情報保護學會論文誌
第14券 第4號, 2004. 8

기가급 VPN을 위한 IPSec 가속기 성능분석 모델*

윤 연 상†‡, 류 광 현, 박 진 섭, 김 용 대, 한 선 경, 유 영 갑
충북대학교

IPSec Accelerator Performance Analysis Model for Gbps VPN*

Yeonsang Yun†‡, Kwang-Hyun Ryoo, Jinsub Park, Yongdae Kim,
Seonkyoung Han and Younggap You
Chungbuk Nat'l University

요 약

본 논문에서는 IPSec 가속기의 성능분석 모델을 제안한다. 제안된 성능분석은 큐잉 모델링을 기반으로 하고 트래픽로드는 포아송 분포를 채택하였다. 성능분석 시 새로운 파라미터로 디코딩지연을 정의하여 시뮬레이션에 이용하였다. 제안된 모델을 이용하여 IPSec 가속장치인 BCM5820의 성능을 분석한 결과, 장비를 통해 실측된 결과와 15% 정도의 차이만을 나타내었다. 제안된 모델을 이용한 성능분석 결과는 IPSec 가속기의 최대성능을 유지하기 위한 서버내의 하드웨어들의 적합한 구조를 제시하고 나아가 고속 네트워크 컴퓨터의 통계적 설계공간탐색에 이용될 수 있다.

ABSTRACT

This paper proposes an IPSec accelerator performance analysis model based a queue model. It assumes Poisson distribution as its input traffic load. The decoding delay is employed as a performance analysis measure. Simulation results based on the proposed model show around 15% differences with respect to actual measurements on field traffic for the BCM5820 accelerator device. The performance analysis model provides with reasonable hardware structure of network servers, and can be used to span design spaces statistically.

Keywords : *IPSec accelerator, M/M/1 system, Poison distribution, Decoding delay*

Ⅰ. 서 론

네트워크 보안의 중요성이 증대됨에 따라 IPSec이나 SSL과 같은 보안 프로토콜 등이 실 제 통신에 응용되고 있다. 이미 운영체제의 선두에 있는 마이크로소프트사의 Windows 계열은 IPSec 프로토콜의 사용을 일반화하고 있다. 하지만 OS와 같은 소프트웨어 상에서 IPSec 프로토콜을 구현할 경우 CPU는 상당한 연산량을 처리해야만 한다. 실제로 최근의 연구결과에서 보안 어플리케이션은 수행 시 CPU 자원의 95% 이상을 소모한다고 밝히고 있다.[1] 이러한 문제점을 극복하기 위한 방안으로 암호화 가속장치들이 제작되어 왔다.[2] IPSec 가속기는 IPSec에서 사용되는 암호 연산을 CPU 대신 처리함으로서 전반적인 시스템의 부하를 분배시키는 역할을 한다.

IPSec 가속기 제작업체는 제품성능을 가속기 내부 칩의 성능에 국한하여 제시하고 있다. 일례로 Broadcom사 BCM5820 모델의 경우 3DES+

접수일 : 2004년 5월 11일 ; 채택일 : 2004년 7월 26일
* 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과이며 충북대학교 컴퓨터정보통신연구소의 일부지원에 의하여 수행되었음.
† 주저자, ‡ 교신저자 : ysyun@hbt.chungbuk.ac.kr

SHA 연산 시 최대 300Mbps의 성능을 보인다고 강조한다.[12] 하지만 실제로 IPSec 가속기를 네트워크 컴퓨터에 장착하여 성능을 측정하였을 경우 50% 정도의 성능만을 나타내었다.[3] 이 성능 역시 네트워크 대역폭이 1Gbps이며 통신방식은 1:1 방식일 경우 그리고 기타 네트워크 컴퓨터의 사양 등이 최상의 조건일 때 얻어진 결과이다. 사실 상 네트워크 및 사용자의 네트워크 컴퓨터 사양이 최적의 상태가 아닐 경우 IPSec 가속기의 선전된 성능은 기대하기 힘들다는 결론이다. 만약 IPSec 가속기를 네트워크 컴퓨터에 장착하였을 경우의 성능분석이 이루어진다면 사용자는 IPSec 가속기의 성능을 최대한 이용하기 위해 적절한 네트워크 환경 및 네트워크 컴퓨터의 사양을 결정할 수 있을 것이다.

본 논문에서는 IPSec 가속기를 네트워크 컴퓨터에 장착하였을 경우의 성능분석 모델을 제안하였다. 주로 성능분석은 장비를 통한 측정 또는 모델링을 통한 시뮬레이션의 방법을 통해 이루어진다. 제안된 성능분석 모델은 시뮬레이션 방법을 이용하였다. 최근 시뮬레이션 방법은 모델링 기법 및 시뮬레이션 툴의 발달로 인해 장비측정결과와 상당히 유사한 결과를 보이고 있다.[4] 본 논문에서는 큐잉모델링 기법을 사용하였다. 제안된 모델의 분석을 위해 사용된 시뮬레이션 툴은 Anylogic4.5이다. Anylogic4.5는 기존의 COVERS의 후속 버전으로 중간 사양의 워크스테이션(PIV 1.7GHz, 512MB RAM)에서 50,000개의 서로 다른 객체를 동시에 프로세싱 할 수 있는 테스트 환경을 지원한다.[5-6]

본 논문의 구성은 다음과 같다. Ⅱ장에서 우선 모델링을 통한 성능분석의 전반적인 개요 및 제안된 성능분석모델을 설명하였다. Ⅲ장은 성능분석모델의 시뮬레이션결과를 설명하였다. 마지막으로 Ⅳ장에서 본 논문의 결론을 맺었다.

Ⅱ. 제안된 성능분석 모델

제안된 성능분석 모델은 IPSec 가속기를 장착한 네트워크 컴퓨터의 큐잉모델, 트래픽로드 그리고 입력 파라미터로 구성된다. 본 절은 제안된 성능분석모델의 각각의 구성요소를 설명하였다.

1. 네트워크 컴퓨터의 큐잉 모델(IPSec 가속기 장착)

일반적인 M/M/1 큐잉모델에서 입력되는 서비스의 도착률(λ)과 프로세서의 처리량(μ, 처리시간 : 1/μ)을 이용하여 사용자가 서비스를 받기 위해 큐 안에서 대기하는 시간은 식 (1)과 같이 계산할 수 있다.[7] M/M/1 큐잉 시스템은 그림 1과 같다.

$$T_q = \frac{\lambda}{\mu(\mu-\lambda)} \quad (1)$$

식 (1)은 서비스들이 큐 내에서 대기하는 평균시간을 의미한다. 응답시간(response time)은 Little 법칙에 따라 큐 내에서의 대기시간과 프로세서에서의 처리시간을 합한 값이며 식 (2)와 같이 계산된다.[7] 이러한 응답시간은 성능분석의 기준이 된다.

$$T_s = \frac{1}{\mu} + \frac{\lambda}{\mu(\mu-\lambda)} \quad (2)$$

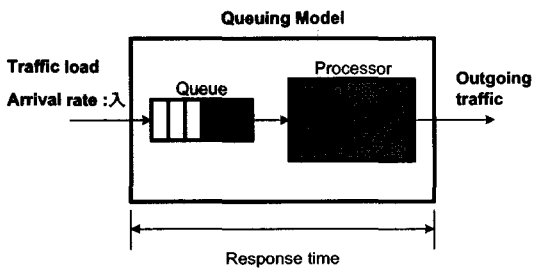


그림 1. 일반적인 큐잉 모델링(M/M/1 시스템)

현재 상용되는 IPSec 가속기는 PCI 인터페이스를 통해 네트워크 컴퓨터에 부착된다. PCI 기반 IPSec 가속기를 네트워크 컴퓨터에 장착했을 경우의 컴퓨터 내부 시스템은 그림 2와 같이 표현된다.

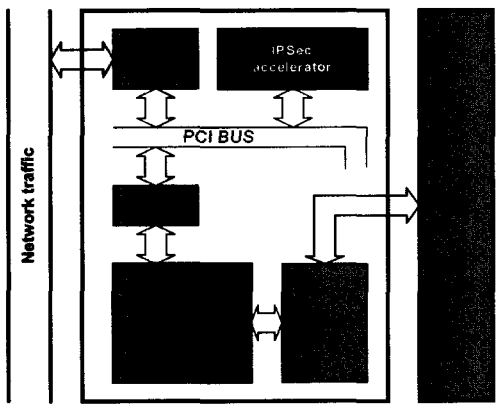


그림 2. IPSec 가속기를 장착한 네트워크 컴퓨터의 시스템 모형

CPU는 메모리로부터 명령을 패치한 뒤 해당 명령을 처리하게 된다. 네트워크 인터페이스 또는 IPSec 가속기는 메모리에 저장되어 있는 명령에 따라 운용된다. 운영체제(OS)는 메모리에서 어떠한 코드를 CPU로 넘겨줄 것인지를 결정한다. IPSec 가속기의 연산기능을 사용하기 위해서는 운영체제와 메모리 그리고 CPU 등의 도움을 받아야 한다. 따라서 IPSec 가속기를 장착한 네트워크 컴퓨터의 모델링을 위해서는 가속기의 성능뿐만 아니라 이상의 네트워크 컴퓨터 구성요소의 성능 또한 파라미터로 정의되어야 한다.

IPSec 가속기를 장착한 시스템을 M/M/1 시스템으로 모델링한 결과를 그림 3에서 나타내었다. 모델링을 통한 분석과정에서 실제 네트워크 트래픽 입력은 가상적인 트래픽 로드 입력으로 대체될 수 있다. 제안된 M/M/1 시스템의 큐(queue)는 IPSec 장착 시스템의 네트워크 인터페이스 입력부분에 해당된다. 즉, 제안된 모델의 큐는 트래픽 로드를 입력받는 부분에 설치하였다. IPSec 가속기는 M/M/1 시스템의 프로세서에 해당된다. IPSec 가속기는 1/μ의 처리시간을 갖는 프로세서로 대체하였다. 그 밖의 PCI버스, CPU, 메모리, 운영체제등 네트워크 트래픽의 입력부터 IPSec 가속기까지 데이터를 이동시키는 경로들은 하나의 통합된 파라미터인 디코딩 지연(decoding delay)으로 정의하여 모델링 하였다.

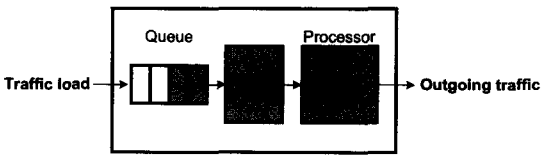


그림 3. IPSec 가속기 장착 시스템의 큐잉 모델링 결과

2. 트래픽로드

IPSec 가속기는 IPSec 프로토콜을 수행하기 위한 암호화 연산 시 운영체제 또는 보안 어플리케이션과 같은 소프트웨어상의 부하를 줄이기 위해 사용된다. 따라서 IPSec 가속기의 입력은 운영체제 또는 보안 어플리케이션의 연산실행 명령이다. 예를 들어 IPSec 가속기를 이용하여 3DES+SHA 과정을 수행하기 위해 운영체제는 CryptoAPI 등과 같은 간단한 함수를 이용하여 IPSec 가속기를 운용할 수 있다. 그리고 운영체제의 연산실행 명령은 네트워크 상으로 입력되는 패킷으로부터 활성화한다.

제안된 성능분석 모델의 트래픽로드는 포아송 분포를 갖는 것으로 보았다. 포아송 분포는 네트워크 트래픽을 모델링하기에 적합한 분포로 알려져 왔다. 하지만 1995년 Paxon과 Floyd의 연구 결과에 따르면 실제의 네트워크가 포아송 분포와는 차이가 있음을 밝히고 있다.[8] 하지만 세션연결을 위한 네트워크 트래픽의 경우, 10^3초의 시간대에서 포아송 분포가 관찰됨을 증명하였다. 세션연결이란 IPSec의 키 교환 프로토콜과 같이 상대방과의 보안연결 설정을 위해 초기 메시지를 전송하는 트래픽이 이에 해당된다. 따라서 포아송 분포는 IPSec 환경에서 트래픽로드로 모델링하기에 적합하다는 결론을 내릴 수 있다.

현재의 네트워크는 Paxson과 Floyd의 연구당시에 비하여 네트워크 속도 및 인터넷 사용자수의 획기적인 증가 추세에 있다. 세션연결 트래픽이 10^3초의 시간대에 이르면 포아송 분포를 따른다는 연구결과는 현재의 사정에 맞게 수정되어야 한다. 인터넷 이용자 및 호스트의 증가추세를 그림 4에서 나타내었다.

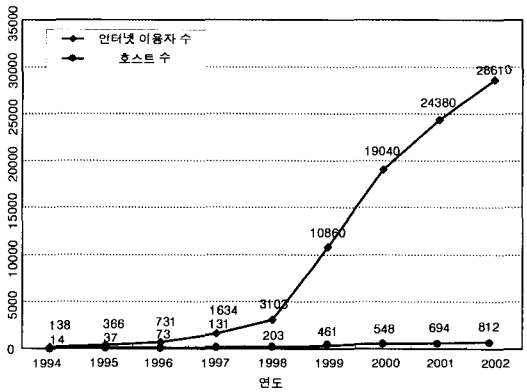


그림 4. 인터넷 이용률 증가 현황[9]

1995년 당시에 비하여 2002년의 인터넷 이용자는 78배가 증가하였다. 반면 호스트의 증가는 인터넷 사용자의 증가에 비해 적은 증가추세를 보였다. 1995년도의 경우 인터넷 사용자에 대한 호스트 수의 비는 10.11%이고 2002년의 경우 2.84%를 기록했다. 즉, 서비스를 요구하는 클라이언트의 수가 서버의 수에 비하여 크게 증가되었음을 확인할 수 있다. 따라서 서버에 대한 입력 트래픽 증가율을 식 (3)의 계산(UHR : user to host ratio)에 의해 얻어낼 수 있다.

Ethernet LAN의 경우 1995년 당시의 네트워

크 속도와 현재를 비교하면 100배 가량의 속도 발전이 이루어졌다(그림 5). 일반적으로 인터넷 전용선을 사용하는 사용자가 증가됨에 따라 1995년 당시 주로 사용했던 56kbps 모뎀과 비교하여 현재는 최소 Mbps 단위의 네트워크 대역폭으로 발전하였다. 결론적으로 현재의 네트워크 속도는 1995년과 비교하여 최소 20배 이상 증가하였음을 알 수 있다.

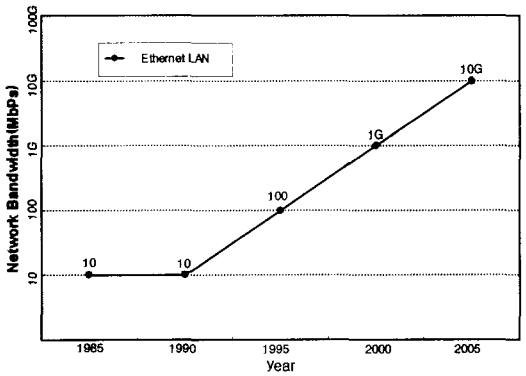


그림 5. 네트워크 전송속도의 발전 현황[10]

식 (3)의 UHR 증가량과 네트워크 속도 증가율을 모두 고려하면 포아송 분포를 나타내는 시간대는 5000배(≃277.67×20) 이상 감소된다. 즉, 포아송 분포의 발생은 1995년 당시의 10^3초를 보였지만 현재 네트워크상에서는 1초대에 발생될 수 있다는 결론이다. 본 논문에서는 최악조건을 감안하여 포아송 분포의 발생 시간대를 10초대로 결정하였다.

$$UHR = \frac{10.11}{2.84} \times 78 = 277.67 \qquad (3)$$

3. 입력 파라미터

제안된 성능분석 모델은 λ, 1/μ, 디코딩지연 이렇게 3개의 파라미터를 갖는다. λ는 제안된 모델로 입력되는 네트워크 패킷의 도착률을 의미한다. 본 논문에서 사용한 시뮬레이션 툴인 Anylogic 4.5에서 제공하는 포아송 분포 발생함수에 λ의 값이 입력된다. 1/μ는 프로세서의 처리시간이다. 이는 IPSec 가속기의 제시된 성능을 입력하였다. 제시된 성능은 IPSec 가속기 내부의 프로세서 최대 속도를 의미하므로 제안된 모델의 프로세서로 대체할 수 있다. 예를 들어 300Mbps의 처리량은 비트 당 약 3.3nsec의 처리시간을 갖는다.

본 논문에서는 기존의 M/M/1 시스템에서 사용되는 λ, μ 파라미터 외에 디코딩지연을 정의하였다. 네트워크로부터 패킷이 입력되어 IPSec 가속기까지 연산명령이 전달되는 과정을 그림 6에서 나타냈었다.

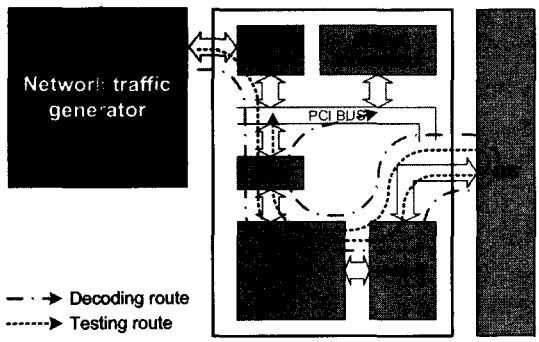


그림 6. IPSec 가속기 장착 네트워크 컴퓨터의 디코딩 과정 및 테스트 과정

제안된 모델링 과정에서 디코딩 루트(decoding route)에서 소요되는 시간을 디코딩지연이라 정의하였다. 네트워크 컴퓨터로 입력된 패킷은 네트워크 인터페이스를 거쳐 CPU의 연산명령처리에 의하여 메모리로 저장된다. CPU로 옮겨지는 과정에서 PCI 버스나 브리지를 거치게 된다. CPU의 연산명령처리는 네트워크 컴퓨터의 응용 소프트웨어에 의하여 제어된다. 이러한 응용 소프트웨어들은 운영체제(OS)의 명령에 따라 CPU의 사용권을 부여받은 뒤 실행된다. 이와 같이 디코딩지연은 네트워크 컴퓨터의 하드웨어 및 운영체제 등과 같은 성능변수에 따라 변화될 수 있다.

테스트 루트는 디코딩지연의 계산을 위해 설정하였다. 본 연구에서는 네트워크 컴퓨터의 디코딩지연 값을 얻기 위해 테스트 프로그램을 제작하였다. 테스트 프로그램은 테스트 루트에 따라 패킷을 인가한 뒤 내부 테스트 프로그램에 의해 다시 네트워크 인터페이스까지 패킷을 옮긴 후 이 동안의 전체시간을 계산한다. 네트워크 트래픽 발생기는 네트워크 컴퓨터로 패킷을 인가한다. 인가된 패킷은 테스트 루트를 거쳐 최종적으로 네트워크 인터페이스까지 도착하게 된다. 이 동안의 시간이 테스트 프로그램을 통해 얻어진 디코딩지연이다. 디코딩지연은 제안된 모델링의 파라미터 값으로 결정된다. 테스트 프로그램이 실행되는 모습을 그림 7과 그림 8에서 보였다.

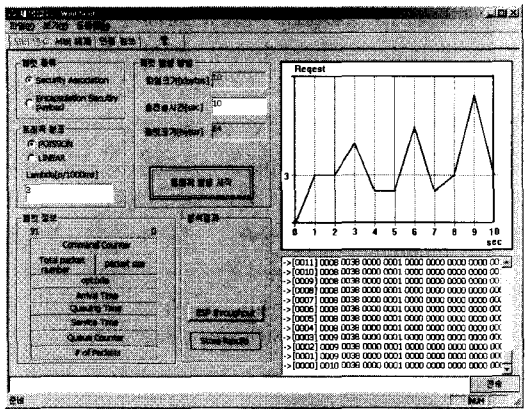


그림 7. 테스트 프로그램-트래픽발생기

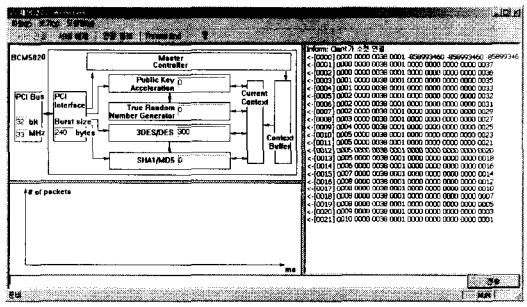


그림 8. 테스트 프로그램-테스트 루트

Ⅲ. 성능분석 모델 및 시뮬레이션 결과

본 절은 제안된 성능분석 모델을 바탕으로 BCM 5820 IPSec 가속기를 네트워크 컴퓨터에 장착하였을 경우로 가정하여 시뮬레이션 한 결과를 설명한다. 시뮬레이션 결과는 Miltchev의 연구[3]에서 수행한 BCM5820 IPSec 가속기를 장착한 네트워크 컴퓨터의 장비측정을 이용한 성능분석 결과와 비교하였다.

1. 파라미터 결정

제안된 성능분석모델의 파라미터 값을 표 1에서 정리하였다. 본 논문에서는 BCM5820 IPSec 가속기의 연산기능 중 3DES+SHA를 이용하였다. BCM5820의 3DES+SHA의 성능(μ)은 300Mbps이다. 이 값을 제안된 모델링에 적용하기 위해 1/μ로 계산하면 0.33nsec/bit이다. 도착률 λ는 Anylogic4.5에서 제공하는 DistriPossion.sample (1/λ) 함수로 발생시킬 수 있다. λ는 0.4msec로 결정하였다. 0.4msec는 서비스 도착간격을 의미한다. 이 수치는 초당 2500개의 패킷이 입력됨과 같은 의미이며 만약 패킷의 크기가 40kbyte라면 1Gbps의 네트워크 대역폭을 갖는다고 가정할 수 있다. 디코딩지연은 제안된 테스트 프로그램을 이용하여 평균 0.5msec의 결과를 얻었다. 테스트 프로그램은 Miltchev의 연구와의 결과비교를 위해 표 1에서 정리한 하드웨어 및 운영체제를 갖는 네트워크 컴퓨터에서 구동되었다. Miltchev의 연구에서 사용된 테스트환경은 구체적으로 표 2에서 보였다.

표 1. 디코딩지연을 구하기 위한 테스트 프로그램 구동환경

구 분	IPSec 가속기를 장착한 네트워크 컴퓨터		Model parameter
하드웨어	CPU	1GHz Intel P3 processor	디코딩지연 : 0.5msec
	Memory	256MB PC133 SDRAM	
	Hard drive	40GB	
운영체제	OS	Windows2000 PRO	

표 2. Miltchev의 연구에서 사용된 테스트환경[3]

구 분	Performance variable	value
네트워크	Bandwidth	1Gbps(host-to-host)
가속장치	IPSec 가속기	BCM5820
하드웨어	CPU	1GHz Intel P3 processor
	Memory	256MB PC133 SDRAM
	Hard drive (DISK)	10GB WDP IDE
	Network adapter	Intel PRO/1000 F
	Mother board	Supermicro 370DE6 Server Works ServersetIII HE-SL chipset with daul PCI buses
운영체제	OS	OpenBSD 3.0

2. 시뮬레이션 결과

시뮬레이션을 통해 얻고자 하는 결과는 패킷크기에 따른 제안된 성능분석모델의 처리율(throughput)이며 단위는 Mbps로 결정하였다. 시뮬레이션 툴은 Anylogic4.5를 이용하였으며 시뮬레이션 과정

에서 발생되는 부하를 분배하기 위해 그림 9와 같이 두 단계로 나누어 진행하였다. 시뮬레이션 1의 결과는 시뮬레이션 2의 파라미터로 입력된다. 첫 번째 단계는 제안된 성능분석모델로 50kbyte의 데이터를 패킷크기로 나누어 전송하였을 경우의 패킷크기마다 얼마의 총 처리시간이 소요되는지를 시뮬레이션 하였다. 두 번째 단계로 단계 1의 결과와 포아송 분포 및 큐잉이론을 제안된 모델에 적용하여 시뮬레이션 하였다.

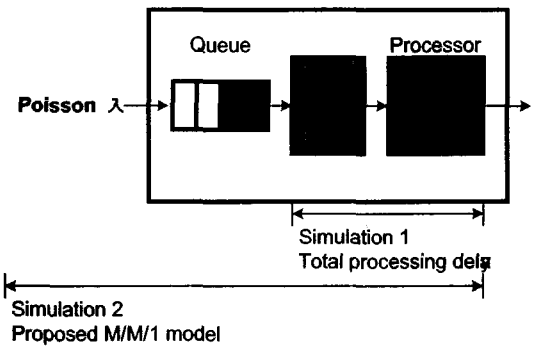


그림 9. 제안된 성능분석 모델의 단계별 시뮬레이션

50kbyte파일을 패킷의 크기에 따라 시뮬레이션 하였을 경우의 패킷별 총 처리시간을 표 3에서 정리하였다. BCM5820의 3DES+SHA 수행속도는 300Mbps(μ)이고 50kbyte파일을 처리하는 시간은 평균 1.333msec를 기록했다. 패킷크기가 64byte인 경우 50kbyte 파일은 총 782개의 패킷으로 나누어 전송되었다. 패킷크기가 증가할수록 디코딩회수가 감소하였고 총 처리시간이 감소하였다.

패킷의 크기(64byte~65546byte)에 따라 각각 시뮬레이션 1의 결과로 얻은 총 처리시간을 달리 적용하여 시뮬레이션을 반복하였다. 반복 회수는 패킷크기마다 각각 100회이며 결과는 시뮬레이션 반복 후 평균값으로 결정하였다. 시뮬레이션 결과와 Miltchev의 연구에서 얻어진 결과를 그림 10에서 나타내었다. 두 결과의 차이는 평균 15.4%이다. 특히 패킷의 크기가 8192바이트 이하의 경우 평균 13.3%의 차이만을 보였다. 현재 네트워크상의 패킷크기는 메시지 전송기준(message transmission unit)의 경우 최대 1500byte, 미디어 스트리밍기준(media streaming unit)은 820byte 의 패킷크기가 가장 많은 분포를 보이고 있다.[11]

표 3. 패킷 크기에 따른 처리시간

(단위 : msec)

64	782		391.0		392.333
128	391		195.5		196.833
256	196		98.0		99.333
512	98		49.0		50.333
1024	49		24.5		25.833
2048	25	0.5	12.5	1.333	13.833
4096	13		6.5		7.833
8192	7		3.5		4.833
16384	4		2.0		3.333
32768	2		1.0		2.333
65536	0		0.0		1.333

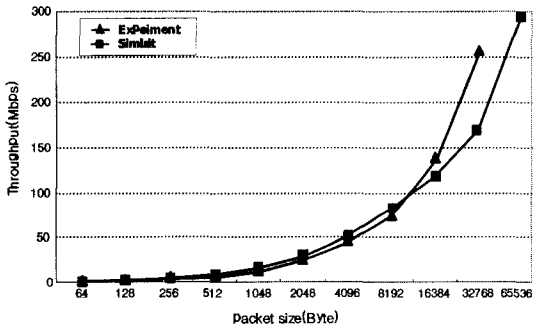


그림 10. 성능분석 결과
Miltchev의 연구[3]: Experiment
제안된 성능분석 모델: Simulation

Ⅳ. 결 론

제안된 성능분석 모델을 이용한 시뮬레이션 결과 실제 장비를 통해 측정한 데이터와 15% 정도의 차이만을 보였다. 이는 제안된 성능분석 모델의 구성요소 즉, 큐잉모델과 트래픽 로드 그리고 모델 파라미터 값이 IPSec 가속기를 장착한 네트워크 컴퓨터와 유사하게 모델링 되었다는 것을 의미한다. 모델 파라미터 중 디코딩지연은 IPSec 가속기를 장착하고자 하는 네트워크 컴퓨터의 성능에 따라 변경된다. 본 연구에서 제작한 테스트 프로그램으로 디코딩지연 값를 얻을 수 있었다. 분석결과(장비측정[3]과 15%정도의 차이)를 미루어 볼 때 디코딩지연 값이 비교적 정확하게 측정되었음을 알 수 있었다.

IPSec은 IPv6에서 필수적으로 제공하는 프로토

콜이며 따라서 IPSec 가속기의 이용량이 증가될 전망이다. 특히 인터넷 보안서버는 많은 양의 IPSec 연산을 요구하며 그 만큼 IPSec 가속기의 고속연산 수행이 서버운용상 중요한 관건이 된다. 제안된 모델을 이용한 성능분석 결과는 IPSec 가속기의 최대성능을 유지하기 위한 서버내의 하드웨어들의 적합한 구조를 제시하고 나아가 고속 네트워크 컴퓨터의 통계적 설계공간탐색에 이용될 수 있다.

참 고 문 헌

[1] M. Merkow and J. Breithaupt, The Complete Guide to Internet Security, AMACOM, 2000.

[2] M. McLoone and J.V. McCanny, "A single-chip IPSec cryptographic processor," IEEE Workshop on Signal Processing Systems, pp. 133-138, Oct. 2002.

[3] S. Miltchev and S. Ioannidis, "A study of the relative costs of network security protocols," In Proceedings of USENIX Annual Technical Conf., Freenix Track, pp. 41-48, June 2002.

[4] I. Cao and M. Anderson, "Web server performance modeling using an M/G/1/K* PS queue," 10th Int'l. Conf. on Telecommunications, vol. 2, pp. 1501-1506, Feb. 2003.

[5] A.V. Borshchev and Y.G. Karpov, "System modeling, simulation and analysis using COVERS active objects," IEEE Workshop on Engineering of Computer Based Systems (ECBS '97), pp. 220-227, Mar 1997.

[6] XJ Technologies, Anylogic4.5 Product Overview, http://www.xjtek.com.

[7] 이호우, 대기행렬이론-확률과정론적 분석, 시그마프레스, 1998.

[8] V. Paxson and S. Floyd, "The failure of Poisson modeling," IEEE/ACM Trans on Networking, vol. 3, pp. 226-244, June 1995.

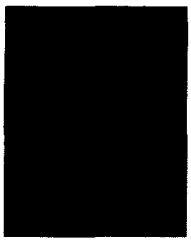
[9] 한국전산원, 2002 국가정보화백서

[10] 윤문길, 인터넷 접속기술, http://mslab.hau.ac.kr/it_02/4.ppt

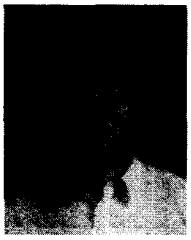
[11] C. Fraleigh and S. Moon, "Packet-level traffic measurements from the SPRINT IP backbone," IEEE Journal of Network, vol. 17, pp. 6-16, Nov. 2003.

[12] Broadcom Co., BCM5820 Product Brief http://www.broadcom.com/collateral/pb/5820-PB04-R.pdf

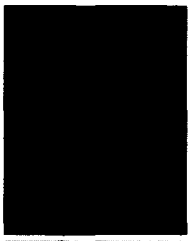
〈著者紹介〉



윤 연 상 (Yeonsang Yun) 학생회원
2004년 2월 : 충북대학교 전기전자공학부 학사
2004년 3월~현재 : 충북대학교 정보통신공학과 석사과정
〈관심분야〉 디지털 회로설계 및 테스트, 임베디드 프로그래밍, 암호 시스템

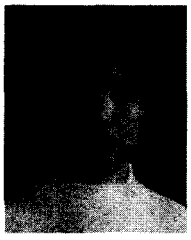


류 광 현 (Kwang-Hyun Ryoo) 학생회원
1998년 2월 : 충북대학교 정보통신공학과 학사
2000년 3월~현재 : 충북대학교 정보통신공학과 석사과정
2003년 10월~현재 : 한성텔레콤(주) 기술연구소 전임연구원
〈관심분야〉 전자공학, 이미지 처리, 암호 시스템



박 진 섭 (Jinsub Park) 학생회원
2004년 8월 : 충북대학교 전기전자공학부 학사
2004년 9월~현재 : 충북대학교 정보통신공학과 석사과정
〈관심분야〉 디지털 회로설계, 암호 시스템

김 용 대 (Yongdae Kim) 학생회원
1990년 2월 : 충북대학교 정보통신공학과 학사
1993년 2월 : 충북대학교 컴퓨터공학과 석사
1989~1998년 : 신흥기술연구소 팀장
2000~현재 : 충북대학교 정보통신공학과 박사과정
〈관심분야〉 Computer arithmetic, ASIC 설계, 암호 시스템



한 선 경 (Yongdae Kim) 학생회원
1991년 2월 : 충북대학교 정보통신공학과 학사
1993년 2월 : 충북대학교 정보통신공학과 석사
1995~현재 : 충북대학교 정보통신공학과 박사과정
〈관심분야〉 Computer arithmetic, Cryptographic system, ASIC 설계

유 영 갑 (Younggap You) 정회원
1975년 : 서강대학교 전자공학과 학사
1975~1979년 : 국방과학연구소 연구원
1981년 : Univ.of Michigan, Ann Arbor 전기전산학과 석사
1986년 : Univ.of Michigan, Ann Arbor 전기전산학과 박사
1986~1988년 : 금성반도체 (주) 책임 연구원
1993~1994년 : 아리조나 대학교 객원교수
1998~2000년 : 오레곤 주립대학교 교환교수
1988~현재 : 충북대학교 정보통신공학과 교수(컴퓨터정보통신연구소)
〈관심분야〉 VLSI 설계 및 테스트, 고속 인쇄회로 설계, 암호학