비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜

서대희°, 백장미°°, 문용혁°, 남택용°, 나재훈°
한국전자통신연구원°
순천향대학교°°
dhseo@etri.re.kr, bjm1453@sch.ac.kr, {yhmoon, tynam, jhnah}@etri.re.kr

Authentication Protocol based on IDAM-AS for Non-Realtime IPTV

Dae-Hee Seo°, Jang-Mi Baek°°, Yong-Hyuk Moon°, Taek Yong Nam°, Jae Hoon Nah°
Electronics and Telecommunications Research Institute°
Soonchunhyang University°°

요 약

최근 인터넷의 급속한 발전은 초고속 인터넷망을 이용해 양방향 텔레비전 서비스의 IPTV에 대한 연구 및 상용화를 촉진하고 있다. IPTV는 초고속 인터넷망을 기반으로 다양한 콘텐츠 및 부가 서비스를 제공하는 방송 통신 융합 서비스중의 하나이다. 그러나 콘텐츠의 재사용에 따른 디바이스의 안전한 보안 서비스를 제공하지 않을 경우 비즈니스 모델의 상용화에 많은 보안 취약성이 발생할 수 있어 이를 위한 연구가 요구되고 있다. 따라서 본 논문에서는 기존의 IPTV에서 적용되고 있는 카드 기반의 취약성을 보완하고 비실시간 IPTV 서비스를 위한 자동화된 재사용 콘텐츠의 멀티 에이전트 시스템인 IDAM-AS를 기반으로 디바이스의 안전한 초기 등록과 인증 과정을 제안한다. 제안 방식은 분산된 에이전트를 관리할 수 있는 IDAM-AS를 정의하고 이를 이용해 사용자의 최소의 정보 입력을 통해 재사용 콘텐츠에 대한 자동화된 서비스가 이루어지도록 하였다.

1. 서 론

적응형 미디어 기술중 IPTV(Internet Protocol Television)는 개인 네트워킹 기술을 기반으로 콘텐츠를 전송/활용하기 위한 상호 연동형 보안 기술이 요구되며 신뢰성을 보장하기 위한 미디어 적응 변환 보안 기술에 대한 연구가 활발하게 이루어지고 있다[1]. 그러나 기존의 IPTV 미디어 보호 기술은 실시간적 보안 솔루션에 개발이 주류를 이루고 있으며, 셋톱박스를 이용해 식별 및 인증을 수행함으로써 비실시간 IPTV 콘텐츠의 적용에서 한계성이 발생하고 있다[2][3]. 따라서 본 논문에서는 비실시간 IPTV에 서 SVC(Scalable Video Codec)를 이용한 원 소스 멀티유스(One source multi-use)의 장점을 활용할 때 비인가 디바이스에 대한 불법적인 데이터 사용에 따른 보안 취약성을 보완하기 위해 안전한 디바이스 등록 및 인증을 위한 자동화된 보안 서비스를 제안한다. 본 논문의 2장에서는 비실시간 IPTV 기술 개요에 대해서 기술하고, 3장에서는 기존의 연구에 대한 보안 분석을 수행한 뒤 4장에서 보안 요구사항을 제시하고자한다. 5장에서는 기존 방식의 취약성을 보완할 수 있는 비실시간 IPTV의 원 소스 멀티 유스를 위한 IDAM-MS(Intelligent Distributed Autonomous Multi-Agent System) 기반의 인증 프로토콜을 제안한 뒤 6장에서 기존 방식과의 비교 분석을 통해 제안 방식을 분석하고 7장에서 결론 및 향후 연구 방향을 제시하고자 한다.

2. Technology Review

IPTV는 디지털 컨버전스에 따른 차별화된 신개념 서비스이다. 특히, 초고속 인터넷 기반으로 멀티미디어 콘텐츠를 양방향 서비스, 개인 맞춤형 서비스를 제공함으로써 기존의 TV와는 차별화된 특징을 갖는다[4].
따라서 이종적인 서비스 환경에서 사용자의 서비스 요구에 따른 품질을 유지할 수 있는 적응형 미디어 부호화 기술인 SVC 기술을 적용한 다양한 연구들이 진행되고 있다. 그러나 비실시간 IPTV 서비스에서 SVC를 적용할 경우 멀티미디어 데이터에 대한 전체적인 암호화/복호화에 따라 계산량 및 지연에 따른 따른 안전한 보안 서비스의 한계성이 문제시 되고 있다[3]. 따라서 선택적인 암호화 방식을 제공하면서 비실시간IPTV에서 인가된 디바이스에 안전하게 콘텐츠를 제공함으로써 고품질 및 안전한 멀티미디어 데이터 서비스에 대한 연구가 반드시 요구된다.

3. 기존 방식 분석

본 장에서는 기존 연구 방식에 대한 연구를 분석하고자 한다.

3.1 Wang 방식

2006년 Wang(외 3명)은 스마트 카드 기반의 원격 사용자 인증을 제안하였다. 본 방식은 원격 사용자가 생성

한 랜덤수와 패스워드를 이용해 일방향 해쉬 함수값으로 사용자를 인증하고 이를 검증한다[5]. 그러나 본 방식의 경우 다음과 같은 보안 취약성을 내포하고 있다.
- 자동화된 인증 방식: 본 방식은 스마트 카드 기반의 사용자 인증 방식으로 로그인에서 4H[1], 인증과정에서 4H의 계산량이 발생한다. 따라서 사용자의 수에 따라 서버의 오버헤드가 발생하며 이를 최소화하기 위하여 자동화된 인증 개체를 구성해야 한다.
- 보안 정책의 적용: 비실시간 보안 서비스를 적용하기 위해서는 각각의 사용자의 인증 정보에 기반한 보안 정책을 적용해야 비인가된 사용자로부터의 멀티미디어 콘텐츠 제공의 안전성을 확보할 수 있다. 그러나 본 방식에서는 제공하지 않는다.
- 비실시간 서비스의 적용성 이종적인 네트워크 환경에서 비실시간 서비스를 위해서는 사용자의 인증 기술과 더불어 접근 제어 및 정책적인 내용을 제공해야 한다. 그러나 본 방식의 경우 스마트 카드를 기반으로 하여 사용자의 인증 과정만을 수행함으로써 접근 제어 및 정책적인 내용을 제공하지 않아 비실시간 서비스의 적용에 한계성이 있다.

3.2 Winkler 방식

2008년 Winkler(외 6명)에 의해 제안된 방식은 인증 관리 기술을 간단하게 초기화하고 익명성과seamless 서비스를 제공하기 위해 SSO에 기반한 IP Multimedia Subsystem을 이용한다[6]. 그러나 본 방식은 다음과 같은 보안 취약성을 내포하고 있다.
- 패스워드 추측 공격: 본 방식의 경우 사용자의 사전 등록 과정에서 공격자는 알려진 정보 b와 사용자의 이전 로그인 정보 $\{ID, T\}$를 이용해 현재의 패스워드 PW와 이전 패스워드 PW'에 대한 비교를 통해 추측 공격이 가능하다.
- 위장 및 수정 공격 공격자가 패스워드 추측 공격으로 패스워드를 추출하였을 경우 위조된 로그인 정보를 생성하여 이를 기반으로 사용자를 위장할 수 있다.
- 보안 정책의 적용: 본 방식은 패스워드 공유의 안전성에 기반하여 일방향 식별을 제공한다. 따라서 위장된 공격자에 대한 검증 및 서비스에 대한 보안 정책 운영에 대한 취약성을 내포하고 있다.

3.3 Pipattanasomporn 방식

2009년 Pipattanasomporn (외 2명)이 제안한 방식으로 스마트 그리드를 위한 멀티 에이전트 시스템을 구현 하였다. 특히, 본 방식은 홈 네트워크의 자동화된 에이전트 관리 시스템인 IDAPS(Intelligent Distributed Autonomous Power System)을 제시하였다[7].
그러나 본 방식은 신뢰된 개체를 기반으로 하드웨어 기반의 추가적인 보안 시스템이 필요할 뿐만 아니라 소프트웨어적인 미들웨어를 통해 보안 서비스를 제공함으로써 사전 정의된 보안 서비스 이외의 추가적인 보안 서비스의 제공이 어렵다. 따라서 스마트 그리드 이외에 자동화된 에이전트 측면에서의 보안 취약성은 다음과 같다.
- 서비스 거부 공격: 제안된 방식은 신뢰된 개체의 TCP/IP 기반으로 에이전트의 메시지를 교환한다. 따라서 TCP/IP 기반의 공개된 채널에서 발생할 수 있는 기밀성 무결성의 보안 서비스가 요구되나 제공하지 않는다.
- 패스워드 기반의 효율성 본 방식은 에이전트 이전에 사용자의 ID/PW 방식에 기반한 인증 방식을 이용함으로써 기존의 PW 인증의 취약점을 그대로 내포하고 있다.
- 자동화된 인증 방식: 에이전트 관리를 위하여 자동화된 개체를 제시하였으나 이를 이용한ID/PW 인증 방식을 제공하나 이는 별도의 에이전트간의 인증 정보 교환이 이루어지지 않아 자동화된 형식의 보안 정보 교환이 어렵다.
- 보안 정책의 적용: 제안 방식은 보안 정책은 제공하지 않는다.

4. 보안 요구사항 분석

비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜 제안을 위한 보안 요구사항은 다음과 같다.
- 인증정보의 안전성 ID/PW 기반으로 경량화된 방식을 이용할 경우 ID/PW에 대한 패스워드 추측 공격에 안전성을 유지할 수 있는 보안 서비스를 제공해야 한다.
- 전송 정보의 보안 사용자 프라이버시 정보에 기반한 전송 정보의 상호 교환시 이에 대한 기밀성무결성 서비스를 제공해야 한다.
- 재전송 공격에 대한 안전성 이전 세션 정보에 기반해 현재의 비밀정보를 유추할 수 없도록 재전송 공격에 안전성을 제공할 수 있는 보안 서비스를 제공해야 한다.
- 서비스 거부 공격: 타임 스탬프를 이용해 서비스 거부 공격에 대한 보안 서비스를 제공해야 한다.
- 패스워드 기반의 효율성 패스워드 생성 및 인증시 클라이언트 측면에서 최소의 연산으로 계산의 효율성을 제공해야 한다.
- 자동화된 인증 방식: 사용자의 입력을 최소화하면서 자동화된 소프트웨어를 기반으로 인증 과정을 수행함으로써 자동화된 형식의 인증 방식을 제공해야 한다.
- 보안 정책: 다양한 사용자들에 대한 차별적인 보안 정책을 적용함으로써 비실시간 IPTV 콘텐츠에 대한 안전성을 확보해야 한다.
- 비실시간 서비스의 적용성 실시간 IPTV 뿐만 아니라 비실시간 IPTV를 위한 콘텐츠의 재사용에 관련된 시스템에 적용할 수 있어야 한다.

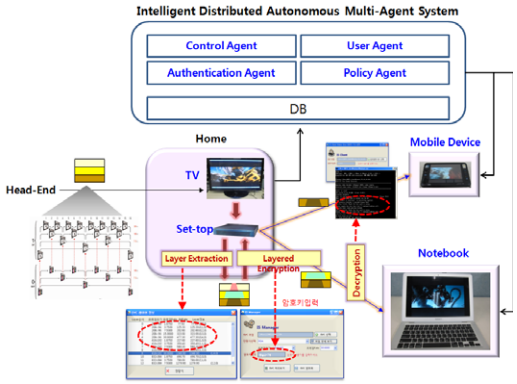
5. 비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜 제안

본 논문은 콘텐츠 재사용을 위한 비실시간IPTV 시스템을 위한 안전한 사용자 인증 프로토콜을 제안하고자 한 미디어 시스템(Intelligent Distributed Autonomous Multi-Agent System: IDAM-AS)을 기반으로 사용자의

1) 일방향 해쉬 연산 및 keyed 및 unkeyed 함수의 계산량

초기 등록 과정과 인증 과정을 수행한다. IDAM-AS는 다음과 같은 에이전트로 구성된다.

· Control Agent : 멀티미디어 콘텐츠의 재사용을 위해 사용자가 구매한 콘텐츠 정보를 저장하고 관리하는 개체
· User Agent : 사용자들의 콘텐츠 사용 유형 및 기호 정보등 사용자의 프라이버시 정보를 저장하고 관리하는 개체
· Authentication Agent : 초기 사용자 등록시 사용자와 초기 인증 과정을 수행하는 개체
· Policy Agent : 콘텐츠를 서로 다른 디바이스에 제공받고자 할 경우 사용자의 정보 및 디바이스 정보에 따라 보안 정책을 유동적으로 관리하는 개체



(그림 1) 비동기 IPTV를 위한 IDAM-AS

5.1 시스템 계수

다음은 비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜을 위한 시스템 계수이다.

* (사용자: u, 무선 디바이스: D, Control Agent:CA, User Agent: UA, Authentication Agent:AA, Policy Agent:PA)

pw : 사용자의 패스워드
r_* : 각 개체에서 생성한 랜덤 수
$H()$: 안전한 해쉬 알고리즘
T_*: 타임 스탬프
n: modular n
e: 이벤트 메시지
ID: 각 개체의 ID
$Content_i$: 비실시간 IPTV에서 제공되는 콘텐츠

5.2 프로토콜

비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜은 콘텐츠 사용을 위한 디바이스 초기 등록 단계와 콘텐츠 제공을 위한 인증 과정으로 구성된다.

1) 초기 등록 단계

초기 등록 단계는 비실시간된 IPTV의 콘텐츠의 재사용을 위해서 IDAM-AS의 에이전트에 디바이스를 등록하여 세션키를 설립하는 단계이다.

① u는 디바이스 초기 등록을 위한 패스워드(pw)를 디바이스에 입력한다.

② pw를 입력받은 디바이스는 a, r_D를 선택하고 A와 h_D를 계산한 뒤 IDAM-AS의 AA에 ID_D, h_D, T_D, A를 전송한다.

$A = g^{r_D} \bmod n,\ h_D = H(pw \oplus T_D),$

③ 디바이스로부터 ID_D, h_D, T_D, A를 수신한 AA는 $\triangle T$를 계산하고 α, β, B를 계산 한 뒤 디바이스에 ID_{AA}, β, T_{AA}를 전송한다.

$\alpha = H(ID_{AA} \oplus T_{AA}),\ B = g^{r_{AA}} \bmod n,$
$\beta = \alpha \oplus B,\ \triangle T = T_{AA} - T_D$

④ 디바이스와 IDAM-AS의 AA는 상호 세션키 k를 다음과 같이 계산하여 안전하게 저장한다.

$k = (g^{r_D r_{AA}} \oplus \triangle T)$

2) 디바이스 인증 단계

비동기 IPTV 시스템에서 콘텐츠를 사용자에게 제공하기 위한 다음과 같은 인증 단계를 수행한다.

① 사용자는 디바이스에 pw를 입력함으로써 콘텐츠 요청 과정을 수행한다.

② 디바이스는 사용자의 pw를 수신한 후 비밀정보 S_D와 이벤트 메시지 e_D 생성한 후 이를 IDAM-AS의 UA에 이를 전송한다.

$S_D = E_k(r_D \| H(pw)),\ e_D = < ID_D, Contents_i, T_{D_1}, S_D >$

③ IDAM-AS의 UA는 이벤트 메시지 e_D에서 디바이스의 ID를 추출한 뒤 ID_D, S_D, $Content_i$를 전송한다.

④ AA는 UA로부터 수신한 ID_D, S_D를 검증한다.

<Verify>

AA는 초기 등록 단계에서 디바이스 ID_D와 설립한 세션키 k를 이용해 S_D를 복호화하여 r_D와 $H(pw)$를 추출한 뒤 $g^{AB} \oplus \triangle T$임을 검증한다.

검증이 올바른 경우 AA는 CA에 S_{AA}를 계산하고 ID_D, $Contents_i$, S_{AA}를 전송한다.

$S_{AA} = E_k(b \| \triangle T \| r_{AA})$

⑤ AA로부터 ID_D, S_{AA}, $Content_i$를 수신한 CA는 $Content_i$에 대한 C_1, C_2를 계산한 뒤 S_{AA}, C_1, C_2를 UA에 전송한다.

$C_1 = \gcd(a,b),\ C_2 = lcm(a,b)$

⑥ UA는 CA로부터 전송된 S_{AA}, C_1, C_2를 기반으로 X, Y를 계산한 뒤 이를 디바이스에 전송하고 PA에 이벤트 메시지 e_D에서 요구한 $Contents_i$에 해당되는 콘텐츠를 요청한다.

$X = (C_1 \oplus S_{AA}),\ Y = (C_2 \oplus S_{AA})$

⑦ PA는 $Contents_i$의 선택적 암호화 영역을 제공하기 위해 h_{PA}를 다음과 같이 계산한 뒤 이를 AA에 전송한다.

$k_d = H(C_1 \oplus C_2 \| SL_i \| T_{PA})$

⑧ 디바이스는 CA로부터 전송된 X, Y를 수신하고 이를 검증하고 검증이 올바른 경우 PA로부터 전송한 콘텐츠를 선택적 영역만을 복호화하여 이를 사용자에게 제공한다.

6. 제안 방식 분석

본 장에서는 비실시간 IPTV를 위한 IDAM-AS 기반의 인증 프로토콜을 기존 방식과 비교 분석한다.

- 인증정보의 안전성: 제안 방식은 사용자의 디바이스에 입력된 패스워드 정보를 기반으로 세션키를 설정하고 IDAM-AS의 자동화된 소프트웨어를 통해 사용자의 정보를 분할하여 관리함으로써 인증정보의 안전성을 유지할 수 있다.
- 전송 정보의 보안: 전송 정보에 대한 세션 키 기반의 암호 통신과 해쉬 알고리즘을 통한 무결성 서비스를 제공한다.
- 재전송 공격 및 서비스 거부 공격에 대한 안전성: 제안 방식의 경우 타임 스탬프 T의 변화량에 따라 현재의 비밀정보를 유추하기 위하여 이전 세션 정보를 이용할 경우 비밀값 추출이 어렵다.
- 서비스 거부 공격: 제안 방식은 콘텐츠 요청 메시지에 대한 응답 메시지를 위한 상호 세션키를 생성시 타임 스탬프를 이용하여 서비스 거부 공격에 대한 안전성을 유지할 수 있다.
- 패스워드 기반의 효율성: 인증 과정에서 사용자는 디바이스에 패스워드 입력과정 1회와 해쉬 연산 1회, 지수승 연산 1회를 수행하여 세션키 및 상호 인증 과정을 수행한다. 따라서 기존 과정에 비해 사용자의 입력 회수는 동일하나 지수승 연산에 대한 계산량은 증가한다.
- 자동화된 인증 방식: 제안 방식은 사용자의 비실시간 콘텐츠의 안전한 재사용을 위하여 자동화된 형태의 IDAM-AS를 제안하고 이를 기반으로 사용자의 패스워드 입력만으로 세션키 설정 및 보안 정책을 적용할 수 있도록 함으로써 자동화된 형태의 인증 및 관리가 가능하도록 하였다.
- 비실시간 서비스의 적용성 및 보안 정책: 제안 방식은 비실시간 IPTV 콘텐츠의 재사용을 위하여 콘텐츠와 사용자에 따라 별도의 추가적인 보안 정책의 활용이 가능하며, 원소스 멀티유즈 콘텐츠를 위한 자동화된 에이전트의 권한 설정으로 실시간 IPTV 서비스에 한계성을 보완하였다.

7. 결 론

IT 기술의 발달은 TV, PC 등 다양한 기기들을 소형화, 통합화 되고 있으며, 통신 사업자의 미디어 진출을 통해 새로운 시장 창출을 시도하고 있다. 특히, IPTV는 방송통신 융합 환경에서 장소와 디바이스에 구애받지 않고 언제 어디서나 자유롭게 서비스를 제공받을 수 있는 유무선 통합 TV 서비스이다.

그러나 사용자의 다양한 형태의 콘텐츠 사용에 따른 비실시간형 IPTV 서비스 및 원 소스 멀티유즈에 따른 안전성 확보는 IPTV 서비스 활성화에 반드시 해결해야 할 선결 과제이다. 따라서 본 논문에서는 비실시간 IPTV 서비스에서 SVC의 선택적 암호화를 인가된 사용자에 제공하기 위한 IDAM-AS 기반의 자동화된 인증 프로토콜을 제안하였다. 제안된 방식은 기존의 연구에서는 자동화된 IDAM-AS을 제안하고 각각의 에이전트를 이용해 사용자의 인증 및 콘텐츠에 대한 정보를 암호화함으로써 안전하게 사용자 콘텐츠의 선택적 암호화 부분을 제공한다. 향후 IDAM-AS를 비실시간 IPTV 서비스에 구현하여 적용함으로써 보다 향상된 형태의 안전한 IPTV 서비스를 제공하고자 한다.

Acknowledgement

본 연구는 지식경제부/방송통신위원회 및 정보통신산업진흥원의 IT 신성장동력핵심기술개발사업의 일환으로 수행하였음. [2008-S-006-01, 유무선 환경의 개방형 IPTV(IPTV2.0) 기술개발]

8. 참고 문헌

[1] ETSI TS 182 027 v2.0.0 (2008-02): Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem.

[2] Y. Guo, C. Lin, H. Yin, Z. Zhao, Design and analysis of IPTV digital copyright management security protocol, in: Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems 2007, pp. 554 - 557, 2007.

[3] 박종열, 문진영, 김정태, 백의현, “ITU-T FG IPTV Security Aspects 표준화 기술 동향,” 전자통신동향분석 제 22권 제 5호, pp130-142, 2007.

[4] J. Kishigami, The role of QoE on IPTV services style, in: Proceedings of the Ninth IEEE International Symposium on Multimedia, 2007, pp. 11 - 13, 2007.

[5] Xiao-Min Wang, Wen-Fang Zhang, Jia-Shu Zhang and Muhammad Khurram Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," Computer Standards & Interfaces Volume 29, Issue 5, pp. 507-512, 2007.

[6] Florian Winkler, Mischa Schmidt, Sebastian Felis, Oleg Neuwirt, Joao da Silva, Nils Richter and Daniele Abbadessa, "Identity Management for IMS-based IPTV," GLOBECOM 08, 2008.

[7] M. Pipattanasomporn, H. Feroze and S. Rahman, "Multi-Agent Systems in a Distributed SmartGrid: Design and Implementation," Proc. IEEE PES 2009 Power Systems Conference and Exposition (PSCE'09), pp.1-8, 2009.