모바일 IPTV의 이동성에 대한 침해 분석 및 대응방안

Analysis of Mobility and Security Requirements for Mobile IPTV

이선영
순천향대학교 정보보호학과

Sun-Young Lee(sunlee@sch.ac.kr)

요약

이동 중에 모바일 단말기를 통하여 IPTV 서비스를 제공하는 와이브로 모바일 IPTV에서 이동성(mobility)은 매우 중요한 요소이면서 보안에 있어서는 취약한 면을 가지고 있는 요소이다. 본 논문에서는 와이브로 모바일 IPTV의 안전한 서비스를 위하여 핸드오버 이외에 제한수신 시스템도 내부에 이동성을 보장하는 기술을 포함하고 있어야 함을 나타내었다. 모바일 IPTV 서비스 이용 중에 발생할 수 있는 보안 위협을 다운로드형 제한수신 시스템(DCAS)을 중심으로 분석하고, 이에 대한 대응 방법으로서 DCAS 호스트에 사용자 디바이스의 주소를 알리는 방법을 제안하였다. 제안 방법을 적용했을 때 사용자 인증 횟수가 감소하여 효율성이 향상됨을 보였다. 또, 한국정보통신기술협회에서 요구하고 있는 보안 요구 사항과의 비교를 통하여 제안 방법을 적용할 때 모바일 IPTV의 이동성이 보장될 수 있음을 보였다.

■ 중심어 : | 모바일 IPTV | 이동성 | 제한수신 시스템 | 보안 요구 사항 |

Abstract

The mobility is one of the most important factor for mobile IPTV. However, mobility is highly vulnerable to eavesdropping and unauthorized access. Generally mobility of mobile services is based on handover techniques. But we showed that mobile IPTV must use other techniques to confirm mobility. In this paper, we analyzed security of wibro mobile IPTV from the viewpoint of mobility. We considered DCAS host must include new addresses of mobile devices. We analyzed total number of authentication for the proposed method. So we showed that proposed method was more efficient than wibro-mobile IPTV. We compared the security of our proposal to the security requirements of TTA.

■ keyword : | Mobile IPTV | Mobility | DCAS | Security Requirements |

I. 서 론

방송과 통신의 융합 서비스로서 주목 받고 있는 IPTV는 단방향 서비스만을 제공하는 기존의 방송과는 달리 통신의 양방향성을 방송에 결합함으로써 다양한 서비스를 제공할 수 있다[1]. 최근 IPTV의 상용화가 활발하게 진행되고 있는 가운데, IPTV에 대한 기술 연구 및 표준화 활동이 국내외적으로 활발하게 이루어지고 있는 상황이다[2][3]. 이동 중에도 이동 단말기를 통하여 IPTV 서비스를 제공할 수 있는 모바일 IPTV에 대한 요구가 증가할 것으로 예상됨에 따라 현재 다양한 표준화 기구에서 모바일 IPTV에 대한 기술 개발 및 표

접수번호 : #100330-002
접수일자 : 2010년 03월 30일
심사완료일 : 2010년 5월 19일
교신저자 : 이선영, e-mail : sunlee@sch.ac.kr

준화 활동이 진행 중에 있다[4][5].

단말의 성능이 떨어지는 모바일 IPTV에서의 기술 개발은 IPTV와는 다른 환경을 고려하여 단말기의 성능 및 통신 대역의 차이를 극복하고 사용자 요구를 충족시킬 수 있는 기술이 개발되어야 한다. 모바일 IPTV는 고정형 IPTV에 비하여 침해 위협이 많을 것으로 생각되고 있으나, 구체적인 침해에 대한 예상 시나리오 및 분석은 이루어지고 있지 않으며 현재 구현 중인 모바일 IPTV에 대한 보안 요구사항에 대한 분석도 이루어지고 있지 않다. 모바일 IPTV에 대한 보안 요구사항은 한국정보통신기술협회(TTA)에서 지정되어 있으나[6], 현재 구현 중인 모바일 IPTV가 이 요구 사항에 대하여 어느 정도 부합하고 있는지에 대한 분석 및 연구도 정확하게 이루어지고 있지 않다. 또, 현재 모바일 IPTV 보안과 관련하여 다운로드형 제한수신 시스템이 주목받고 있으나, 제한수신 시스템의 개발에 초점이 맞추어져 있어 이동성에 대한 내용을 다루고 있지 않다.

본 논문에서는 현재 와이브로를 이용하여 구현되고 있는 모바일 IPTV에 대한 침해 위협을 분석하고, 위협에 대한 대응 방법으로서 모바일 IPTV의 이동성 기술과는 별도로 서비스 보안 기술 내부에서 이동성을 포함하는 방법을 제안 한다. 사용자 인증 횟수를 비교하여 제안 방법의 효율성을 평가한다. 또, 와이브로 모바일 IPTV의 기술이 TTA의 보안 요구 사항에 부합하는 정도를 분석한다.

본 논문은 2장에서 모바일 IPTV의 개요, 3장 이동성과 관련된 보안 위협, 4장 이동성 문제에 대한 대응 방법 제안, 5장 결론으로 구성된다.

II. 모바일 IPTV

모바일 IPTV란 IPTV의 장점과 모바일 TV의 장점을 함께 제공할 수 있는 서비스로서, 무선 구간에서 언제 어디서나 IPTV 서비스를 이용할 수 있는 서비스를 말한다. 본 논문에서 대상으로 하고 있는 와이브로 모바일 IPTV의 모델을 [그림 1]에 나타내었다[7]. 모바일 IPTV의 보안 요구사항은 서비스 보안, 콘텐츠 보안, 단말 보안, 가입자 보안 영역으로 구분할 수 있다. TTA의 표준 문서에서 이들 보안 요구 사항을 ITU-T에서 규정하고 있는 보안 요구 사항들을 수용하면서 기술하고 있다[6]. 모바일 IPTV의 보안 요구 사항 중 사용자에게 콘텐츠를 안전하게 전달하기 위한 서비스 보안 기술로서 제한수신 시스템(CAS)과 수신된 콘텐츠의 관리를 위한 콘텐츠 보안 기술인 DRM, 모바일 IPTV에서 가장 핵심이 되는 이동성(Mobility)과 관련된 보안 기술이 있다.

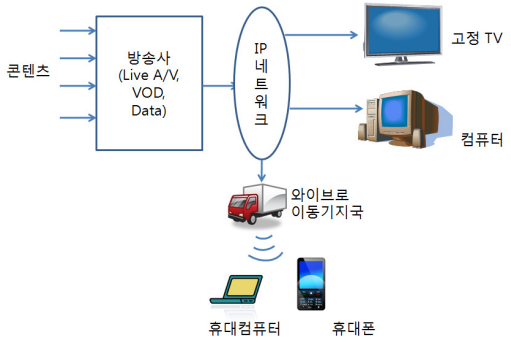

그림 1. 와이브로를 이용한 모바일 IPTV의 구성도[7]

1. 제한수신 시스템(Conditional Access System: CAS)과 DRM(Digital Right Management)

제한수신 시스템은 암호화된 방송 콘텐츠를 유선이나 위성, 인터넷을 통하여 수신자에게 보내고, 시청료를 지불한 수신자에게만 암호를 복호할 수 있는 권한을 부여함으로써 유료 서비스를 가능하게 한다. 제한수신 시스템 주요 기능은 스크램블링/디스크램블링(srcambling /descrambling) 기능, 자격제어(Entitlement Control) 기능, 자격관리(Entitlement Management) 기능으로 나눌 수 있다[8-10].

제한수신 시스템 중 모바일 IPTV에 적용하기 적합한 기술로서 다운로드형 제한수신 시스템(Downloadable CAS; DCAS)이 있다[11-14]. DCAS는 셋탑 박스에 제한수신 모듈(CAS)이 미리 설치되어 있는 것이 아니라 방송수신을 제어하는 기능을 다운로드 가능한 형태로

구현하는 것을 말하며, 소프트웨어로만 구현될 수 있으므로 모바일 IPTV에 적합하다. [그림 3]은 DCAS 구성도이다.

DRM은 사용자에게 부여된 권한에 따라 디지털 콘텐츠의 사용 권한을 지속적으로 통제하는 방식으로서 저작권 보호 기술 및 암호 알고리즘을 이용한 콘텐츠의 배포 관리, 워터 마킹 기술을 이용한 콘텐츠 관리 기술까지 포함하여 다루고 있다. 미리 DRM을 적용한 후 콘텐츠를 유통해야 하기 때문에 실시간으로 콘텐츠가 제공되는 방송 서비스에는 적합하지 않은 부분이 있으나, 주문형 방송에서 활용할 수 있다.

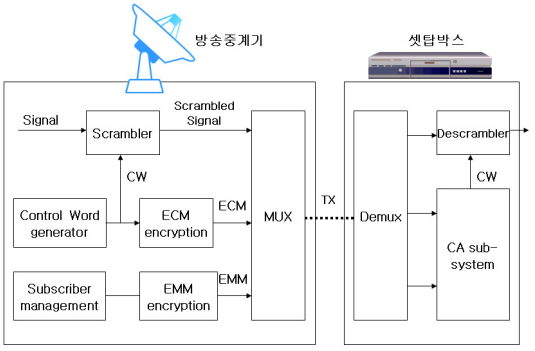

그림 2. 제한수신 시스템의 모델

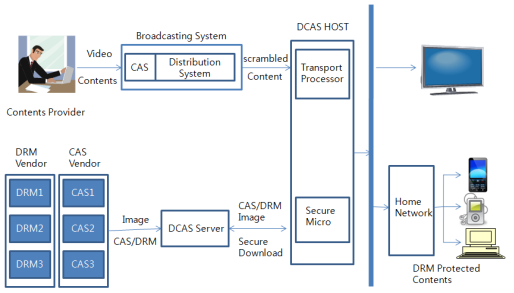

그림 3. DCAS 구성도

2. 이동성(Mobility)

무선망과 인터넷이 통합되어 언제 어디서나 자유로이 인터넷을 이용할 수 있는 네트워크 환경이 기대되는 와이브로 표준은 시속 60Km 이하의 이동성을 지원하며 실내외에서 끊김없이 무선 인터넷 서비스를 제공할 수 있도록 설계되어 있다[15]. 와이브로에서 이동시 네트워크 서브넷이 다른 새로운 제어국(ACR, Access Control Router)으로 단말이 이동하면 현재 통신 중인 세션(Session)을 유지하기 위하여 IP 계층의 이동성 지원 프로토콜을 수행해야 한다. IETF의 NetLMM (Netwrok-based Localized mobility Management) WG에서 표준화를 시작한 프록시 이동 IPv6(Proxy Mobile IPv6: PMIPv6)[16] 기술은 IPv6 이동성을 위하여 단말에 어떠한 수정도 가하지 않고 네트워크에 위치한 라우터들이 단말 대신 IPv6 이동성을 관리해 주는 프로토콜이다. IPv6를 탑재한 단말이 와이브로 망에서 서브넷이 다른 지역으로 이동할 때 핸드오버 지연 시간을 최소화하기 위한 핸드오버 메커니즘이 많이 제안되어 있다[17-19]. [그림 4]는 PMIPv6의 초기등록 절차 및 핸드오버 절차를 나타낸다. 이 핸드오버 절차에 의하여 인증 받지 못한 이용자가 무단으로 와이브로를 이용하기는 어렵다.

III. 이동성과 관련된 보안 위협

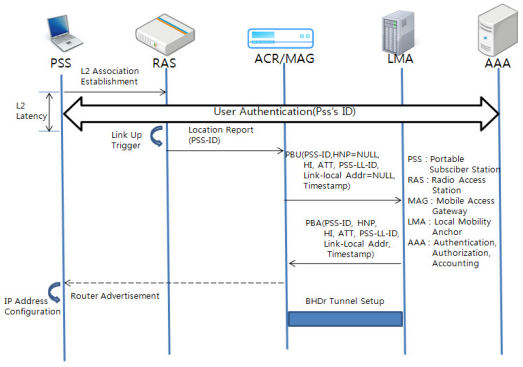

그림 4. 와이브로에서 PMIPv6의 핸드오버 절차

모바일 IPTV 서비스에 대한 보안 위협으로서는 와이브로에 대한 공격과 제한수신 시스템 및 DRM에 대한 공격이 있다. 본 논문에서는 와이브로 가입자이지만 모바일 IPTV 서비스 비가입자에 의한 침해를 중심으로 다룬다. 고정형 IPTV 및 케이블 방송에서는 제한수신 시스템이 카드 형태의 보안 매체 내에 존재하므로 외부

의 공격으로부터 안전하다. 그러나, 모바일 IPTV에서는 이동성을 위한 핸드오버 및 이에 따른 지연 시간에 의해 서비스, 콘텐츠 및 보안 모듈이 공격 받을 가능성이 있다. 따라서, 본 논문에서는 모바일 IPTV에 대한 다양한 위협들 중에서 IPTV 서비스가 진행 중에 이용자 단말이 이동하여 다른 네트워크에 접속되는 핸드오버가 일어나는 경우의 침해 위협에 대하여 다룬다.

1. 와이브로 모바일 IPTV 모델

본 논문의 모바일 IPTV는 [그림 1]의 와이브로 모바일 IPTV 모델을 따르고, 이동성 지원을 위하여 TTA에서 표준으로 제정된 와이브로에서의 프록시 모바일 IPv6[13]를 채용하여 그 핸드오버 절차를 따르고 있다고 가정한다. 또, 안전한 와이브로 서비스를 위하여 EAP-TLS 기반의 와이브로 상호 인증 방법을 적용하고[20], 제한수신 시스템으로서 소프트웨어로만 구현되는 DCAS를 이용한다고 가정한다.

2 제한수신 시스템의 이동성 문제

2.1 제어 워드(CW)의 전송 문제

모바일 기기가 다른 네트워크로 이동하면 와이브로 핸드오버에 의해 새로운 IP 주소를 할당받게 된다. 이에 따라 데이터들도 해당 IP 주소로 전송되게 되는데 데이터와 함께 제한수신 시스템과 관련된 제어 워드도 새로운 주소로 전송되어야 한다. 제한수신 시스템은 모바일 기기로 주기적으로 제어워드(CW)를 전송하게 되는데 제한수신 시스템에 모바일 기기의 IP 주소에 대한 정보가 없으면 제어 워드를 올바른 주소로 전송할 수 없고, 제어 워드가 없으면 스크램블링된 방송 데이터를 디스크램블링 할 수 없다. 디스크램블링되지 않으면 서비스 가입자는 방송을 재생하여 볼 수 없으므로, 방송 서비스가 제대로 이루어지지 않는다. 따라서, 모바일 기기에 새 IP주소가 할당되면 이 주소를 제한수신 호스트에도 알려야 할 필요가 있다..

2.2 제한수신 모듈의 다운로드 문제

다운로드형 제한수신 시스템은 보안 위협이 더욱 심각할 수 있다. 제한수신 모듈 및 키 관리, 사용자 인증을 소프트웨어로 구현하는 DCAS을 이용할 경우 발생할 수 있는 문제를 [그림 5]에 나타내었다. 제한수신 호스트가 이용자의 IP주소를 보관하고 있을 경우에도 DCAS를 사용할 경우 악의적인 사용자가 와이브로의 핸드오버 지연 시간 동안에 직전의 IP 주소를 입수하여 DCAS 호스트에 제한수신 모듈의 다운로드를 요청할 수 있다. 이 시점은 핸드오버가 발생하기 전에 모바일 기기에 대한 디바이스 인증 및 모바일 IPTV 서비스에 대한 사용자 인증이 모두 끝난 상태이므로 부가적인 인증 없이 공격자의 기기에 제한수신 모듈이 다운로드 되고, 콘텐츠가 전송되며, 제어 워드가 전송된다. 또 악의적인 사용자가 서비스 키의 재전송을 요청하면 DCAS 호스트는 서비스 키를 전송하게 되고, 이후 악의적인 사용자는 핸드오버가 종료되어 정당한 사용자의 새로운 IP주소가 DCAS 호스트에 전해질 때까지 제한수신 콘텐츠를 이용할 수 있다. [그림 5]의 (6)번 절차 이후에 정당한 사용자는 변경된 CAS 모듈과 서비스 키를 가지고 있지 않으므로 콘텐츠를 이용할 수 없고, 다시 인증 절차를 수행해야 하며, 이는 서비스 이용의 단절을 가져오므로 이용자 편의성을 도모할 수 없게 된다.

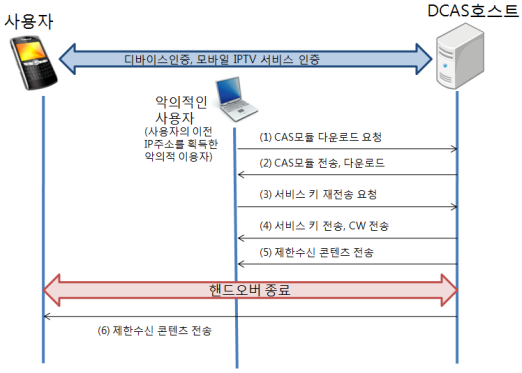

그림 5. 제한 수신 모듈의 다운로드 취약점

IV. 이동성 문제에 대한 대응 방법 제안

1. 이동시의 DCAS 다운로드 절차

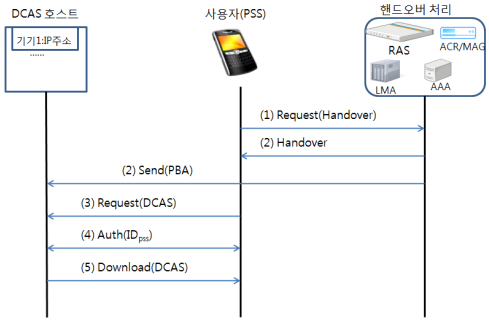

그림 6. 와이브로 모바일 IPTV의 이동성 취약점에 대한 대응 방법

3장에서 와이브로 모바일 IPTV에 대한 문제점으로 IPTV의 이동성과 관련된 문제를 지적하였다. 현재 와이브로 모바일 IPTV 모델에서는 DCAS 호스트가 모바일 IP주소에 대한 내용을 다루고 있지 않고 있으나, IP 주소에 대한 내용을 보관하고, 변경이 일어났을 경우에 대한 대응이 가능하도록 제한수신 모듈 또는 제한수신 호스트가 구성되어야 한다. 이들 문제를 해결하기 위한 방법을 [그림 6]에서 나타내었다. 사용자가 모바일 IPTV를 시청하면서 필요에 의해 DCAS 모듈을 다운로드하기 위한 절차에 사용되는 함수 및 인수를 아래와 같이 정의 한다.

- Request() : 요청
- Auth() : 인증
- Send() : 전송
- Download() : 다운로드
- IDpss : 사용자 디바이스의 ID, 시리얼 번호

3장에서 지적한 모바일 IPTV의 이동성과 관련된 취약점에 대하여 아래의 절차로 대응할 수 있다.

(1) 사용자 디바이스는 RAS에 핸드오버 요청한다.
(2) [그림 4]의 핸드오버 처리 절차에 의해 핸드오버 처리 후, DCAS 호스트에 디바이스의 새로운 주소를 포함한 PBA를 전송하고, DCAS 호스트는 사용자 디바이스의 새 주소를 기록한다.
(3) 사용자 디바이스가 DCAS 호스트에게 새로운 DCAS 모듈 다운로드를 요청한다.
(4) DCAS 호스트와 사용자 디바이스 사이에서 디바이스 인증 수행 후 DCAS 호스트는 DCAS 서버에 CAS 모듈 다운로드 요청하여 CAS 모듈 획득한다.
(5) DCAS 호스트는 CAS 모듈을 사용자 디바이스에 다운로드한다.

핸드오버가 발생할 때마다 DCAS 호스트에서 사용자 디바이스의 주소가 변경되므로, 주기적으로 전송되는 제어워드가 올바르게 전송되어 항상 디스크램블링을 할 수 있게 되므로 제어 워드의 전송문제가 해결될 수 있다. 제한수신 모듈의 다운로드 문제를 해결하기 위해서는 핸드오버가 발생할 때마다 이전 주소로의 정보 전송을 중지하고, 이미 인증된 사용자에 대해서도 제한수신 모듈의 다운로드 및 변경 시에는 디바이스 인증 및 사용자 인증을 요구하도록 시스템을 구현할 필요가 있다. 그러나, 모든 정보 및 보안 모듈이 소프트웨어 다운로드 형태로 구성되는 DCAS에서 콘텐츠 이용 도중 사용자 정보를 입력하는 것은 이용자 편의성을 저해하므로 제한수신 모듈 다운로드 시에 디바이스 인증만 수행할 것을 제안하였다. 바꾸어 말하면 제어 워드 전송 문제 및 제한수신 모듈의 다운로드 문제는 모두 이동성과 관련된 문제이면서 핸드오버 처리를 하는 과정에서 DCAS 호스트에 사용자 디바이스의 변경된 주소를 알려주어 문제를 해결할 수 있다. 또한, 악의적인 중간자가 서비스 이용자의 자격 관련 정보를 입수하여도 사용자와 같은 주소를 획득하지 않는 한 서비스를 이용할 수 없으므로 모바일 IPTV에 대한 다양한 공격에 대응할 수 있다.

2. 효율성 평가

와이브로 모바일 IPTV와 1절에서 제안한 방법을 적용한 모바일 IPTV의 성능을 비교하기 위하여 사용자 인증의 횟수를 비교하기로 한다. 사용자 인증이란 사용자 ID와 패스워드를 이용하는 방법으로서 사용자가 직접 정보를 입력하는 방법을 말하며, 처리 과정에서 많은 시간 및 연산을 필요로 하여 전체적인 성능에 많은

영향을 미치는 요소이다. 일정시간 동안 n회의 핸드오버가 발생하고, 사용자는 제한 수신 모듈을 k회 다운로드 요청한다고 두자. 또, 제한 수신 모듈의 다운로드는 자주 발생되는 것이 아니므로 $n \geq k$라고 가정한다.

와이브로 모바일 IPTV에서 공격자는 핸드오버가 발생할 때마다 제한 수신 모듈의 다운로드를 요청할 수 있으므로, 이에 대응하기 위해서는 핸드오버가 발생할 때마다 사용자 인증을 수행해야 한다. 일정 시간동안 수행되는 총 사용자 인증의 횟수를 N_1이라 두면 N_1은 최초의 서비스 이용 시의 사용자 인증을 포함하여 다음과 같이 계산된다.

$$N_1 = n + k + 1$$

이에 대하여 제안한 방식에서는 제한 수신 모듈을 다운로드할 때에만 사용자 인증이 요구되므로 사용자 인증 횟수 N_2는

$$N_2 = k + 1$$

로 된다. 디바이스 인증을 사용할 경우에는 1회의 사용자 인증과 k회의 디바이스 인증을 수행하게 된다. $N_1 > N_2$이므로 같은 정도의 안전성을 확보하는 데 제안 방식이 더 효율적이라고 할 수 있다.

3 제안 방법과 보안 요구 사항의 비교

제안한 방법의 성능 평가를 위하여 한국정보통신기술협회(TTA)에서 제시한 모바일 IPTV의 보안 요구사항[6]과 비교하기로 한다. TTA는 보안 기술을 보안 일반, 서비스 보안, 콘텐츠 보안, 단말 보안, 가입자 보안으로 분류하고 총 14개 항목의 보안 요구사항을 규정하고 있다. [표 1]은 TTA의 보안 요구 사항을 나타낸다. 본 논문에서는 이 규정을 REQ1부터 REQ14로 표시하고 와이브로 모바일 IPTV와 제안 방법을 적용한 모바일 IPTV가 TTA의 보안 요구사항을 어느 정도 지원하고 있는지 [표 2]에 나타내었다.

표 1. TTA의 모바일IPTV 보안요구사항

보안 분류	번호	내 용
보안 일반	REQ1	보안기술은 모바일 IPTV환경에서 효율적이어야 함.
	REQ2	전송 및 저장 과정에서 콘텐츠가 불법 유출되어서는 안됨
서비스 보안	REQ3	서비스에 대한 접근제어는 이동성을 지원해야 함.
	REQ4	접근제어 모듈은 device mobility를 고려한 안전한 변경 및 관리가 가능해야 함.
	REQ5	서비스에 대한 보안레벨의 변경이 가능해야 함.
	REQ6	트랜스코딩이 발생하는 중간 경로에서 서비스의 불법적인 사용/전달/삽입을 방지해야 함.
	REQ7	서비스 중간 경로에 설치된 악의적인 액세스 장치가 사용자의 서비스 자격 관련 데이터의 가로채기/변조/삭제/부정생성 등을 방지해야 함.
콘텐츠 보안	REQ8	콘텐츠 복사방지, 재분배 관리 기능은 이동성을 지원해야 함.
	REQ9	콘텐츠 특성에 따라 차별화된 usage rule 및 보안 기능 적용을 지원해야 함.
	REQ10	단말에 대해 불법 콘텐츠 추적이 가능해야 함.
	REQ11	트랜스코딩이 발생하는 중간 경로에서 콘텐츠의 불법적인 사용/전달/삽입을 방지해야 함.
	REQ12	서비스 중간 경로에 설치된 악의적인 액세스 장치가 사용자의 콘텐츠 및 메타데이터의 가로채기/변조/삭제/부정생성 등을 방지해야 함.
단말 보안	REQ13	사용자/단말 이동성 보장을 위한 안전한 소프트웨어 다운로드 및 관리를 지원해야 함.
가입자 보안	REQ14	서비스제공자는 이동성을 가지는 사용자에 대한 인증이 가능해야 함.

표 2. TTA 보안 요구 사항과 와이브로 모바일 IPTV, 제안 방법을 이용한 모바일 IPTV의 보안 기술 비교

보안 분류	번호	관련 기술	WiBro-IPTV	제안방법 적용IPTV
보안 일반	REQ1	–	○	○
	REQ2	암호 및인증	○	○
서비스 보안	REQ3	제한수신시스템	×	○
	REQ4	제한수신시스템	×	○
	REQ5	제한수신시스템, 트랜스코딩	×	×
	REQ6	트랜스코딩	×	×
	REQ7	제한수신시스템, 암호/인증	×	○
콘텐츠 보안	REQ8	DRM	×	×
	REQ9	트랜스코딩	×	×
	REQ10	추적기술	×	×
	REQ11	트랜스코딩	×	×
	REQ12	제한수신시스템, 암호/인증	×	○
단말 보안	REQ13	다운로드	△	△
가입자 보안	REQ14	사용자 인증	○	○

[표 2]에서 "○"은 지원됨을, "×"는 지원되지 않음을, "△"은 부분적으로 지원됨을 의미한다. [표 2]에서 REQ3, REQ4, REQ7, REQ12는 이동성과 관련된 사항이고, 그 중 REQ4, REA7, REQ12처럼 와이브로 모바일 IPTV에서 지원되지 못했던 보안 요구 사항이 제안 방식을 이용하여 지원될 수 있음을 보여주고 있다. [표 2]에서 와이브로 모바일 IPTV와 제안 방법을 이용한 IPTV에서 모두 "×"로 표시된 것은 REQ5, REQ6, REQ8, REQ9, REQ10, REQ11이다. 이중 REQ5, REQ6, REQ9, REQ11은 트랜스코딩[21]과 관련된 내용으로서 향후 모바일 IPTV 구현에 있어서 집중적으로 연구되어야 할 분야임을 내포하고 있다.

IV. 결 론

IPTV의 발전 및 사용자 요구에 의해 모바일 IPTV에 대한 요구가 증가하고 있고, 이에 대한 많은 연구와 개발이 진행되고 있다. 기본적으로 모바일 IPTV 에 있어서의 보안 요구 사항은 서비스 보호 및 콘텐츠 보호라는 부분에 있어서는 고정형 IPTV와 동일하나 구현에 있어서는 이들 보호 기술이 이동성을 제공해야 한다는 면이 다른 부분이다. 현재까지 개발되어 공개되고 있는 IPTV 보안 기술, 특히 제한수신 시스템은 이동성에 대한 부분을 다루고 있지 않다. 본 논문에서는 와이브로 모바일 IPTV에서 특히 이동성과 관련하여 발생할 수 있는 보안 위협으로서 제어 워드의 전송문제와 핸드오버 지연 시간 동안의 위협을 지적하고 이에 대한 대응 방안으로서 이동성과 관련된 내용을 제한수신 시스템 내에 포함하는 방법을 제안하였다. 같은 정도의 보안성을 전제로 하였을 때 요구되는 사용자 인증의 횟수를 비교하여 제안 방법이 와이브로 모바일 IPTV보다 효율적임을 나타내었다. 그러나, 핸드오버가 발생할 때마다 핸드오버 처리 이외에 새 주소를 DCAS 호스트에 전송하는 처리가 필요하므로 이로 인해 콘텐츠의 끊김 현상이 더욱 자주 발행할 가능성이 있다. 향후 이에 대한 대응 방법도 필요할 것으로 생각된다.

와이브로 모바일 IPTV의 보안 기술과 제안 방법을 적용한 모바일 IPTV의 보안 기술이 TTA의 모바일 IPTV 보안 요구사항에 어느 정도 부합되고 있는지를 비교하여, 제안 방법을 적용하였을 경우 이동성에 대한 보안이 더 향상될 수 있음을 보였다.

참 고 문 헌

[1] 윤장우, 이현우, 류원, 김봉태, "IPTV 서비스 및 기술 진화 방향", 한국통신학회지(정보와 통신) 제25권, 제8호, pp.3-11, 2008.

[2] 최락권, "IPTV 서비스 구현을 위한 핵심 기술 연구", 대한전자공학회지, 제35권, 제3호, pp.29-43, 2008.

[3] 박종봉, "IPTV 서비스, 국내외 현황과 향후 발전 모습", TTA Journal, No.122, pp.62-67, 2009.

[4] 박수홍, "Mobile IPTV 기술 및 국내외 표준화 동향", HN Focus, Vol.20, pp.48-54, 2008.

[5] H. Shirazi, J. Cosmas, D. Sutts, N. Brich, and P. Dlay, "Security Architectures in Mobile Integrated Pay-TV Conditional Access System," Proceeding of 13th International Telecommunications Network Strategy and Planning Symposium, 2008.

[6] TTA, "Non-NGN 기반 Mobile IPTV 요구사항", TTAK.KO-08.0021, 2009.

[7] 이진호, "Mobile IPTV를 위한 DCAS 기술", 모바일 IPTV 보안 심층 세미나, pp.141-158, 2009.

[8] 이선영, "CAS와 DRM을 중심으로 한 모바일 IPTV 보안 기술", 정보보호학회지, 제19권, 제5호, pp.65-72, 2009.

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

[10] 우제학, 노창현, 이완복, "IPTV 콘텐츠 보호 기술의 비교 - CAS와 DRM 중심으로", 한국콘텐

츠학회논문지, 제6권, 제8호, pp.157-164, 2006.
[11] 정영호, 정준영, 구한승, 조용성, 유응식, 권오형, “다운로더블 제한수신 시스템 기술”, 전자공학회지, 제35권, 제9호, pp.975-984, 2008.
[12] 김영모, 고병수, “다운로드형 제한수신시스템 기술 동향”, 한국방송공학회지, 제13권, 제4호, pp.54-64, 2008.
[13] Y. Jeong, S. Kim, H. Kim, H. Koo, and E. Kwon, ″A Novel Protocol for Downloadable CAS,″ IEEE Transactions on Consumer Electronics, Vol.54, No.3, 2008.
[14] 김재경, 문준우, 복혜영, “방송 통신 융합 환경에서 DCAS(Downloadable CAS)를 활용한 SimulCrypt 구축 및 운영방안”, 한국인터넷정보학회 추계학술발표대회 논문집, 제9권, 제2호, pp.69-74, 2008.
[15] 장희진, 한연희, 방정호, “와이브로 망에서 IPv6^ 단말의 고속 핸드오버 최적화 방안”, TTA Journal 103, pp.50-56, 2006.
[16] IETF RFC 5213, ″Proxy Mobile IPv6,″ 2008.
[17] 김수득, 이종혁, 정태명, “Proxy Mobile IPv6에서의 안전한 Fast Handover 기법”, 한국인터넷정보학회 학술발표대회 논문집, pp.17-20, 2009.
[18] TTA, “와이브로에서의 프록시 모바일 IPv6 적용”, TTAK.KO-10.0284, 2008.
[19] 장희진, 한연희, 황승희, “와이브로 망에서 IPv6 이동 단말의 교차 계층 핸드오버 기법”, 정보과학회논문지 :정보통신 제34권, 제1호, pp.48-61, 2007.
[20] TTA, “EAP-TLS 기반의 휴대인터넷(와이브로) 상호 인증 방법”, TTAK.KO-06.0206, 2009.
[21] 헨드리, 김문철, 함상진, 이근식, 박근수, “스케일러블 비디오 부호화에 대한 계층적 부호 기법”, 2006 한국방송공학회학술대회 논문집, pp.307-312, 2006.

저 자 소 개

이 선 영(Sun-Young Lee) 정회원

- 1993년 2월 : 부경대학교 전자계산학과(이학사)
- 1995년 2월 : 부경대학교 전자계산학과(이학석사)
- 2001년 3월 : 일본동경대학 전자정보공학(공학박사)
- 2004년 3월 ~ 현재 : 순천향대학교 정보보호학과 교수

<관심분야> : 콘텐츠 보안, 암호이론, 정보이론, 정보보안