IP-TV를 위한 안전한 그룹관리 프로토콜[1)]

김인환*, 김정윤*, 최형기*
*성균관대학교 정보통신공학부
e-mail:ihkim@hit.skku.edu

Secure Group Management Protocol for IP-TV

In-Hwan Kim*, Jung-Yoon Kim*, Hyoung-Kee Choi*
*School of Information Communication, Sung Kyun Kwan University

요 약

IP-TV 서비스는 통신/방송 융합서비스로서 데이터 스트림이 송출되는 Server로부터 QoS가 보장되는 IP망을 통해 디지털 영상 방송이나 양방향 서비스를 가입자 단말까지 제공하는 서비스이다. IP-TV 서비스는 보안을 위해 CAS(Conditional Access System)를 사용하고, 또한 효율적인 콘텐츠의 전송을 위해 IP Multicast를 사용하게 된다.

보안 기능이 제공되지 않는 IP Multicast는 익명성을 허용하게 하여 eavesdropping, denial of service(DoS) Attack등이 가능하고, 또한 AAA(Authentication, Accounting, Authorization) 기능이 제공되지 않는다. IP-TV에서는 보안을 제공하기위해 Application 계층에서 CAS를 운용하게 되는데, 이는 Network계층에서 보안문제를 해결하는 것 보다 비효율적이다.

본 논문에서는 기존의 IGMP프로토콜을 확장, 개선하여 상호인증을 통해 CAS Server와 연계하여 IP-TV에 적합하게 만든 프로토콜을 제시함으로서, 이와 같은 문제점들을 해결하였다.

1. 서론

현대 산업의 Trend로서 고객의 요구를 충족시키기 위해, 각 산업 가치사슬 간의 융합화와 복합화가 발생하고 있다. 특히 통신 산업을 중심으로 융합화 사례가 지속적으로 출현하고 있는데, IP-TV는 좋은 예로서 통신과 방송이 융합된 형태이다. 멀티미디어 컨텐츠의 확산과 광대역(IP) Network의 발전이 이러한 통신/방송 산업구조의 변화를 이끌고 있다. 통신과 방송서비스의 융합에 따른 음성, 데이터, 방송을 모두 아우르는 TPS(Triple Play Service)가 본격 도입되었고, 향후, 통신/방송 융합에 기반한 홈네트워크 서비스로 진화, 발전 할 것으로 예상되고 있다.

이러한 배경을 바탕으로 IP-TV가 새로운 이슈로 떠오르고 있다. IP-TV는 기존 방송서비스의 단점인 단방향 서비스의 한계를 초고속 인터넷의 장점과 융합시킴으로서 인터넷 초고속망(IP) 및 TV 단말을 기반으로 방송과 완전한 양방향 데이터 서비스를 동시에 제공한다.

IP-TV 서비스를 이용하는 가입자들은 일반 TV와 마찬가지로 원하는 패키지를 선별해 고급정보나 프로그램을 유료로 시청하는 것이 가능하며, 세분화되고 다양한 장르의 채널에서 가입자 성향에 적절한 채널들만을 신청해 볼 수 있는 등 선택의 폭이 매우 넓어진다. 이는 가입자가 원하는 유료 콘텐츠의 시청 시간 및 프로그램에 따라 차등 적용하기 위한 Conditional Access System(CAS)[1]의 기능을 요구하게 되었다. CAS는 정당한 수신료를 지불하는 사람만이 프로그램을 시청 할 수 있도록 함으로써, 다양한 서비스를 제공 할 수 있게 하였다.

IP-TV 서비스는 멀티미디어 콘텐츠를 여러 가입자에게 효율적으로 전송하기 위해 Multicast를 사용하게 된다. 1:n 통신을 위해 Multicast는 그룹을 관리하는 IGMP[2] Protocol을 사용하게 된다. IGMP는 그룹에 가입하기위한 Join메시지, 그룹을 떠날 때 사용하는 Leave 메시지, 그리고 질의를 위한 Query메시지로 구분된다. 그러나 IGMP는 인증되지 않은 누구나 메시지를 전송할 수 있는 익명성을 갖고 있어서, 제약 없이 누구나 Join 메시지를 보내고 Multicast 그룹에 들어갈 수 있게 되어 쉽게 DoS Attack이 가능해지고, 또한 사업자는 유저의 사용정보를 알 수 없었다[3], [4].

본 논문에서는, Application 계층에서 이루어지던 CAS의 보안 이슈를 Network계층에서 해결하고자 한다. 7계층인 Application에서 이루어지던 보안 문제를 4계층에서 해결하여, 좀 더 빠르고 효율적인 통신이 이루어지게 한다. 우리는 기존의 IGMP를 개선 확장하여, IP-TV에 적합한 새로운 프로토콜을 제안 하고, 이 프로토콜을 사용하여 Authentication, Account, Authorization(AAA)기능[5] 을 제공하고 Multicast의 단점을 보완하여 좀 더 효율적으로 IP-TV의 보안문제를 해결하고자 한다.

"본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음"

2. 관련 연구

Multicast의 단점을 해결하고 AAA기능을 지원하기 위한 Multicast에 대한 많은 연구가 진행되어있다. Multicast Data의 안전한 전송을 위해 IETF의 MSEC Working Group에 의해 Group Security Architecture[6]가 개발되었고, 또한 GAC/GKM[7]과 같은 프로토콜도 제안되었다.

또한, Edge Node를 사용한 인증을 통하여, 안전한 Multicast 환경을 만들고 AAA기능을 제공하는 IGAP[8] 프로토콜도 제안되어 있다.

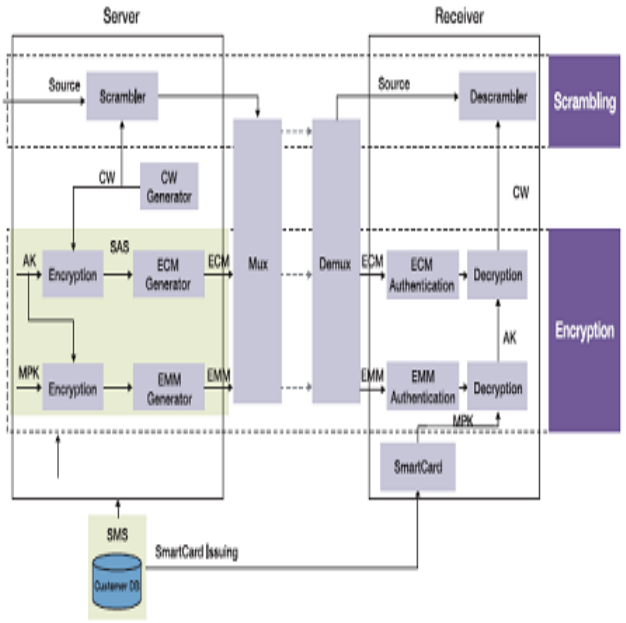
3. Conditional Access System(CAS)

CAS는 스크램블링(Scrambling)과 디스크램블링(Descrambling)을 통하여 데이터 스트림의 보안을 유지하는 보안 솔루션이다. CAS의 기술은 크게 두 부분으로 이루어진다. 인증 되지 않은 수신기로부터 서비스를 보호하기 위한 스크램블링(Scrambling)기술과 특정수신기만 볼 수 있도록 키로 전달하는 암호화(Encryption)기술로 구성된 수신제한기능, 그리고 이를 바탕으로 사용자에게 다양한 형태의 서비스를 제공하기 위한 사용자 서비스 지원기능으로 나눌 수 있다[1]. <그림 1>은 CAS의 구조를 보여주고 있다.

스크램블링(Scrambling)은 원래의 신호에 변형을 가하여 스크램블된 형태의 신호만으로는 수신권한이 없는 수신자는 시청 할 수 없도록 하는 것이고, 디스크램블링(Dscrambling)은 스크램블링된 프로그램을 원래의 신호대로 복원하는 과정을 말한다. 스크램블링과 디스크램블링에는 CW(Control Word)라는 키를 사용한다. Content Server에서는 CW로 데이터 스트림을 스크램블링하고 시청자 측의 수신기에서는 CW를 사용하여 데이터 스트림을 디스크램블링하여 서비스를 시청 할 수 있게 된다. 이 CW는 보안을 위하여 수초마다 갱신되며 AK(Authorization Key)를 사용하여 암호화되어 ECM(Entitlement Control Message)를 통해 사용자에게 전달된다. ECM은 암호화된 CW와 서비스를 접근하기 위해 필요한 요구 조건들을 전송하는 역할을 한다.

AK는 CW를 암호화하는 역할을 함으로써, CAS의 보안을 강화하고, MPK(Master Private Key)로 암호화되어 EMM (Entitlement Management Message)을 통하여 시청자에게 전달되며, 약 한달 주기로 갱신된다. 또한, EMM은 수신기의 보안장치인 스마트카드 내에 자격을 부여하거나 갱신하는 기능을 지원한다.

MPK는 AK의 암호화에 사용되며, 각 가입자에 고유하다. 이 키는 SettopBox내의 스마트카드 내에 저장되며 스마트카드가 수명이 다할 때 까지 변경되지 않는다[9], [10].



<그림 1. CAS의 구조>

Type	Max Resp. Time	Checksum
Group Address		
Version	*Report Type*	*Identifier*
Message Size		*Reserved*
Message		

<그림 2. messsage 형식>

4. 새로운 프로토콜

우리는 이번 장을 통해 현재 Multicast가 가지는 문제점들을 해결하고, IP-TV에 맞게 구성된 새로운 프로토콜을 설명할 것이다. 제안되는 프로토콜은 IP Multicast 그룹의 Join과 Leave 과정에서 가입자의 인증정보를 추가하여, 기존의 IGMP 프로토콜을 확장 개선하였다.

가. 프로토콜 메시지 형식

우리가 제안한 프로토콜 메시지의 처음 8Byte는 IGMPv2와 같은 필드로 구성되어 있다. <그림 2>에 제안하는 프로토콜의 메시지 형식이 나타나 있다

Type: IGMP와 다른 Type으로 Join(0x60), Query(0x61), Leave(0x62)이다.
Version: 일시적으로 "0x10"으로 명시한다.
Report Type: Join, Query, Leave의 상세적인 타입을

정의한다.

Identifier: SettopBox의 ID이다

Message Size: Message 필드의 길이를 나타낸다. 0에서 64까지의 값을 가진다.

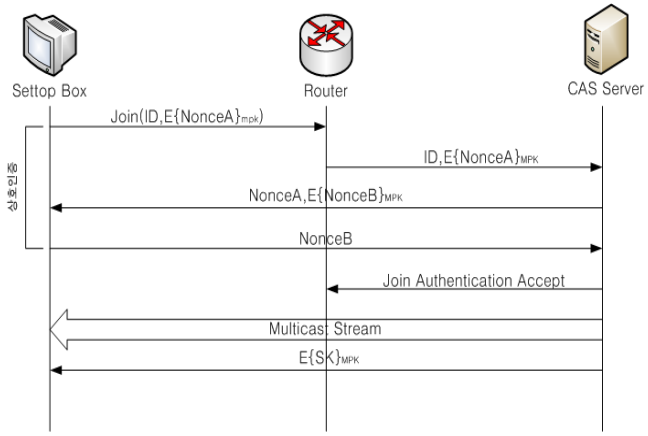
Message: Authentication과 Accounting을 위한 정보가 포함된다.

나. Join 절차

새로운 그룹 관리 프로토콜의 메시지는 Join 메시지에 가입자 정보를 포함하고, 이것을 받은 라우터는 이 정보를 CAS Server에게 전송하면서 SettopBox와 CAS Server사이에 상호인증이 시작된다. <그림 3>이 Join 과정을 표현하고 있다. 각각의 단계에 따른 설명은 다음에 나와 있다.

1) SettopBox Join메시지에 각 SettopBox의 유일한 식별자인 ID를 무작위로 생성된 랜덤 값 NonceA를 MPK로 암호화한 값과 함께 라우터로 전송한다.
2) Join메시지를 받은 Router는 메시지에 포함된 SettopBox의 ID와 MPK로 암호화된 NonceA를 CAS Server에 전송한다.
3) CAS Server는 각 SettopBox ID를 보고 그에 맞는 MPK로 메시지를 복호화한 후, NonceA와 자신이 생성한 NonceB를 MPK로 암호화 하여 SettopBox에게 전송한다. SettopBox는 NonceB를 MPK로 복호화 하여 다시 CAS Server에게 전송함으로써, 상호인증을 한다.
4) Multicast Stream이 SettopBox로 전달되고, CAS Server는 SK(Session Key)를 SettopBox에 전송한다.

Join 메시지에 인증에 사용되는 정보를 함께 보내서 SetopBox와 CAS Server간의 상호 인증을 하게 된다. 이를 통하여, 인증되지 않은 사용자로부터의 DoS Attack과 Replay Attack을 방지하고, 정확하고 확실한 AAA 기능을 지원하게 된다.



<그림 3. Join 과정>

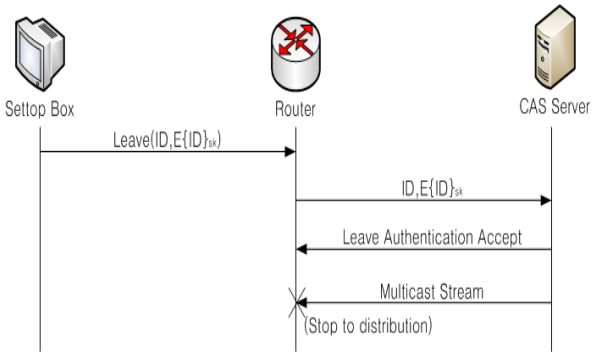
Join과정이 끝나면서, CAS Server는 SettopBox에 SK를 전달하게 되는데, 이 SK는 Leave절차에서 ID를 암호화하는데 사용되게 된다. 이 SK의 사용으로 Replay Attack을 방지할 수 있게 된다.

다. Leave 절차

Leave 절차에서는 SettopBox는 Leave 메시지에 자신의 ID와 SK로 암호화된 ID를 함께 전송하게 된다. <그림 4>가 새로운 프로토콜의 Leave 과정에 대해 나타내고 있다.

SK는 SettopBox의 ID를 암호화하는데 사용되며, 이 키는 매 Join시마다 CAS Server가 새롭게 갱신하여 Leave 과정에서 사용된다. SK를 사용하여, Join시와 마찬가지로 DoS Attack과 Replay Attack을 막고, AAA 기능을 제공하게 된다.

제안된 프로토콜의 Leave 과정은 기존 IGMP Leave 과정에 SK 사용을 더해서, 크게 떨어지지 않은 속도로, 더 높은 보안성을 제공하게 되었다.



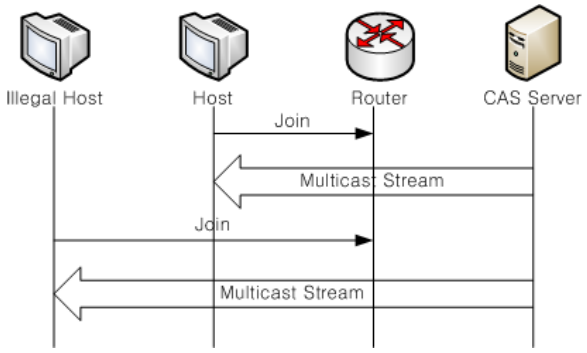
<그림 4. Leave 과정>

5. 프로토콜 성능평가

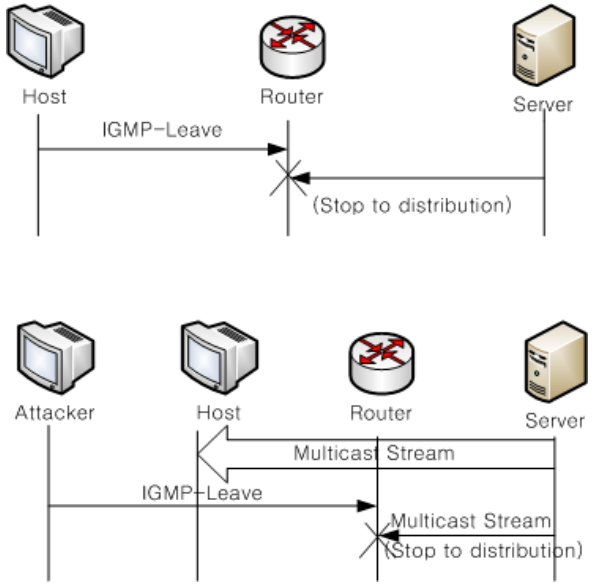
이번 장을 통해 기존의 IGMP에서 갖고 있던 문제점들을 살펴보고 우리가 제안한 프로토콜이 이 문제점들을 어떻게 해결하는지 살펴보고자 한다.

<그림 5>를 보면 IGMP의 Join시 문제점이 나타나 있다. 누구나 Join 메시지를 전송할 수 있어, 일반 사용자나 불법적인 사용자 모두 Multicast Stream을 수신할 수 있다. 우리가 제안한 프로토콜에서는 MPK와 Nonce 값들을 사용한 상호인증을 통해 이 문제점을 막고, AAA기능까지 제공하게 되었다.

Leave시의 문제점은 <그림 6>에 나타나 있다. 공격자는 정상적인 사용자인 것처럼 위장을 하여 메시지를 라우터에게 보내게 된다. 정상적인 사용자는 Multicast Stream을 수신하지 못하게 되는 DoS Attack이 가능해졌다. 우리가 제안한 프로토콜은 Join시 인증을 받고, SK를 사용자가 얻게 되면서, 인증된 사용자만이 정상적인 Leave절차를



<그림 5. IGMP Join시 가능한 문제점>



<그림 6. 일반 IGMP Leave와 Leave시 가능한 공격>

할 수 있게 된다. 또한, Join시 마다 변화하는 SK를 사용하여 Replay Attack도 방지하게 된다.

본 논문에서 제안된 프로토콜은 기존 IGMP의 약간의 변형과 상호 인증을 통해 크게 떨어지지 않은 속도로 안전한 통신환경을 구축하였다.

6. 결론 및 향후 연구

본 논문에서는 가입자의 인증과 관련된 정보를 포함하여 Join 과정과 Leave 과정을 수행하는 새로운 프로토콜을 제시하였다. Join시 MPK를 이용하여 상호인증 과정을 거치고 Leave시 SK를 사용하여, DoS Attack 및 Replay Attack을 방지하고, AAA 기능을 제공할 수 있게 되었다.

이 새로운 프로토콜은 기존의 IGMP를 개선 ,확장하여 IP-TV에 적합하게 설계되었기 때문에, IP-TV의 보안문제를 Network 계층에서 보다 쉽고 빠르게 해결하였다.

이와 비슷하게 IP-TV의 보안을 위해 많은 연구가 진행되고 있다. 그러나 아직까지 IP-TV에 대한 표준이 제정되지 않은 상황이라, IP-TV를 위한 연구에 많은 어려움이 존재하고 있다. 그렇지만, IP-TV의 성공적인 상용화와 활성화를 위해서는 지속적인 연구를 통해 표준이 제정되고, 이후로도 더욱 효율적인 IP-TV 서비스를 위해 연구와 개발이 꾸준히 이루어져야 한다.

본 논문에서는 유선환경의 IP-TV와 Multicast에 집중하였다. 현대사회에서는 무선 통신이 점점 더 각광받고 있는데, 무선 통신 환경은 Low Battery, Low Bandwidth 와 Low Performance가 특징이므로 더욱 효율적인 보안 메커니즘이 필요하게 된다. 이에 따라 추후 무선 통신 환경에서의 IP-TV와 Multicast의 보안에 대한 연구 역시 진행하겠다.

참고문헌

[1] 김용만, “디지털 방송을 위한 CAS(Conditional Access System)개발", 전자공학회지.

[2] W. C. Fenner, Internet Group Management Protocol, Version 2 IETF

[3] P. Judge and M. Ammar, "Security issues and solutions in multicast content distribution: A survey", IEEE Netw.Mag., vol.17, no.1, pp.30-36, Jan. 2003.

[4] M. Moyer, J. Rao, and P. Rohatgi, "A servey of security issues in multicast communications", IEEE Netw.MAG., vol.13, no.6, pp.12-23, Nov. 1999.

[5] C. Mets, "AAA protocols: Authentication,Authorization, and Accounting for the Internet", IEEE Internet Computing, December 1999.

[6] T. Hardjono and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[7] Li-Xin, Zhang-peng, and Ye-Chengqing,“GAC/GK-M: A Group Access Contorol Architecture for Secure Multicast", IEEE Communication, Circuits and Systems, 2005. Proceedings. 2005 International Conference on, vol.1, pp.502-507, May. 2005

[8] Hayashi, T.; Tanabe, A.; Andou, D.; Izutsu, K.; Satou, H.; He, H.; Tawbi, W., "IGAP: secure group management protocol for multicast content delivering network," Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings. The 2004 Joint Conference of the 10th Asia-Pacific Conference on , vol.2, no., pp. 626-630 vol.2, 29 Aug.-1 Sept. 2004

[9] 백의현, 박광로, “IPTV 서비스 기술”, IT SoC Magazine

[10] 홍인화, 이석필, “IPTV 기술 동향”, IT Soc Magazine