰은 R값을 통해 판별이 가능하다. 만약 공격자가 소유한 셋톱박스의 스마트카드로부터 사용하지 않은 토큰을 생성한다 해도 해쉬값에 포함된 스마트카드의 IP주소 때문에 다른 사용자로 위장한 메시지에서는 사용할 수 없다. 따라서 제안하는 기법은 위에서 제시한 요구사항을 만족한다.

5. 결론 및 향후과제

본 논문에서는 IP 네트워크 상에서 CAS를 통해 이루어지는 방송 서비스에서 발생할 수 있는 멀티캐스트 그룹 관리의 문제를 해결하기 위한 기법을 제안하였다. 멀티캐스트를 사용하는 환경에서 콘텐츠의 보호를 위해 CAS가 적용된 점을 활용하여 이미 교환된 키를 이용해 인증을 위해 서명이나 키 교환을 하지 않고 그룹에 가입/탈퇴 할 수 있는 자격을 증명하게 하였다. 제안하는 기법을 적용하면 현재 멀티캐스트와 CAS를 통해 제공되는 서비스를 보다 안전하게 제공할 수 있다.

라우터에 추가되는 연산은 DoS 공격에 취약해지는 문제가 발생할 수 있다. 따라서 제안하는 기법은 최소한의 연산을 추가하여 문제를 해결하고자 하였다. 향후, 추가된 연산으로 인해 라우터의 데이터 처리량이 얼마나 영향을 주는지 파악하고 DoS 공격에 얼마나 영향을 받을 수 있는지에 대한 분석이 필요하다.

참고문헌

[1] S. Deering, "Host Extensions for IP Multicasting", http://www.rfc-editor.org/rfc/rfc1112.txt, 1989.

[2] W. Fenner, "Internet Group Management Protocol, Version 2," http://www.rfc-editor.org/rfc/rfc2236.txt, 1997

[3] B. Cain, S. Deering, I. Kouvelas, B. Fenner and A. Thyagarajan, "Internet Group Management Protocol, Version 3," http://www.rfc-editor.org/rfc/rfc3376.txt, 2002.

[4] Huanhuan Zhao, Yong Xu and Xiaowei Zhu, "An Optimization of Rekeying Scheme for Secure Multicast," International conference on Web Information Systems and Mining 2010, 2010

[5] Vijayakumar P., Bose S., Kannan A., Subramanian S.S., "An Effective Key Distribution Protocol for Secure Multicast Communication," International Conference on Advanced Computing 2010

[6] Islam S. and Atwood J.W., "The Internet Group Management Protocol with Access Control(IGMP-AC)," IEEE Conference on Local Computer Networks, 2006

[7] Tsunemasa Hayashi, Akihiro Tanabe and Hiroaki Satou, "IGAP: Secure Group Management Protocol for Multicast Content Delivering Network," International Symposium on Multi-Dimensional Mobile Communications, 2004

[8] EBU Project Group B/CA, "Functional model of a conditional access system," EBU Technical Review, Dec, 1995

[9] Herve Benoit, "Digital Television," Focal Press, 2002

[10] M. Christensen, K. Kimball, F. Solensky, "Considerations for Internet Group Management Protocol(IGMP) and Multicast Listener Discovery(MLD) Snooping Switches," http://www.rfc-editor.org/rfc/rfc4541.txt, 2006