논문 2008-03-27

DOCSIS 3.0 보안 시스템 기반 IPTV CAS를 위한 키 관리 기법

(A Key Management Scheme for IPTV CAS in DOCSIS 3.0 Security System)

구 한 승*, 이 진 환, 송 윤 정, 권 오 형, 이 수 인
(Han-Seung Koo, Jin-Hwan Lee, Yun-Jeong Song, O-Hyung Kwon, Soo In Lee)

Abstract : A novel scheme is presented for Traffic Encryption Key (TEK) rekeying with low communication overhead for an Internet Protocol television (IPTV) conditional access system over Data-Over-Cable Service Interface Specifications (DOCSIS) 3.0. The proposed scheme utilizes the DOCSIS system synchronization for periodic TEK rekeying instead of a conventional TEK rekeying negotiation process. Analysis shows that the communication overhead is only 0.012 Kbps when TEK rekeying frequency is 1 second.

Keywords : DOCSIS 3.0, Conditional Access System, IPTV, Key Management, Rekeying

Ⅰ. 소개

2006년 8월 미국 CableLabs는 Hybrid Fiber and Coaxial (HFC) 망에서 160Mbps 이상의 하향 전송속도 및 120Mbps 이상의 상향 전송속도를 제공할 수 있는 Data Over Cable System Interface (DOCSIS) 3.0 규격을 발표하였다[1, 2]. DOCSIS 3.0 규격은 2004년 12월부터 본격적으로 개발이 시작되었으며, 2006년 8월에 1차 버전의 규격이 발표된 이래로 2008년 2월까지 7차례의 수정 규격을 발표하고 있다. DOCSIS 3.0 규격은 이전에 발표되었던 DOCSIS 1.0/1.1/2.0 버전에 비해 채널 결합(channel bonding)기술을 사용해 하향 및 상향 전송속도를 획기적으로 늘렸으며, Quality of Service (QoS)가 강화된 Internet Protocol (IP) 멀티캐스트(multicast) 방식, 향상된 보안 전송 방식, Internet Protocol version 6 (IPv6) 방식 등이 새롭게 추가되었다[2]. 이로써 케이블 방송 사업자들은 통신 사업자들의 Fiber To The Home (FTTH) 서비스에 대응할 경쟁력 있는 기술을 갖추게 되었으며, 향후 IP Protocol Television (IPTV)를 DOCSIS 3.0 시스템의 핵심 서비스 (killer application)로 고려하고 있다[3-7].

IPTV 서비스는 기존 디지털 방송과 마찬가지로 제한수신서비스를 필요로 한다. 제한수신서비스는 사용자로부터 요금을 받는 조건으로 고품질의 방송 콘텐츠를 제공하는 서비스를 의미한다. 제한수신서비스 종류에는 방송사가 미리 준비한 패키지(package)중에서 하나를 가입(subscription)하는 가입 서비'와 특정 방송 프로그램 또는 프로그램 집합을 프로그램 방송 전에 신청하는 Pay-Per-View (PPV)서비스, 그리고 인터넷이나 TV 리모콘을 사용해 프로그램을 즉석에서 구매해 시청하는 Impulse Pay-Per-View (IPPV) 서비스등이 존재한다[8, 9].

제한수신서비스는 제한수신시스템(Conditional Access System, CAS)을 통해 제공된다[8, 10-13]. CAS는 암호화 기법을 기반으로 다양한 제한수신서비스에 대한 시청 자격을 제어한다. 즉, CAS는 제한수신서비스를 신청하지 않은 사용자가 유료채널을 시청하는 것을 방지할 뿐 아니라, 제한수신서비스를 신청한 사용자들 중에서도 정확히 자신이 신청한 제한수신서비스만을 시청하도록 한다.

DOCSIS 3.0 기반 IPTV 시스템에서는 단 방향(one-way) 시스템 기반의 MPEG CAS를 사용하는

* 교신저자(Corresponding Author)
논문접수 : 2008. 11. 05., 채택확정 : 2008. 12. 22.
구한승, 이진환, 송윤정, 권오형, 이수인 : 한국전자통신연구원(ETRI), 방송시스템연구부

것보다 양방향 통신 채널을 사용하는 DOCSIS 3.0 보안 시스템을 활용하면 더욱 효과적으로 IPTV CAS를 구성할 수 있다. DOCSIS 3.0 시스템은 DOCSIS 3.0 보안 시스템을 통해 헤드엔드(headend)에 위치하는 Cable Modem Termination System (CMTS)에서부터 사용자 측에 위치하는 Cable Modem (CM)까지 전송되는 데이터를 Multiple Access Control (MAC) 계층(layer)에서 암호화 기법을 사용해 보호한다[1]. 특히 DOCSIS 3.0 보안 시스템에서는 CMTS와 CM이 128비트 Advanced Encryption Standard (AES)와 3-Data Encryption Standard (DES) 암호화 엔진을 장착하고 있기 때문에, MPEG 기반 CAS처럼 송신기 측에 방송 트래픽을 암호화하는 스크램블러(scrambler)와 수신기 측에 암호화된 트래픽을 복호화하는 디스크램블러(descrambler)를 별도로 구성할 필요가 없어진다. 이것은 간결한 전송 시스템 구성이 가능함을 의미하며, 결국 방송 사업자의 운영 비용을 절감시킨다. 또한, CMTS는 CM이 망 접속 시 Early Authentication and Encryption (EAE)[1] 기능을 통해 X.509 인증서(certificate)기반으로 CM을 인증할 뿐 아니라, 인증서(certificate)의 유효성 검사를 Online Certificate Status Protocol (OCSP) 또는 Certificate Revocation List (CRL) 방식으로 확인할 수 있다. 그리고 DOCSIS 3.0 보안 시스템은 복제된 CM을 검출할 수 있는 메커니즘을 가지고 있어 해킹된 CM이 유료 서비스를 받는 것을 방지할 수 있다. 이뿐만 아니라, DOCSIS 3.0 보안 규격은 CM의 펌웨어(firmware)를 안전하게 다운로딩(downloading)할 수 있는 Secure Software Downloading 기능을 제공한다. 따라서 CM의 보안 모듈에 문제가 발생할 경우 언제든지 온라인(online) 상으로 개선된 보안 모듈을 다운로딩(downloading)하는 것이 가능하다.

제한수신 시스템은 고품질의 콘텐츠를 전달해야 하기 때문에 매우 높은 보안 수준을 요구한다. 하지만, 그림 1에 그려져 있듯이 DOCSIS 3.0 보안 시스템이 양방향 IPTV CAS에 알맞은 효과적인 보안 기능들을 가지고 있음에도 불구하고 제한수신시스템에서 요구하는 보안 수준을 만족하지 못한다. 예를 들면, IPTV 트래픽을 암호화하는 Traffic Encryption Key (TEK)의 갱신 주기를 DOCSIS 3.0 보안 시스템 규격에서 24시간으로 권고하고 있는 점을 들 수 있다[1]. DOCSIS 3.0 보안 규격에서는 TEK의 주기적 갱신 주기로 1 ~ 604,800초 사이의 값을 설정할 수 있도록 규정하고 있지만

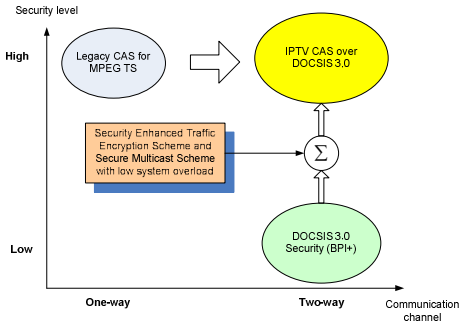


그림 1. MPEG CAS 와 DOCSIS 3.0 기반 IPTV CAS간의 보안 레벨 비교

Fig. 1. Security Level Comparison between MPEG CAS and DOCSIS 3.0 IPTV CAS

CM의 CPU 오버헤드(overhead)를 감안해 24시간의 갱신 주기를 권고하고 있다[14]. 하지만, MPEG 기반 CAS의 경우 트래픽에 대한 보안 수준을 높이기 위해 트래픽 암호화 키인 CW를 1 ~ 20초 간격으로 갱신하고 있다[10-13].

유료 방송에 있어서 시청 자격 관리는 방송 사업자의 수익과 직접 관련되기 때문에 높은 수준의 보안 시스템을 통해 수행되어야 한다. 따라서 본 논문에서 제안하는 DOCSIS 3.0 보안 시스템 기반 IPTV CAS 역시 전송되는 유료 방송 데이터의 보안 레벨을 높이기 위해 기존 MPEG 시스템 기반 CAS처럼 1 ~ 20초 정도의 아주 짧은 주기로 유료 방송 데이터 암호용 키를 갱신해야 한다[10-13].

DOCSIS 3.0 보안 시스템에서는 전송되는 IP 트래픽에 대한 기밀성(confidentiality) 보장을 위해 트래픽 암호화 키 (Traffic Encryption Key, TEK)를 사용한다. 이 TEK은 대칭 키 기반으로 운용되며, 그 갱신 주기는 1 ~ 604,800초 범위 내에서 결정된다. 하지만, CMTS와 CM은 TEK 갱신 주기마다 TEK 갱신 협상 (TEK rekeying negotiation)이라는 MAC 관리 과정 (MAC management process)을 반드시 수행해야 하기 때문에 TEK 갱신 주기를 짧게 할수록 시스템 오버헤드(overhead)가 증가되는 단점이 발생한다[14]. 따라서 DOCSIS 3.0 보안 규격에서는 시스템 오버헤드(overhead)를 회피하기 위해 TEK 갱신 주기를 24시간으로 설정하도록 권고하고 있다.

MPEG 시스템 기반 CAS에서는 제어 단어(control word, CW)가 유료 방송 트래픽에 대한 암호용 키의 역할을 수행한다. 본 논문에서 제안하는 DOCSIS 3.0 보안 시스템 기반 IPTV CAS에서

는 그 역할을 TEK이 수행한다. 하지만, 현재의 DOCSIS 3.0 보안 시스템에서는 TEK를 CAS가 요구하는 1 ~ 20초의 아주 짧은 간격으로 갱신 하는 것은 시스템 오버헤드(overhead) 관점에서 매우 부담스러운 일이다[14]. 따라서 DOCSIS 3.0 보안 시스템을 IPTV CAS에 사용하기 위해서는 TEK을 매우 짧은 주기로 갱신 하더라도 DOCSIS 시스템에 미치는 오버헤드(overhead)를 최소화 할 수 있는 주기적 TEK 갱신 기법이 요구된다.

본 논문에서는 DOCSIS 3.0 기반 IPTV CAS에서 TEK를 유료 방송 데이터 암호용 키로 사용하고, 그 갱신 주기를 MPEG CAS 수준만큼 짧게 설정하더라도 시스템 오버헤드(overhead)가 적게 발생되는 기법을 제안한다. 제안 기법에서는 DOCSIS 시스템 시간 동기 기능과 해쉬(hash) 함수[15, 16]를 사용해 TEK 갱신 협의과정을 최초 1회만 수행할 수 있도록 한다. 또한, 해쉬(hash) 함수를 사용해 키를 갱신할 때 발생할 수 있는 보안 취약점을 분석하고, 이를 해결하기 위한 방법도 제안한다.

II. 배경 기술

1. DOCSIS 3.0 시스템에서의 TEK 갱신 방법

본 논문에서 제안하는 TEK 갱신 방법에 대하여 설명하기 앞서, 일반적인 닥시스 시스템에서 트래픽 암호에 사용되는 암호화 키를 갱신하는 방법에 대하여 그림 2를 참조로 설명하기로 한다.

그림 2는 일반적인 닥시스 시스템에서의 트래픽 암호 키 갱신 방법을 나타낸 흐름도이다. 그림 2에 도시된 바와 같이, 먼저 CM과 CMTS간 양방향 통신 채널을 형성하기 위하여, CMTS 등록 과정을 수행한다. CM과 CMTS간의 통신 채널이 형성되면, CM은 인증 정보 메시지(Authentication information message)를 이용하여 닥시스 시스템의 최상위 인증기관(RCA: Root Certification Authority)이 발행한 CM의 인증서(예를 들어, Manufacturer CA 또는 CableLabs Mfg CA 등)를 CMTS에 전달한다.

CM이 인증서를 CMTS에 전달하는 과정은 선택사항으로, 특정 환경에서는 CMTS가 CM으로부터 전송된 인증 정보 메시지를 무시할 수도 있다. 그러나, CMTS가 해당 CM의 인증서를 획득할 다른 방법이 없다면, CMTS는 반드시 인증 정보 메시지를 통해 해당 인증서들을 획득해야 한다.

CM은 닥시스 MAC(Media Access Control) 트래픽 복호화를 위해 필요한 TEK를 얻기 위해 먼저 Authorization Key (AK)를 얻어야 한다. AK를 얻기 위해 CM은 모뎀 내 AK Finite State Machine (FSM)을 실행시킨다. 그리고 나서 AK FSM은 AK 요청을 위한 권한 인증 요청 메시지(Authorization Request Message)를 생성한 후 CMTS에 전달한다.

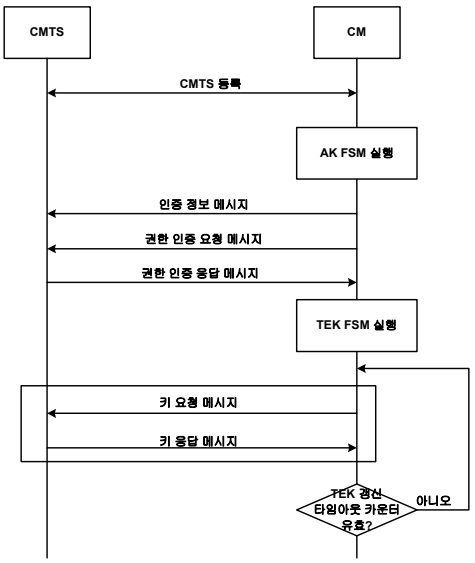


그림 2. DOCSIS 3.0 시스템에서의 TEK 갱신 흐름
Fig. 2. TEK Rekeying Flow in DOCSIS 3.0 System

권한 인증 요청 메시지를 수신한 CMTS는 CM 인증 정보를 바탕으로, 해당 CM이 AK를 수신할 자격이 있는지를 판단한다. 만약 CM이 AK를 수신할 자격이 없다고 판단하면, 권한 인증 거절 메시지(Authorization Reject Message)를 CM에 전달한다. 그러나, 반대로 CM이 AK를 수신할 자격이 있다고 판단하면, 권한 인증 응답 메시지(Authorization Response Message)를 CM에 전달한다. 권한 인증 응답 메시지에는 AK가 포함되어 CM으로 전달된다.

AK를 수신한 CM은 바로 TEK FSM을 실행한다. 여기서 TEK FSM은 CMTS가 전송한 권한 인증 응답 메시지 내의 보안연계 지시자(Securiy Association-Descriptor)에 포함된 SAID(Security Association ID)의 수만큼 생성된다. 생성된 TEK FSM은 CMTS에 SAID 각각 해당하는 TEK를 키 요청 메시지(Key Request Message)를 통해 요청

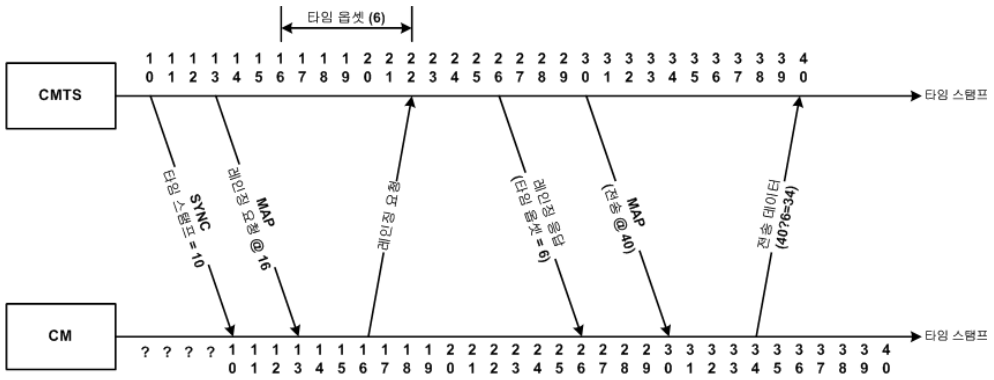


그림 3. DOCSIS 3.0 시스템에서의 초기 레인징 과정 예
Fig. 3. Example of Initial Ranging in DOCSIS 3.0 System

한다.

CM으로부터 키 요청 메시지를 수신한 CMTS는 키 요청 메시지 내 HMAC Digest (Hash Message Authentication Code Digest)를 통해, 수신한 메시지가 유효한 CM으로부터 온 것인지를 검증한다. 만약 검증에 실패하면, CMTS는 해당 CM에 키 거절 메시지(Key Reject Message)를 전달한다. 그러나, 검증에 성공하면 키 응답 메시지(Key Reply Message)를 전달한다.

이때, 트래픽 암호화 키 파라미터 값들은 3-DES Encrypt Decrypt Encrypt (EDE) 모드를 통해 암호화된다. 이후, TEK FSM은 해당 트래픽 암호화 키의 유효 기간이 만료되기 전 다시 CMTS에 키 요청 메시지를 전달해, 새로 갱신된 TEK를 요청한다. 이 과정을 TEK 갱신 협상 과정이라 한다.

CMTS로부터 TEK를 수신한 CM은 TEK 갱신 타임 아웃 카운터가 유효한지 판단하고, 타임 아웃 카운터가 만료되었다면 '키 요청메시지' 전달 단계서부터 다시 수행하면서 TEK를 발급받는다. 그러나, 타임 아웃 카운터가 만료되지 않았다면, '키 응답메시지' 전달 단계를 통해 CMTS로부터 수신한 TEK를 이용하여 데이터를 암호화한다.

이상에서 설명한 바와 같은 일반적인 TEK 갱신 방법은 미리 설정된 시간 간격으로 TEK를 갱신할 때마다 TEK 갱신 협상 (TEK rekeying negotiation)을 필요로 하기 때문에, TEK 갱신 주기를 매우 짧게 줄일 경우 시스템 오버헤드 관점에서 부담이 된다. 따라서, TEK를 매우 짧은 주기로 갱신하면서도 닥시스 시스템에 미치는 오버헤드를 최소화할 수 있는 주기적 TEK 갱신 기법이 요구된다.

2. 레인징 프로세스

닥시스 시스템에서 상향 통신을 수행하기 위해서는 TDMA(Time Division Multiple Access) 방식을 사용하기 때문에, CMTS와 CM간 시스템 시간 동기를 잃게 된다면 CM은 CMTS와 더 이상 양방향 통신을 할 수 없게 된다. 따라서 닥시스 시스템은 CMTS와 CM간의 안정적인 양방향 통신을 지원하기 위해 시스템 운영중에 지속적으로 시스템 시간 동기를 정확하게 유지하여야만 한다.

따라서 CMTS는 주기적으로 32비트 크기의 타임 스탬프(time stamp)를 포함하는 싱크 메시지(Sync Message)를 CM에 방송(broadcasting)하여, 시스템 클록(clock)의 주파수를 동기시킨다. 그러나, CM과 CMTS간의 서로 다른 물리적 거리 때문에 발생하는 신호 전달 지연 에러, 즉 시스템 클록 위상 에러는 싱크 메시지만으로 보상할 수 없다. 따라서 닥시스 시스템은 싱크 메시지를 이용해 클록 주파수 에러를 보상하는 것 이외에 시스템 클록 위상 에러의 보상이 요구된다.

닥시스 시스템은 시스템 클럭의 위상 에러를 보상하기 위해 그림 3에 도시된 바와 같이 CMTS 클록과 CM 클록간 신호 전달 지연 값인 타임 옵셋(time offset) 값을 계산하는 레인징 과정을 수행한다. 그림 3는 닥시스 시스템이 수행하는 여러 레인징 과정 중 초기 레인징 과정의 예를 나타낸 것이

다.

그림 3에서 두 시간 축은 각각 CMTS와 CM에서의 타임 옵셋 단위의 타임 스탬프 값을 나타낸다. 타임 옵셋 단위는 예를 들어, 97.65625 나노 초(nano second)를 의미하며, 타임 스탬프 카운터는 예를 들어, 419.43초의 주기를 가진다. 그림 3의 경우 CM에 대한 타임 옵셋 값은 6이 됨을 알 수 있다. 즉, CMTS가 동기를 맞추기 위해 방송한 싱크 메시지에 타임 스탬프를 10으로 설정하여 방송하면, 싱크 메시지를 수신한 CM은 메시지 내에 포함된 타임 스탬프를 이용하여 현재 CM의 시간을 설정한다.

그리고, CMTS가 MAP에 레인징 요청 메시지를 실어 CM에 전송하면, CM은 레인징 요청 메시지에 설정된 정보를 토대로 CMTS 레인징 요청 메시지를 전송한다. 여기서, CMTS가 레인징 요청 메시지에 설정한 값을 16이라고 가정하면, CM은 CM의 시간이 16이 되는 시점에 레인징 요청 메시지를 전송한다.

CM에서 전송된 레인징 요청 메시지를 수신한 CMTS는 메시지를 수신한 시간을 확인하고, 설정한 값과의 차이를 확인하여 타임 옵셋 값으로 설정한다. 그림 3에서는 CM에서 16초에 전송한 레인징 요청 메시지가 CMTS에 22초에 전달되었기 때문에, 타임 옵셋은 6이 된다. CMTS는 이 값을 CM에 레인징 응답 메시지에 포함시켜 전달함으로써, 단말이 타임 옵셋만큼 이전에 메시지를 전송할 수 있도록 한다.

Ⅲ. 시스템 동기 기반 TEK 갱신 기법

1. 제안하는 TEK 갱신 흐름

그림 4는 본 논문에서 제안하는 방법에 따른 트래픽 암호 키 갱신 방법을 나타낸 흐름도이다. 그림 4에 도시된 바와 같이 본 논문에서 제안하는 방법에 따라 TEK를 갱신하는 경우, CMTS와 CM간에 수행되던 TEK 갱신 협상 절차의 반복이 생략되어 있음을 알 수 있다.

그림 4에 대해 좀 더 상세히 살펴보면, 먼저 CM과 CMTS간 양방향 통신 채널을 형성하기 위하여 CMTS 등록 과정을 수행하는 단계에서부터 권한 인증 응답 메시지를 CM에 전달하는 단계까지는 그림 2에 도시한 일반적인 과정과 동일하다.

즉, CM의 전원이 최초 켜질 경우, CM과 CMTS 간의 통신 채널도 형성되어 있지 않을 뿐만 아니라,

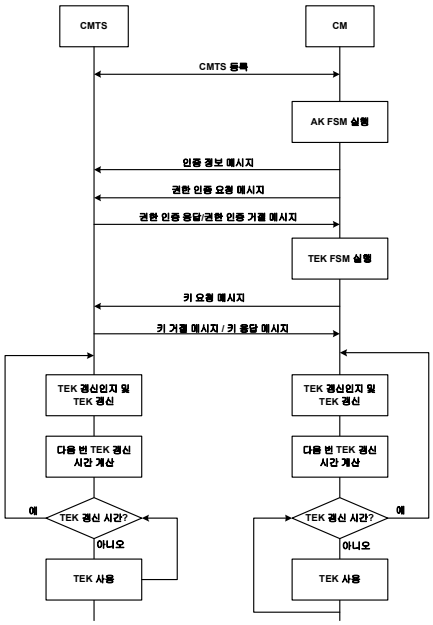


그림 4. 제안하는 시스템 동기 기반 TEK 갱신 기법

Fig. 4. Proposed TEK Rekeying Scheme based on System Synchronization

CM이 통신을 위해 필요한 AK와 TEK도 발급되어 있지 않은 상태이다. 따라서 먼저 CM과 CMTS간 통신 채널을 형성하기 위해 CM은 CMTS에 등록 절차를 수행하고, AK FSM을 실행한다.

그리고 CM은 인증 정보 메시지를 이용하여 자신의 인증서를 CMTS에 전달한다. 이때, CM이 CMTS에 자신의 인증서를 전달하는 과정은 선택적으로 수행될 수 있다. 즉, CMTS는 CM의 인증서를 인증 정보 메시지를 통하지 않고서도 획득할 수 있기 때문에, 반드시 이 과정이 수행될 필요는 없다. 그러나, CMTS가 CM의 인증서를 획득할 방법이 없다면, CMTS는 반드시 인증 정보 메시지를 통해 CM의 인증서를 획득해야 한다.

다음 CM은 트래픽 암호화 키를 얻기 위한 절차를 수행한다. 여기서 트래픽 암호화 키는 닥시스 MAC 트래픽 복호화를 위해 필요한 키를 의미한다. 트래픽 암호화 키를 얻기 위해서는 먼저 AK를 얻어야 한다. 따라서 CM은 인증 요청 메시지를 통해 CMTS에 AK를 요청하고, 이를 수신한 CMTS는 AK를 수신할 자격이 있는 CM에 한해서 AK를 포함한 권한 인증 응답 메시지를 CM으로 전달한다.

만약 CMTS가 판단한 결과 CM이 AK를 수신할 자격이 없다고 판단하면, CMTS는 CM으로 권한 인증 거절 메시지를 전달한다. 그림 4에서는 권한 인증 응답 메시지와 권한 인증 거절 메시지가 '권한 인증 응답/권한 인증 거절 메시지' 전달 절차를 통해 한꺼번에 전달되는 것으로 표기하였으나 이는 두 메시지를 동시에 전달하는 것이 아니고 CMTS에서의 판단 결과에 따라 각각 다른 메시지를 전달한다는 것을 의미한다.

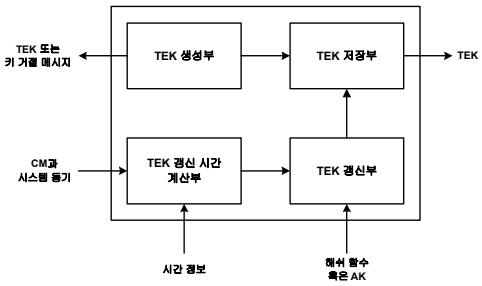
AK를 수신한 CM은 실질적으로 트래픽 암호화를 위해 필요한 트래픽 암호화 키 획득 절차를 수행한다. 이를 위해 먼저 TEK FSM을 실행한 후, CMTS로 키 요청 메시지를 통해 TEK의 발급을 요청한다.

키 요청 메시지를 수신한 CMTS는 키를 요청한 CM이 유효한 CM인지 여부를 판단하고, 만약 유효한 CM이라면 CM으로 제공할 TEK를 발급하여 키 응답 메시지에 포함하여 제공한다. 그러나 CM이 유효한 CM이 아니라면, CMTS는 권한 인증 거절 메시지를 제공한다. 이때, TEK 파라미터 값들은 다양한 방법으로 암호화되어 CM으로 전달될 수 있으며, 본 논문에서는 3-DES EDE 모드를 통해 암호화한다고 가정한다.

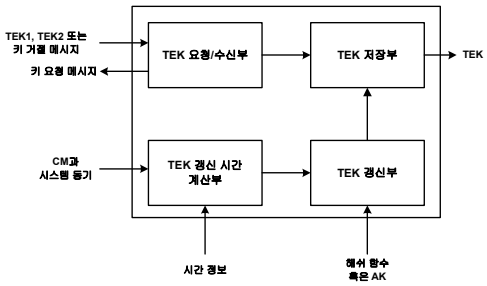
TEK를 발급받은 CM은 기존에 CMTS와 함께 수행하던 트래픽 암호화 키 갱신 협상 절차 없이 갱신 시점을 미리 계산하고, 계산된 갱신 시점에 발급받은 TEK를 갱신한다. 즉, CMTS와 CM간 시스템 시간 동기를 통해 CMTS와 CM이 각각 정확한 트래픽 암호화 키 갱신 시점을 계산한 후, 계산으로 얻어진 시각에 도달되면 CMTS와 CM이 각각 기존 트래픽 암호화 키를 해쉬 함수를 이용하여 갱신하는 방법을 사용한다.

CMTS와 CM은 미리 계산한 갱신 시점이 다가오면 TEK의 갱신을 인지한 후 TEK를 갱신하고, TEK 재발급 시간을 각각 계산한다. 이 시간은 CMTS와 CM간의 시스템 시간 동기를 통해 계산된다. 갱신된 TEK를 통해 데이터를 암호화하면서 이용하다가, CMTS와 CM은 현재 시간이 TEK 재발급 시간 즉, TEK를 갱신할 시간인지의 여부를 각각 판단하고, 갱신할 시간이라면 해쉬 함수를 활용해 기존 TEK를 새로운 TEK로 갱신하는 'TEK 갱신인지 및 TEK 갱신'단계 이후의 절차를 수행한다.

그러나, 갱신할 시간이 아니라면, CMTS와 CM은 각각 'TEK 갱신인지 및 TEK 갱신'단계에서 갱신된 TEK를 이용하여 지속적으로 데이터를 암호화한다.



(a) CMTS TEK 갱신부 구조



(b) CM TEK 갱신부 구조

그림 5. CMTS/CM TEK 갱신부 구조
Fig. 5. Architecture of CMTS/CM TEK Rekeying Block

2. CMTS와 CM에서의 TEK 갱신부 구조

그림 5(a)는 CMTS에 위치한 TEK 갱신부의 구조도이고, 그림 5(b)는 CM에 위치한 TEK 갱신부의 구조도이다.

CMTS에 위치한 TEK 갱신부와 CM에 위치한 TEK 갱신부는 각각 TEK 저장부, TEK 갱신 시간 계산부 및 TEK 갱신부를 포함한다. 그리고 CMTS에 위치한 TEK 갱신부는 TEK 생성부를, CM에 위치한 TEK 갱신부는 TEK 요청/수신부를 더 포함한다.

TEK 저장부는 CMTS에서 생성된 혹은 CMTS와 CM이 각각 갱신한 TEK를 저장하여, 트래픽을 암호화하는데 이용되도록 한다.

TEK 갱신 시간 계산부는 CMTS와 CM간에 시스템 동기화 절차를 통해 시간 동기가 맞춰진 이후, TEK 갱신 시점을 계산하여 TEK를 갱신하도록 한다. 이때 그림 5(a) 및 그림 5(b)에서는 TEK 갱신 시간 계산부가 시간 정보를 외부로부터 입력받는 것으로 표현하였으나, 반드시 이와 같이 한정되는 것은 아니다. TEK 갱신 시간의 계산 방법에 대해

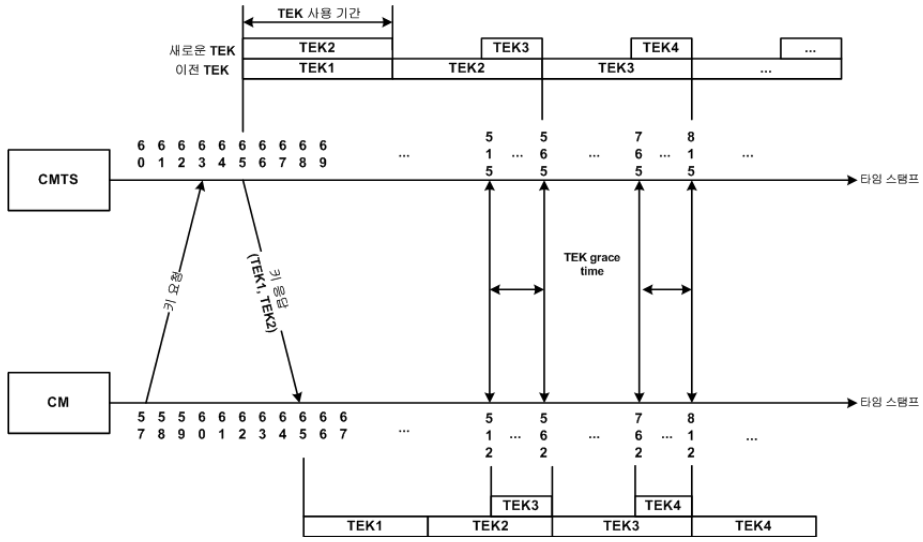


그림 6. 제안하는 TEK 갱신 시간 계산 예
Fig. 6. Example of Proposed TEK Rekeying Time Calculation

서는 추후 설명하기로 한다.

TEK 갱신부는 TEK 갱신 시간 계산부에서 계산된 갱신 시간이 도래하면, 이미 발급받아 사용중인 TEK에 대한 갱신을 수행한다. 이때, TEK의 갱신을 위해서는 TEK와 함께 해쉬 함수를 이용하여 TEK를 갱신하거나, 또는 AK를 수신하여 TEK를 갱신하도록 한다.

다음 CMTS의 TEK 생성부는 CM이 최초 동작시, CM의 TEK 요청/수신부로부터 전달된 키 요청 메시지를 토대로 초기 TEK를 생성한다. 이때, 초기 TEK를 생성할 때에는 암호화된 두 개의 TEK 즉, TEK1 및 TEK2를 생성하여 CM에 전송할 뿐만 아니라 TEK 저장부에 저장되도록 한다. 본 논문에서는 초기 TEK가 생성될 때 TEK1 및 TEK2가 동시에 생성되는 것을 예로 하여 설명하나, 반드시 이와 같이 한정되는 것은 아니다.

그리고 TEK 생성부는 CM으로부터 수신한 키 요청 메시지를 참조로 해당 CM이 유효한 CM인지 여부를 판단하여 유효할 경우 생성한 두 개의 TEK를 출력하고, 유효하지 않은 경우 이를 알리는 권한 인증 거절 메시지를 생성하여 출력한다. 이때 CM이 유효한지 아닌지의 여부는 키 요청 메시지에 포함된 HMAC-Digest를 바탕으로 판단하며, 이는 이미 알려진 사항으로 본 논문에서는 상세한 설명을 생략하기로 한다.

CM의 TEK 요청/수신부는 CMTS로 TEK를 요청하는 키 요청 메시지를 생성하여 전달할 뿐만 아니라, CMTS로부터 초기에 생성된 암호화된 두 개의 TEK를 수신한다. 만약 CMTS가 키 요청 메시지를 전달한 CM이 유효한 CM이 아니라고 판단한 경우, TEK 요청/수신부는 CMTS의 TEK 생성부로부터 권한 인증 거절 메시지를 수신하기도 한다.

이상에서 설명한 갱신부를 이용하여 실질적으로 TEK 재발급을 위한 시스템 동기 방법 및 TEK 갱신 시간 계산 방법에 대하여 그림 6을 참조로 다음 절에서 설명하기로 한다.

3. TEK 갱신 시간 계산

그림 6은 본 논문에서 제안한 방법에 따른 트래픽 암호 키 갱신 시각 계산을 나타낸 예시도이다. 그림 6에 도시된 바와 같이, CM은 CM 등록 절차 중 타임 스탬프 값이 57이 될 때, 키 요청 메시지를 사용해 CMTS에 TEK를 요청한다고 가정한다. 그 다음 CMTS는 암호화된 두 개의 TEK(TEK1, TEK2)를 생성하고, 생성된 TEK들을 키 응답 메시지를 통해 타임 스탬프 값이 예를 들어, 65가 될 때 해당 CM에 전달한다. 이때, 두 개의 TEK를 생성하는 것은, 키 사용의 연속성을 좋게 하기 위함이다. 이는 닥시스 규격에 이미 정의되어 있는 사항으로 본 논문에서는 상세한 설명을 생략하기로 한다.

CMTS가 키 응답 메시지에 TEK들을 포함하여 CM에 전달할 때, 타임 스탬프 값인 D_{active} 값도 함께 포함하여 전달한다. 여기서 D_{active}는 TEK 사용 기간(TEK active time period)을 의미한다. CM은 타임 스탬프 값이 65가 될 때 키 응답 메시지를 수신하고, 해당 메시지 내에 포함된 암호화되어 있는 TEK1과 TEK2를 복호화한 후 닥시스 트래픽 복호화에 순서대로 사용한다. 이때, TEK1과 TEK2 중 닥시스 데이터 트래픽 복호화에 사용될 TEK는 닥시스 MAC 패킷 헤더에 포함된 키 시퀀스(KEY_SEQ) 필드 값과 토글(TOGGLE) 필드 값을 이용해 구분한다. 여기서 CM에 키 응답 메시지가 도착하는 시각을 $T_{KeyReply}$로 정의한다.

CM은 TEK1과 TEK2를 사용하다가, TEK2의 사용 기간이 만료되기 전에 끊김없이 트래픽 암호화 서비스를 제공하기 위해 CMTS에 새로운 TEK를 요청해야 한다. 다시 말해, CM이 TEK1을 이용하여 암호화된 데이터를 복호화하다가, TEK1의 사용 만료 시각이 도래하면 바로 TEK2를 이용하여 데이터를 복호화한다. 그리고 TEK2를 이용하여 데이터를 복호화하면서 TEK2의 사용 기간이 만료되기 전에 새로운 TEK를 요청해야 한다. 이 요청 시점을 $T_{InitUpdate}$ 즉, TEK 갱신 시간(rekeying time)으로 명명하며, 식 (1)을 통해 계산할 수 있다. 식 (1)은 TEK를 최초로 갱신할 때 사용한다.

$$T_{InitUpdate} = T_{KeyReply}[+]2D_{active}[-]\frac{O_i}{2}[-]\Delta_{grace} \quad (1)$$

여기서 "A[+]B"와 "A[-]B"는 타임 스탬프 값이 A인 위치에서 각각 B만큼 앞 또는 뒤로 이동하라는 것을 의미한다. 또한 Δ_{grace}는 TEK 사용 만료 시각으로부터 CM이 실제로 새로운 TEK를 요청하는 시점까지의 시간 차이를 나타낸다. O_i는 i번째 CM의 타임 옵셋 값을 의미한다.

식 (1)을 그림 6에 예시된 바에 따라 $T_{KeyReply}$는 65, D_{active}는 250, O_i는 그림 3에서 계산한 바를 예로 하여 6, Δ_{grace}는 TEK 사용 만료 시각 565로부터 TEK 요청 시점인 515까지의 시간 차이인 50으로 설정하여 계산한다면, $T_{InitUpdate}$는 512가 됨을 알 수 있다. 따라서, CM은 타임 스탬프 값이 512가 되는 시점에 CMTS에 새로운 TEK의 발급 절차를 수행한다.

CM의 타임 스탬프 값이 $T_{InitUpdate}$가 되었을 때, CM은 TEK2를 해쉬 함수의 입력 값으로 취해 TEK3을 얻는다. 이후 닥시스 MAC 패킷 헤더에 있는 키 시퀀스 번호(Key sequence number) 값이 1만큼 증가된 닥시스 트래픽부터 새로 생성한 TEK3을 이용하여 복호화한다.

TEK3와 같이 최초로 TEK를 갱신하는 시각을 계산한 후의 나머지 모든 TEK들은 다음 식 (2)를 이용하여 갱신 시각을 계산한다.

$$T_{NxtUpdate} = T_{PrevUpdate}[+]D_{active} \quad (2)$$

여기서 $T_{PrevUpdate}$는 현재 닥시스 트래픽 복호화에 사용되고 있는 TEK를 갱신한 시점을 의미한다. 즉, 본 논문에서 제안한 방식에서는 식 (1)을 통해 계산된 512가 $T_{PrevUpdate}$가 된다. 이를 식 (2)에 적용한다면, D_{active} = 250이기 때문에, $T_{NxtUpdate}$는 762가 된다.

따라서, CM은 타임 스탬프 값이 762가 되는 시점에 TEK3를 해쉬 함수의 입력 값으로 취해 TEK4를 생성한다. 그리고 새로 생성된 TEK4는 타임 스탬프 값이 762 이후 닥시스 트래픽 패킷 헤더의 키 시퀀스 번호 값이 1만큼 증가된 트래픽에 대한 복호화에 사용된다.

4. TEK 생성 방법

본 논문에서 제안한 방법에서는 TEK를 갱신하기 위해 해쉬 함수를 사용한다. 그러나, 해쉬 함수를 이용해 새로운 암호화 키를 생성할 경우, 기존 TEK만을 입력 값으로 취할 경우 기존 TEK가 해킹될 때 새로 갱신된 모든 TEK들이 연달아 노출될 위험이 발생할 수 있다. 따라서, 이와 같은 보안 취약점을 막기 위해, 본 논문에서는 기존 TEK 이외에 AK, $T_{PrevUpdate}$, SAID, CM_ID를 또 다른 입력 값들로 취하여 식 (3)과 같이 갱신에 이용한다.

$$TEK_{old} = HASH(TEK_{old}, AK_i, T_{PrevUpdate}, SAID, CM\_ID) \quad (3)$$

따라서, 단순히 TEK 한 개에 대한 정보가 누출되었다고 하더라도, 이후 갱신될 모든 TEK들을 알아내는 것은 불가능하다. 경우에 따라서는 AK 대신 UGK(User Group Key)를 기존 TEK와 함께 해쉬 함수의 입력 값으로 사용할 수도 있다. AK를 사용

하는 경우는 CMTS가 CM으로 유니캐스트(unicast) 서비스를 제공하는 경우이고, UGK를 사용하는 경우는 그룹 멀티캐스트(group multicast) 서비스를 제공하는 경우이다.

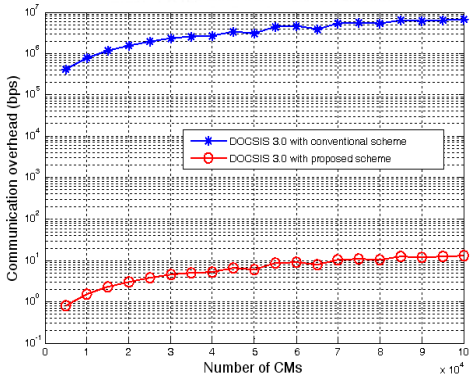
그림 6에서는 CM의 관점에서 TEK를 갱신하기 위한 시각을 계산하는 예를 설명하였으나, CMTS에서도 CM에서와 동일한 방법으로 TEK 갱신 시각을 계산하게 된다.

IV. 성능 평가

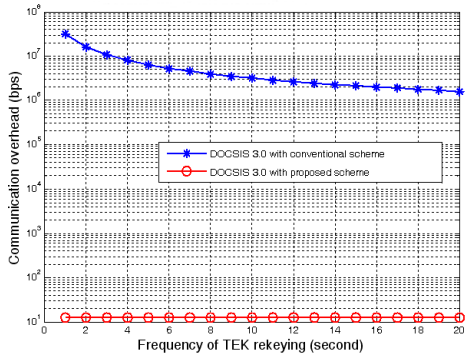
그림 7은 DOCSIS 3.0 with Conventional Scheme (DCS)와 DOCSIS 3.0 with Proposed Scheme (DPS)간 통신 오버헤드 (communication overhead)를 비교한 모의 실험 결과를 나타낸다. 본 모의 실험에서 가입자의 서비스 시작 시점과 서비스 유지 시간은 [17, 18]에서 설명한대로 각각 푸아송 분포 (Poisson distribution)[19]와 지수 함수 분포 (exponential distribution)[19]를 따른다. 모의 실험 결과에서 보듯, 제안한 기법인 DPS는 DOCSIS 3.0 보안 시스템 기반의 DCS 보다 통신 오버헤드 (communication overhead)가 매우 크게 줄어든 것을 확인할 수 있다. 예를 들어 그림 7 (a)의 경우, 현재 망에 운영 중인 CM의 개수가 100,000 개일때, DCS의 평균 통신 오버헤드 (communication overhead) 값은 약 6,730 Kbps인 것에 비해, DPS의 평균 통신 오버헤드 (communication overhead) 값이 약 0.012 Kbps에 불과하다. 그림 7의 경우, TEK의 갱신 주기를 1초로 설정했을 때 DCS의 평균 통신 오버헤드 (communication overhead) 값은 약 33,650 Kbps인 것에 비해, DPS의 평균 통신 오버헤드 (communication overhead) 값은 약 0.012 Kbps에 불과하다.

V. 결 론

본 논문에서는 IPTV 트래픽 암호화 키인 TEK에 대한 키 갱신 (rekeying) 주기를 MPEG 기반 CAS 수준인 1 ~ 20초 정도로 매우 짧게 하면서도 시스템 오버헤드(overhead)를 현재 DOCSIS 3.0 보안 시스템 보다 줄일 수 있는 기법을 제안했다. 제안 기법에서는 DOCSIS 시스템 시간 동기 기능과 해쉬(hash) 함수를 사용해 TEK 갱신 협의과정을 최초 1회만 수행하도록 해 빈번한 TEK 갱신 협의



(a) TEK 갱신 주기를 5초로 설정한 후 CM의 개수에 따른 통신 오버헤드 비교



(b) CM의 개수를 100,000으로 설정 한 후 TEK 갱신 주기에 따른 통신 오버헤드 비교

그림 7. 통신 오버헤드 비교
Fig. 7. Comparison of Communications Overhead

과정에 의한 시스템 오버헤드(overhead)가 발생되지 않도록 하였다. 또한 해쉬(hash) 함수 사용으로 인해 발생할 수 있는 보안 취약점은 해쉬(hash) 함수의 입력 값으로 TEK 뿐만 아니라 AK를 함께 취하도록 함으로써 해결하였다.

제안된 기법을 기존 DOCSIS 3.0 보안 시스템의 TEK 갱신 기법과 시스템 오버헤드(overhead) 관점에서 비교한 결과 현재 네트워크에서 운영 중인 CM의 개수가 100,000개 이고 TEK의 갱신 주기를 5초로 설정했을 경우, 제안한 방식의 평균 통신 오버헤드 (communication overhead) 값이 약 0.012 Kbps인 것에 비해 기존 DOCSIS 3.0 보안 시스템의 평균 통신 오버헤드 (communication overhead)

값은 약 6,730 Kbps 가 됨을 확인하였다. 또한, TEK의 갱신 주기를 1초로 설정했을 때 제안한 기법의 평균 통신 오버헤드 (communication overhead) 값은 약 0.012 Kbps인 것에 비해 DOCSIS 3.0 보안 시스템의 평균 통신 오버헤드 (communication overhead) 값은 약 33,650 Kbps 가 됨을 확인하였다.

참 고 문 헌

[1] Data-Over-Cable Service Interface Specifications DOCSIS3.0: Security Specification: CableLabs, CM-SP-SECv3.0-I07-080215, 2008.

[2] Data-Over-Cable Service Interface Specifications DOCSIS3.0: MAC and Upper Layer Protocol Interface Specification: CableLabs, CM-SP-MULPIv3.0-I07-080215, 2008.

[3] H. Abramson, "The Evolution to IPTV over DOCSIS® 3.0 and Modular-CMTS," in SCTE Cable-Tec EXPO 2007,2007.

[4] N. Ben-Natan, "IPTV: The Real Competitive Threat for Cable?," in SCTE 2006 Conference on Emerging Technologies, 2006.

[5] M. Patrick, "Architecture for Economic Deployment of IPTV with DOCSIS 3.0," in CableLabs, 2007 Winter Conference, 2007.

[6] M. Patrick and G. Joyce, "Delivering Economical IP Video over DOCSIS by Bypassing the M-CMTS with DIBA," in SCTE 2007 conference on Emerging Technologies, 2007.

[7] W. Cooper and G. Lovelace, "IPTV Guide: Delivering audio and video over broadband," Lovelace Consulting.

[8] EBU Project Group, "Functional model of a conditional access sytem," in EBU Technical Review Winter'95, 1995, pp.64-77.

[9] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broadcasting," in Proceedings of the IEEE, 1995, pp.944-957.

[10] M. Unbehaun and M. Scholz, "Key Design Issues for Efficient Broadcasting of Traffic Information Services," in Vehicular Technology Conference, 2007. VTC 2007 - Spring .IEEE 65th, 2007, pp.2496-2500.

[11] T. Yoshimura, "Conditional Access System for Digital Broadcasting in Japan," in Proceedings of IEEE,2006.

[12] M. Zhu, M. Zhang, X. Chen, D. Zhang, and Z. Huang, "A Hierarchical Key Distribution Scheme for Conditional Access System in DTV Broadcasting," in Computational Intelligenceand Security, 2006 International Conference on, 2006.

[13] F. K. Tu, C. S. Laih, and H. H. Tung, "On key distribution management for conditional access system onpay-TV system," Consumer Electronics, IEEE Transactionson, vol.45, pp.151-158, 1999.

[14] Cisco, "DOCSIS 1.0 Baseline Privacy on the Cisco CMTS," http://www.cisco.com

[15] Secure Hash Standard: NIST, FIPS PUB 180-2, 2003.

[16] C. Yang and C. Li, "Access control in a hierarchy using one-way hash functions," Computers & Security, vol.23, pp.659-664, 2004.

[17] K. C. Almeroth and M. H. Ammar, "Multicast group behavior in the Internet's multicast backbone (MBone)," Communications Magazine, IEEE, vol.35, pp.124-129, 1997.

[18] K. C. Almeroth and M. H. Ammar, "Collecting and modeling the join/leave behavior of multicast group members in the mbone," in Proc.ofHPDC,1996,pp.209-216.

[19] A. Leon-Garcia, Probability and Random Processes For EE's : Prentice-Hall ,Inc. Upper Saddle River, NJ, USA, 2007.

저 자 소 개

구 한 승 (Han-Seung Koo)

1999년 2월 : 충남대학교 전자공학과 학사
2001년 2월 : 충남대학교 전자 공학과 석사
2008년 8월 : 충남대학교 전자공학과 박사
2001년~현재 : 한국전자통신연구원 (ETRI)
관심분야 : 디지털 방송 보안, 멀티캐스트 키 관리
Email : koohs@etri.re.kr

이 진 환 (Jin-Hwan Lee)

1987년 2월 : 한국항공대학교 통신공학과 학사
2002년 2월 : 한국정보통신대학 통신공학과 석사
1989년~현재 : 한국전자통연구원 (ETRI) 책임연구원
관심분야 : 디지털방송시스템, 제한수신시스템
Email : jinhwan@etri.re.kr

송 윤 정 (Yun-Jeong Song)

1987년 2월: 경북대학교 공과대학 전자공학과 (공학사)
1990년 8월: 경북대학교 공과대학 전자공학과 (공학석사)
2004년 2월: 충남대학교 전자공학과 (공학박사)
1990년 7월 ~ 현재: 한국전자통신연구원 책임연구원
관심분야 디지털 신호처리, 디지털 모뎀, 방송시스템
Email : yjsong@etri.re.kr

권 오 형 (O-Hyung Kwon)

1981년 2월 : 서강대학교 전자공학과 학사
1983년 2월 : 서강대학교 전자공학과 석사
2004년 : 서강대학교 전자공학과 박사
1983년~현재 : 한국전자통신연구원 (ETRI) 팀장
관심분야 : 디지털케이블방송, DCAS
Email : ohkwon@etri.re.kr

이 수 인 (Soo In Lee)

1987년 2월 : 경북대학교 전자공학과 학사
1989년 2월 : 경북대학교 전자공학과 석사
1996년 2월 : 경북대학교 전자공학과 박사
1990년~현재 : 한국전자통연구원(ETRI) 부장
관심분야 : CATV, DTV, DMB
Email : silee@etri.re.kr