Wireless IPTV QoS를 위한 보안에 관한 연구†

홍성화*, 길준민**,‡
*목포해양대학교 해양정보통신공학과
**대구가톨릭대학교 IT공학부
e-mail: shhong@mmu.ac.kr, jmgil@cu.ac.kr

A Study on the Security for the Wireless IPTV QoS

Sung-Hwa Hong*, Joon-Min Gil**
*Dept of Maritime Inform. & Comm., Mokpo National Maritime University
**School of Information Technology Eng., Catholic University of Daegu

요 약

유선 IPTV 멀티캐스팅 서비스에서 증가되는 네트워크 트래픽 로드에 따른 화상 품질 측정과 화상 품질 변화에 대한 연구는 IPTV 서비스에 대한 관심이 현실화됨에 따라 필요하게 되었다. 또한, 다양한 무선 이동 단말의 등장으로 무선 IPTV 연구에서의 네트워크 트래픽 로드에 따른 화상 품질의 효과가 주어지는 네트워크 성능 확인 및 이를 활용하기 위한 보안에 대한 필요가 증대하게 되었다. 따라서 테스트 환경을 학교 네트워크로 확장하여 실제 IPTV 서비스 환경과 비슷한 학교 네트워크에서 네트워크 트래픽 로드 증가에 따른 무선 IPTV 멀티캐스팅 서비스에서의 보안 방안에 대해 연구하고자 한다.

1. 서론

IT 컨버전스는 미디어, 통신, 인터넷이 각 영역별로 구축한 네트워크-단말기-콘텐츠의 수직적인 가치사슬을 수평적으로 융합하고 있다. 아날로그 기술 하에서는 네트워크-단말기-콘텐츠가 수직계열화 하고 있으나 디지털 융합 기술로 인해 네트워크, 단말기, 콘텐츠가 수평적으로 융합화 되고 있다[1-5].

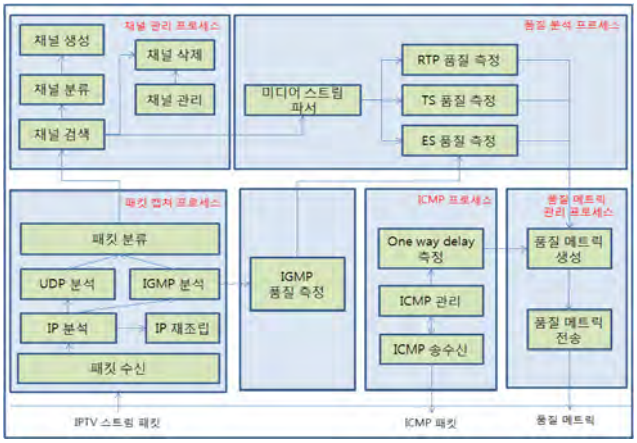
IT 기술에 급성장과 서비스의 융·복합화가 가속화됨에 따라 영상 서비스 및 영상관련 제품의 수요가 급격하게 증가하고 있다. 최근 네트워크 서비스의 동향은 IPTV(IP Television), VoIP(Voice over IP), VoD(Video on Demand)와 같은 사용자의 고급 멀티미디어 콘텐츠 서비스에 대한 품질에 대한 욕구에 순응하는 방향으로 발전하고 있다. 특히, 대용량 디지털 콘텐츠 산업의 발전으로 인하여 점점 더 차별화 된 품질 서비스와 그에 따른 품질관리에 대한 강한 필요성이 증가하고 있다. 하지만 현재시장은 값비싼 외산장비에 의존하고 있어 국내사업자들도 큰 부담감을 안고 있는 실정에 있다.

유선 상에서의 품질보장 서비스를 통한 다양한 멀티미디어 서비스의 확산을 위해서는 사용자가 서비스 이용에 불편함을 느끼지 않을 정도의 품질 요건을 갖출 필요가 있다. 가령, 인터넷 전화 및 IPTV와 같이 IP망을 쓰는 신규 음성·영상통화 서비스와 IPTV 서비스의 경우 기존의 PSTN(Public Switched Telephone Network)과 HD급의 지상파TV와 비슷한 품질을 제공하지 못한다면 신규 서비스로서 확산을 기대하기는 어렵다.

따라서, 현재의 유선망에서의 IPTV 만이 아니라 무선 상에서의 IPTV 서비스 품질 유지를 위한 보안에 대한 중요성이 증대하고 있다. 하지만 서비스 품질이라는 것이 소비자 개개인의 주관에 따라 다르게 나타날 것이므로 객관적이고 측정 가능한 방법으로 품질을 평가하여 궁극적인 서비스 품질을 보증하기 위한 기술 개발이 필요하다[3-9]. 또한 무선 상에서의 다른 사용자의 접근을 허용하지 않으면서, 원활한 서비스 품질을 유지하기 위한 방안이 점점 증대하고 있다.

2. IPTV

'IPTV 서비스 품질측정 S/W'의 전체 프로세스 구조는 (그림 1)과 같이 구성되어 있다.



(그림 1) IPTV 서비스 품질측정 S/W 블록 구성도

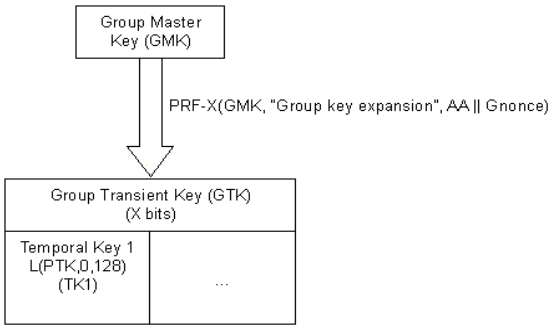
† 이 논문은 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. NRF-2014R1A1A2055463).
‡ 교신저자

정보 설정의 '버전 관리' 프로세스는 품질 측정 S/W의 버전을 주기적으로 검사하여 새로운 버전이 배포 서버에 있을 경우 업그레이드를 수행한다. 정보 설정의 '설정 정보 Load' 프로세스는 품질 측정 S/W의 초기 구동 시 설정 정보를 cfg 파일로부터 읽어서 품질 측정 S/W가 구동하기 위한 환경을 구성한다. 정보 설정의 '설정 정보 저장' 프로세스는 관리 서버에서 정의한 설정 정보를 TCP/IP 통신을 통하여 전송 받은 다음, cfg 파일로 저장하여 품질 측정 S/W 구동 환경을 구성한다.

품질 측정의 '패킷 수신' 프로세스는 네트워크로부터 유입되는 패킷을 복사하여 IPTV 미디어 스트림 패킷을 필터링한다. 품질 측정의 '채널관리' 프로세스는 필터링된 미디어 스트림 패킷을 채널별로 분류한다. 품질 측정의 '품질 분석' 프로세스는 채널별로 분류된 미디어 스트림을 채널별로 품질을 분석하여 품질 지표를 생성한다. 품질 측정의 'ICMP' 프로세스는 One Way Delay를 측정하기 위해서 ICMP 패킷을 송수신하고 RTT(Round Trip Time)를 계산한다.

3. IPTV Security

'그룹 키 계층은 그룹 키를 유도하기 위해 PRF-128이나 PRF-256을 사용한다. (그림 2)는 그룹 키 계층의 키들 간의 상관관계를 도식화한 것이다. 그룹 키 계층은 Group Master Key(GMK)를 취하여 Group Transient key(GTK)를 발생시킨다. GTK는 MAC이 브로드캐스트 및 멀티캐스트 통신(broadcast/multicast communication)을 방지하기 위해 사용하는 임시 키로 세분화된다. 그룹 키들은 단일 인증자와 그 인증자에 의해 인증된 모든 요청자들 간에 사용된다. 인증자는 그룹 임시 키를 갱신하고자 할 때마다 새로운 Group Transient Keys를 유도해야 한다. Group Master Key (GMK)는 256 비트로 구성되어 그룹 키 계층을 유도하기 위해 사용된다. GMK는 실난수를 사용하여 초기화된다. 어떤 GMK이든 간에, GMK가 일단 손상되었다면, 데이터의 노출을 감소하기 위하여 AP에 설정한 시간(time interval)내에 재-초기화되어야 한다.



(그림 2) 그룹 키 계층

(그림 2)에서 GNonce는 IEEE 802.1X 인증자에 의해 제공된 난수 혹은 가상 난수값이다.

-The Group Transient Key (GTK)는 다음과 같은 식에 의해 GMK로부터 유도된다.

GTK <= PRF-X(GMK, Group key expansion || AA || GNonce)

TKIP의 경우에는 X = 256을 사용하고, CCMP, WRAP, 및 WEP는 X = 128을 사용한다. AA는 IEEE 802 번지수를 나타내고 GNonce는 사전에 정의한 비트열을 나타낸다.

-Temporal Key 1 (TK1)는 다음 식과 같이 GTK의 비트 0-127에 해당된다:

TK1 <= L(GTK, 0, 128)

IEEE 802.1X는 MLME-SETKEYS.request이 전제된 IEEE 802.11에 TK1을 설정하고 있는데, 이 값을 번역한 것이 이 키의 암호규약 명세가 된다.

- Temporal Key 2 (TK2)가 유도되는 경우 그 값은 다음 식과 같이 GTK의 비트 128-255에 해당된다:

TK2 <= L(GTK, 128, 128)

IEEE 802.1X는 MLME-SETKEYS.request이 전제된 IEEE 802.11에 TK2를 설정하고 있는데, 이 값을 번역한 것이 이 키의 암호규약 명세가 된다.

인증자가 그룹 키를 갱신하는 이유는 다음과 같은 몇 가지 이유에서이다.

1. STA의 제휴취소(disassociation)나 인증취소(deauthentication)시에 인증자는 GTK를 변경한다.
2. TKIP의 무결성 검사가 실패하면 그룹 키 갱신을 트리거한다.
3. 혹은 관리 이벤트(management event)가 그룹 키 갱신을 트리거하기도 할 수도 있다.

4. 결론

네트워크 트래픽 부하를 근거로 IPTV 서비스망을 통하여 멀티캐스트 실시간 방송을 통해 실제 상황과 유사한 환경에서 영상 품질 평가를 위한 지표들을 측정하고, 측정된 네트워크 측정요소를 향후 V-Factor와 ETSI TR 101 209[13] 측정 근거로 하여 비교 분석을 할 계획이다. 이러한 IPTV는 현재 유선을 중심으로 운영되고 있으나, 무선 네트워크에서도 많은 관심을 보여주고 있다. 무선 네트워크는 유선에 비하여 속도가 느리다는 단점이 있으나 여러 가지 장점, 첫째는 이동성과 설치 및 유지보수, 그리고 재 배치시의 간편성, 둘째, 긴급 및 임시 네트워크 구축의 필요성, 셋째, 유선 연결이 어려운 곳의 케이블 설치 문제 해결, 넷째, 재해시 네트워크 단절문제 해결 등으로 인하여 급속히 확산되고 있다. 또한 이러한 무선 IPTV에서의 보안 문제가 더욱 중요시되고 있다.

참고문헌

[1] "ISO/IEC 13818-1 MPEG-2 Part1: System", ISO/IEC JTC1/SG29/WG11, Nov. 1994.
[2] "ISO/IEC 19818-4 MPEG-2 Part4: Conformance Testing", ISO/IEC JTC1/SG29/WG11, Nov. 1998.
[3] "ITU-T Rec. H.264 / ISO/IEC 11496-10: Advanced Video Coding" JVT-E022, Sep. 2002.
[4] "ITU-T Rec. J.144, Objective perceptual video quality measurement techniques for digital television in the presence of a full reference", Mar. 2004.
[5] "ETR290 Digital Video Broadcasting(DVB); Measurement Guidance for DVB systems", May, 1997.
[6] "A Layman's Guide to PCR Measurements", Tektronix.
[7] "RFC 3376, Internet Group Management Protocol, Version 2", Nov. 1997.
[8] "RFC 2362, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol", Jun. 1998.
[9] "RFC 3550, RTP : A Transport Protocol for Real-Time Applications", Jul. 2003.
[10] "RFC 2733, An RTP Payload Format for Generic Forward Error Correction", Dec. 1999.
[11] "RFC 1305, Network Time Protocol (version 3)", Mar. 1992.
[12] "ETSI EN 300 468 Digital Video Broadcasting(DVB); Specification for Service Information(SI) in DVB systems", Nov. 2004.
[13] "ETSI TR 101 209 : Digital Video Broadcasting (DVB) Measurement Guidelines for DVB systems", May 2001.