Mobile IPTV 환경에서 빠른 로밍 서비스를 위한 키 확립 프로토콜+

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

Key Establishment Protocol for Fast Roaming Service in Mobile IPTV Environment

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

요 약

최근 디지털화의 가속 및 통신 인프라의 확충 등으로 인해 IP 네트워크로 연결되어 영상 및 음성 정보를 서로 공유할 수 있는 환경이 제공되고 통합 서비스에 대한 수요가 증가하면서 Mobile IPTV 서비스가 새로운 서비스 모델로 각광받고 있다. 그러나 IPTV에서 발생하는 보안위협 외에 무선 네트워크에서 발생할 수 있는 보안위협을 안고 있다. 또한 Mobile IPTV의 특성상 이동이 잦아 기존의 보안 기술로는 QoS 및 QoE를 제공하기에는 어려운 실정이다. 따라서 본 논문에서는 Mobile IPTV 환경에서 빠른 로밍 서비스를 위한 키 관리 프로토콜을 제안하여 안전성 및 효율성을 제공하고자 한다.

1. 서론

방송과 통신의 융합 흐름은 더욱 가속화 전망을 보이고 있으며, 특히 광대역 통합망 환경이 구축되면서 IPTV는 빠른 성장세를 보이고 있다. 그러나 콘텐츠 및 서비스 모델의 차별화를 가져오지 못하면서 예상보다 저조한 가입자 유치와 수익성을 나타내고 있다. 따라서 세계시장 선점 및 원천기술 확보를 위해 새로운 서비스 모델 개발에 박차를 가하면서 Mobile IPTV가 새로운 서비스 모델로 각광을 받고 있다. Mobile IPTV는 무선 구간에서 이동성을 지원하여 언제 어디서나 자유롭게 IPTV서비스를 이용하도록 하는 서비스이다[1][2]. Mobile IPTV는 무선 네트워크를 이용하여 서비스를 제공함에 따라 기존의 IPTV에서 나타난 보안위협 외에 무선 네트워크상에서 일어날 수 있는 보안 위협이 추가적으로 발생할 위협이 높다. 따라서 본 논문에서는 차세대 Mobile IPTV 환경에서 빠른 로밍을 제공하면서도 안전성 및 효율성을 제공하고자 키 관리 프로토콜에 관한 연구를 진행하였다. 본 논문의 구성은 다음과 같다. 2장에서는 요구사항에 대하여 분석하고, 3장에서는 기존 방식에 대하여 분석한다. 4장에서는 제안방식을 기술하고 5장에서는 제안방식을 분석한다. 마지막으로 6장에서는 결론 및 향후 연구방향으로 논문을 마치도록 한다.

2. 요구사항

Mobile IPTV 에서는 다음과 같은 요구사항을 고려해야 한다.

- 기밀성 : Mobile IPTV 상에서 전송되는 데이터는 정당한 사용자와 인증서버만이 확인할 수 있어야 한다.
- 무결성 : 무선 네트워크를 통해 전송되는 데이터가 위/변조 되거나 파괴되지 않도록 해야 한다.
- 인증 : Mobile IPTV 서비스를 제공받고자 접근하는 디바이스가 전송한 정보 및 데이터의 출처가 확인되고 정당한 디바이스라는 것을 검증할 수 있어야 한다.
- 접근제어 : Mobile IPTV 서비스에 정당한 접근을 제외한 모든 불법적인 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.
- 빠른 로밍 인증: 로밍 시 끊김 없는 서비스를 제공하기 위해서는 인증 소요시간이 짧으며, 경량화된 인증에 대한 고려가 필요하다.

3. 로밍 확장성을 높인 인증 방식

본 방식은 빠른 로밍을 지원하기 위한 확장성 높은 인증 프레임워크에 관한 것으로, 직/간접적으로 구성된 도메인간의 일반적인 신뢰 관계를 바탕으로 계층적 캐싱을 구성한다. 계층적 인증 캐싱을 이용할 경우 확장성을 보장함은 물론 인증 지연 및 인증으로 인한 망의 오버헤드를 줄일 수 있으며, 일반적인 신뢰 관계를 갖는 도메인 간의 부드러운 로밍을 지원할 수 있는 확장 가능한 인증 체계를 제공한다[3]. 그러나 초기 로밍을 위한 인증단계 및 캐싱 에이전트 후보 등록으로 인한 지연이 발생한다는 문제점이 존재한다.

+ 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구결과임.

4. 제안방식

본 연구에서 제안한 빠른 로밍 서비스를 위한 키 관리 (FRKM: Fast Roaming Key Management) 프로토콜은 Mobile IPTV 환경에서 홈 네트워크에서 외부 네트워크로 이동 시 빠른 로밍 서비스를 제공할 수 있도록 안전하고 효율적인 키 관리 프로토콜이다.

4.1 시스템 계수

본 프로토콜에서 사용하는 프로토콜은 다음과 같다.

- $*$: 각각의 개체($AAAH$: 홈 인증서버, $AAAF$: 지역 인증서버, SU_i : i번째 가입자($i=1,2,...,n(0<n\in Z)$))
- ID_* : 개체의 아이디
- KID_* : 키 확립을 위한 가입자의 아이디
- skv : 키 확립을 위한 비밀 값
- x, y : 마스터 키 생성을 위한 값
- α, β : 지역키 생성을 위한 값
- e : $G_1 \times G_2 \rightarrow G_2$ 겹선형 사상
- KU_*/KR_* : ID기반 공개키/개인키 쌍
- MK : 마스터키, LK : 지역키
- cw : 스크램블 데이터 복호화 키
- $E_*[\ ]$: $*$의 키로 암호화

4.2 FRKM 프로토콜

빠른 로밍 서비스를 위한 키 관리 프로토콜은 마스터 키생성을 위한 단계, 지역키 생성을 위한 단계와 로밍 단계로 이루어지며, 키 확립을 위한 비밀 값은 가입자 등록 시 분배되었다고 가정한다.

4.2.1 마스터키 생성

홈 인증서버, 지역 인증서버, 가입자는 각각 ID기반 공개키/개인키 쌍을 생성한다. 홈 인증서버는 마스터키를 생성하고 가입자에게 마스터키를 생성할 수 있는 값을 전송한다. 가입자는 전송받은 값을 기반으로 마스터키를 생성한다.

$$AAAH: KU_{AAAH} = g^{ID_{AAAH}},\ KR_{AAAH} = g^{ID_{AAAH}} \cdot svk$$
$$AAAF: KU_{AAAF} = g^{ID_{AAAF}},\ KR_{AAAF} = g^{ID_{AAAF}} \cdot svk$$
$$SU_i: KU_{SU_i} = g^{ID_{SU_i}},\ KR_{SU_i} = g^{ID_{SU_i}} \cdot svk$$

$$AAAH: x = g^{ID_{AAAH}} \cdot cw,\ \ y = e(KR_{AAAH}, KU_{SU_i} \cdot cw)$$
$$AAAH: MK = e(g^{ID_{AAAH}} \cdot svk, g^{ID_{SU_i}} \cdot cw)$$
$$AAAH \rightarrow SU_i: E_{KU_{SU_i}}[x,y]$$

$$SU_i: y' = e(KR_{SU_i}, x),\ y` \stackrel{?}{=} y$$
$$SU_i: MK = e(g^{ID_{SU_i}} \cdot svk, g^{ID_{AAAH}} \cdot cw)$$

4.2.2 지역키 생성

지역 인증서버는 로컬키를 생성하고 가입자에게 로컬키를 생성할 수 있는 값을 전송한다. 가입자는 전송된 값을 기반으로 로컬키를 생성한다..

$$AAAF: \alpha = g^{ID_{AAAF}} \cdot cw,\ \ \beta = e(KR_{AAAF}, cw \cdot g^{ID_{SU_i}})$$
$$AAAF \rightarrow SU_i: E_{SU_i}[\alpha,\beta]$$

$$SU_i: \beta' = e(KR_{SU_i}, \alpha),\ \beta` \stackrel{?}{=} \beta$$
$$SU_i: LK = e(g^{ID_{SU_i}} \cdot svk, g^{ID_{AAAF}} \cdot cw)$$

4.2.3 확립키를 이용한 로밍

가입자가 지역내 로밍시 지역키를 기반으로 인증을 제공받을 수 있으며, 홈 인증서버의 개입없이 지역인증서버가 가입자를 인증하기 때문에 빠른 로밍 서비스를 제공할 수 있다. 기존의 지역외 로밍은 지역 인증서버간 가입자의 정보를 공유하여 인증함으로써 제공하였으나 이는 가입자의 개인정보 노출 및 지역 인증서버간 통신로 확보에 대한 비용문제를 초래할 수 있다. 따라서 지역외 로밍시 홈 인증서버가 개입하여 마스터키를 기반으로 인증하여 지역 인증서버간 정보 공유 및 통신확보를 제외하여 안전성 및 효율성을 극대화 할 수 있다.

5. 제안 방식 분석

제안방식은 기밀성을 제공하기 위해 ID기반 공개키/개인키 쌍을 이용하여 통신상의 데이터를 암호화하여, 겹선형 사상기반 인증 프로토콜로 인증 및 무결성을 제공할 수 있다. 또한 정당하게 인증을 받지 않은 사용자는 서비스 및 키 확립에 참여할 수 없으며, 빠른 로밍 인증을 위해 개체간 각각 공유키를 설정하여 로밍 시 인증을 위한 키로 사용한다. 그러나 개체간 공유키 개수 증가로 인한 연산량이 증가하는 문제점이 있으나, 겹선형 사상을 기반으로 하여 연산량을 최대한 줄일 수 있도록 하였다.

6. 결론

제안방식은 Mobile IPTV 환경에서 빠른 로밍을 위한 키 확립 프로토콜을 제안하여 안전성과 효율성을 제공할 수 있도록 하였다. 로컬키는 지역내 이동시 로밍을 위한 키로 사용되며, 마스터키는 지역외 이동시 로밍을 위한 키로 사용한다. Mobile IPTV 환경에서 로밍은 빈번하게 일어나지만 지역내 로밍은 복잡한 인증과정을 거치지 않고 설립한 키를 통해 이루어지며, 지역외 로밍은 지역 인증서버간 정보를 공유하는 것 보다 홈 인증서버의 개입을 통해 인증을 제공하는 것이 네트워크의 효율성 및 비용절감 효과를 가져 올 수 있다. 향후 지역외 로밍 및 Mobile IPTV 서비스 환경에서 실시간 방송 서비스를 위한 멀티캐스트 키 관리에 관한 연구가 필요할 것으로 사료된다.

참고문헌

[1] 박수홍, “Mobile IPTV 기술 및 국내외 표준화 동향, HN FOCUS, Vol. 20, pp. 48-54, 2008

[2] 이상화, “최근 모바일 IPTV 동향,” IITA 주간기술동향, 통권 1327호, pp. 15-25, 2007.

[3] 이희진, 송유경, 이명수, 김종권, "계층적 캐싱을 이용해 로밍 확장성을 높인 인증 프레임워크," 정보과학회논문지, 제 32권 5호, pp.561-573, 2005.