通信情報保護學會誌
第 10 券 第 1 號, 2000. 3

한국형 한정 수신 시스템의 성능 분석 결과

봉 호*, 류 종 호*, 조 현 숙**, 염 흥 열*

요 약

본 논문에서는 큐잉 이론을 바탕으로 한국형 한정 수신 시스템인 Digipass-2 성능 분석을 한다. 기간별 예상 가입자 수 증가에 따른 최적의 키 생성 및 전달 주기를 산정하고, 최적의 키 관리 주기에 따른 최대/최소 키 전달 시간을 산정한다. 또한 기간별 예상 가입자수 증가에 따른 과금 데이터 수집에 최적 전용선 용량을 산정하고, 과금 데이터 수집을 위한 최적의 시스템 용량을 산정한다.

Ⅰ. 서 론

케이블이나 위성 방송시스템에서 방송 수신이 비허가된 자의 방송 도청 문제는 방송 업계의 오랜 문제이기도 하다. 지금까지는 적법한 소비자들이 매달 고액의 시청료나 엄청난 접속 요금을 지불함으로서 도청 행위에 대한 손실을 보상해야만 했다. 이에 따라 위성 방송의 안전한 내용 전달은 서비스 제공자들에게 매우 중요한 사항으로 대두되었다. 이 문제의 해결책으로 위성 방송 수신기에 저가의 하드웨어 보안 장치를 삽입하므로서 위성 방송 도청과 같은 사기 행위를 방지한다. 한정 수신 시스템(CAS : Conditional Access System)의 일부 역할을 이 하드웨어 장치가 맡는다.

한정 수신 시스템은 평문(방송정보)을 모든 수신자가 수신되도록 하는 것이 아니라 수신 권한(Entitlement)이 있는 수신자만이 특정 방송 채널의 수신을 가능케 하는 시스템이다. 이는 암호 기술에서 스크램블링 및 디스크램블링 기능, 인증(Authentication) 기술을 이용한 가입자 신분 확인 기능, 그리고 접근 제어 기능들은 한정 수신 방송시스템을 실현하기 위한 핵심 기술들이다. 한정 수신 시스템을 실현하기 위해서는 스크램블링의 강도가 어느 정도 높아야 하고, 스크램블링 및 디스크램블링을 위한 관련 파라메터들은 암호학적으로 안전한 알고리즘을 사용하여 수신단으로 안전하게 전달되어야 한다. 방송망에 적용 가능한 한정 액세스는 크게 스크램블러의 비밀키인 제어워드(CW : Control Word)를 분배하는 기능과 CW를 암호화하여 전달하는데 이용되는 인증키(AK : Authentication Key)를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현될 수 있다.

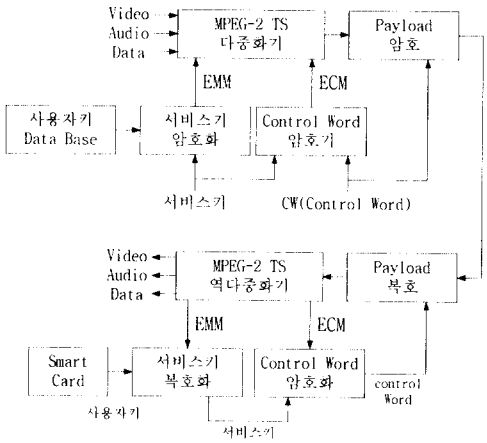


그림 1. MPEG-2에서 ECM과 EMM 역할의 예

* 순천향대학교 전자공학과 정보보호 및 디지털통신 연구실(youjh@elec.sch.ac.kr)
** 한국전자통신연구원

CW(제어워드)를 인증키로 암호화하여 전달한 메시지를 ECM(Entitlement Control Message)이라고 하고, 인증키를 전달하는 위한 메시지를 EMM(Entitlement Management Message)이라고 한다. 예로 MPEG-2(Moving Picture Experts Group-2)의 한정 수신 시스템의 개념이 그림 1에 도시되어 있다.[1][2][3][4]

한정 수신시스템은 수신료를 시청시간 및 시청한 프로그램에 따라 차등적으로 적용하는 등 다양한 서비스를 제공할 수 있으나, 이를 실현할 경우에 발생하는 여러 가지 해결해야할 문제점이 남아있다. 즉, 일반적으로 관리상에서 발생할 수 있는 서비스 가입 등록, 서비스 가입자 관리, 서비스 관리 등과 한정 수신시스템 상에서 발생할 수 있는 키 생성 속도 및 전달 시간, 전용선 Capacity, 시스템 용량 등의 문제들을 고려해야 할 필요성이 있다. 따라서, 앞으로 디지털 위성 방송 유료 서비스의 질을 개선하고, 효율적으로 상용화하기 위해서는 기간별 예상 가입자 등록 수, 예상 유료 채널 시청 등록 가입자 수, 유료 채널 등록 가입자 월간 예상 유료 프로그램 시청 건수, 유료 방송 가입자중 예상 Credit 및 Token 가입 비율, 그리고 Credit 가입자중 예상 PPV (Pay-Per-View) 및 예약신청 가입 비율 등을 미리 조사한 후, 이를 기초로 하여 한정 수신 시스템의 상용화를 위한 시스템 최적화를 실현해야 할 것이다.

본 논문에서는 시스템 성능 향상을 위해서는 최적의 키 생성 및 전달 주기를 산정, 최적의 키관리 주기에 따른 최대 및 최소 키 전달 시간 산정, 과금 데이터 수집을 위한 최적의 전용선 Capacity 산정, 그리고 과금 데이터 수집을 위한 최적의 시스템 용량을 산정 한다. 본 논문의 2장에서는 시스템 성능 분석을 위한 기본 개념으로 큐잉 이론(Queuing Analysis)을 설명하고, 3장에서 한정 수신 시스템의 성능 분석을 분석하며, 마지막 4장에서는 간단한 결론을 맺기로 한다.

II. 큐잉 이론의 개념

큐잉 이론(Queuing Analysis)은 키 생성/전달 주기 산정, 최대/최소 키 전달시간 산정, 시스템 용량 산정, 전용선 Capacity 산정을 하기 위해 이용된다. 본 장에서는 큐잉 이론 기본 개념을 설명한다.

통신에서 동기적 온라인이란 상대 개체가 통신 순간에 다른 통신 상대와 대면하는 것이다. 시스템에서 통신 모듈은 상대 개체가 반드시 있어야 하는 것을 요구할 수도 있고, 또는 메시지를 통해서 통신할 수도 있다. 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 상호 연동성을 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.[6]

큐잉 모델의 대표적인 형태는 단일 큐잉 모델(Single Server Queue)과 멀티 서버 큐잉(Multi Server Queue) 모델이 있다. 단일 서버 큐잉 시스템은 그림 2와 같다. 시스템의 중앙에 위치한 것은 서버(Server)이며 아이템(Items)에 서비스를 제공한다. 도착한 아이템들은 대기열(Waiting Line)에 대기한다. 서버가 한 아이템에 대한 처리를 완수하면 아이템은 서버를 떠나게 된다.[7]

그림 2는 큐잉 모델에서 사용되는 기본적 파라메터가 표기되어 있다. 아이템들(Items)은 초당 평균 도착율 λ로 시스템에 도착한다. 어떤 정해진 시간 내에 몇 개의 아이템들이 대기열(Queue)에서 대기한다. 서버는 평균 서비스 시간 s로 아이템을 처리한다. 이용률(Utilization)은 서버가 동작하는 시간과 s의 비율이다.

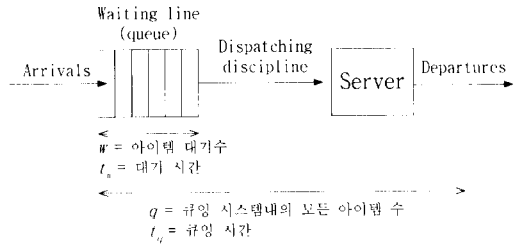


그림 2. 단일서버 큐잉 시스템 구조 및 파라메터

표 1. 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	: q 의 표준편차
σ_{tq}	: t_q 의 표준편차
w	: 서비스를 기다리는 아이템의 평균 대기 수
t_w	: 서비스를 기다리는 아이템의 평균 대기 시간
σ_w	: w 의 표준편차
M	: 서버들의 개수

도착율(Arrival Rate)은 시스템을 통과하는 트래픽의 비율로서, 증가하게 되면 이용률이 증가하여 밀집 현상이 발생하며 대기열의 길이와 대기 시간이 증가한다. 이론적인 최대 입력률은 시스템에 의해 조정될 수 있으며 단일 서버인 경우에 λ값은 $\lambda_{\max} = 1/s$ 이 된다. 표 1은 그림 2에서 사용되는 표기법을 요약한다. 몇 가지 다른 파라메터도 사용된다.

대기열은 시스템이 거의 포화 상태에 이를 때까지 커질 수 있으므로, 응답 시간 요구(Response Time Requirement)나 버퍼 크기(Buffer Size)는 단일 서버인 경우에 이론적으로 입력률을 70~90%로 제한한다. 이 모델을 형성하기 위해 아이템 수(Item Population)와 대기열 크기(Queue Size)는 무한하고 시스템에 도착되는 아이템들은 FIFO(First-In First-Out)을 기본 원칙으로 처리됨을 가정한다.

멀티서버 큐잉(Multiserver Queue) 모델은 그림 3과 같다. 이 경우에는 다양한 서버가 존재하고 대기열을 공유한다. 만일 아이템이 도착한다면 적어도 하나의 서버가 아이템을 처리하게 된다.

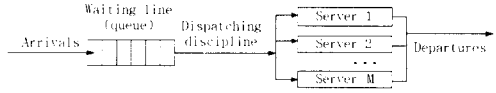


그림 3. 멀티서버 큐잉 시스템

표 2. 기본적 큐잉 관계

$\rho =$	λs	단일 서버에 의한
$\rho =$	$\frac{\lambda s}{M}$	멀티 서버에 의한
$q =$	λt_q	
$w =$	λt_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 입력률의 공식은 $\lambda_{\max} = M/s$ 같이 된다.

큐잉 시스템에서 사용되는 파라메터들은 상호간에 밀접한 관계를 지닌다. 입력에 따라 도착율(Arrival Rate), 서비스 시간(Service Time)이 주어지고 출력 정보 관련에 따라 아이템 대기(Items Waiting), 대기 시간(Waiting Time), 아이템 큐드(Items Queued), 큐잉 시간(Queuing Time)이 주어진다. 표 2는 시스템 파라미터들간의 관계식을 제공한다.

평균값 w, t_w, q, t_q 이 주어지면 그에 따른 표준편차 $\sigma_q, \sigma_{tq}, \sigma_w, \sigma_{tw}$ 도 구해진다. 단 주어진 문제의 도착율은 Poisson 분포를 갖게되며 서비스 시간에 대한 확률 밀도 함수는 지수적으로 증가한다고 가정한다.

1. 단일 서버 큐의 관계식

서버의 서비스 시간은 일반적으로 세 가지 유형으로 (M/G/1, M/M/1, M/D/1) 나눌 수 있다.

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 3. 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)

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

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

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

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

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

본 논문에서는 M/M/1과 M/D/1 유형을 이용한다. 표 3의 (a)에서 지수(Exponential) 서비스 시간의 표준편차가 '0'인 경우에는 상수(constant) 서비스 시간과 동일하게 된다. 표 3의 (b)는 상수 서비스 시간인 경우에 관계식이다. 단 각 세션별로 나누어 서비스하는 FQ(Fair Queuing)의 방법을 사용하지 않으며 아이템은 큐(대기열)에서 이탈하지 않는다고 가정한다.[2]

2. 멀티서버 큐의 관계식

표 4는 멀티서버 큐에 대한 공식이 나열되었다. 공식은 M/M/N의 경우에만 사용되며 지수 서비스 시간은 각 N개 서버들마다 동일한 시간을 갖는다. 멀티서버인 경우에 모든 서버는 균등하게 부하 되며 동일한 서비스 시간을 갖음을 가정한다.

표 4. (M/M/N)인 경우 멀티서버 큐잉의 공식

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

: 모든 서버가 활동중인 경우에 대한 확률

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

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

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

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

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

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

III. 한정 수신 시스템의 성능 분석

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

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

최적의 전용선 용량 결정은 큐잉 이론에 바탕을 두고 있다. 본 장에는 이를 이용하여 Digipass-2의 성능을 분석한다. 기본적으로 여기서 제시된 결과는 한정 액세스만을 위한 결과이므로 여기에 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 4의 시스템의 문제점은 입력량이 회선의 용량보다 더 많은 기간 동안 있을 수 있으므로, 임시의 초과입력을 견딜 수 있도록 시스템에 버퍼를 포함시켜야 한다는 점이다.

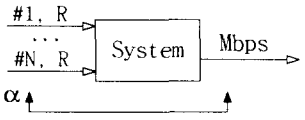


그림 4. 기본 시스템 개념

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

입력이 출력을 초과할 때 초과된 부분(backlog)은 버퍼에 저장된다.[5][1] 비용을 최소화하기 위해 최소크기의 버퍼와 최소크기의 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.

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

방송망에 한정 액세스는 크게 스크램블러의 비밀키인 제어워드(CW : Control Word)를 분배하는 기능과 CW를 암호화하여 전달하는데 이용되는 인증키(AK : Authentication Key)를 분배하는 기능, 그리고 스크램블링과 디스크램블링 기능으로 실현될 수 있다. CW를 인증키로 암호화하여 전달하는 메시지를 ECM이라 하고, 인증키를 전달하는 위한 메시지를 EMM이라 한다.[1][2] 그림 5에 MPEG(Moving Picture Experts Group)-2에서 ECM과 EMM에 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 전송 주기를 5초와 0.1초 사이에서 임의적으로 선택한다.

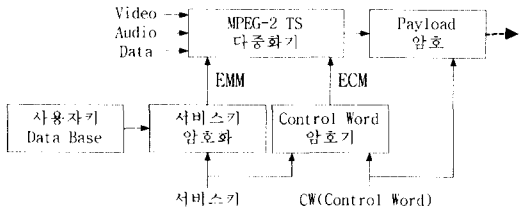


그림 5. ECM과 EMM 메시지 생성

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/ $3600_{(EMM)}$)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 분석

할 것이다.

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 MATLAB 시뮬레이션 소스는 다음과 같다.

- 'utilization에 대한 버퍼량' MATLAB 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/D/1에서의 이용률(Utilization) ρ과 이에 따른 평균 버퍼 수 q는 다음 표 5와 같다.

결과적으로 이용률(utilization) ρ는 0.83~0.78에 이르고 이에 따라 시스템 내에 존재하여야 하는 최소 평균 버퍼 크기는 2.856~2.163이 된다.

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.

다른 경우를 고려해 보기로 한다. 가입자수는 1000명으로 가정한다. ECM은 전송주기 마다 256 bytes를 전송하고 EMM은 전송주기 마다 256 bytes를 전송한다고 가정한다. 그리고 전송 주기를 5초와 0.1초 사이에서 임의적으로 설정한다.

표 5. 각 경우에 대한 이용률 및 버퍼량 (M/D/1)

전달주기 [sec]	ρ	q	t_q [μsec]	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

위 가정은 고정된 1000개의 입력 채널을 지닌 시스템이 초당 최대량 λ_{max} = 10(1/10초마다 전달) $\times \alpha \times$1000(가입자수)$\times$(256$\times 8_{(ECM)}$ +256$\times$8/3600$_{(EMM)}$)를 그리고 초당 최소량 λ_{min} = 0.2(5초마다전달)$\times \alpha \times$1000(가입자수)$\times$(256$\times 8_{(ECM)}$ + 256$\times$8/3600$_{(EMM)}$)을 입력으로 받아들이는 것을 의미한다. 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 0.1sec~5sec로 설정하였다. 전달주기가 변동하게 되면 λ의 값이 유동하게 된다. ρ값은 일반적인 시스템 테스트를 통해 통계 낼 수 있으므로 위에서 조건을 통해 구해진 ρ값의 범위를 이용한다. 따라서

ρ 값은 0.78~0.83 으로 정하고 이용되는 공식은 다음과 같다.

- $\lambda = \frac{\alpha NR}{\text{전달주기}}$
- $q = \frac{\rho^2}{2(1-\rho)} + \rho$
- $t_q = \frac{(2-\rho)}{2M(1-\rho)}$
- $\rho = \frac{\lambda}{M} = \frac{\alpha NR}{M} \frac{1}{\text{전달주기}}$

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 다음을 통해 구한다.

- 경우 1 : M = 1.544 Mbps (1,000 가입자)

ρ	λ [Mbps]	전달주기[sec]	q	t_q [μsec]
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

- 경우 2 : M = 44.736 Mbps (1,000 가입자)

ρ	λ [Mbps]	전달주기[msec]	q	t_q [μsec]
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

- 경우 3 : M = 155 Mbps (1,000 가입자)

ρ	λ [Mbps]	전달주기[msec]	q	t_q [μsec]
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

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 전달주기가 다양한 형태가 변화된다고 가정하에 이루어진다. 이 모델의 MATLAB 시뮬레이션 소스는 다음과 같다.

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

```
time=0.1 :  %% 전달주기 0.1초인 경우
N=500 :  %% 가입자 수
R=256*8+256*8/3600:
        %% 초당 입력량(EMM+ECM)
M=1024284400:  %% 최대 데이터 전송
a=1, x=1;
  while (x == 1)
  rho(a) = (0.5*N*R/time) / M:
  q(a) = rho(a) / (1-rho(a)):
  M =
  M-(256*8/3600*1000+256*8*1000)/1000:
  tq(a) = 1/(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(Utilization) ρ과 이에 따른 평균 버퍼 수 q는 다음 표 6과 같다.

결과적으로 이용률(utilization) 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 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 위 M/D/1과 동일한 조건이다. ρ 값은

표 6. 각 경우에 대한 이용률 및 버퍼량 (M/M/1)

전달주기	ρ	q	t_q [μsec]	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

0.78~0.83 이며 이용되는 공식은 다음과 같다.

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

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 다음을 통해 구한다.

• 경우 1 : M = 1.544 Mbps

ρ	λ [Mbps]	전달주기[sec]	q	t_q [μsec]
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

• 경우 2 : M = 44,736 Mbps

ρ	λ [Mbps]	전달주기[msec]	q	t_q [μsec]
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

• 경우 3 : M = 155 Mbps

ρ	λ [Mbps]	전달주기[msec]	q	t_q [μsec]
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

2. 과금 데이터 수집을 위한 최적의 시스템 용량 산정 및 최적의 전용선 Capacity산정

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

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

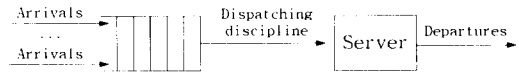


그림 6. M/D/1 단일서버 큐

이 모델에서 평균 도착율 λ은 각 입력채널에 입력되는 소스들에 시간당 사용률 α을 곱한 것이며, 일정 서비스 시간을 갖는 M/D/1 단일 서버 큐의 공식은 표 3에 표기되어 있다.

ρ은 사용된 전체 입력용량의 이용률 또는 분률을 의미하고, 서비스 시간 s는 한 비트를 전송하는 데 소요되는 시간을 의미한다. 과금 데이터 프레임은 버퍼의 크기와 지연을 ρ의 함수로 도시한다. PPV은 1초당 256 bytes를 전송하고 과금 데이터는 1시간당 256 bytes를 전송한다고 하자. 가입자 수는 일정 형태로 변화한다. 일반적으로 사용되는 평균 버퍼 크기는 ρ 파라메터에 의해 조정되며 M에 의해서는 직접적으로 영향받지 않는다.

각 라인 당 도착율은 공통적으로 최대 도착 λ_{max} $=1\times$(가입자수)$\times(256\times 8_{(PPV)}+256\times 8/3600_{(과금데이터)})$에 소스가 전송하는 시간의 평균분율 $\alpha=0.5$ 을 곱하여 사용된다.

표 7. 각 경우에 대한 이용률 및 버퍼량 (M/D/1)

가입자수	ρ	q	t_q [μsec]	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.

아래의 여섯 가지는 가입자수가 200% 증가 한 경우를 추정한 것이다. 이용률 ρ와 이에 따른 평균 버퍼 수 q는 다음 표 7과 같다.

결과적으로 이용률(utilization) 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 있다.

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 Capacity이기도 하다. 구해진 파라메터 값들은 표 8에 기재되어 있다.

표 8에서는 초기 버퍼량을 1.875로 고정한 다음 각 입력량에 대한 최적 전용선 Capacity와 시스템 용량을 구한 것이다. 입력 용량 λ값이 증분 하더라도 출력용량 M을 증가시킴으로서 시스템의 오버플로우를 막는다. 또한 임의적으로 다른 초기 버퍼량을 기준으로 계산하는 것도 가능하다.

표 8. 고정된 버퍼에 대한 각 전용회선 용량 (M/D/1)

가입자수	q	t_q [μsec]	λ [bps]	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

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

앞에서는 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/D/1 단일 서버 큐를 고려하였다.

표 9. 각 경우에 대한 이용률 및 버퍼량

가입자수	ρ	q	t_q [μsec]	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	-

이제부터는 Possion 도착율을 갖고 일정한 서비스 시간을 유지하는 M/M/1 단일 서버 큐를 고려하겠다. 일정 서비스 시간을 갖는 M/M/1 단일 서버

큐의 공식은 표 3에 나열되어 있다.

여기에서도 위 M/D/1 단일 서버 큐에서 가정을 그대로 사용한다. 예를 들어, PPV은 1초당 256 bytes를 전송하고 과금데이터는 1시간당 256 bytes를 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)$\times(256\times8_{(PPV)}+256\times8/3600_{(과금데이터)})$ 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 bps 가 된다.

가입자수가 200% 증가한 여섯 가지 경우를 시뮬레이션 하였다. 이용률(utilization) ρ와 이에 따른 평균 버퍼 수 q는 다음 표 9와 같다.

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.

표 10. 고정된 버퍼에 대한 각 전용회선 용량

가입자수	q	t_q [μsec]	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

이제 가입자 수가 200% 증가하더라도 초기 버퍼량(500명 가입자 수에서 구해진 값)을 시스템에 계속적으로 고정시키고, 오직 M값을 유동적인 파라메터로 정하기로 한다. 여기에 M값은 최적의 전용선 Capacity이기도 하다. 계산된 파라메터 값은 표 10에 기재되어 있다.

표 10에는 초기 버퍼량을 1.875로 고정한 다음 각 입력량에 대한 최적 전용선 Capacity와 시스템 용량을 구한 것이다. 입력 용량 λ값이 증분 하더라도 출력용량 M을 증가시킴으로서 시스템의 오버플로우를 막는다. 또한 임의적으로 다른 초기 버퍼량을 구하여 계산하는 것도 가능하다.

IV. 결 론

본 논문에서는 큐잉 이론(Queuing Analysis)을 바탕으로 하여 기간별 예상 가입자수 증가에 따른 과금 데이터 수집을 위한 최적의 전용선 Capacity 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 실제 구현에 이용될 수 있도록 연구하고자 한다.

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.

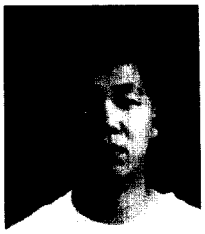
[4] Etsi Technical Report, Digital Video Broadcasting(DVB): Suppo rt for use of scrambling and Conditional Access (CA)with digital broadcasting systems, 1996.10.

[5] 조현숙, 임춘식, "DigiPass: KoreaSat DBS 0의 Conditional Access System", 전자공학회지, 제22권 제7호, pp 768-775, 1995년 7월.

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

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

〈著者紹介〉



봉 호 (Ho Bong)
1998년 2월 순천향대학교 전자공학과 졸업
1998년 2월~현재: 순천향대학교 전자공학과 석사과정
〈관심분야〉 컴퓨터보안, 네트워크 보안, 암호이론

류 종 호 (Jong-Ho Yu)
1998년 2월 순천향대학교 전자공학과 졸업
1998년 2월 ~ 현재: 순천향대학교 전자공학과 석사과정
〈관심분야〉 네트워크 보안, 전자화폐

조 현 숙 (Hyun-Sook Cho)
전남대학교 수학과 졸업
충북대학교 대학원 전자계산학과 졸업 (석사)
1982년~ 현재: 한국전자통신연구원 책임연구원 정보보호연구본부 본부장
〈주관심분야〉 Network Security, Conditional Access

염 흥 열 (Heung-Youl Youm)
1981년 2월 한양대학교 전자공학 졸업
1983년 2월 한양대학교 전자통신공학 석사
1990년 2월 한양대학교 전자통신공학 박사
1982년 12월 ~ 1990년 9월 한국전자통신연구소 선임연구원
1990년 9월 ~ 현재 순천향대학교 공과대학 정보기술공학부 부교수
〈주관심분야〉 암호이론, 부호이론, 이동통신분야