IPTV 서비스 환경에서 AAA 서버를 이용한 멀티캐스트 그룹키 분배 기술에 관한 연구+

문종식, 이임영
순천향대학교 컴퓨터학부
e-mail:comnik528@sch.ac.kr

A Study on Multicast Group Key Distribution Technology using AAA Server in IPTV Service Environment

Jong-Sik Moon, Im-Yeong Lee
Division of Computer Science and Engineering, Soonchunhyang University

요 약

현대 사회는 IT 기술의 발전과 인터넷 및 디바이스의 발전으로 인해 다양한 기술이 융합된 컨버전스 현상이 급진전되고 있으며, 방송과 통신의 융합 흐름은 더욱 가속화될 전망을 보이고 있으며, 특히 현재 제공되고 있는 IPTV(Internet Protocol Television) 서비스를 통해 빠른 성장세를 보이고 있다. 그러나 이와 같은 IPTV는 기존 IP 네트워크 기반으로 서비스를 제공하고 있으며, 이는 이전의 사이버공격 기술이 그대로 적용될 수 있는 문제점을 내포하고 있다. 따라서 본 연구에서는 IPTV 실시간 방송 서비스 환경에서 AAA 서버를 이용한 멀티캐스트 키 관리 기술을 제안하였다. 멀티캐스트 키 구조는 계층적 트리 방식을 적용하였으며, ID 기반 멀티캐스트 키 관리 기술을 제안하여 안전하고 효율적인 서비스를 제공할 수 있도록 하였다.

1. 서론

최근 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 새로운 문화적 변환기를 맞이하고 있다. 또한 콘텐츠, 네트워크 및 단말 분야에서 디지털 컨버전스 현상이 급진전되어 기존 통신과 방송의 경계가 허물어지고 있다. 이와 같은 변화는 현대 사회에서 디지털화의 가속 및 통신 인프라의 확충 등으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보를 서로 공유할 수 있는 환경이 제공되고 있다. 따라서 방송과 통신의 융합 흐름은 더욱 가속화될 전망을 보이고 있으며, 특히 현재 제공되고 있는 IPTV(Internet Protocol Television) 서비스를 통해 빠른 성장세를 보이고 있다. 현재 IPTV는 ISP(Internet Service Provider) 3사에 의해 VoD(Video on Demand), 실시간 방송 서비스 등 다양한 서비스 및 콘테츠 제공으로 많은 가입자를 유치하고 있다. 그 중 실시간 방송 서비스는 기존의 지상파 방송 뿐만아니라 케이블 방송까지 다양한 채널을 확보하여 경쟁력을 확보해 나가고 있다. 그러나 이와 같은 IPTV는 기존 IP 네트워크 기반으로 서비스를 제공하고 있으며, 이는 이전의 사이버공격 기술이 그대로 적용될 수 있는 문제점을 내포하고 있다. 즉, IP 네트워크를 통해 IPTV를 제공받는데 있어 쿠키에 의한 개인정보 수집, 해킹·악성코드 등 불법적인 개인정보 수집, 바이러스 등에 의한 기술적 개인정보 유출, IP 망을 통한 광고 안내 및 구매 권유 등이 가능하며, 사용자가 리모트 컨트롤을 사용하여 채널을 돌리거나 물건을 구매하는 등의 조작 행위 정보가 제 3자의 해킹에 노출될 우려가 있고, 방송사업자가 아닌 개인도 자체 방송서비스를 제공할 수 있는 환경이 조성됨에 따라 무분별하게 타인의 동의 없이 사생활을 촬영·방송 하는 등 불법제어, 콘텐츠 불법 유통, 서비스 도용, 비인가자 접근 등의 문제점이 발생할 수 있다. 이러한 보안 취약점을 해결하고자 IPTV는 CAS(Conditional Access System) 및 DRM(Digital Right Management)을 적용하고 있으나, IPTV의 실시간 방송 서비스 보안 위협에 대한 보안 기술은 많은 취약점을 내포하고 있다. 또한 IPTV 실시간 방송은 멀티캐스트 전송 방식을 사용하고 있어 멀티캐스트 키 관리 방식에 대한 연구가 필요하다. 따라서 본 연구에서는 IPTV 실시간 방송 서비스 환경에서 AAA 서버를 이용한 멀티캐스트 키 관리 기술을 제안하였다. 멀티캐스트 키 구조는 계층적 트리 방식을 적용하였으며, ID 기반[1] 멀티캐스트 키 관리 기술을 제안하여 안전하고 효율적인 서비스를 제공할 수 있도록 하였다. 본 논문은 구성은 다음과 같다. 2장에서는 보안 요구사항에 대하여 분석하고, 3장에서는 기존 연구에 대하여 분석한다. 4장에서는 AAA 서버를 이용한 멀티캐

+본 연구는 교육과학기술부와 한국산업기술재단의 지역혁신인력양성사업으로 수행된 연구결과임.

스트 키 관리 방식을 제안하고, 5장에서는 제안방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구방향으로 논문을 마치도록 한다.

2. 보안 요구사항

IPTV는 인터넷과 방송이 융합된 신규 서비스로서, 기존의 인터넷과 방송에서 발생하던 보안 위협을 모두 내포하고 있으며, 그 중 멀티캐스트 키 관리 측면에서의 보안 요구 사항은 다음과 같다.

- 기밀성 : 멀티캐스트 키 관리 통신에 사용되는 데이터는 정당한 개체만이 확인할 수 있어야 한다. 기밀성은 정보를 해석할 수 없도록 암호화를 통해서 이루어진다.
- 무결성 : 정보 시스템에 저장되어 있거나 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다. 만약 위조, 삭제 및 변조가 되었다면 그 사실을 확인할 수 있어야 한다. 전송된 데이터의 무단 변경을 감지할 수 있게 하기 위해 전자 서명 등을 이용한다.
- 인증 : 정당한 사용자만이 멀티캐스트 키를 분배 받을 수 있어야 한다. 그 실체의 신분이 거짓이 아닌 정당한 사용자라는 것을 검증할 수 있어야 한다.
- 접근제어 : 정보 자원에 대한 읽기나 변경 등의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.

3. 기존 연구

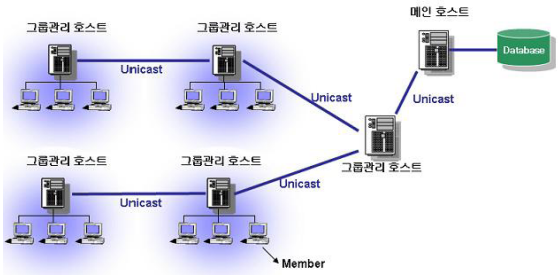
기존에 연구된 멀티캐스트 키 관리 기술에 관한 연구는 다음과 같다.

3.1 안전한 멀티캐스트 전송을 위한 효율적인 그룹 관리 방법

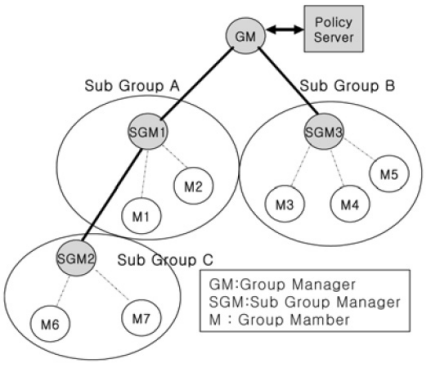
많은 중요한 정보들이 인터넷을 통해 전송 되고 있으나, 이들은 정보는 수많은 위험에 노출되어 있다. 그리고 멀티캐스트 서비스도 다양해지고 보편화 되고 있는 만큼 서비스의 종류도 다양해지고 있다. 그룹에 새로운 멤버가 가입하거나 탈퇴하는 경우 기존 멤버들이 사용하던 그룹키는 갱신되어야 한다. 그러나 기존의 방법은 키 교환 때문에 성능이 저하되는 문제가 있다. 본 논문에서는 안전한 멀티캐스트 데이타 전달을 위해서 가입과 탈퇴가 빈번한 멀티캐스트 그룹에 대해서 안전한 데이타 전달을 위한 효율적인 그룹 관리 기법을 제안하였다[4]. 그러나 그룹 가입을 위한 키 획득 단계에서 중간자공격이 가능하며, 전송되는 메시지가 수정가능하고 전방향 및 후방향 안전성을 제공하지 못한다.

3.2 유·무선 서비스를 위한 적응적 그룹키 관리 기법

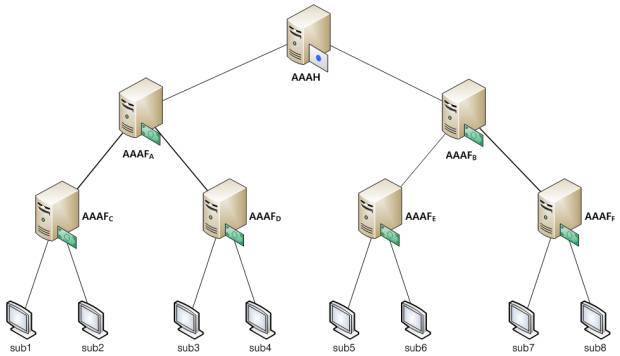
본 논문은 오버레이 멀티캐스트 기반에서 유무선 서비스를 위한 적응적 키관리 기법을 제안하였다. IP 멀티캐스트의 라우터 기능을 어플리케이션에서 처리하고, 적응적인 그룹관리를 위해서 유니캐스트와 멀티캐스트의 두 가지 통신기법으로 그룹키를 분배한다. 또한, 안전한 그룹키 관리를 위해 멤버의 그룹 가입과 탈퇴시에 키의 갱신을 수행하며, 주기적인 메시지 교환으로 멤버의 상태를 체크하여 비정상적인 그룹탈퇴의 경우에는 동적인 키의 갱신을 통하여 전방향 안전성과 후방향 안전성의 보안적 요구사항을 충족시킨다. 구룹키는 갱신된 키의 분배를 우선적으로 하였으며, 대칭키를 이용한 암호화 기법과 이전의 그룹키를 사용하는 두 가지의 기법을 적응적으로 사용하는 기법에 대해서 제안하였다[5]. 그러나 탈퇴한 멤버는 키를 가지고 탈퇴할 수 없다고 가정하였으나, 이는 전방향 안전성을 만족하기 위한 절대적 가정사항 이라는 문제점이 있다. 따라서 전방향 안전성에 취약하다.



(그림 1) 멀티캐스트 전송을 위한 효율적인 그룹관리 방법 네트워크 구조도



(그림 2) 적응적 그룹키 관리 기법 계층적 그룹 구조



(그림 3) 제안방식 키 관리 구조도

4. 트리형식의 ID 기반 멀티캐스트 그룹키 분배 방식

본 연구에서 제안한 트리형식의 ID 기반 멀티캐스트 그룹키 분배 방식(TMGD : Tree Multicast Group key Distribution)는 IPTV 실시간 방송에서 데이터 및 방송을 위한 그룹키를 분배 받는데 있어 안전하고 효율적으로 키를 분배할 수 있는 기술을 제안하였다. TMGD는 멤버의 가입 및 탈퇴에 관한 사항은 고려하지 않았으며, 현재의 IPTV 서비스 환경 상 연산량을 고려하지 않았다. 따라서 ID 기반 공개키 방식을 사용하여 그룹키를 분배하는 방식을 제안하였다.

4.1 시스템 계수

본 제안 방식에서 사용하는 시스템 파라미터는 다음과 같다.

- * : 개체($AAAH$: 홈 인증서버, $AAAF$: 지역 인증서버, SUB_i : i번째 가입자($i=1,2,...,n$))
- ID_* : 개체의 아이디
- SV_{GK} : 가입 시 전달받는 비밀 값
- x, y : 그룹키 생성 값
- e : $G_1 \times G_2 \rightarrow G_2$ 겹선형 사상
- KU_*/KR_* : ID기반 공개키/개인키 쌍
- KGK : 데이터 암호화를 위한 메인 그룹 키
- cw : 스크램블 데이터 복호화 키
- $E_*[\ ]$: *의 키로 암호화

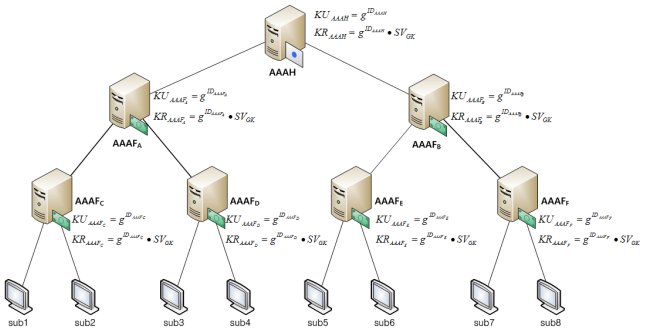
4.2 TMGD 프로토콜

TGMD 프로토콜은 IPTV 서비스 상에서 멀티캐스트 구룹키 분배에 관하여 제안을 하였으며, 각 개체가 보유하고 있는 비밀 값은 가입 시 안전하게 분배 되었다고 가정한다. 또한 지역 인증서버와 홈 인증 서버 간에는 안전하게 분배되었다고 가정한다. 프로토콜의 설명은 트리에서 동일한 차수에 있는 경우($AAAF_A$, $AAAF_B$)는 좌측 노드와의 통신만 설명한다. 이는 부모 노드에서 자식노드에게 보내는 메시지는 동일하기 때문이다. 다만 암호화되는 메시지 및 그룹키 생성을 위한 값에서 각 노드의 아이디만 변경된다.

Phase 1. ID 기반 공개키 생성 단계

step 1. 각 개체는 자신의 아이디와 가입시 전달받은 비밀 값을 통해 ID 기반 공개키/개인키 쌍을 생성한다.

$$AAAH: KU_{AAAH} = g^{ID_{AAAH}},\ KR_{AAAH} = g^{ID_{AAAH}} \bullet SV_{GK}$$
$$AAAF_i: KU_{AAAF_i} = g^{ID_{AAAF_i}},\ KR_{AAAF_i} = g^{ID_{AAAF_i}} \bullet SV_{GK}$$
$$SUB_i: KU_{SUB_i} = g^{ID_{SUB_i}},\ KR_{SUB_i} = g^{ID_{SUB_i}} \bullet SV_{GK}$$



(그림 4) 공개키 생성 흐름도

Phase 2. 그룹키 분배 단계

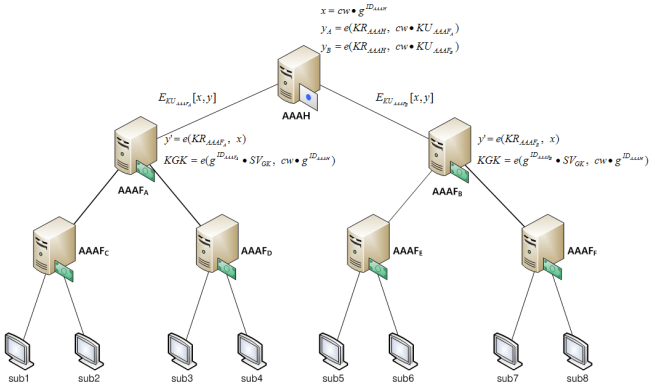
step 2. 홈 인증서버는 그룹키 생성을 위한 값을 다음과 같이 생성하고 자신의 자식노드($AAAF_A$, $AAAF_B$)의 공개키로 암호화하여 전송한다.

$$x = cw \bullet g^{ID_{AAAH}}$$
$$y = e(KR_{AAAH}, cw \bullet KU_{AAAF_A})$$
$$E_{KU_{AAAF_A}}[x,y]$$

step 3. 지역 인증서버($AAAF_A$, $AAAF_B$)는 메시지를 복호화 한 후, 다음과 같이 전송된 x값으로 y'를 생성하고 값을 검증하고 그룹키를 생성한다. 이후 다시 자신의 자식노드($AAAF_C$, $AAAF_D$, $AAAF_E$, $AAAF_F$)에게 그룹키 생성을 위한 값을 암호화하여 전송한다.

$$y' = e(KR_{AAAF_A}, x)$$
$$KGK = e(g^{ID_{AAAF_A}} \bullet SV_{GK},\ cw \bullet g^{ID_{AAAH}})$$
$$E_{KU_{AAAF_C}}[x,y]$$

step 4. 최하단의 지역 인증서버는($AAAF_C$, $AAAF_D$, $AAAF_E$, $AAAF_F$) 위와 같이 동일한 방법으로 값을 검증하고 메인 그룹키를 생성한 다음, 자신에게 속해있는 가입자들에게 값을 전송한다. 이후 가입자는 그룹키 생성이 완료되었으면, 이를 가지고 메시지를 암호화하거나 복호화할 수 있다.



(그림 5) 그룹키 분배 단계 흐름도

5. 제안 방식 분석

제안 방식을 2장에서 도출한 보안 요구사항에 맞추어 분석하면 다음과 같으며, 기존 방식과의 비교 분석은 <표 1>과 같다. 그룹키를 생성하기 위해 전송되는 메시지는 ID 기반 공개키로 암호화되며, 그룹키는 전송되는 것이 아니라 각 개체가 보유한 비밀 값과 전송된 값을 연산하여 생성하므로 그룹키에 대한 기밀성이 보장된다. 또한 전송되는 메시지의 위조 및 변조에 대하여 검증할 수 있다. 그리고 인증 받은 개체만이 멀티캐스트 그룹키를 생성할 수 있으며, 이후의 통신에서 그룹키를 사용하여 인증을 제공받을 수 있다. 정당하지 않은 개체는 그룹키 자체를 생성할 수 없으며, 서비스를 제공받을 수 없다.

3.1 방식은 그룹 가입을 위한 키 획득 단계 및 전송되는 메시지를 수정할 수 있기 때문에 기밀성, 무결성, 접근제어 등을 제공할 수 없으며, 중간자공격으로부터 안전하지 않다. 3.2 방식은 안전성 및 효율성을 제공하기 위해 가정사항이 너무 많아 이를 검증할 수 없다.

<표 1> 제안 방식 분석표

	3.1	3.2	TMGD
기밀성	공개키와 대칭키 방식을 혼용하여 사용하나 안전성을 제공하지 못함	대칭키 방식을 사용하여 기밀성 제공	ID 기반 공개키 방식을 사용하며, 그룹키는 각 개체가 사전 공유 값 및 전송 값을 통해 생성
무결성	전송되는 메시지 자체가 수정 가능	안전하다고 가정	전송되는 메시지에 대하여 검증 가능
인증	제공	제공	제공
접근제어	메시지 자체를 수정할 수 있기 때문에 정당하지 않은 사용자도 위장하여 접근할 수 있음	정당하지 않은 사용자는 그룹키를 생성할 수 없으며 서비스에 접근할 수 없음	정당하지 않은 사용자는 그룹키를 생성할 수 없으며 서비스에 접근할 수 없음

6. 결론

네트워크 및 컴퓨터 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보를 서로 공유할 수 있는 환경이 제공되고 있다. 따라서 방송과 통신의 융합 흐름은 더욱 가속화될 전망을 보이고 있으며, 특히 현재 제공되고 있는 IPTV서비스를 통해 빠른 성장세를 보이고 있다. 그러나 이와 같은 IPTV는 기존 IP 네트워크 기반으로 서비스를 제공하고 있으며, 이는 이전의 사이버공격 기술이 그대로 적용될 수 있는 문제점을 내포하고 있다. 따라서 본 연구에는 트리형식의 ID 기반 멀티캐스트 그룹키 분배 방식(TMGD : Tree Multicast Group key Distribution)는 IPTV 실시간 방송에서 데이터 및 방송을 위한 그룹키를 분배 받는데 있어 안전하고 효율적으로 키를 분배할 수 있는 기술을 제안하였다. 향후 멀티캐스트 그룹키 관리를 위해 멤버의 가입 및 탈퇴에 대한 연구와 전방향 안전성 및 후방향 안전성을 제공할 수 있는 기술에 관한 연구가 필요할 것으로 사료된다.

참고문헌

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," CRYPTO'84, pp.47-53, 1984.

[2] K. Koyama and K. Ohta, "Identity-based conference key distribution systems," Proceedings of Crypto '87, lecture Notes in omputer Science no. 293, Springer-Verlag, 1988, pp.175-184.

[3] Y. Yacobi, "Attack on the Koyama-Ohta Identity-based key distribution systems," Proceedings of Cryto'87, Lecture Notes in Computer Science no. 293, Springer-Verlag, 1988, pp.429-433.

[4] 고훈, 장의진, 김선호, 신용태, "안전한 멀티캐스트 전송을 위한 효율적인 그룹 관리 방법," 정보과학회논문지 제 33권 제 1호, pp.9~15, 2006

[5] 이광겸, 박상진, 김대원, 김경민, 신용태, "오버레이 멀티캐스트 기반에서 유·무선 서비스를 위한 적응적 그룹키 관리 기법," 정보과학회 추계학술발표회 논문집 Vol.32, No.2. pp.103~105, 2005.