제한수신시스템을 위한 키 관리 메카니즘과 성능향상 방안

조 현 숙† · 이 상 호††

요 약

이 논문에서는 제한수신시스템의 일반구조 및 암/복호화에 사용되는 키의 안전성을 위한 키관리 메카니즘 그리고 시스템 성능 향상을 위한 키 계층 구조의 개선에 대해서 살펴본다. 또한 시스템 성능 분석을 위한 기본 개념으로 큐잉 이론(queuing theory)을 설명하고, 디지털 방송 유료화 서비스의 실현 및 시스템 성능 향상을 위한 시스템 최적화 방안으로서 몇 가지 산정된 자료률 기초로 하여 최적의 키 생성 및 전달 주기, 최적의 키관리 주기에 따른 최대/최소 키 전달 시간, 과금 데이터처리를 위한 전용선의 용량 및 시스템 용량을 산정 한다.

키워드 : 제한수신시스템, 제어 단어, 자격권한메시지, 자격관리메시지, 스크램블러/디스크램블러

A New Key Management Mechanism and Performance Improvement for Conditional Access System

Hyun-Sook Cho† · Sang-Ho Lee††

ABSTRACT

The Conditional Access System is the complete system for ensuring that broadcasting services are only accessible to those who are entitled to receive them. Four major parts to this system are scrambling, descrambling, authentication and encryption. For the proper operation, which means hard-to-break and uninterrupted service, secure key management and efficient delivery mechanism are very important design factors to this system. Performance analysis is another important factor to this system that is used in massive subscriber environment. In this thesis, one of the secure and efficient key management mechanisms is proposed. For the secrecy of this mechanism, hierarchical stacking of keys and key generation matrix are proposed. For the proof of efficient delivery of those keys, simulation results and performance analysis, which is based on queuing analysis, are presented. Lastly, optimal key generation and delivery period, maximal and minimal key deliver time, and communication capacity for data collection are presented for various subscriber volume.

Key word : Conditional Access System(CAS), Control Word(CW), Entitlement Contol Message(ECM), Entitlement Management Message(EMM), Scrambler/Discrambler

1. 서 론

방송에서의 제한수신시스템(CAS : Conditional Access System)이란 송신기에서 스크램블된 신호를 수신측의 수신 권한을 받은 가입자만 프로그램을 시청할 수 있도록 하는 시스템으로, 신호의 질을 손상시키지 않고 스크램블링(scrambling)/디스크램블링(descrambling)하는 과정은 아날로그 신호보다는 디지털에서 더 간단하기 때문에 일반적으로 제한수신 방송시스템으로 디지털을 이용한다.

디지탈 TV 방송에서의 제한수신시스템의 기본 요건은 첫째로, 프로그램 및 데이터는 통신 연결상태에서 미가입자의 불법 도/시청을 막을 수 있도록 보호되어야 하며, 둘째로 시청료를 지불한 정당한 가입자만이 프로그램을 시청할 수 있도록 가입자 신분 확인(authentication)기능과 접근 제어(access control) 기능이 있어야 한다. 언급된 두 가지 기능은 결국 자원(프로그램 및 데이타)과 가입자 보호를 위한 것으로, 자원의 보호메카니즘으로는 스크램블링/디스크램블링이 있고, 가입자 보호메카니즘으로는 인가된 가입자들에게 해당 시청 자격(entitlement)을 주는 기술이 있다. 자격은 프로그램 및 데이타의 스크램블링에 필요한 관련 파라메터와 수신자의 시청 권리를 말하며 자격통제와 자격관리로 대별할 수 있다.

스크램블링 및 디스크램블링 기능, 인증 기술을 이용한 가입자 신분 확인 기능, 그리고 접근 제어 기능들이 제한수신 방송시스템을 실현하기 위한 핵심 기술들이다. 제한수신 시스템을 실현하기 위해서는 스크램블링 및 디스크램블링을 위한 관련 파라메터들은 암호학적으로 안전한 알고리즘을 사용하여 수신단으로 안전하게 전달되어야 한다. 방송망에 적용 가능한 제한수신은 크게 스크램블러(scrambler)의 비밀키인 제어워드(CW : Control Word)를 분배하는 기능과 제어단어를 암호화하여 전달하는데 이용되는 인증키(AK :

† 정 회 원 : 한국전자통신연구원 정보보호기술연구본부장
†† 종신회원 : 충북대학교 컴퓨터과학과 교수
논문접수 : 2000년 10월 9일, 심사완료 : 2001년 1월 16일

Authentication Key)를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현된다. 제어단어를 인증키로 암호화하여 방송수신측에 전달하는 메시지를 자격통제메시지(ECM : Entitlement Control Message)라고 하고, 인증키를 전달하는 위한 메시지를 자격관리메세지(EMM : Entitlement Management Message)라고 한다.

기존의 케이블방송 제한수신시스템은 케이블에 연결되어 있는 사용자만이 비디오 및 오디오 신호를 수신할 수 있고, 별도의 셋톱 박스를 부가하여 특정 프로그램의 액세스를 제한하며, 사용자의 액세스 빈도를 저장하는 계수기를 포함하여 과금을 처리하고, 교환기가 사용자의 요구에 응하여 선택적으로 프로그램을 분배한다는 원칙 하에 설계되었다. 또한 비용의 절감, 세계 시장 규모의 확대, 장비의 호환성 등의 이유 때문에 각 나라뿐만 아니라, 국제적 표준안을 규정 및 연구해가고 있다.

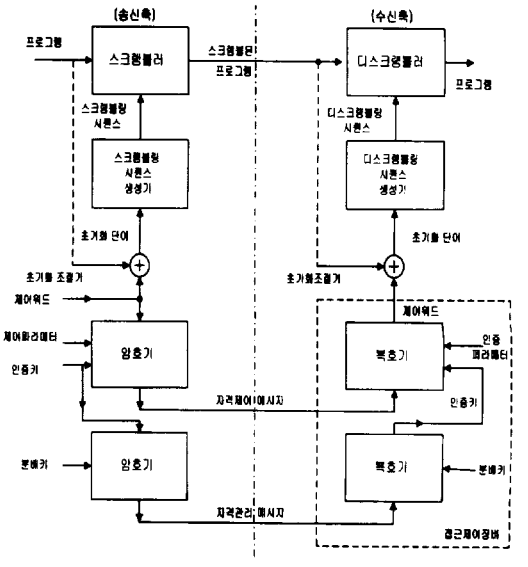
본 논문의 제2장에서는 제한수신시스템의 일반 구조 및 암/복호화에 사용되는 키를 효율적으로 생성 - 사용하기 위한 안전한 키관리 메커니즘의 설계에 대해 살펴보도록 한다. 제3장에서는 성능 향상을 위해 제안한 키 계층을 설명하며, 제4장에서는 시스템 성능 분석을 위한 기본 개념으로 큐잉 이론(queuing theory)을 설명하고, 제5장에서 디지털 방송 유료화 서비스의 실현 및 시스템 성능 향상을 위한 시스템 최적화 방안으로서 몇 가지 산정된 자료를 기초로 하여 최적의 키 생성 및 전달 주기, 최적의 키관리 주기에 따른 최대/최소 키 전달 시간, 과금 데이터처리를 위한 전용선의 용량 및 시스템 용량을 산정한다. 그런 이후 마지막 제6장에서 간단한 결론을 맺는다.

2. 제한수신시스템의 일반구조 및 성능 향상을 위한 키 계층

제한수신시스템이 갖추어야 하는 기본적인 요건은 첫째로, 시청료를 지불한 정당한 가입자만이 프로그램을 시청할 수 있어야 하고, 둘째, 미가입자의 불법 도/시청을 막을 수 있는 스크램블링의 강도가 높아야될 뿐만 아니라, 디스클램블링에 필요한 키를 알아내는 것을 막을 수 있어야 한다.

2.1. 제한수신시스템의 일반기능 및 구조

(그림 1)은 제한수신시스템의 일반적 구성을 도시한 것이다. 디스크램블링은 스크램블링된 프로그램을 원래의 신호대로 복원하는 과정을 말하며, 제어워드라는 파라미터를 가진 수신기들에서만 디스크램블된 프로그램의 시청이 가능하다. 스크램블링의 안전도는 스크램블링을 위해서 생성되는 의사난수열의 안전도에 의존하며, 디지탈 신호를 스크램블링하기 위해서 블럭 암호화 같은 방법이 사용될 수 있으나, 스크램블링의 가장 쉽고 빠른 방법은 PRBS(Pseudo Ran-



(그림 1) 제한수신시스템의 일반적인 구조

dom Bit Sequences)생성기에 의해 생성된 PRBS에 XOR하는 방법이다. PRBS 생성기에 초기 데이타는 제어단어와 주기계수기로 만들어지며, 이 제어단어는 스크램블러와 인가된 디스크램블러들에게만 알려진 비밀 파라메터이다.

프로그램을 디스크램블하기 위해 필요로 한 권한과 관련 키들을 자격이라 한다. 이 기능은 암호화된 제어워드들과 프로그램을 접근하기 위해 필요로 한 요구 조건들을 분배, 즉 난수 발생의 초기치인 제어워드를 암호화하고 그 제어워드를 자격통제메시지를 통해 전송한다.

수신기는 이 ECM을 받게되면, 암호화된 제어단어와 제어조건들을 스마트카드라고 하는 보안장치(security device)로 보내게 되어, 스마트카드는 먼저 합당한 데이터인지를 체크한 후 제어단어를 복호화하여 디스크램블러로 보내게 되며, 가입자는 디스크램블된 프로그램을 시청할 수 있다. ECM은 보통 한 개의 패킷으로 구성되어 주기적으로 전송되며, 그때마다 새로운 제어단어가 암호화되어 전송된다. 제어단어를 주기적으로 바꾸는 이유는 스크램블링의 의사난수의 규칙성을 찾을 수 없도록 하여 비화도를 높이려는 것이다.

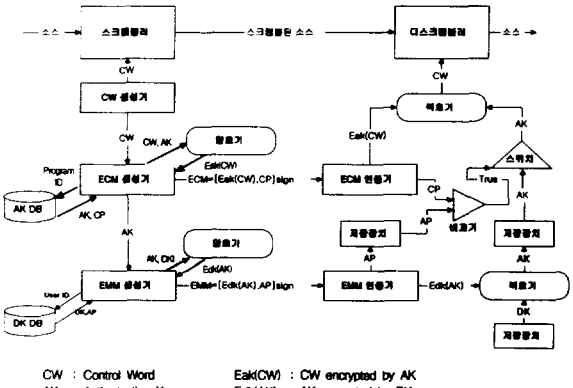
ECM 내에는 암호화된 제어단어외에 프로그램 정보와 접근 파라메터도 함께 전송된다. 모든 수신기는 전송된 자격통제 메시지를 수신할 수 있으며, 그중 제어단어와 접근 파라메터를 수신기와 접속된 스마트 카드로 전달하고, 스마트 카드에서는 프로그램 취득 조건 및 자격을 심사한 후 정당한 수신자로 판명되면, 스마트 카드내의 서비스 키를 이용하여 제어단어를 해독하고 디스크램블에 필요한 난수의 초기치를 발생한다. 자격 통제 메시지의 송/수신은 ECM의 주기 계수기에 의해 방송될 프로그램과 동기화된다.

가입자들에게 자격을 전달하는 기능은 EMM에 실어서 보낸다. EMM은 수신기의 보안장치인 스마트카드내에 자격

〈표 1〉 제한수신시스템 구성요소의 특징

	명 칭	특 징
송신부	스크램블러	• 대표적인 예가 PRBS(Pseudo Random Bit Sequences)를 이용하는 것. • PRBS는 초기화워드에 의하여 초기화되어 임의의 비트열을 발생. • PRBS에서 생성된 비트열과 소스의 비트열을 혼합함.
	초기화워드 생성기	• 제어워드와 소스에서 추출한 Clock 정보에 의하여 조종됨 • PRBS는 제어워드만으로도 초기화 될 수 있으며, 제어워드+클럭정보를 이용하여도 가능
	제어워드 생성기	• 스크램블러와 디스크램블러를 조종하는데 기준이 되는 정보를 발생시킴. • 제어워드의 짧은 생성주기는 허가 없이 디스크램블링할 수 있는 가능성을 줄여줌
	ECM 생성기	• ECM생성기는 프로그램별로 인증키를 가지고 있는 인증키 DB에서 해당 프로그램에 대한 인증키를 넘겨받아 암호기를 이용하여 암호화. • ECM은 또한 수신측의 수신조건과 비교하여 맞는 조건을 가진 수신기만이 해독할 수 있도록 전자서명을 첨가하여 구성.
	암호기	• 특정한 데이터를 어떤 키에 의하여 암호화하는 장치. • ECM의 경우 데이터는 제어워드, 키는 인증키, 키는 분배 키가 된다.
	인증키 DB	• 인증키 DB는 각 프로그램에 할당된 인증키와 제어 파라미터를 저장하는 곳으로 ECM 생성기에 의하여 검색.
	분배키 DB	• 분배키 DB는 각 수신기에 할당된 분배키와 인증 파라미터를 저장하는 곳으로 EMM 생성기에 의하여 검색.
수신부	ECM 인증기	• ECM 인증은 전자서명을 확인하여 송신기에 보낸 메시지임을 확인. • ECM중 암호화된 제어워드와 제어 파라미터를 분리하여 제어 워드는 복호기로 제어 파라미터는 비교기로 보냄.
	EMM 인증기	• EMM 인증은 전자서명을 확인하여 송신기에 보낸 메시임을 확인. • EMM 중 암호화된 분배 키와 인증 파라미터를 분리하여 분배 키는 복호기로 인증 파라미터는 저장장치로부터 분배 키를 넘겨받아 해독한 다음 인증키를 저장하는 기억장치로 넘김.
	복호기	• 특정한 데이터를 어떤 키에 의하여 해독하는 장치로 ECM의 경우 데이터는 암호화된 제어워드, 키는 인증키가 되고 EMM의 경우 데이터는 암호화된 인증키, 키는 분배 키가 됨.
	저장장치	• 키 또는 인증 파라미터를 기억하는 장치.
	비교기	• EMM으로 전송되어 온 인증 파라미터와 ECM으로 전송되어 온 제어 파라미터를 비교하여 참인 경우 인증키 전송 스위치를 동작.
	스위치	• 저장장치에 저장된 인증키를 ECM 복호기에 전달하는 중간과정. • 비교기에 나온 결과값이 '참' 일때만 ECM 복호기로 키를 전달.
	디스크램블러	• 스크램블된 신호를 원래의 상태로 환원시키는 장치.

을 부여하거나 갱신하는 기능을 지원하며, 각 수신자의 주소에 의한 인식 기능을 이용하여 수신자의 서비스 키를 바꾸거나 통제하는 통제 취득기능의 지원도 가능하다. 자격관리기능은 앞으로 시청할 프로그램의 수신자격에 대한 정보관리 기능이므로 일괄 동작으로 실행된다. 따라서, 전송할 프로그램과 동기화되어 전달될 필요는 없으며, EMM을 형성하여 특수 채널을 통해 방송되거나 우편등의 매체로도 전달 가능하다.



(그림 2) 제한수신시스템의 논리적인 구조

언급된 ECM과 EMM 안전한 전송 및 관리를 위해 비밀키와 암호화 알고리즘이 요구되며, 근래에 설계된 대부분의 제한수신시스템은 정보를 안전하게 저장하고 수행하기 위해 보통 스마트카드를 사용하고 있다.

(그림 2)는 (그림 1)의 일반적인 구조를 방송 환경에서의 구현을 위해 논리적으로 표현한 구조이며, 이에 대한 각 구성요소의 특징1은 <표 1>과 같다.

2.2 제한수신시스템의 키관리

제한 수신 시스템 키관리에 중점을 두는 점은 새로운 가입자의 추가나 기존 가입자의 삭제를 용이하게 하고 가입자 증가에 따른 메시지의 증가를 최소화하는 것이다. 이를 위해서는 서비스 및 과금 형태에 따라 그룹을 형성하고 키를 공유해야 한다. 따라서 공유되는 그룹키(GK : Group Key)의 갱신 및 그룹내에서 특정 가입자의 삭제는 문제시 될 수 있다. 가입자의 추가 및 삭제의 용이함을 위해서 키의 체계를 계층적 단계를 두고 분배하는 것이 효율적이다. 즉 실제 서비스 요소는 각 그룹별로 그룹키로 암호화하고 자격을 가진 가입자들에게 해당 그룹키를 각 가입자의 고유한 개인키를 이용하여 암호화하여 전달하는 것이다. 가입자의 추가시에는 새로운 가입자에게만 그룹 키를 전달하면 되므로 메시지 증가의 부담이 크게 감소한다. 특정 그룹에

서 가입자의 삭제는 그룹이 공유하는 그룹키를 갱신함으로서 용이하게 해결할 수 있다.

키 분배시 사용되는 알고리즘은 관용키 알고리즘과 공개키 알고리즘 모두 사용될 수 있으며 관용키 알고리즘을 사용할 경우에는 가입자는 자신이 가입한 모든 방송국과의 비밀키를 유지해야 하며 이는 새로운 방송국에 가입하고자 할 때 스마트 카드에 새로운 정보를 입력해야 한다. 모든 방송국이 가입자의 마스터키를 공유할 수 있으나 보안상 취약할 수 있으므로 방송국의 안전성이 요구된다. 공개키를 사용할 경우에는 사용자는 자신의 스마트 카드에 단지 자신의 비밀키만을 보관하고 방송국들에게는 사용자의 가입 여부에 따라 사용자의 공개키를 유지하여 마스터키로서 사용하면 된다.

키 관리 시스템은 4개의 계층으로 구성되며 상위 계층부터 제어단어(control word), 개인키(Private key), 분배키(distribution key), 마스터키(master key)의 순서로 구성된다. 각 키는 자신의 상위 키를 암호화하여 분배하는데 사용되며 역할 및 특징은 <표 2>와 같다.

〈표 2〉 제한수신시스템의 키 계층 구조

키 종류	갱신기간 (권고)	특 징
Control Word (CW)	10초 이내	• 프로그램을 스크램블링 하기 위하여 사용되며 서비스 채널별로 고유. • 높은 안전성을 위해 제어단어(CW)는 ECM을 이용해 짧은 주기 매번 갱신.
Private Key (PK)	1~ 3개월	• 개인 키(PK)는 제어단어의 암호화에 사용되며 가입자의 그룹 형성에 따라 각 가입자에게 고유하거나 각 그룹에 고유. • 사용자에게는 비밀로 유지되며EMM을 이용해서 갱신.
Distribution Key (DK)	5분~ 24시간	• 분배키(DK)는 개인키의 암호화에 사용되며 가입자의 그룹 형성에 따라 개인 키 와 그룹 키로 구분(개인키는 가입자 주소로 식별되는 각 가입자에게 고유하며 그룹 키는 그룹 주소로 식별되는 개별 그룹에 고유) • 키는 스마트 카드내에 저장되며 EMM을 이용해 갱신.
Master Key (MK)	변경되지 않음	• 마스터키는 분배키의 암호화에 사용되며 각 가입자마다 고유. • 스마트카드의 라이프 싸이클(life cycle) 동안 변경 무.

2.3 제한 수신 시스템 키 분배 절차

키 분배 절차는 마스터키의 발급, 분배키 및 인증키 분배 그리고 제어단어 분배의 절차로 행해진다.

2.3.1 마스터키 발급

가입자가 스마트 카드를 발급 받으면 스마트 카드 내에는 라이프 싸이클 동안 변하지 않는 마스터키가 저장되어 있으며 가입자가 등록한 방송국은 이와 동일한 마스터키를 관리 해야 한다. 마스터키는 분배키의 분배/갱신과 과금 정보의 보호에 사용된다.

2.3.2 분배키 분배

분배키는 그룹 키와 개인 키로 구분되며 인증 키의 암호화에 사용되며, 가입자가 처음 가입시 EMM을 이용하여 획득하고, 그룹내의 가입자 변동시에도 이요된다. 이 메시지 내에는 메시지의 무결성을 위한 단방향 해쉬 함수 값인 H를 포함한다. 가입자는 방송된 EMM 메시지를 수신하여 자신의 마스터키로 메시지를 복호화 하고 해쉬 함수로 해쉬 값 H를 생성하여 전송되어온 값과 비교한 후 분배키를 획득한다.

2.3.3 인증키 분배

인증 키는 제어단어의 보호를 위해 사용되며 서비스 채널별로 고유하다. 프로그램 방송시 개별 가입자 또는 가입자 그룹에 대하여 분배키로 암호화되어 EMM에 실려 방송된다. 가입자는 EMM을 수신하면 이미 획득된 자신의 분배키로 메시지를 복호화하고 해쉬 값을 생성하여 수신된 값과 비교하여 검증한 후 인증 키를 획득한다.

2.3.4 제어단어 분배

제어단어는 실제 방송 프로그램을 스크램블링 하는데 사용되며 유료 채널 별로 고유하고 방송시 ECM에 실려 방송된다. 가입자들은 이미 분배된 인증 키로 이 메시지를 복호화 한 후 제어단어를 획득하여 스크램블된 프로그램을 디스크램블 하는데 사용한다.

2.4 제한수신엔진과 스마트 카드

제한 수신 시스템은 스크램블링/디스크램블링 기능과 자격 관리 및 자격 제어 기능이 필요함을 이미 설명한 바 있다. 일반적으로 송신측의 스크램블링은 하드웨어 장비로 실현되며 디스크램블링 기능은 수신기 즉, 셋톱박스 내의 하나의 칩으로 구현된다. 자격 제어와 자격 관리는 송신측에서는 제한 수신 엔진과 수신측에서는 스마트 카드가 각각 그 기능을 수행하게 된다

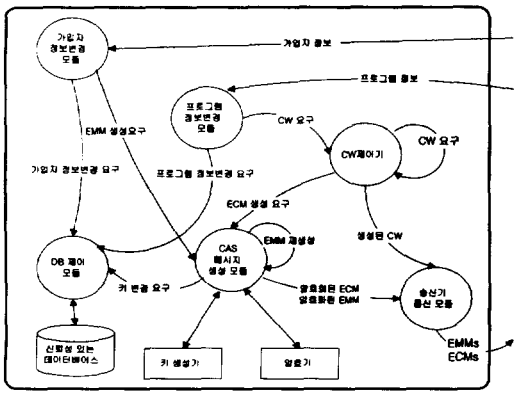
2.4.1 제한 수신 엔진

제한 수신 엔진내의 데이터베이스는 안전하게 운용되어야 하며, 여기에는 개인 키를 포함하는 가입자 정보와 직접 권한 키를 포함하는 유료 채널 프로그램 정보 및 가입자가 가입하는 그룹 키 정보 등을 저장하고 관리한다. 키 생성 모듈은 자격 관리와 자격 제어에 필요한 암호 키를 생성하는 역할을 담당하며, 암호화 모듈은 EMM과 ECM의 암호화 서비스를 제공한다.

가입자 정보 변경 모듈(SUM : Subscriber Update Module)은 외부의 가입자 관리시스템(SMS : Subscriber Management System)으로부터 가입자 정보를 받아서 키의 생성이 필요한 경우 키를 생성하고 이를 DB 제어 모듈(DAM :

Database Access Module)을 통해서 데이터베이스에 반영한다. DB 제어 모듈은 모든 키 정보를 유지 관리하고 다른 모듈로부터의 데이터베이스 조회 요구를 받는다. CAS 메시지 생성 모듈(CGM : CAS Message Generation Module)은 가입자 정보 변경 모듈로부터 EMM 생성 요구를 받아서 데이터베이스 내의 가입자에 해당하는 분배키 즉, 개인키(PK) 또는 그룹 키(GK)를 조회하여 이를 근거로 암호화된 EMM을 생성하고 송신기 통신 모듈(TCM : Transmitter Communication Module)로 전달하고, 해당 그룹내의 인증 키로 동작하는 직접권한 키(DEK, Direct Entitlement Key)의 주기적인 변경을 위하여 스스로 EMM 재생성 요구를 활성화한다.

프로그램 정보 변경 모듈(PUM : Program Update Module)은 유료프로그램 정보를 수신하면 동작되는 모듈로 해당 프로그램 정보를 데이터베이스에 저장하고 제어단어 생성 모듈(CWG : CW Generation Module)에게 제어단어의 생성을 요구한다. 이 요구를 수신한 제어단어 생성 모듈은 생성한 제어단어를 스크램블러에게 전달하기 위하여 송신기 통신 모듈로 전송함과 동시에 제한수신 메시지 생성 모듈에 인증키를 이용한 제어단어의 암호화 과정인 ECM 생성을 요구한다. 제어단어는 새로운 프로그램의 생성시 또는 주기적으로 변경되어야 하므로 제어단어 생성 모듈은 이를 주기적으로 활성화하는 역할도 수행한다. 송신기 통신 모듈은 제한 수신 엔진과 송신기 사이의 통신 기능을 담당하여 모든 제한 수신 메시지를 송신기에 전달한다. 이들에 대한 자료 흐름은 (그림 3)과 같다.

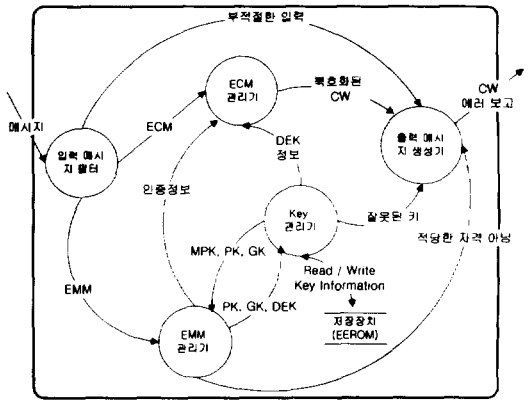


(그림 3) 제한수신엔진의 자료흐름

2.4.2 스마트 카드

스마트카드는 카드 칩 운영체제(COS : Chip Operating System)에 의해 운용되며 외부로부터의 제한적인 메시지의 해석과 동작만을 허용하는 tamper-resident한 장치이다.

입력 메시지 필터는 수신기로부터의 입력을 받아서 해당 명령이 적합한 메시지임을 판단하여, 부적절한 메시지인 경우에는 출력 메시지 생성기를 통해 에러를 출력하고 적절한 메시지인 경우에만 EMM 관리기 및 ECM 관리기로 분기한다. EMM 관리기는 입력 메시지 필터로부터의 EMM을 Key 관리기로부터의 스마트 카드의 비활성 메모리에 저장되어 있는 분배키인 개인키와 그룹 키를 이용하여 해당 EMM을 해석하고 그룹 키 또는 직접권한 키 및 기타 정보를 재저장한다. 만약 해석 과정 중에 에러를 발견한 경우에는 해당 EMM을 버리고 자격에 에러가 있음을 출력 메시지 생성기를 통해 수신기에게 알린다. ECM을 수신한 ECM 관리기는 Key 관리기로부터의 직접 권한 키 정보를 읽어오고 이를 이용하여 복호화 과정을 거쳐서 정상적인 경우에 제어단어를 출력하여 출력 메시지 생성기를 통해 수신기에 전달한다. 비활성 메모리 영역에 저장되어 있는 키 관련 정보는 매우 안전하게 보관/관리되고 EMM에 의하여 주기적으로 변경되어야 하며 이 역할을 Key 관리기가 수행한다. 스마트 카드에서의 자세한 자료 흐름은 (그림 4)에 도시하였다.



(그림 4) 스마트카드의 자료 흐름

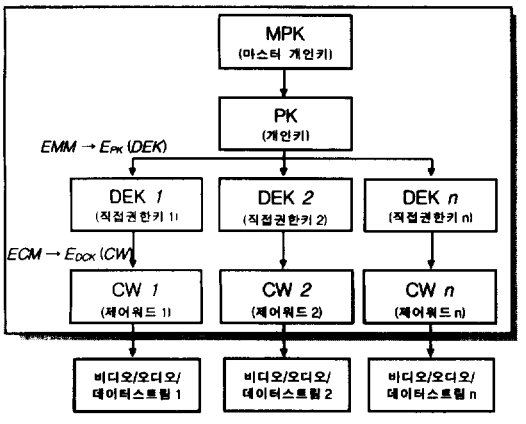
2.4.3 제한수신엔진과 스마트 카드와의 관계

제한 수신 엔진과 스마트 카드에서의 기능 대응 관계를 보면, 워크스테이션 이상에서 구현되는 송신측의 제한수신 엔진 보다는, 메모리 사용의 제약, 8비트 프로세서 능력의 한계, 저속의 입출력 속도 등의 취약점을 가진 스마트 카드를 안전하고 효율적으로 설계할 수 있느냐가 전체 제한 수신 시스템의 성능과 직결된다고 할 수 있다. 제한 수신 엔진과 스마트 카드의 구현을 위해서는 안전하다고 인지할 수 있는 만큼의 기간 내에 키의 갱신을 반영할 수 있어야 하고, 키의 변경 시에도 유료방송 서비스가 중단되어서는 안되며, 가입자가 키의 갱신을 인지할 수 없어야 한다. 또한 비용과 안전성에 대한 적절한 수준 등도 고려해야 하다.

3. 성능 향상을 위한 키 계층

제한 수신시스템에서는 일반적으로 분배키에 해당하는

개인키와 인증 키에 해당하는 직접 권한 키를 가지는 (그림 5)와 같은 키 계층 구조를 나타내고 있다. 이와 같은 키 계층 구조는 개개의 서비스 스트림 당 하나의 제어단어와 이를 암호화하기 위한 직접 권한키를 갖고 이들은 다시 개인키에 의해 제어되는 구조이다. 즉, 각 서비스 스트림은 채널로서 구분되며 채널의 데이터는 제어단어에 의해서 스크램블 된다. 제어단어는 직접 권한키로 암호화되며 ECM 메시지를 통해서 방송된다. 그러므로 각 채널의 ECM 메시지를 액세스하기 위해서는 직접 권한키의 액세스가 가능 해야만 한다. 또한 직접 권한키는 개인키로 암호화되어 EMM 메시지를 통하여 가입자에게 자격을 부여한다.

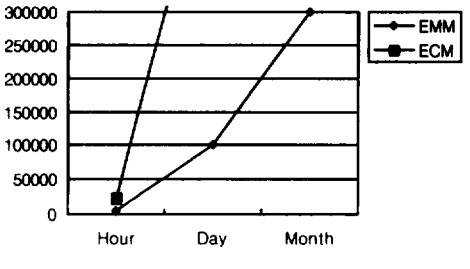


(그림 5) 일반적인 키 계층도

이와 같은 키 계층 구조는 모든 가입자 개개인에게 제어단어를 해석할 수 있는 직접 권한키를 전송하기 때문에 유료 채널의 수가 증가하고 가입자가 늘어날수록 CAS 메시지 양도 기하급수적으로 늘어날 것이다.

가입자에게 카드 발급 초기에 저장되는 마스터 개인키와 주기적 또는 가입자의 요구에 의해 주기적으로 변경하여야 하는 개인키는 모든 가입자에게 다른 키 값을 제공하여야 하며 채널 그룹에 할당되는 직접 권한 키는 그룹의 수만큼 필요하며 이는 ECM의 생성시 제어단어인 제어단어의 암호화에 사용되는 키로서 사용 빈도가 가장 높다.

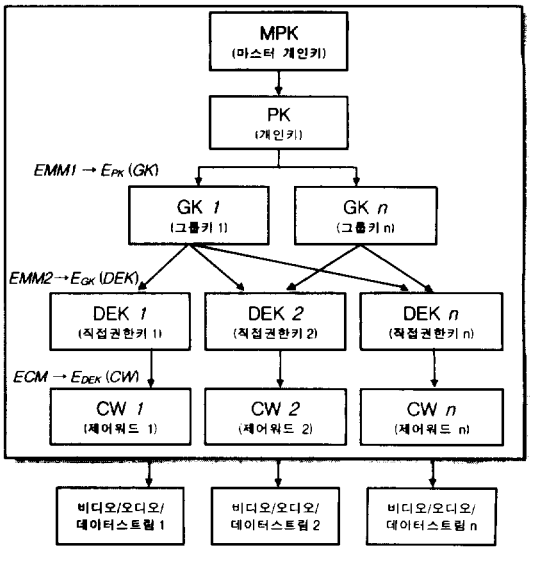
(그림 6)은 가입자 10만명을 기준으로 100개의 유료 채널이 운용되고 직접 권한키는 하루에 한번, 개인키는 한달에 한번 변경됨을 가정하였을 경우, 시간/하루/한달 기준으로 EMM과 ECM 메시지 양에 대한 계산치를 도시하였다.



(그림 6) 일반적인 키 계층 구조에서의 CAS 메시지량의 산출

제한 수신 시스템은 방송을 근간으로 하는 일방향 서비스로 전체 서비스 스트림의 일부만을 CAS메시지의 송신에 사용할 수 있는 제약이 있으므로 CAS메시지를 적게 생성할수록 시스템이 안정적이고 효율적이다. 즉 제한 수신 시스템의 성능 개선을 위해서는 기존의 구조에 비해 매우 적은 양의 CAS메시지만으로 서비스가 가능한 다음의 방식을 제안하고자 한다.

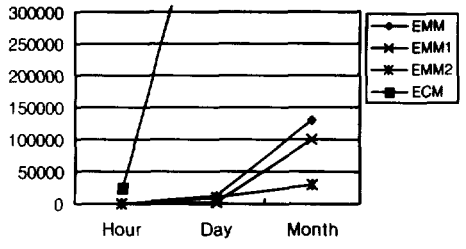
각 가입자는 자신의 개인키를 가지며 복수개의 서비스 그룹 키를 가질 수 있고, 이 그룹 키는 각 채널에 할당되는 여러 개의 직접 권한키를 가질 수 있으며 독립적인 직접 권한키는 여러 그룹 키에 중복되어 포함될 수 있으므로 두 단계의 EMM인 EMM1과 EMM2를 전송하지만 생성되는 CAS메시지 양은 현저히 줄일 수 있을 것이다. 이 구조를 (그림 7)에 도시하였다. EMM1은 그룹 키를 개인키로 암호화하여 전송하는 자격 관리 메시지를 의미하며, EMM2는 직접 권한키를 그룹 키로 암호화하여 전송하는 자격 관리 메시지로 두 단계의 EMM에 대한 식별자를 필요로 한다. 두 단계의 EMM을 모두 수신하고 해석한 스마트 카드는 최종적으로 직접 권한키로 암호화된 제어단어를 해독할 수 있다.



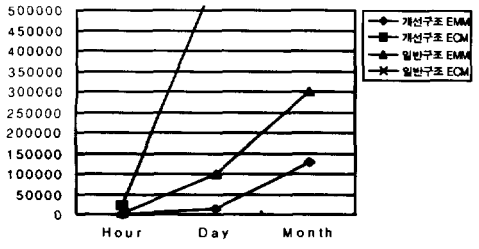
(그림 7) 성능 개선된 키 계층도

(그림 8)은 가입자 10만명을 기준으로 100개의 유료 채널이 운용되며 직접 권한키는 하루에 한번, 개인키는 한달에 한번 변경됨을 가정하였을 경우, 시간/하루/한달 기준으로 EMM과 ECM 메시지 양을 도시하였다.

(그림 6)과 (그림 8)에서는 동일한 양의 ECM이 발생하지만, (그림 9)에서 성능 개선된 키 구조에서의EMM 양은 이전의 키 구조에 비해서 절반 이하로 줄어듬을 알 수 있다. 이 결과는 단지 10만명의 가입자를 기준으로 계산한 값으



(그림 8) 성능 개선된 키 계층 구조에서의 CAS 메시지량의 산출



(그림 9) CAS 메시지 양에 대한 비교

로 실제 서비스 환경에서의 가입자의 수는 훨씬 더 많으며 이때의 CAS메시지 양은 더욱 더 증가할 것이다.

키의 사용 빈도에 따라서 키의 노출 가능성이 커지므로 키의 종류에 따른 생성 과정을 달리할 필요가 있을 것이다.

4. 큐잉 이론(Queuing Theory)

큐잉이론은 키 생성/전달 주기 산정, 최대/최소 키 전달 시간 산정, 시스템 용량 산정, 전용선 용량 산정을 하기 위해 이용된다. 본 장에서는 큐잉 이론 기본 개념을 설명한다.

통신에서 동기적 온라인이란 상대 개체가 통신 순간에 다른 통신 상대와 대면하는 것이다. 메시지를 통해서 통신이 구현되는 경우에, 메시지가 처리되기를 기다리며 대기하고 있는 곳을 큐(queue)라 한다. 큐는 버퍼 같은 일종의 저장 영역이다. 큐는 시스템 버퍼에 과부하를 막을 수 있으며, 기계나 네트웍이 다운되는 경우에도 안전하게 메시지를 저장할 수 있다는 장점이 있다. 이런 안전성에 대한 대가는 버퍼에 메시지를 쓰고 읽는데 따른 여분의 비용이다. 실시간 응용이나 상호연동성을 지닌 통신 시스템의 성능은 응답 시간과 시스템의 작업처리량에 기초를 둔다. 큐잉 이론은 각 패킷을 처리하는 시스템의 최대 지연시간을 줄이기 위한 간단한 방법과 시스템의 최대 성능을 제공한다.

큐잉 모델의 대표적인 형태는 단일서버큐잉(single server queue)모델과 멀티서버큐잉(multi server queue) 모델이 있다. 단일서버큐잉 시스템에서 도착된 아이템들은 대기열(waiting line)에 대기한다. 서버가 한 아이템에 대한 처리를 완수하면 아이템은 서버를 떠나게 된다.

<표 3>은 큐잉 모델에서 사용되는 기본적 파라미터가 표기되어 있다. 아이템들은 초당 평균 도착율 λ로 시스템에 도착한다. 어떤 정해진 시간 내에 몇 개의 아이템들이 대기열에서 대기한다. 서버는 평균 서비스 시간 s로 아이템을 처리한다. 이용률은 서버가 동작하는 시간과 s의 비율이다.

〈표 3〉 큐잉 분석을 위해 사용된 표기법

기호		의 미
λ	:	초당 아이템 도착 수
s	:	각 아이템의 평균 서비스 시간
σ_s	:	서비스 시간의 표준편차
ρ	:	이용률(utilization)
q	:	시스템 내에 존재하는 총 아이템의 평균 수
t_q	:	시스템 내에 아이템들의 평균 소비 시간
σ_q	:	q의 표준편차
σ_{tq}	:	t_q의 표준편차
w	:	서비스를 기다리는 아이템의 평균 대기 수
t_w	:	서비스를 기다리는 아이템의 평균 대기 시간
σ_w	:	w의 표준편차
M	:	서버들의 개수

도착율은 시스템을 통과하는 트래픽의 비율로서, 증가하게 되면 이용률이 증가하여 밀집 현상이 발생하며 대기열의 길이와 대기 시간이 증가한다. 이론적인 최대 입력율은 시스템에 의해 조정될 수 있으며 단일 서버인 경우에 λ값은 $\lambda_{max} = 1/s$ 이 된다.

대기열은 시스템이 거의 포화 상태에 이를 때까지 커질 수 있으므로, 응답 시간 요구나 버퍼 크기는 단일 서버인 경우에 이론적으로 입력률을 70~90%로 제한한다. 이 모델을 형성하기 위해 아이템 수와 대기열 크기는 무한하고 시스템에 도착되는 아이템들은 FIFO (First-In First-Out)를 기본 원칙으로 처리됨을 가정한다.

멀티서버 큐잉 모델의 경우에는 다양한 서버가 존재하고 대기열을 공유한다. 만일 아이템이 도착한다면 적어도 하나의 서버가 아이템을 처리하게 된다.

〈표 4〉 기본적 큐잉 관계

$\rho = \lambda s$	단일 서버에 의한
$\rho = \frac{\lambda s}{M}$	멀티 서버에 의한
$q = \lambda t_q$	
$w = \lambda t_w$	
$t_q = t_w + s$	
$q = w + \rho$	단일 서버에 의한
$q = w + M_\rho$	멀티 서버에 의한

하나의 서버가 자유롭게 되자마자 아이템은 대기열에서 서버로 dispatching discipline을 사용하여 강제적으로 이동하게 된다. 시스템에 M개의 독립적 서버가 존재한다면, ρ는 각 서버의 이용률을 나타내고 M_ρ는 전체 시스템의 이용률을 의미한다. 시스템에 유입될 수 있는 최대 입력률은 $\lambda_{max} = M/s$ 같이 된다.

큐잉 시스템에서 사용되는 파라메터들은 상호간에 밀접한 관계를 지닌다. 입력에 따라 도착율, 서비스 시간이 주어지고 출력 정보 관련에 따라 아이템 대기, 대기 시간, 아

이템 큐드, 큐잉 시간이 주어진다. <표 4>에서는 <표 3>에 나타나 있는 큐잉 분석을 위해 사용된 표기법에 따라 시스템 파라미터들간의 관계식을 기술한다.

주어진 문제의 도착율이 Poisson 분포를 갖고, 서비스 시간에 대한 확률 밀도 함수는 지수적으로 증가한다고 가정했을 때, 평균값 w, t_w, q, t_q이 주어지면 그에 따른 표준편차 $\sigma_q, \sigma_{tq}, \sigma_w, \sigma_{tw}$도 구할 수 있다.

4.1 단일 서버 큐의 관계식

서버의 서비스 시간은 일반적으로 세 가지 유형으로 (M/G/1, M/M/1, M/D/1) 나눌 수 있다. 여기에서 유형의 표기는 다음과 같은 의미를 지닌다.

X/Y/N X : 아이템간의 도착 시간 분포,
Y : 서비스 시간 분포,
N : 서버의 개수.
G : general independent arrivals or service times.
M : negative exponential distribution.
D : deterministic arrivals or fixed length service.

<표 5> 단일 서버 큐잉의 공식

(a) 지수(exponential) 서비스 시간(M/M/1)

$$q=\frac{\rho}{1-\rho},\qquad w=\frac{\rho^2}{1-\rho}$$

$$t_q=\frac{s}{1-\rho},\qquad t_w=\frac{\rho s}{1-\rho}$$

$$\sigma_q=\frac{\sqrt{\rho}}{1-\rho},\qquad \sigma_{tq}=\frac{s}{1-\rho}$$

$$\Pr[q=N]=(1-\rho)\rho^N$$

$$\Pr[q\le N]=\sum_{i=0}^{N}(1-\rho)\rho^i$$

$$\Pr[t_q\le t]=1-e^{-(1-\rho)t/s}$$

$$m_{tq}(r)=t_q\times\log_e\left(\frac{100}{100-r}\right)$$

$$m_{tw}(r)=\frac{t_w}{\rho}\times\log_e\left(\frac{100\rho}{100-r}\right)$$

(b) 상수(constant) 서비스 시간(M/D/1)

$$q=\frac{\rho^2}{2(1-\rho)}+\rho$$

$$w=\frac{\rho^2}{2(1-\rho)},\qquad t_q=\frac{s(2-\rho)}{2(1-\rho)}$$

$$t_w=\frac{\rho s}{2(1-\rho)},\qquad \sigma_q=\frac{1}{1-\rho}R$$

$$R=\sqrt{\rho-\frac{3\rho^2}{2}-\frac{5\rho^3}{6}-\frac{\rho^4}{12}}$$

$$\sigma_{tq}=\frac{s}{1-\rho}\sqrt{\frac{\rho}{3}-\frac{\rho^2}{12}}$$

<표 5>의 (a)에서 지수(exponential) 서비스 시간의 표준편차가 '0'인 경우에는 상수(constant) 서비스 시간과 동일하게 된다. <표 5>의 (b)는 상수 서비스 시간인 경우에 관계식이다. 본 논문에서는 M/M/1과 M/D/1 유형을 이용한다. 단, 각 세션별로 나누어 서비스하는 FQ(Fair Queuing)의 방법을 사용하지 않으며 아이템은 큐(대기열)에서 이탈하지 않는다고 가정한다.

4.2 멀티서버 큐의 관계식

<표 6>은 멀티서버 큐에 대한 공식이 나열되었다. 공식은 M/M/N의 경우에만 사용되며 지수 서비스 시간은 각 N개 서버들마다 동일한 시간을 갖는다. 멀티서버인 경우에 모든 서버에 균등하게 부하 되고 동일한 서비스 시간을 갖는다고 가정한다.

<표 6> (M/M/N)인 경우 멀티서버 큐잉의 공식

$$k=\left(\sum_{N=0}^{M-1}\frac{(M\rho)^N}{N!}\Big/\sum_{N=0}^{M}\frac{(M\rho)^N}{N!}\right)$$

: 모든 서버가 활동중인 경우에 대한 확률

$$B=\frac{1-K}{1-\rho K},\qquad q=B\frac{\rho}{1-\rho}+M\rho$$

$$w=B\frac{\rho}{1-\rho},\qquad t_q=\frac{B}{M}\frac{s}{1-\rho}+s$$

$$t_w=\frac{B}{M}\frac{s}{1-\rho}$$

$$\sigma_{tq}=\frac{s}{M(1-\rho)}\sqrt{B(2-B)+M^2(1-\rho)^2}$$

$$\Pr[t_w>t]=Be^{-M(1-\rho)t/s}$$

$$t_d=\frac{s}{M(1-\rho)}$$

5. 성능 향상을 위한 최적화 방안

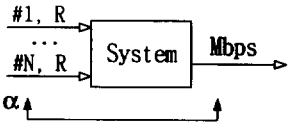
이번 장에서는 각 시스템 조건 및 입출력 채널 조건에 따라 최적의 키 생성/전달 주기와 키관리 주기에 따른 최대/최소 키 전달시간을 산정하고, 또한 과금 데이터 수집을 위한 최적의 시스템 용량 산정 및 최적의 전용선 용량을 산정한다.

5.1 최적의 키 생성/전달 주기와 키관리 주기에 따른 최대/최소 키 전달시간 산정

최적의 전용선 용량 결정은 큐잉 이론에 바탕을 두고 있다. 기본적으로 여기서 제시된 결과는 제한수신을 위한 결과이므로 트래픽 채널을 위한 데이터 속도가 더해짐을 가정한다. 전용선의 출력 용량 결정은 다중장치가 통계적 다중 장치라고 가정하고 분석하였다. 멀티플렉서는 수 개의 단말 장치가 고속의 한 회선을 공유할 수 있도록 지원하는 장치로서 회선 비용을 감소시켜주는 이점이 있으나 네트워크 지연에 원인이 될 정도로 응답 시간에 상당한 영향을 미친다. (그림 10)의 시스템 문제점은 입력량이 회선의 용량보다 더 많은 기간 동안 있을 수 있으므로, 임시의 초과입력을 견딜 수 있도록 시스템에 버퍼를 포함시켜야 한다는 점이다.

입력이 출력을 초과할 때 초과된 부분(backlog)은 버퍼에 저장된다. 비용을 최소화하기 위해 최소크기의 버퍼와 최소

크기의 데이터 전송률을 이용해야 한다. 그러나 두 구성 요소 중 한쪽 성분이 감소되면 다른 쪽 성분은 증가되므로 두 구성요소의 조율이 요구된다. 시스템에서 이루어지는 압축의 정도는 K로 표기한다. $\alpha < K < 1$ 인 경우에는 통계 시분할 멀티플렉서로 구성요소를 조율한다. $K < \alpha$ 인 경우에 입력은 멀티플렉서의 용량을 초과한다.

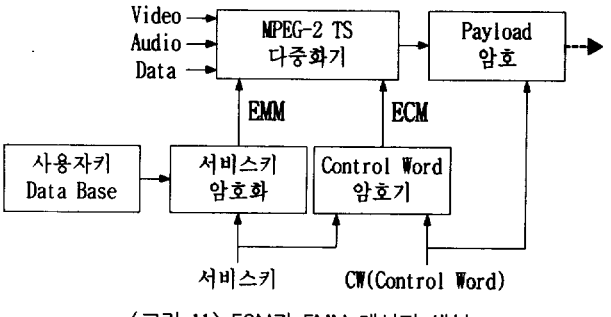


N : 입력 소스의 수 (N의 회선)
R : 각 소스의 데이터 속도 [bps]
M : 다중회선의 유효용량 [bps]
α : 소스가 전송하는 시간의 평균분율 ($0 < \alpha < 1$)
$K = M / NR$: 최대 입력 대 다중화된 회선 비율

(그림 10) 통신 시스템 기본 개념

시스템의 최적화를 위해 큐잉 이론의 단일 서버 큐 시스템을 이용한다. 단일 서버 큐는 서비스 시간 분포에 따라 3가지 유형을 나타내고 있지만, 성능 분석은 상수 서비스 시간(M/D/1)과 지수 서비스 시간(M/M/1)으로 나누어 분석 할 것이다.

방송에서의 제산수신 액세스는 크게 스크램블러의 비밀키인 제어워드를 분배하는 기능과 제어단어를 암호화하여 전달하는데 이용되는 인증키를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현될 수 있다. (그림 11)에 MPEG(Moving Picture Experts Group)-2에서 ECM과 EMM의 생성과정을 도시하였다. 이 제한 수신 메시지 생성과 관련된 버퍼의 크기와 지연을 ρ의 함수로 도시한다. 일반적으로 사용되는 평균 버퍼크기는 ρ 파라메터에 의해 조정되며 M에 의해서는 직접적으로 영향받지 않는다. 가입자수는 1000명으로 가정한다. ECM은 5~0.1초마다 256 bytes를 전송하고 EMM은 5~1/10 시간마다 256 bytes를 전송한다고 가정한다. 그리고 전송주기를 5초와 0.1초 사이에서 임의적으로 선택한다.



(그림 11) ECM과 EMM 메시지 생성

위 가정은 고정된 1000개의 입력 채널을 지닌 시스템이 초당 최대량 $\lambda_{max} = 10(1/10초마다\ 전달) \times \alpha \times 1000(가입자수) \times (256 \times 8_{(ECM)} + 256 \times 8 / 3600_{(EMM)})$를 그리고 초당 최소량 $\lambda_{min} = 0.2(5초마다\ 전달) \times \alpha \times 1000(가입자수) \times (256 \times 8_{(ECM)} + 256 \times 8 / 3600_{(EMM)})$를 입력으로 받아들이는 것을 의미하다. 소스 당 평균 입력량이 50%라고 가정하자. 따라서 α값은 0.5가 되므로 1000개 소스를 입력으로 받아들이는 시스템은 총 입력을 최대 10242844 (1/10초)에서 최소 204.85688(5초마다) 사이로 갖는다.

성능 분석은 상수 서비스 시간(M/D/1) 유형과 지수 서비스 시간(M/M/1) 유형으로 나누어 분석할 것이다.

5.1.1 Possion 도착율을 갖고 M/D/1 단일 서버 큐인 경우

이 모델의 시스템 입력채널에 입력된 평균 도착율 λ는 채널의 수(가입자 수)는 고정되어 있고 전달 주기가 다양한 형태가 변화된다고 가정 하에 이루어진다. 이 모델의 시뮬레이션 소스는 다음과 같다.

● 'utilization에 대한 버퍼량' 시뮬레이션 소스
(전달주기 0.1초인 경우)

```
time = 0.1;                    %% 전달주기 0.1초인 경우
N    = 1000;                   %% 가입자 수
R    = 256*8+256*8/3600;       %% 초당입력량(EMM+ECM)
sM   = 1024284400;             %% 최대 데이터 전송
a=1, x=1;
while (x == 1)
        rho(a) = (0.5*N*R/time)/M;
        q(a)   = ((0.5*(rho(a)*rho(a))/(1-rho(a)))+rho(a));
        M      = M-(256*8/3600*1000+256*8*1000)/1000;
        tq(a)  = (2-rho(a))/(M*(1-rho(a)));
        if (M <= 10346307.07)
                x = 0;
        end
        a = a + 1;
end
plot(rho, q); xlabel('rho'); ylabel('q');
title(['utilization에 대한 버퍼량']);
```

전달주기를 임의적으로 선택한 경우에 M/D/1에서의 이용률 ρ과 이에 따른 평균 버퍼 수 q는 <표 7>과 같다. 이용률 ρ는 0.83~0.78에 이르고 이에 따라 시스템 내에 존재하여야 하는 최소 평균 버퍼 크기는 2.856~2.163이 된다.

〈표 7〉 각 경우에 대한 이용률 및 버퍼량 (M/D/1)

전달주기 [초]	ρ	q	t_q [μ초]	M [bps]
0.1	0.83	2.856	0.278	12340775.9
0.2	0.83	2.856	0.557	6170388.2
0.4	0.82	2.688	1.049	3122818.4
0.6	0.82	2.688	1.574	2081878.9
0.8	0.81	2.537	1.981	1580685.8
1.0	0.81	2.537	2.476	1264548.6
2.0	0.80	2.400	4.686	640177.75
3.0	0.80	2.400	6.941	426785.14
4.0	0.79	2.276	8.772	324140.60
5.0	0.78	2.163	10.965	262636.90

즉 이용률이 감소하게 되면 q값이 감소하게 되고 이에 따라

시스템내 각 비트의 지연은 증가하게 되는 것을 알 수 있다. 이를 통해 최적의 키생성 및 전달 주기를 설정할 수 있다. 시스템에서 한 비트당 머무는 시간이 t_q이므로 입력되는 데이터와 t_q의 곱이 전달 주기가 된다.

ECM은 전송주기 마다 256바이트를 전송하고 EMM은 전송주기 마다 256바이트를 전송한다고 가정한다. 그리고 전송 주기를 5초와 0.1초 사이에서 임의적으로 설정하였다.

위 가정은 고정된 1000개의 입력 채널을 지닌 시스템이 초당 최대량 λ_{max} = 10(1/10초마다 전달)× α ×1000(가입자수)×(256× $8_{(ECM)}$ +256×8/ $3600_{(EMM)}$)를 그리고 초당 최소량 λ_{min} =0.2(5초마다전달)× α ×1000(가입자수)×(256× $8_{(ECM)}$ + 256 ×8/ $3600_{(EMM)}$)을 입력으로 받아들이는 것을 의미하다. 소스당 평균 입력량이 50%라고 가정하자. 따라서 α값은 0.5가 되므로 1000개 소스를 입력으로 받아들이는 시스템은 총 입력을 최대 10242844 (1/10초)에서 최소 204.85688 (5초마다) 사이로 갖는다. 다중회선 유효용량 M을 일정값으로 고정하기로 하자. M의 값으로 세 가지를 선택한다(경우 1 : 1.544, 경우 2 : 44.736, 경우 3 : 155 Mbps).

각 경우마다 입력되는 데이터 값은 위의 가정과 같이 유동적으로 변하게 된다. 이에 따른 각 파라메터 값들의 변동을 알아보기로 한다. 전달주기는 0.1초~5초로 설정하였다. 전달주기가 변동되면 λ의 값이 유동하게 된다. ρ값은 일반적인 시스템 테스트를 통해 통계 낼 수 있으므로 <표 7>에서 구해진 ρ값은 0.78~0.83 으로 정하고 이용되는 공식은 식 (1)과 같다.

$$
\begin{aligned}
&\cdot\ \lambda = \frac{\alpha NR}{\text{전달주기}} \\
&\cdot\ q = \frac{\rho^2}{2(1-\rho)} + \rho \qquad (1) \\
&\cdot\ t_q = \frac{(2-\rho)}{2M(1-\rho)} \\
&\cdot\ \rho = \frac{\lambda}{M} = \frac{\alpha NR}{M}\ \frac{1}{\text{전달주기}}
\end{aligned}
$$

이를 이용하여 대표적인 전송 속도인 DS1 속도(경우1), DS3 속도(경우2), 그리고 SDH-1 기본 속도(경우3)의 전송장치를 사용했을 경우의 최적의 키관리 주기에 따른 최대/최소키 전달 시간 산정도 <표 8>, <표 9>, <표 10>을 통해 구한다.

〈표 8〉 최대/최소키 전달시간(M/D/1,전송속도 DS1)

● 경우 1 : M = 1,544 Mbps(1,000 가입자)

ρ	λ[Mbps]	전달주기[sec]	q	t_q [μ sec]
0.78	1.20432	0.851	2.168	1.791
0.79	1.21976	0.840	2.276	1.861
0.80	1.23520	0.829	2.400	1.938
0.81	1.25064	0.819	2.537	2.023
0.82	1.26608	0.809	2.688	2.117
0.83	1.28152	0.801	2.856	2.223

〈표 9〉 최대/최소키 전달시간(M/D/1, 전송속도 DS3)

● 경우 2 : M = 44,736 Mbps(1,000 가입자)

ρ	λ[Mbps]	전달주기[msec]	q	t_q [μ sec]
0.78	34.894080	29.354	2.168	0.061
0.79	35.341440	28.983	2.276	0.063
0.80	35.788800	28.620	2.400	0.066
0.81	36.236160	28.267	2.537	0.069
0.82	36.683520	27.922	2.688	0.072
0.83	37.130880	27.586	2.856	0.076

〈표10〉 최대/최소키 전달시간(M/D/1,전송속도 SDH-1)

● 경우 3 : M = 155 Mbps(1,000 가입자)

ρ	λ[Mbps]	전달주기[msec]	q	t_q [μ sec]
0.78	120.90	8.472	2.168	0.017
0.79	122.45	8.365	2.276	0.017
0.80	124.00	8.260	2.400	0.018
0.81	125.55	8.158	2.537	0.019
0.82	127.10	8.059	2.688	0.020
0.83	128.65	8.001	2.856	0.021

5.1.2 Possion 도착율을 갖고 M/M/1 단일 서버 큐인 경우

이 모델의 시스템 입력채널에 입력된 평균 도착율 λ는 채널의 수(가입자 수)는 고정되어 있고 전달 주기가 다양한 형태가 변화된다고 가정하에 이루어진다. 이 모델의 시뮬레이션 소스는 다음과 같다.

● 'utilization에 대한 버퍼량' 시뮬레이션 소스
(전달주기 0.1초인 경우)

```
time = 0.1;                    %% 전달주기 0.1초인 경우
N    = 1000;                   %% 가입자 수
R    = 256*8+256*8/3600;       %% 초당입력량(EMM+ECM)
M    = 1024284400;             %% 최대 데이터 전송
a=1, x=1;
while (x == 1)
        rho(a) = (0.5*N*R/time)/M;
        q(a)   = ((0.5*(rho(a)*rho(a))/(1-rho(a)))+rho(a));
        M      = M-(256*8/3600*1000+256*8*1000)/1000;
        tq(a)  = (2-rho(a))/(M*(1-rho(a)));
        if (M <= 10346307.07)
                x = 0;
        end
        a = a + 1;
end
plot(rho, q); xlabel('rho'); ylabel('q');
title(['utilization에 대한 버퍼량']);
```

전달주기를 임의적으로 선택한 경우에 M/M/1에서의 이용률 ρ과 이에 따른 평균 버퍼 수 q는 <표 11>과 같다.

결과적으로 이용률 ρ는 0.83~0.78에 이르고 이에 따라 시스템 내에 존재하여야 하는 최소 평균 버퍼 크기는 2.688~2.163이 된다. 이를 통해 최적의 키생성 및 전달 주기를 설정할 수 있다. 시스템에서 한 비트당 머무는 시간이 t_q이므로 입력되는 데이터와 t_q의 곱이 전달 주기가 된다.

다른 경우를 고려해 보기로 한다. 가입자수는 1000명으로

〈표 11〉 각 경우에 대한 이용률 및 버퍼량(M/M/1)

전달주기	ρ	q	t_q [μ sec]	M [bps]
0.1	0.83	2.688	0.444	12491273.2
0.2	0.83	2.688	0.889	6245636.83
0.4	0.82	2.537	1.644	3200888.9
0.6	0.82	2.537	2.497	2107581.1
0.8	0.81	2.400	3.124	1600444.4
1.0	0.81	2.400	3.905	1280355.5
2.0	0.80	2.276	7.345	648281.30
3.0	0.80	2.276	11.018	432187.50
4.0	0.79	2.163	13.845	328296.30
5.0	0.78	2.163	17.306	262636.90

가정한다. ECM은 전송주기 마다 256 bytes를 전송하고 EMM은 전송주기 마다 256 bytes를 전송한다고 가정한다. 그리고 전달 주기는 5초와 0.1초 사이에서 임의적으로 설정하였다. 위 가정은 M/D/1과 동일한 조건이다. ρ값은 0.78~0.83 이며 이용되는 공식은 다음과 같다.

$$\bullet\ \lambda=\frac{\alpha NR}{\text{전달주기}} \quad \bullet\ q=\frac{\rho}{1-\rho} \quad \bullet\ t_q=\frac{s}{1-\rho}$$
$$\bullet\ \rho=\frac{\lambda}{M}=\frac{\alpha NR}{M}\frac{1}{\text{전달주기}} \tag{2}$$

식 (2)를 이용하여 대표적인 전송 속도인 DS1 속도(경우 1), DS3 속도(경우2), 그리고 SDH-1 기본 속도(경우3)의 전송장치를 사용했을 경우의 최적의 키관리 주기에 따른 최대/최소키 전달 시간 산정은 <표 12>, <표 13>, <표 14>를 통해 구한다.

〈표 12〉 최대/최소키 전달시간(M/M/1,전송속도 DS1)

● 경우 1 : M = 1,544 Mbps

ρ	λ[Mbps]	전달주기[sec]	q	t_q [μ sec]
0.78	1.20432	0.851	4.882	2.943
0.79	1.21976	0.840	4.556	3.084
0.80	1.23520	0.829	4.263	3.238
0.81	1.25064	0.819	4.000	3.408
0.82	1.26608	0.809	3.762	3.598
0.83	1.28152	0.801	3.545	3.809

〈표 13〉 최대/최소키 전달시간(M/M/1,전송속도 DS3)

● 경우 2 : M = 44,736 Mbps

ρ	λ[Mbps]	전달주기[msec]	q	t_q [μ sec]
0.78	34.894080	29.354	4.882	0.101
0.79	35.341440	28.983	4.556	0.106
0.80	35.788800	28.620	4.263	0.111
0.81	36.236160	28.267	4.000	0.117
0.82	36.683520	27.922	3.762	0.124
0.83	37.130880	27.586	3.545	0.131

〈표 14〉 최대/최소키 전달시간(M/M/1,전송속도 SDH-1)

● 경우 3 : M = 155 Mbps

ρ	λ[Mbps]	전달주기[msec]	q	t_q [μ sec]
0.78	120.90	8.472	4.882	0.029
0.79	122.45	8.365	4.556	0.030
0.80	124.00	8.260	4.263	0.032
0.81	125.55	8.158	4.000	0.033
0.82	127.10	8.059	3.762	0.035
0.83	128.65	8.001	3.545	0.037

5.2 과금 데이터 수집을 위한 최적의 시스템 용량 산정 및 최적의 전용선 용량산정

과금 데이터는 PPV(Pay-Per-View) 서비스와 프로그램 당 서비스 요금으로 가정한다. PPV는 1초 단위로 전달되며 프로그램 당 요금은 1시간당 요금으로 하며, 각 데이터의 길이는 256바이트로 한다.

5.2.1 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/D/1 단일 서버 큐

평균 도착율 λ은 각 입력채널에 입력되는 소스들에 시간당 사용률 α을 곱한 것이며, 일정 서비스 시간을 갖는 M/D/1 단일 서버 큐의 공식은 아래 식 (3)과 같다.

$$\bullet\ \lambda=\alpha NR \quad \bullet\ s=\frac{1}{M}$$
$$\bullet\ q=\frac{\rho^2}{2(1-\rho)}+\rho \quad \bullet\ t_q=\frac{s(2-\rho)}{2(1-\rho)}$$
$$\bullet\ \rho=\lambda s=\alpha NR/M=\frac{\alpha}{k}=\frac{\lambda}{M} \tag{3}$$
$$\bullet\ \sigma_q=\frac{1}{1-\rho}\sqrt{\rho-\frac{3\rho^2}{2}-\frac{5\rho^3}{6}-\frac{\rho^4}{12}}$$

ρ은 사용된 전체 입력용량의 이용률 또는 분률을 의미하고, 서비스 시간 s는 한 비트를 전송하는데 소요되는 시간을 의미한다. 과금 데이터 프레임은 버퍼의 크기와 지연을 ρ의 함수로 도시한다. PPV는 1초당 256 바이트를 전송하고 과금 데이터는 1시간당 256 바이트를 전송한다고 하자. 가입자수는 일정 형태로 변화한다. 일반적으로 사용되는 평균 버퍼 크기는 ρ 파라미터에 의해 조정되며 M에 의해서는 직접적으로 영향받지 않는다. 각 라인 당 도착율은 공통적으로 최대 도착 $\lambda_{max}=1\times(\text{가입자수})\times(256\times 8_{(PPV)}+256\times 8/3600_{(과금데이터)}$에 소스가 전송하는 시간의 평균분율 $\alpha=0.5$을 곱하여 사용된다.

〈표 15〉 각 경우에 대한 이용률 및 버퍼량(M/D/1)

가입자수	ρ	q	t_q [μ sec]	버퍼 증가량
500	0.75	1.875	4.881	-
1000	0.80	2.40	2.928	1.28
2000	0.81	2.54	1.528	1.0583
4000	0.82	2.69	0.800	1.0591
8000	0.83	2.84	0.419	1.0739
16000	0.84	3.05	0.221	-

즉 시스템은 각 가입자 소스들의 합을 기준으로 $\lambda=\alpha NR=$(가입자 수)$\times$1024.2844 [bps] 만큼 받아들인다. 가입자수는 200% 증가 한 경우를 추정한 것이다. 이용률 ρ와 이에 따른 평균 버퍼 수 q는 <표 15>와 같다.

결과적으로 이용률 ρ는 0.75~0.84에 이르고 이에 따라 시스템 내에 존재하여야 하는 최소 평균 버퍼 크기는 1.875~3.05가 된다. 가입수가 두 배로 증가하게 되면 다중회선 평균 유효 용량을 두 배로 증가해야 하지만 시스템 내의

버퍼는 평균 1.117배 늘려야 하는 것을 알 수 있었다.

모든 단말장치가 활발하게 사용된다 하더라도 대부분의 시간 동안 단말장치는 데이터 입력이 없다. 사용자 증가에 따른 버퍼의 증가는 데이터 전송량이 많은 경우에는 상당히 효율적으로 작동되나 전송량이 적은 경우에는 비효율적이 된다. 즉 시스템내의 버퍼의 증가는 비용적인 측면에서 비효율적 것이 된다.

따라서 가입자 수가 200% 증가하더라도 초기 버퍼량(500명 가입자 수에서 구해진 값)을 시스템에 계속적으로 고정시키고, 단지 M값을 유동적인 파라메터로 정하기로 한다. 여기에 M값은 최적의 전용선 용량이기도 하다. 구해진 파라미터 값들은 <표 16>에 기재되어 있다.

<표 16>에서는 초기 버퍼량을 1.875로 고정한 다음 각 입력량에 대한 최적 전용선 용량과 시스템 용량을 구한 것이다. 입력 용량 λ값이 증가하더라도 출력용량 M을 증가시킴으로서 시스템의 오버플로우를 막는다. 또한 임의적으로 다른 초기 버퍼량을 기준으로 계산하는 것도 가능하다.

〈표 16〉 고정된 버퍼에 대한 각 전용회선 용량 (M/D/1)

가입자수	q	t_q [μ sec]	λ[Mbps]	M[bps]
500	1.875	4.881	512142.2	682856.268
1000	1.875	2.440	1024284.0	1365712.000
2000	1.875	1.220	2048568.8	2731425.067
4000	1.875	0.610	4097137.6	5462850.133
8000	1.875	0.305	8194275.2	10925700.27
16000	1.875	0.152	16388550.4	21851400.53

5.2.2 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/M/1 단일 서버 큐

5.2의 (5.2.1)에서는 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/D/1 단일 서버 큐를 고려하였다. 여기에서는 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/M/1 단일 서버 큐를 고려하고, 위 M/D/1 단일 서버 큐에서 가정을 그대로 사용한다. 예를 들어, PPV은 1초당 256bytes를 전송하고 과금데이터는 1시간당 256bytes를 전송한다고 하자. 가입자수는 초기 500명으로 설정한 다음 200%씩 증가시킨다. 일반적으로 사용되는 평균 버퍼크기는 파라메터 ρ에 의해 조정되며 M에 의해서는 직접적으로 영향받지 않는다. 500개의 채널에 최대 도착 λ_{max}가 1×500(가입자수)$\times(256\times 8_{(PPV)}+256\times 8/3600_{(과금데이터)})$임을 의미한다. 즉 2048.5733 bps인 500개 소스를 입력으로 받아들이는 시스템이다. 소스당 평균 입력량이 50%라고 가정하자. 따라서 α값은 0.5이므로 시스템이 받아들이는 평균 입력량은 $\lambda=\alpha NR=$(가입자수)$\times$1024.2844 bps가 된다.

가입자수가 200% 증가한 여섯 가지 경우를 시뮬레이션 하였다. 이용률 ρ와 이에 따른 평균 버퍼 수 q는 <표 17>과 같다.

〈표 17〉 각 경우에 대한 이용률 및 량 (M/M/1)

가입자수	ρ	q	t_q [μ sec]	버퍼 증가량
500	0.77	3.348	8.489	-
1000	0.80	4.000	4.881	1.195
2000	0.81	4.263	2.569	1.066
4000	0.82	4.555	1.355	1.068
8000	0.83	4.882	0.717	1.075
16000	0.84	5.250	0.381	-

결과적으로 이용률 ρ는 0.77~0.84에 이르고 이에 따라 시스템 내에 존재하여야 하는 최소 평균 버퍼 크기는 3.348~5.250이 된다. 가입자수가 두 배로 증가하게 되면 다중회선 평균 유효 용량을 두 배로 증가해야 하지만 시스템 내의 버퍼는 평균 1.101배 늘려야 하는 것을 알 수 있다.

이제 가입자 수가 200% 증가하더라도 초기 버퍼량(500명 가입자 수에서 구해진 값)을 시스템에 고정시키고, 오직 M값을 유동적인 파라메터로 정하기로 한다. 여기에 M값은 최적의 전용선 용량이기도 하다. 계산된 파라미터 값은 <표 18>에 기재되어 있다.

〈표 18〉 고정된 버퍼에 대한 각 전용회선 용량(M/M/1)

가입자수	q	t_q [μ sec]	λ[bps]	M[bps]
500	3.348	8.489	512142.2	665119.740
1000	3.348	4.244	1024284.0	1330238.961
2000	3.348	2.122	2048568.8	2660478.961
4000	3.348	1.061	4097137.6	5320957.922
8000	3.348	0.530	8194275.2	10641915.840
16000	3.348	0.265	16388550.4	21283831.690

<표 18>에는 초기 버퍼량을 3.348로 고정한 다음 각 입력량에 대한 최적 전용선 용량과 시스템 용량을 구한 것이다. 입력 용량 λ값이 증가하더라도 출력용량 M을 증가시킴으로서 시스템의 오버플로우를 막는다. 또한 임의적으로 다른 초기 버퍼량을 구하여 계산하는 것도 가능하다.

6. 결 론

본 논문에서는 제한수신 시스템에서의 키 관리 계층을 개선하여 제안하였고, 제안된 키 계층에 의해 시뮬레이션 환경에서, 가입자 입장에서의 시청권한 변경에 따른 가입자의 불편 유무와 제한수신메시지 양의 오버플로우 등에 대한 성능 검증을 실시한 결과 운용상에서의 시스템 결함을 발견하지 못하였다. 하지만, 시뮬레이션 환경에서는 실제 운용시의 다양한 가입자의 요구를 반영한 성능 분석과 과금 수집을 위한 시스템의 최적 용량 등에 대한 정량적인 분석이 어려워, 큐잉 이론)을 바탕으로 하여 기간별 예상 가입자수 증가에 따른 과금 데이터 수집을 위한 최적의 전용선 용량 산정을 했고, 기간별 예상 가입자수 증가에 따른

과금 데이터 수집을 위한 최적의 시스템 용량을 산정 하여 보았다. 향후 알고리즘을 보다 세션별 계층적 구조로 적용할 수 있도록 하고 성능 향상을 위한 키 계층을 적용한 시뮬레이션이 필요하다.

참 고 문 헌

[1] 한국전자통신연구원, "지상파 디지털 방송기술 연구", 한국전자통신연구원, 1996.

[2] Mark Buer, Joe Wallance, "Integrated Security for Digital Video Broadcast," IEEE Transactions on Consumer Electronics, Vol.42, No.3, 1996, 9.

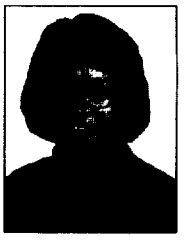
[3] 조진만, 은성경, 조현숙, "위성방송의 제한수신 서비스를 위한 스마트카드 기술", JCCI' 96, 1996.

[4] ETSI Technical Report, Digital Video Broadcast- ing(DVB) ; Support for use of scrambling and Conditional Access(CA)with digital broadcasting systems, 1996.10.

[5] 조현숙, 임춘식, "DigiPass : KoreaSat DBS의 Conditional Access System", 전자공학회지, 제22권 제7호, 1995년 7월, pp.768-775.

[6] J. Robert, U. Mocci and J. Virtamo, "Broadband Network Teletraffic," Springer, 1996.

[7] W. Stallings, "High-Speed Networks," Prentics Hall, 1998.



조 현 숙

e-mail : hscho@etri.re.kr

1979년 전남대학교 수학과 졸업(학사)

1991년 충북대학교 대학원 전자계산학과 졸업(석사)

2001년 충북대학교 대학원 전자계산학과 졸업(박사)

1982년~현재 한국전자통신연구원 책임연구원 정보보호기술연구본부장

관심분야 : Network Security, Mobile security, Conditional Access

이 상 호

e-mail : shlee@chungbuk.ac.kr

1976년 숭실대학교 전자계산학과 졸업

1981년 숭실대학교 대학원 전자계산학과 석사 졸업

1989년 숭실대학교 대학원 전자계산학과 박사 졸업

1981년~현재 충북대학교 컴퓨터과학과 교수

1990년~1991년 호주 텔레콤 연구소, 방문연구원

1992년~1993년 캐나다 UBC, 방문연구원

관심분야 : Network Protocol, Network Security